ICOM

取扱説明書

PoE HUB

VE-SW8

IEEE802.3at/IEEE802.3af規格準拠

はじめに

1 ご使用になる前に

2 Configurationメニュー

3 Monitorメニュー

4 Diagnosticsメニュー

5 Maintenanceメニュー

6 ご参考に

Icom Inc.

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

はじめに

このたびは、本製品をお買い上げいただきまして、まことにありがとうございます。
本製品は、IEEE802.3at規格、IEEE802.3af規格に準拠した8ポートHUBです。
ご使用の前に、この取扱説明書をよくお読みいただき、本製品の性能を十分発揮していただくとともに、末長くご愛用くださいますようお願い申し上げます。

登録商標/著作権

本書の表記について

本書は、次の表記規則にしたがって記述しています。
「　」表記：本製品の各メニューと、そのメニューに属する設定画面の名称を(「 」)で囲んで表記します。
[　]表記：各設定画面の設定項目名を([ ])で囲んで表記します。
〈　〉表記：設定画面上に設けられたコマンドボタンの名称を(〈 〉)で囲んで表記します。
※本書は、PoE v2.1.5のファームウェアを使用して説明しています。
※本書では、Windows 10の画面を例に説明しています。
※本書中の画面は、OSのバージョンや設定によって、お使いになるパソコンと多少異なる場合があります。
※本製品の仕様、外観、その他の内容については、改良のため予告なく変更されることがあり、本書の記載とは一部異なる場合があります。

本製品の特長について

◎IEEE802.3at規格/IEEE802.3af規格準拠の8ポートHUB
※1ポートあたり最大30W、機器全体では120Wまで給電可能
◎Comboポート(LAN/SFP：光ケーブル接続)搭載
◎SFPポートの動作状態監視

出荷時のおもな設定値

本体IPアドレス	：192.168.2.1/24	(Configuration > System > IP > IP Interfaces)
デフォルトゲートウェイ	：192.168.2.254	(Configuration > System > IP > IP Routes)
内部時計の自動設定	：Disabled(無効)	(Configuration > System > NTP > Mode)
NTPサーバー	：空白(未設定)	(Configuration > System > NTP > Server)
タイムゾーン	：空白(未設定)	(Configuration > System > Time > Time Zone)
DHCPサーバー機能	：Disabled(無効)	(Configuration > DHCPv4 > Server > Mode > Global Mode)
管理者ID	：admin	(Configuration > Security > Switch > Users > admin)
管理者パスワード	：admin	(Configuration > Security > Switch > Users > admin)

不正アクセス防止のアドバイス
本製品に設定するすべてのパスワードは、容易に推測されないものにしてください。
数字だけでなくアルファベット(大文字/小文字)や記号などを組み合わせた長く複雑なものにされることをおすすめします。

三和システムサービス株式会社
〒330-0854　埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211　FAX 048-653-2217

1章　ご使用になる前に

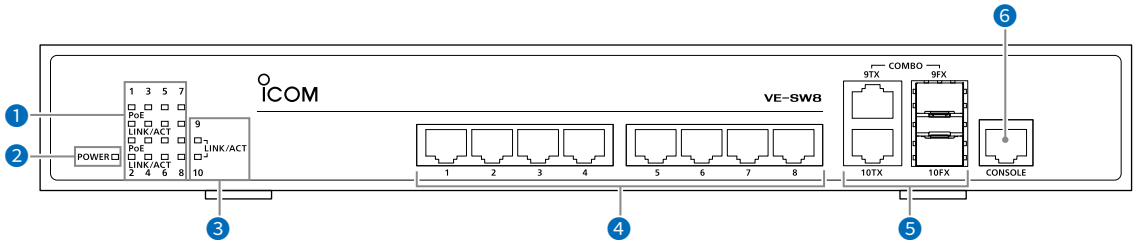
各部の名称と機能…… **1-2**
前面部…… 1-2
後面部…… 1-3

設定のしかた…… **1-4**
設定用のパソコンに固定IPアドレスを設定する …… 1-4
設定画面にアクセスするには…… 1-5
設定画面の名称と機能について…… 1-6
本体IPアドレスを変更する …… 1-7
内部時計を設定する…… 1-8
パスワードを変更する…… 1-9

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

各部の名称と機能

前面部



❶ PoEポートランプ(1～8) ……

PoE
- 橙点灯：給電時
- 消　灯：未給電時★

LINK/ACT
- 緑点灯：リンク時
- 緑点滅：データ通信中
- 消　灯：リンク未確立時

❷ POWERランプ.....

- 橙点灯：電源ON時
- 消　灯：電源OFF時

❸ Comboポートランプ(9～10)

LINK/ACT
- 緑点灯：リンク時
- 緑点滅：データ通信中
- 消　灯：リンク未確立時

❹ PoEポート(1～8) ……

PoE給電に対応したポートです。ネットワーク機器のLANポートとLANケーブルで接続します。
※PoE受電機能対応のネットワーク機器を接続する場合は、カテゴリー5e以上のLANケーブルをご用意ください。

❺ Comboポート(9～10) ……

Comboポートは、LANポート(TX)とSFPポート(FX)の1組で、どちらか一方を選択して使用します。
SFPポートに別売のSFPトランシーバーを取り付けると、光ファイバーケーブルを接続できます。(P.6-8)
※このポートに給電機能はありません。

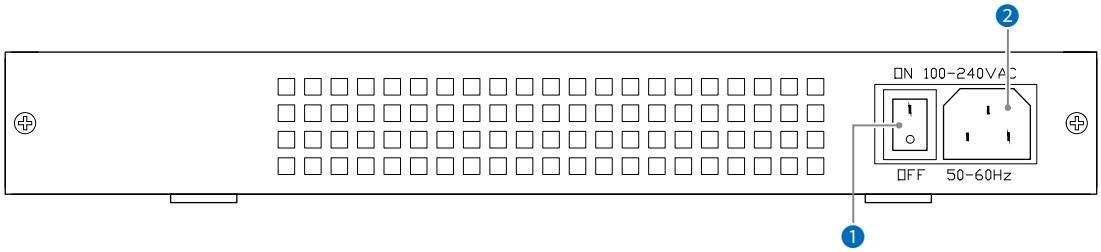
❻ CONSOLEポート ……

設定用のポートです。ターミナルソフトウェアを使用して本製品を設定にするときに、市販のUSBコンソールケーブル(RJ-45タイプ)でパソコンと接続します。

★PoEポート単体の給電電力が上限(30W)を超える場合、または装置全体で給電電力が120Wを超える場合は、橙点滅になります。

各部の名称と機能

後面部



❶ **電源スイッチ** …… 本製品の電源をON/OFFするスイッチです。
※電源ケーブルを接続してから、スイッチをONにしてください。

❷ **電源コネクター** …… 本製品に付属の電源ケーブルを接続します。

三和システムサービス株式会社
〒330-0854　埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211　FAX 048-653-2217

設定のしかた

出荷時、本製品のIPアドレスは「192.168.2.1」、DHCPサーバー機能は「無効」に設定されています。
本製品の設定画面にアクセスするときは、接続するパソコンに固定IPアドレスの設定が必要です。

設定用のパソコンに固定IPアドレスを設定する

Windows 10を例に、固定IPアドレス(例：192.168.2.100)をパソコンに設定する手順について説明します。

1 〈スタート〉(ロゴボタン)で右クリックし、表示されたメニューで[ネットワーク接続(W)]をクリックします。

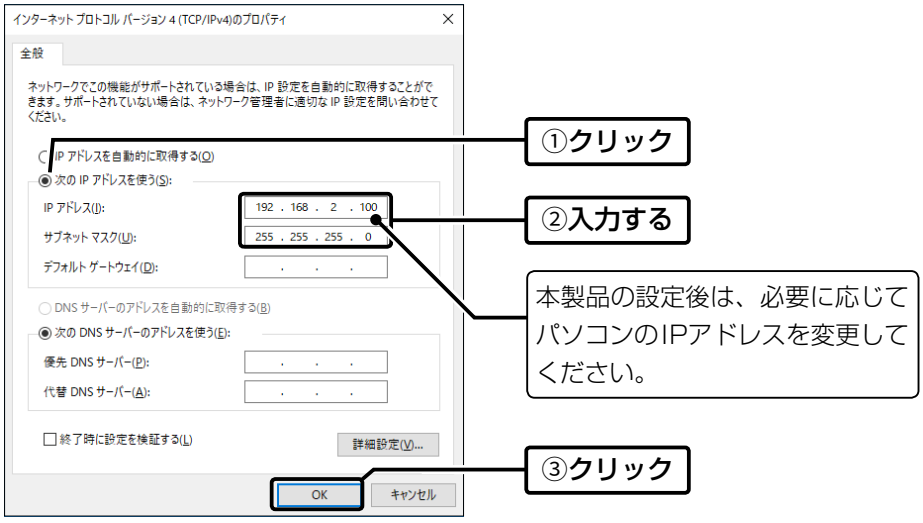
2 [アダプターのオプションを変更する]をクリックします。

3 [イーサネット]を右クリックし、表示されたメニューで[プロパティ(R)]をクリックします。

4 [ユーザーアカウント制御]のメッセージが表示された場合は、〈続行(C)〉をクリックします。

5 「イーサネットのプロパティ」画面で、[インターネットプロトコル バージョン4(TCP/IPv4)]を選択し、〈プロパティ(R)〉をクリックします。
「インターネット プロトコル バージョン 4 (TCP/IPv4)のプロパティ」画面(別画面)が表示されます。

6 [次のIPアドレスを使う(S)]をクリックし、[IPアドレス(I)](例：192.168.2.100)と[サブネットマスク(U)](例：255.255.255.0)を入力して、〈OK〉をクリックします。



7 〈OK〉をクリックします。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

1 ご使用になる前に

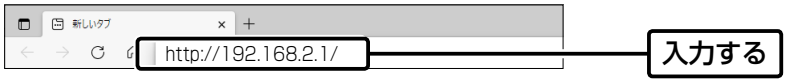
設定のしかた

設定画面にアクセスするには

本製品に接続したパソコンのWWWブラウザーから、本製品の設定画面にアクセスする手順について説明します。

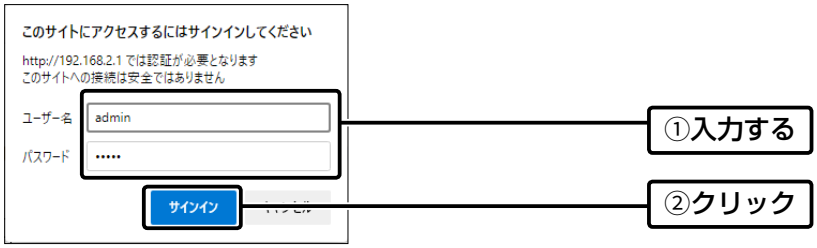
1 WWWブラウザーを起動します。

2 本製品に設定されたIPアドレスをWWWブラウザーのアドレスバーに入力します。
出荷時、本製品のIPアドレスは「192.168.2.1」に設定されています。



3 [Enter]キーを押します。
[ユーザー名]と[パスワード]を求める画面が表示されます。

4 [ユーザー名]欄に「admin」、[パスワード]欄に「admin」(出荷時の設定)を入力し、〈サインイン〉をクリックすると、設定画面が表示されます。



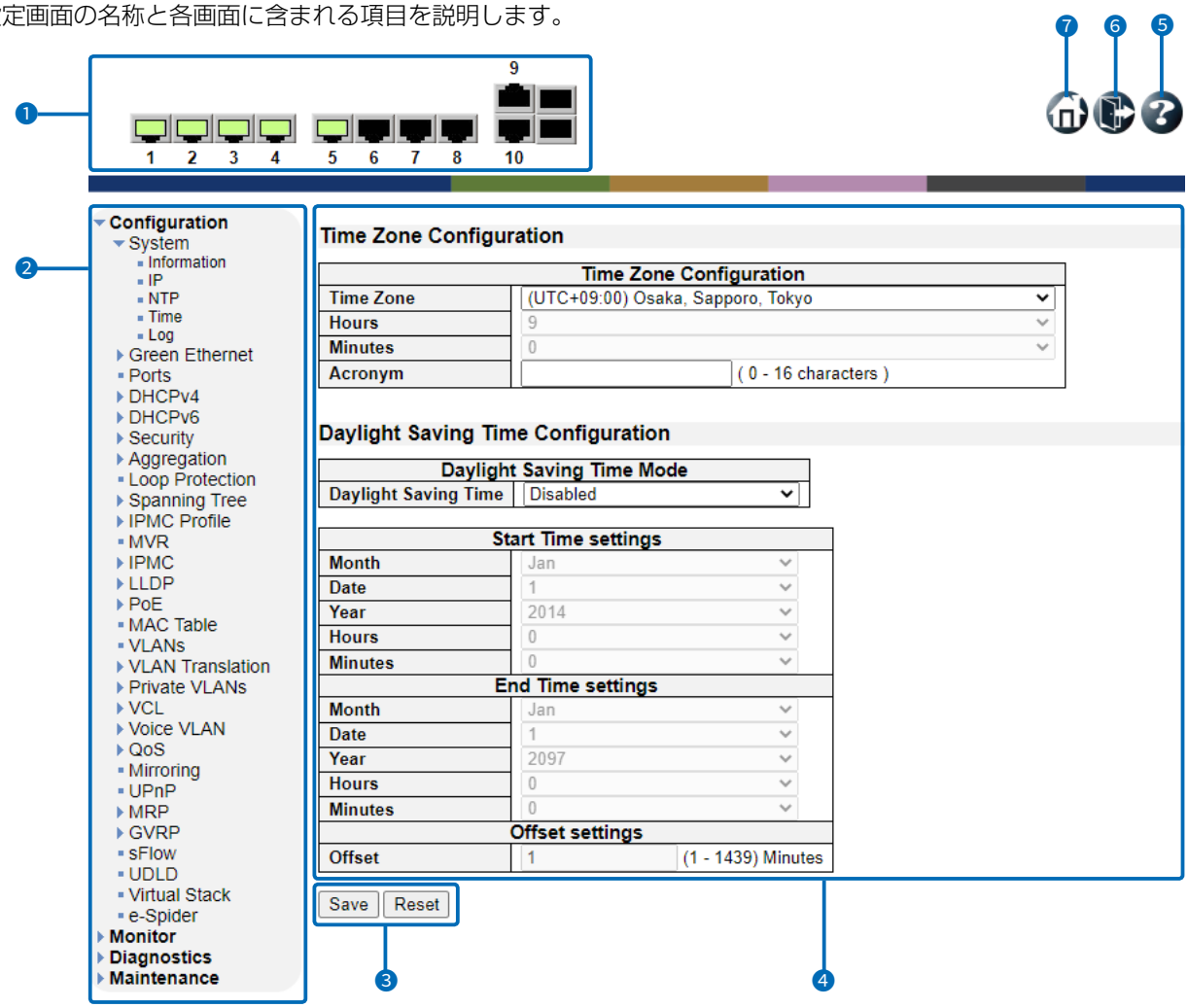
WWWブラウザーについて
本書の説明では、Microsoft Edge (Chromiumベース)を使用しています。
※設定画面が正しく表示できるように、WWWブラウザーのJavaScript機能およびCookieは有効にしてください。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

設定のしかた

設定画面の名称と機能について

設定画面の名称と各画面に含まれる項目を説明します。



❶ ポート状態表示 ……

各ポートの状況が表示されます。
（消灯：リンク未確立時、緑点灯：リンク時、灰点灯：ポート無効時）
クリックすると、そのポートの「Detailed Statistics」画面（P.3-15）へ移動します。

❷ 設定画面選択メニュー ……

各メニューのタイトル上にマウスポインターを合わせてクリックすると、そのメニューに含まれる設定画面へのリンクが表示されます。

❸ 設定ボタン ……

設定した内容の登録や取り消しをします。
※表示画面によって、表示されるボタンの種類や位置が異なります。

❹ 設定画面表示エリア ……

［設定画面選択メニュー］で選択したメニューに含まれる設定画面へのリンク（例：Configuration→Time）をクリックしたとき、その内容が表示されます。

❺ ヘルプボタン ……

設定画面のヘルプ（英文）を確認するときにクリックします。

❻ ログアウトボタン ……

設定画面からログアウトするときにクリックします。

❼ ホームボタン ……

「Information」画面（P.3-5）に戻るときにクリックします。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

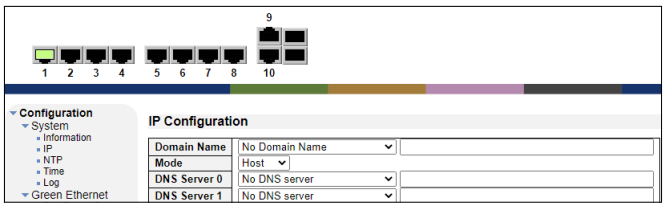
設定のしかた

Configuration > System > IP

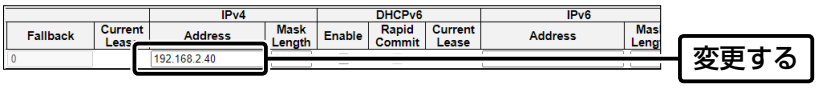
本体IPアドレスを変更する

既存のネットワークと重複しないように、本製品のIPアドレスを変更します。
※各画面で保存した変更内容は、再起動(電源再投入)するまで有効です。
　再起動後も有効にする場合は、〈Save Configuration〉(手順5)をクリックしてください。

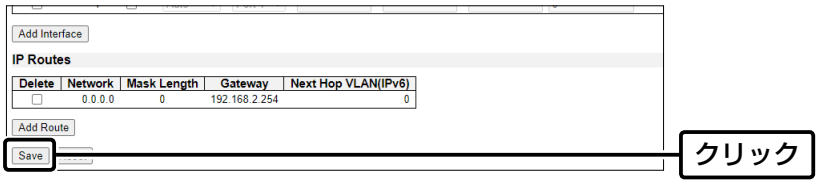
1 「Configuration」→「System」→「IP」の順でクリックします。
「IP」画面が表示されます。



2 [IP Interfaces]項目の[IPv4]欄で設定を変更します。(例：192.168.2.40)

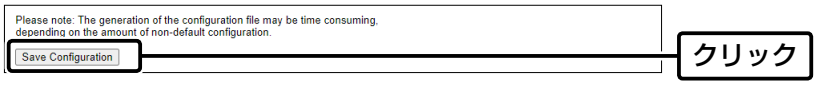


3 「IP」画面の〈Save〉をクリックします。
変更した内容が有効になります。



4 「Maintenance」→「Configuration」→「Save startup-config」の順でクリックします。
「Save startup-config」画面が表示されます。

5 「Save startup-config」画面の〈Save Configuration〉をクリックします。
※再起動後も、変更した内容が有効になります。



三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

設定のしかた

Configuration > System > NTP

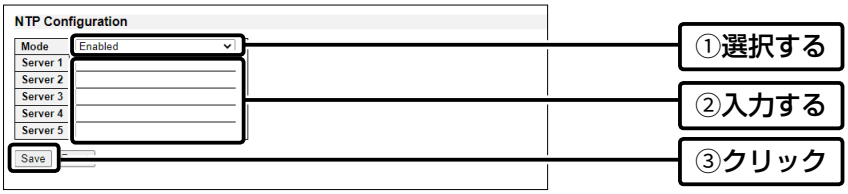
Configuration > System > Time

内部時計を設定する

本製品の内部時計を正確に表示させるため、NTPサーバーとタイムゾーンを設定されることをおすすめします。
※各画面で保存した変更内容は、再起動(電源再投入)するまで有効です。
　再起動後も有効にする場合は、〈Save Configuration〉(手順6)をクリックしてください。

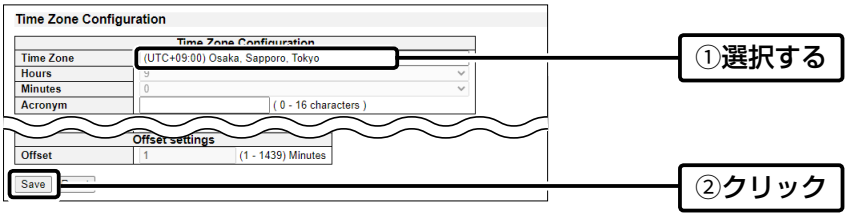
1 「Configuration」→「System」→「NTP」の順でクリックします。
「NTP」画面が表示されます。

2 [NTP Configuration]項目の[Mode]欄で「Enabled」(有効)を選択、
アクセスするNTPサーバーのIPアドレス(最大5件)を入力して、「NTP」画面の〈Save〉をクリックします。
NTPサーバーにアクセスできると、内部時計が設定されます。



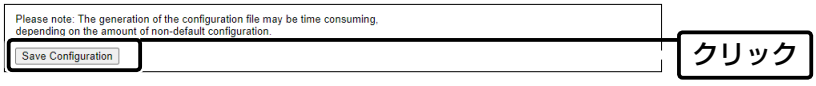
3 「Configuration」→「System」→「Time」の順でクリックします。
「Time」画面が表示されます。

4 [Time Zone Configuration]項目の[Time Zone]欄でタイムゾーンを選択し、
「Time」画面の〈Save〉をクリックします。
選択したタイムゾーンの時差が内部時計に反映されます。



5 「Maintenance」→「Configuration」→「Save startup-config」の順でクリックします。
「Save startup-config」画面が表示されます。

6 「Save startup-config」画面の〈Save Configuration〉をクリックします。
※再起動後も、変更した内容が有効になります。



ご注意
自動的に内部時計を設定するために、NTPサーバーへの問い合わせ先(経路)設定が必要です。

三和システムサービス株式会社
〒330-0854　埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211　FAX 048-653-2217

設定のしかた

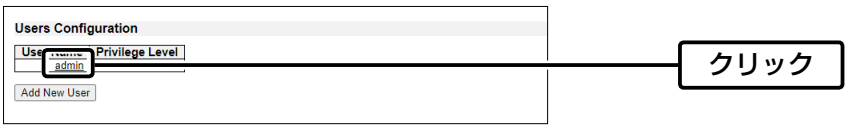
Configuration > Security > Switch > Users

パスワードを変更する

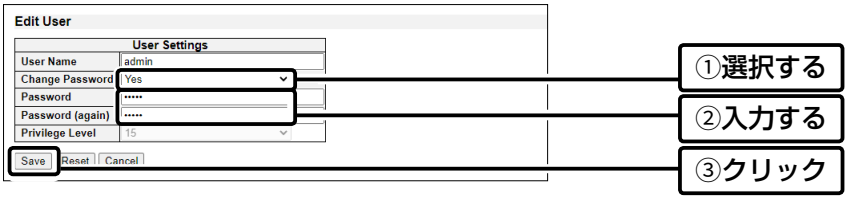
出荷時、本製品の設定画面には、ユーザー名「admin」、パスワード「admin」でアクセスできます。
パスワードを設定することで、管理者以外がWWWブラウザーから本製品の設定を変更できないようにします。
※各画面で保存した変更内容は、再起動(電源再投入)するまで有効です。
　再起動後も有効にする場合は、〈Save Configuration〉(手順5)をクリックしてください。

1 「Configuration」→「Security」→「Switch」→「Users」の順でクリックします。
「Users」画面が表示されます。

2 [Users Configuration]項目の[User Name]欄で「admin」をクリックします。
編集画面が表示されます。

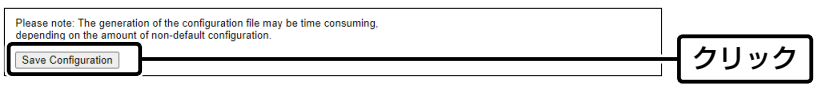


3 [User Settings]項目の[Change Password]欄で「Yes」を選択し、
任意の英数字/記号(半角31文字以内)で新しいパスワードを入力して、「Users」画面の〈Save〉をクリックします。



4 「Maintenance」→「Configuration」→「Save startup-config」の順でクリックします。
「Save startup-config」画面が表示されます。

5 「Save startup-config」画面の〈Save Configuration〉をクリックします。
※再起動後も、変更した内容が有効になります。



不正アクセス防止のアドバイス
本製品に設定するすべてのパスワードは、容易に推測されないものにしてください。
数字だけでなくアルファベット(大文字/小文字)や記号などを組み合わせた長く複雑なものに変更されることをおすすめします。

ご注意
管理者パスワードを忘れた場合、設定画面にアクセスするには、工場出荷時(初期値)の状態に戻す必要があります。
※6-7ページにしたがって、本製品本体で初期化操作をしてください。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

2章 Configurationメニュー

「Information」画面 …… 2-7
System Information Configuration …… 2-7

「IP」画面 …… 2-8
IP Configuration …… 2-8
IP Interfaces …… 2-10
IP Routes …… 2-13

「NTP」画面 …… 2-14
NTP Configuration …… 2-14

「Time」画面 …… 2-15
Time Zone Configuration …… 2-15
Daylight Saving Time Configuration …… 2-16

「Log」画面 …… 2-18
System Log Configuration …… 2-18

「Port Power Savings」画面 …… 2-19
Port Power Savings Configuration …… 2-20

「Ports」画面 …… 2-21
Port Configuration …… 2-21

「Mode」画面 …… 2-25
DHCP Server Mode Configuration …… 2-25

「Excluded IP」画面 …… 2-26
DHCP Server Excluded IP Configuration …… 2-26

「Pool」画面 …… 2-27
DHCP Server Pool Configuration …… 2-27

「Pool Configuration」画面 …… 2-28
DHCP Pool Configuration …… 2-28

「Snooping」画面 …… 2-31
DHCP Snooping Configuration …… 2-31
Port Mode Configuration …… 2-31

「Relay」画面 …… 2-32
DHCP Relay Configuration …… 2-32

「Snooping」画面 …… 2-34
DHCPv6 Snooping Configuration …… 2-34

「Relay」画面 …… 2-36
DHCPv6 Relay Configuration …… 2-36

「Users」画面 …… 2-37
Users Configuration …… 2-37

「Add User」画面/「Edit User」画面 …… 2-38
Add User/Edit User …… 2-38

「Privilege Levels」画面 …… 2-39
Privilege Level Configuration …… 2-39

「Auth Method」画面 …… 2-40
Authentication Method Configuration …… 2-40
Command Authorization Method Configuration …… 2-41
Accounting Method Configuration …… 2-42

「SSH」画面 …… 2-43
SSH Configuration …… 2-43

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

下記は、前ページからのつづきです。

「HTTPS」画面 …… 2-44
HTTPS Configuration …… 2-44
「Access Management」画面 …… 2-46
Access Management Configuration …… 2-46
「System」画面 …… 2-47
SNMP System Configuration …… 2-47
「Destinations」画面 …… 2-48
Trap Configuration …… 2-48
「SNMP Trap Configuration」画面 …… 2-49
SNMP Trap Configuration …… 2-49
「Sources」画面 …… 2-51
Trap Configuration …… 2-51
「Communities」画面 …… 2-52
SNMPv3 Community Configuration …… 2-52
「Users」画面 …… 2-53
SNMPv3 User Configuration …… 2-53
「Groups」画面 …… 2-55
SNMPv3 Group Configuration …… 2-55
「Views」画面 …… 2-56
SNMPv3 View Configuration …… 2-56
「Access」画面 …… 2-57
SNMPv3 Access Configuration …… 2-57
「Statistics」画面 …… 2-58
RMON Statistics Configuration …… 2-58
「History」画面 …… 2-59
RMON History Configuration …… 2-59
「Alarm」画面 …… 2-60
RMON Alarm Configuration …… 2-60
「Event」画面 …… 2-62
RMON Event Configuration …… 2-62
「Port Security」画面 …… 2-63
Port Security Configuration …… 2-63
「NAS」画面 …… 2-66
Network Access Server Configuration …… 2-67
「Ports」画面 …… 2-78
ACL Ports Configuration …… 2-78
「Rate Limiters」画面 …… 2-80
ACL Rate Limiter Configuration …… 2-80
「Access Control List」画面 …… 2-81
Access Control List Configuration …… 2-81

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

下記は、前ページからのつづきです。

「ACE Configuration」画面 …… 2-83
ACE Configuration …… 2-83
MAC Parameters …… 2-86
VLAN Parameters …… 2-87
ARP Parameters …… 2-88
IP Parameters …… 2-91
IPv6 Parameters …… 2-93
ICMP Parameters/ICMPv6 Parameters …… 2-95
UDP Parameters/UDPv6 Parameters/TCP Parameters/TCPv6 Parameters …… 2-96
Ethernet Type Parameters …… 2-98

「Configuration」画面 …… 2-99
IP Source Guard Configuration …… 2-99
Port Mode Configuration …… 2-99

「Static Table」画面 …… 2-100
Static IP Source Guard Table …… 2-100

「Configuration」画面 …… 2-101
IPv6 Source Guard Configuration …… 2-101

「Static Table」画面 …… 2-102
IPv6 Source Guard Static Table …… 2-102

「Port Configuration」画面 …… 2-103
ARP Inspection Configuration …… 2-103
Port Mode Configuration …… 2-104

「VLAN Configuration」画面 …… 2-105
VLAN Mode Configuration …… 2-105

「Static Table」画面 …… 2-106
Static ARP Inspection Table …… 2-106

「Dynamic Table」画面 …… 2-107
Dynamic ARP Inspection Table …… 2-107

「RADIUS」画面 …… 2-108
RADIUS Server Configuration …… 2-108

「TACACS+」画面 …… 2-110
TACACS+ Server Configuration …… 2-110

「Common」画面 …… 2-112
Common Aggregation Configuration …… 2-112

「Groups」画面 …… 2-113
Aggregation Group Configuration …… 2-113

「LACP」画面 …… 2-114
LACP System Configuration …… 2-114
LACP Port Configuration …… 2-114

「Loop Protection」画面 …… 2-115
Loop Protection Configuration …… 2-115

「Bridge Settings」画面 …… 2-117
STP Bridge Configuration …… 2-117

「MSTI Mapping」画面 …… 2-120
MSTI Configuration …… 2-120

下記は、前ページからのつづきです。

「MSTI Priorities」画面 …… 2-122
MSTI Configuration …… 2-122
「CIST Ports」画面 …… 2-123
STP CIST Port Configuration …… 2-123
「MSTI Ports」画面 …… 2-125
MSTI Port Configuration …… 2-125
MST1～7 MSTI Port Configuration …… 2-126
「Profile Table」画面 …… 2-127
IPMC Profile Configurations …… 2-127
「IPMC Profile Rule Settings」画面 …… 2-128
IPMC Profile [Profile Name] Rule Settings (In Precedence Order) 2-128
「Address Entry」画面 …… 2-130
IPMC Profile Address Configuration …… 2-130
「MVR」画面 …… 2-131
MVR Configurations …… 2-131
「Basic Configuration」画面 …… 2-135
IGMP Snooping Configuration …… 2-135
Port Related Configuration …… 2-136
「VLAN Configuration」画面 …… 2-137
IGMP Snooping VLAN Configuration …… 2-137
「Port Filtering Profile」画面 …… 2-139
IGMP Snooping Port Filtering Profile Configuration …… 2-139
「Basic Configuration」画面 …… 2-140
MLD Snooping Configuration …… 2-140
Port Related Configuration …… 2-141
「VLAN Configuration」画面 …… 2-142
MLD Snooping VLAN Configuration …… 2-142
「Port Filtering Profile」画面 …… 2-144
MLD Snooping Port Filtering Profile Configuration …… 2-144
「LLDP」画面 …… 2-145
LLDP Configuration …… 2-145
「LLDP-MED」画面 …… 2-148
LLDP-MED Configuration …… 2-148
「PoE」画面 …… 2-158
Power Over Ethernet Configuration …… 2-158
「Schedule Scheme」画面 …… 2-161
Schedule Scheme Configuration …… 2-161
「MAC Table」画面 …… 2-162
MAC Address Table Configuration …… 2-162
「VLANs」画面 …… 2-164
Global VLAN Configuration …… 2-164
Port VLAN Configuration …… 2-165
「Port to Group Configuration」画面 …… 2-169
VLAN Translation Port Configuration …… 2-169
「VLAN Translation Mappings」画面 …… 2-170
VLAN Translation Mapping Table …… 2-170

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

下記は、前ページからのつづきです。

「Mapping Configuration」画面 …… 2-171
Mapping Parameters …… 2-171
「Membership」画面 …… 2-172
Private VLAN Membership Configuration …… 2-172
「Port Isolation」画面 …… 2-173
Port Isolation Configuration …… 2-173
「MAC-based VLAN」画面 …… 2-174
MAC-based VLAN Membership Configuration …… 2-174
「Protocol to Group」画面 …… 2-175
Protocol to Group Mapping Table …… 2-175
「Group to VLAN」画面 …… 2-176
Group Name to VLAN mapping Table …… 2-176
「IP Subnet-based VLAN」画面 …… 2-177
IP Subnet-based VLAN Membership Configuration …… 2-177
「Configuration」画面 …… 2-178
Voice VLAN Configuration …… 2-178
Port Configuration …… 2-179
「OUI」画面 …… 2-180
Voice VLAN OUI Table …… 2-180
「Port Classification」画面 …… 2-181
QoS Port Classification …… 2-181
「Tag Classification」画面 …… 2-183
QoS Ingress Port Tag Classification Port 1～10 …… 2-183
「Port Policing」画面 …… 2-184
QoS Ingress Port Policers …… 2-184
「Queue Policing」画面 …… 2-185
QoS Ingress Queue Policers …… 2-185
「Port Scheduler」画面 …… 2-186
QoS Egress Port Schedulers …… 2-186
「Port Shaping」画面 …… 2-187
QoS Egress Port Shapers …… 2-187
「Port Scheduler and Shapers」画面 …… 2-188
QoS Egress Port Scheduler and Shapers Port 1～10 …… 2-188
「Port Tag Remarking」画面 …… 2-190
QoS Egress Port Tag Remarking …… 2-190
「Tag Remarking」画面 …… 2-191
QoS Egress Port Tag Remarking Port 1～10 …… 2-191
「Port DSCP」画面 …… 2-193
QoS Port DSCP Configuration …… 2-193
「DSCP-Based QoS」画面 …… 2-194
DSCP-Based QoS Ingress Classification …… 2-194
「DSCP Translation」画面 …… 2-195
DSCP Translation …… 2-195
「DSCP Classification」画面 …… 2-196
DSCP Classification …… 2-196

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

下記は、前ページからのつづきです。

「QoS Control List」画面 …… 2-197
QoS Control List Configuration …… 2-197
「QCE Configuration」画面 …… 2-199
QCE Configuration …… 2-199
Key Parameters …… 2-200
EtherType Parameters …… 2-202
LLC Parameters …… 2-202
SNAP Parameters …… 2-203
IPv4 Parameters …… 2-204
IPv6 Parameters …… 2-205
UDP Parameters/TCP Parameters …… 2-206
Action Parameters …… 2-207
「Storm Policing」画面 …… 2-208
Global Storm Policer Configuration …… 2-208
「Mirroring」画面 …… 2-209
Mirror & RMirror Configuration Table …… 2-209
Mirror & RMirror Configuration …… 2-211
「UPnP」画面 …… 2-214
UPnP Configuration …… 2-214
「Ports」画面 …… 2-215
MRP Overall Port Configuration …… 2-215
「MVRP」画面 …… 2-216
MVRP Global Configuration …… 2-216
MVRP Port Configuration …… 2-216
「Global config」画面 …… 2-217
GVRP Configuration …… 2-217
「Port config」画面 …… 2-218
GVRP Port Configuration …… 2-218
「sFlow」画面 …… 2-219
sFlow Configuration …… 2-219
「UDLD」画面 …… 2-222
UDLD Port Configuration …… 2-222
「Virtual Stack」画面 …… 2-223
Virtual Stacking Configuration …… 2-223
「e-Spider」画面 …… 2-224
e-Spider …… 2-224
「Display Topology」画面 …… 2-225
e-Spider …… 2-225
「IP Setting」画面 …… 2-226
e-Spider …… 2-226
「Status/Setting」画面 …… 2-227
e-Spider …… 2-227

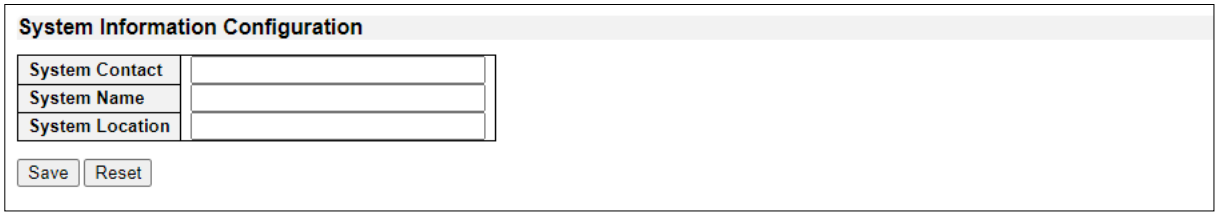
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Information」画面

Configuration > System > Information

本製品のシステム情報を設定します。

System Information Configuration



System Contact ……　管理対象ノードの連絡先を、255文字以内で入力します。
使用できる文字列は、32～126までのASCII文字です。

System Name ……　管理対象ノードのシステム名称を255文字以内で入力します。
Telnet/SSHで本製品に接続したとき、ここで設定した本体名称が表示されます。
使用できる文字列は、半角英数字(a～z、A～Z、0～9、－)です。
※「－(ハイフン)」を本体名称の先頭、または末尾に使用すると、登録できません。

System Location……　管理対象ノードの場所を、255文字以内で入力します。
使用できる文字列は、32～126までのASCII文字です。

〈Save〉 ……　設定した内容を保存するボタンです。

〈Reset〉 ……　設定内容を変更したとき、変更前の状態に戻すボタンです。

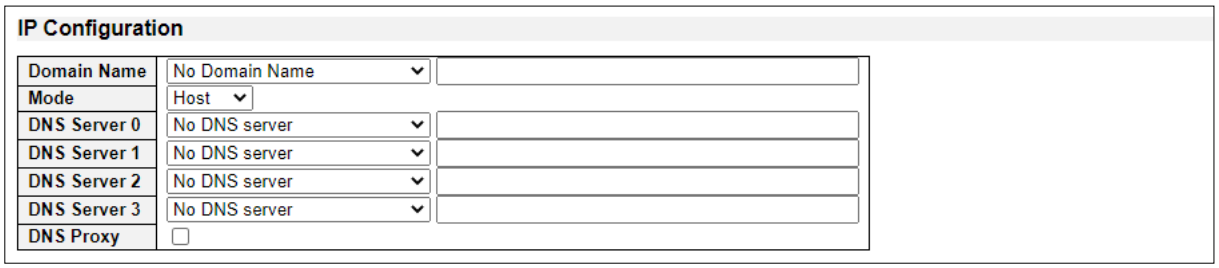
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「IP」画面

Configuration > System > IP

IPの基本設定、インターフェース、経路情報を設定します。
※インターフェースは最大8件まで、経路情報は最大32件まで登録できます。

IP Configuration



Domain Name ……

本製品が所属しているローカルドメイン名を入力します。
設定したドメイン内の名前に対するクエリでローカルドメインを省略した場合、自動でドメイン名を補います。
たとえば、ドメイン名が「example.com」に設定されていてPING宛先に「test」を指定した場合、「test.example.com」として処理されます。

No Domain Name：
ドメイン名を使用しません。

Configured Domain Name：
指定されたローカルドメイン名を入力します。

From any DHCPv6 interfaces：
DHCPv6サーバーからDHCPv6対応インターフェースに通知された最初のドメイン名を使用します。

From this DHCPv6 interface：
本製品のDHCPv6対応インターフェースから通知されたドメイン名を使用します。

Mode ……

IPスタックの動作モードを設定します。

Host：
インターフェース間のIPトラフィックは、ルーティングされません。

Router：
IPトラフィックは、すべてのインターフェース間でルーティングされます。

「IP」画面

Configuration > System > IP

IP Configuration

DNS Server 0～3 ……

本製品のDNSサーバーを設定します。
使用できるサーバーは4つあり、DNS Server 0の優先度が最も高く、DNS Server 3の優先度が最も低くなります。

No DNS server：
DNSサーバーを使用しません。

Configured IPv4 or IPv6：
DNSサーバーをIPv4ユニキャストアドレス、またはIPv6ユニキャストアドレス（リンクローカルアドレスを除く）で指定します。
DNSサービスを利用するために、PINGなどを使用して設定されたDNSサーバーまで到達できるか確認してください。

From any DHCPv4 interfaces：
DHCPv4サーバーからDHCPv4対応インターフェースに通知された最初のDNSサーバーを使用します。

From this DHCPv4 interface：
本製品のDHCPv4対応インターフェースから通知されたDNSサーバーを使用します。

From any DHCPv6 interfaces：
DHCPv6サーバーからDHCPv6対応インターフェースに通知された最初のDNSサーバーを使用します。

From this DHCPv6 interface：
本製品のDHCPv6対応インターフェースから通知されたDNS サーバーを使用します。

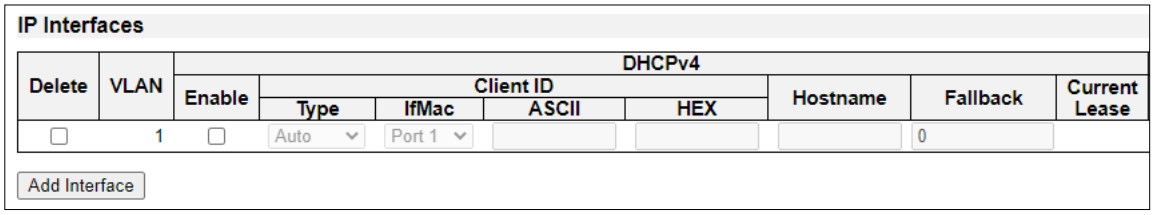
DNS Proxy ……

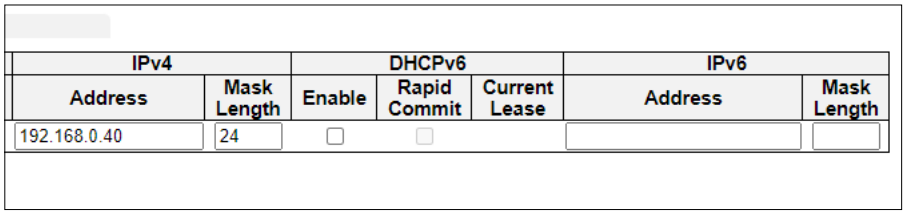
本製品のDNSプロキシ機能を設定します。
DNSプロキシ機能とは、端末からのDNS要求をDNSサーバーに中継し、DNSリゾルバーとして端末に代理応答する機能です。
DNSプロキシ機能を使用することで、本製品のアドレスをネットワーク上の端末にDNSサーバーとして設定している場合、本製品が接続する先のDNSサーバーのアドレスが変更になったときでも、端末側の設定を変更する必要がありません。
※IPv4のDNSプロキシのみ対応しています。

「IP」画面

Configuration > System > IP

IP Interfaces





Delete …… 登録された内容を削除するとき、ボックスにチェックマークを入れます。

VLAN …… IPインターフェースが所属するVLAN ID番号を設定します。
※異なるID番号のネットワークとは通信できません。
※新しいインターフェースを作成するときだけ、入力できます。

DHCPv4

Enabled …… DHCPv4クライアント機能を有効にするとき、ボックスにチェックマークを入れます。
DHCPv4クライアント機能を有効にした場合、DHCPv4プロトコルを使用してインターフェースの IPv4アドレスとマスク(サブネットマスク)を設定します。

Client ID Type …… DHCPオプション61(クライアントID)の種類を設定します。

Client ID IfMac …… DHCPv4クライアント機能が有効で、[Client ID Type]欄が「IF_MAC」の場合、選択したインターフェースのハードウェアMACアドレスがクライアントIDとして使用されます。

Client ID ASCII …… DHCPv4クライアント機能が有効で、[Client ID Type]欄が「ASCII」の場合、使用するクライアントIDをASCII 文字で入力します。

Client ID HEX …… DHCPv4クライアント機能が有効で、[Client ID Type]欄が「HEX」の場合、使用するクライアントIDを16進数で入力します。

Hostname …… DHCPオプション12(ホスト名)を設定します。
ホスト名が空白の場合、「Informaition」画面の[System Name]欄で設定したシステム名称か、「estax」につづいてシステムMACアドレスの下位3バイトをホスト名として使用します。

「IP」画面

Configuration > System > IP

IP Interfaces

Fallback Timeout……

DHCPサーバーにIPアドレスを要求するときの待ち時間を設定します。
設定できる範囲は、「0～4294967295」(秒)です。
※設定した時間が経過すると、手動で設定したIPv4アドレスがIPv4インターフェースのアドレスとして使用されます。(フォールバックアドレス)
「0」に設定した場合、DHCPサーバーからIPアドレスが取得できるまで要求をつづけます。

Current Lease……

DHCPサーバーから取得したIPアドレスが表示されます。
IPアドレスが取得できなかった場合は、空白になります。

IPv4

Address……

インターフェースのIPv4アドレスを手動で設定します。
DHCP機能が有効になっている場合は、フォールバックアドレスを設定します。
※IPv4アドレスの手動設定や、DHCP機能有効時にフォールバックアドレスが必要ない場合は、空白のままにしてください。

Mask……

IPv4ネットワークのマスク(サブネットマスク)のビット数(プレフィックス長)を設定します。
設定できる範囲は、「0～30」です。
DHCP機能が有効になっている場合は、フォールバックアドレスのマスクを設定します。
※IPv4アドレスの手動設定や、DHCP機能有効時にフォールバックアドレスが必要ない場合は、空白のままにしてください。

DHCPv6

Enable……

DHCPv6クライアント機能を有効にするとき、ボックスにチェックマークを入れます。
DHCPv6クライアント機能を有効にした場合、DHCPv6プロトコルを使用してインターフェースのIPv6アドレスを設定します。

Rapid Commit……

DHCPv6クライアント機能が有効で、Rapid Commit(高速コミット)機能を使用するとき、ボックスにチェックマークを入れます。
高速コミット機能使用時、DHCPv6クライアントが請求メッセージを送信後、サーバーから高速コミット対応の応答メッセージを受信するとすぐに、待機中のプロセスを終了します。

Current Lease……

DHCPサーバーから取得したIPアドレスが表示されます。
IPアドレスが取得できなかった場合は、空白になります。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「IP」画面

Configuration > System > IP

IP Interfaces

IPv6

Address …… インターフェースのIPv6アドレスを設定します。
IPv6ユニキャストアドレスだけが使用できます。(IPv4互換アドレス、IPv4射影アドレスを除く)
※IPv6アドレスが必要ない場合は、空白のままにしてください。

Mask …… IPv6アドレスのマスクビット数(プレフィックス長)を設定します。
設定できる範囲は、「1～128」です。
※IPv6アドレスが必要ない場合は、空白のままにしてください。

〈Add Interface〉 …… IPインターフェースを追加するボタンです。
※最大8件まで登録できます。

ご参考

IPv6アドレスについて

IPv6アドレスは、128ビットのアドレス長を持ち、最大4桁の8つのフィールドをコロン(:)で区切った上で、16進数で表記されます。
(例：fe80:0000:0000:0000:0215:c5ff:fe03:4dc7)
※0000となるフィールド(:で区切られた部分)が2つ以上連続する場合、「::」に省略できます。(例：fe80::215:c5ff:fe03:4dc7)
「::」に省略できるのは、1つのアドレス内で1ヵ所だけです。
※IPv4アドレスを指定する場合は、「::192.1.2.34」のように入力してください。

IPv6　DAD(重複アドレス検出)について

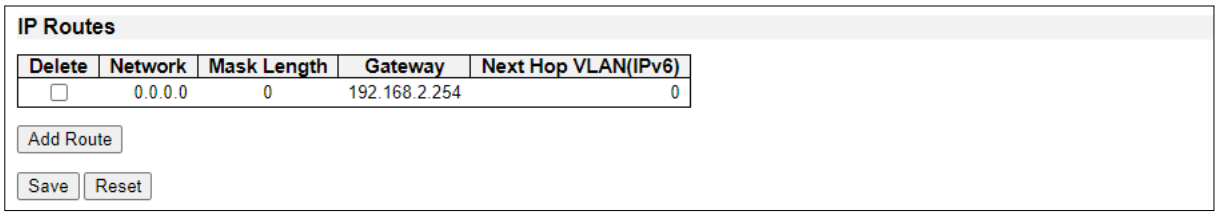
リンクローカルアドレスは、一意に割り当てられることになっているハードウェアアドレスに基づくインターフェースIDに基づきます。
DAD(重複アドレス検出)がアドレスの重複を検出したら、インターフェースを無効にする必要があります。

アドレスの重複を解決するには手動で確認・再設定が必要です。
たとえば、ループがVLANで発生しているかどうか、またはVLAN内のデバイスと同じハードウェアアドレスのデバイスが存在するかどうかを確認します。
特定のリンクローカルアドレスが使用中のIPv6リンク上で固有であることを確認したあと、特定のIPv6インターフェースを削除してから再度追加してください。

「IP」画面

Configuration > System > IP

IP Routes



Delete …… 登録された内容を削除するとき、ボックスにチェックマークを入れます。

Network …… 宛先IPアドレス、またはホストアドレスをドット付き10進表記、またはIPv6表記で設定します。
デフォルトルートの場合は、「0.0.0.0」か「::」(IPv6表記)を使用できます。

Mask Length …… 宛先IPアドレス、またはホストアドレスのマスク(サブネットマスク)のビット数(プレフィックス長)を設定します。
設定した経路に適格であるために一致する必要があるネットワーク部の長さを指定します。
設定できる範囲は「0～32」(IPv6の場合は128まで)です。
デフォルトルートの場合は、「0」を設定します。

Gateway …… IPゲートウェイのIPアドレスをドット付き10進表記、またはIPv6表記で設定します。
ゲートウェイとネットワークは、同じ表記を使用してください。

Next Hop VLAN (Only for IPv6) …… IPv6プロトコルを使用するときの、ネクストホップを設定します。
設定できる範囲は「1～4095」です。
IPv6ゲートウェイアドレスがリンクローカルアドレスの場合は、ネクストホップVLANを指定する必要があります。
IPv6ゲートウェイアドレスがリンクローカルアドレスでない場合、設定したネクストホップVLANは無効になります。
※設定したVLAN IDのIPv6インターフェースを有効にしてください。

〈Add Route〉 …… IP経路情報を追加するボタンです。
※最大32件まで登録できます。

〈Save〉 …… 設定した内容を保存するボタンです。

〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「NTP」画面

Configuration > System > NTP

本製品の内部時計を自動設定するとき、アクセスするタイムサーバーの設定です。

NTP Configuration

Mode ……　本製品の自動時計設定機能を設定します。
「Enabled」(有効)に設定すると、インターネット上に存在するNTPサーバーに日時の問い合わせをして、内部時計を自動設定します。

Server 1～5 ……　アクセスするNTPサーバーのIPアドレス(IPv4、またはIPv6)、またはドメイン名を設定します。
※IPv6表記については、2-12ページをご参照ください。

〈Save〉 ……　設定した内容を保存するボタンです。

〈Reset〉 ……　設定内容を変更したとき、変更前の状態に戻すボタンです。

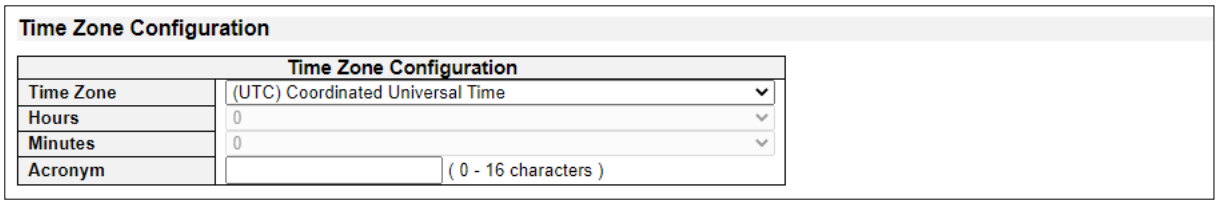
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Time」画面

Configuration > System > Time

タイムゾーンやサマータイムを設定します。

Time Zone Configuration



Time Zone …… タイムゾーンを設定します。
※初期設定では何も設定されていません。
特に問題なければ、「(UTC+09:00)Osaka, Sapporo, Tokyo 」を選択してください。
※詳細な設定をする必要がある場合は、「Manual Setting」を選択してください。

Hours/Minutes …… 選択したタイムゾーンとUTC(協定世界時)の差が表示されます。
[Time Zone]欄で「Manual Setting」を選択した場合は、UTCとの差を入力してください。

Acronym …… タイムゾーン識別用の頭字語を16文字以内で設定します。
※「‘’」(シングルクォーテーション2つ)は空文字列になります。

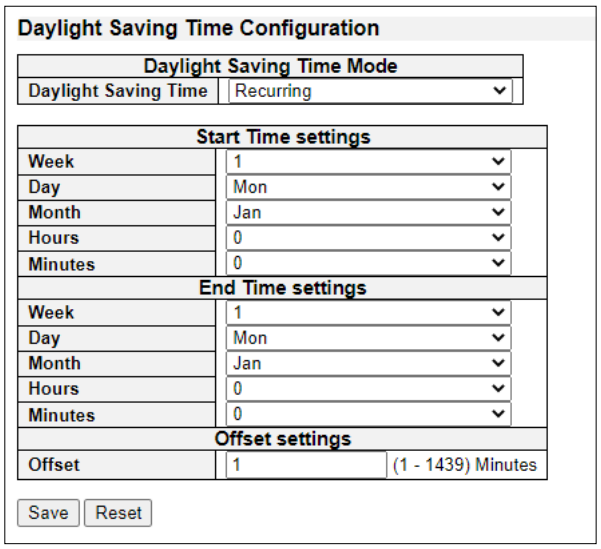
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Time」画面

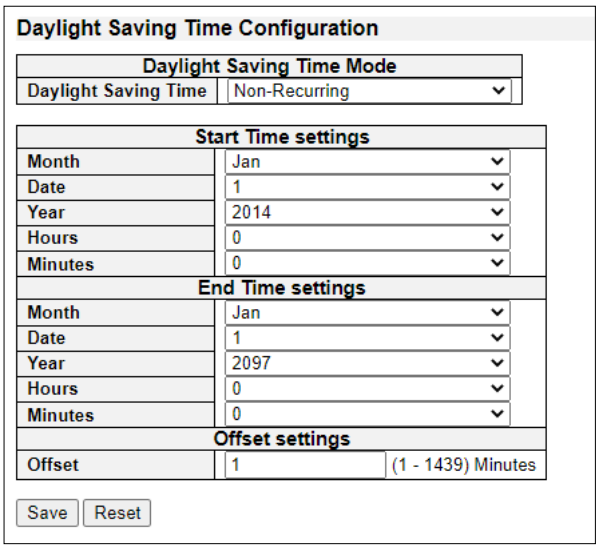
Configuration > System > Time

Daylight Saving Time Configuration

Daylight Saving Time : Recurring



Daylight Saving Time : Non-Recurring



Daylight Saving Time Mode

Daylight Saving Time …… サマータイムの設定をします。
サマータイムを使用すると、サマータイム期間は[Offset]欄で設定した時間だけ時計が進みます。

Disabled :
サマータイムを使用しません。

Recurring :
設定されたサマータイム期間を、毎年繰り返します。

Non-Recurring :
設定された期間内だけサマータイムを使用します。

Start Time settings Daylight Saving Time : Recurring
Week/Day/Month/Hours/Minutes
…… 毎年サマータイムを開始する日時(週番号、曜日、月、時、分)を設定します

End Time settings Daylight Saving Time : Recurring
Week/Day/Month/Hours/Minutes
…… 毎年サマータイムを終了する日時(週番号、曜日、月、時、分)を設定します。

Start Time settings Daylight Saving Time : Non-Recurring
Month/Date/Year/Hours/Minutes
…… サマータイムを開始する日時(月、日、年、時、分)を設定します。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Time」画面

Configuration > System > Time

Daylight Saving Time Configuration

End Time settings (Daylight Saving Time : Non-Recurring)

Month/Date/Year/Hours/Minutes

…… サマータイムを終了する日時(月、日、年、時、分)を設定します。

Offset settings

Offset …… サマータイム期間中、進める時間を設定します。
設定できる範囲は、「1～1439」(分)です。

〈Save〉 …… 設定した内容を保存するボタンです。

〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

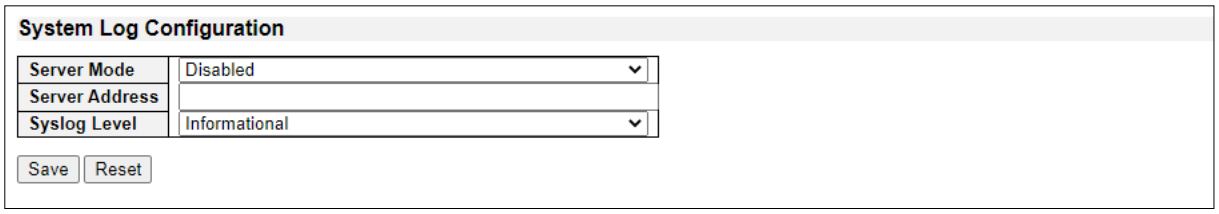
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Log」画面

Configuration > System > Log

指定したSyslogサーバーにログ情報を出力するための設定です。

System Log Configuration



Server Mode ……

Syslogサーバーを使用するか設定します。
「Enabled」(有効)に設定した場合、SyslogメッセージはSyslogサーバーに送信されます。
Syslogメッセージは、UDPポート514を使用してSyslogサーバーへ送信されます。
UDPはコネクションレス型の通信プロトコルで確認応答機能に対応していないため、Syslogサーバーは送信者へ応答パケットを送り返しません。
Syslogパケットは、Syslogサーバーが存在しない場合でも常に送信されます。

Server Address ……

SyslogサーバーのIPv4ホストアドレスを設定します。
本製品のDNS機能を使用する場合、ドメイン名でも設定できます。

Syslog Level ……

Syslogサーバーに送信するメッセージの種類を設定します。

Error：
重大度コードがError(3)以下のメッセージを送信します。

Warning：
重大度コードがWarning(4)以下のメッセージを送信します。

Notice：
重大度コードがNotice(5)以下のメッセージを送信します。

Informational：
重大度コードがInformational(6)以下のメッセージを送信します。

〈Save〉 ……

設定した内容を保存するボタンです。

〈Reset〉 ……

設定内容を変更したとき、変更前の状態に戻すボタンです。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Port Power Savings」画面

Configuration > Green Ethernet > Port Power Savings

ポートの省電力機能について設定します。

EEEについて
EEE(Energy Efficient Ethernet)は、トラフィック使用率が低いときやデータが流れていないときに一部の回路を停止して、消費電力を削減する機能です。
ポートがデータを送信すると、すべての回路が通電します。
通電にかかる時間(ウェイクアップ時間)は、1Gbitリンクで17マイクロ秒、それ以外で30マイクロ秒です。
データ送信時は、受信デバイスと送信デバイス両方のすべての回路が通電していることを確認するために、ウェイクアップ時間が必要です。
LLDPプロトコルを使用して、ウェイクアップ時間情報を交換できます。

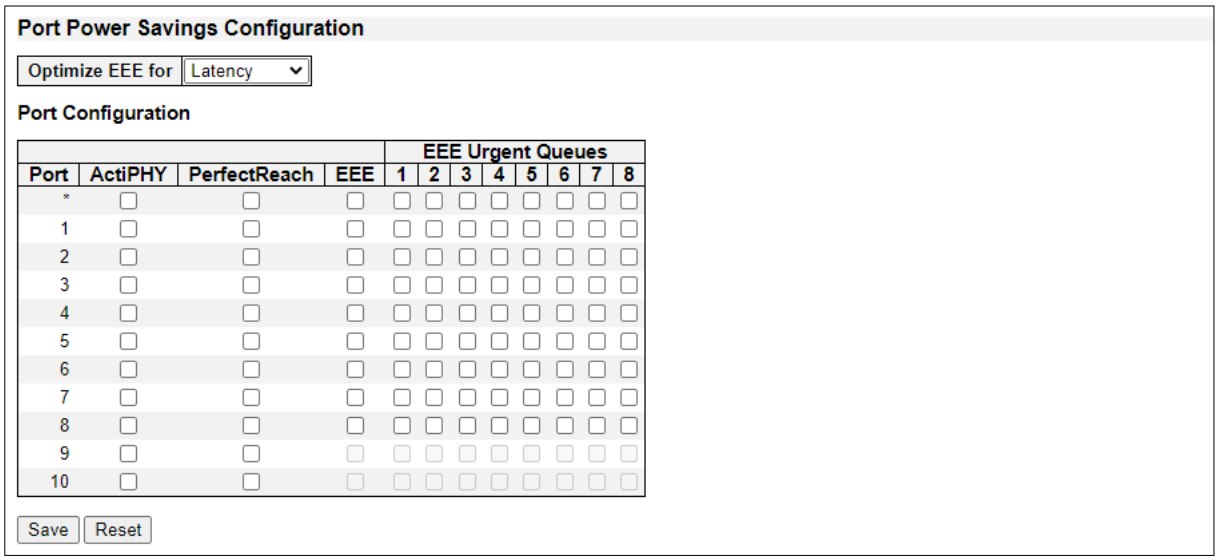
EEEは、1Gbit、または100Mbit全二重モードにネゴシエートされたオートネゴシエーションモードのポートで動作します。
EEEに対応していないポートは、EEEを有効にできません。
消費電力を節約するためにポートの電源がOFFになると、ポートの電源が入るまでのあいだに送信したデータはバッファーに格納されます。
ポートのON/OFFにはオーバーヘッドがあるため、送信するまでにバッファーに格納されるデータを増やし、一度に多くのデータを送信すると、より多くの消費電力を節約できますが、トラフィックにある程度の遅延が生じます。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Port Power Savings」画面

Configuration > Green Ethernet > Port Power Savings

Port Power Savings Configuration



Optimize EEE for ……

EEE機能を使用するとき、消費電力の削減を優先するか、トラフィック遅延時間の削減を優先するかを選択します。

Port Configuration

Port ……

本製品のポート番号が表示されます。
※「*」の設定を変更すると、すべてのポートに反映されます。

ActiPHY ……

リンクダウンしているポートを省電力モードにする機能を設定します。
ケーブルが挿入されているかを確認するために、少しのあいだポートの電源がオンになります。

PerfectReach ……

挿入されているケーブルの長さによって、ポートを省電力モードにする機能を設定します。

EEE ……

ポートごとにEEEを使用するか設定します。
消費電力を削減するために、送信データの準備ができていてもすぐに送信せず、データ・バーストの送信準備が整うまでキューに入れられますが、トラフィックの遅延が発生します。
必要に応じて、フレームをUrgentキューにマップすることで、特定のフレームの待機時間を最小限に抑えられます。
Urgentキューが送信するデータを取得すると回路の電源が入り、遅延はウェイクアップ時間まで短縮されます。
※キューの詳細は、「QOS」メニューで設定できます。

EEE Urgent Queues ……

データが利用可能になると、すぐにフレームを送信するキューを選択します。
選択されていないキューのデータは、データ・バーストが送信できるようになるまで送信されません。

〈Save〉 ……

設定した内容を保存するボタンです。

〈Reset〉 ……

設定内容を変更したとき、変更前の状態に戻すボタンです。

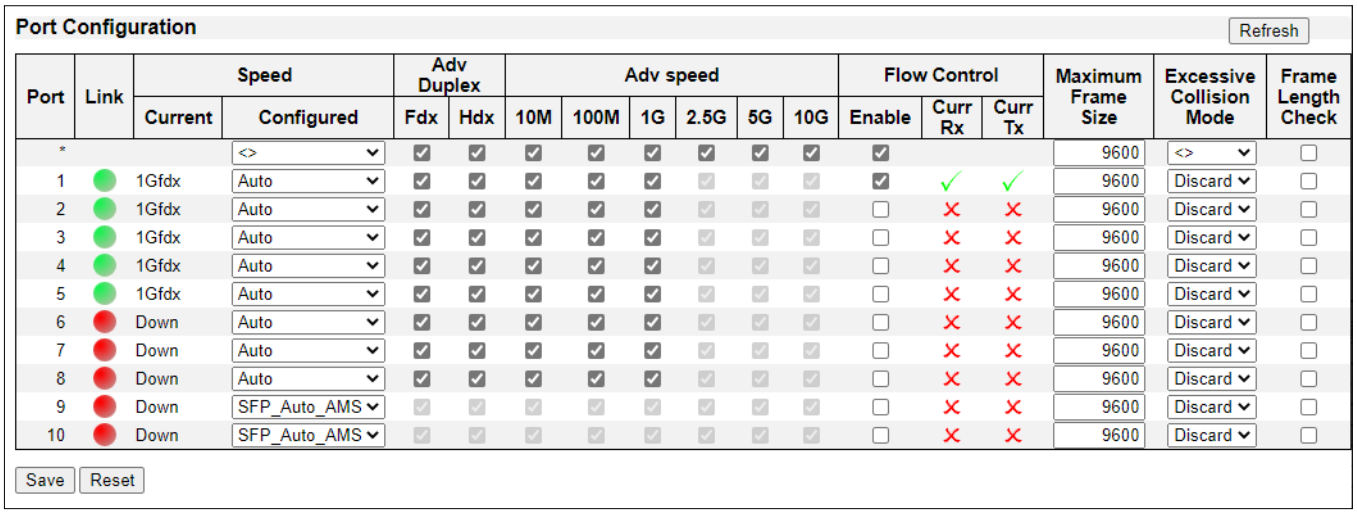
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Ports」画面

Configuration > Ports

ポートの状態確認や、ポートの設定をします。

Port Configuration



Port Configuration

Refresh

Port	Link	Speed		Adv Duplex		Adv speed						Flow Control			Maximum Frame Size	Excessive Collision Mode	Frame Length Check
		Current	Configured	Fdx	Hdx	10M	100M	1G	2.5G	5G	10G	Enable	Curr Rx	Curr Tx			
*			<>	☑	☑	☑	☑	☑	☑	☑	☑	☑			9600	<>	☐
1		1Gfdx	Auto	☑	☑	☑	☑	☑	☐	☐	☐	☑	✓	✓	9600	Discard	☐
2		1Gfdx	Auto	☑	☑	☑	☑	☑	☐	☐	☐	☐	✗	✗	9600	Discard	☐
3		1Gfdx	Auto	☑	☑	☑	☑	☑	☐	☐	☐	☐	✗	✗	9600	Discard	☐
4		1Gfdx	Auto	☑	☑	☑	☑	☑	☐	☐	☐	☐	✗	✗	9600	Discard	☐
5		1Gfdx	Auto	☑	☑	☑	☑	☑	☐	☐	☐	☐	✗	✗	9600	Discard	☐
6		Down	Auto	☑	☑	☑	☑	☑	☐	☐	☐	☐	✗	✗	9600	Discard	☐
7		Down	Auto	☑	☑	☑	☑	☑	☐	☐	☐	☐	✗	✗	9600	Discard	☐
8		Down	Auto	☑	☑	☑	☑	☑	☐	☐	☐	☐	✗	✗	9600	Discard	☐
9		Down	SFP_Auto_AMS	☐	☐	☐	☐	☐	☐	☐	☐	☐	✗	✗	9600	Discard	☐
10		Down	SFP_Auto_AMS	☐	☐	☐	☐	☐	☐	☐	☐	☐	✗	✗	9600	Discard	☐

Save Reset

Port …… 本製品のポート番号が表示されます。

Link …… 現在のリンク状態が表示されます。

緑：リンク中

赤：リンクダウン

「Ports」画面

Configuration > Ports

Port Configuration

Speed

Current …… 現在のリンク速度が表示されます。

Configured …… 使用可能なリンク速度を選択します。
ポートごとにサポートされている速度が表示されます。

Disabled：
ポートを無効にします。

Auto：
接続する機器の対応可能速度から、最適な速度とモードが自動選択されます。
（オートネゴシエーションモード）

10Mbps HDX：
メタルケーブル用のポートを10Mbps 半二重モードに固定します。

10Mbps FDX：
メタルケーブル用のポートを10Mbps 全二重モードに固定します。

100Mbps HDX：
メタルケーブル用のポートを100Mbps 半二重モードに固定します。

100Mbps FDX：
メタルケーブル用のポートを100Mbps 全二重モードに固定します。

1Gbps FDX：
1Gbps 全二重モードに固定します。

SFP_Auto_AMS：
SFPポートがAMS（Auto Media Select）モードになり、速度が自動選択されます。
AMSモードでは、挿入されているケーブルの種類（メタルケーブル/光ケーブル）を自動で判別します。
メタルケーブル用のポートは、Autoモードに設定されます。
※本製品では、SFP ROMを検出してケーブルを自動判別します。
　一部のSFPは検出できない場合があります。

100-FX：
100-FXのSFPポートに設定します。
メタルケーブル用のポートとしては使用できません。

1000-X：
1000-XのSFPポートに設定します。
メタルケーブル用のポートとしては使用できません。

※1000-XのAMSモードのポートでは、メタルケーブル用のポートが優先されます。
※100-FXのAMSモードのポートでは、メタルケーブル用のポートが優先されます。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Ports」画面

Configuration > Ports

Port Configuration

Adv Duplex

Fdx/Hdx ……

デュプレックスモードを自動判別する場合(オートネゴシエーションモード)、指定されたデュプレックスモードだけを接続する機器にアドバタイズします。
初期設定では、デュプレックスモードを自動判別する場合、対応しているすべてのデュプレックスをアドバタイズします。

Adv speed

10M/100M/1G/2.5G/5G/10G ……

速度を自動判別する場合(オートネゴシエーションモード)、指定された速度だけを接続する機器にアドバタイズします。
初期設定では、速度を自動判別する場合、ポートはサポートされているすべての速度をアドバタイズします。

Flow Control

Enable ……

フロー制御機能を有効にするとき、ボックスにチェックマークを入れます。
ポートのリンク速度設定によって、動作が異なります。
◎リンク速度が「Auto」に設定されている場合、設定した内容が接続する機器にアドバタイズされます。
[Curr Rx]と[Curr Tx]には、直近のネゴシエーション結果が表示されます。
◎リンク速度が固定されている場合、[Curr Rx]と[Curr Tx]には設定した内容が表示されます。
※100-FX規格はオートネゴシエーションに対応していないため、100-FXモードの場合、フロー制御機能は常に無効になります。

Curr Rx ……

ポーズフレームを受信したとき、送信を一時停止するかどうかが表示されます。

Curr Tx……

ポーズフレームを送信するかどうかが表示されます。

Maximum Frame Size ……

最大フレームサイズ(FCSを含む)を設定します。
設定できる範囲は、「1518～9600」(バイト)です。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Ports」画面

Configuration > Ports

Port Configuration

Excessive Collision Mode …… 過度なコリジョン(衝突)を検出したときの動作を設定します。

Discard：
衝突を16回検出すると、フレームを破棄します。

Restart：
衝突を16回検出すると、バックオフアルゴリズムを再起動します。

Frame Length Check…… フレーム長チェック機能を有効にするとき、ボックスにチェックマークを入れます。
イーサネットフレームには、1535以下の値でフレームのペイロード長(バイト単位)を示すEtherType/Lengthフィールドが含まれています。
EtherType/Lengthフィールドの値が1535を超える場合は、「EtherType」として使用され、フレームのペイロードにカプセル化されているプロトコルを示します。
フレーム長チェック機能を有効にすると、EtherType/Lengthフィールドの値と実際のペイロード長が一致しない場合、ペイロード長が1536バイト未満のフレームは削除されます。
フレーム長チェック機能を無効にすると、ペイロード長が一致していなくてもフレームは削除されません。
※ドロップカウンターは、ペイロード長の不一致で削除されたフレームをカウントしません。

〈Save〉 …… 設定した内容を保存するボタンです。

〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

〈Refresh〉 …… 最新の状態に更新するボタンです。
※設定内容を変更したときは、変更前の状態に戻ります。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Mode」画面

Configuration > DHCPv4 > Server > Mode

DHCPサーバーの使用についての設定です。

DHCP Server Mode Configuration

Global Mode

Mode …… システムのDHCPサーバー機能を設定します。

VLAN Mode

Enabled …… VLANごとのDHCPサーバー機能を設定します。
DHCPサーバー機能を有効にするとき、ボックスにチェックマークを入れます。

〈Save〉 …… 設定した内容を保存するボタンです。

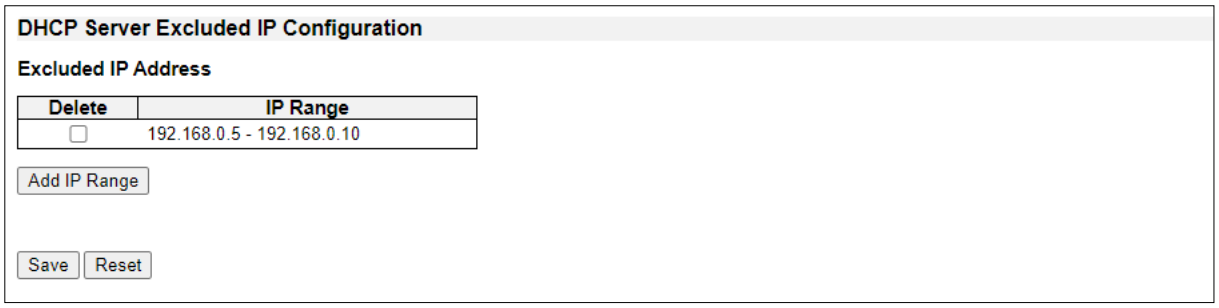
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Excluded IP」画面

Configuration > DHCPv4 > Server > Excluded IP

DHCPサーバー機能を使用するときに、割り当てを除外するIPアドレスを設定します。

DHCP Server Excluded IP Configuration



Excluded IP Address

Delete …… 登録された内容を削除するとき、ボックスにチェックマークを入れます。

IP Range …… クライアントへの割り当てを除外するIPアドレスの範囲を設定します。
1番目の除外IPアドレス範囲は、2番目の除外IPアドレス範囲以下に設定してください。
※除外IPアドレス範囲に設定されたIPアドレスが1つだけの場合は、1番目と2番目の除外IPアドレス範囲のいずれか、または両方に入力できます。

〈Add IP Range〉 …… 除外するIPアドレス範囲を追加するボタンです。

〈Save〉 …… 設定した内容を保存するボタンです。

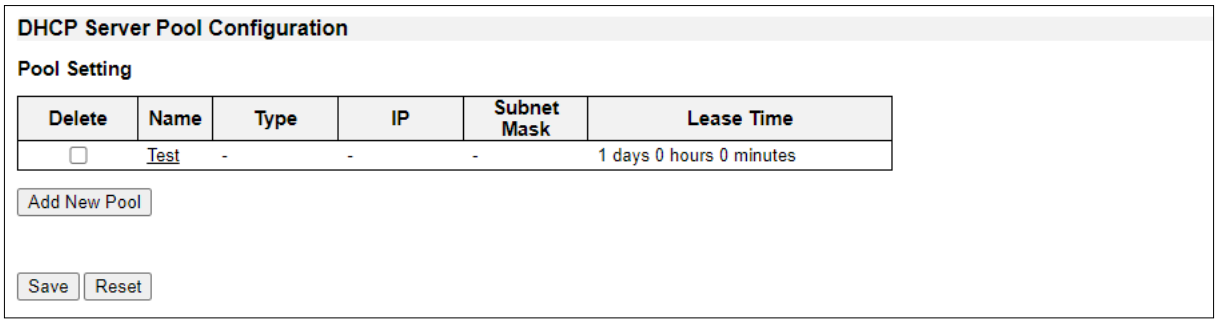
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Pool」画面

Configuration > DHCPv4 > Server > Pool

DHCPアドレスプールについて設定します。
DHCPアドレスプールの設定に応じて、DHCPサーバーはIPアドレスと設定パラメーターをDHCPクライアントへ通知します。

DHCP Server Pool Configuration



Pool Setting

Delete ……
登録された内容を削除するとき、ボックスにチェックマークを入れます。

Name ……
プール名を設定します。
〈Add New Pool〉をクリック後、プール名を設定してから〈Save〉をクリックすると、デフォルト設定のDHCPアドレスプールが追加されます。
各プール名のリンク先をクリックすると、「Pool Configuration」画面へ移動します。
「Pool Configuration」画面でタイプ、IPアドレス、サブネットマスク、リース時間などが設定できます。
※スペースは入力できません。

Type ……
プールの種類が表示されます。
※設定していない場合は、「-」が表示されます。

Network：
複数のDHCPクライアントにIPアドレスを割り当てます。

Host：
クライアント識別子、またはハードウェアアドレスによって識別される特定のDHCPクライアントにIPアドレスを割り当てます。

IP ……
DHCP アドレスプールのネットワークアドレスが表示されます。
※設定していない場合は、「-」が表示されます。

Subnet Mask……
DHCPアドレスプールのサブネットマスクが表示されます。
※設定していない場合は、「-」が表示されます。

Lease Time……
リース時間が表示されます。

〈Add New Pool〉 ……
除外するIPアドレス範囲を追加するボタンです。

〈Save〉 ……
設定した内容を保存するボタンです。

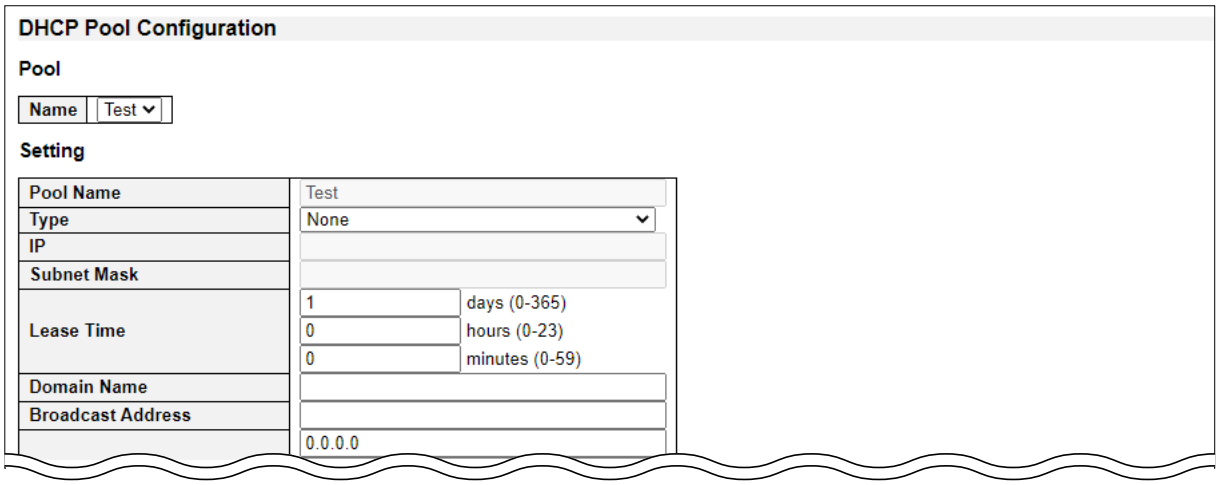
〈Reset〉 ……
設定内容を変更したとき、変更前の状態に戻すボタンです。

「Pool Configuration」画面

Configuration > DHCPv4 > Server > Pool

DHCPプールの詳細な設定を登録します。

DHCP Pool Configuration



Pool

Name …… 設定するプールを選択します。

Setting

Name …… 選択したプール名が表示されます

Type …… プールの種類を選択します。

Network：
複数のDHCPクライアントにIPアドレスを割り当てます。

Host：
クライアントID、またはハードウェア(MAC)アドレスで識別される特定のDHCPクライアントにIPアドレスを割り当てます。

IP …… DHCPアドレスプールのネットワークアドレスを指定します。

Subnet Mask…… DHCPアドレスプールのサブネットマスクを指定します。
（DHCPオプション1）

Lease Time…… DHCPサーバーが割り当てるIPアドレスの有効期間を指定します。
（DHCPオプション51、58、59）
※リース期間を無期限に設定する場合は、すべて0を指定してください。

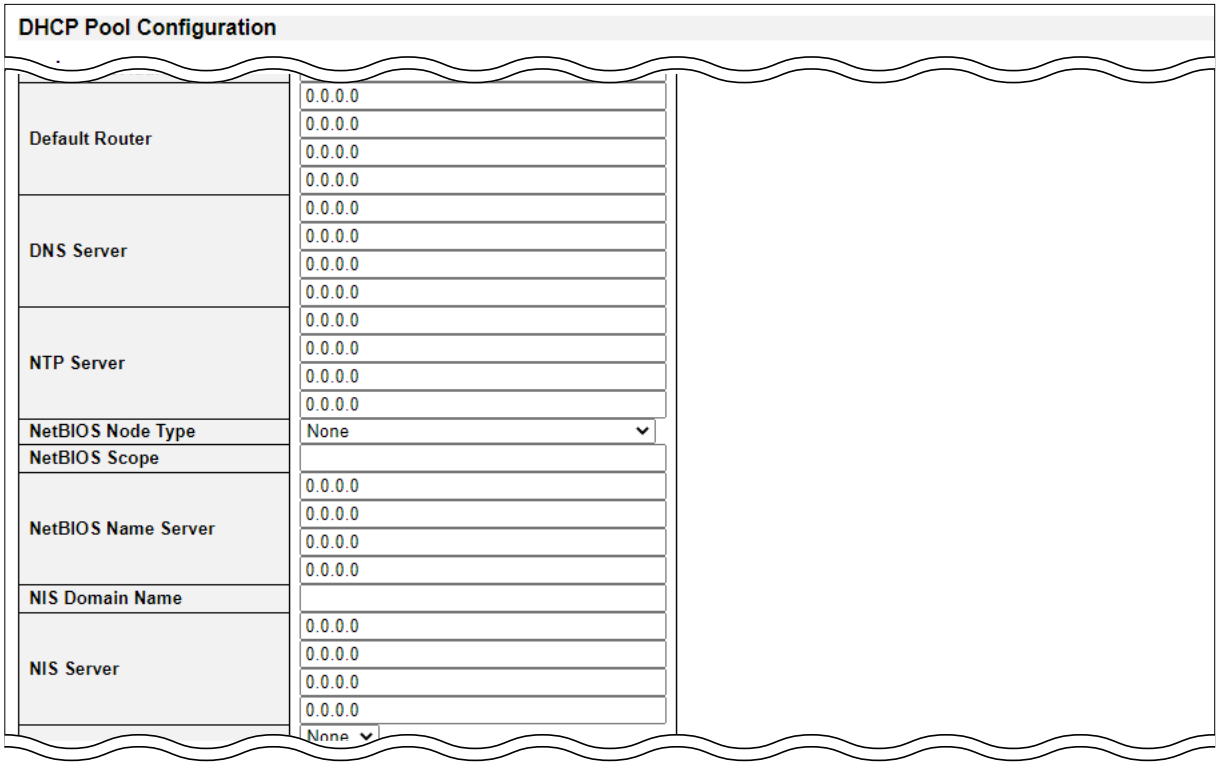
Domain Name …… DNS経由でホスト名を解決するときに、クライアントが使用するドメイン名を指定します。（DHCPオプション15）

Broadcast Address …… クライアントのサブネットで使用中のブロードキャスト･アドレスを指定します。
（DHCPオプション28）

「Pool Configuration」画面

Configuration > DHCPv4 > Server > Pool

DHCP Pool Configuration



Default Router ····· クライアントのサブネット上にあるルーターのIPアドレスのリストを指定します。（DHCPオプション3）

DNS Server ····· クライアントが使用できるドメイン・ネーム・システム・ネーム・サーバーのリストを指定します。（DHCPオプション6）

NTP Server ····· クライアントが使用できるNTPサーバーのIPアドレスのリストを指定します。（DHCPオプション42）

NetBIOS Node Type ····· RFC 1001/1002の定義にしたがって、NetBIOS over TCP/IPクライアントのノードタイプを指定します。（DHCPオプション46）

NetBIOS Scope ····· RFC 1001/1002の定義にしたがって、クライアントのNetBIOS over TCP/IPスコープ・パラメーターを指定します。（DHCPオプション47）

NetBIOS Name Server ····· NBNSネームサーバーのリストを優先度順に指定します。（DHCPオプション44）

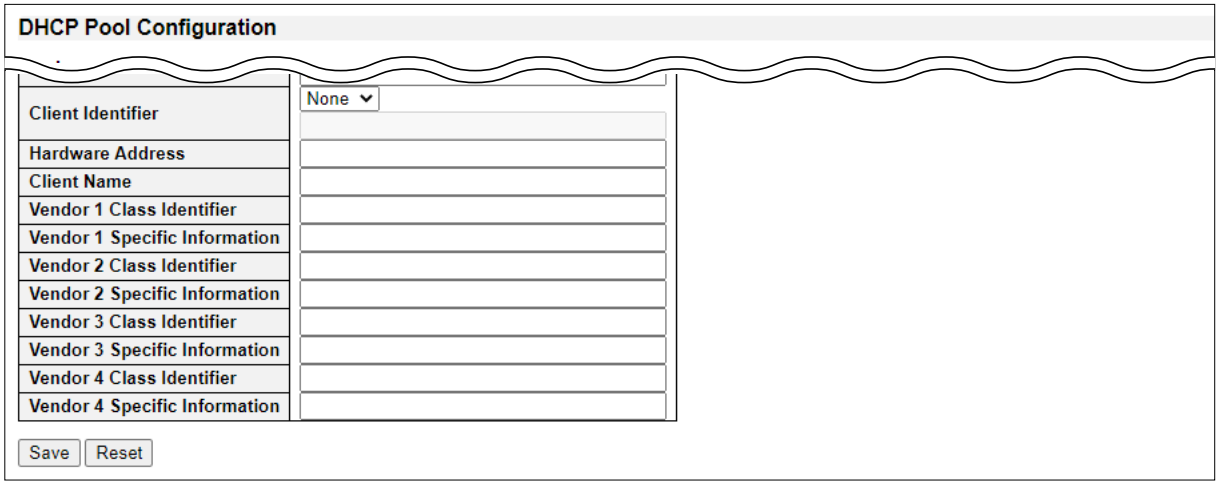
NIS Domain Name ····· クライアントのNISドメイン名を指定します。（DHCPオプション40）

NIS Server ····· クライアントが使用可能なNISサーバーのIPアドレスのリストを指定します。（DHCPオプション41）

「Pool Configuration」画面

Configuration > DHCPv4 > Server > Pool

DHCP Pool Configuration



Client Identifier…… [Type]欄が「Host」のとき、使用するクライアントの種類とクライアントIDを指定します。(DHCPオプション61)

None：
クライアントIDを指定しません。

Name：
ハードウェア(MAC)アドレス以外でクライアントIDを指定します。

MAC：
ハードウェア(MAC)アドレスでクライアントIDを指定します。

Hardware Address…… 使用できません。

Client Name …… 使用できません。

Vendor 1～4 Class Identifier ベンダークラス識別子を指定します。(DHCPオプション60)
ベンダークラス識別子(VCI)は、DHCPクライアントが自身のベンダー・タイプと構成を識別するためにオプションで使用されます。
DHCPサーバーは、対応するベンダー情報(オプション43)を、ベンダークラス識別子を送信してきたクライアントに通知します。

Vendor 1～4 Specific Information
…… ベンダークラス識別子(オプション60)ごとのベンダー固有情報を指定します。(DHCPオプション43)

〈Save〉…… 設定した内容を保存するボタンです。

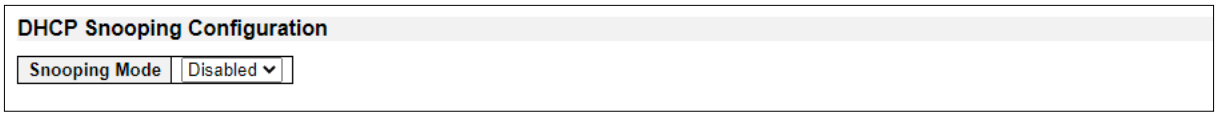
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Snooping」画面

Configuration > DHCPv4 > Snooping

DHCPスヌーピングについて設定します。

DHCP Snooping Configuration



Snooping Mode ……

DHCPスヌーピングを使用するかどうかを設定します。

Enabled：
DHCPスヌーピングを有効にします。
DHCPスヌーピングを有効にすると、DHCP要求はtrusted(信頼された)ポートに転送され、trustedポートからの応答パケットだけが許可されます。

Disabled：
DHCPスヌーピングを無効にします。

Port Mode Configuration

Mode ……

DHCPスヌーピングを使用するとき、各ポートのモードを設定します。

Trusted：
DHCPメッセージの信頼された送信元(trustedポート)に設定します。

Untrusted：
DHCPメッセージの信頼されない送信元(untrustedポート)に設定します。

〈Save〉 ……

設定した内容を保存するボタンです。

〈Reset〉 ……

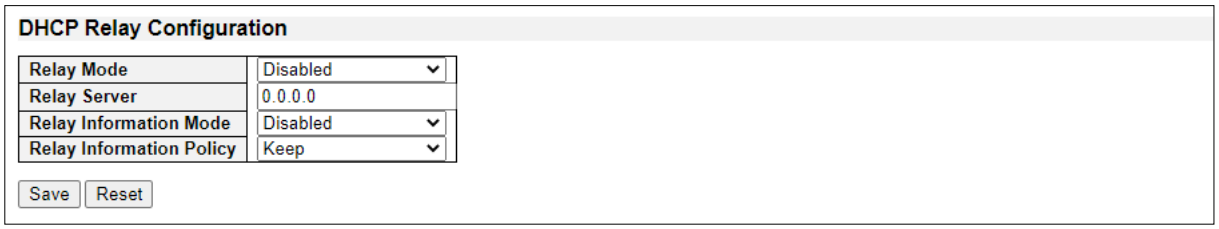
設定内容を変更したとき、変更前の状態に戻すボタンです。

「Relay」画面

Configuration > DHCPv4 > Relay

DHCPリレーについて設定します。
DHCPリレーを使用すると、DHCPクライアントとDHCPサーバーが同じサブネットドメインにない場合、DHCPリレーエージェントがDHCPメッセージを転送します。
DHCPリレーエージェントは、DHCPメッセージを受信したインターフェースのIPアドレスをパケットのGIADDRフィールドに埋め込んで、DHCPサーバーに転送します。
DHCPサーバーは、GIADDRフィールドの値を使用して、割り当てられたサブネットを判別します。
※VLANインターフェースのIPアドレスとPVID(ポートVLAN ID)の設定が正しいことを確認してください。

DHCP Relay Configuration



Relay Mode …… DHCPリレーを使用するかどうかを設定します。

Enabled：
DHCPリレーを有効にします。
DHCPリレーを有効にすると、DHCPクライアントとDHCPサーバーが同じサブネットドメインにない場合、DHCPリレーエージェントがDHCPメッセージを転送します。

Disabled：
DHCPリレーを無効にします。

Relay Server …… DHCPリレーサーバーのIPアドレスを設定します。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Relay」画面

Configuration > DHCPv4 > Relay

DHCP Relay Configuration

Relay Information Mode ……

DHCPオプション82(リレーエージェント情報オプション)を使用するかどうかを設定します。
オプション82で使用するサーキットIDの形式は、「[vlan_id][module_id][port_no]」です。
最初の4文字はVLAN ID、5文字目と6文字目はモジュール ID(スタンドアロンデバイスでは常に0、スタック可能デバイスでは常にスイッチ ID)、最後の2文字はポート番号です。
例:「00030108」は、VLAN IDが3、スイッチIDが1、8番ポートのDHCPメッセージ受信形式を意味します。
オプション82で使用するリモートIDは、スイッチのMACアドレスになります。

Enabled:
DHCPサーバーへ転送時にオプション82をDHCPメッセージへ挿入し、DHCPクライアントへ転送時にDHCPメッセージから削除します。
DHCPリレーが有効になっている場合だけ機能します

Disabled:
オプション82を使用しません。

Relay Information Policy ……

オプション82(リレーエージェント情報オプション)が有効になっている場合、リレーエージェント情報がすでに含まれているDHCPメッセージを受信したときの動作を設定します。

Replace:
リレーエージェント情報がすでに含まれているDHCPメッセージを受信したときに、元のリレーエージェント情報と置き換えます。

Keep:
リレーエージェント情報がすでに含まれているDHCPメッセージを受信したときに、元のリレーエージェント情報を保持します。

Drop:
リレーエージェント情報がすでに含まれているDHCPメッセージを受信したときに、パケットを破棄します。

〈Save〉 …… 設定した内容を保存するボタンです。

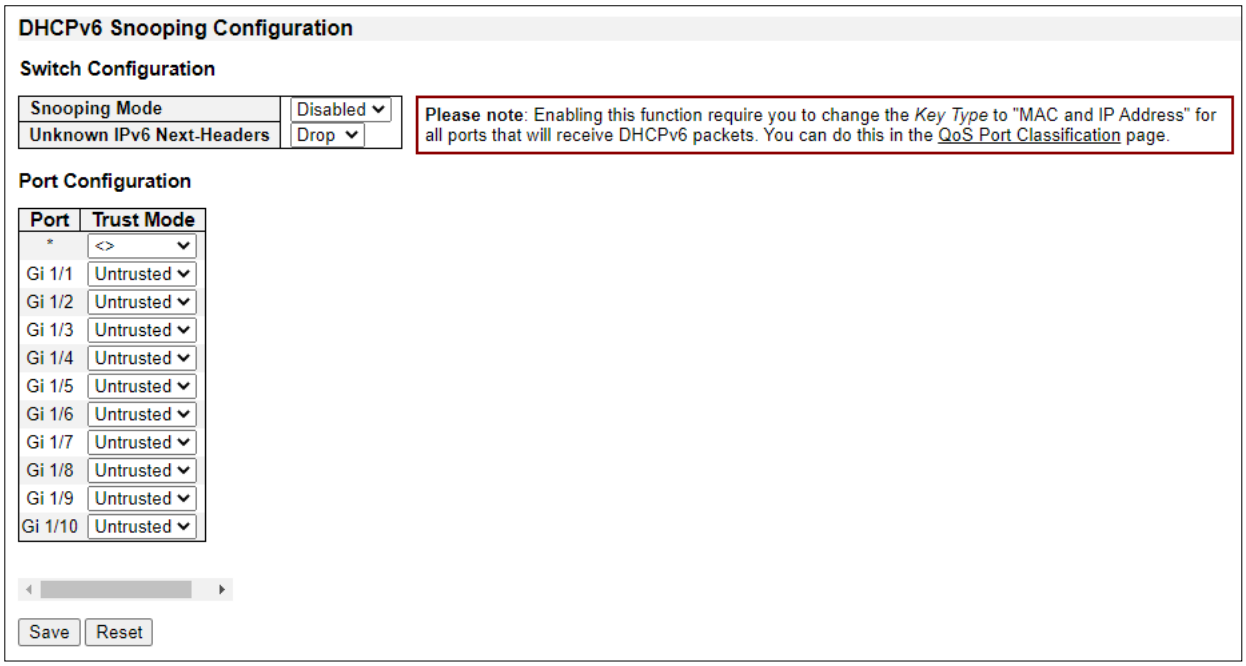
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Snooping」画面

Configuration > DHCPv6 > Snooping

DHCPv6(IPv6経由のDHCP)のスヌーピングを設定します。

DHCPv6 Snooping Configuration



Switch Configuration

Snooping Mode ……

DHCPv6スヌーピングを使用するかどうかを設定します。

Enabled：
DHCPv6スヌーピングを有効にします。
DHCPv6スヌーピングを有効にすると、DHCPv6クライアント要求はtrusted(信頼された)ポートに転送され、trustedポートからの応答パケットだけが許可されます。

Disabled：
DHCPv6スヌーピングを無効にします。

Unknown IPv6 Next-Headers

不明なNext Headerフィールド値のIPv6パケットに対する動作を設定します。
DHCPv6クライアントへのすべてのIPv6パケットを解析してDHCPv6メッセージかどうかを判別しますが、不明なIPv6拡張ヘッダーが検出された場合、解析を続行できません。
※詳細は、RFC7610　セクション5　3項を参照してください。

Drop：
不明なIPv6拡張ヘッダーを持つパケットを破棄します。
安全性は高くなりますが、トラフィックの中断につながる可能性があります。

Allow：
不明なIPv6拡張ヘッダーを持つパケットを許可します。
トラフィックの中断を防げますが、安全性は低くなります。

「Snooping」画面

Configuration > DHCPv6 > Snooping

DHCPv6 Snooping Configuration

Port Configuration

Trust Mode…… DHCPv6スヌーピングを使用するとき、各ポートのモードを設定します。

Trusted：
DHCPv6メッセージの信頼された送信元(trustedポート)に設定します。

Untrusted：
DHCPv6メッセージの信頼されない送信元(untrustedポート)に設定します。

〈Save〉…… 設定した内容を保存するボタンです。

〈Reset〉…… 設定内容を変更したとき、変更前の状態に戻すボタンです。

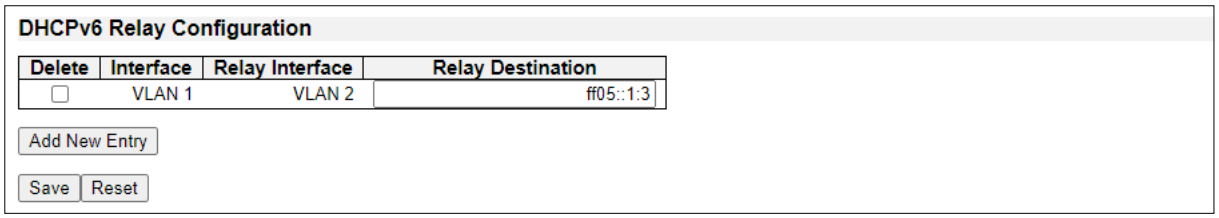
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Relay」画面

Configuration > DHCPv6 > Relay

VLANごとのDHCPv6リレーについて設定します。

DHCPv6 Relay Configuration



Delete …… 登録された内容を削除するとき、ボックスにチェックマークを入れます。

Interface …… インターフェースIDを指定します。

Relay Interface…… 中継に使用するインターフェースのIDを指定します。

Relay Destination …… DHCP要求が転送されるDHCPv6サーバーのIPv6アドレスを、RFC5952で定義されている推奨表記にしたがって指定します。
「ff05::1:3」(初期設定)は、任意のDHCPサーバーになります。

〈Add New Entry〉…… DHCPv6リレー設定を追加するボタンです。

〈Save〉 …… 設定した内容を保存するボタンです。

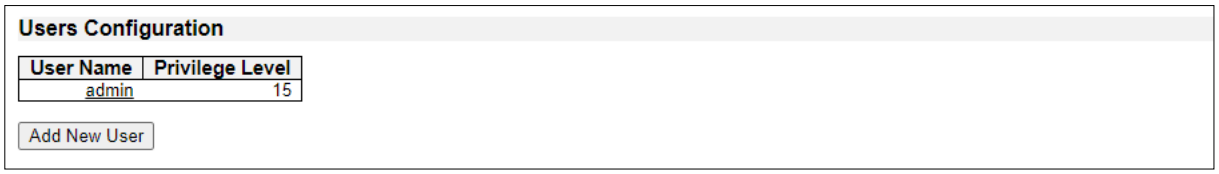
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Users」画面

Configuration > Security > Switch > Users

登録されているユーザーが表示されます。
別のユーザーとしてログインする場合は、一度ブラウザーを閉じてください。

Users Configuration



User Name……　ユーザー名が表示されます。
各ユーザー名のリンク先をクリックすると、「User Edit」画面へ移動します。

Privilege Level……　ユーザーの特権レベルが0～15で表示されます。
特権レベルが15の場合、本製品のすべての設定グループが制御できます。
14以下の場合は、「Privilege Levels」画面の設定にしたがいます。
ユーザーの特権レベルが設定グループのアクセス権を持つ特権レベル以上のとき、各設定グループにアクセスできます。
初期設定では、特権レベル5でほとんどの設定グループの読み取り専用アクセス権を持ち、特権レベル10で読み取り/書き込みアクセス権を持っています。
※システムメンテナンス(ソフトウェアのアップロード、初期化など)には、権限レベル15のアカウントが必要です。
通常、管理者アカウントは特権レベル15、標準ユーザーアカウントは特権レベル10、ゲストアカウントは特権レベル5に設定します。

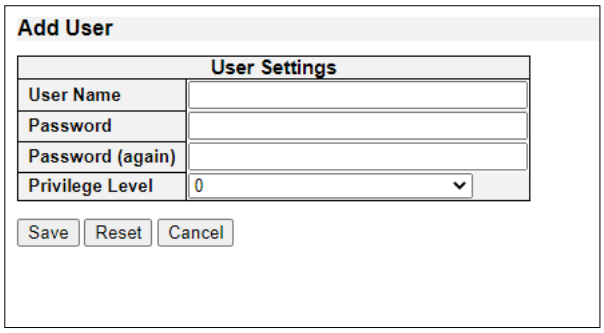
〈Add New User〉……　クリックして新しいユーザーを追加します。
※最大20ユーザーまで登録できます。

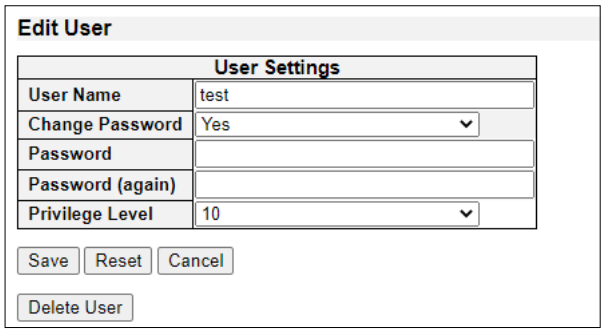
「Add User」画面 / 「Edit User」画面

Configuration > Security > Switch > Users

ユーザーの追加や、登録済みのユーザー設定を変更します。

Add User/Edit User





User Name……

ユーザー名を1～31文字で設定します。
使用できる文字は、英数字、または_(アンダースコア)です。

Password ……

パスワードを0～31文字で設定します。
使用できる文字は、英数字、記号(スペースを含む)です。

Privilege Level ……

ユーザーの特権レベルを設定します。
設定できる範囲は、「0」～「15」です。
特権レベルが15の場合、本製品のすべての設定グループが制御できます。
14以下の場合は、「Privilege Levels」画面の設定にしたがいます。
ユーザーの特権レベルが設定グループのアクセス権を持つ特権レベル以上のとき、各設定グループにアクセスできます。
出荷時の設定では、特権レベル5でほとんどの設定グループの読み取り専用アクセス権を持ち、特権レベル10で読み取り/書き込みアクセス権を持っています。
※システムメンテナンス(ソフトウェアのアップロード、初期化など)には、権限レベル15のアカウントが必要です。
通常、管理者アカウントは特権レベル15、標準ユーザーアカウントは特権レベル10、ゲストアカウントは特権レベル5に設定します。

〈Save〉……

設定した内容を保存するボタンです。

〈Reset〉 ……

設定内容を変更したとき、変更前の状態に戻すボタンです。

〈Cancel〉……

設定内容を変更したとき、変更前の状態に戻し、「Users」画面に戻るボタンです。

〈Delete User〉 ……

表示されているユーザーを削除するボタンです。
※「Add User」画面では表示されません。
※初期設定で登録されている管理者ユーザー(Admin)は、削除できません。

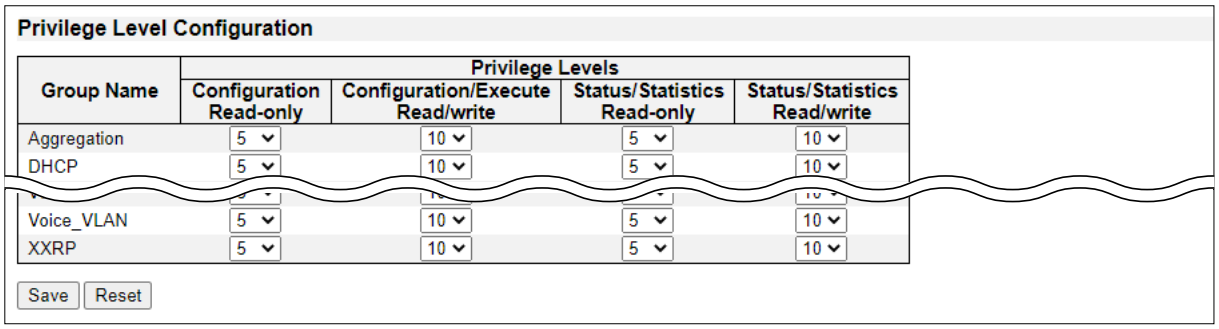
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Privilege Levels」画面

Configuration > Security > Switch > Privilege Levels

設定グループごとの特権レベルを設定します。

Privilege Level Configuration



Group Name ……

特権グループを設定できる各設定グループ名が表示されます。
ほとんどの設定グループは1つの要素(LACP、RSTP、QoSなど)で構成されますが、下記の設定グループは複数の要素を含みます。

System ：Contact、Name、Location、Time Zone、Daylight Saving Time、Log

Security ：Authentication、System Access Management、Port (Dot1x port、MAC based、MAC Address Limitを含む)、ACL、HTTPS、SSH、ARP Inspection、IP source guard

IP ：「ping」以外

Ports ：「VeriPHY」以外

Diagnostics ：ping、VeriPHY

Debug ：コマンドラインインターフェース(CLI)でしか使用できません。

Privilege Levels ……

各設定グループにアクセスできる特権レベルを設定します。
設定できる範囲は、「0」(最低)～「15」(最高)です。
すべての設定グループで、それぞれの権限を持つ特権レベルを設定します。

Configuration Read-only：
設定内容の読み取りだけができます。

Configuration/Execute Read/write：
設定内容の読み取り/書き込みができます。

Status/Statistics Read-only：
ステータスと統計の読み取りだけができます。

Status/Statistics Read/write：
ステータスと統計の読み取り/書き込み(統計情報の削除など)ができます。

〈Save〉 …… 設定した内容を保存するボタンです。

〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Auth Method」画面

Configuration > Security > Switch > Auth Method

Authentication(認証)、Authorization(認可)、Accounting(アカウンティング)について設定します。

Authentication Method Configuration

ユーザーが設定画面にログインするときの認証方法を、管理クライアントが使用するプロトコルごとに設定します。

Client ……　管理クライアントのプロトコルが表示されます。

Methods ……　ログインするときの認証方法を設定します。

no：
認証は無効になります。
※ログインできません。

local：
認証に本製品のローカルユーザーデータベースを使用します。

radius：
認証にリモートRADIUSサーバーを使用します。

tacacs：
認証にリモートTACACS+サーバーを使用します。

リモートサーバーがオフラインの場合、認証にリモートサーバーを使用すると認証要求がタイムアウトし、ユーザーが承認、または拒否されるまで、設定した認証方法が左から順に試行されます。
認証サーバーが稼働していない場合でも、ユーザーがローカルユーザーデータベースを使用してログインできるようにするため、プライマリ認証にリモートサーバーを使用する場合は、セカンダリ認証を「Local」に設定することをおすすめします。

「Auth Method」画面

Configuration > Security > Switch > Auth Method

Command Authorization Method Configuration

CLIコマンドの許可方法を、管理クライアントが使用するプロトコルごとに設定します。

Client …… 管理クライアントのプロトコルが表示されます。

Method…… ユーザーが使用できるCLIコマンドの許可方法を設定します。

no：
コマンド許可は無効になります。
ユーザーの特権レベルに応じたCLIコマンドが使用できます。

tacacs：
コマンド許可にリモートTACACS+サーバーを使用します。
すべてのリモートサーバーがオフラインの場合、ユーザーの特権レベルに応じたCLIコマンドが使用できます。

Cmd Lvl …… リモートTACACS+サーバーを使用するとき、設定したレベル以上の特権レベルを持つすべてのコマンドの使用を許可します。
設定できる範囲は、「0～15」です。

Cfg Cmd …… リモートTACACS+サーバーを使用するとき、構成コマンドの使用を許可するかどうかを設定します。

「Auth Method」画面

Configuration > Security > Switch > Auth Method

Accounting Method Configuration

コマンドとexec(ログイン)アカウンティングについて、管理クライアントが使用するプロトコルごとに設定します。

Client …… 管理クライアントのプロトコルが表示されます。

Method …… アカウンティング方法について設定します。

no：
アカウンティングは無効になります。

tacacs：
アカウンティングにリモートTACACS+サーバーを使用します。

Cmd Lvl …… アカウンティングにリモートTACACS+サーバーを使用するとき、記録するコマンドの特権レベルを設定します。
設定できる範囲は、「0～15」です。
※空白にすると、コマンドの使用を監視しません。

Exec …… exec(ログイン)を記録するかどうかを設定します。

〈Save〉 …… 設定した内容を保存するボタンです。

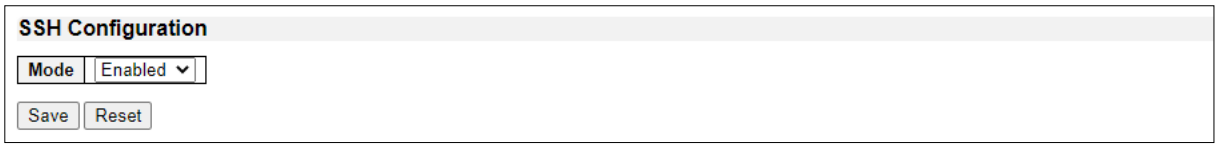
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「SSH」画面

Configuration > Security > Switch > SSH

SSHクライアントからのアクセスについて設定します。

SSH Configuration



Mode…… 本製品へのSSHプロトコルによるアクセス許可を設定します。
※SSHを使用すると、SSHクライアントプログラムを使用して設定する内容を暗号化して通信できます。
※SSHを使用するには、別途SSHクライアントをご用意ください。

Enabled：
SSHプロトコルによるアクセスを有効にします。

Disabled：
SSHプロトコルによるアクセスを無効にします。

〈Save〉…… 設定した内容を保存するボタンです。

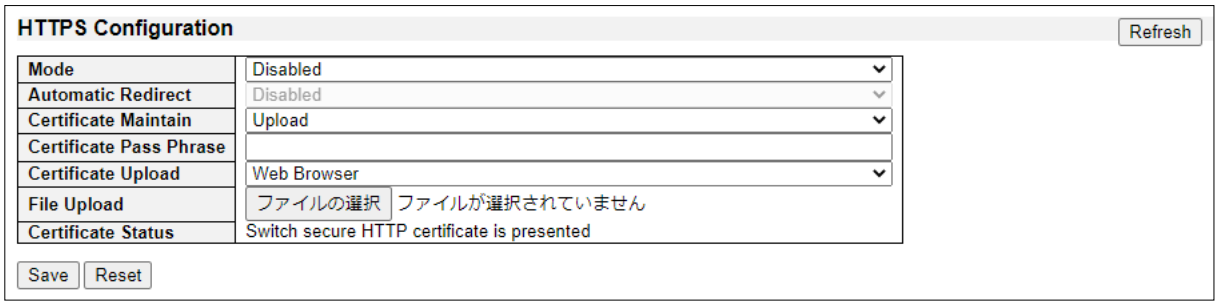
〈Reset〉…… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「HTTPS」画面

Configuration > Security > Switch > HTTPS

HTTPSは、WWWブラウザーから設定画面にアクセスするためのプロトコルです。
HTTPSを使用すると、パスワードやデータが暗号化されるため、TelnetやHTTPでのアクセスより安全性が向上します。

HTTPS Configuration



Mode ……

本製品へのHTTPSプロトコルによるアクセスの許可を設定します。

Enabled：
HTTPSプロトコルによるアクセスを有効にします。

Disabled：
HTTPSプロトコルによるアクセスを無効にします。

Automatic Redirect ……

HTTPSプロトコルによるアクセスが有効に設定されているとき、HTTP接続を自動的にHTTPS接続にリダイレクトするかを設定します。
本製品に登録した証明書がWWWブラウザーによって信頼できないと判断された場合、セキュリティー保持のためリダイレクトされないことがあります。
リダイレクトされなかった場合は、HTTPS接続を手動で初期化してください。

Enabled：
リダイレクトを有効にします。

Disabled：
リダイレクトを無効にします。

Certificate Maintain ……

使用する証明書を管理します。

None：
証明書を変更しません。

Delete：
登録されている証明書を削除します。

Upload：
証明書(PEM形式)を登録します。
アップロード方法はWWWブラウザー経由、またはURL経由から選択できます。

Generate：
RSA暗号方式の自己署名証明書を作成します。

Certificate Pass Phrase ……

[Certificate Maintain]欄で「Upload」を選択したときに表示されます。
登録する証明書がパスフレーズで保護されている場合は、パスフレーズを入力します。

「HTTPS」画面

Configuration > Security > Switch > HTTPS

HTTPS Configuration

Certificate Upload ……

[Certificate Maintain]欄で「Upload」を選択したときに表示されます。
証明書(PEM形式)の登録方法を選択します。
※登録する証明書に、証明書と秘密鍵の両方が含まれている必要があります。
証明書と秘密鍵が別ファイルの場合は、Linux catコマンドを使用して1つのPEMファイルに結合してください。(例：cat my.cert my.key > my.pem)
※新しいバージョンのブラウザー(Firefox v37やChrome v39など)では、DSA署名方式の証明書はサポート対象外で、RSA暗号方式の証明書が推奨されています。

Web Browser：
WWWブラウザー経由で証明書を登録します。

URL：
証明書のURLを指定します。

File Upload ……

WWWブラウザー経由で証明書を登録するときに、使用するファイルを選択します。

URL ……

証明書ファイルのURLを63文字以内で入力します。
サポートされているプロトコルは HTTP、HTTPS、FTFP、FTPです。
URLは、「<protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>]/<file_name>」の形式で指定します。
(例：tftp://10.10.10.10/new_image_path/new_image.dat、
http://username:password@10.10.10.10:80/new_image_path/new_image.dat)
使用できる文字は、半角英数字(A～Z、a～z、0～9、.、－)、スペースです。
※「－(ハイフン)」は1文字目に入力できません。
※ファイル名が「.(ドット)」だけの場合は登録できません。

Certificate Status ……

証明書のステータスが表示されます。

Switch secure HTTP certificate is presented.
HTTP証明書は登録済みです。

Switch secure HTTP certificate is not presented.
HTTP証明書が未登録です。

Switch secure HTTP certificate is generating ...
HTTP証明書を作成しています。

〈Save〉 ……

設定した内容を保存するボタンです。

〈Reset〉 ……

設定内容を変更したとき、変更前の状態に戻すボタンです。

〈Refresh〉 ……

最新の状態に更新するボタンです。
※設定内容を変更したときは、変更前の状態に戻ります。

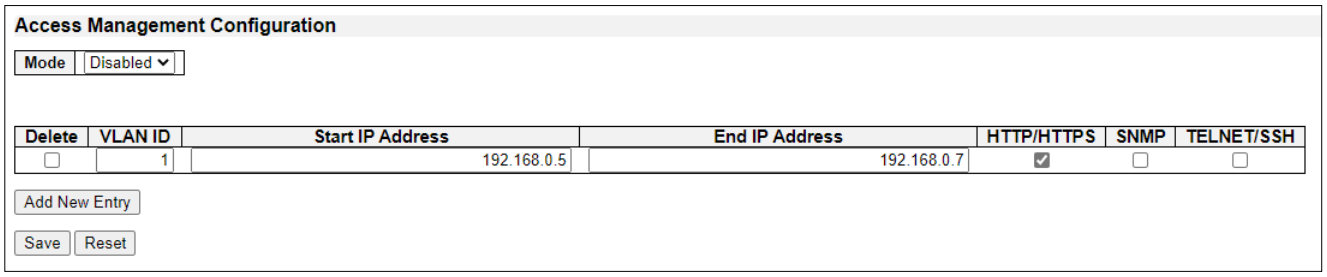
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Access Management」画面

Configuration > Security > Switch > Access Management

本製品の各種情報にアクセスできるユーザーとプロトコルを制限します。
※最大16件まで登録できます。

Access Management Configuration



Mode …… 登録したIPアドレス以外のユーザーからのアクセスを制限するかを設定します。

Enabled：
登録したIPアドレス以外のユーザーからのアクセスを制限します。

Disabled：
IPアドレスでのアクセス制限を使用しません。

Delete …… 登録された内容を削除するとき、ボックスにチェックマークを入れます。

VLAN ID …… VLAN IDを指定します。

Start IP Address/End IP Address …… 本製品の各種情報にアクセスできるユーザーのIPユニキャストアドレス範囲を指定します。

HTTP/HTTPS …… 指定したIPアドレス範囲のユーザーに、HTTP/HTTPSプロトコルで本製品へのアクセスを許可するとき、ボックスにチェックマークを入れます。
チェックマークが入っていないと、ユーザーのIPアドレスが指定したIPアドレス範囲と一致していても、HTTP/HTTPSプロトコルで本製品へアクセスできません。

SNMP …… 指定したIPアドレス範囲のユーザーに、SNMPプロトコルで本製品へのアクセスを許可するとき、ボックスにチェックマークを入れます。
チェックマークが入っていないと、ユーザーのIPアドレスが指定したIPアドレス範囲と一致していても、SNMPプロトコルで本製品へアクセスできません。

TELNET/SSH …… 指定したIPアドレス範囲のユーザーに、Telnet/SSHプロトコルで本製品へのアクセスを許可するとき、ボックスにチェックマークを入れます。
チェックマークが入っていないと、ユーザーのIPアドレスが指定したIPアドレス範囲と一致していても、Telnet/SSHプロトコルで本製品へアクセスできません。

〈Add New Entry〉 …… アクセスできるユーザーのIPアドレス範囲を追加するボタンです。

〈Save〉 …… 設定した内容を保存するボタンです。

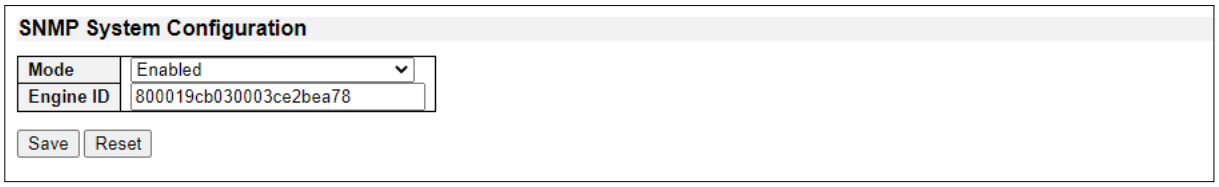
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「System」画面

Configuration > Security > Switch > SNMP > System

IPネットワークにおいて、ネットワーク上の各ホストから本製品の情報を自動的に収集して、ネットワーク管理をするときの設定です。

SNMP System Configuration



Mode…… 本製品のSNMP機能を設定します。

Enabled：
SNMP機能を有効にします。

Disabled：
SNMP機能を無効にします。

Engine ID…… SNMPv3 エンジンIDを、10～64桁の偶数(16進数)で指定します。
※すべて0やすべてFは設定できません。
※指定したエンジンIDのユーザーだけがローカルユーザーとして本製品にアクセスできます。
エンジンIDを変更すると、現在のローカルユーザーが本製品にアクセスできなくなりますのでご注意ください。

〈Save〉…… 設定した内容を保存するボタンです。

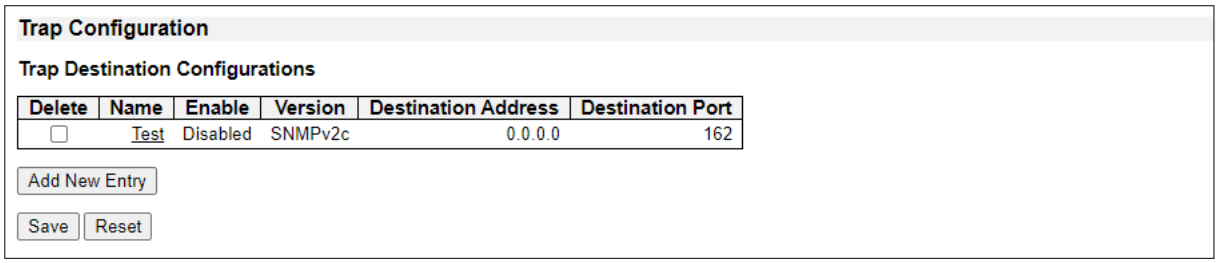
〈Reset〉…… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Destinations」画面

Configuration > Security > Switch > SNMP > Trap > Destinations

登録したSNMPトラップ設定一覧が表示されます。

Trap Configuration



Trap Destination Configurations

Delete …… 登録された内容を削除するとき、ボックスにチェックマークを入れます。

Name …… SNMPトラップ名が表示されます。
各トラップ名のリンク先をクリックすると、「SNMP Trap Configuration」画面へ移動します。

Enable …… SNMPトラップが有効かどうか表示されます。

Version…… 使用するSNMPプロトコル(SNMPv1、SNMPv2c、SNMPv3)が表示されます。

Destination Address …… SNMPトラップの宛先IPアドレス、またはホスト名が表示されます。

Destination Port …… SNMPトラップの宛先ポートが表示されます。
SNMPエージェントは設定されたポートを介してSNMPメッセージを送信します。

〈Add New Entry〉…… クリックして新しいSNMPトラップ設定を追加します。

〈Save〉 …… 設定した内容を保存するボタンです。

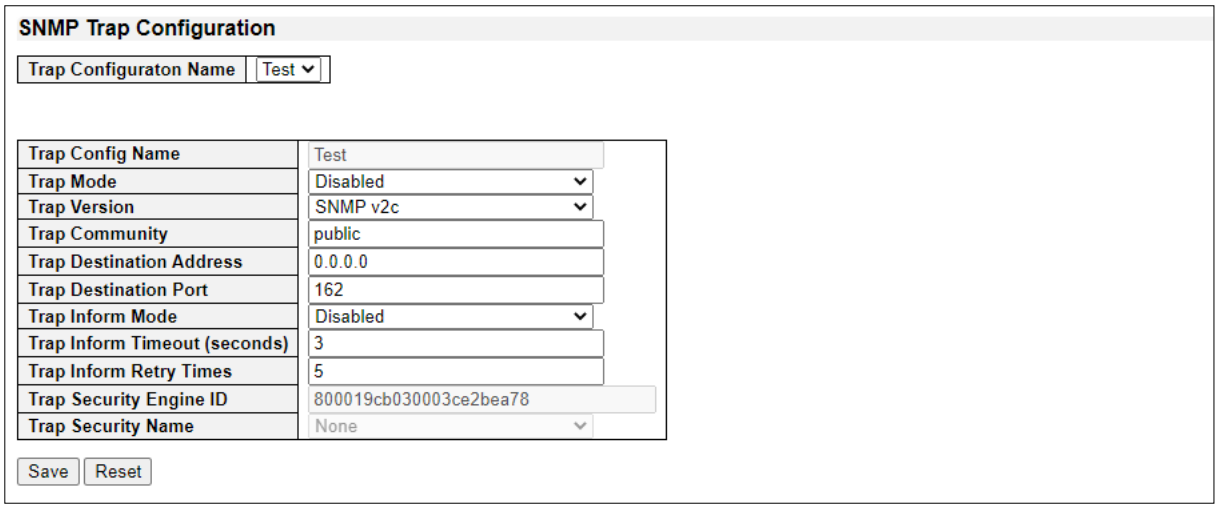
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「SNMP Trap Configuration」画面

Configuration > Security > Switch > SNMP > Trap > Destinations

SNMPトラップについて設定します。

SNMP Trap Configuration



Trap Configuration Name …… 設定を変更するSNMPトラップを選択します。

Trap Config Name …… SNMPトラップ名を、32文字以内で入力します。
使用できる文字列は、33～126までのASCII文字です。

Trap Mode …… SNMPトラップを有効にするかを設定します。

Enabled：
SNMPトラップを有効にします。

Disabled：
SNMPトラップを無効にします。

Trap Version …… 使用するSNMPプロトコルを指定します。

Trap Community …… SNMPトラップパケットを送信するときのコミュニティ名を、0～63文字で入力します。
使用できる文字列は、33～126までのASCII文字です。

Trap Destination Address …… SNMPトラップの宛先を、IPアドレス（ドット付き10進表記、またはIPv6表記）かホスト名で指定します。
ホスト名で指定する場合、使用できる文字列は、半角英数字（a～z、A～Z、0～9、.、－）です。
※スペースは使用できません。
※「－（ハイフン）」や「.（ドット）」を先頭、または末尾に使用すると、登録できません。

Trap Destination Port …… SNMPトラップの宛先ポートを指定します。
SNMPエージェントは指定したポートを介してSNMPメッセージを送信します。
設定できる範囲は、「1～65535」です。

「SNMP Trap Configuration」画面

Configuration > Security > Switch > SNMP > Trap > Destinations

SNMP Trap Configuration

Trap Inform Mode …… SNMPトラップ通知を有効にするかを設定します。

Trap Inform Timeout (seconds) SNMPトラップ通知のタイムアウト時間を設定します。
設定できる範囲は、「0～2147」(秒)です。

Trap Inform Retry Times …… SNMPトラップ通知の再試行時間を設定します。
設定できる範囲は、「0～255」です。

Trap Security Engine ID …… SNMPエンジンIDを、10桁から64桁までの偶数(16進数)で指定します。
SNMPv3は、ユーザー認証とプライバシー機能のためにUSMを使用してトラップを送信、通知します。
トラップの送信と通知には、エンジンIDが必要です。
※すべて「0」やすべて「F」は使用できません。

Trap Security Name …… SNMPトラップのセキュリティー名を指定します。
SNMPv3は、ユーザー認証とプライバシー機能のためにUSMを使用してトラップを送信、通知します。
トラップの送信と通知には、セキュリティー名が必要です。

〈Save〉 …… 設定した内容を保存するボタンです。

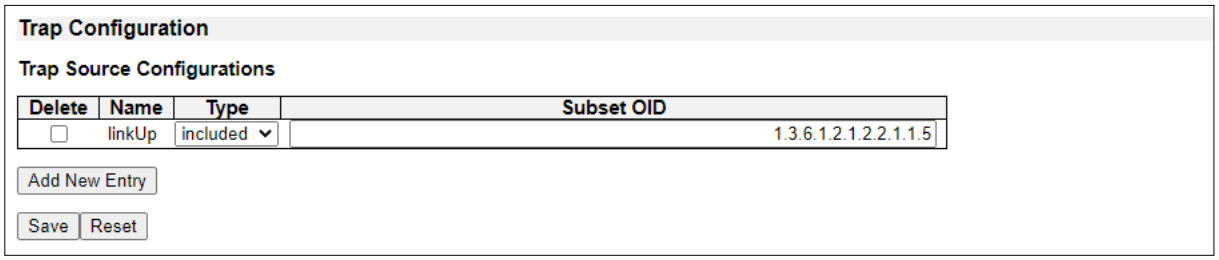
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Sources」画面

Configuration > Security > Switch > SNMP > Trap > Sources

SNMPトラップソースについて設定します。
「included」フィルターと1つ以上一致し、「excluded」フィルターと一致しない場合、指定したトラップソースのトラップが送信されます。

Trap Configuration



Trap Source Configurations

Delete …… 登録された内容を削除するとき、ボックスにチェックマークを入れます。

Name …… SNMPトラップソース名を指定します。

Type …… フィルターの種類を指定します。

included：
指定したトラップソースを含むトラップを送信します。

excluded：
指定したトラップソースを含むトラップは送信しません。

Subset OID…… サブセットOIDを指定します。
サブセットOIDは、トラップ名によって異なります。
たとえば、「ifIndex」はlinkUpとlinkDownのサブセットOIDです。
サブセットOIDは、「.（ドット）」で区切られた1つ以上のデジタル番号（0～4294967295）、または「*（アスタリスク）」で指定してください。
※「*（アスタリスク）」を先頭に使用すると、登録できません。
※1つのOIDを構成するサブOIDは、最大128個までです。

〈Add New Entry〉…… クリックして新しいSNMPトラップソースを追加します。
※最大32件まで登録できます。

〈Save〉 …… 設定した内容を保存するボタンです。

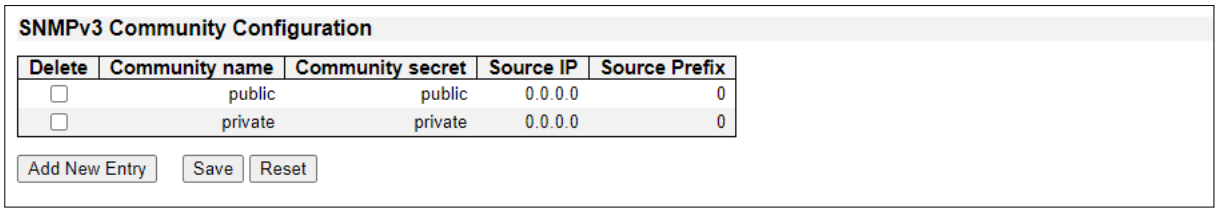
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Communities」画面

Configuration > Security > Switch > SNMP > Communities

SNMPv3コミュニティテーブルを設定します。
インデックスキーは[Community]です。

SNMPv3 Community Configuration



Delete …… 登録された内容を削除するとき、ボックスにチェックマークを入れます。

Community name …… SNMPグループのコミュニティ名を1～32文字で指定します。
使用できる文字列は、33～126までのASCII文字です。

Community secret …… SNMPv1やSNMPv2cを使用したSNMPエージェントへのアクセスを許可するコミュニティ名を、1～32文字で指定します。
使用できる文字列は、33～126までのASCII文字です。

Source IP …… SNMPアクセス元アドレスを指定します。
[Source Prefix]欄との組み合わせで、ソースアドレスの特定範囲のサブネットに制限できます。

Source Prefix …… SNMPアクセス元アドレスのプレフィックス長を指定します。

〈Add New Entry〉 …… クリックして新しいコミュニティを追加します。

〈Save〉 …… 設定した内容を保存するボタンです。

〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

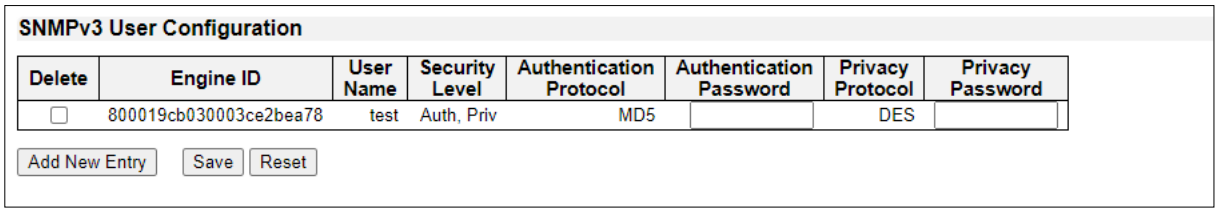
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Users」画面

Configuration > Security > Switch > SNMP > Users

SNMPv3ユーザーテーブルを設定します。
インデックスキーは[Engine ID]と[User Name]です。

SNMPv3 User Configuration



Delete …… 登録された内容を削除するとき、ボックスにチェックマークを入れます。

Engine ID…… SNMPエンジンIDを、10桁から64桁までの偶数（16進数）で指定します。
※すべて「0」やすべて「F」は使用できません。

SNMPv3アーキテクチャは、メッセージレベルのセキュリティーにUSM（User-based Security Model）を使用し、アクセス制御にVACM（View-based Access Control Model）を使用します。
USMエントリの場合、usmUserEngineIDとusmUserNameがエントリのキーです。
単純なエージェントでは、usmUserEngineIDは常にそのエージェント独自のsnmpEngineIDの値になります。
usmUserEngineIDは、このユーザーが通信できるリモートSNMPエンジンのsnmpEngineIDの値をとることもできます。
ユーザー・エンジンIDがシステム・エンジンIDと等しい場合は、ローカルユーザーになります。
それ以外の場合は、リモートユーザーになります。

User Name…… ユーザー名を1～32文字で指定します。
使用できる文字列は、33～126までのASCII文字です。

Security Level …… セキュリティーレベルを設定します。
※一度登録した内容は変更できません。
　登録前に正しく設定されていることを確認してください。

NoAuth, NoPriv：
ユーザー認証とプライバシー機能を使用しません。

Auth, NoPriv：
ユーザー認証は使用しますが、プライバシー機能は使用しません。

Auth, Priv：
ユーザー認証とプライバシー機能の両方を使用します。

「Users」画面

Configuration > Security > Switch > SNMP > Users

SNMPv3 User Configuration

Authentication Protocol ……
使用するユーザー認証プロトコルを指定します。
※一度登録した内容は変更できません。
　登録前に正しく設定されていることを確認してください。

None(空白)：
ユーザー認証プロトコルを使用しません。

MD5：
MD5認証プロトコルを使用します。

SHA：
SHA認証プロトコルを使用します。

Authentication Password ……
認証パスワードを指定します。
MD5認証プロトコルを使用する場合は、8～32文字で指定します。
SHA認証プロトコルを使用する場合は、8～40文字で指定します。
使用できる文字列は、33～126までのASCII文字です。

Privacy Protocol ……
使用するプライバシー・プロトコルを指定します。

None(空白)：
プライバシー機能を使用しません。

DES：
DESプロトコルを使用します。

AES：
AESプロトコルを使用します。

Privacy Password ……
プライバシーパスワードを8～32文字で指定します。
使用できる文字列は、33～126までのASCII文字です。

〈Add New Entry〉……
クリックして新しいユーザーを追加します。

〈Save〉 ……
設定した内容を保存するボタンです。

〈Reset〉 ……
設定内容を変更したとき、変更前の状態に戻すボタンです。

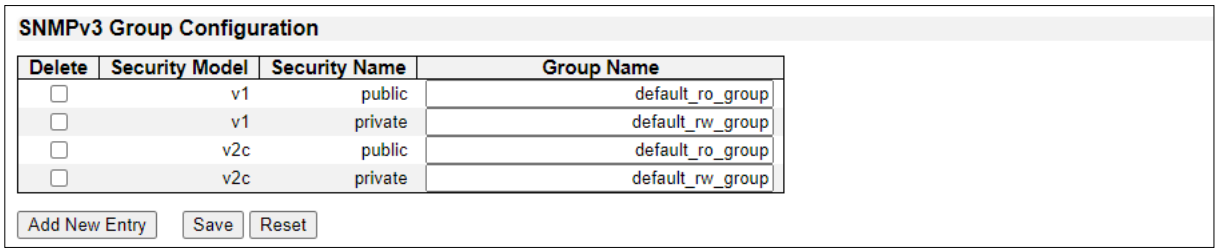
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Groups」画面

Configuration > Security > Switch > SNMP > Groups

SNMPv3グループテーブルを設定します。
インデックスキーは[Security Model]と[Security Name]です。

SNMPv3 Group Configuration



Delete …… 登録された内容を削除するとき、ボックスにチェックマークを入れます。

Security Model …… 使用するセキュリティーモデルを指定します。

v1 ：SNMPv1プロトコルを使用します。

v2c ：SNMPv2cプロトコルを使用します。

usm ：USMを使用します。

Security Name …… セキュリティー名を1～32文字で指定します。
使用できる文字列は、33～126までのASCII文字です。

Group Name …… グループ名を1～ 32文字で指定します。
使用できる文字列は、33～126までのASCII文字です。

〈Add New Entry〉 …… クリックして新しいグループを追加します。

〈Save〉 …… 設定した内容を保存するボタンです。

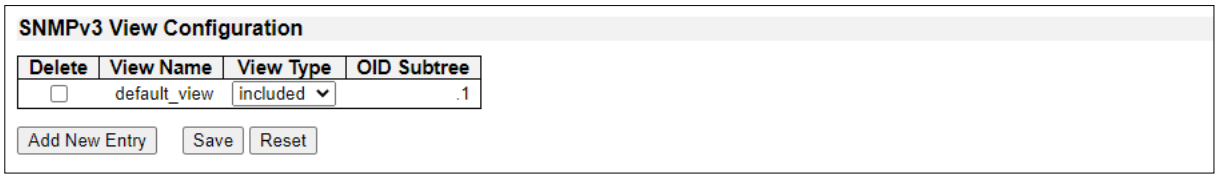
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Views」画面

Configuration > Security > Switch > SNMP > Views

SNMPv3ビューテーブルを設定します。
インデックスキーは[View Name]と[OID Subtree]です。

SNMPv3 View Configuration



Delete …… 登録された内容を削除するとき、ボックスにチェックマークを入れます。

View Name …… SNMPビューの名称を1～32文字で指定します。
使用できる文字列は、33～126までのASCII文字です。

View Type …… SNMPビューの種類を指定します。

included ：指定したOIDサブツリーを対象に含めます。

excluded ：指定したOIDサブツリーを除外します。

※通常は、[View Type]欄が「excluded」のビューを登録した場合、OIDサブツリーの長さが「excluded」ビューを越える「included」ビューを登録する必要があります。

OID Subtree …… サブツリーのルートを定義するOIDを指定します。
OIDは、「.(ドット)」で区切られた1つ以上のデジタル番号(0～4294967295)、または「*(アスタリスク)」で指定してください。
※1つのOIDを構成するサブOIDは、最大128個までです。

〈Add New Entry〉 …… クリックして新しいSNMPビュー設定を追加します。

〈Save〉 …… 設定した内容を保存するボタンです。

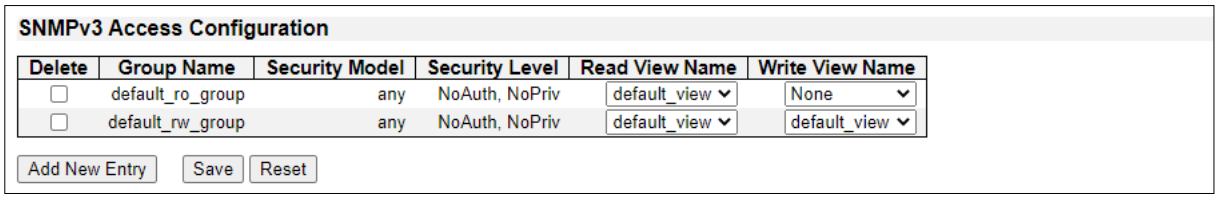
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Access」画面

Configuration > Security > Switch > SNMP > Access

SNMPv3アクセステーブルを設定します。
インデックスキーは、[Group Name]、[Security Model]、[Security Level]です。

SNMPv3 Access Configuration



Delete …… 登録された内容を削除するとき、ボックスにチェックマークを入れます。

Group Name …… 「Groups」画面で設定したグループから、グループ名を選択します。

Security Model …… セキュリティーモデルを指定します。

any ：SNMPv1、SNMPv2c、USMのうちのどれかを使用します。

v1 ：SNMPv1プロトコルを使用します。

v2c ：SNMPv2cプロトコルを使用します。

usm ：USMを使用します。

Security Level …… セキュリティーレベルを設定します。
※一度登録した内容は変更できません。
登録前に正しく設定されていることを確認してください。

NoAuth, NoPriv：
ユーザー認証とプライバシー機能を使用しません。

Auth, NoPriv：
ユーザー認証は使用しますが、プライバシー機能は使用しません。

Auth, Priv：
ユーザー認証とプライバシー機能の両方を使用します。

Read View Name …… 「Views」画面のビューテーブルから、読み取り用MIBビューを選択します。

Write View Name …… 「Views」画面のビューテーブルから、書き込み用MIBビューを選択します。

〈Add New Entry〉 …… クリックして新しいSNMPアクセス設定を追加します。

〈Save〉 …… 設定した内容を保存するボタンです。

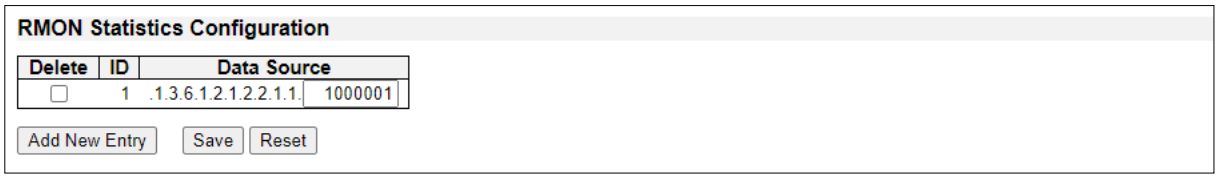
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Statistics」画面

Configuration > Security > Switch > RMON > Statistics

RMON統計情報テーブルを設定します。
インデックスキーは[ID]です。

RMON Statistics Configuration



Delete …… 登録された内容を削除するとき、ボックスにチェックマークを入れます。

ID …… IDを指定します。
設定できる範囲は、「1～65535」です。

Data Source …… 監視するポートIDを指定します。
スイッチスタッキングを使用している場合は、
「1000000 * (スイッチID － 1) ＋ ポート番号」になります。
たとえば、スイッチ3 ポート5の場合、値は2000005です。

〈Add New Entry〉…… クリックして新しい監視対象を追加します。

〈Save〉 …… 設定した内容を保存するボタンです。

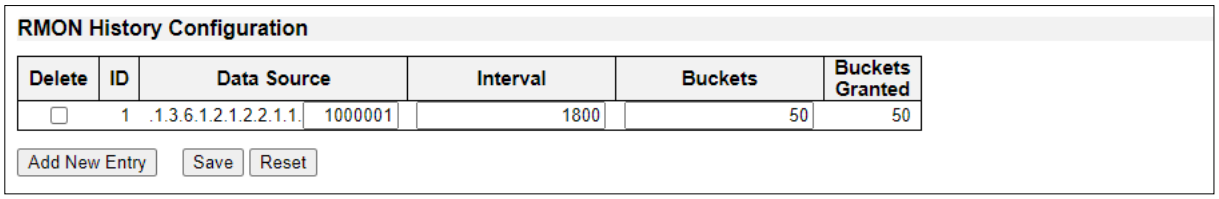
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「History」画面

Configuration > Security > Switch > RMON > History

RMON履歴テーブルを設定します。
インデックスキーは[ID]です。

RMON History Configuration



Delete …… 登録された内容を削除するとき、ボックスにチェックマークを入れます。

ID …… IDを指定します。
設定できる範囲は、「1～65535」です。

Data Source …… 監視するポートIDを指定します。
スイッチスタッキングを使用している場合は、
「1000000 * (スイッチID － 1) ＋ ポート番号」になります。
たとえば、スイッチ3 ポート5の場合、値は2000005です。

Interval…… 統計情報データを履歴に保存する間隔を指定します。
設定できる範囲は、「1～3600」(秒)です。

Buckets …… RMON履歴に保存される最大データ数を指定します。
設定できる範囲は、「1～3600」です。

Buckets Granted…… RMON履歴に保存されるデータ数が表示されます。

〈Add New Entry〉…… クリックして新しいRMON履歴の監視対象を追加します。

〈Save〉 …… 設定した内容を保存するボタンです。

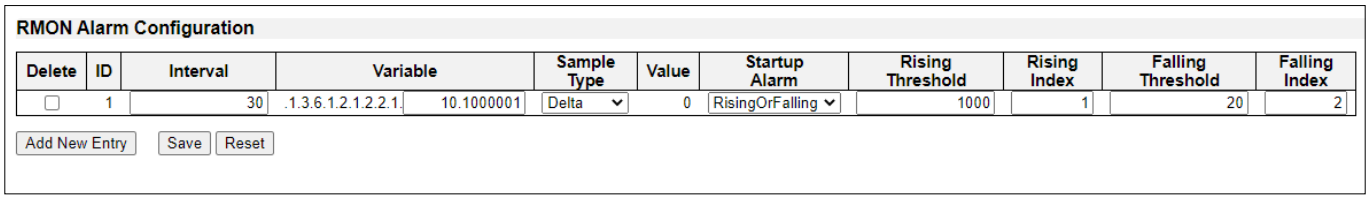
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Alarm」画面

Configuration > Security > Switch > RMON > Alarm

RMONアラームテーブルを設定します。
インデックスキーは[ID]です。

RMON Alarm Configuration



Delete ……　登録された内容を削除するとき、ボックスにチェックマークを入れます。

ID ……　IDを指定します。
設定できる範囲は、「1～65535」です。

Interval……　監視対象の値を取得し、しきい値と比較する間隔を指定します。
設定できる範囲は、「1～$2^{31}-1$」(秒)です。

Variable ……　監視対象のOIDを、「XXX.YYY」形式で指定します。

Sample Type ……　指定したOIDの値をしきい値と比較する方法を指定します。

Absolute：
取得した値をしきい値と比較します。

Delta：
前回取得した値と、今回取得した値の差をしきい値と比較します。

Value……　最後に取得した値が表示されます。

Startup Alarm ……　比較するしきい値を選択します。

Rising：
取得した値を上昇しきい値と比較し、上昇しきい値を上回るとアラームをトリガーします。

Falling：
取得した値を下降しきい値と比較し、下降しきい値を下回るとアラームをトリガーします。

RisingOrFalling：
取得した値を上昇しきい値、下降しきい値と比較し、上昇しきい値を上回るか、下降しきい値を下回るとアラームをトリガーします。

Rising Threshold ……　上昇しきい値を指定します。
設定できる範囲は、「−2147483648～2147483647」です。

Rising Index ……　上昇しきい値を上回ったときのイベントIDを指定します。
設定できる範囲は、「0～65535」です。
※「0」に設定した場合、イベントは実行されません。
※イベントは「Event」画面で設定します。

「Alarm」画面

Configuration > Security > Switch > RMON > Alarm

RMON Alarm Configuration

Falling Threshold…… 下降しきい値を指定します。
設定できる範囲は、「−2147483648～2147483647」です。

Falling Index …… 下降しきい値を下回ったときのイベントIDを指定します。
設定できる範囲は、「0～65535」です。
※「0」に設定した場合、イベントは実行されません。
※イベントは「Event」画面で設定します。

〈Add New Entry〉…… クリックして新しいRMONアラーム設定を追加します。

〈Save〉 …… 設定した内容を保存するボタンです。

〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

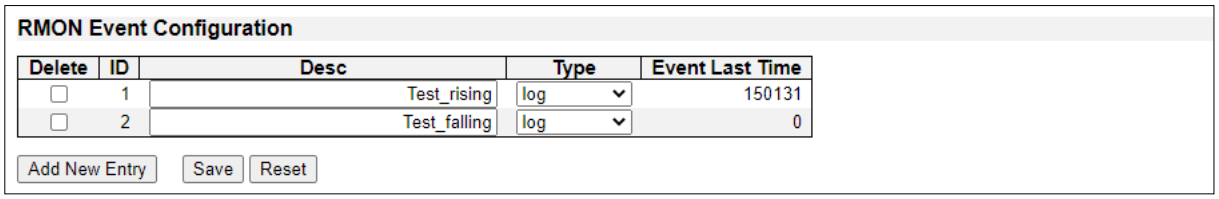
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Event」画面

Configuration > Security > Switch > RMON > Event

RMONイベントテーブルを設定します。
インデックスキーは[ID]です。

RMON Event Configuration



Delete …… 登録された内容を削除するとき、ボックスにチェックマークを入れます。

ID …… IDを指定します。
設定できる範囲は、「1～65535」です。

Desc …… イベントの説明を0～127文字で入力します。

Type …… イベントの通知方法を指定します。

none：
SNMPログは作成せず、SNMPトラップも送信しません。

log：
SNMPログを作成します。

snmptrap：
SNMPトラップを送信します。

logandtrap：
SNMPログを作成し、SNMPトラップを送信します。

Event Last Time …… 最後にイベントを実行したときの、sysUpTime値が表示されます。

〈Add New Entry〉 …… クリックして新しいRMONイベントを追加します。

〈Save〉 …… 設定した内容を保存するボタンです。

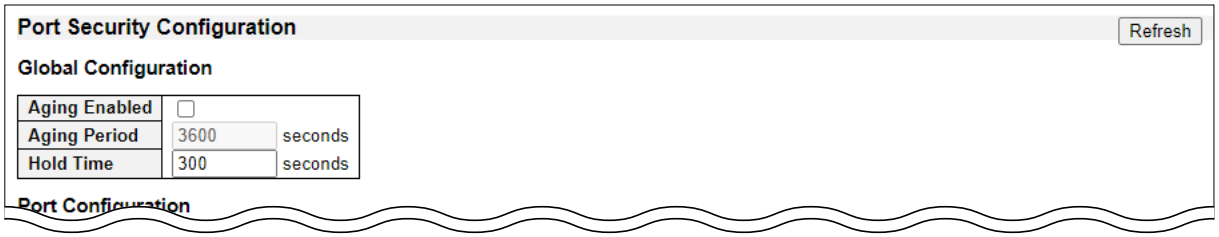
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Port Security」画面

Configuration > Security > Network > Port Security

ポートセキュリティーについて設定します。
ポートセキュリティーを使用すると、特定のポートに対するユーザー数を制限できます。
ユーザーは、MACアドレスとVLAN IDで識別されます。
ポートセキュリティーが有効になっている場合、ポートの最大ユーザー数を[Limit]欄で設定します。
最大ユーザー数を超えると、[Violation Mode]欄の設定が実行されます。

Port Security Configuration



〈Refresh〉 …… 最新の状態に更新するボタンです。

Global Configuration

Aging Enabled …… セキュアMACアドレスのエージングについて設定します。
エージングを有効にした場合、[Aging Enabled]欄で設定された期間が過ぎるとセキュアMACアドレスが期限切れになります。

Aging Period …… エージングが有効な場合に、エージング期間を指定します。
ほかの機能でも同様のセキュリティー機能を使用している場合、すべての機能の中で最も短いエージング期間を使用します。
設定できる範囲は、「10～10000000」(秒)です。

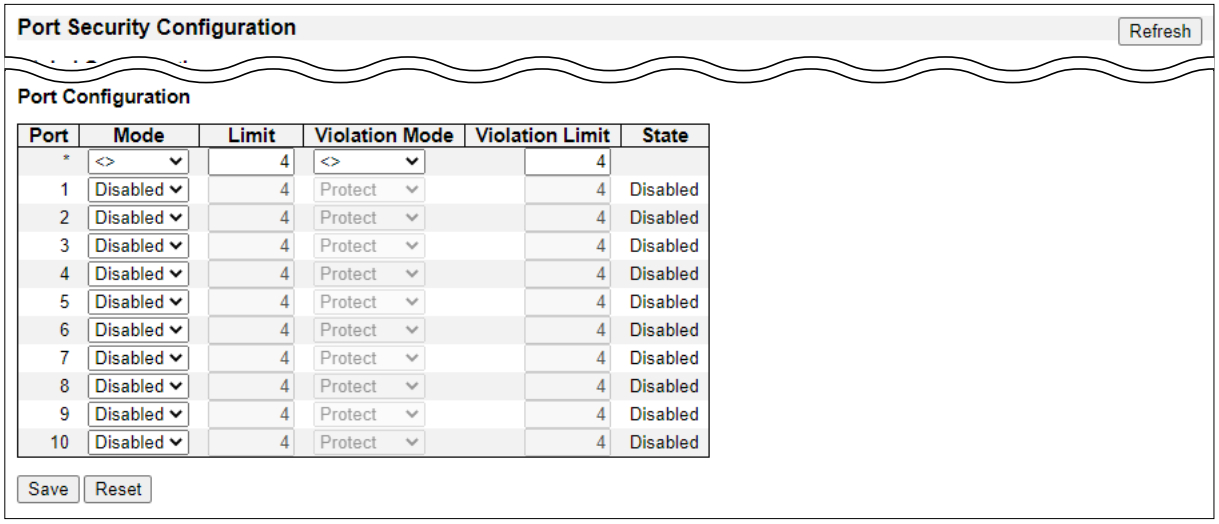
Hold Time …… セキュアMACアドレスが最大数に達している場合に、違反MACアドレスがMACアドレステーブルに保持される時間を指定します。
設定できる範囲は、「10～10000000」(秒)です。
おもに、違反MACアドレスに関する通知が有効な場合に、同じMACアドレスが通知を繰り返さないようにするため、MACアドレステーブルに違反MACアドレスを保持します。

エージングについて
たとえば、エンドホストが他社製のスイッチかHUBに接続され、そのスイッチかHUBをポートセキュリティーが有効になっている本製品のポートに接続しているとき、セキュアMACアドレスの最大数を超えない場合にエンドホストの転送を許可します。
エンドホストがログオフ、またはエンドホストの電源が切られたときに、エージングが無効の場合、エンドホストは本製品のリソースを占有し、転送が許可されつづけます。
エージングを有効にすると、エンドホストがセキュアMACアドレスと判断されたときにタイマーが開始されます。
タイマーが終了すると、エンドホストからのフレームの検索を開始し、エンドホストからのフレームが次のエージング期間内に見つからなかった場合、エンドホストは切断されていると見なされ、対応するリソースが解放されます。

「Port Security」画面

Configuration > Security > Network > Port Security

Port Security Configuration



Port	Mode	Limit	Violation Mode	Violation Limit	State
*	<>	4	<>	4	
1	Disabled	4	Protect	4	Disabled
2	Disabled	4	Protect	4	Disabled
3	Disabled	4	Protect	4	Disabled
4	Disabled	4	Protect	4	Disabled
5	Disabled	4	Protect	4	Disabled
6	Disabled	4	Protect	4	Disabled
7	Disabled	4	Protect	4	Disabled
8	Disabled	4	Protect	4	Disabled
9	Disabled	4	Protect	4	Disabled
10	Disabled	4	Protect	4	Disabled

Port Configuration

Port …… 本製品のポート番号が表示されます。

Mode …… ポートセキュリティー機能を有効にするかどうかを設定します。
※ポートセキュリティー機能が無効でも、ほかの機能がポートセキュリティー機能を使用している場合があります。

Limit …… セキュアMACアドレスの最大数を指定します。
設定できる範囲は、「0～1023」です。
最大数を超えると、[Violation Mode]欄の設定が実行されます。

「Port Security」画面

Configuration > Security > Network > Port Security

Port Security Configuration

Violation Mode ……

セキュアMACアドレスが[Limit]欄で設定した上限に達したときの動作を指定します。

Protect：
[Limit]欄で設定した上限に達したあとは、新しいMACアドレスの転送を許可しません。

Restrict：
[Limit]欄で設定した上限に達したあとのMACアドレスが、違反MACアドレスとして登録されます。
違反MACアドレスは、[Hold Time]欄で設定した期間終了時にMACアドレステーブルから削除されます。

Shutdown：
[Limit]欄で設定した上限に達したあと、MACアドレスが1つ追加されると、ポートをシャットダウンします。
ポートがシャットダウン状態になると、すべてのセキュアMACアドレスがポートから削除され、新しいMACアドレスが学習されなくなります。
ポートを再起動するには3つの方法があります。
◎「Configuration」→「Ports」の[Configured]欄で、「Disabled」にしてからもとの設定に戻します。
◎ポートセキュリティー設定を変更します。
◎本製品を再起動します。

Violation Limit ……

[Violation Mode]欄で「Restrict」を選択したとき、違反MACアドレスの最大数を指定します。
設定できる範囲は、「1～1023」です。

State……

現在のポートセキュリティーの状態が表示されます。

Disabled：
ポートセキュリティーが無効です。

Ready：
ポートセキュリティーが有効で、[Limit]欄で設定した上限に達していないときに表示されます。

Limit Reached：
ポートセキュリティーが有効で、[Limit]欄で設定した上限に達したときに表示されます。

Shutdown：
[Violation Mode]欄で「Shutdown」を選択した場合に、ポートセキュリティーによってポートをシャットダウンしたときに表示されます。

〈Save〉 ……

設定した内容を保存するボタンです。

〈Reset〉 ……

設定内容を変更したとき、変更前の状態に戻すボタンです。

「NAS」画面

Configuration > Security > Network > NAS

システム全体、またはポートごとの認証システム(IEEE 802.1X認証、MACベース認証)について設定します。

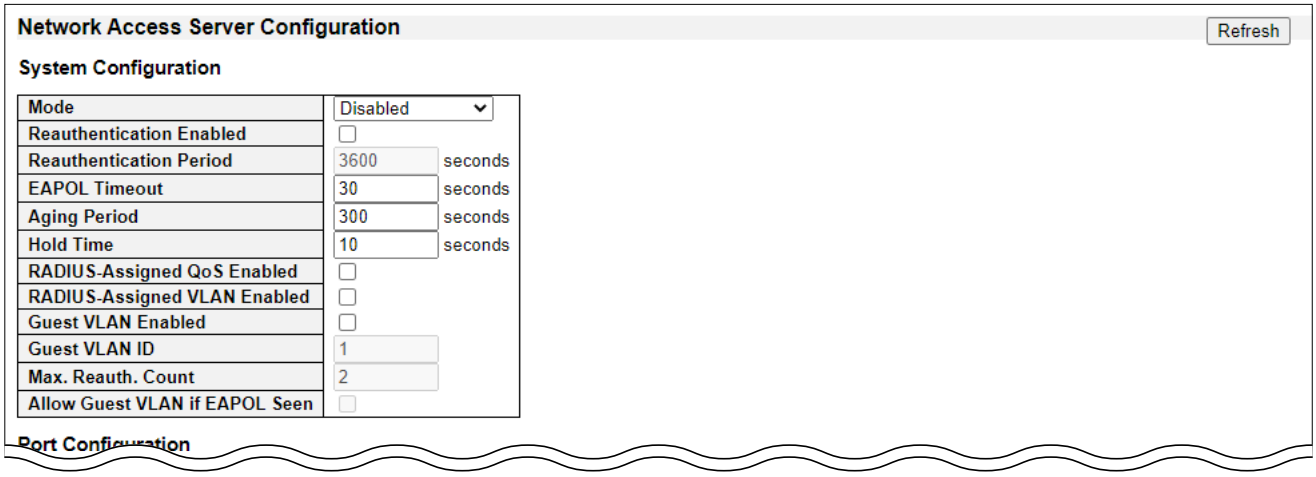
IEEE 802.1X認証では、資格情報を最初に送信するようユーザーに要求し、ネットワークへの不正アクセスを防止するポートベースのアクセス制御手順が定義されています。
1つ以上のセントラルサーバーかバックエンドサーバーが、ユーザーのネットワークへのアクセスを許可、または拒否します。
認証に使用するバックエンドサーバー(RADIUSサーバー)は、「Configuration」→「Security」→「AAA」メニューで設定できます。
IEEE802.1X規格ではポートベースの動作が定義されています。
IEEE標準規格ではないモードを使用するとセキュリティーの問題を解決できます。

MACベース認証では、同じポートで複数のユーザーを認証できるため、IEEE 802.1Xサプリカントソフトウェアをシステムにインストールする必要はありません。
本製品が、ユーザーMACアドレスを使用してバックエンドサーバーに対して認証を要求します。
侵入者は偽のMACアドレスを作成する可能性があるため、MACベース認証はIEEE 802.1X認証よりも安全性が低くなります。

「NAS」画面

Configuration > Security > Network > NAS

Network Access Server Configuration



〈Refresh〉 …… 最新の状態に更新するボタンです。
※設定内容を変更したときは、変更前の状態に戻ります。

System Configuration

Mode …… NAS(ネットワークアクセスサーバー)が有効か無効かを設定します。
無効に設定すると、すべてのポートでフレームの転送が許可されます。

Reauthentication Enabled …… 認証されたサプリカント/クライアントの定期的な再認証を有効にするとき、ボックスにチェックマークを入れます。
有効にすると、[Reauthentication Period]欄で設定した時間が経過後、再認証されます。
IEEE 802.1X認証のポートで再認証を使用して、新しいデバイスがポートに接続されているかどうか、またはサプリカントが接続されなくなったかどうかを検出できます。
MACベース認証のポートの場合、再認証はRADIUSサーバー設定が変更されたときに役立ちます。
本製品とクライアント間の通信は関係しないため、クライアントがポート上に存在するかは確認できません。
※詳細は、[Aging Period]の説明を参照してください。

Reauthentication Period …… [Reauthentication Enabled]欄にチェックマークが入っているとき、接続されたクライアントを再認証するまでの期間を指定します。
設定できる範囲は、「1～3600」(秒)です。

EAPOL Timeout …… EAP-Request/Identityフレームの再送時間を指定します。
設定できる範囲は、「1～65535」(秒)です。
※MACベース認証のポートには影響しません。

「NAS」画面

Configuration > Security > Network > NAS

Network Access Server Configuration

Aging Period ……

ポートのセキュリティー機能が「Single 802.1X」、「Multi 802.1X」、または「MAC-Based Auth.」の場合のエージング期間を指定します。
設定できる範囲は、「10～1000000」(秒)です。

NASがポートセキュリティー機能を使用してセキュアMACアドレスを設定する場合、MACアドレスのアクティビティを定期的にチェックし、一定期間内にアクティビティが検出されない場合はリソースを解放する必要があります。

[Reauthentication Enabled]欄が有効で、「Port-based 802.1X」を使用しているポートの場合、ポートに接続されなくなったサプリカントは次回の再認証時に削除されるため、エージングは必要ありません。
ただし、[Reauthentication Enabled]欄が無効の場合、エントリをエージングしないとリソースが解放されません。
「MAC-Based Auth.」を使用しているポートの場合、[Reauthentication Enabled]欄が有効でも本製品とクライアントは直接通信しません。
そのため、クライアントがまだ接続されているかどうかは検出されず、エントリをエージングしないとリソースが解放されません。

Hold Time ……

ポートのセキュリティー機能が「Single 802.1X」、「Multi 802.1X」、または「MAC-Based Auth.」の場合の待機時間を設定します。
RADIUSサーバーがクライアントのアクセスを拒否したか、RADIUSサーバー要求がタイムアウトしたためにクライアントがアクセスを拒否された場合、設定した期間クライアントは認証されていない状態のままになります。
MACベース認証では、待機時間中にクライアントが送信した新しいフレームは無視されます。
設定できる範囲は、「10～1000000」(秒)です。
※タイマーは、認証中はカウントされません。
※RADIUSサーバー要求のタイムアウト時間は、「Configuration」→「Security」→「AAA」メニューで設定できます。

RADIUS-Assigned QoS Enabled…

システム全体のRADIOUS QoS割り当てについて設定します。
RADIUS QoS割り当てを使用すると、認証されたサプリカントからのトラフィックに割り当てられるトラフィッククラスを一元管理できます。
この機能を利用するには、RADIUSサーバーが特定のRADIUS属性を送信するように設定してください。
※詳細は、「QoSクラスの識別に使用されるRADIUS属性値について」(P.2-74)を参照してください。

有効にすると、各ポートの[RADIUS-Assigned QoS Enabled]欄の設定によって、RADIUSサーバーから通知されたQoSクラスを使用するかが決まります。
無効にすると、RADIUSサーバーからのQoSクラス通知はすべてのポートで無効になります。

「NAS」画面

Configuration > Security > Network > NAS

Network Access Server Configuration

RADIUS-Assigned VLAN Enabled

システム全体の動的VLAN割り当てについて設定します。
動的VLAN割り当てを使用すると、認証されたサプリカントに割り当てられるVLANを一元管理できます。
ポートは、RADIUSサーバーからの情報に基づいてVLANが割り当てられます。
動的VLAN割り当てを使用するには、RADIUSサーバーが特定のRADIUS属性を送信するように設定してください。
※詳細は、「VLAN IDの識別に使用されるRADIUS属性値について」(P.2-75)を参照してください。

有効にすると、各ポートの[RADIUS-Assigned VLAN Enabled]欄の設定によって、動的VLAN割り当てが有効かどうかが決まります。
無効にすると、動的VLAN割り当てはすべてのポートで無効になります。

Guest VLAN Enabled……

システム全体のゲストVLAN機能について設定します。
ゲストVLANは通常はネットワークアクセスが制限されていて、認証が失敗した場合に802.1X非対応のクライアントへ割り当てられます。
※詳細は、「ゲストVLAN有効時の動作について」(P.2-76)を参照してください。

有効にすると、各ポートの[Guest VLAN Enabled]欄の設定によって、ポートをゲストVLAN に割り当てるかどうかが決まります。
無効にすると、ゲストVLANはすべてのポートで無効になります。

Guest VLAN ID……

[Guest VLAN Enabled]欄を有効にしたとき、ポートのVLANがゲストVLANに変更されるときのポートVLAN IDを指定します。
設定できる範囲は、「1～4095」です。

Max. Reauth. Count ……

[Guest VLAN Enabled]欄を有効にしたとき、ポートをゲストVLANに割り当てるまでに EAP-Request/Identityフレームを送信しつづける回数を指定します。
設定できる範囲は、「1～255」です。

Allow Guest VLAN if EAPOL Seen

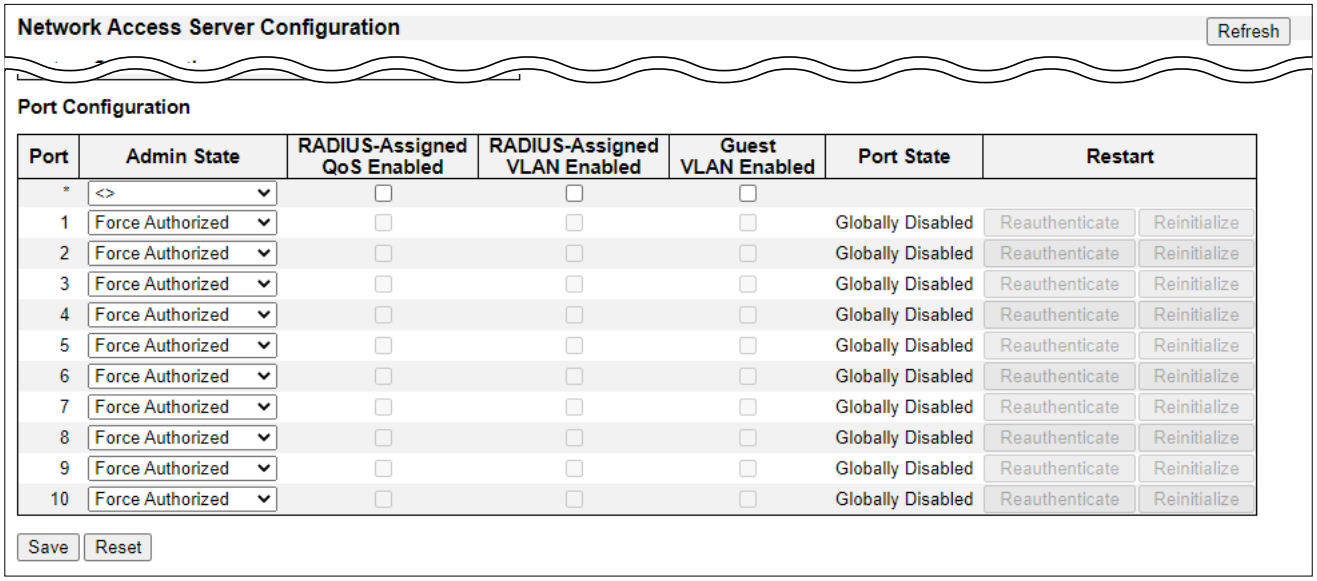
[Guest VLAN Enabled]欄を有効にしたとき、ゲストVLAN割り当て時の動作を設定します。
本製品は、ポートがEAPOLフレームを受信したことがあるかどうかを記録しています。
ポートをゲストVLANに割り当てるかどうかを決めるとき、有効か無効かによってEAPOLフレームの受信履歴を考慮するかどうかが決まります。
無効に設定すると、過去にEAPOLフレームをポートで受信したことがない場合にだけゲストVLANに入ります。
有効に設定すると、過去にEAPOLフレームを受信したことがある場合でも、ゲストVLANに入ります。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「NAS」画面

Configuration > Security > Network > NAS

Network Access Server Configuration



Port Configuration

Port …… 本製品のポート番号が表示されます。

Admin State …… 「System Configuration」の[Mode]欄で「Enabled」を選択したときに、各ポートの認証方法を指定します。

Force Authorized：
ポートがリンクアップしたときにEAP-Successフレームを送信し、認証なしでポート上にいるすべてのクライアントの通信を許可します。

Force Unauthorized：
ポートがリンクアップしたときにEAP-Failureフレームを送信し、ポート上にいるすべてのクライアントの通信を遮断します。

「NAS」画面

Configuration > Security > Network > NAS

Network Access Server Configuration

Admin State（つづき）……

Port-based 802.1X：
802.1X認証は、サプリカント（ユーザー）、オーセンティケーター（スイッチ）、認証サーバー（RADIUSサーバー）で構成されます。
オーセンティケーターは仲介装置として動作し、サプリカントと認証サーバーとのあいだで要求と応答を転送します。
サプリカントとスイッチとのあいだで送信されるフレームはEAPOL（EAP Over LANs）フレームと呼ばれる特殊な802.1Xフレームで、EAPパケットをカプセル化します。（RFC3748）
スイッチとRADIUSサーバーとのあいだで送信されるフレームはRADIUSパケットと呼ばれ、スイッチのIPアドレス、名前、サプリカントのポート番号などの属性とともに、EAPパケットをカプセル化します。
EAPは、MD5チャレンジ認証、PEAP、TLS などのさまざまな認証方法をサポートしています。
オーセンティケーター（スイッチ）は、サプリカントと認証サーバーが使用している認証方法や、特定の方法に必要な情報交換フレームの数を知る必要がなく、受信したフレームのEAPパケット部分をカプセル化し、転送するだけです。
認証が完了すると、RADIUSサーバーは認証結果（成功、または失敗）を含むパケットを送信します。
スイッチは認証結果をサプリカントに転送するだけでなく、認証結果を含むパケットを使用して、サプリカントに接続されているポートの通信を許可、または遮断します。

ご注意
2つのバックエンドサーバーが有効で、タイムアウト時間がX秒に設定され、リストの最初のサーバーがダウンしているがデッド状態とは判断されていないとします。
サプリカントがX秒よりも短い間隔でEAPOL-Startフレームを再送信すると、スイッチはサプリカントから新しいEAPOL-Startフレームを受信するたびに進行中のバックエンド認証サーバー要求を中断するため、認証されることはありません。
また、サーバーはデッド状態と判断されていないため（X秒が経過していないため）、スイッチは同じサーバーにバックエンド認証サーバー要求を送りつづけます。
このループを回避するために、サーバーのタイムアウトは、サプリカントのEAPOL-Startフレーム再送信レートよりも小さい値に設定してください。
※タイムアウト時間は、「Configuration」→「Security」→「AAA」メニューで設定します。

「NAS」画面

Configuration > Security > Network > NAS

Network Access Server Configuration

Admin State（つづき）……

Single 802.1X：
「Port-based 802.1X」では、サプリカントが認証されると、ポート全体でネットワークアクセスが許可されます。
そのため、ポートに接続されている他のクライアント（HUBなど）は、認証されたクライアントにピギーバックし、実際に認証されていなくてもネットワークにアクセスできるようになります。
このセキュリティー違反を防ぐために、「Single 802.1X」を使用します。
「Single 802.1X」はIEEE標準規格ではありませんが、「Port-based 802.1X」と同じ特性を多く備えています。
「Single 802.1X」では、1つのポートで同時に2つ以上のサプリカントが認証を受られません。
通常のEAPOLフレームは、サプリカントとスイッチ間の通信に使用されます。
1つのポートに複数のサプリカントが接続されている場合、ポートがリンクアップしたときに最初に接続されたサプリカントが認証を試行します。
最初のサプリカントが一定時間内に認証されなかった場合、別のサプリカントが認証を試行します。
サプリカントが正常に認証されると、認証されたサプリカントだけがアクセスを許可されます。
※サポートされているすべてのモードの中で最も安全な認証方式です。
※正常に認証されると、ポートセキュリティー機能は、サプリカントのMACアドレスを保護するために使用されます。

Multi 802.1X：
「Multi 802.1X」は、「Single 802.1X」と同様に IEEE標準規格ではありませんが、同じ特性を多く備えています。
「Multi 802.1X」では、複数のサプリカントが同じポートで同時に認証を受けられます。
各サプリカントは個別に認証され、ポートセキュリティー機能を使用してMACテーブルで保護されます。
「Multi 802.1X」では、スイッチがサプリカントへ送信するEAPOLフレームの宛先MACアドレスとして、BPDUに含まれるMACアドレスを使用できません。
これは、ポートに接続されているすべてのサプリカントがスイッチから送信された要求に応答するためです。
代わりにスイッチは、サプリカントから送信された最初のEAPOL-Start、またはEAP-Response/Identityフレームに含まれるサプリカントのMACアドレスを使用します。
サプリカントが接続されていない場合だけ、スイッチはBPDUに含まれるMACアドレスを宛先としてEAP-Request/Identityフレームを送信し、ポート上に存在する可能性のあるサプリカントを起動します。
※ポートに接続できるサプリカントの最大数は、「Configuration」→「Security」→「Network」メニューの「Port Security」画面で設定できます。

「NAS」画面

Configuration > Security > Network > NAS

Network Access Server Configuration

Admin State（つづき）……

MAC-based Auth.：
「Port-based 802.1X」とは異なり、MACベース認証は標準規格ではありません。
MACベース認証では、ユーザーはクライアントと呼ばれ、スイッチはクライアントに代わってサプリカントとして動作します。
クライアントから送信された最初のフレームはスイッチにスヌープされ、スイッチはRADIUSサーバーへの認証要求でクライアントのMACアドレスをユーザー名とパスワードの両方として使用します。
6バイトのMACアドレスは、「xx-xx-xx-xx-xx-xx」形式（xは小文字、16進数）に変換されます。

認証が完了すると、RADIUSサーバーは認証結果（成功/失敗）を送信し、スイッチはポートセキュリティー機能を使用して、クライアントの通信を許可、または拒否します。
通信が許可されてはじめて、クライアントからのフレームがスイッチで転送されます。
MACベース認証はIEEE 802.1X規格に準拠しておらず、EAPOLフレームを使用しません。
IEEE 802.1X認証に対して、MACベース認証ではクライアントは認証に特別なサプリカントソフトウェアを必要としませんが、MACアドレスが悪意のあるユーザーによってスプーフィングされると、どんなユーザーでもアクセスできるようになります。
※スイッチはMD5チャレンジ認証方式だけに対応しているので、RADIUSサーバーはそれに応じて設定する必要があります。
※ポートに接続できるクライアントの最大数は、「Configuration」→「Security」→「Network」メニューの「Port Security」画面で設定できます。

「NAS」画面

Configuration > Security > Network > NAS

Network Access Server Configuration

RADIUS-Assigned QoS Enabled …

「System Configuration」の[RADIUS-Assigned QoS Enabled]欄が「Enabled」に設定されている場合、ポートごとにQoSクラス割り当てを使用するかどうか設定します。
サプリカントが認証されると、RADIUSサーバーから送信されるAccess-Acceptパケットに含まれるQoSクラス情報に基づいてトラフィックが分類されます。
以下の場合、ポートのQoSクラスは本製品に設定されたQoSクラスになります。
◎認証/再認証が失敗した場合
◎Access-AcceptパケットがQoSクラスを伝送しなくなった場合
◎無効なパケット
◎サプリカントがポートに存在しなくなった場合

※この機能は、シングルサプリカントモード(Port-based 802.1X、Single 802.1X)のときに使用できます。

QoSクラスの識別に使用されるRADIUS属性値について
RFC4675では、Access-Acceptパケット内のQoSクラスを識別するため属性値(User-Priority-Table)について定義されています。
パケット内の最初の値が使用され、有効にするには次の基準にしたがいます。
◎属性値の8つのオクテットはすべて同一で、使用できる文字は「0～7」(ASCII文字)です。

「NAS」画面

Configuration > Security > Network > NAS

Network Access Server Configuration

RADIUS-Assigned VLAN Enabled

「System Configuration」の[RADIUS-Assigned VLAN Enabled]欄が「Enabled」に設定されている場合、ポートごとに動的VLAN割り当てを使用するかどうか設定します。
動的VLAN割り当てを使用すると、サプリカントが認証されたときにRADIUSサーバーから送信されるRADIUS Access-Acceptパケットに含まれるVLAN ID情報に基づいて、ポートのVLAN IDを設定します。
RADIUSサーバーから有効なVLAN ID情報を受信すると、ポートのVLAN IDはRADIUSサーバーから通知されたVLAN IDに変更されます。
一度VLAN IDが割り当てられると、ポートへのすべてのトラフィックは、RADIUSサーバーが割り当てたVLAN IDで分類、およびスイッチングされます。
以下の場合、ポートのVLAN IDは本製品に設定されたVLAN IDになります。
◎認証/再認証に失敗した場合
◎RADIUS Access-AcceptパケットがVLAN IDを含まなくなった場合
◎サプリカントがポート上に存在しなくなった場合

※この機能は、シングルサプリカントモード(Port-based 802.1X、Single 802.1X)のときに使用できます。
※割り当てられたVLANは、「Monitor」→「VLANs」メニュー「Membership」画面で確認できます。

VLAN IDの識別に使用されるRADIUS属性値について
RFC2868とRFC3580では、Access-Acceptパケット内の VLAN IDの識別に使用される属性値について定義されています。
有効にするには次の基準にしたがいます。
◎Tunnel-Medium-Type、Tunnel-Type、Tunnel-Private-Group-ID属性値が、Access-Acceptパケットに1つ以上含まれている。
◎スイッチは、Tagの値が同じで、次の条件を満たす最初のアトリビュートの組み合わせを探します。
(Tag==0を使用する場合、Tunnel-Private-Group-IDにTagを含める必要はありません。)
・Tunnel-Medium-Typeの値が「6」(IEEE-802)。
・Tunnel-Typeの値が「13」(VLAN)。
・Tunnel-Private-Group-IDの値が、VLAN ID。
※VLAN IDは「1～4095」(10進数、ASCII文字)で、先頭の「0」は削除されます。

「NAS」画面

Configuration > Security > Network > NAS

Network Access Server Configuration

Guest VLAN Enabled……

「System Configuration」の[Guest VLAN Enabled]欄で「Enabled」を選択したときに、ポートごとにゲストVLANを使用するかを設定します。
ゲストVLANを使用すると、設定に応じてポートをゲストVLANに割り当てます。
※EAPOLベースの認証(Port-based 802.1X、Single 802.1X、Multi 802.1X)で使用できます。
※割り当てられたVLANは、「Monitor」→「VLANs」メニューの「Membership」画面で確認できます

ゲストVLAN有効時の動作について
ゲストVLAN対応ポートがリンクアップすると、EAP-Request/Identityフレームの送信を開始します。
EAP-Request/Identityフレームの送信回数が[Max. Reauth. Count]欄の値を超えてもEAPOLフレームを受信してない場合、[Allow Guest VLAN if EAPOL Seen]欄が有効のときは、ポートをゲストVLANに割り当てます。
[Allow Guest VLAN if EAPOL Seen]欄が無効のときは、EAPOLフレームをポートで受信したことがあるかどうかを履歴で確認し、EAPOLフレームを受信したことがなければ、ポートをゲストVLANに割り当てます。
※EAP-Request/Identityフレームの送信間隔は、[EAPOL Timeout]欄で設定します。
※ポートがリンクダウンするか、ポートの[Admin State]欄を変更すると、履歴はクリアされます。
それ以外の場合、ゲストVLANには移動しませんが、[EAPOL Timeout]欄で設定した送信間隔でEAP-Request/Identityフレームを送信しつづけます。
ゲストVLANに割り当てられたポートは認証済みと判断され、ポートに接続されているすべてのクライアントはこのVLAN上でアクセスを許可されます。
スイッチはゲストVLANを割り当てるとき、EAPOL-Successフレームを送信しません。
ゲストVLANに割り当てられている間、スイッチはリンクのEAPOLフレームを監視し、EAPOLフレームを受信すると、すぐにゲストVLANからポートを取り出し、ポートの設定にしたがってサプリカントの認証を開始します。
EAPOLフレームを受信した場合、[Allow Guest VLAN if EAPOL Seen]欄が無効になっているポートは、ゲストVLANに戻ることができません。

「NAS」画面

Configuration > Security > Network > NAS

Network Access Server Configuration

Port State …… ポートの状態が表示されます。

Globally Disabled：
システム全体でNASが無効(「System Configuration」の[Mode]欄が「Disabled」)になっているときに表示されます。

Link Down：
システム全体でNASが有効ですが、ポートがリンクダウンしているときに表示されます。

Authorized：
ポートが「Force Authorized」、またはシングルサプリカントモードで、サプリカントが承認されているときに表示されます。

Unauthorized：
ポートが「Force Unauthorized」、またはシングルサプリカントモードで、サプリカントがRADIUSサーバーに承認されていないときに表示されます。

X Auth/Y Unauth：
ポートはマルチサプリカントモードで、許可されているクライアント(X)と許可されていないクライアント(Y)が表示されます。

Restart…… 「System Configuration」の[Mode]欄が「Enabled」で、[Admin State]欄がEAPOLベース、またはMACベースの認証のときに使用できます。
※ボタンをクリックしても、設定した内容は保存されません。

〈Reauthenticate〉
EAPOLベースの認証の場合、ポートのクワイエット期間が終了するたびに再認証をスケジュールするボタンです。
MACベース認証の場合、すぐに再認証するボタンです。
※ポート上の認証されたクライアントに対してだけ有効で、クライアントが一時的に承認されていない状態にはなりません。

〈Reinitialize〉
ポート上のクライアントを初期化し、すぐに再認証するボタンです。
再認証の進行中、クライアントは承認されていない状態になります。

〈Save〉 …… 設定した内容を保存するボタンです。

〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

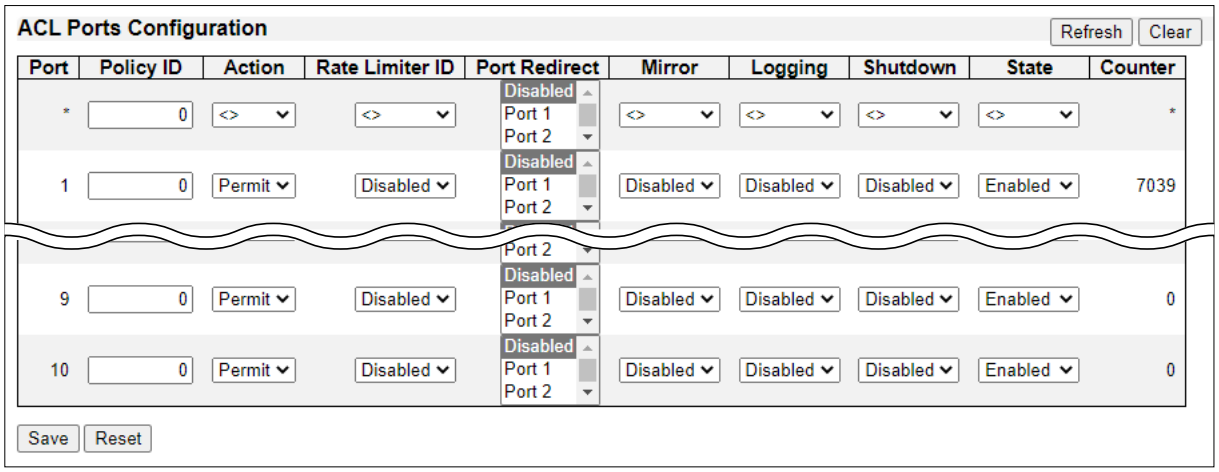
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Ports」画面

Configuration > Security > Network > ACL > Ports

アクセスコントロールリスト(ACL)のパラメーター(ACE)を設定します。
ポートで受信したフレームと一致するACEが見つかるまで、ACEを順番に確認します。

ACL Ports Configuration



〈Refresh〉 …… 最新の状態に更新するボタンです。
※設定内容を変更したときは、変更前の状態に戻ります。

〈Clear〉 …… すべてのポートのカウンター値を0にするボタンです。

Port …… 本製品のポート番号が表示されます。

Policy ID …… ポートに適用するポリシーを選択します。
設定できる範囲は、「0～255」です。

Action …… 転送を許可する(Permit)か拒否する(Deny)かを選択します。

Rate Limiter ID …… ポートに適用するレートリミッターのIDを選択します。
設定できる範囲は、「1～16」、または「Disabled」(無効)です。

Port Redirect …… フレームの転送先ポートを選択します。
設定できる範囲は、「Port1」～「Port10」、または「Disabled」(無効)です。
※[Action]欄で「Permit」を選択したときは、設定できません。

Mirror …… ポートで受信したフレームをミラーリングするかどうか選択します。

Enabled：
ポートで受信したフレームをミラーリングします。

Disabled：
ポートで受信したフレームをミラーリングしません。

「Ports」画面

Configuration > Security > Network > ACL > Ports

ACL Ports Configuration

Logging ……

ポートで受信したフレームをシステムログに記録するかどうか選択します。
※ログメッセージには、4バイトのCRCは含まれません。
※パケット長がシステムログメモリーサイズや1518より短く(VLANタグを含まない)、ロギングレートが制限されているときだけ動作します。

Enabled：
ポートで受信したフレームを、システムログに記録します。

Disabled：
ポートで受信したフレームを、システムログに記録しません。

Shutdown ……

フレームを受信したとき、ポートをシャットダウンするかどうかを選択します。
※パケット長が1518より短い(VLANタグを含まない)ときだけ動作します。

Enabled：
フレームを受信したポートをシャットダウンします。

Disabled：
フレームを受信しても、シャットダウンしません。

State……

ポート状態を選択します。

Enabled：
ポートを起動します。
設定を変更することで、シャットダウンしたポートを再起動できます。

Disabled：
ポートをシャットダウンします。

Counter ……

フレームがACEに一致した回数が表示されます。

〈Save〉 ……

設定した内容を保存するボタンです。

〈Reset〉 ……

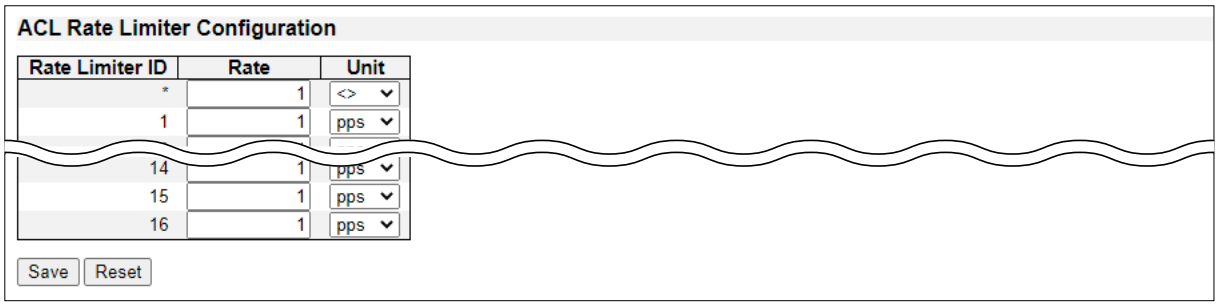
設定内容を変更したとき、変更前の状態に戻すボタンです。

「Rate Limiters」画面

Configuration > Security > Network > ACL > Rate Limiters

ACLレート制限について設定します。

ACL Rate Limiter Configuration



Rate Limiter ID…… レートリミッターIDが表示されます。

Rate …… レートの上限を設定します。
設定できる範囲は、「0～3276700」(pps)、または「0～1000000」(kbps)(100kbps刻み)です。

Unit …… レートの単位を「pps」(packets per second)、または「kbps」(kbits per second)から選択します。

〈Save〉 …… 設定した内容を保存するボタンです。

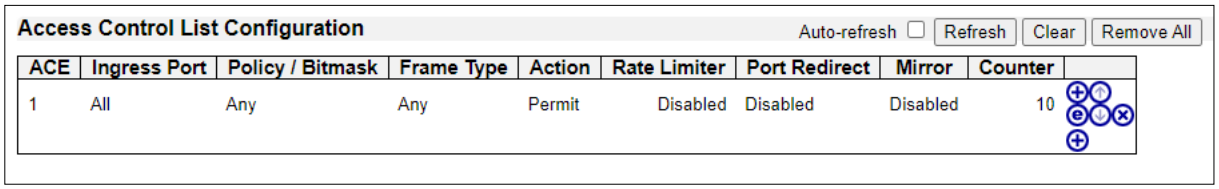
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Access Control List」画面

Configuration > Security > Network > ACL > Access Control List

アクセスコントロールリスト(ACL)を構成するアクセスコントロールエントリ(ACE)が表示されます。
ACEは最大256件まで登録できます。
内部プロトコルに使用される予約済みACEは編集や削除、優先順序の変更ができず、優先順位は最も高くなります。

Access Control List Configuration



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈Clear〉 ……　すべてのACEのカウンター値を0にするボタンです。

〈Remove All〉 ……　すべてのACEを削除するボタンです。

ACE ……　ACE IDが表示されます。

Ingress Port ……　ACEを適用するポートが表示されます。

All　：すべてのポートに適用されます。

1～10：表示されているポートに適用されます。

Policy / Bitmask ……　条件となるポリシー番号とビットマスクが表示されます。

Frame Type ……　条件となるフレームタイプが表示されます。

Any　：フレームタイプでフィルタリングしません。

EType　：イーサネットタイプのフレームをフィルタリングします。
※ARP、IPv4、IPv6フレームは、ACEに一致しないと判断されます。

ARP　：ARPフレームをフィルタリングします。

IPv4　：すべてのIPv4フレームをフィルタリングします。

IPv4/ICMP　：ICMPプロトコルのIPv4フレームをフィルタリングします。

IPv4/UDP　：UDPプロトコルのIPv4フレームをフィルタリングします。

IPv4/TCP　：TCPプロトコルのIPv4 フレームをフィルタリングします。

IPv4/Other　：ICMP/UDP/TCPプロトコル以外のIPv4フレームをフィルタリングします。

IPv6　：IPv6フレームをフィルタリングします。

「Access Control List」画面

Configuration > Security > Network > ACL > Access Control List

Access Control List Configuration

Action ……
ACEに一致するフレームを受信したときの動作が表示されます。

Permit：
ACEに一致するフレームを転送、学習します。

Deny：
ACEに一致するフレームを破棄します。

Filter：
ACEに一致するフレームをフィルタリングします。

Rate Limiter ……
使用するレートリミッターIDが表示されます。
「Disabled」と表示されているときは、無効になります。

Port Redirect ……
ACEに一致するフレームの転送先ポートが表示されます。
「Disabled」が表示されているときは、フレームは転送されません。

Mirror ……
ACEに一致するフレームを受信したとき、ミラーポートにミラーリングするかが表示されます。

Enabled：
ポートで受信したフレームをミラーリングします。

Disabled：
ポートで受信したフレームをミラーリングしません。

Counter ……
フレームがACEに一致した回数が表示されます。

 ……
1つ前にACEを追加するボタンです。
一番下に表示されているボタンをクリックすると、リストの最後にACEが追加されます。

 ……
ACEを編集するボタンです。
「ACE Configuration」画面に移動します。

 ……
1つ上に移動するボタンです。

 ……
1つ下に移動するボタンです。

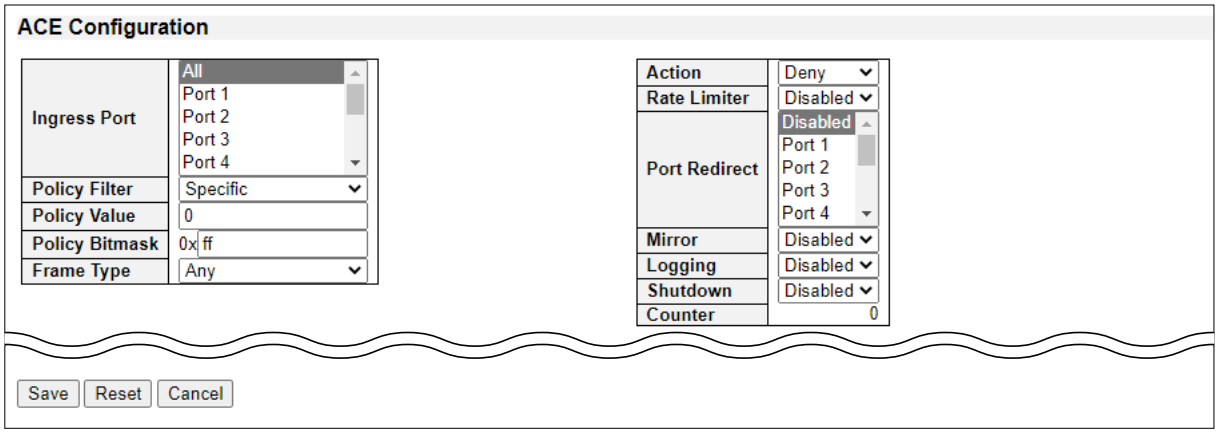
 ……
ACEを削除するボタンです。

「ACE Configuration」画面

Configuration > Security > Network > ACL > Access Control List

アクセスコントロールエントリ(ACE)を設定します。
設定できる項目は、[Frame Type]欄の設定によって異なります。
最初にACEの入力ポートを選択し、次にフレームタイプを選択すると、選択したフレームタイプに応じた設定項目が表示されます。
設定した条件を満たすフレームがACEに一致したと判断されます。

ACE Configuration



Ingress Port ……

ACEが適用される入力ポートを選択します。

All ：すべてのポートに適用されます。

1～10 ：表示したポートに適用されます。

Policy Filter ……

ポリシー番号でフィルタリングするかを設定します。

Any ：ポリシー番号ではフィルタリングしません。

Specific ：設定したポリシー番号でフィルタリングします。
ポリシー番号を指定するための項目が表示されます。

Policy Value ……

[Policy Filter]欄で「Specific」を選択したときに、ポリシー番号を入力します。
設定できる範囲は、「0～255」です。

Policy Bitmask ……

[Policy Filter]欄で「Specific」を選択したときに、ポリシービットマスクを入力します。
設定できる範囲は、「0x0～0xff」です。
[Policy Bitmask]欄で指定したバイナリービット値が「0」のビットは、フィルタリング条件に含まれません。

「ACE Configuration」画面

Configuration > Security > Network > ACL > Access Control List

ACE Configuration

Frame Type ……

フレームタイプでフィルタリングするかを設定します。
フレームタイプは相互排他です。

Any：
フレームタイプではフィルタリングしません。

Ethernet Type：
イーサネットタイプのフレームをフィルタリングします。
※ARP、IPv4、IPv6フレームは、ACEに一致しないと判断されます。
IEEE 802.3で定義されているLength/Typeフィールドの値は10進数で1536以上(16進数で0600以上)で、0x800(IPv4)、0x806(ARP)、または0x86DD(IPv6)以外のときにフレームがACEに一致したと判断されます。

ARP：
ARPフレームをフィルタリングします。

IPv4：
IPv4フレームをフィルタリングします。

IPv6：
IPv6フレームをフィルタリングします。

Action ……

ACEに一致するフレームを受信したときの動作を指定します。

Permit ：ACEに一致するフレームを許可します。

Deny ：ACEに一致するフレームを破棄します。

Filter ：ACEに一致するフレームをフィルタリングします。

Rate Limiter ……

使用するレートリミッターIDを指定します。
設定できる範囲は、「1」～「16」、または「Disabled」(無効)です。

Port Redirect ……

[Action]欄を「Deny」、または「Filter」に設定したときに、ACEに一致するフレームの転送先ポートを選択します。
レートリミッターはこれらのポートに影響します。
設定できる範囲は、「Port1」～「Port10」、または「Disabled」(無効)です。

Mirror ……

ACEに一致するフレームを受信したとき、ミラーポートにミラーリングするかどうかを選択します。
レートリミッターはミラーポートには影響しません。

Enabled ：ポートで受信したフレームをミラーリングします。

Disabled ：ポートで受信したフレームをミラーリングしません。

Logging ……

ACEに一致するフレームを受信したとき、システムログに記録するかどうかを選択します。
※ログメッセージには、4バイトのCRCは含まれません。
※パケット長がシステムログメモリーサイズや1518より短く(VLANタグを含まない)、ロギングレートが制限されているときだけ動作します。

Enabled ：ACEに一致するフレームをシステムログに記録します。

Disabled ：ACEに一致するフレームをシステムログに記録しません。

「ACE Configuration」画面

Configuration > Security > Network > ACL > Access Control List

ACE Configuration

Shutdown …… ACEに一致するフレームを受信したとき、ポートをシャットダウンするかどうかを選択します。
※パケット長が1518より短い場合(VLANタグを含まない)ときだけ動作します。

Enabled ：ACEに一致するフレームを受信したポートをシャットダウンします。

Disabled ：ACEに一致するフレームを受信しても、ポートをシャットダウンしません。

Counter …… フレームがACEに一致した回数が表示されます。

〈Save〉 …… 設定した内容を保存するボタンです。

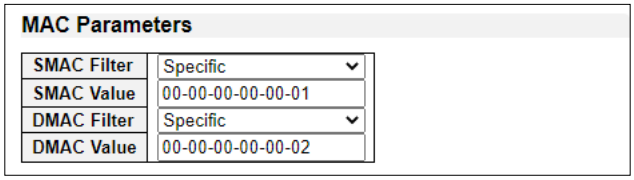
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

〈Cancel〉 …… 設定内容を変更したとき、変更前の状態に戻し、「Access Control List」画面に戻るボタンです。

「ACE Configuration」画面

Configuration > Security > Network > ACL > Access Control List

MAC Parameters



SMAC Filter ……

[Frame Type]欄で「Ethernet Type」、または「ARP」を選択したときに、送信元MACアドレスでフィルタリングするかを選択します。

Any ：送信元MACアドレスではフィルタリングしません。

Specific ：設定した送信元MACアドレスでフィルタリングします。
送信元MACアドレスを指定するための項目が表示されます。

SMAC Value ……

[SMAC Filter]欄で「Specific」を選択したときに、送信元MACアドレスを指定します。
使用できる形式は、「xx-xx-xx-xx-xx-xx」、「xx.xx.xx.xx」、「xxxxxx」(xは16進数)です。
設定した送信元MACアドレスのパケットがACEに一致します。

DMAC Filter ……

宛先MACアドレスでフィルタリングするかを選択します。

Any ：宛先MACアドレスではフィルタリングしません。

MC ：マルチキャストのフレームをフィルタリングします。

BC ：ブロードキャストのフレームをフィルタリングします。

UC ：ユニキャストのフレームをフィルタリングします。

Specific ：設定した宛先MACアドレスでフィルタリングします。
宛先MACアドレスを指定するための項目が表示されます。

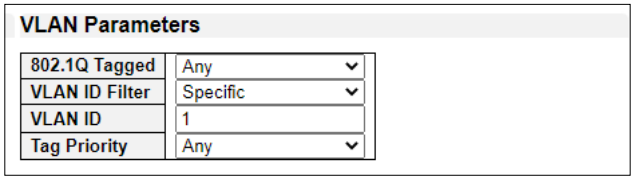
DMAC Value ……

[DMAC Filter]欄で「Specific」を選択したときに、宛先MACアドレスを指定します。
使用できる形式は、「xx-xx-xx-xx-xx-xx」、「xx.xx.xx.xx」、「xxxxxx」(xは16進数)です。
設定した宛先MACアドレスのパケットがACEに一致します。

「ACE Configuration」画面

Configuration > Security > Network > ACL > Access Control List

VLAN Parameters



802.1Q Tagged ……

フレームに802.1Qタグが含まれるかどうかでフィルタリングするかを設定します。

Any ：802.1Qタグではフィルタリングしません。

Enabled ：タグ付きフレームをフィルタリングします。

Disabled ：タグなしフレームをフィルタリングします。

VLAN ID Filter ……

VLAN IDでフィルタリングするかを設定します。

Any ：VLAN IDではフィルタリングしません

Specific ：設定したVLAN IDでフィルタリングします。
VLAN IDを指定するための設定項目が表示されます。

VLAN ID ……

[VLAN ID Filter]欄で「Specified」を選択したときに、VLAN IDを指定します。
設定できる範囲は、「1～4095」です。
設定したVLAN IDのパケットがACEに一致します。

Tag Priority ……

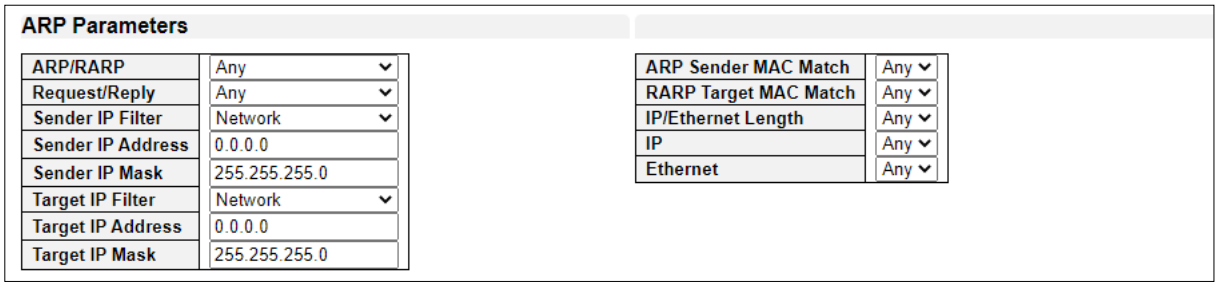
タグに含まれる優先度(PCPフィールド値)を指定します。
設定した優先度のフレームがACEに一致します。
設定できる範囲は、「0」～「7」、または「0-1」、「2-3」、「4-5」、「6-7」、「0-3」、「4-7」、「Any」です。
「Any」に設定したときは、タグの優先度でフィルタリングしません。

「ACE Configuration」画面

Configuration > Security > Network > ACL > Access Control List

ARP Parameters

[Frame Type]欄で「ARP」が選択されているときに設定できます。



ARP/RARP……

オペレーションコードの種類(ARP/RARP)でフィルタリングするかを設定します。

Any ：オペレーションコードの種類(ARP/RARP)ではフィルタリングしません。

ARP ：オペレーションコードがARPのフレームをフィルタリングします。

RARP ：オペレーションコードがRARPのフレームをフィルタリングします。

Other ：不明なオペレーションコードのフレームをフィルタリングします。

Request/Reply……

オペレーションコードの種類(要求/応答)でフィルタリングするかを設定します。

Any ：オペレーションコードの種類(要求/応答)ではフィルタリングしません。

Request ：オペレーションコードがARP要求、またはRARP要求のフレームをフィルタリングします。

Reply ：オペレーションコードがARP応答、またはRARP応答のフレームをフィルタリングします。

Sender IP Filter……

送信元IPアドレスでフィルタリングするかを設定します。

Any ：送信元IPアドレスではフィルタリングしません。

Host ：設定した送信元IPホストアドレスでフィルタリングします。
送信元IPアドレスを指定するための設定項目が表示されます。

Network ：設定した送信元IPネットワークアドレスでフィルタリングします。
送信元IPアドレスを指定するための設定項目が表示されます。

Sender IP Address……

[Sender IP Filter]欄で「Host」、または「Network」を選択したときに、送信元IPアドレスを小数点付き10進表記で指定します。
※「0.0.0.0」など、無効なIPアドレスも設定できます。
通常、無効なIPアドレスを設定した場合は、フレームを破棄するように設定します。

Sender IP Mask……

[Sender IP Filter]欄で「Network」を選択したときに、送信元のサブネットマスクをドット付き10進表記で指定します。

「ACE Configuration」画面

Configuration > Security > Network > ACL > Access Control List

ARP Parameters

Target IP Filter……

宛先IPアドレスでフィルタリングするかを設定します。

Any ：宛先IPアドレスではフィルタリングしません

Host ：設定した宛先IPホストアドレスでフィルタリングします。
宛先IPアドレスを指定するための設定項目が表示されます。

Network ：設定した宛先IPネットワークアドレスでフィルタリングします。
宛先IPアドレスを指定するための設定項目が表示されます。

Target IP Address ……

[Target IP Filter]欄で「Host」、または「Network」を選択したときに、宛先IPアドレスをドット付き10進表記で指定します。
※「0.0.0.0」など、無効なIPアドレスも設定できます。
通常、無効なIPアドレスを設定した場合は、フレームを破棄するように設定します。

Target IP Mask ……

[Target IP Filter]欄で「Network」を選択したときに、宛先のサブネットマスクをドット付き10進表記で指定します。

ARP Sender MAC Match……

SHA(送信元ハードウェアアドレス)フィールドの値でフィルタリングするかを選択します。

Any ：SHAフィールド値ではフィルタリングしません。

0 ：SHAフィールド値がフレームの送信元ハードウェアアドレスと一致しないARPフレームをフィルタリングします。

1 ：SHAフィールド値がフレームの送信元ハードウェアアドレスと一致するARPフレームをフィルタリングします。

RARP Target MAC Match ……

THA(宛先ハードウェアアドレス)フィールドの値でフィルタリングするかを選択します。

Any ：THAフィールド値ではフィルタリングしません。

0 ：THAフィールド値がフレームの宛先ハードウェアアドレスと一致しないRARPフレームをフィルタリングします。

1 ：THAフィールド値がフレームの宛先ハードウェアアドレスと一致するRARPフレームをフィルタリングします。

IP/Ethernet Length ……

HLN(ハードウェアアドレス長)フィールド値とPLN(プロトコルアドレス長)フィールド値でフィルタリングするかを設定します。

Any ：HLNフィールド値とPLNフィールド値ではフィルタリングしません。

0 ：HLNフィールド値が0x06(イーサネット)以外、またはPLNフィールド値が0x04(IPv4)以外のARP/RARPフレームをフィルタリングします。

1 ：HLNフィールド値が0x06(イーサネット)で、PLNフィールド値が0x06(IPv4)のARP/RARPフレームをフィルタリングします。

「ACE Configuration」画面

Configuration > Security > Network > ACL > Access Control List

ARP Parameters

IP …… HRD(ハードウェアアドレス空間)フィールド値でフィルタリングするかを設定します。

- **Any** ：HRDフィールド値ではフィルタリングしません。
- **0** ：HRDフィールド値が1(イーサネット)以外のARP/RARPフレームをフィルタリングします。
- **1** ：HRDフィールド値が1(イーサネット)のARP/RARPフレームをフィルタリングします。

Ethernet …… PRO(プロトコルアドレス空間)フィールド値でフィルタリングするかを設定します。

- **Any** ：PROフィールド値ではフィルタリングしません。
- **0** ：PROフィールド値が0x800(IP)以外のARP/RARPフレームをフィルタリングします。
- **1** ：PROフィールド値が0x800(IP)のARP/RARPフレームをフィルタリングします。

「ACE Configuration」画面

Configuration > Security > Network > ACL > Access Control List

IP Parameters

[Frame Type]欄で「IPv4」が選択されているときに設定できます。

IP Protocol Filter ……

IPプロトコルでフィルタリングするかを選択します。

Any ：IPプロトコルではフィルタリングしません。

ICMP ：ICMPプロトコルのIPv4フレームをフィルタリングします。
ICMPパラメーターを設定するための設定項目が表示されます。
(P.2-95)

UDP ：UDPプロトコルのIPv4フレームをフィルタリングします。
UDPパラメーターを設定するための設定項目が表示されます。
(P.2-96)

TCP ：TCPプロトコルのIPv4フレームをフィルタリングします。
TCPパラメーターを設定するための設定項目が表示されます。
(P.2-96)

Other ：指定したIPプロトコルでフィルタリングします。
IPプロトコルを設定するための設定項目が表示されます。

IP Protocol Value ……

[IP Protocol Filter]欄で「Other」を選択したときに、フィルタリング対象のIPプロトコルの値を指定します。
設定できる範囲は、「0～255」です。
設定したIPプロトコルのフレームがACEに一致します。

IP TTL ……

TTL(Time to Live)フィールド値でフィルタリングするかを設定します。

Any ：TTLフィールド値ではフィルタリングしません。

Non-zero ：TTLフィールド値が0より大きいIPv4フレームをフィルタリングします。

Zero ：TTLフィールド値が0のIPv4フレームをフィルタリングします。

IP Fragment ……

IPv4フレームのMF(More Fragment)ビットとFRAG OFFSET(フラグメントオフセット)フィールドの値でフィルタリングするかを設定します。

Any ：MFビットとFRAG OFFSETフィールドの値ではフィルタリングしません。

Yes ：MFビットが1、またはFRAG OFFSETフィールド値が0より大きいIPv4フレームをフィルタリングします。

No ：MFビットが0かつFRAG OFFSETフィールド値が0のIPv4 フレームをフィルタリングします。

「ACE Configuration」画面

Configuration > Security > Network > ACL > Access Control List

IP Parameters

IP Option ……

オプションフィールドの値でフィルタリングするかを設定します。

Any ：オプションフィールド値ではフィルタリングしません。

Yes ：オプションフィールドが設定されているIPv4フレームをフィルタリングします。

No ：オプションフィールドが設定されていないIPv4フレームをフィルタリングします。

SIP Filter ……

送信元IPアドレスでフィルタリングするかを設定します。

Any ：送信元IPアドレスではフィルタリングしません。

Host ：設定した送信元IPホストアドレスでフィルタリングします。
送信元IPアドレスを指定するための設定項目が表示されます。

Network ：設定した送信元IPネットワークアドレスでフィルタリングします。
送信元IPアドレスを指定するための設定項目が表示されます。

SIP Address ……

[SIP Filter]欄で「Host」、または「Network」を選択したときに、送信元IPアドレスを小数点付き10進表記で指定します。
※「0.0.0.0」など、無効なIPアドレスも設定できます。
通常、無効なIPアドレスを設定した場合は、フレームを破棄するように設定します。

SIP Mask……

[SIP Filter]欄で「Network」を選択したときに、送信元のサブネットマスクをドット付き10進表記で指定します。

DIP Filter……

宛先IPアドレスでフィルタリングするかを設定します。

Any ：宛先IPアドレスでフィルタリングしません。

Host ：設定した宛先IPホストアドレスでフィルタリングします。
宛先IPアドレスを指定するための設定項目が表示されます。

Network ：設定した宛先IPネットワークアドレスでフィルタリングします。
宛先IPアドレスを指定するための設定項目が表示されます。

DIP Address ……

[DIP Filter]欄で「Host」、または「Network」を選択したときに、宛先IPアドレスを小数点付き10進表記で指定します。
※「0.0.0.0」など、無効なIPアドレスも設定できます。
通常、無効なIPアドレスを設定した場合は、フレームを破棄するように設定します。

DIP Mask ……

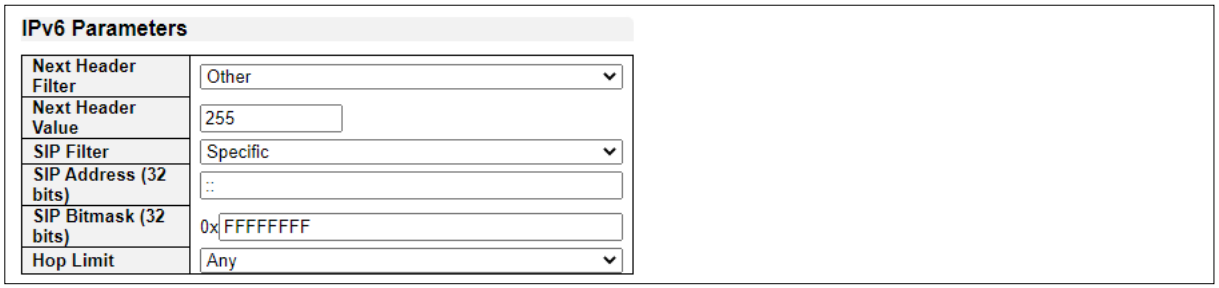
[DIP Filter]欄で「Network」を選択したときに、宛先のサブネットマスクをドット付き10進表記で指定します。

「ACE Configuration」画面

Configuration > Security > Network > ACL > Access Control List

IPv6 Parameters

[Frame Type]欄で「IPv6」が選択されているときに設定できます。



Next Header Filter ……

IPv6フレームのNext Headerフィールドの値でフィルタリングするかを設定します。

Any ：Next Headerフィールドの値ではフィルタリングしません。

ICMP ：ICMPプロトコルのIPv6フレームをフィルタリングします。
ICMPパラメーターを設定するための設定項目が表示されます。
(P.2-95)

UDP ：UDPプロトコルのIPv6フレームをフィルタリングします。
UDPパラメーターを設定するための設定項目が表示されます。
(P.2-96)

TCP ：TCPプロトコルのIPv6フレームをフィルタリングします。
TCPパラメーターを設定するための設定項目が表示されます。
(P.2-96)

Other ：設定したNext Headerフィールド値でフィルタリングします。
Next Headerフィールド値を指定するための設定項目が表示されます。

Next Header Value ……

[Next Header Filter]欄で「Other」を選択したときに、Next Headerフィールド値を指定します。
設定できる範囲は、「0～255」です。
設定したNext Headerフィールドを含むフレームがACEに一致します。

「ACE Configuration」画面

Configuration > Security > Network > ACL > Access Control List

IPv6 Parameters

SIP Filter……

送信元IPv6アドレスでフィルタリングするかを設定します。

Any ：送信元IPv6アドレスではフィルタリングしません。

Specific ：送信元IPv6アドレスでフィルタリングします。
送信元IPv6アドレスを指定するための設定項目が表示されます。

SIP Address (32 bits) ……

[SIP Filter]欄で「Specific」を選択したときに、送信元IPv6アドレスの下位32ビットを指定します。

SIP Bitmask (32 bits) ……

[SIP Filter]欄で「Specific」を選択したときに、送信元IPv6アドレスのマスクを指定します。
設定できる範囲は、「0x00000000～0xFFFFFFFF」です。
[SIP BitMask]欄で指定したバイナリービット値が「0」のビットは、フィルタリング条件には含まれません。
たとえば、[SIP Address]欄を「2001::3」、[SIP BitMask]欄を「0xFFFFFFFE」に設定した場合、送信元IPv6アドレスが2001::2、または2001::3のフレームをフィルタリングします。

Hop Limit……

IPv6フレームのHop Limitフィールドの値でフィルタリングするかを設定します。

Any ：Hop Limitフィールド値ではフィルタリングしません。

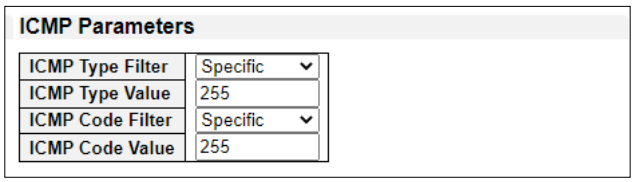
0 ：Hop Limitフィールドが0のIPv6フレームをフィルタリングします。

1 ：Hop Limitフィールドが0より大きいIPv6フレームをフィルタリングします。

「ACE Configuration」画面

Configuration > Security > Network > ACL > Access Control List

ICMP Parameters/ICMPv6 Parameters



ICMP Type Filter …… ICMPフレームのTypeフィールドの値でフィルタリングするかを設定します。

Any ：Typeフィールドの値ではフィルタリングしません。

Specific ：設定したTypeフィールドの値でフィルタリングします。
Typeフィールドの値を指定するための項目が表示されます。

ICMP Type Value…… [ICMP Type Filter]欄で「Specific」を選択したとき、Typeフィールドの値を指定します。
設定できる範囲は、「0～255」です。
設定したTypeフィールドのフレームがACEに一致します。

ICMP Code Filter…… ICMPフレームのCodeフィールドの値でフィルタリングするかを設定します。

Any ：Codeフィールドの値ではフィルタリングしません。

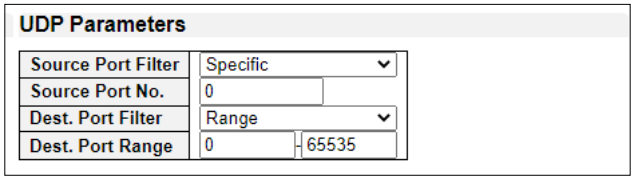
Specific ：設定したCodeフィールドの値でフィルタリングします。
Codeフィールドの値を指定するための項目が表示されます。

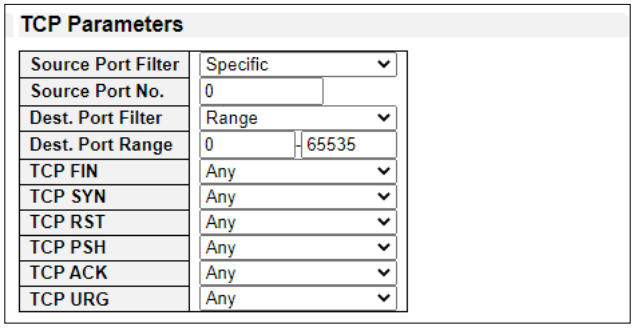
ICMP Code Value …… [ICMP Code Filter]欄で「Specific」を選択したとき、Codeフィールドの値を指定します。
設定できる範囲は、「0～255」です。
設定したCodeフィールドのフレームがACEに一致します。

「ACE Configuration」画面

Configuration > Security > Network > ACL > Access Control List

UDP Parameters/UDPv6 Parameters/TCP Parameters/TCPv6 Parameters





Source Port Filter ……

TCP/UDPフレームの送信元ポート番号フィールドでフィルタリングするかを設定します。

Any ：送信元ポート番号ではフィルタリングしません。

Specific ：設定した送信元ポート番号でフィルタリングします。
送信元ポート番号を指定するための項目が表示されます。

Range ：設定した送信元ポート番号範囲でフィルタリングします。
送信元ポート番号範囲を指定するための項目が表示されます。

Source Port No. ……

[Source Port Filter]欄で「Specific」を選択したときに、送信元ポート番号を指定します。
設定できる範囲、「0～65535」です。
設定した送信元ポート番号のパケットがACEに一致します。

Source Port Range……

[Source Port Filter]欄で「Range」を選択したときに、送信元ポート番号範囲を指定します。
設定できる範囲は、「0～65535」です。
設定した送信元ポート番号内のパケットがACEに一致します。

Dest. Port Filter ……

TCP/UDPフレームの宛先ポート番号フィールドでフィルタリングするかを設定します。

Any ：宛先ポート番号ではフィルタリングしません。

Specific ：設定した宛先ポート番号でフィルタリングします。
宛先ポート番号を指定するための項目が表示されます。

Range ：設定した宛先ポート番号範囲でフィルタリングします。
宛先ポート番号範囲を指定するための項目が表示されます。

Dest. Port No. ……

[Dest. Port Filter]欄で「Specific」を選択したときに、宛先ポート番号を指定します。
設定できる範囲は、「0～65535」です。
設定した宛先ポート番号のパケットがACEに一致します。

Dest. Port Range ……

[Dest. Port Filter]欄で「Range」を選択したときに、宛先ポート番号範囲を指定します。
設定できる範囲は、「0～65535」です。
設定した宛先ポート番号内のパケットがACEに一致します。

「ACE Configuration」画面

Configuration > Security > Network > ACL > Access Control List

UDP Parameters/UDPv6 Parameters/TCP Parameters/TCPv6 Parameters

TCP FIN ……

TCPフレームのFINビットでフィルタリングするかを設定します。
FINビットが「1」のとき、コネクションの切断要求であることを意味します。

Any ：FINビットではフィルタリングしません。
0 ：FINビットが「0」のTCPフレームをフィルタリングします。
1 ：FINビットが「1」のTCPフレームをフィルタリングします。

TCP SYN……

TCPフレームのSYNビットでフィルタリングするかを設定します。
SYNビットが「1」のとき、コネクションの接続要求であることを意味します。

Any ：SYNビットではフィルタリングしません。
0 ：SYNビットが「0」のTCPフレームをフィルタリングします。
1 ：SYNビットが「1」のTCPフレームをフィルタリングします。

TCP RST ……

TCPフレームのRSTビットでフィルタリングするかを設定します。
RSTビットが「1」のとき、コネクションを強制切断することを意味します。

Any ：RSTビットではフィルタリングしません。
0 ：RSTビットが「0」のTCPフレームをフィルタリングします。
1 ：RSTビットが「1」のTCPフレームをフィルタリングします。

TCP PSH……

TCPフレームのPSHビットでフィルタリングするかを設定します。
PSHビットが「1」のとき、データをすぐに上位のアプリケーションに渡すことを意味します。

Any ：PSHビットではフィルタリングしません。
0 ：PSHビットが「0」のTCPフレームをフィルタリングします。
1 ：PSHビットが「1」のTCPフレームをフィルタリングします。

TCP ACK……

TCPフレームのACKビットでフィルタリングするかを設定します。
ACKビットが「1」のとき、確認応答番号フィールドが有効なことを意味します。

Any ：ACKビットではフィルタリングしません。
0 ：ACKビットが「0」のTCPフレームをフィルタリングします。
1 ：ACKビットが「1」のTCPフレームをフィルタリングします。

TCP URG……

TCPフレームのURGビットでフィルタリングするかを設定します。
URGビットが「1」のとき、緊急で処理しなければいけないデータが含まれていることを意味します。

Any ：URGビットではフィルタリングしません。
0 ：URGビットが「0」のTCPフレームをフィルタリングします。
1 ：URGビットが「1」のTCPフレームをフィルタリングします。

「ACE Configuration」画面

Configuration > Security > Network > ACL > Access Control List

Ethernet Type Parameters

[Frame Type]欄で「Ethernet Type」が選択されているときに設定できます。

EtherType Filter …… フレームのEtherTypeフィールドでフィルタリングするかを設定します。

Any ：EtherTypeフィールドではフィルタリングしません。

Specific ：設定したEtherTypeフィールド値でフィルタリングします。
EtherType値を指定するための項目が表示されます。

Ethernet Type Value …… [EtherType Filter]欄で「Specific」を選択したとき、EtherType値を指定します。
設定できる範囲は、0x800(IPv4)、0x806(ARP)、0x86DD(IPv6)を除く「0x600～0xFFFF」です。
設定したEtherType値のパケットがACEに一致します。

「Configuration」画面

Configuration > Security > Network > IP Source Guard > Configuration

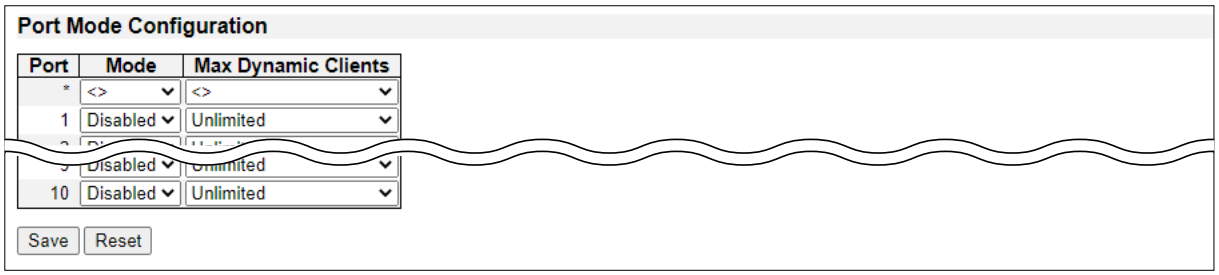
IPソースガードについて設定します。

IP Source Guard Configuration

Mode ……　システム全体でIPソースガードを使用するか選択します。

〈Translate dynamic to static〉…　すべての動的IPソースガードテーブルのエントリを、静的IPソースガードテーブルのエントリに変換するボタンです。

Port Mode Configuration



Port ……　本製品のポート番号が表示されます。

Mode ……　ポートごとにIPソースガードを使用するかどうかを選択します。
「IP Source Guard Configuration」の[Mode]欄で「Enabled」を選択したとき、「Enabled」に設定したポートでIPソースガードが使用できます。

Max Dynamic Clients ……　学習できる動的クライアントの最大数を指定します。
設定できる範囲は、「0」～「2」、または「Unlimited」(無制限)です。
「0」に設定した場合、静的IPソースガードテーブルと一致したIPパケットだけが転送されます。

〈Save〉 ……　設定した内容を保存するボタンです。

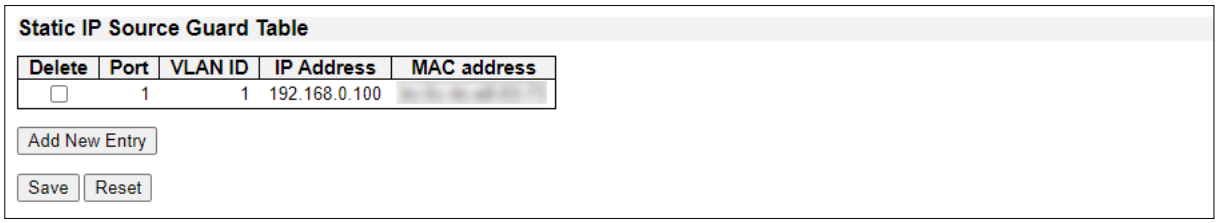
〈Reset〉 ……　設定内容を変更したとき、変更前の状態に戻すボタンです。

「Static Table」画面

Configuration > Security > Network > IP Source Guard > Static Table

静的IPソースガードテーブルを設定します。
※最大112件まで登録できます。

Static IP Source Guard Table



Delete …… 登録された内容を削除するとき、ボックスにチェックマークを入れます。

Port …… ポート番号を選択します。

VLAN ID …… VLAN IDを指定します。

IP Address …… 送信元IPアドレスを指定します。

MAC address …… 送信元MACアドレスを指定します。

〈Add New Entry〉 …… クリックして新しいエントリを追加します。

〈Save〉 …… 設定した内容を保存するボタンです。

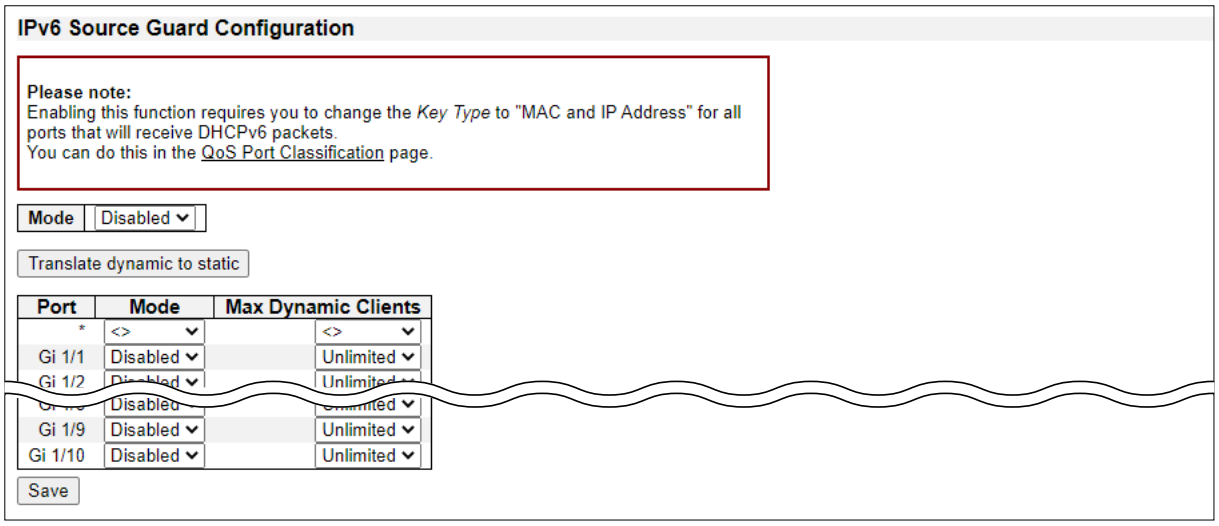
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Configuration」画面

Configuration > Security > Network > IPv6 Source Guard > Configuration

IPv6ソースガードについて設定します。

IPv6 Source Guard Configuration



Mode……システム全体で、IPv6ソースガードを使用するか選択します。

〈Translate dynamic to static〉…すべての動的IPソースガードテーブルのエントリを、静的IPソースガードテーブルのエントリに変換するボタンです。

Port……本製品のポート番号が表示されます。

Mode……ポートごとにIPソースガードを使用するかどうかを選択します。
システム全体のIPv6ソースガードを有効にしたとき、「Enabled」に設定したポートでIPソースガードが使用できます。

Max Dynamic Clients……学習できる動的クライアントの最大数を指定します。
設定できる範囲は、「0」～「2」、または「Unlimited」(無制限)です。
「0」に設定した場合、静的IPソースガードテーブルと一致したIPv6パケットだけが転送されます。

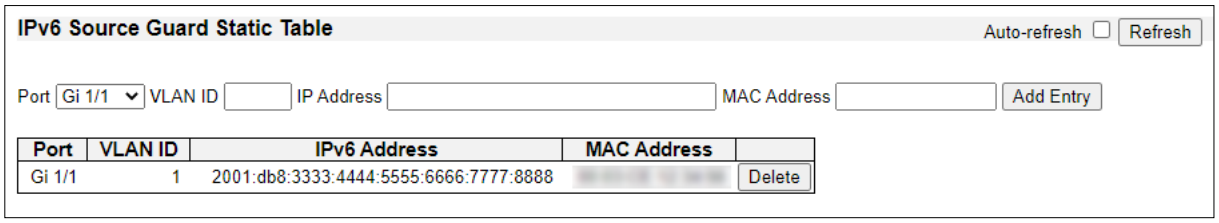
〈Save〉……設定した内容を保存するボタンです。

「Static Table」画面

Configuration > Security > Network > IPv6 Source Guard > Static Table

静的IPv6ソースガードテーブルを設定します。
※最大112件まで登録できます。

IPv6 Source Guard Static Table



Auto-refresh …… 自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 …… 最新の状態に更新するボタンです。

Port [ポート番号] VLAN ID [VLAN ID] IP Address [IPアドレス] MAC Address [MACアドレス] ……
静的IPv6ソースガードテーブルに追加する内容を入力します。
※MACアドレスは「xx:xx:xx:xx:xx:xx」形式で入力してください。

〈Add Entry〉 …… 入力した内容を静的IPv6ソースガードテーブルに追加するボタンです。

Port …… ポート番号が表示されます。

VLAN ID …… VLAN IDが表示されます。
VLAN IDが割り当てられていない場合、「0」が表示されます。

IPv6 Address …… 送信元IPv6アドレスが表示されます。

MAC address …… 送信元MACアドレスが表示されます。

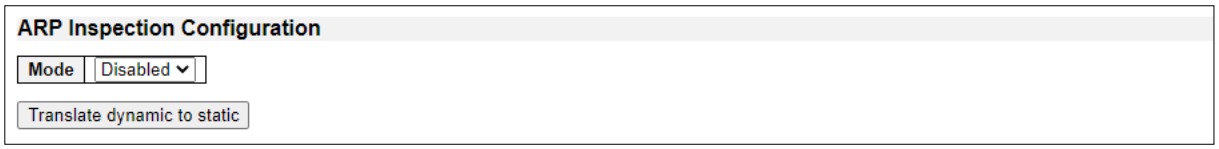
〈Delete〉 …… 登録した内容を削除するボタンです。

「Port Configuration」画面

Configuration > Security > Network > ARP Inspection > Port Configuration

ARPインスペクションについて設定します。

ARP Inspection Configuration



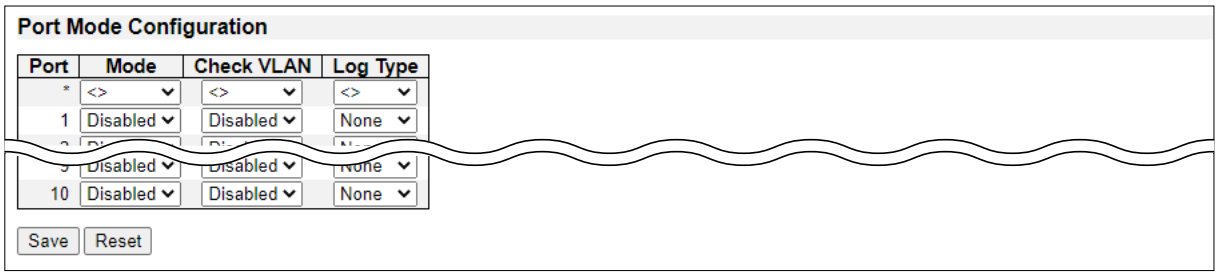
Mode…… システム全体でARPインスペクションを使用するか設定します。

〈Translate dynamic to static〉… すべての動的ARPインスペクションテーブルのエントリを、静的ARPインスペクションテーブルのエントリに変換するボタンです。

「Port Configuration」画面

Configuration > Security > Network > ARP Inspection > Port Configuration

Port Mode Configuration



Port …… 本製品のポート番号が表示されます。

Mode …… ポートごとにARPインスペクションを使用するかを選択します。
「ARP Inspection Configuration」の[Mode]欄で「Enabled」を選択したとき、「Enabled」に設定したポートでARP インスペクションが使用できます。

Check VLAN …… ARPインスペクションをVLAN単位で有効にするかどうかを選択します。

Enabled：
VLAN単位のARPインスペクションを有効にします。
ARPインスペクションのログタイプは、「VLAN Configuration」画面の設定にしたがいます。

Disabled：
VLAN単位のARPインスペクションを無効にします。
ARPインスペクションのログタイプは、ポートごとの[Log Type]欄の設定にしたがいます。

Log Type …… ARPインスペクションが有効なポートで、[Check VLAN]欄を「Disabled」に設定したときに、ARPインスペクションのログを記録するかどうか選択します。

None ：システムログに記録しません。
Deny ：拒否されたエントリをシステムログに記録します。
Permit ：許可されたエントリをシステムログに記録します。
ALL ：すべてのエントリをシステムログに記録します。

〈Save〉 …… 設定した内容を保存するボタンです。

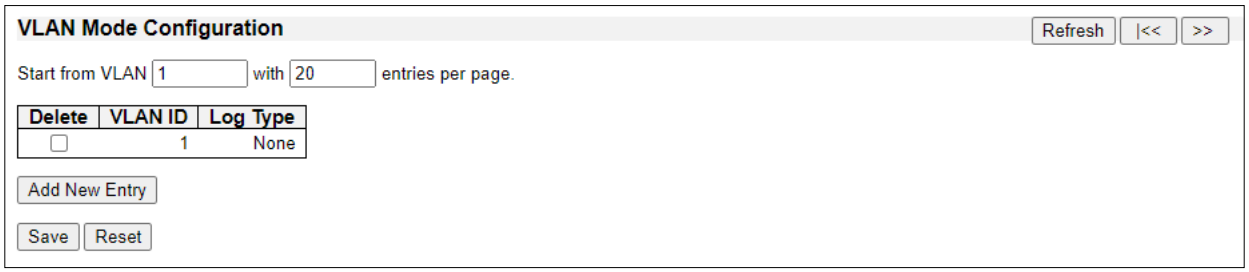
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「VLAN Configuration」画面

Configuration > Security > Network > ARP Inspection > VLAN Configuration

ARPインスペクションを使用するときに、VLANごとのログについて設定します。
※「Port Configuration」画面で、VLAN単位のARPインスペクションを有効に設定してください。

VLAN Mode Configuration



〈Refresh〉 …… 最新の状態に更新するボタンです。
※設定内容を変更したときは、変更前の状態に戻ります。

〈|<<〉…… 最初のページに戻るボタンです。

〈>>〉 …… 次のページに進むボタンです。

Start from VLAN [VLAN ID] with [表示数] entries per page.
…… ページ表示の設定です。
VLANテーブルのうち、VLAN IDの一番小さいエントリがはじめに表示されます。
[VLAN ID]欄で、VLANテーブルの開始VLAN IDを指定できます。
[表示数]欄で1ページあたりの表示数を指定できます。(最大9999件まで)

Delete …… 登録された内容を削除するとき、ボックスにチェックマークを入れます。

VLAN ID …… 検査対象とするVLAN IDを指定します。

Log Type…… VLANごとに、ARPインスペクションのログを記録するかどうか選択します。

None ：システムログに記録しません。
Deny ：拒否されたエントリをシステムログに記録します。
Permit ：許可されたエントリをシステムログに記録します。
ALL ：すべてのエントリをシステムログに記録します。

〈Add New Entry〉…… クリックして新しいVLANの設定を追加します。

〈Save〉 …… 設定した内容を保存するボタンです。

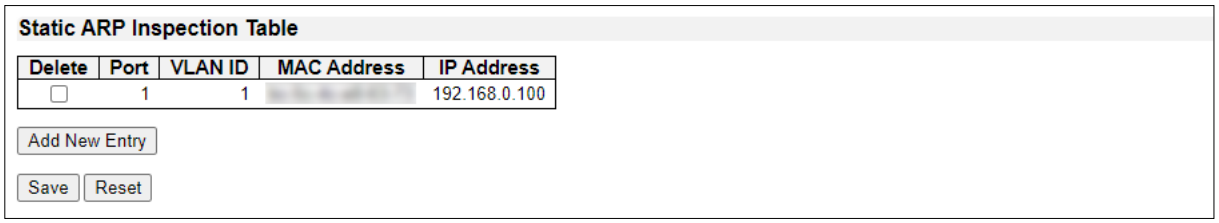
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Static Table」画面

Configuration > Security > Network > ARP Inspection > Static Table

静的ARPインスペクションテーブルを設定します。
※最大256件まで登録できます。

Static ARP Inspection Table



Delete …… 登録された内容を削除するとき、ボックスにチェックマークを入れます。

Port …… ポート番号を選択します。

VLAN ID …… VLAN IDを指定します。

MAC address …… MACアドレスを指定します。

IP Address …… IPアドレスを指定します。

〈Add New Entry〉 …… クリックして、新しいIPアドレスとMACアドレスの組み合わせを追加します。

〈Save〉 …… 設定した内容を保存するボタンです。

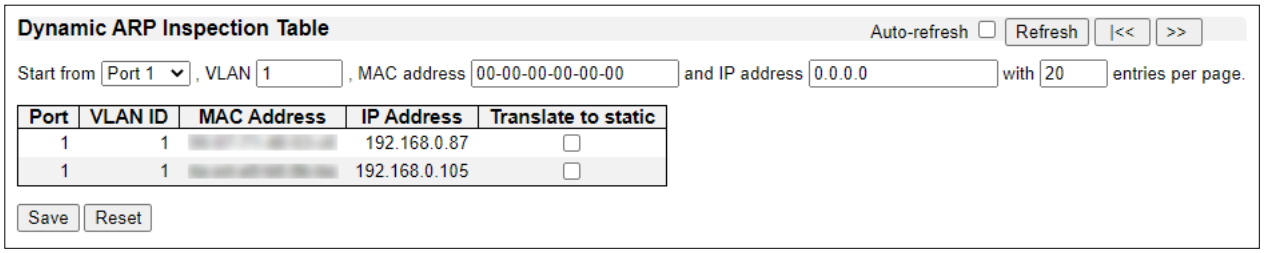
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Dynamic Table」画面

Configuration > Security > Network > ARP Inspection > Dynamic Table

動的ARPインスペクションテーブルが表示されます。
動的ARPインスペクション テーブルにはMACアドレスとIPアドレスの組み合わせが最大256件まで登録され、ポート番号、VLAN ID、MAC アドレス、IP アドレスでソートされます。
すべてのエントリは、DHCPスヌーピング機能を使用して学習します。

Dynamic ARP Inspection Table



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈|<<〉 ……　最初のページに戻るボタンです。

〈>>〉 ……　次のページに進むボタンです。

Start from［ポート番号］, VLAN［VLAN ID］, MAC address［MACアドレス］and IP address［IPアドレス］with［表示数］entries per page.
……　動的ARPインスペクションテーブルのうち、VLAN IDの一番小さいエントリがはじめに表示されます。
［ポート番号］、［VLAN ID］、［MACアドレス］、［IPアドレス］欄で、テーブルの開始位置を指定できます。
［表示数］欄で1ページあたりの表示数を指定できます。（最大99件まで）

Port ……　本製品のポート番号が表示されます。

VLAN ID ……　ARPトラフィックが許可されたVLAN IDが表示されます。

MAC Address ……　ユーザーからARPリプライで通知されたMACアドレスが表示されます。

IP Address ……　ユーザーIPアドレスが表示されます。

Translate to static ……　静的ARPインスペクションテーブルのエントリに変換するとき、ボックスにチェックマークを入れます。

〈Save〉 ……　設定した内容を保存するボタンです。

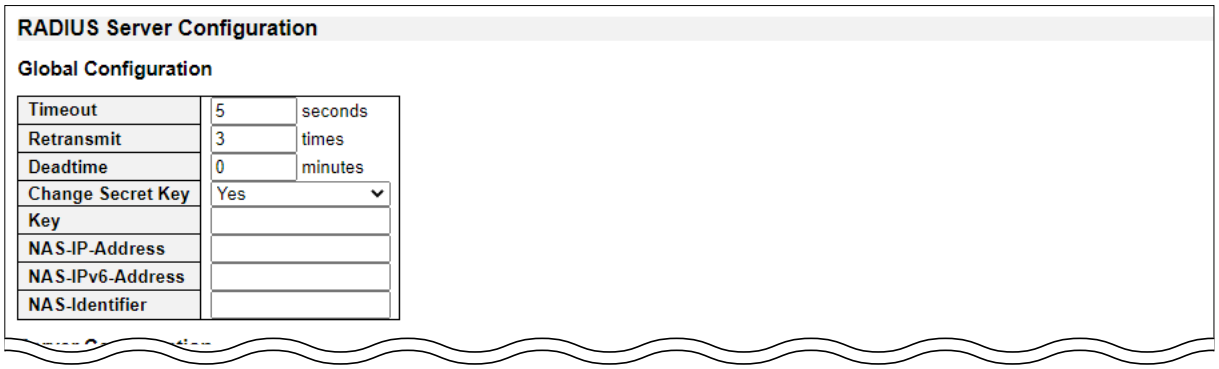
〈Reset〉 ……　設定内容を変更したとき、変更前の状態に戻すボタンです。

「RADIUS」画面

Configuration > Security > AAA > RADIUS

RADIUSサーバーについて設定します。
※最大5台まで登録できます。

RADIUS Server Configuration



Global Configuration(すべてのRADIUSサーバーで共通の設定です。)

Timeout …… RADIUS要求を再送する前に、RADIUSサーバーからの応答を待機する時間を設定します。
設定できる範囲は、「1～1000」(秒)です。

Retransmit …… 応答していないサーバーに、RADIUS要求を再送する回数を設定します。
設定できる範囲は、「1～1000」です。
最後の送信後にサーバーが応答しなかった場合、サーバーはデッド状態と判断されます。

Deadtime …… デッド状態と判断されたサーバーに、新しい要求を送信しない時間を設定します。
設定できる範囲は、「0～1440」(分)です。
設定した期間、デッド状態と判断されたサーバーへの接続を試行しなくなります。
※複数のRADIUSサーバーが登録されているときに、0より大きい値を設定すると有効になります。

Change Secret Key …… 共有秘密鍵を変更するかどうかを選択します。

Key …… [Change Secret Key]欄で「Yes」を選択したときに、RADIUSサーバーとの共有秘密鍵を、63文字以内で指定します。

NAS-IP-Address …… RADIUS Access-RequestパケットのAttribute 4で使用する、NASのIPv4アドレスを指定します。
空白の場合は、発信インターフェースのIPアドレスが使用されます。

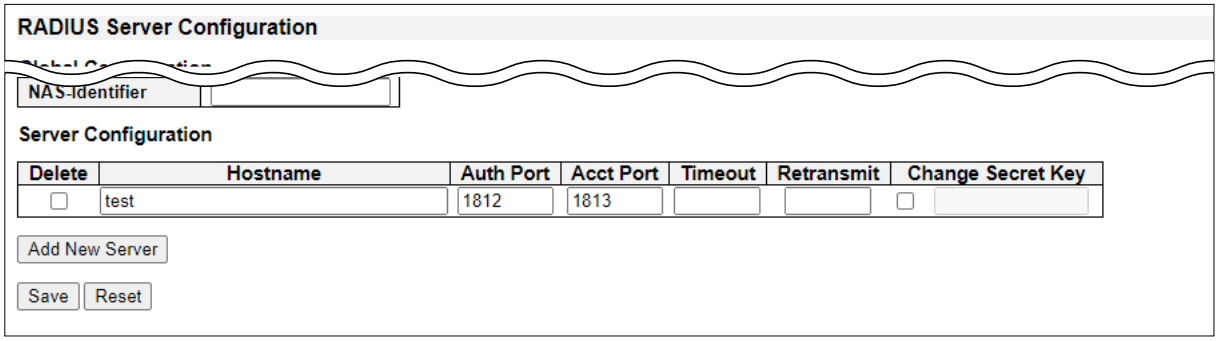
NAS-IPv6-Address …… RADIUS Access-RequestパケットのAttribute 95で使用する、NASのIPv6アドレスを指定します。
空白の場合は、発信インターフェースのIPアドレスが使用されます。

NAS-Identifier …… RADIUS Access-RequestパケットのAttribute 32で使用する、NASの識別子を最大253文字以内で指定します。
このフィールドを空白のままにすると、NASの識別子はパケットに含まれません。

「RADIUS」画面

Configuration > Security > AAA > RADIUS

RADIUS Server Configuration



Server Configuration(RADIUSサーバーごとの設定です。)

Delete …… 登録された内容を削除するとき、ボックスにチェックマークを入れます。

Hostname …… RADIUSサーバーのIPアドレス(IPv4/IPv6)、またはホスト名を入力します。

Auth Port …… 認証のためにRADIUSサーバーで使用するUDPポートを指定します。
「0」に設定すると、認証が無効になります。

Acct Port …… アカウンティングのために RADIUSサーバーで使用するUDPポートを指定します。
「0」に設定すると、アカウンティングが無効になります。

Timeout …… 「Global Configuration」の[Timeout]欄で設定したタイムアウト時間を使用しないときに、サーバーごとにタイムアウト時間を設定します。
空白の場合は、「Global Configuration」の[Timeout]欄で設定したタイムアウト時間を使用します。

Retransmit …… 「Global Configuration」の[Retransmit]欄で設定した再送回数を使用しないときに、サーバーごとに再送回数を設定します。
空白の場合は、「Global Configuration」の[Retransmit]欄で設定した再送回数を使用します。

Change Secret Key …… 共有秘密鍵を変更するとき、ボックスにチェックマークを入れます。
空白の場合は、「Global Configuration」の[Change Secret Key]欄で設定した共有秘密鍵を使用します。

〈Add New Server〉 …… クリックして新しいRADIUSサーバーを追加します。

〈Save〉 …… 設定した内容を保存するボタンです。

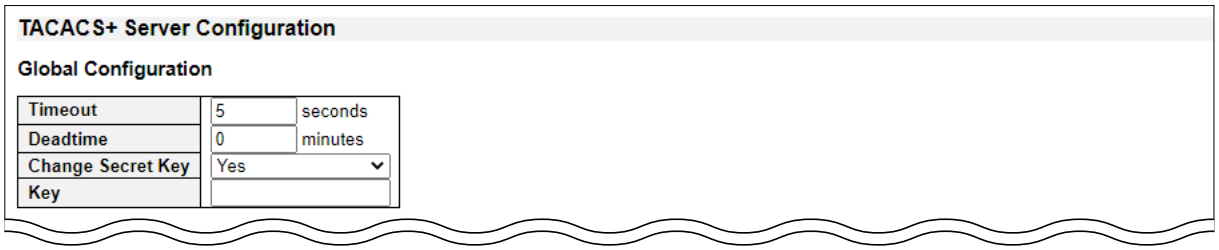
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「TACACS+」画面

Configuration > Security > AAA > TACACS+

TACACS+サーバーについて設定します。
※最大5台まで登録できます。

TACACS+ Server Configuration



Global Configuration(すべてのTACACS+サーバーで共通の設定です。)

Timeout …… TACACS+サーバーがデッド状態と判断されるまで待機する時間を設定します。
設定できる範囲は、「1～1000」(秒)です。

Deadtime…… デッド状態と判断されたサーバーに、新しい要求を送信しない時間を設定します。
設定できる範囲は、「0～1440」(分)です。
設定した期間、デッド状態と判断されたサーバーへの接続を試行しなくなります。
※複数のTACACS+サーバーが登録されているときに、0より大きい値を設定すると有効になります。

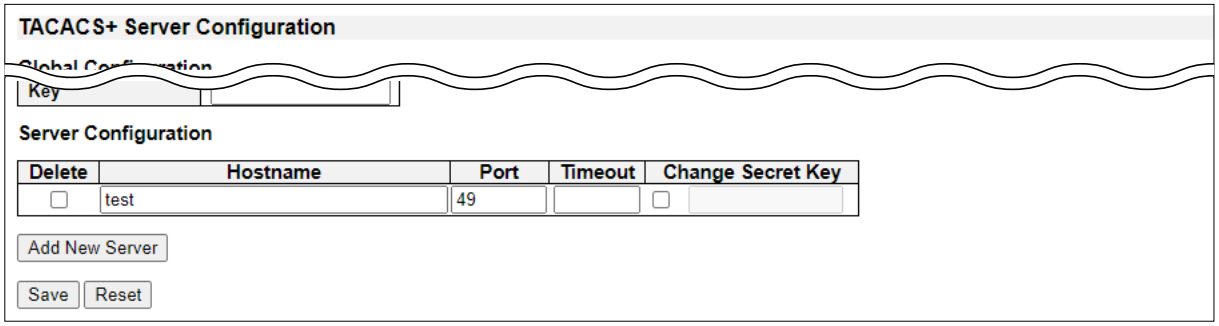
Change Secret Key …… 共有秘密鍵を変更するかどうかを選択します。

Key …… [Change Secret Key]欄で「Yes」を選択したときに、TACACS+サーバーとの共有秘密鍵を、63文字以内で指定します。

「TACACS+」画面

Configuration > Security > AAA > TACACS+

TACACS+ Server Configuration



Server Configuration(TACACS+サーバーごとの設定です。)

Delete …… 登録された内容を削除するとき、ボックスにチェックマークを入れます。

Hostname …… TACACS+サーバーのIPアドレス(IPv4/IPv6)、またはホスト名を入力します。

Port …… 認証のためにTACACS+サーバーで使用するTCPポートを指定します。

Timeout …… 「Global Configuration」の[Timeout]欄で設定したタイムアウト時間を使用しないときに、サーバーごとにタイムアウト時間を設定します。
空白の場合は、「Global Configuration」の[Timeout]欄で設定したタイムアウト時間を使用します。

Change Secret Key …… 共有秘密鍵を変更するとき、ボックスにチェックマークを入れます。
空白の場合は、「Global Configuration」の[Change Secret Key]欄で設定した共有秘密鍵を使用します。

〈Add New Server〉 …… クリックして新しいTACACS+サーバーを追加します。

〈Save〉 …… 設定した内容を保存するボタンです。

〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Common」画面

Configuration > Aggregation > Common

リンクアグリゲーションの負荷分散方式の組み合わせを設定します。
設定は、システム全体に適用されます。

Common Aggregation Configuration

Hash Code Contributors

Source MAC Address …… 宛先ポートの決定に送信元MACアドレスを使用するとき、ボックスにチェックマークを入れます。

Destination MAC Address …… 宛先ポートの決定に宛先MACアドレスを使用するとき、ボックスにチェックマークを入れます。

IP Address …… 宛先ポートの決定にIPアドレスを使用するとき、ボックスにチェックマークを入れます。

TCP/UDP Port Number …… 宛先ポートの決定にTCP/UDPポート番号を使用するとき、ボックスにチェックマークを入れます。

〈Save〉 …… 設定した内容を保存するボタンです。

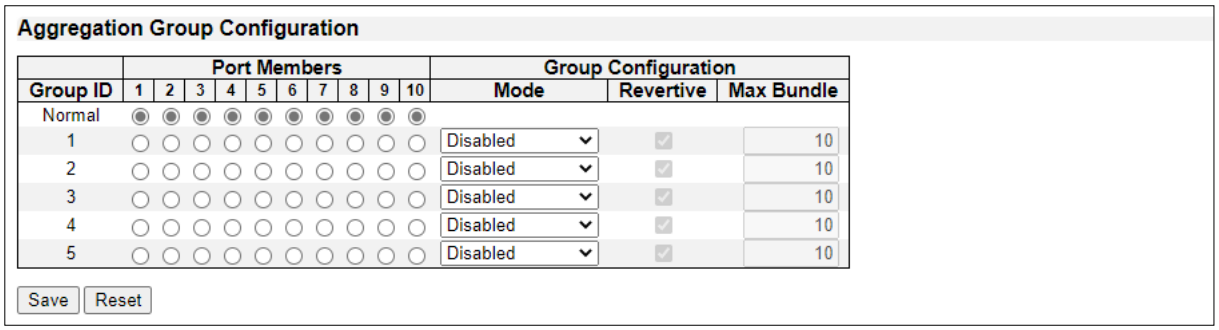
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Groups」画面

Configuration > Aggregation > Groups

リンクアグリゲーショングループを設定します。

Aggregation Group Configuration



Group ID ……

グループIDが表示されます。
「Normal」は、リンクアグリゲーションを使用しないグループです。

Port Members 1～10 ……

ポートごとに所属するグループを選択します。
※1ポートは複数のグループに所属できません。
※全二重モードのポートだけがリンクアグリゲーションを使用できます。
　グループ内のポートは、同じ速度で動作している必要があります。

Group Configuration

Mode ……

アグリゲーショングループの動作を選択します。

Disabled：
リンクアグリゲーションは無効になります。

Static：
静的リンクアグリゲーションモードで動作します。

LACP (Active)：
LACP activeモードで動作します。
詳細は、IEEE 802.1AX-2014のセクション6.4.1を参照してください。

LACP (Passive)：
LACP passiveモードで動作します。
詳細は、IEEE 802.1AX-2014のセクション6.4.1を参照してください。

Revertive ……

[Mode]欄で「LACP (Active)」、または「LACP (Passive)」に設定したときに、優先度の高いリンクが使用できるようになると、自動でハッシュ値を再計算するかどうかを設定します。

Max Bundle ……

[Mode]欄で「LACP (Active)」、または「LACP (Passive)」に設定したときに、バンドルできるポート数を指定します。

〈Save〉 ……

設定した内容を保存するボタンです。

〈Reset〉 ……

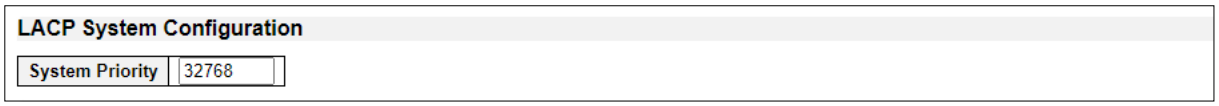
設定内容を変更したとき、変更前の状態に戻すボタンです。

「LACP」画面

Configuration > Aggregation > LACP

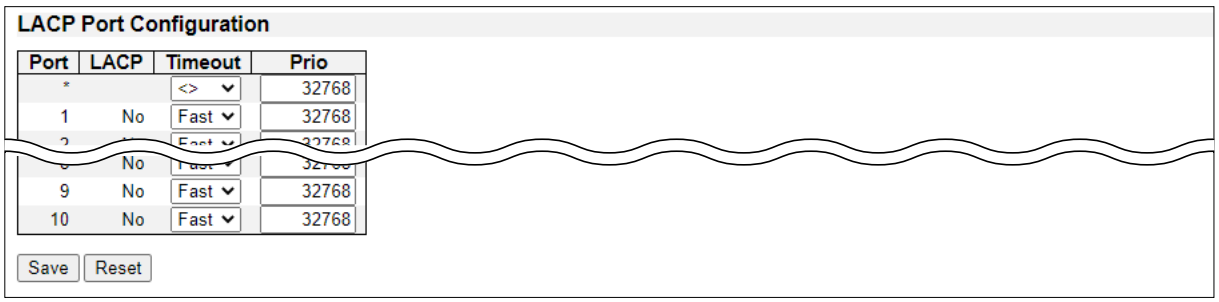
LACPについて設定します。

LACP System Configuration



System Priority …… システム全体の優先度を設定します。
設定できる範囲は、「1～65535」です。

LACP Port Configuration



Port …… 本製品のポート番号が表示されます。

LACP …… アグリゲーショングループに所属しているかどうかが表示されます。

Timeout …… BPDU(Bridge Protocol Data Unit)の送信間隔を設定します。

Fast ：毎秒LACPパケットを送信します。

Slow ：30秒ごとにLACPパケットを送信します。

Prio …… ポートの優先度を設定します。
設定できる範囲は、「1～65535」です。
数値が小さいほど、優先度が高くなります。
LACPパートナーが本製品でサポートされているグループよりも大きなグループを構築する場合、アクティブになるポートと障害発生に備えてスタンバイになるポートを判断します。

〈Save〉 …… 設定した内容を保存するボタンです。

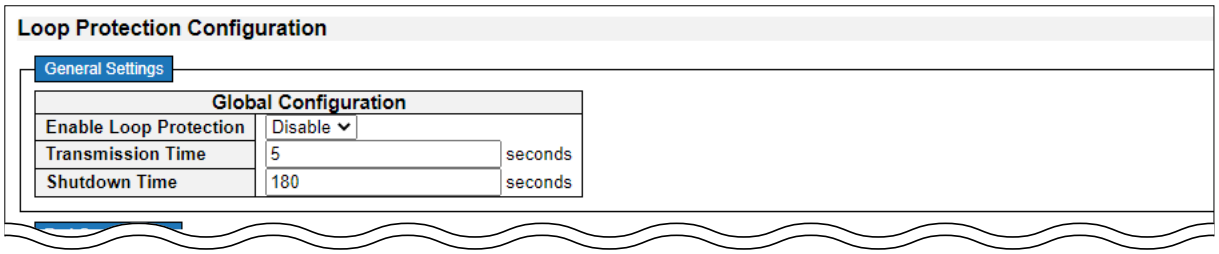
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Loop Protection」画面

Configuration > Loop Protection

ループプロテクションについて設定します。

Loop Protection Configuration



General Settings

Enable Loop Protection ……　システム全体で、ループプロテクションを有効にするかどうかを設定します。

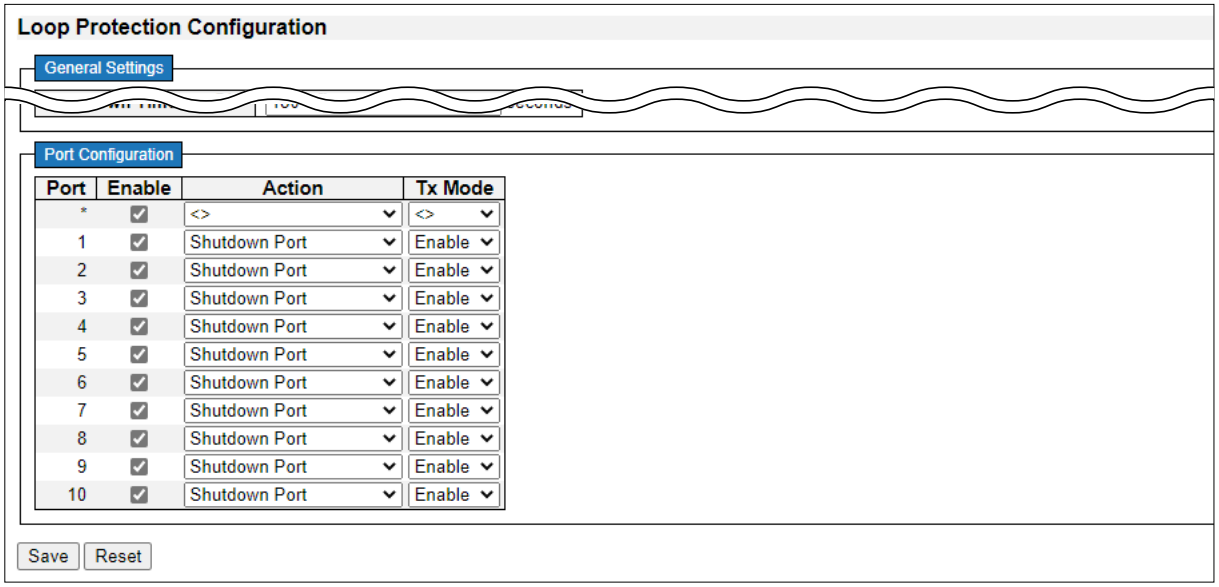
Transmission Time……　PDU(ループ保護データユニット)の送信間隔を設定します。
設定できる範囲は、「1～10」(秒)です。

Shutdown Time ……　ループが検出されるとポートをシャットダウンするように設定しているときに、シャットダウンを解除するまでの期間を設定します。
設定できる範囲は、「0～604800」(秒)(最大7日)です。
「0」に設定すると、本製品が再起動するまで、ポートはシャットダウンしたままになります。

「Loop Protection」画面

Configuration > Loop Protection

Loop Protection Configuration



Port Configuration

Port …… 本製品のポート番号が表示されます。

Enable …… ポートごとにループプロテクションを有効にするかどうかを設定します。

Action …… ポートでループが検出されたときの動作を選択します。

Shutdown Port：
ポートをシャットダウンします。

Shutdown Port and Log：
ポートをシャットダウンし、システムログに記録します。

Log Only：
ポートをシャットダウンせずに、システムログに記録します。

Tx Mode …… ポートの送信動作を設定します。

Enabled ：ポートがPDUを生成します。

Disabled ：PDUを生成せずに、ループしたPDUを検索するだけになります。

〈Save〉 …… 設定した内容を保存するボタンです。

〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

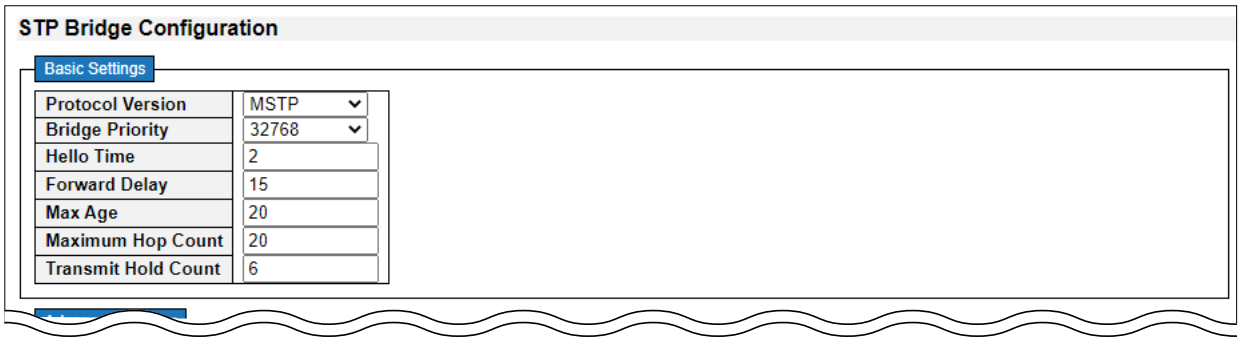
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Bridge Settings」画面

Configuration > Spanning Tree > Bridge Settings

システム全体のSTP(スパニングツリープロトコル)について設定します。

STP Bridge Configuration



Basic Settings

Protocol Version ……

プロトコルの種類を「MSTP」、「RSTP」、「STP」から選択します。

Bridge Priority ……

ブリッジの優先度を選択します。
数値が小さいほど、優先度が高くなります。
ブリッジIDは、ブリッジの優先度とMSTIインスタンス番号、本製品のMACアドレス(6バイト)で構成されます。
◎[Protocol Version]欄を「MSTP」に設定したときは、CISTの優先度を設定します。
◎それ以外の場合は、STP/RSTPブリッジの優先度を設定します。

Hello Time ……

BPDUの送信間隔を設定します。
設定できる範囲は、「1～10」(秒)です。
※初期設定(2秒)から変更すると、ネットワークに悪影響を及ぼす可能性があります。

Forward Delay ……

転送遅延タイマーを設定します。
転送遅延タイマーは、ルートポート(RP)と指定ポート(DP)がListening状態からLearning状態、Learning状態からForwarding状態に遷移するときの待機時間です。
設定できる範囲は、「4～30」(秒)です。
※初期設定(15秒)から変更すると、ネットワークに悪影響を及ぼす可能性があります。

Max Age ……

最大エージタイマーを設定します。
最大エージタイマーは、ルートブリッジがBPDUを送信する間隔です。
指定した時間内にルートブリッジからBPDUを受信しなければ、スパニングツリーを再計算します。
設定できる範囲は、「6～40」(秒)です。
※「([Forward Delay] － 1) * 2」以下に設定してください。
※初期設定(20秒)から変更すると、ネットワークに悪影響を及ぼす可能性があります。

「Bridge Settings」画面

Configuration > Spanning Tree > Bridge Settings

STP Bridge Configuration

Maximum Hop Count…… MSTを使用しているときに、ルートブリッジが送信するBPDUの最大ホップ数を指定します。
経由したブリッジが設定値を超えると、BPDUが破棄されます。
設定できる範囲は、「6～40」です。

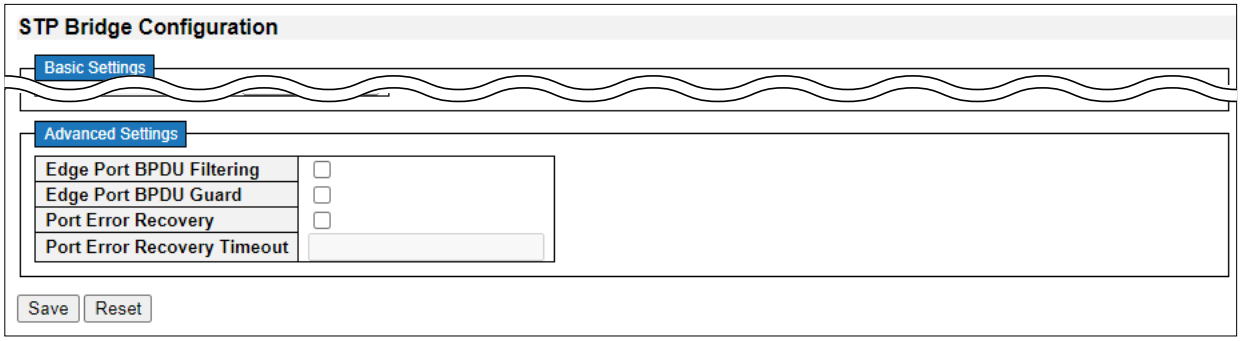
Transmit Hold Count…… ブリッジポートが1秒あたりに送信するBPDU数を設定します。
設定した値を超えると、次のBPDU送信が遅延します。
設定できる範囲は、「1～10」です。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Bridge Settings」画面

Configuration > Spanning Tree > Bridge Settings

STP Bridge Configuration



Advanced Settings

Edge Port BPDU Filtering …… エッジポートがBPDUを送受信するかどうかを設定します。

Edge Port BPDU Guard …… エッジポートがBPDUを受信したときに、ポートをerror-disabled状態にするかどうかを設定します。
ポートはerror-disabled状態になり、アクティブなトポロジーから削除されます。

Port Error Recovery …… error-disabled状態のポートを一定時間後に自動で有効にするかどうかを設定します。
無効に設定した場合、error-disabled状態になったポートは、手動で有効にする必要があります。
本製品を再起動しても、ポートを再度有効にできます。

Port Error Recovery Timeout … error-disabled状態のポートを有効にするまでの時間を設定します。
設定できる範囲は、「30～86400」(秒)(最大24時間)です。

〈Save〉 …… 設定した内容を保存するボタンです。

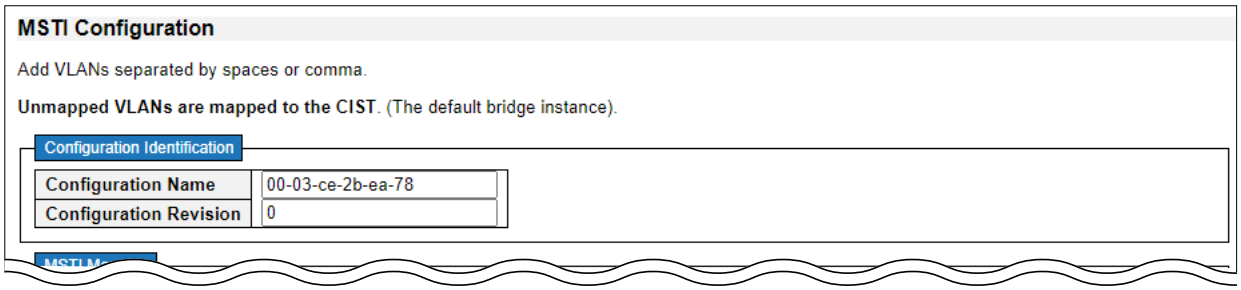
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「MSTI Mapping」画面

Configuration > Spanning Tree > MSTI Mapping

VLANとMSTブリッジインスタンスのマッピングについて設定します。

MSTI Configuration



Configuration Identification

Configuration Name ……

VLANとMSTIのマッピング設定を識別するためのリージョン名を、32文字以内で設定します。
スパニングツリーを共有するために、同じリージョン内の機器とリージョン名とリビジョン番号[Configuration Revision]、VLANとMSTIのマッピング設定を同じにしてください。

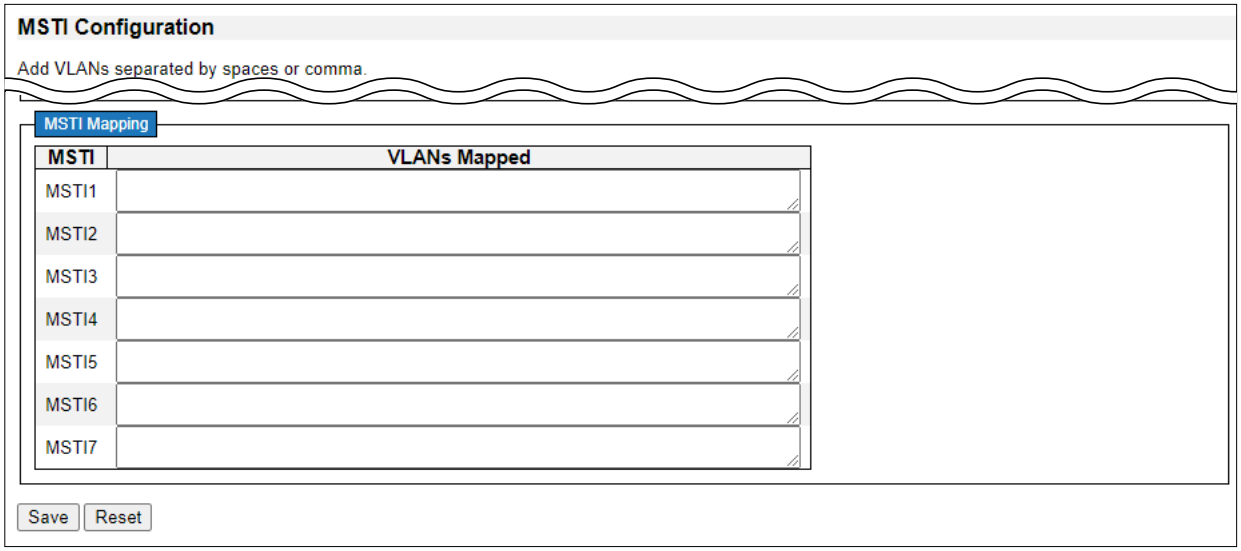
Configuration Revision ……

MSTIのリビジョン番号を設定します。
設定できる範囲は、「0～65535」です。

「MSTI Mapping」画面

Configuration > Spanning Tree > MSTI Mapping

MSTI Configuration



MSTI Mapping

MSTI …… ブリッジインスタンスが表示されます。
CISTは、MSTIにマッピングされていないすべてのVLANに関連付けられるため、マッピングするVLANを指定できません。

VLANs Mapped …… MSTIにマッピングするVLANを設定します。
設定できるVLANは、「1～4094」です。
VLANは単数(xx)、または範囲(xx-yy)で指定できます。
複数指定する場合は、それぞれをコンマかスペースで区切ってください。
(例：2,5,20-40)
1つのVLANを複数のMSTIにマッピングすることはできません。
VLANがマッピングされていない未使用のMSTIは、空白にしてください。

〈Save〉 …… 設定した内容を保存するボタンです。

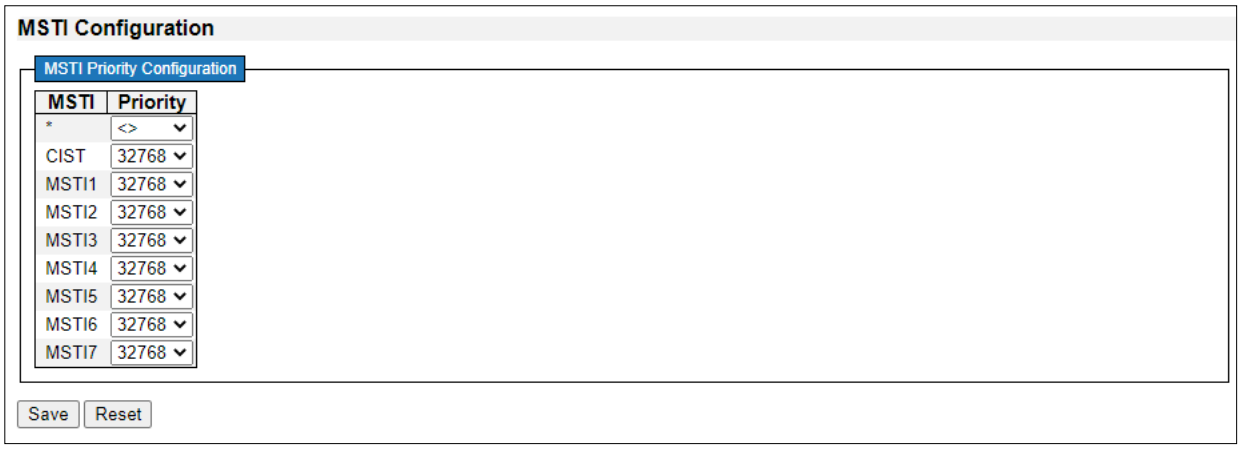
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「MSTI Priorities」画面

Configuration > Spanning Tree > MSTI Priorities

MSTブリッジインスタンスの優先度を設定します。

MSTI Configuration



MSTI Priority Configuration

MSTI …… ブリッジインスタンスが表示されます。
CISTは特殊なインスタンスで、常に有効になっています。

Priority …… ブリッジの優先度を設定します。
設定できる範囲は、「0」～「61440」(4096刻み)です。
数値が小さいほど、優先度が高くなります。
ブリッジの優先度とMSTインスタンス番号、スイッチのMACアドレス(6バイト)でブリッジIDを構成します。

〈Save〉 …… 設定した内容を保存するボタンです。

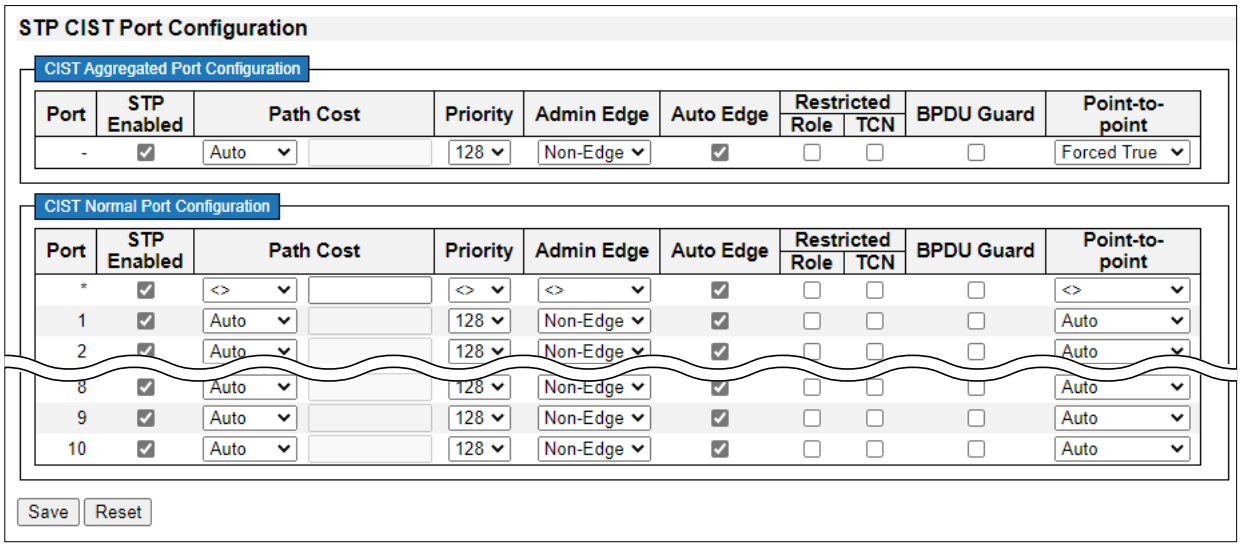
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「CIST Ports」画面

Configuration > Spanning Tree > CIST Ports

CISTポートについて設定します。
※リンクアグリゲーションポートと物理ポートの設定が含まれています。

STP CIST Port Configuration



CIST Aggregated Port Configuration/CIST Normal Port Configuration

Port …… 本製品のポート番号が表示されます。

STP Enabled …… STPを有効にするかどうかを設定します。

Path Cost …… ポートで発生するパスコストを設定します。
パスコストは、ネットワークのアクティブトポロジーを確立するときに使用され、パスコストの最も小さいポートがForwarding状態になります。
◎「Auto」を選択すると、802.1Dの推奨値を使用して、物理リンク速度に応じたパスコストが設定されます。
◎「Specific」を選択すると、任意の値を入力できます。
設定できる範囲は、「1～200000000」です。

Priority …… ポートの優先度を設定します。
同じポートコストを持つポートを比較するために使用されます。
優先度が最も小さいポートがForwarding状態になります。

Admin Edge …… ポートがエッジポートかどうかを選択します。
ポートが初期化されたときのoperEdgeフラグ値になります。

operEdge(state flag)について
ポートにブリッジが取り付けられておらず、直接エッジデバイスに接続しているかどうかを示すブーリアン型のフラグです。
Forwarding状態への移行は、ほかのポートよりエッジポート(operEdge=true)の方が高速です。
エッジポートかどうかは、[AdminEdge]欄と[AutoEdge]欄の設定に基づいて判断されます。
値は、「Monitor」→「Spanning Tree」→「STP Detailed Bridge Status」画面の[Edge]欄で確認できます。

「CIST Ports」画面

Configuration > Spanning Tree > CIST Ports

STP CIST Port Configuration

Auto Edge ……

自動エッジ検出を有効にするかどうかを設定します。
自動エッジ検出機能を使用すると、BPDUがポートで受信されたかどうかからエッジポートかどうか(operEdgeフラグ値)を自動で判断します。

Restricted Role ……

ポートをCIST、または任意のMSTIのルートポートとして使用するかどうかを設定します。
チェックマークを入れると、最も小さいルートパスコストを持っているとしてもルートポートとしては使用されず、ルートポートの決定後、代替ポートに設定されます。
管理外のブリッジを接続したときに、スパニングツリーのアクティブトポロジーに影響を与えないようにするための機能です。
この機能はルートガードとも呼ばれます。
※設定を変更すると、スパニングツリー接続が切断される可能性があります。

Restricted TCN ……

受信したトポロジー変更通知(TNC)やトポロジー変更をほかのポートに伝達するかを設定します。
チェックマークを入れると、受信したトポロジー変更通知やトポロジー変更を他のポートに伝達しません。
設定を変更すると、スパニングツリーのアクティブトポロジーが変更されたあと、機器の位置情報が継続的に正しく学習されなかった場合に、一時的に切断される可能性があります。
管理外のブリッジが接続されたか、接続されたLANの物理リンク状態が頻繁に変化することが原因で、学習したアドレスがクリアされないようにするための機能です。

BPDU Guard ……

有効なBPDUを受信したときに、ポート自体を無効にするかどうかを設定します。
この機能によってerror-disabled状態になったポートには、「Bridge Settings」画面にある[Port Error Recovery]欄の設定が適用されます。

Point-to-point ……

ポートがポイントツーポイントリンク(直接機器が接続されている)かどうかを設定します。
シェアードリンク(HUBなどで複数の機器が接続されている)よりもポイントツーポイントリンクの方が速くForwarding状態へ移行します。

Forced True ：trueに固定します。
Forced False ：falseに固定します。
Auto ：自動で判別します。

〈Save〉 ……

設定した内容を保存するボタンです。

〈Reset〉 ……

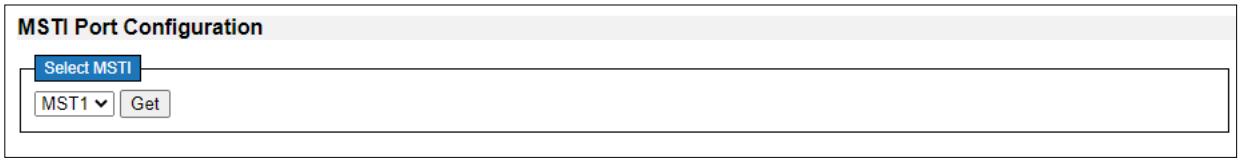
設定内容を変更したとき、変更前の状態に戻すボタンです。

「MSTI Ports」画面

Configuration > Spanning Tree > MSTI Ports

MSTIポートについて設定します。
MSTIポートは、本製品のポートに適用される各MSTインスタンスのアクティブなCISTポート(物理ポート)ごとにインスタンス化された仮想ポートです。
はじめに、MSTIポート設定を表示するMSTインスタンスを選択してください。
※リンクアグリゲーションポートと物理ポートの設定が含まれています。

MSTI Port Configuration



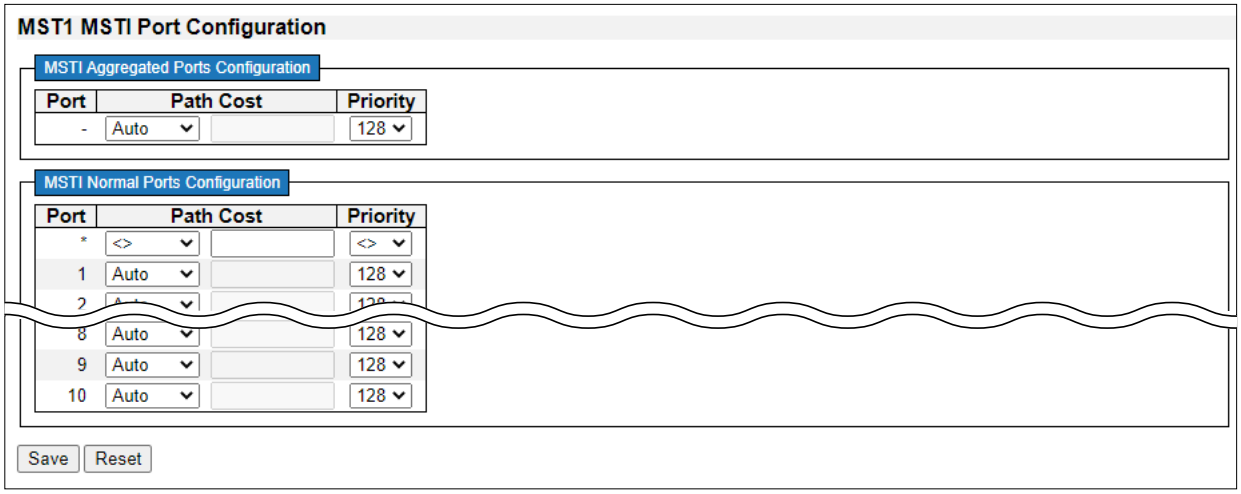
Select MSTI

〈Get〉…… クリックすると、選択したMSTインスタンスの設定画面に移動します。

「MSTI Ports」画面

Configuration > Spanning Tree > MSTI Ports

MST1～7 MSTI Port Configuration



MSTI Aggregated Ports Configuration/MSTI Normal Ports Configuration

Port …… 本製品のポート番号が表示されます。
自動エッジ検出機能を使用すると、BPDUがポートで受信されたかどうかからエッジポートかどうか(operEdgeフラグ値)を自動で判断します。

Path Cost …… ポートで発生するパスコストを設定します。
パスコストは、ネットワークのアクティブトポロジーを確立するときに使用され、パスコストの最も小さいポートがForwarding状態になります。
◎「Auto」を選択すると、802.1Dの推奨値を使用して、物理リンク速度に応じたパスコストが設定されます。
◎「Specific」を選択すると、任意の値を入力できます。
設定できる範囲は、「1～200000000」です。

Priority …… ポートの優先度を設定します。
同じポートコストを持つポートを比較するために使用されます。
優先度が最も小さいポートがForwarding状態になります。

〈Save〉 …… 設定した内容を保存するボタンです。

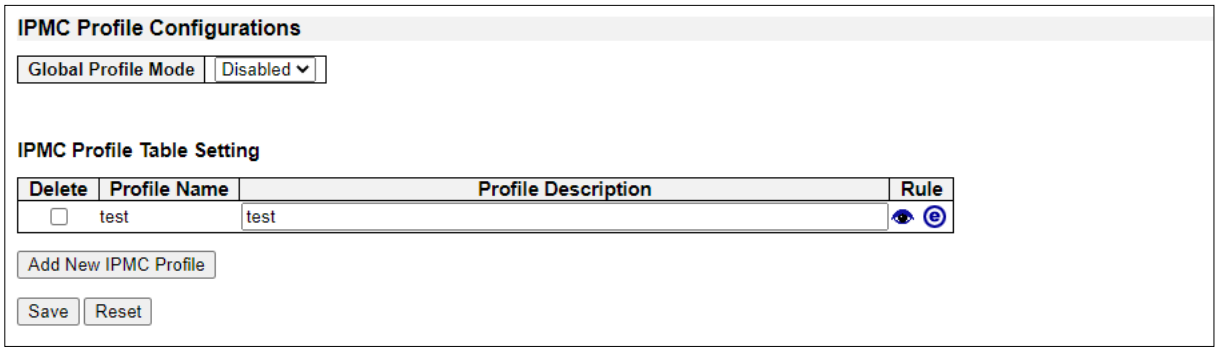
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Profile Table」画面

Configuration > IPMC Profile > Profile Table

IPMCプロファイルについて設定します。
IPMCプロファイルは、IPマルチキャストストリームのアクセス制御に使用されます。
最大64個のプロファイルと、1つのプロファイルにつき最大128個のルールを作成できます。

IPMC Profile Configurations



Global Profile Mode ……
システム全体でIPMCプロファイルを有効にするかどうかを設定します。
有効になっている場合に、プロファイル設定に基づいてフィルタリングを実行します。

IPMC Profile Table Setting

Delete ……
登録された内容を削除するとき、ボックスにチェックマークを入れます。

Profile Name ……
プロファイルテーブルのインデックスに使用される名前を、英数字16文字以内で設定します。

Profile Description ……
プロファイルについての説明を英数字64文字以内で設定します。
ブランク文字やスペースは使用できません。
説明を区切る場合は、「_(アンダースコア)」か「-(ハイフン)」を使用してください。

 ……
プロファイルのルール一覧を表示するボタンです。

 ……
プロファイルのルールを編集するボタンです。
「IPMC Profile Rule Settings」画面に移動します。

〈Add New IPMC Profile〉 ……
クリックして新しいIPMCプロファイルを追加します。
※新しいIPMCプロファイルを追加するときは、[Profile Name]欄を入力してから〈Save〉をクリックしてください。

〈Save〉 ……
設定した内容を保存するボタンです。

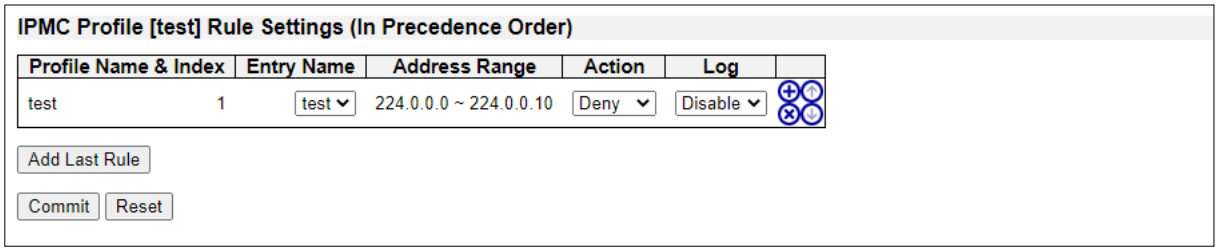
〈Reset〉 ……
設定内容を変更したとき、変更前の状態に戻すボタンです。

「IPMC Profile Rule Settings」画面

Configuration > IPMC Profile > Profile Table

IPMCプロファイルのフィルタリングルールを設定します。
ルールが優先度順に表示されます。
最初のルールエントリの優先度が最も高く、最後のルールエントリの優先度が最も低くなります。
※プロファイルに[Action]欄が「Permit」(許可)のルールが含まれていない場合、プロファイルはすべてのグループに対して「Deny」(拒否)アクションを実行します。

IPMC Profile [Profile Name] Rule Settings (In Precedence Order)



Profile Name & Index …… プロファイル名と、ルールのインデックス番号が表示されます。

Entry Name …… ルールで使用するアドレス範囲を指定します。
「Address Entry」画面で設定したアドレス範囲テーブルから選択できます。
※「-」(なし)は選択できません。

Address Range …… [Entry Name]欄で選択したアドレス範囲が表示されます。
アドレス範囲は、「Address Entry」画面で設定します。

Action …… グループアドレスがルールのアドレス範囲と一致するJoin/Reportフレームを受信したときの動作を設定します。

Permit：
ルールで指定した範囲に一致するグループアドレスを登録します。

Deny：
ルールで指定された範囲に一致するグループアドレスは削除されます。

Log …… グループアドレスがルールのアドレス範囲と一致するJoin/Reportフレームを受信したときに、システムログに記録するかどうかを設定します。

Enable：
ルールで指定した範囲に一致するグループアドレスの対応する情報をシステムログに記録します。

Disable：
ルールで指定した範囲に一致するグループアドレスの対応する情報をシステムログに記録しません。

「IPMC Profile Rule Settings」画面

Configuration > IPMC Profile > Profile Table

IPMC Profile [Profile Name] Rule Settings (In Precedence Order)

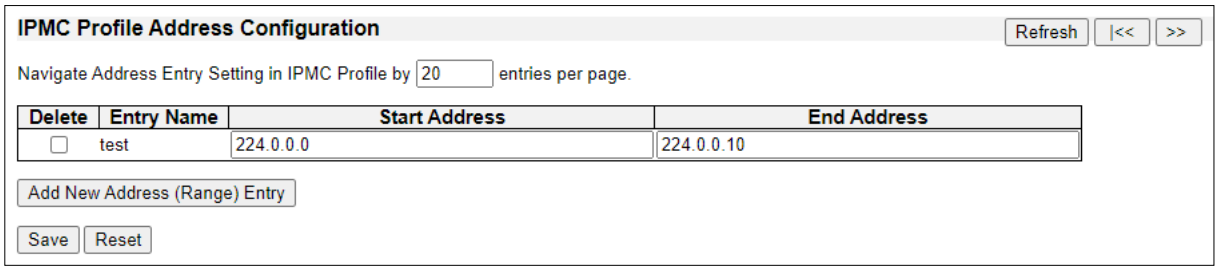
⊕ ……	1つ前にルールを追加するボタンです。
⊗ ……	ルールを削除するボタンです。
↑ ……	1つ上に移動するボタンです。
↓ ……	1つ下に移動するボタンです。
〈Add Last Rule〉 ……	クリックしてプロファイルのルールリストの最後に新しいルールを追加します。 ※新しいルールを追加するときは、[Entry Name]欄を選択してから〈Commit〉をクリックしてください。
〈Commit〉 ……	プロファイルのルール変更を保存するボタンです。
〈Reset〉 ……	設定内容を変更したとき、変更前の状態に戻すボタンです。

「Address Entry」画面

Configuration > IPMC Profile > Address Entry

IPMCプロファイルで使用するアドレス範囲テーブルを設定します。
※最大128個まで登録できます。

IPMC Profile Address Configuration



〈Refresh〉 …… 最新の状態に更新するボタンです。
※設定内容を変更したときは、変更前の状態に戻ります。

〈|<<〉…… 最初のページに戻るボタンです。

〈>>〉 …… 次のページに進むボタンです。

Navigate Address Entry Setting in IPMC Profile by [表示数] entries per page.
…… ページ表示の設定です。
[表示数]欄で1ページあたりの表示数を指定できます。

Delete …… 登録された内容を削除するとき、ボックスにチェックマークを入れます。

Entry Name …… アドレス範囲テーブルのインデックスとして使用する名前を、英数字16文字以内で設定します。

Start Address/End Address … IPv4/IPv6マルチキャストグループのアドレス範囲を設定します。

〈Add New Address (Range) Entry〉 クリックして新しいアドレス範囲を追加します。
※新しいアドレス範囲を追加するときは、[Entry Name]、[Start Address]、[End Address]欄を入力してから〈Save〉をクリックしてください。

〈Save〉 …… 設定した内容を保存するボタンです。

〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「MVR」画面

Configuration > MVR

MVR(Multicast VLAN Registration)について設定します。

MVR機能は、マルチキャストVLANを使用してマルチキャストトラフィックを転送・制御する機能です。
マルチキャストテレビアプリケーションでは、パソコンやネットワークテレビ、セットトップボックスがマルチキャストストリームを受信できます。
複数のセットトップボックス、またはパソコンを1つのサブスクライバーポート(レシーバーポートに設定された物理ポート)に接続できます。
加入者がチャンネルを選択すると、セットトップボックス、またはパソコンはマルチキャストグループに参加するために、接続されているスイッチにIGMP/MLD Reportメッセージを送信します。
マルチキャストVLANとのあいだでマルチキャストデータを送受信するアップリンクポートを、ソースポートと呼びます。

クエリア(Queryメッセージを送信するルーター)はソースポートに接続してください。
MVR VLANの静的メンバーシップを与えられたデバイスは、ダウンストリーム(レシーバーポート)からアップストリーム(ソースポート)にIGMP Reportを転送しますが、ダウンストリームからのQueryメッセージは破棄します。
MVR VLANメンバーが正しく構成されたら、[Interface Channel Profile]欄でIPMCプロファイルを、選択してください。
チャンネルプロファイルは、「Configuration」→「IPCM Profile」→「Profile Table」画面で設定されたIPCMプロファイルから選択します。
IPCMプロファイルを使用する場合は、「Configuration」→「IPCM Profile」→「Profile Table」→[Global Profile Mode]欄を「Enabled」に設定してください。
※最大4件まで登録できます。

MVR Configurations

MVR Mode ……

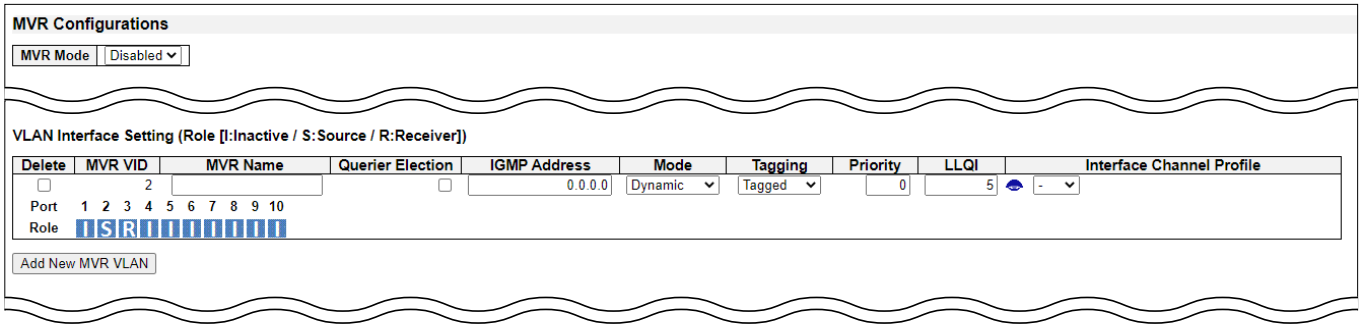
システム全体でMVRを使用するかを設定します。
未登録のIPトラフィックをVLAN内にフラッディングするかどうかは、IGMP/MLDスヌーピングの設定によって異なります。
MVRグループテーブルがいっぱいのときに、フラッディング制御を有効にすることをおすすめします。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「MVR」画面

Configuration > MVR

MVR Configurations



VLAN Interface Setting (Role [I:Inactive / S:Source / R:Receiver])

Delete …… 登録された内容を削除するとき、ボックスにチェックマークを入れます。

MVR VID …… マルチキャストVLAN IDを指定します。

MVR Name …… MVR VLANの名称を英数字16文字以内で設定します。
※登録後も設定を変更できます。

Querier Election …… クエリア選定の対象とするかどうかを設定します。
VLAN内で最も小さいIPv4/IPv6アドレスの装置がクエリアとして選定され、クエリアになった装置がQueryメッセージを送信します。
無効にすると、クエリアとして動作しません。

IGMP Address …… 本製品がクエリアとして動作するときに、IGMPパケットのIP ヘッダーに含まれる送信元アドレスとなるIPv4アドレスを設定します。

Mode …… MVRのモードを設定します。

Dynamic：
動的MVRメンバーシップレポートをソースポートから出力します。

Compatible：
MVRメンバーシップレポートをソースポートから出力しません。

Tagging …… トラバースされたIGMP/MLD制御フレームをタグなしで送信するか、MVR VIDでタグ付けするかを選択します。

Priority …… トラバースされたIGMP/MLD制御フレームの優先度を設定します。

「MVR」画面

Configuration > MVR

MVR Configurations

LLQI ……

クエリアとして動作時、Queryメッセージを送信してからマルチキャストグループメンバーシップからポートを削除するまでの待機時間を設定します。
待機時間が経過してもレシーバーポートでIGMP/MLD Reportメンバーシップを受信しなかった場合、マルチキャストグループメンバーシップからポートを削除します。
設定できる範囲は、「0～31744」(×0.1秒)です。

Interface Channel Profile……

MVR VLANのチャンネルフィルタリング条件として、IPMCプロファイルを選択します。

 ……

[Interface Channel Profile]欄で選択したプロファイルの、ルール一覧を表示するボタンです。

Port ……

本製品のポート番号が表示されます。

Role ……

ポートの役割を設定します。
※Management VLANポートをソースポートに設定することは推奨されません。
※[Role]に表示されているアイコンをクリックすると、ポートの役割が切り替わります。
MVR機能が無効(Inactive)の場合は「I」、ソースポートの場合は「S」、レシーバーポートの場合は「R」が表示されます。

Inactive：
MVR機能を使用しません。

Source：
ソースポートとして使用します。
ソースポートは、マルチキャストデータを送受信するアップリンクポートです。
ソースポートにサブスクライバーを直接接続することはできません。

Receiver：
レシーバーポートとして使用します。
マルチキャストデータだけを受信するサブスクライバーポートを、レシーバーポートに設定してください。
IGMP/MLDメッセージを送信してマルチキャストグループに参加してから、データを受信できるようになります。

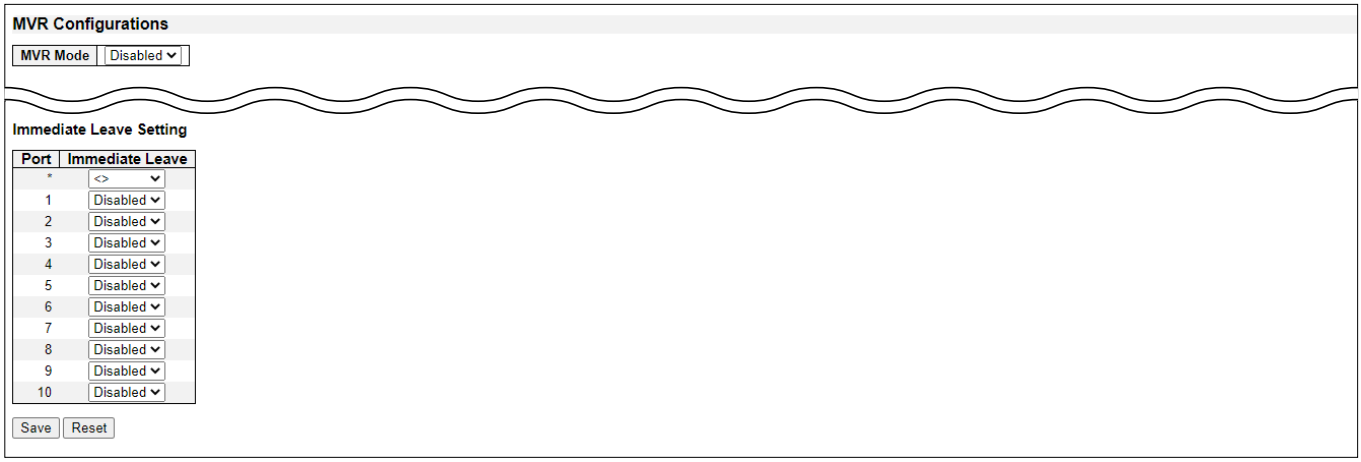
〈Add New MVR VLAN〉……

クリックして新しいMVR VLANを追加します。
※新しいMVR VLANを追加するときは、[MVR VID]欄を入力してから〈Save〉をクリックしてください。

「MVR」画面

Configuration > MVR

MVR Configurations



Immediate Leave Setting

Port …… 本製品のポート番号が表示されます。

Immediate Leave…… ファストリーブ機能を使用するかどうかを設定します。
ファストリーブ機能を使用すると、ホストからのIGMPv2/MLDv1 leaveメッセージを受信したときに、メンバーシップQueryメッセージを送信することなくグループからホストを削除し、データの転送を停止します。
※IGMPv2/MLDv1ホストがポートに複数接続されている場合は、無効にすることをおすすめします。

〈Save〉 …… 設定した内容を保存するボタンです。

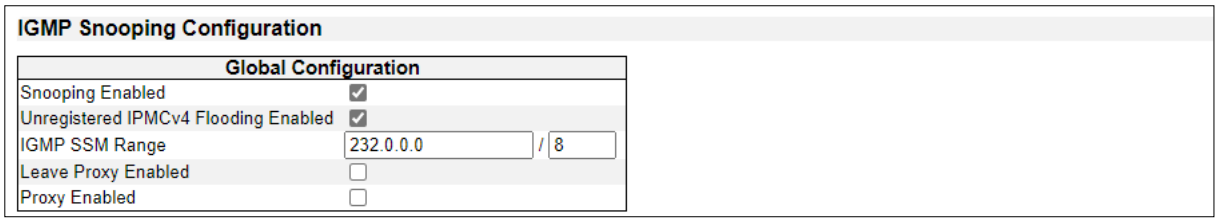
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Basic Configuration」画面

Configuration > IPMC > IGMP Snooping > Basic Configuration

IGMPスヌーピングについて設定します。

IGMP Snooping Configuration



Global Configuration

Snooping Enabled ……　システム全体でIGMPスヌーピングを有効にするかを設定します。

Unregistered IPMCv4 Flooding Enabled
……　未登録のIPMCv4トラフィックをVLAN内にフラッディングするかどうかを設定します。
フラッディング制御は、IGMPスヌーピング使用時に有効な機能です。
IGMPスヌーピングが無効になっている場合、設定に関わらず未登録のIPMCv4トラフィックは常にフラッディングされます。

IGMP SSM Range ……　SSM(Source-Specific Multicast)で使用するアドレス範囲を、IPv4マルチキャストアドレスとプレフィックス長で設定します。
SSM対応のホストとルーターは、アドレス範囲内のグループに対してSSMサービスを実行します。

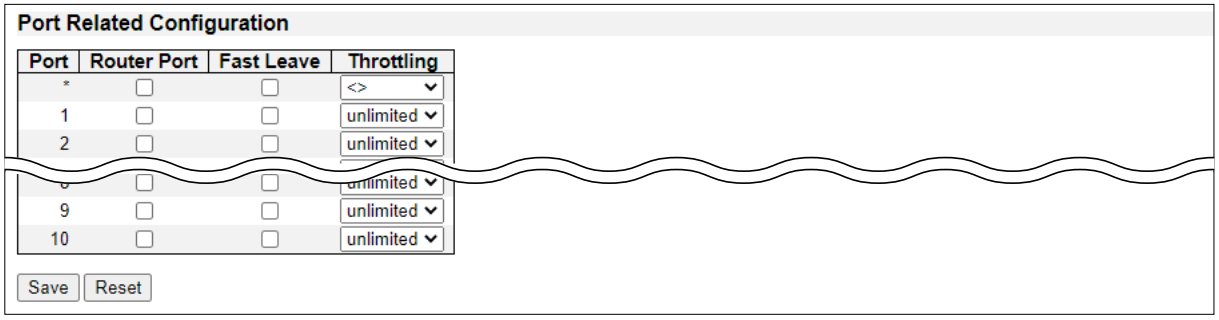
Leave Proxy Enabled……　IGMP Leaveプロキシーを使用するかどうかを設定します。
IGMP Leaveプロキシーを使用すると、不要なleaveメッセージをルーター側に転送しないようにできます。

Proxy Enabled ……　IGMPプロキシーを使用するかどうかを設定します。
IGMPプロキシーを使用すると、不要なjoinメッセージやleaveメッセージをルーター側に転送しないようにできます。

「Basic Configuration」画面

Configuration > IPMC > IGMP Snooping > Basic Configuration

Port Related Configuration



Port …… 本製品のポート番号が表示されます。

Router Port …… ルーターポートとして機能するポートを指定します。
ルーターポートは、レイヤー3 マルチキャストデバイス、またはIGMPクエリアが接続されているポートです。
アグリゲーションメンバーのポートがルーターポートとして選択されている場合、アグリゲーション全体がルーターポートとして機能します。

Fast Leave …… ファストリーブ機能を使用するかどうかを設定します。
ファストリーブ機能を使用すると、ホストからのIGMPv2 leaveメッセージを受信したときに、メンバーシップQueryメッセージを送信することなくグループからホストを削除し、データの転送を停止します。
※IGMPv2ホストがポートに複数接続されている場合は、無効にすることをおすすめします。

Throttling …… 所属するマルチキャストグループの上限を設定します。

〈Save〉 …… 設定した内容を保存するボタンです。

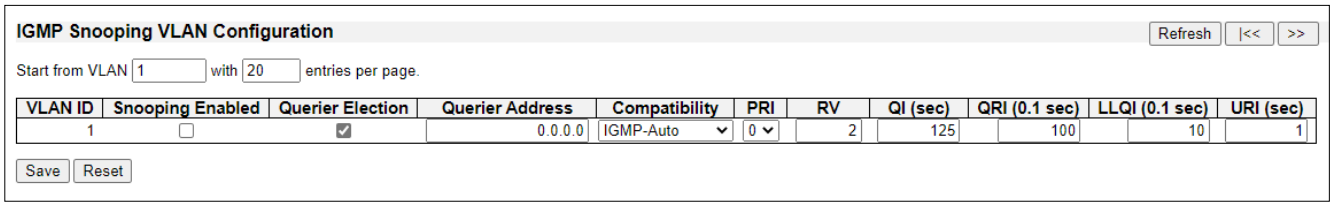
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「VLAN Configuration」画面

Configuration > IPMC > IGMP Snooping > VLAN Configuration

IGMPスヌーピングのVLANインターフェースについて設定します。
※IGMPスヌーピングのVLANインターフェースを作成する前に、「Configuration」→「System」→「IP」画面でIPインターフェースを設定してください。

IGMP Snooping VLAN Configuration



〈Refresh〉 …… 最新の状態に更新するボタンです。
※設定内容を変更したときは、変更前の状態に戻ります。

〈|<<〉…… 最初のページに戻るボタンです。

〈>>〉 …… 次のページに進むボタンです。

Start from VLAN [VLAN ID] with [表示数] entries per page.
…… ページ表示の設定です。
VLANテーブルのうち、VLAN IDの一番小さいエントリがはじめに表示されます。
[VLAN ID]欄で、VLANテーブルの開始VLAN IDを指定できます。
[表示数]欄で1ページあたりの表示数を指定できます。(最大99件)

VLAN ID …… VLAN IDが表示されます。

Snooping Enabled …… IGMPスヌーピングを有効にするかどうかを設定します。
VLANは最大8個まで使用できます。

Querier Election …… クエリア選定の対象とするかどうかを設定します。
VLAN内で最も小さいIPアドレスの装置がクエリアとして選定され、クエリアになった装置がQueryメッセージを送信します。
無効にすると、クエリアとして動作しません。

Querier Address …… クエリア選定時に、IPヘッダーに含まれる送信元IPv4アドレスを設定します。

Compatibility…… IGMPのバージョンを「IGMP-Auto」、「Forced IGMPv1」、「Forced IGMPv2」、「Forced IGMPv3」から選択します。
ネットワーク内にあるそれぞれのホストとルーターで動作しているIGMPバージョンに応じて適切に運用することで、互換性が保証されます。

「VLAN Configuration」画面

Configuration > IPMC > IGMP Snooping > VLAN Configuration

IGMP Snooping VLAN Configuration

PRI …… IGMP制御フレームの優先度を選択します。
設定できる範囲は、「0」(ベストエフォート)～「7」(優先度高)です。

RV …… RV(Robustness Variable)を設定します。
RVは、ネットワーク上で予想されるパケット損失を調整するためのパラメーターです。
設定できる範囲は、「1～255」です。

QI (sec) …… QI(Query Interval)を設定します。
QIは、クエリアがQueryメッセージを送信する間隔です。
設定できる範囲は、「1～31744」(秒)です。

QRI (0.1 sec) …… QRI(Query Response Interval)を設定します。
QRIは、IGMP General Queryメッセージに対する最大応答待機時間です。
設定できる範囲は、「0～31744」(×0.1秒)です。

LLQI (0.1 sec) …… LLQI(Last Listener Query Interval)を設定します。
LLQIは、group-specific、またはgroup-and-source-specific Queryメッセージへの応答を待機する時間です。
待機時間は、[LLQI]で設定した時間に[Last Member Query Count]値を乗算した時間です。
設定できる範囲は、「0～31744」(×0.1秒)です。

URI (sec) …… URI(Unsolicited Report Interval)を設定します。
URIは、ホストがグループのメンバーであることを通知するために送信するunsolicited IGMP reportの送信間隔です。
設定できる範囲は、「0～31744」(秒)です。

〈Save〉 …… 設定した内容を保存するボタンです。

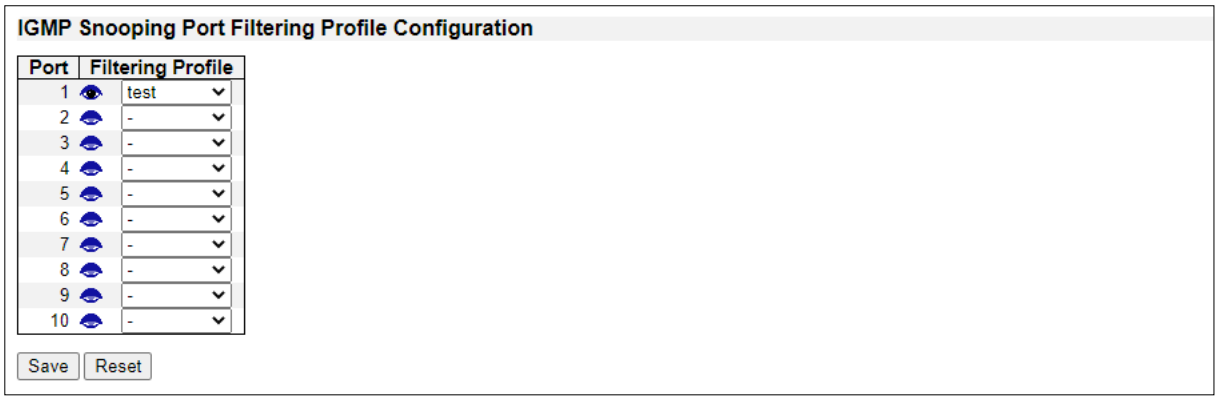
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Port Filtering Profile」画面

Configuration > IPMC > IGMP Snooping > Port Filtering Profile

IGMPスヌーピングのポートフィルターについて設定します。

IGMP Snooping Port Filtering Profile Configuration



Port …… 本製品のポート番号が表示されます。

 …… [Filtering Profile]欄で選択したプロファイルの、ルール一覧を表示するボタンです。

Filtering Profile…… IPMCプロファイルテーブルからフィルタリング条件を選択します。
※IPMCプロファイルテーブルは「Configuration」→「IPMC Profile」→「Profile Table」画面で設定します。

〈Save〉 …… 設定した内容を保存するボタンです。

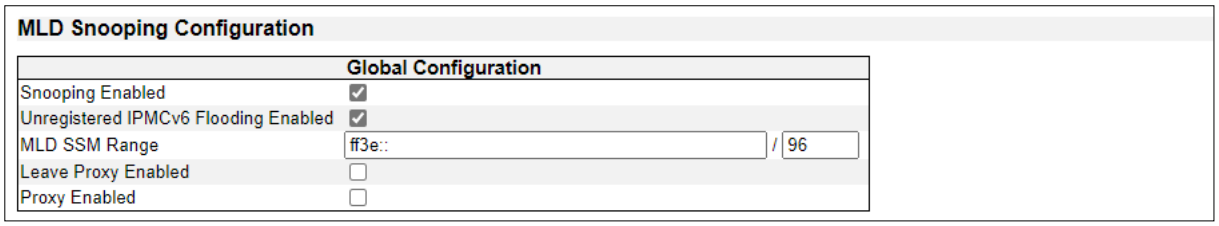
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Basic Configuration」画面

Configuration > IPMC > MLD Snooping > Basic Configuration

MLDスヌーピングについて設定します。

MLD Snooping Configuration



Global Configuration

Snooping Enabled ……　システム全体でMLDスヌーピングを有効にするかを設定します。

Unregistered IPMCv6 Flooding Enabled
……　未登録のIPMCv6トラフィックをVLAN内にフラッディングするかどうかを設定します。
フラッディング制御は、MLDスヌーピング使用時に有効な機能です。
MLDスヌーピングが無効になっている場合、設定に関わらず未登録のIPMCv6トラフィックは常にフラッディングされます。

MLD SSM Range……　SSM(Source-Specific Multicast)で使用するアドレス範囲を、IPv6マルチキャストアドレスとプレフィックス長(8～128)で設定します。
SSM対応のホストとルーターは、アドレス範囲内のグループに対してSSMサービスを実行します。

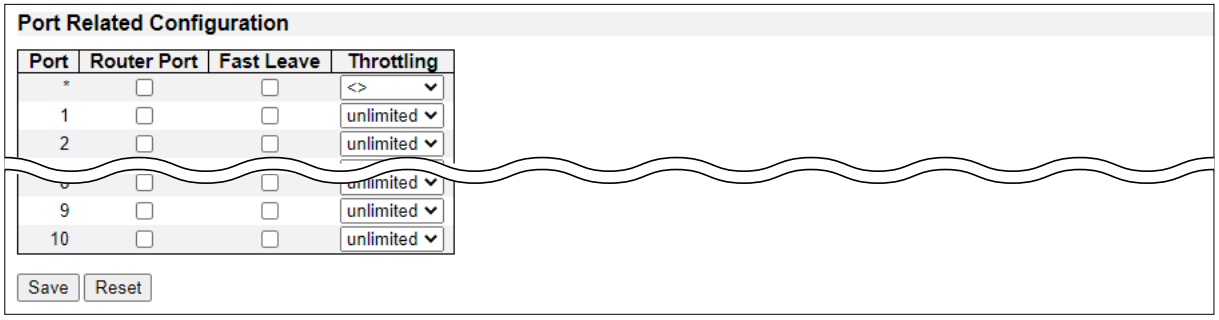
Leave Proxy Enabled……　MLD Leaveプロキシーを使用するかどうかを設定します。
MLD Leaveプロキシーを使用すると、不要なleaveメッセージをルーター側に転送しないようにできます。

Proxy Enabled ……　MLDプロキシーを使用するかどうかを設定します。
MLDプロキシーを使用すると、不要なjoinメッセージやleaveメッセージをルーター側に転送しないようにできます。

「Basic Configuration」画面

Configuration > IPMC > MLD Snooping > Basic Configuration

Port Related Configuration



Port …… 本製品のポート番号が表示されます。

Router Port …… ルーターポートとして機能するポートを指定します。
ルーターポートは、レイヤー3 マルチキャストデバイス、またはMLDクエリアが接続されているポートです。
アグリゲーションメンバーのポートがルーターポートとして選択されている場合、アグリゲーション全体がルーターポートとして機能します。

Fast Leave …… ファストリーブ機能を使用するかどうかを設定します。
ファストリーブ機能を使用すると、ホストからのMLDv1 leaveメッセージを受信したときに、メンバーシップQueryメッセージを送信することなくグループからホストを削除し、データの転送を停止します。
※MLDv1ホストがポートに複数接続されている場合は、無効にすることをおすすめします。

Throttling …… 所属するマルチキャストグループの上限を設定します。

〈Save〉 …… 設定した内容を保存するボタンです。

〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

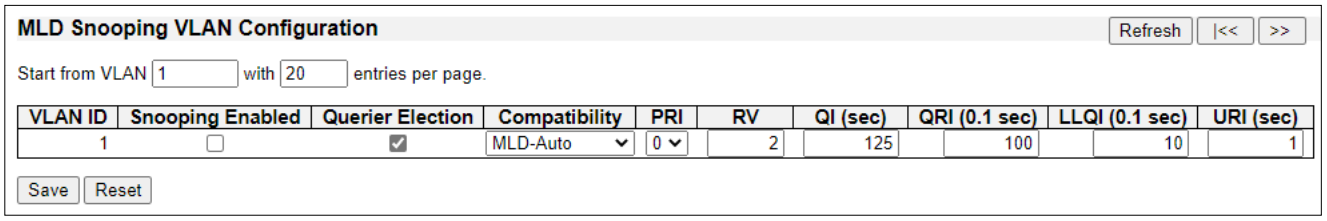
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「VLAN Configuration」画面

Configuration > IPMC > MLD Snooping > VLAN Configuration

IGMPスヌーピングのVLANインターフェースについて設定します。
※IGMPスヌーピングのVLANインターフェースを作成する前に、「Configuration」→「System」→「IP」画面でIPインターフェースを設定してください。

MLD Snooping VLAN Configuration



〈Refresh〉 …… 最新の状態に更新するボタンです。
※設定内容を変更したときは、変更前の状態に戻ります。

〈|<<〉…… 最初のページに戻るボタンです。

〈>>〉 …… 次のページに進むボタンです。

Start from VLAN [VLAN ID] with [表示数] entries per page.
…… ページ表示の設定です。
VLANテーブルのうち、VLAN IDの一番小さいエントリがはじめに表示されます。
[VLAN ID]欄で、VLANテーブルの開始VLAN IDを指定できます。
[表示数]欄で1ページあたりの表示数を指定できます。(最大99件)

VLAN ID …… VLAN IDが表示されます。

Snooping Enabled …… MLDスヌーピングを有効にするかどうかを設定します。
VLANは最大8個まで使用できます。

Querier Election …… クエリア選定の対象とするかどうかを設定します。
VLAN内で最も小さいIPアドレスの装置がクエリアとして選定され、クエリアになった装置がQueryメッセージを送信します。
無効にすると、クエリアとして動作しません。

Compatibility…… MLDのバージョンを「MLD-Auto」、「Forced MLDv1」、「Forced MLDv2」から選択します。
ネットワーク内にあるそれぞれのホストとルーターで動作しているMLDバージョンに応じて適切に運用することで、互換性が保証されます。

「VLAN Configuration」画面

Configuration > IPMC > MLD Snooping > VLAN Configuration

MLD Snooping VLAN Configuration

PRI …… MLD制御フレームの優先度を選択します。
設定できる範囲は、「0」(ベストエフォート)～「7」(優先度高)です。

RV …… RV(Robustness Variable)を設定します。
RVは、ネットワーク上で予想されるパケット損失を調整するためのパラメーターです。
設定できる範囲は、「1～255」です。

QI (sec) …… QI(Query Interval)を設定します。
QIは、クエリアがQueryメッセージを送信する間隔です。
設定できる範囲は、「1～31744」(秒)です。

QRI (0.1 sec) …… QRI(Query Response Interval)を設定します。
QRIは、MLD General Queryメッセージに対する最大応答待機時間です。
設定できる範囲は、「0～31744」(×0.1秒)です。

LLQI (0.1 sec) …… LLQI(Last Listener Query Interval)を設定します。
LLQIは、Multicast Address Specific、またはMulticast Address and Source Specific Queryメッセージへの応答を待機する時間です。
スイッチはVersion 1 Multicast Listener Doneメッセージを受信したときに、ホストがグループを離れたか確認するためQueryメッセージを送信します。
設定できる範囲は、「0～31744」(×0.1秒)です。

URI (sec) …… URI(Unsolicited Report Interval)を設定します。
URIは、ホストがグループのメンバーであることを通知するために送信するunsolicited MLD reportの送信間隔です。
設定できる範囲は、「0～31744」(秒)です。

〈Save〉 …… 設定した内容を保存するボタンです。

〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

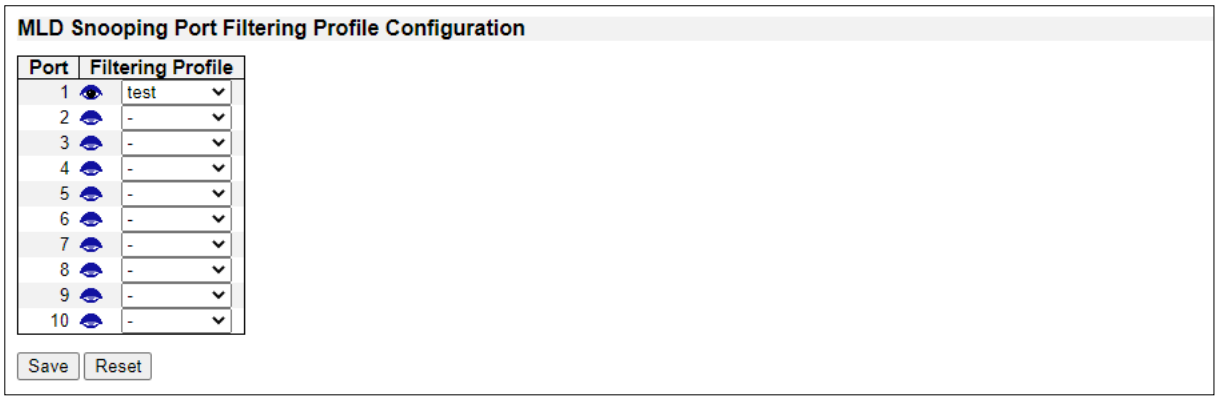
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Port Filtering Profile」画面

Configuration > IPMC > MLD Snooping > Port Filtering Profile

MLDスヌーピングのポートフィルターについて設定します。

MLD Snooping Port Filtering Profile Configuration



Port …… 本製品のポート番号が表示されます。

…… [Filtering Profile]欄で選択したプロファイルの、ルール一覧を表示するボタンです。

Filtering Profile…… IPMCプロファイルテーブルからフィルタリング条件を選択します。
※IPMCプロファイルテーブルは「Configuration」→「IPMC Profile」→「Profile Table」画面で設定します。

〈Save〉 …… 設定した内容を保存するボタンです。

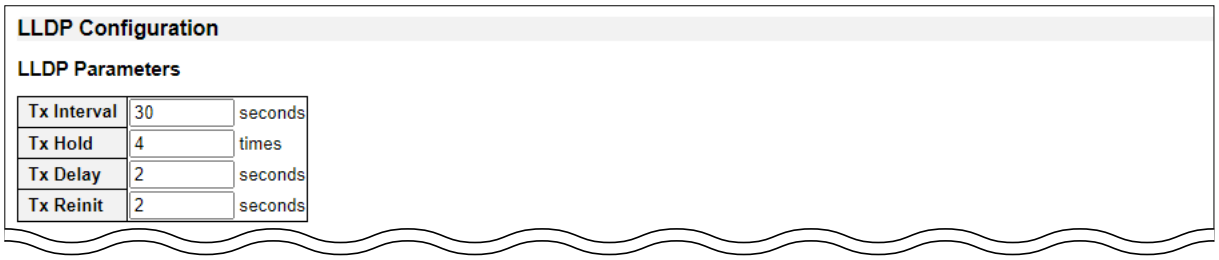
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「LLDP」画面

Configuration > LLDP > LLDP

LLDPインターフェースについて設定します。

LLDP Configuration



LLDP Parameters

Tx Interval ……

LLDPフレームの送信間隔を設定します。
設定できる範囲は、「5～32768」(秒)です。
LLDPフレームを定期的に隣接しているデバイス(ネイバー)に送信することで、ネットワークの探索情報を最新の状態にします。

Tx Hold……

LLDP情報の有効期間の乗数を設定します。
各LLDPフレームには、LLDPフレーム内の情報を有効とする期間に関するフィールドが含まれています。
LLDP情報の有効期間は、[Tx Interval]×[Tx Hold](秒)です。
設定できる範囲は、「2～10」(回)です。

Tx Delay ……

IPアドレスなどの設定が変更されてからLLDPフレームを送信するまでの時間を設定します。
設定できる範囲は、「1～8192」(秒)です。
※[Tx Interval]の1/4以下に設定してください。

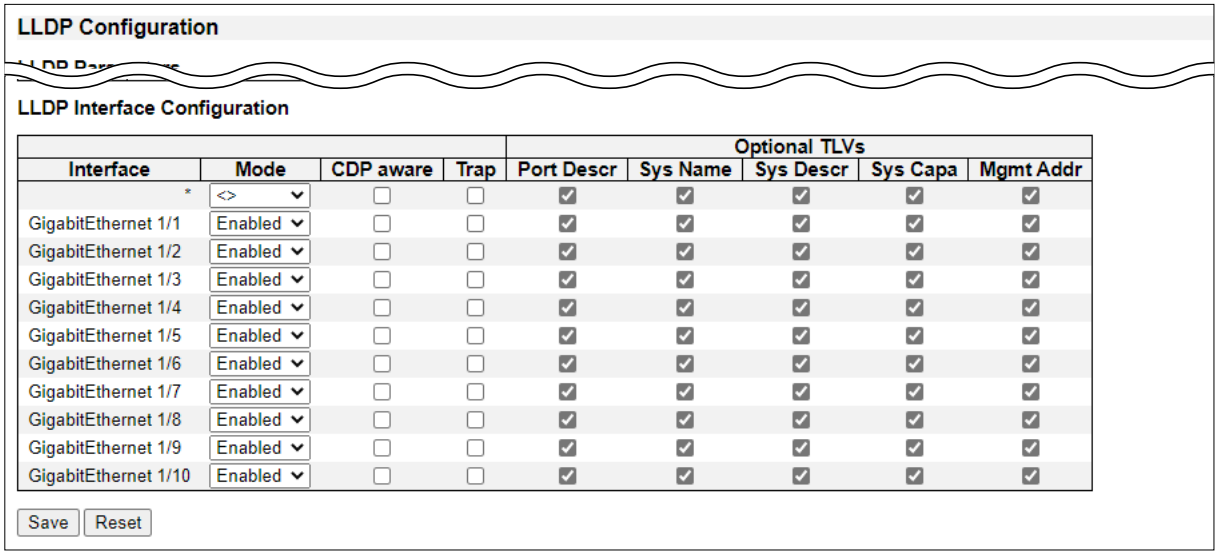
Tx Reinit ……

インターフェースやLLDP機能が無効になったり、本製品が再起動したりしたときに、LLDP shutdownフレームをネイバーに送信してから、LLDPを初期化するまでの時間を設定します。
shutdownフレームは、LLDP情報が無効になったことを通知するためのフレームです。
設定できる範囲は、「1～10」(秒)です。

「LLDP」画面

Configuration > LLDP > LLDP

LLDP Configuration



LLDP Configuration

LLDP Interface Configuration

Interface	Mode	CDP aware	Trap	Optional TLVs				
				Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/1	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/2	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/3	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/4	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/5	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/6	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/7	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/8	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/9	Enabled	☐	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/10	Enabled	☐	☐	☑	☑	☑	☑	☑

Save Reset

LLDP Interface Configuration

Interface …… 本製品のインターフェース名が表示されます。

Mode …… LLDPのモードを選択します。

Disabled：
LLDP情報を送信せず、ネイバーからのLLDP情報を破棄します。

Enabled：
LLDP情報を送信し、ネイバーからのLLDP情報を収集します。

Rx only：
LLDP情報を送信しませんが、ネイバーからのLLDP情報は収集します。

Tx only：
LLDP情報を送信しますが、ネイバーからのLLDP情報は破棄します。

「LLDP」画面

Configuration > LLDP > LLDP

LLDP Configuration

CDP aware……

CDPに対応するかどうかを選択します。
有効にしたとき、受信したCDPフレームをデコードします。
※CDPフレームの送信には対応していません。
※CDPフレームはインターフェースのLLDPが有効な場合だけデコードされます。
※すべてのインターフェースで[CDP Aware]が無効になっている場合、ネイバーから受信したCDPフレームをほかのデバイスに転送します。
1つ以上のインターフェースで[CDP Aware]が有効になっている場合、CDPフレームを転送しません。
※インターフェースの[CDP Aware]が無効になっている場合、CDP情報はすぐには破棄されませんが、保持時間を超えると破棄されます。

LLDPネイバーテーブルに記録できるCDP TLVだけがデコードされ、ほかのTLVはすべて破棄されます。
認識されないCDP TLVや破棄されたCDPフレームは、LLDP統計には表示されません。
CDP TLV情報は、下記のとおり「Monitor」→「LLDP」→「Neighbors」画面に記録されます。
◎CDP TLV Device IDは、[Chassis ID]欄に記録されます。
◎CDP TLV Addressは、[Management Address]欄に記録されます。
CDP TLV Addressは複数のアドレスを含む場合がありますが、[Management Address]欄には最初のアドレスだけが表示されます。
◎CDP TLV Port IDは、[Port ID]欄に記録されます。
◎CDP TLV Version and Platformは、[System Capabilities]欄に記録されます。
CDPとLLDPはどちらも「system capabilities」に対応していますが、CDPではサポートしていて、LLDPではサポートしていない機能は、[System Capabilities]欄に「others」と表示されます。

Trap …… LLDPで収集した情報に変更があったときに、SNMPトラップで通知するかどうかを設定します。

Port Descr …… 送信するLLDP情報にport descriptionを含めるとき、ボックスにチェックマークを入れます。

Sys Name …… 送信するLLDP情報にsystem nameを含めるとき、ボックスにチェックマークを入れます。

Sys Descr …… 送信するLLDP情報にsystem descriptionを含めるとき、ボックスにチェックマークを入れます。

Sys Capa …… 送信するLLDP情報にsystem capabilityを含めるとき、ボックスにチェックマークを入れます。

Mgmt Addr…… 送信するLLDP情報にmanagement addressを含めるとき、ボックスにチェックマークを入れます。

〈Save〉 …… 設定した内容を保存するボタンです。

〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「LLDP-MED」画面

Configuration > LLDP > LLDP-MED

LLDP-MEDについて設定します。
※LLDP-MEDに対応したVoIPデバイスに適用されます。

LLDP-MED Configuration

Fast Start Repeat Count

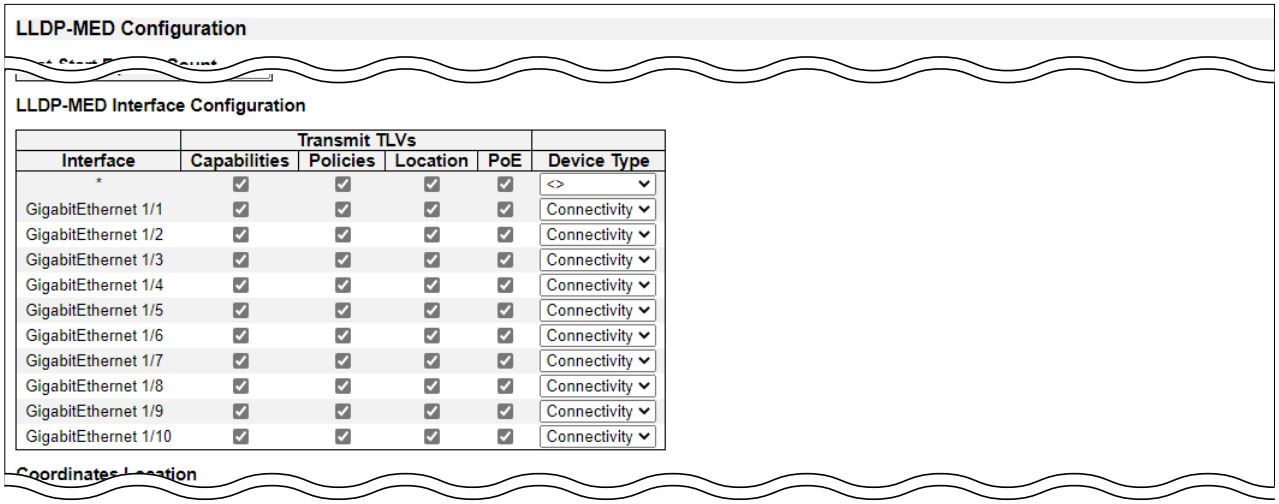
Fast start repeat count ……

エンドポイントデバイスの迅速な起動と緊急通話サービスでのロケーション情報の検出は、VoIPシステム全般の重要な要素です。
さらに、LLDPパケットデータユニット(LLDPU)のスペースを節約し、不適切なネットワークポリシーによって発生するセキュリティーとシステムの整合性の問題を軽減するために、特定のエンドポイントタイプに関連する情報だけをアドバタイズすることをおすすめします。(たとえば、音声通話を許可されたデバイスだけに音声ネットワークポリシーをアドバタイズします。)
これらの関連プロパティを達成するために、LLDP-MEDにはプロトコルとプロトコル上のアプリケーション層との間のLLDP-MED fast start処理機能が実装されています。
はじめに、ネットワーク接続デバイスは、LLDPDU内のLLDP TLVだけを送信します。
LLDP-MED対応のエンドポイントデバイスが検出されると、LLDP-MED対応機器はLLDP-MED TLVが付加されたLLDPDUの送信を開始します。
新しいLLDP-MEDネイバーが検出されると、LLDP-MED情報を新しいネイバーにできるだけ早く共有するためにLLDP-MED fast start処理を開始し、一時的にLLDPDUを1秒間隔で送信します。
LLDP-MED fast startによる送信を複数回繰り返すことで、ネイバー間伝送中のLLDPフレームのロストを防ぎ、ネイバーがLLDPフレームを受信する可能性が高くなります。
[Fast start repeat count]欄では、LLDP-MED fast startによる送信回数を設定します。
新しい情報を含むLLDPフレームを受信したとき、設定した回数だけLLDPフレームを1秒間隔で送信します。
LLDP-MEDやLLDP-MED fast startメカニズムは、LLDP-MEDネットワーク接続デバイスとエンドポイントデバイス間のリンクでだけ実行され、ネットワーク接続デバイスを含むLANインフラストラクチャ間のリンク、またはその他の種類のリンクには適用されません。

「LLDP-MED」画面

Configuration > LLDP > LLDP-MED

LLDP-MED Configuration


LLDP-MED Configuration

LLDP-MED Interface Configuration

Interface	Transmit TLVs				Device Type
	Capabilities	Policies	Location	PoE	
*	☑	☑	☑	☑	<>
GigabitEthernet 1/1	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/2	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/3	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/4	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/5	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/6	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/7	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/8	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/9	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/10	☑	☑	☑	☑	Connectivity

Coordinates Location

LLDP-MED Interface Configuration

Interface …… 本製品のインターフェース名が表示されます。

Transmit TLVs Capabilities … 送信するLLDP-MED情報にCapabilities TLVを含めるとき、ボックスにチェックマークを入れます。

Transmit TLVs Policies …… 送信するLLDP-MED情報にnetwork-policy TVLを含めるとき、ボックスにチェックマークを入れます。

Transmit TLVs Location …… 送信するLLDP-MED情報にlocation TVLを含めるとき、ボックスにチェックマークを入れます。

Transmit TLVs PoE …… 送信するLLDP-MED情報にExtended Power-via-MDI TLV(PoE情報)を含めるとき、ボックスにチェックマークを入れます。

「LLDP-MED」画面

Configuration > LLDP > LLDP-MED

LLDP-MED Configuration

Device Type ……

デバイスの種類を選択します。
LLDP-MEDデバイスの種類は、下記で定義されたネットワーク接続デバイス、または特定のクラスのエンドポイントデバイスに分類されます。

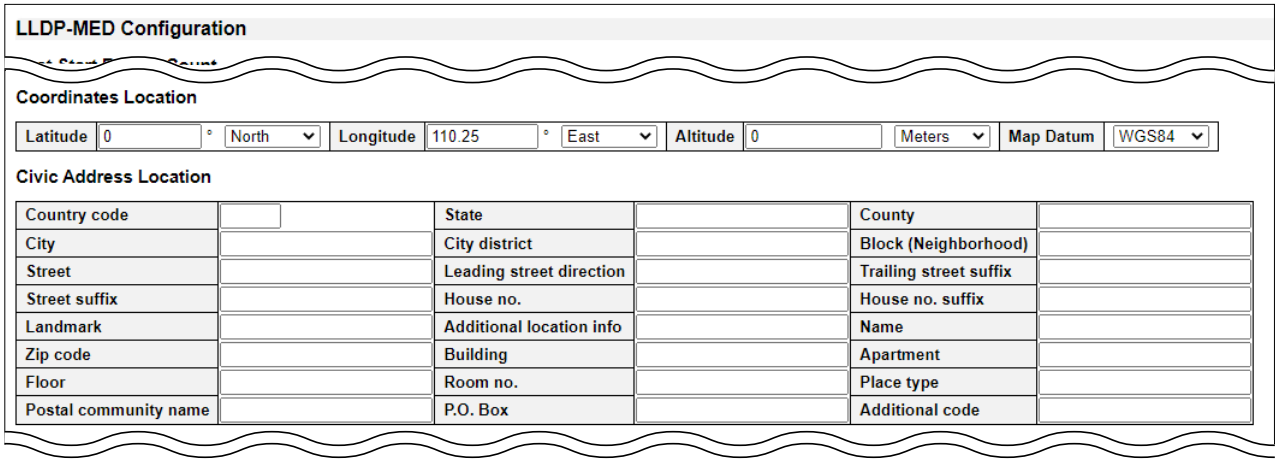
Connectivity：
ネットワーク接続デバイスとして動作します。
ネットワーク接続デバイスは、LLDP-MEDエンドポイントデバイスにIEEE 802ベース LANインフラストラクチャへのアクセスを提供するLLDP-MEDデバイスです。
LLDP-MEDネットワーク接続デバイスは、次のどれかのテクノロジーに基づくLANアクセスデバイスです。
1. LAN スイッチ/ルーター
2. IEEE 802.1 ブリッジ
3. IEEE 802.3 レピータ（歴史的な理由から含まれています。）
4. IEEE 802.11 ワイヤレスアクセスポイント
5. IEEE 802.1ABとMED拡張機能に対応し、任意の方法でIEEE 802フレームを中継できるデバイス。

End-point：
エンドポイントデバイスとして動作します。
エンドポイントデバイスはネットワークの終端に位置し、IEEE 802 LANテクノロジーベースのIP通信サービスを提供するLLDP-MEDデバイスです。
※LLDP-MED情報の交換を開始できるのは、エンドポイントデバイスだけです。スイッチは常にネットワーク接続デバイスである必要がありますが、2台のネットワーク接続デバイスが同時に接続されている場合、エンドポイントデバイスとして機能するように設定すると、LLDP-MED情報の交換を開始できます。

「LLDP-MED」画面

Configuration > LLDP > LLDP-MED

LLDP-MED Configuration



Coordinates Location

Latitude ……

緯度を設定し、「North」(北緯)か「South」(南緯)を選択します。
設定できる範囲は、「0.0000～90.0000」(度)です。

Longitude ……

経度を設定し、「East」(東経)か「West」(西経)を選択します。
設定できる範囲は、「0.0000～180.0000」(度)です。

Altitude ……

高度を設定します。
設定できる範囲は、「-2097151.9～2097151.9」です。
高度の種類を下記から選択できます。

Meters：
[Map Datum]欄で指定した測地系で定義された高度をメートル単位で設定します。

Floors：
建物の階数を設定します。
建物の外では、指定された緯度と経度の地点が0.0(グラウンドレベル)になります。
建物内では、メインエントランスが0.0になります。

Map Datum……

測地系を選択します。

WGS84(Geographical 3D)：
世界測地系1984、CRSコード4327、グリニッジ子午線を使用します。

NAD83/NAVD88：
North American datums(北米測地基準系) 1983、CRS コード 4269、グリニッジ子午線を使用します。
鉛直基準面は、North American Vertical Datum of 1988(NAVD88)を使用します。
※潮汐(ちょうせき)水域から離れた、陸上の位置を参照するときに使用します。

NAD83/MLLW：
North American datums(北米測地基準系) 1983、CRS コード 4269、グリニッジ子午線を使用します。
鉛直基準面は、平均低低潮面(MLLW：Mean Lower Low Water)です。
※海水面上の位置を参照するときに使用します。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「LLDP-MED」画面

Configuration > LLDP > LLDP-MED

LLDP-MED Configuration

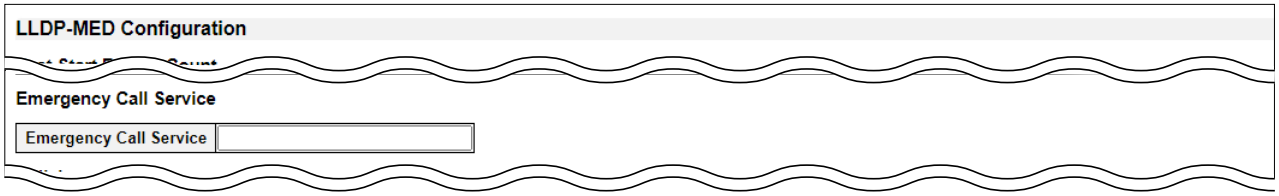
Civic Address Location
IETF Geopriv Civic Address based Location Configuration Information(Civic Address LCI)を設定します。
すべての住所情報の合計文字数が、250文字以内になるように設定してください。
※2文字の国名コードは、250文字の制限には含まれません。

Country code	ISO 3166で定義された2文字の国名コードをASCII文字(大文字)で指定します。(例: JP、USなど)
State	国の下位区分(都道府県、州、地域など)を入力します。
County	郡、教区、地区を入力します。
City	市を入力します。(例：Copenhagen)
City district	区町村を入力します。
Block (Neighborhood)	区画を設定します。
Street	通りの名前を入力します。(例：Poppelvej)
Leading street direction	通りの方角を入力します。(例：N)
Trailing street suffix	通りのサフィックスを入力します。(例：SW)
Street suffix	通りのサフィックス(種類)を入力します。(例：Ave.、Platz)
House no.	番地を入力します。(例：21)
House no. suffix	番地のサフィックスを入力します。(例：A、1/2)
Landmark	ランドマークの名前を入力します。(例：Columbia University)
Additional location info	その他の位置情報を入力します。(例：South Wing)
Name	居住者の名前を入力します。(例：Flemming Jahn)
Zip code	郵便番号を入力します。(例：2791)
Building	建物の構造を入力します。(例：Low Library)
Apartment	部屋の種類(Apartment、Suite)を入力します。(例：Apt. 42)
Floor	階数を入力します。(例：4)
Room no.	部屋番号を入力します。(例：450F)
Place type	場所の種類を入力します。(例：Office)
Postal community name	郵便コミュニティ名を入力します。(例：Leonia)
P.O. Box	私書箱を入力します。(例：12345)
Additional code	追加コードを入力します。(例：1320300003)

「LLDP-MED」画面

Configuration > LLDP > LLDP-MED

LLDP-MED Configuration



Emergency Call Service

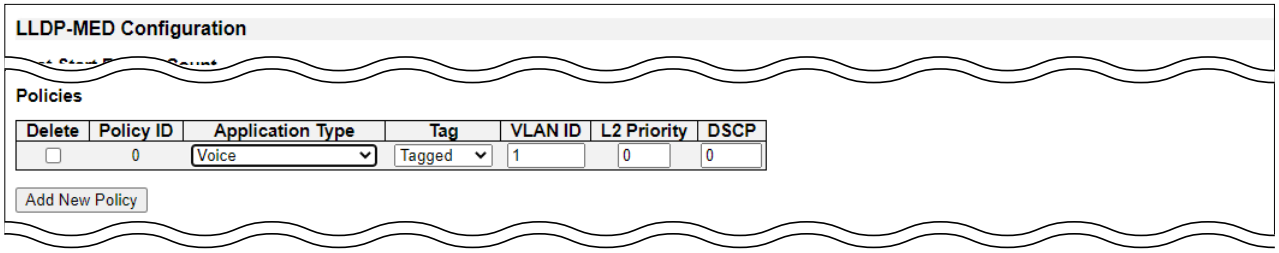
Emergency Call Service ……

TIAやNERAなどで定義されている緊急通報サービス(110/119/118など)に使用するELIN(Emergency Location Identification Number)の数値を設定します。
緊急通報サービスのELIN IDのデータフォーマットは、緊急通報時に使用されるELIN IDを従来のCAMA、またはISDNトランクベースのPSAPに伝送するように定義されています。

「LLDP-MED」画面

Configuration > LLDP > LLDP-MED

LLDP-MED Configuration



Policies

Network Policy Discoveryを使用すると、ポート上の特定のプロトコルアプリケーションセットに適用されるレイヤー2/レイヤー3設定とVLAN設定との不一致の問題を、効率的に検出、診断できます。
不適切なネットワークポリシー設定は、VoIP環境では音声品質の低下やサービスの損失を頻繁に招く可能性があります。

ポリシーは、対話型音声サービスやビデオサービスなど、特定のリアルタイムなネットワークポリシー要件を持つアプリケーションだけに使用することを想定しています。
以下のネットワークポリシー属性がアドバタイズされます。
1. Layer 2 VLAN ID (IEEE 802.1Q-2003)
2. Layer 2 priority値 (IEEE 802.1D-2004)
3. Layer 3 DSCP(Diffserv code point)値 (IETF RFC 2474)

ネットワークポリシーは、指定されたポートでサポートされている複数のアプリケーションタイプと関連付けてアドバタイズできます。
以下のアプリケーションタイプが定義されています。
1. Voice
2. Guest Voice
3. Softphone Voice
4. Video Conferencing
5. Streaming Video
6. Control/Signalling(1～5のメディアタイプに対して、個別のネットワークポリシーを条件付きでサポートする)

大規模なネットワークでは、組織全体で複数のVoIPポリシーをサポートし、アプリケーションタイプごとに異なるポリシーをサポートする場合があります。
LLDP-MEDでは、異なるアプリケーションタイプに対応した複数のポリシーを、ポートごとにアドバタイズできます。
同じネットワーク接続デバイス上の異なるポートは、認証されたユーザーIDやポート設定に基づいて、異なるポリシーをアドバタイズする場合があります。

LLDP-MEDは、ネットワーク接続デバイスとエンドポイントデバイス間以外のリンクで動作することを想定していないため、LANへのアグリゲーションリンク内で使用される複数のネットワークポリシーのアドバタイズは不要です。

Delete …… 登録された内容を削除するとき、ボックスにチェックマークを入れます。

Policy ID …… ポリシーIDが表示されます。
ポリシーIDは0から順に自動で割り振られます。

「LLDP-MED」画面

Configuration > LLDP > LLDP-MED

LLDP-MED Configuration

Application Type ……

アプリケーションタイプを選択します。

1. Voice：
専用のIP電話端末や対話型音声サービスに対応した類似機器に使用します。
これらのデバイスは、切り離されたVLAN上に設置しデータアプリケーションと分離することで、設置を簡単にし、セキュリティーを強化します。

2. Voice Signalling (conditional)：
ボイスメディアとは異なるボイスシグナリング用のポリシーを必要とするネットワークトポロジーに使用します。
「Voice」アプリケーションポリシーでアドバタイズされているネットワークポリシーをすべて適用する場合は、「Voice Signalling」タイプをアドバタイズしないでください。

3. Guest Voice：
独自のIP電話装置や対話型音声サービスに対応した類似機器を使用して、ゲストユーザーやビジター向けに機能が制限された音声サービスをサポートします。

4. Guest Voice Signalling (conditional)：
ゲストボイスメディアとは異なるゲストボイスシグナリング用のポリシーを必要とするネットワークトポロジーに使用します。
「Guest Voice」アプリケーションポリシーでアドバタイズされているネットワークポリシーをすべて適用する場合は、「Guest Voice Signalling」タイプをアドバタイズしないでください。

5. Softphone Voice：
デスクトップパソコンやノートパソコンなど、一般的なデータ処理用デバイス上のソフトフォンアプリケーションに使用します。
このクラスのエンドポイントの多くは、マルチプルVLANをサポートしていません。マルチプルVLANを一切サポートしていない場合、タグなしVLAN、または1つのタグ付きdata specific VLAN を使用するように設定します。
[Tag]欄で、ネットワークポリシーがタグなし(untagged)VLANを使用するように設定した場合、L2 Priority値は無視され、DSCP値だけが考慮されます。

6. Video Conferencing：
ビデオ会議専用の機器や、リアルタイムのインタラクティブビデオ/オーディオサービスに対応した類似機器で使用します。

7. Streaming Video：
ブロードキャストやマルチキャストでのビデオコンテンツ配信、および特定のネットワークポリシー処理を必要とするストリーミングビデオサービスに対応した類似のアプリケーションで使用します。
バッファリングでTCPに依存するビデオアプリケーションでの使用は想定していません。

8. Video Signalling (conditional)：
ビデオメディアと異なるビデオシグナリング用のポリシーを必要とするネットワークトポロジーに使用します。
「Video Conferencing」アプリケーションポリシーでアドバタイズされているネットワークポリシーをすべて適用する場合は、「Video Signalling」タイプをアドバタイズしないでください。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「LLDP-MED」画面

Configuration > LLDP > LLDP-MED

LLDP-MED Configuration

Tag…… 指定したアプリケーションタイプが使用するVLANを、タグ付き(tagged)かタグなし(untagged)から選択します。

Untagged：
タグなしフレーム形式を使用しているため、IEEE 802.1Q-2003で定義されているタグヘッダーは含まれません。
タグなしの場合、VLAN IDとL2 priority値は無視され、DSCP値だけが考慮されます。

Tagged：
IEEE 802.1Q タグ付きフレーム形式を使用し、VLAN IDとL2 priority値、DSCP値が使用されます。
タグ付きの場合は、タグヘッダーと呼ばれる追加のフィールドが含まれています。
また、IEEE 802.1Q-2003 で定義されているPriority taggedフレームも含まれます。

VLAN ID …… IEEE 802.1Q-2003で定義されている、インターフェースのVLAN ID(VID)を設定します。

L2 Priority …… IEEE 802.1D-2004で定義されている、Layer 2 Priority値を設定します。
設定できる範囲は、「0～7」です。
「0」に設定したときは、IEEE 802.1D-2004 で定義されている既定の優先度を使用します。

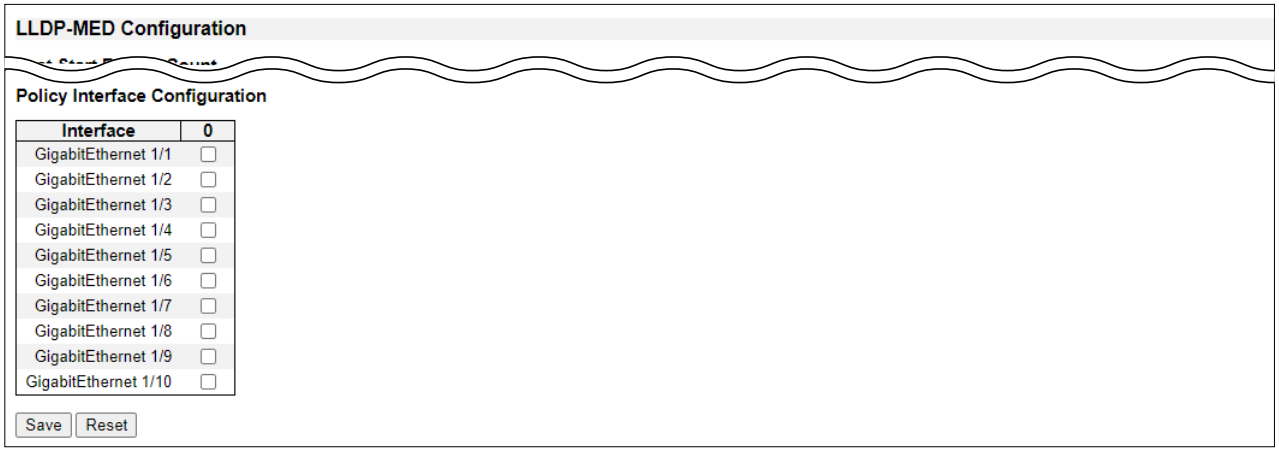
DSCP …… IETF RFC 2474で定義されている、Diffserv使用時の DSCP値を設定します。
設定できる範囲は、「0～63」です。
「0」に設定したときは、RFC 2475で定義されているデフォルトのDSCP値を使用します。

〈Add New Policy〉 …… クリックして新しいポリシーを追加します。
※最大32件まで登録できます。

「LLDP-MED」画面

Configuration > LLDP > LLDP-MED

LLDP-MED Configuration



Policy Interface Configuration

認証されたユーザーIDやインターフェース設定に基づいて、一意のネットワークポリシー、または同じネットワークポリシーセットの異なる属性を、インターフェースにアドバタイズできます。

Interface …… 本製品のインターフェース名が表示されます。

Policy ID …… 設定したポリシーのポリシーIDが表示されます。
インターフェースにポリシーを適用するとき、ボックスにチェックマークを入れます。

〈Save〉 …… 設定した内容を保存するボタンです。

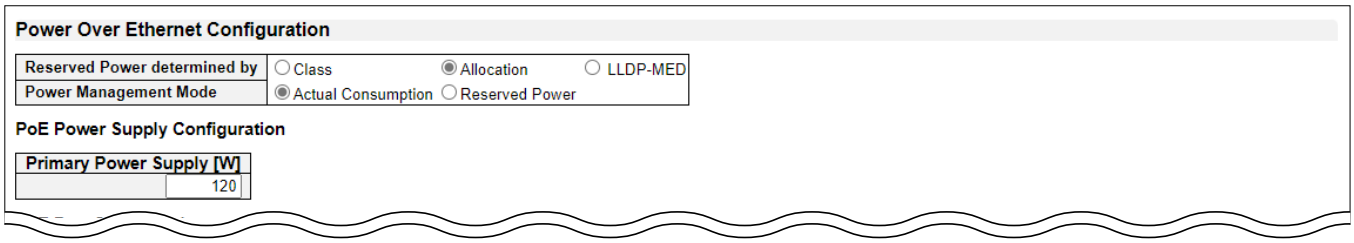
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「PoE」画面

Configuration > PoE > PoE

PoEについて設定します。

Power Over Ethernet Configuration



Reserved Power determined by …

ポートからPD(受電機器)への供給電力量を決める方法を設定します。
※すべてのモードで、ポートに供給された電力よりも多くの電力を使用した場合、ポートはシャットダウンされます。

Allocated mode：
ポートごとに、供給する最大電力量を割り当てます。
各ポート/PDの最大供給電力は、[Maximum Power [W]]欄で設定します。

Class mode：
ポートに接続されたPDの電力クラスに応じて、供給する電力量を自動で決定します。
4つの電力クラスが存在し、それぞれの供給電力は4、7、15.4、30Wです。
※[Maximum Power [W]]欄の設定は無効になります。

LLDP-MED mode：
LLDPプロトコルを使用してPoE情報を交換し、供給する電力量を決定します。
LLDP情報が使用できない場合、クラスモードを使用して供給する電力量を決定します。
※[Maximum Power [W]]欄の設定は無効になります。

Power Management Mode ……

ポートをシャットダウンするタイミングを設定します。

Actual Consumption：
すべてのポートの電力消費量が電源装置が供給できる電力量を超えた場合、または特定のポートの電力消費量がそのポートで決められた電力量を超えた場合、ポートをシャットダウンします。
[Priority]欄で設定した優先度の順でポートをシャットダウンします。
2つのポートの優先度が同じ場合、ポート番号が大きいポートをシャットダウンします。

Reserved Power：
各ポートの供給電力の合計が、電源装置が供給できる電力量を超えると、ポートをシャットダウンします。
PDが電源装置から供給できる電力以上の電力を要求した場合、ポートはシャットダウン状態になります。

PoE Power Supply Configuration

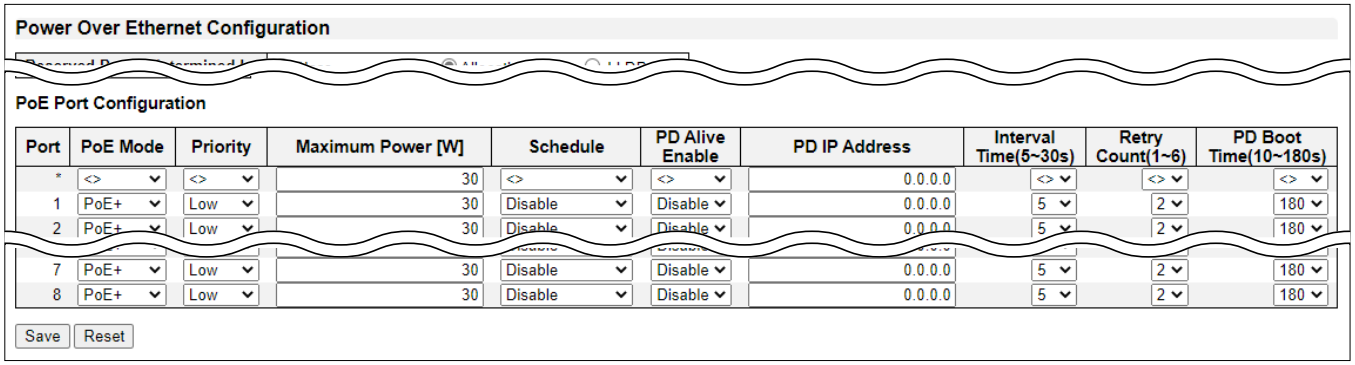
Primary Power Supply [W] ……

PDが使用できる電力量を決めるために、電源装置から供給する電力量を設定します。
設定できる範囲は、「1～120」(W)です。

「PoE」画面

Configuration > PoE > PoE

Power Over Ethernet Configuration



PoE Port Configuration

Port …… 本製品のポート番号が表示されます。

PoE Mode …… PoEの動作モードを選択します。

Disabled：
PoEは無効です。

PoE：
PoE(IEEE 802.3af)を使用します。
電力クラス4のPDへの供給は、15.4Wに制限されます。

PoE+：
PoE+(IEEE 802.3at)を使用します。
電力クラス4のPDへの供給は、30Wに制限されます。

Priority …… ポートの優先度を、「Low」、「High」、「Critical」から選択します。
リモートデバイスが電源装置から供給する電力よりも多くの電力を必要とする場合、優先度が低いポートの中で、ポート番号が大きいポートから順にPoE給電を停止します。

Maximum Power [W] …… リモート・デバイスに供給する最大電力を設定します。
設定できる範囲は、「0～30」(W)です。

Schedule …… PoEポートからの給電を有効にする日時を、あらかじめ設定したスケジュールから選択します。
スケジュールは、「Schedule scheme」画面で設定します。

「PoE」画面

Configuration > PoE > PoE

Power Over Ethernet Configuration

PD Alive Enable ……
ポートに接続されているPDの状態を確認するために、定期的にpingを試行するかどうかを設定します。

PD IP Address ……
ポートに接続されているPDのIPアドレスを入力します。
入力されたIPアドレス宛てにpingを試行し、PDから応答がなかった場合、そのポートでPoEを無効にします。
pingを試行する間隔は、[Interval Time(5～30s)]欄で設定します。
PoEが無効になったポートは、[PD Boot Time(10～180s)]欄で設定した時間が経過後、ふたたびPoEが有効になります。

Interval Time(5～30s) ……
pingを試行する間隔を設定します。
設定できる範囲は、「5～30」(秒)です。

Retry Count(1～6) ……
pingに応答がなかったときの、再試行回数を設定します。
設定できる範囲は、「1～6」(回)です。

PD Boot Time(10～180s) ……
pingへ応答がなくPoEが無効になったPoEポートで、ふたたびPoEを有効にするまでの時間を設定します。
設定できる範囲は、「10～180」(秒)です。

〈Save〉 ……
設定した内容を保存するボタンです。

〈Reset〉 ……
設定内容を変更したとき、変更前の状態に戻すボタンです。

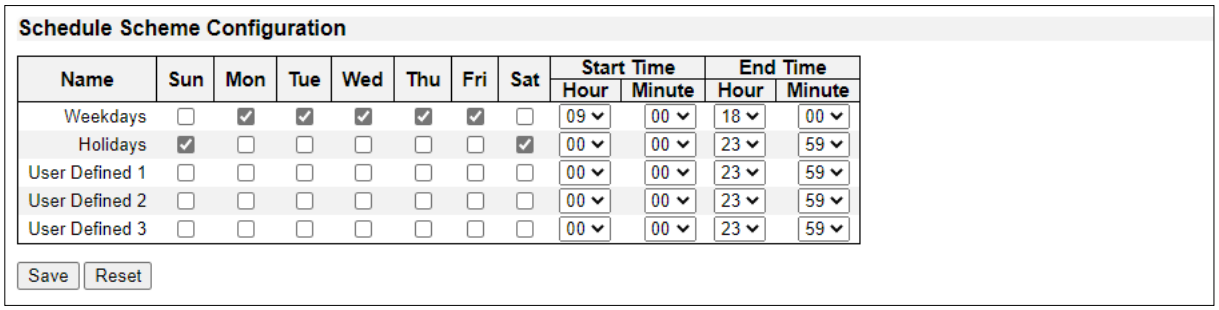
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Schedule Scheme」画面

Configuration > PoE > Schedule Scheme

PoEスケジュールについて設定します。
設定した時間に電源が供給されます。

Schedule Scheme Configuration



Name …… PoEスケジュールの名前が表示されます。
あらかじめ設定されたPoEスケジュールが2つと、ユーザー定義のPoEスケジュールが3つあります。
※すべてのPoEスケジュールは、ご使用の環境にあわせて手動で設定できます。
※PoEスケジュールを使用するには、「Configuration」→「PoE」→「PoE」画面の［Schedule］欄でPoEポートに適用するPoEスケジュールを選択してください。

Weekdays：
あらかじめ設定されたPoEスケジュールです。
初期設定は、月曜日から金曜日の午前9時から午後6時です。

Holidays：
あらかじめ設定されたPoEスケジュールです。
初期設定は、土曜日と日曜日の終日です。

User Defined 1～3：
ユーザー定義のPoEスケジュールです。

Sun/Mon/Tue/Wed/Thu/Fri/Sat … PoEポートからの給電を有効にする曜日を設定します。

Start Time/End Time…… PoEポートからの給電を有効にする時間を設定します。

〈Save〉 …… 設定した内容を保存するボタンです。

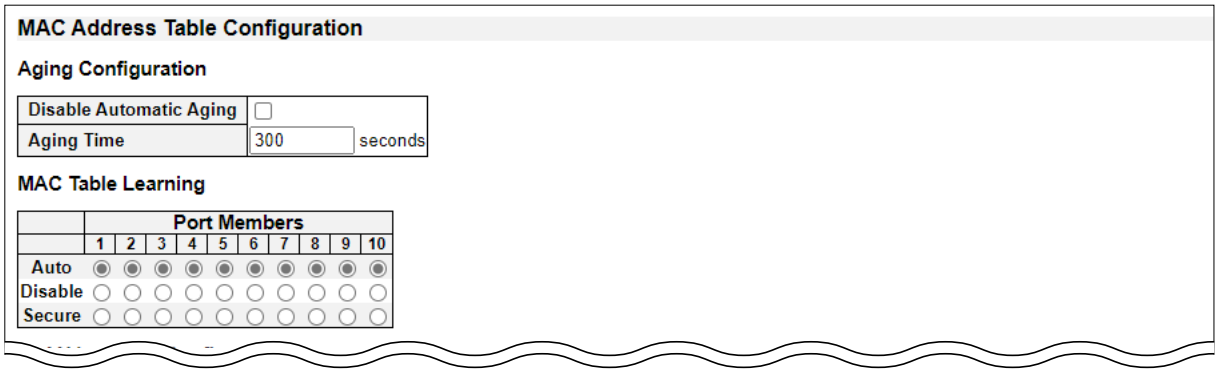
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「MAC Table」画面

Configuration > MAC Table

動的MACアドレステーブルについての設定します。
「Static MAC Table Configuration」では、静的MACアドレステーブルを設定します。
静的MACアドレステーブルには、最大64件まで登録できます。
静的MACアドレステーブルは、VLAN IDとMACアドレスでソートされます。

MAC Address Table Configuration



Aging Configuration

Disable Automatic Aging ……

MACアドレステーブルの動的エントリは、登録されてから[Aging Time]欄で設定した時間経過後、自動で削除されます。(エージング)
MACアドレステーブルの自動エージングを無効にするときに、ボックスにチェックマークを入れます。

Aging Time……

エージング時間を設定します。
設定できる範囲は、「10～1000000」(秒)です。

MAC Table Learning ……

ポートのMACアドレス学習モードを選択します。
学習モード設定がグレー表示されているポートは、802.1XのMACベース認証を使用しているなど、別の機能が学習モードを制御しているため設定を変更できません。

Auto：
不明な送信元MACアドレスを持つフレームを受信すると、自動的に学習します。

Disable：
MACアドレス学習を無効にします。

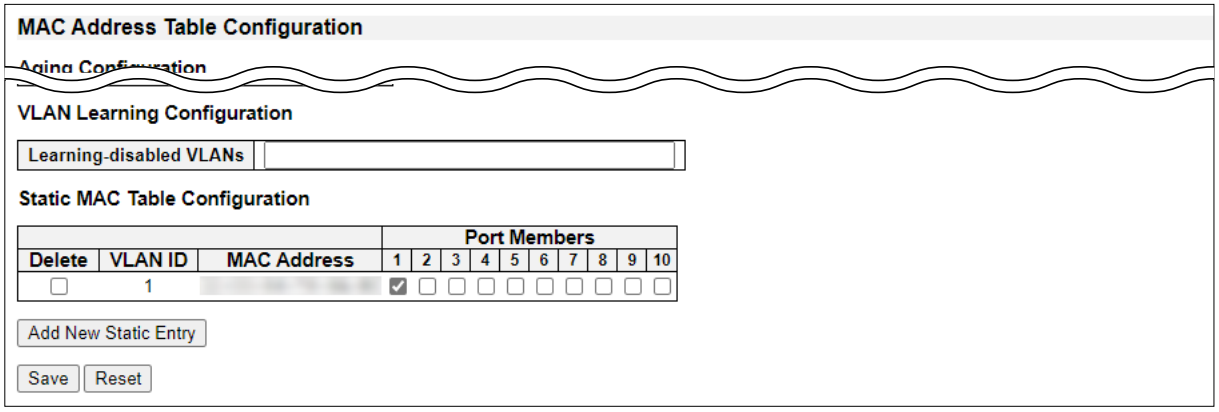
Secure：
静的MACアドレステーブルのエントリだけを学習し、ほかのすべてのフレームを破棄します。

ご注意
Secureモードに変更する前に、本製品の管理に使用しているデバイスを静的MACアドレステーブルに追加してください。
管理用デバイスを静的MACアドレステーブルに登録していないと、Secureモード以外の別のポートを使用するか、シリアルインターフェース経由でしか本製品にアクセスできなくなります。

「MAC Table」画面

Configuration > MAC Table

MAC Address Table Configuration



VLAN Learning Configuration

Learning-disabled VLANs ……

MACアドレス学習を使用しないVLANを、VLAN IDで指定します。
学習機能を無効にしているVLANで新しいMACアドレスを受信しても、MACアドレスを学習しません。
VLANは単数(xx)、または範囲(xx-yy)で指定できます。
複数指定する場合は、それぞれをコンマかスペースで区切ってください。
たとえば、「1,10-13,200,300」と入力した場合、VLAN ID 1、10、11、12、13、200、300が対象になります。

Static MAC Table Configuration

Delete ……

登録された内容を削除するとき、ボックスにチェックマークを入れます。

VLAN ID ……

VLAN IDを入力します。

MAC Address ……

MACアドレスを入力します

Port Members ……

所属するポートにチェックマークを入れます。

〈Adding a New Static Entry〉…

クリックして新しい静的MACアドレス設定を追加します。
※新しい設定を追加するときは、[VLAN ID]、[MAC address]欄を入力してから〈Save〉をクリックしてください。

〈Save〉 ……

設定した内容を保存するボタンです。

〈Reset〉 ……

設定内容を変更したとき、変更前の状態に戻すボタンです。

「VLANs」画面

Configuration > VLANs

VLANについて設定します。

Global VLAN Configuration

Global VLAN Configuration

Allowed Access VLANs	1
Ethertype for Custom S-ports	88A8

Allowed Access VLANs ……

許可VLANを設定します。
[Mode]欄で「Access」を選択したポート(アクセスポート)にだけ影響します。
それ以外のポートは、[Allowed VLANs]欄で設定したVLANのメンバーになります。
VLANは単数(xx)、または範囲(xx-yy)で指定できます。
複数指定する場合は、それぞれをコンマかスペースで区切ってください。
たとえば、「1,10-13,200,300」と入力した場合、VLAN ID 1、10、11、12、13、200、300が対象になります。

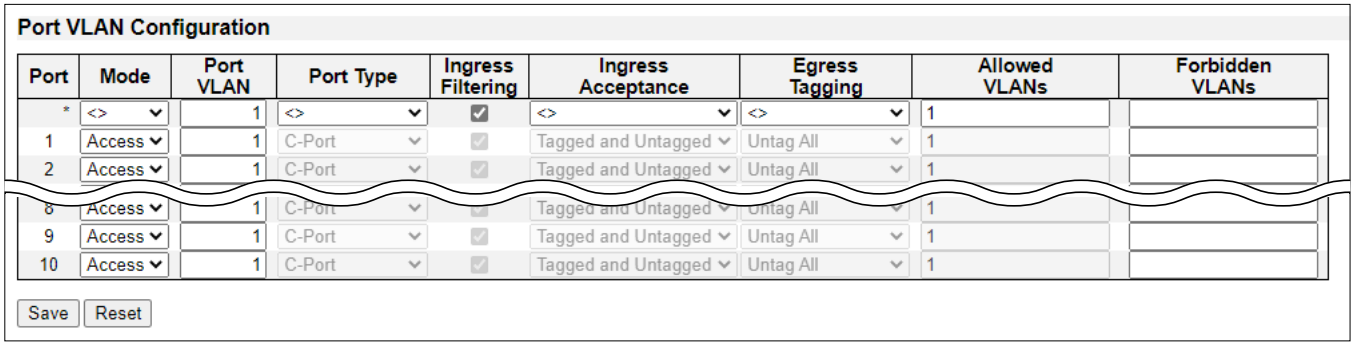
Ethertype for Custom S-ports

[Port Type]欄で「S-Custom-Port」を選択したポートに使用するethertype/TPIDを16進数で設定します。

「VLANs」画面

Configuration > VLANs

Port VLAN Configuration



Port ……　本製品のポート番号が表示されます。

Mode ……　ポートの動作を設定します。
選択したモードによって、設定できる項目が異なります。
グレー表示の項目には、選択したモードによって自動で設定された値が表示されます。

Access：
エンドステーションへの接続に使用します。
Voice VLANなどの動的機能を使用する場合、バックグラウンドでポートに収容するVLANが追加される場合があります。
アクセスポートには、次の特性があります。
◎ポートVLAN(アクセスVLAN)と呼ばれる1つのVLANを収容します。
◎タグなし(untagged)フレームとC-Tag付き(C-tagged)フレームが使用できます。
◎アクセス VLAN に分類されていないすべてのフレームを破棄します。
◎すべてのフレームをタグなしで送信します。

Trunk：
複数のVLANで同時にトラフィックを伝送できます。
通常は、他のスイッチへの接続に使用します。
トランクポートには、次の特性があります。
◎[Allowed VLANs]欄で収容するVLANを制限できます。
◎収容していないVLANに分類されたフレームは破棄します。
◎デフォルトでは、ポートVLAN(ネイティブVLAN)に分類されたフレームを除くすべてのフレームが送信時にタグ付けされます。
ポートVLANに分類されたフレームは、送信時にC-Tagでタグ付けされません。
◎送信時にタグ付けするかどうかを設定できます。
送信時にすべてのフレームにタグ付けする場合は、タグなしフレームを受信できなくなります。

Hybrid：
トランクポートの機能にポート設定を追加したモードです。
ハイブリッドポートには、トランクポートの特性に加えて次の特性があります。
◎使用するVLANタグを設定できます。
◎受信時のフィルタリングが設定できます。
◎受信できるタグの種類と送信時に使用するタグの種類を個別に設定できます。

「VLANs」画面

Configuration > VLANs

Port VLAN Configuration

Port VLAN ……

ポートVLAN ID(PVID)を設定します。
設定できる範囲は、「1～4095」です。

フレーム受信時、下記の場合は受信したフレームはポートVLANに分類されます。
◎ポートでVLANが無効に設定されている
◎タグなしフレームを受信した
◎ポートでVLANが有効になっているが、フレームに優先順位タグが付けられている(VLAN IDが0)

フレーム送信時、[Egress Tagging]欄が「untag Port VLAN」に設定されている場合、ポートVLANに分類されたフレームはタグ付けされません。

※ポートVLANは、アクセスモードのポートでは「アクセスVLAN」と呼ばれ、トランクモード、またはハイブリッドモードのポートでは「ネイティブVLAN」と呼ばれます。

Port Type ……

ハイブリッドモードのポートで、特定のVLANで受信時にVLANタグに応じてフレームを分類するかどうかと、タグを使用する場合はどのTPIDを分類するかを変更できます。
送信時は、必要に応じてタグ付けします。
タグ付けするときのTPIDはポートタイプによって異なります。

Unaware：
◎受信時に、すべてのフレームをポートVLANに分類します。
◎送信時にタグを削除しません。

C-Port：
◎受信時に、VLANタグに含まれるTPIDが0x8100のフレームを、タグに含まれるVLAN IDに分類します。
フレームがタグなし、または優先度タグ付きの場合、フレームをポートVLANに分類します。
◎送信時に必要に応じてC-Tagでタグ付けします。

S-Port：
◎受信時に、VLANタグに含まれるTPIDが0x88A8のフレームを、タグに含まれるVLAN IDに分類します。
フレームがタグなし、または優先度タグ付きの場合、フレームをポートVLANに分類します。
[Ingress Acceptance]欄でタグ付きフレームだけを受信するように設定している場合は、TPIDが0x88A8のフレーム以外は破棄されます。
◎送信時に必要に応じてS-Tagでタグ付けします。

ご注意
[Ingress Acceptance]欄で「Tagged and Untagged」を選択したS-portでは、Cタグ付きフレームはS-Tag付きフレームと同じように扱われます。
[Ingress Acceptance]欄で「Untagged Only」を選択したS-portでは、優先後の低いS-Tag付きフレームは破棄されます。
C-Tag付きフレームはタグ付きフレームとみなされないため破棄されず、VLANタグに埋め込まれたVLAN IDに分類されます。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「VLANs」画面

Configuration > VLANs

Port VLAN Configuration

Port Type(つづき) ……

S-Custom-Port：
◎受信時に、VLANタグに含まれるTPIDが[Ethertype configured for Custom-S ports]欄で設定した値と一致するフレームを、タグに含まれるVLAN IDに分類します。
優先度タグ付きの場合、フレームをポートVLANに分類します。
[Ingress Acceptance]欄でタグ付きフレームだけを受信するように設定している場合は、TPIDが一致しないフレーム以外は破棄されます。
◎送信時に必要に応じて任意のS-Tagでタグ付けします。

ご注意
[Ingress Acceptance]欄で「Tagged and Untagged」を選択したcustom S-portでは、C-Tag付きフレームはS-Tag付きフレームと同じように扱われます。
[Ingress Acceptance]欄で「Untagged Only」を選択したcustom S-portでは、優先後の低いS-Tag付きフレームは破棄されます。
C-Tag付きフレームはタグ付きフレームとみなされないため破棄されず、VLANタグに埋め込まれた VLAN IDに分類されます。

Ingress Filtering ……

ハイブリッドポートで受信時のフィルタリングを有効にする場合、ボックスにチェックマークを入れます。
アクセスポートとトランクポートでは常に有効になります。
有効に設定した場合、ポートに収容されていないVLANに分類されたフレームは破棄されます。
無効に設定した場合は、ポートに収容されていないVLANに分類されたフレームは転送されますが、ポートから送信はされません。

Ingress Acceptance ……

ハイブリッドポートで受信するフレームを選択します。

Tagged and Untagged：
タグ付きフレームとタグなしフレームの両方を受信します。
タグ付きフレームの条件は、[Port Type]欄の説明を参照してください。

Tagged Only：
[Port Type]欄で設定したタグ付きフレームだけを受信します。

Untagged Only：
タグなしフレームだけを受信します。
タグなしフレームの条件は、[Port Type]欄の説明を参照してください。

「VLANs」画面

Configuration > VLANs

Port VLAN Configuration

Egress Tagging ……

トランクポート、またはハイブリッドポートで送信するとき、フレームにタグ付けするかどうかを設定します。

Untag Port VLAN：
ポートVLANに分類されたフレームはタグなしで送信します。
ほかのフレームは関連するタグ付きで送信します。

Tag All：
ポートVLANに分類されたかどうかに関わらず、すべてのフレームをタグ付きで送信します。

Untag All：
ポートVLANに分類されたかどうかに関わらず、すべてのフレームをタグなしで送信します。
※ハイブリッドポートでだけ選択できます。

Allowed VLANs ……

トランクポート、またはハイブリッドポートに収容するVLANを設定します。
アクセスポートは、1つのVLAN(アクセスVLAN)しか収容できません。
VLANは単数(xx)、または範囲(xx-yy)で指定できます。
複数指定する場合は、それぞれをコンマかスペースで区切ってください。
たとえば、「1,10-13,200,300」と入力した場合、VLAN ID 1、10、11、12、13、200、300が対象になります。
ポートにVLANを収容しない場合は、空白にしてください。

Forbidden VLANs ……

ポートに収容しないようにするVLANを設定します。
MVRPやGVRPなどの動的VLANプロトコル使用時、設定したVLANにポートが所属しないようにできます。
すべてのVLANの収容を許可する場合は、空白にします。

〈Save〉 ……

設定した内容を保存するボタンです。

〈Reset〉 ……

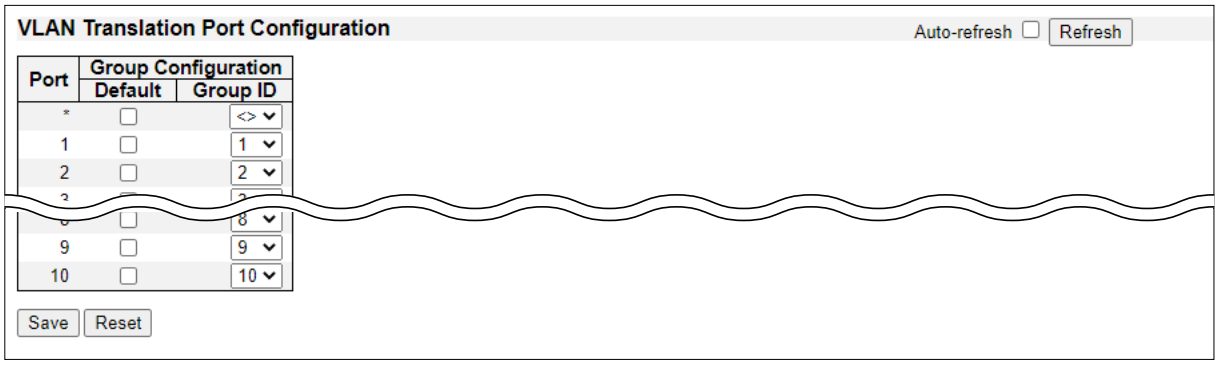
設定内容を変更したとき、変更前の状態に戻すボタンです。

「Port to Group Configuration」画面

Configuration > VLAN Translation > Port to Group Configuration

VLAN変換についてポートごとに設定します。
「Configuration」→「VLAN Translation」→「VLAN Translation Mappings」画面で設定したマッピンググループをポートに設定すると、設定したグループのすべてのVLAN変換が有効になります。

VLAN Translation Port Configuration



Auto-refresh ……
3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……
最新の状態に更新するボタンです。
※設定内容を変更したときは、変更前の状態に戻ります。

Port ……
本製品のポート番号が表示されます。

Group Configuration

Default ……
デフォルトのVLAN変換設定グループを使用するときは、ボックスにチェックマークを入れます。

Group ID ……
使用するVLAN変換設定グループを選択します。
設定できる範囲は、「1」～「10」です。
VLAN変換のマッピング設定を、グループIDで識別されるグループに登録します。
登録したグループを使用するようにポートを設定するだけで、VLAN変換のマッピングを簡単に使用するように設定できます。
1つのポートで使用できるグループは、一度に1つだけです。
複数ポートで同じグループを使用できます。
※デフォルトでは、ポート番号と同じIDのグループを使用するように設定されています。
たとえば、ポート1はGIDが1のグループを使用します。

〈Save〉 ……
設定した内容を保存するボタンです。

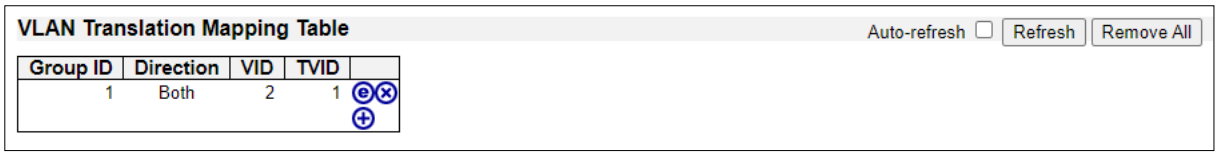
〈Reset〉 ……
設定内容を変更したとき、変更前の状態に戻すボタンです。

「VLAN Translation Mappings」画面

Configuration > VLAN Translation > VLAN Translation Mappings

VLAN変換設定グループに登録されたVID(変換元VLAN ID)とTVID(変換後VLAN ID)のマッピング設定が表示されます。

VLAN Translation Mapping Table



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈Remove All〉……　すべてのマッピング設定を削除するボタンです。

Group ID ……　VLAN変換のマッピング設定を登録したグループの、グループIDが表示されます。
登録したグループを使用するようにポートを設定するだけで、VLAN変換のマッピングを簡単に使用するように設定できます。
1つのポートで使用できるグループは、一度に1つだけです。
複数ポートで同じグループを使用できます。

Direction ……　VLAN変換機能を使用する方向が表示されます。

Ingress　：ポートで受信したフレームのVLAN IDを変換します。

Egress　：ポートから送信するフレームのVLAN ID を変換します。

Both　：送受信の両方でVLAN IDを変換します。

VID……　変換元のVLAN IDが表示されます。

TVID ……　変換後のVLAN IDが表示されます。

ⓔ ……　マッピング設定を編集するボタンです。
「Mapping Configuration」画面に移動します。

⊕ ……　マッピング設定を追加するボタンです。
「Mapping Configuration」画面に移動します。

⊗ ……　マッピング設定を削除するボタンです。

「Mapping Configuration」画面

Configuration > VLAN Translation > VLAN Translation Mappings

VLAN変換のマッピングを設定します。

Mapping Parameters

Group ID …… VLAN変換のマッピング設定を、グループIDで識別されるグループに登録します。
設定できる範囲は、「1 ～ 10」です。
登録したグループを使用するようにポートを設定するだけで、VLAN変換のマッピングを簡単に使用するように設定できます。
1つのポートで使用できるグループは、一度に1つだけです。
複数ポートで同じグループを使用できます。

DIR …… VLAN変換機能を使用する方向を設定します。

Ingress ：ポートで受信したフレームのVLAN IDを変換します。

Egress ：ポートから送信するフレームのVLAN ID を変換します。

Both ：送受信の両方でVLAN IDを変換します。

VID …… 変換元のVLAN IDを設定します。
設定できる範囲は、「1 ～4095」です。

TVID …… 変換後のVLAN IDを設定します。
設定できる範囲は、「1 ～4095」です。

〈Save〉 …… 設定した内容を保存するボタンです。

〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

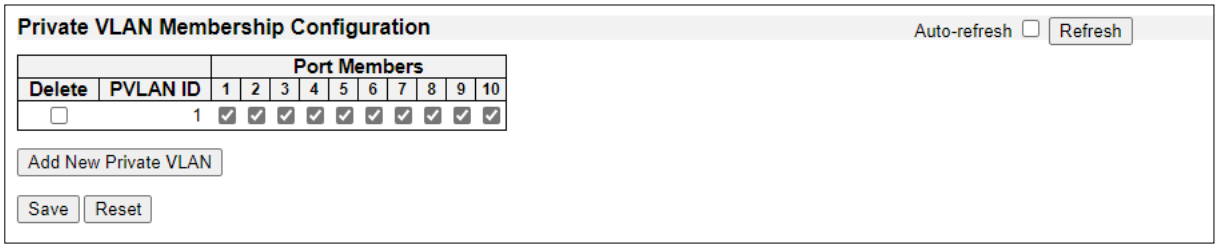
〈Cancel〉 …… 設定内容を変更したとき、変更前の状態に戻し、「VLAN Translation Mappings」画面に戻るボタンです。

「Membership」画面

Configuration > Private VLANs > Membership

プライベートVLANのメンバーシップを設定します。
プライベートVLANは送信元ポートマスクに基づいていて、VLANへ接続しないため、VLAN IDとプライベート VLAN ID に同じ値を設定できます。
パケットを転送できるようにするには、ポートがVLANとプライベートVLANの両方に所属する必要があります。
VLAN非対応ポートは1つのVLANにしか所属できませんが、複数のプライベートVLANに所属させられます。

Private VLAN Membership Configuration



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。
※設定内容を変更したときは、変更前の状態に戻ります。

Delete ……　登録された内容を削除するとき、ボックスにチェックマークを入れます。

PVLAN ID ……　プライベートVLANのVLAN IDを設定します。
設定できる範囲は、「1～10」です。

Port Members ……　プライベートVLANに所属するポートを選択します。

〈Add New Private VLAN〉 ……　クリックして新しいプライベートVLANを追加します。

〈Save〉 ……　設定した内容を保存するボタンです。

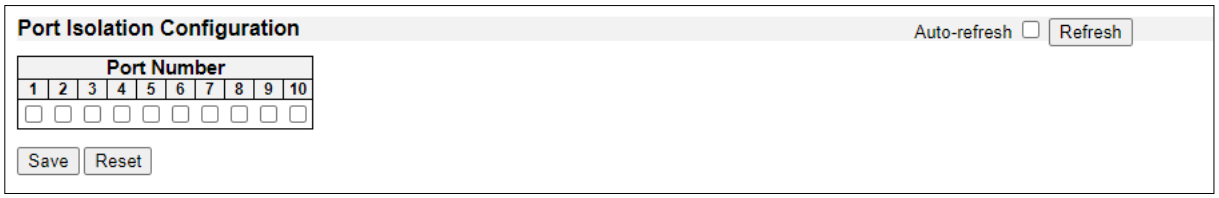
〈Reset〉 ……　設定内容を変更したとき、変更前の状態に戻すボタンです。

「Port Isolation」画面

Configuration > Private VLANs > Port Isolation

プライベートVLANに所属するポートのポート分離について設定します。
隔離ポートに設定すると、同じVLAN、またはプライベートVLANに所属するほかの隔離ポートとの通信を禁止できます。

Port Isolation Configuration



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。
※設定内容を変更したときは、変更前の状態に戻ります。

Port Number ……　隔離ポートに設定するとき、ボックスにチェックマークを入れます。

〈Save〉 ……　設定した内容を保存するボタンです。

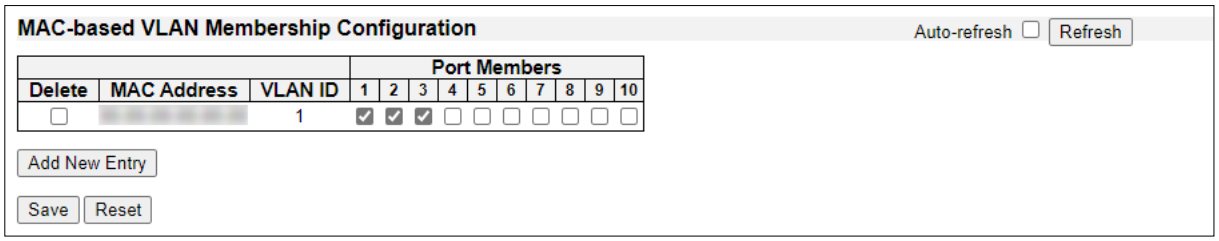
〈Reset〉 ……　設定内容を変更したとき、変更前の状態に戻すボタンです。

「MAC-based VLAN」画面

Configuration > VCL > MAC-based VLAN

MACアドレスからVLAN IDへのマッピングを設定します。
※最大256件登録できます。

MAC-based VLAN Membership Configuration



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。
※設定内容を変更したときは、変更前の状態に戻ります。

Delete ……　登録された内容を削除するとき、ボックスにチェックマークを入れます。

MAC Address ……　MACアドレスを設定します。
※ユニキャストMACアドレスは使用できますが、ブロードキャスト、またはマルチキャストMACアドレスは使用できません。

VLAN ID ……　MACアドレスをマッピングするVLAN IDを設定します。
設定できる範囲は、「1～4095」です。

Port Members ……　所属するポートのボックスにチェックマークを入れます。
※1つ以上のポートを選択しないと登録できません。

〈Add New Entry〉……　クリックして新しいマッピング設定を追加します。

〈Save〉 ……　設定した内容を保存するボタンです。

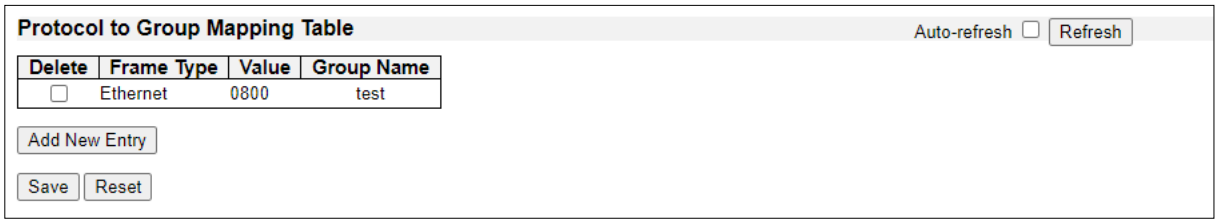
〈Reset〉 ……　設定内容を変更したとき、変更前の状態に戻すボタンです。

「Protocol to Group」画面

Configuration > VCL > Protocol-based VLAN > Protocol to Group

プロトコルからグループ名へのマッピングを設定します。
※プロトコルごとにマッピングできるグループ名は1つだけです。
※最大128件登録できます。

Protocol to Group Mapping Table



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。
※設定内容を変更したときは、変更前の状態に戻ります。

Delete ……　登録された内容を削除するとき、ボックスにチェックマークを入れます。

Frame Type ……　フレームタイプを「Ethernet」、「LLC」、「SNAP」から選択します。
※フレームタイプによって[Value]欄で設定する項目が異なります。

Value……　[Frame Type]欄で選択したフレームタイプごとに、設定できる値が異なります。

Frame TypeがEthernetの場合：
etypeの値を設定します。
設定できる範囲は、「0x0600～0xffff」です。

Frame TypeがLLCの場合：
DSAPとSSAPを設定します。
◎DSAPは「0x00～0xff」で設定します。
◎SSAPは「0x00～0xff」で設定します。

Frame TypeがSNAPの場合：
OUI(Organizationally Unique Identifier)とPID(Protocol ID)を設定します。
◎OUIは「xx-xx-xx」(xxは0x00～0xffの16進数)で設定します。
◎OUIが「000000」の場合、PIDはSNAP上で実行されているプロトコルのEthernet type(EtherType)フィールドの値を設定します。
設定できる範囲は、「0x0600～0xffff」です。
OUIが特定のベンダーOUIの場合、PIDはベンダーがSNAP上で実行しているプロトコルに割り当てられた値を設定します。
設定できる範囲は、「0x0000～0xffff」です。

Group Name ……　グループごとに固有の名称を16文字以内の英数字で入力します。
※特殊文字や「_(アンダースコア)」は使用できません。

〈Add New Entry〉……　クリックして新しいマッピング設定を追加します。

〈Save〉 ……　設定した内容を保存するボタンです。

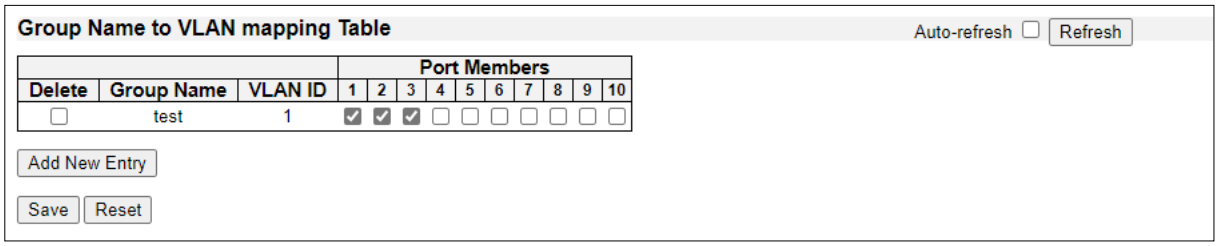
〈Reset〉 ……　設定内容を変更したとき、変更前の状態に戻すボタンです。

「Group to VLAN」画面

Configuration > VCL > Protocol-based VLAN > Group to VLAN

「Protocol to Group」画面で登録したグループ名からVLAN IDへのマッピングを設定します。
※マッピングするグループは、あとからでも登録できます。
※最大256件登録できます。

Group Name to VLAN mapping Table



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。
※設定内容を変更したときは、変更前の状態に戻ります。

Delete ……　登録された内容を削除するとき、ボックスにチェックマークを入れます。

Group Name ……　グループ名を16文字以内の英数字で入力します。
「Protocol to Group」画面でプロトコルへのマッピングを設定したグループ名を使用するか、新しいグループ名を登録したあとに「Protocol to Group」画面でプロトコルへのマッピングを設定します。

VLAN ID ……　グループ名をマッピングするVLAN IDを設定します。
設定できる範囲は、「1～4095」です。

Port Members ……　所属するポートのボックスにチェックマークを入れます。
※1つ以上のポートを選択しないと登録できません。

〈Add New Entry〉……　クリックして新しいマッピング設定を追加します。

〈Save〉 ……　設定した内容を保存するボタンです。

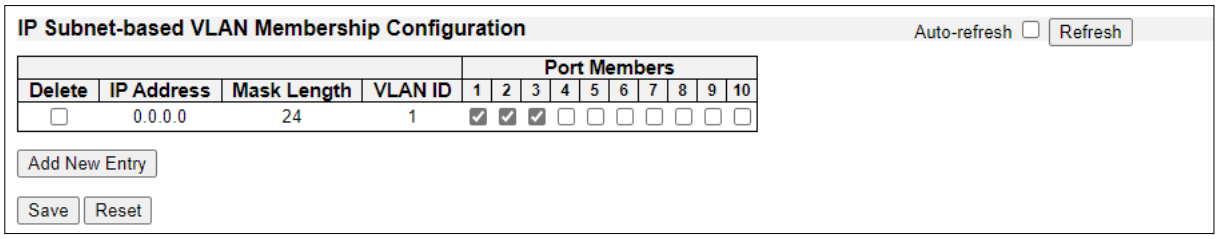
〈Reset〉 ……　設定内容を変更したとき、変更前の状態に戻すボタンです。

「IP Subnet-based VLAN」画面

Configuration > VCL > IP Subnet-based VLAN

IPサブネットからVLAN IDへのマッピングを設定します。
※最大128件登録できます。

IP Subnet-based VLAN Membership Configuration



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。
※設定内容を変更したときは、変更前の状態に戻ります。

Delete ……　登録された内容を削除するとき、ボックスにチェックマークを入れます。

IP Address ……　サブネットのIPアドレスを設定します。
サブネットのホストアドレスを設定すると、自動で変換されます。

Mask Length ……　サブネットマスクを設定します。

VLAN ID ……　IPサブネットにマッピングするVLAN IDを設定します。
1つのIPサブネットにマッピングできるVLAN IDは1つだけです。

Port Members ……　所属するポートのボックスにチェックマークを入れます。
※1つ以上のポートを選択しないと登録できません。

〈Add New Entry〉 ……　クリックして新しいマッピング設定を追加します。

〈Save〉 ……　設定した内容を保存するボタンです。

〈Reset〉 ……　設定内容を変更したとき、変更前の状態に戻すボタンです。

「Configuration」画面

Configuration > Voice VLAN > Configuration

Voice VLANについて設定します。
音声トラフィックをVoice VLANに転送することで、ネットワークトラフィックを分類し、スケジューリングできます。
ポートごとに2つのVLAN(音声用とデータ用)を設定することをおすすめします。
IPデバイスをスイッチに接続する前に、IP電話のVoice VLAN IDを正しく設定してください。

Voice VLAN Configuration

Mode ……

Voice VLANを有効にするかを設定します。
Voice VLANを有効にする場合は、MSTP機能を無効にしてください。
Voice VLANとMSTP機能の両方が有効なときは、受信フィルタリングが競合します。

Enabled：
Voice VLANを有効にします。

Disabled：
Voice VLANを無効にします。

VLAN ID ……

Voice VLAN IDを設定します。
設定できる範囲は、「1～4095」です。
※VID、MVR VID、PVIDと同じIDは設定できません。

Aging Time……

Voice VLAN使用時のエージング期間を設定します。
設定できる範囲は、「10～10000000」(秒)です。
[Port Mode]欄が「Auto」以外で[Port Security]欄が「Disabled」の場合は、ハードウェアのエージング期間を使用します。
実際のエージング期間は、設定したエージング期間から設定したエージング期間の2倍のあいだになります。

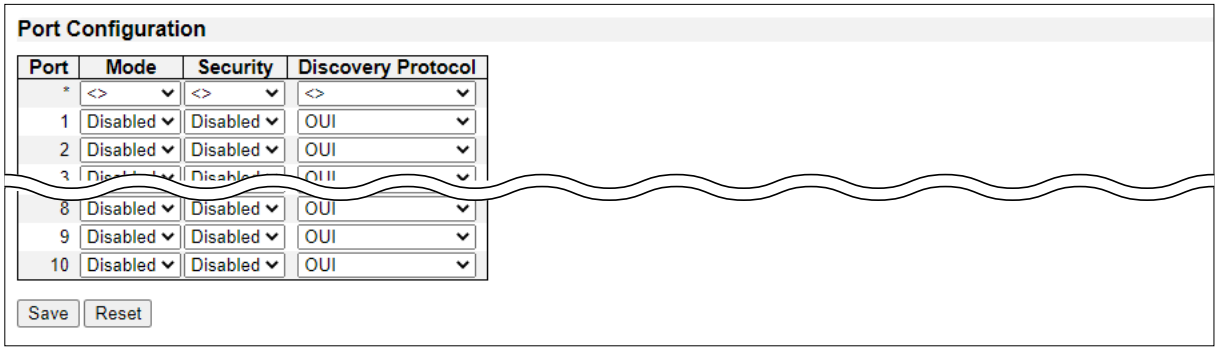
Traffic Class ……

すべてのVoice VLANのトラフィッククラスを設定します。

「Configuration」画面

Configuration > Voice VLAN > Configuration

Port Configuration



Port …… 本製品のポート番号が表示されます。

Mode …… Voice VLANの動作モードを設定します。

Disabled：
Voice VLANには収容しません。

Auto：
自動検出モードを有効にします。
VoIP電話が接続されているかどうかを検出し、Voice VLANメンバーを自動的に設定します。

Forced：
Voice VLANに収容します。

Security …… Voice VLANポートのセキュリティーについて設定します。

Enabled：
Voice VLAN内のすべての非テレフォニックMACアドレスからのトラフィックが10秒間ブロックされます。

Disabled：
Voice VLANセキュリティーを無効にします。

Discovery Protocol …… [Port Mode]欄で「Auto」を選択したとき、Voice VLANポートの検出プロトコルを設定します。
検出プロトコルを「LLDP」または「Both」に設定する場合は、LLDPを有効に設定してください。
検出プロトコルを「OUI」、または「LLDP」に変更すると、自動検出プロセスが再開されます。

OUI ：OUIアドレスでテレフォニーデバイスを検出します。

LLDP ：LLDPを使用してテレフォニーデバイスを検出します。

Both ：OUIアドレスとLLDPの両方を使用します。

〈Save〉 …… 設定した内容を保存するボタンです。

〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

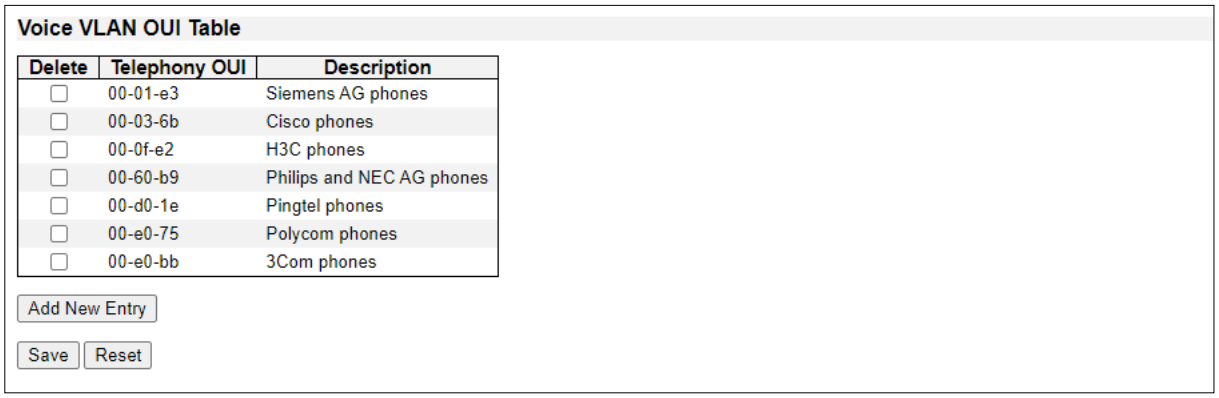
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「OUI」画面

Configuration > Voice VLAN > OUI

Voice VLANで使用するOUI(Organizationally Unique Identifier)テーブルを設定します。
OUIテーブルを変更すると、OUIプロセスの自動検出が再開されます。
※最大16件まで登録できます。

Voice VLAN OUI Table



Delete …… 登録された内容を削除するとき、ボックスにチェックマークを入れます。

Telephony OUI …… OUIアドレスを「xx-xx-xx」(xは16進数)の形式で設定します。
OUIアドレスは、IEEEによってベンダーに割り当てられた固有の識別子です。

Description…… OUIアドレスの説明を0～32文字で入力します。
通常、OUIが割り当てられたベンダーの名称を設定します。

〈Add New Entry〉…… クリックして、新しいOUIを追加します。

〈Save〉 …… 設定した内容を保存するボタンです。

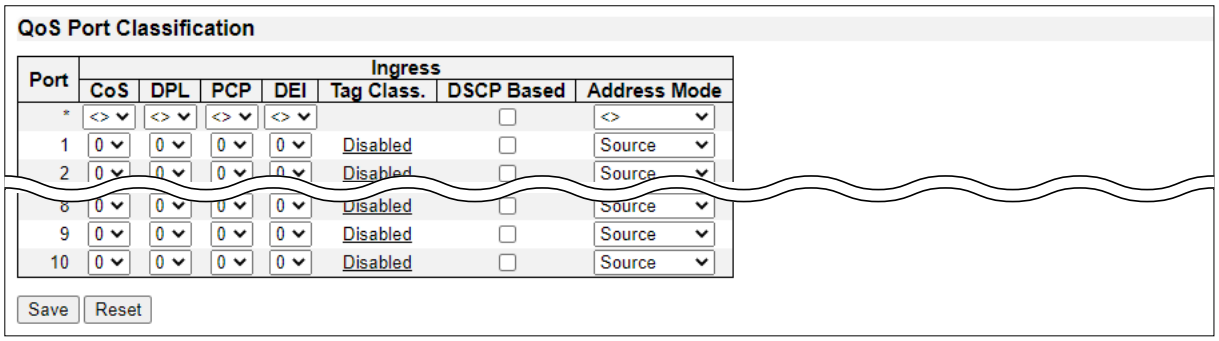
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Port Classification」画面

Configuration > QoS > Port Classification

基本となるQoS(Quality of Service)のクラス分類について設定します。

QoS Port Classification



Port ····· 本製品のポート番号が表示されます。

Ingress

CoS ····· デフォルトのCoS(Class of Service)値を設定します。
設定できる範囲は、「0」～「7」です。
すべてのフレームは、CoS値で分類されます。
CoS、キュー、優先度は、1対1でマッピングされます。
CoS値が「0」の場合、優先度が最も低くなります。
[Tag Class.]欄が「Enabled」の場合、VLAN対応のポートで受信したタグ付きフレームは、フレームのVLANタグに含まれるPCP値とDEI値に基づいて分類されます。
それ以外の場合、フレームはデフォルトのCoS値で分類されます。
分類されたCoSは、QCLの設定によって上書きできます。

DPL ····· デフォルトのDPL(Drop Precedence Level)値を設定します。
すべてのフレームは、DPL値で分類されます。
[Tag Class.]欄が「Enabled」の場合、VLAN対応のポートで受信したタグ付きフレームは、フレームのVLANタグに含まれるPCP値とDEI値に基づいて分類されます。
それ以外の場合、フレームはデフォルトのDPL値で分類されます。
分類されたDPLは、QCLの設定によって上書きできます。

PCP ····· デフォルトのPCP値を設定します。
すべてのフレームは、PCP値で分類されます。
VLAN対応のポートで受信したタグ付きフレームは、フレームのVLANタグに含まれるPCP値で分類されます。
それ以外の場合、フレームはデフォルトの PCP値で分類されます。

「Port Classification」画面

Configuration > QoS > Port Classification

QoS Port Classification

DEI ……

デフォルトのDEI 値を設定します。
すべてのフレームは、DEI値で分類されます。
VLAN対応のポートで受信したタグ付きフレームは、フレームのVLANタグに含まれるDEI値で分類されます。
それ以外の場合、フレームはデフォルトのDEI値で分類されます。

Tag Class. ……

タグ付きフレームの分類について表示されます。
設定のリンク先をクリックすると、「Tag Classification」画面へ移動します。
※VLAN非対応のポートには影響しません。
VLAN非対応のポートで受信したタグ付きフレームは、常にデフォルトのCoS値とDPL値で分類されます。

Disabled：
タグ付きフレームに対して、デフォルトのCoS値とDPL値を使用します。

Enabled：
タグ付きフレームに対して、マッピングされた PCP値とDEI値を使用します。

DSCP Based ……

DSCPベースの分類設定を有効にするとき、ボックスにチェックマークを入れます。

Address Mode ……

QCL（QoS Control List）による分類で、送信元アドレス（SMAC/SIP）を使用するか宛先アドレス（DMAC/DIP）を使用するかを選択します。

Source：
送信元アドレスをマッチングに使用します。

Destination：
宛先アドレスをマッチングに使用します。

〈Save〉 ……

設定した内容を保存するボタンです。

〈Reset〉 ……

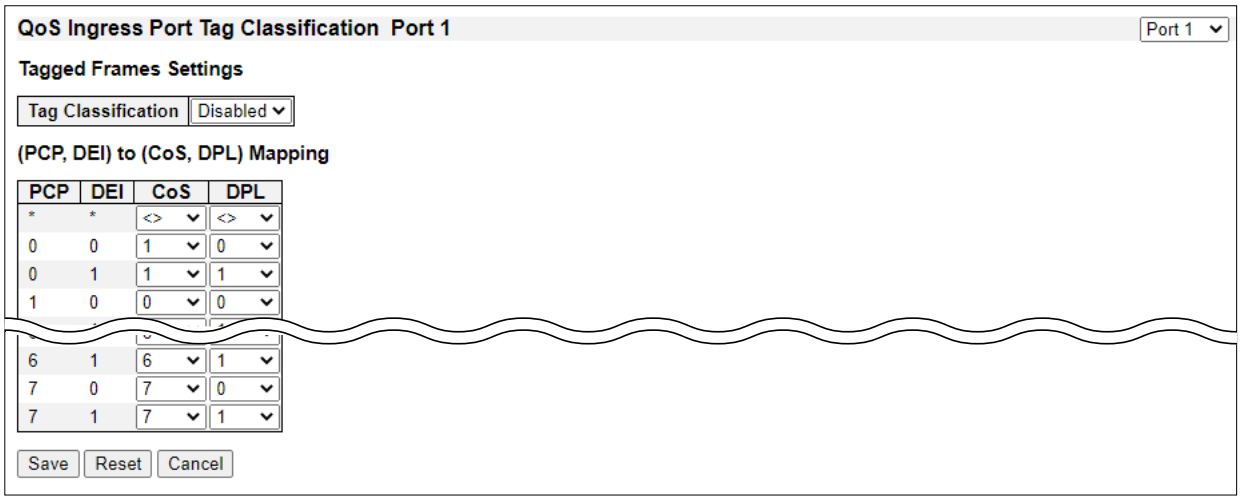
設定内容を変更したとき、変更前の状態に戻すボタンです。

「Tag Classification」画面

Configuration > QoS > Port Classification

受信ポートごとに、タグ付きフレームの分類について設定します。

QoS Ingress Port Tag Classification Port 1～10



Tagged Frames Settings

Tag Classification ……

タグ付きフレームの分類について設定します。

Disabled：
タグ付きフレームに対して、デフォルトのCoS値とDPL値を使用します。

Enabled：
タグ付きフレームに対して、マッピングされた PCP値とDEI値を使用します。

(PCP, DEI) to (CoS, DPL) Mapping ……

[Tag Classification]欄で「Enabled」を選択したとき、PCP値/DEI値からCoS値/DPL値へのマッピングについて設定します。

〈Save〉 ……

設定した内容を保存するボタンです。

〈Reset〉 ……

設定内容を変更したとき、変更前の状態に戻すボタンです。

〈Cancel〉 ……

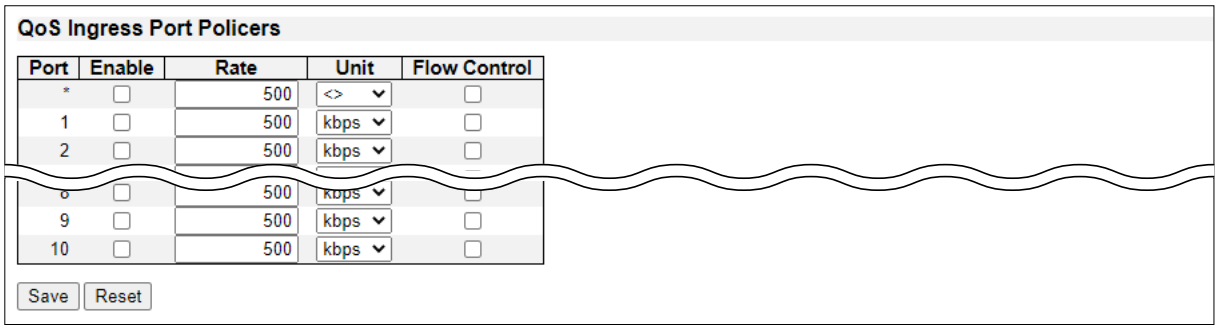
設定内容を変更したとき、変更前の状態に戻し、「Port Classification」画面に戻るボタンです。

「Port Policing」画面

Configuration > QoS > Port Policing

受信ポートごとに、ポートポリサーについて設定します。

QoS Ingress Port Policers



Port …… 本製品のポート番号が表示されます。

Enable …… ポートポリサーを有効にするとき、ボックスにチェックマークを入れます。

Rate …… ポートポリサーのレートを設定します。
[Unit]欄で「kbps」、または「fps」を選択したとき、設定できる範囲は「100～3276700」です。
[Unit]欄で「Mbps」、または「kfps」を選択したとき、設定できる範囲は「1～3276」です。
※ポートポリサーが対応しているレートのうち、最も近い値に自動で切り上げられます。

Unit …… ポートポリサーのレートの単位を、「kbps」、「Mbps」、「fps」、「kfps」から選択します。

Flow Control …… フロー制御が有効なポートで、フレームを破棄するかわりにポーズフレームを送信するときは、ボックスにチェックマークを入れます。

〈Save〉 …… 設定した内容を保存するボタンです。

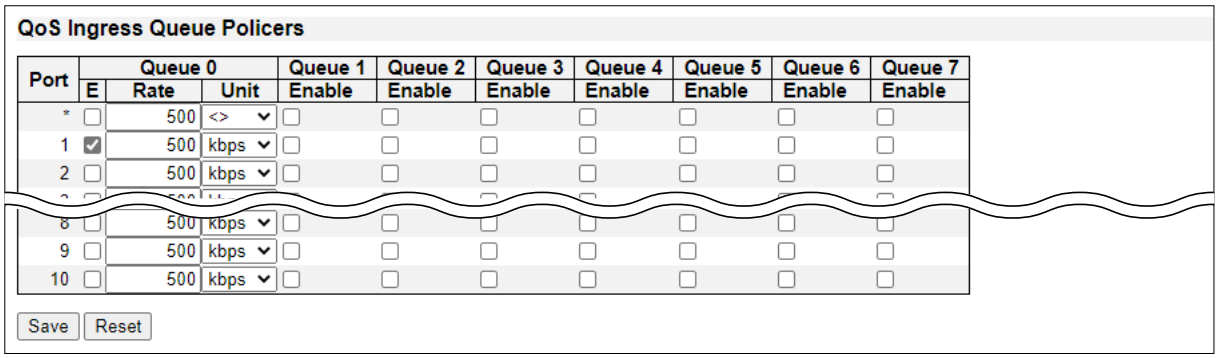
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Queue Policing」画面

Configuration > QoS > Queue Policing

受信ポートごとに、キューポリサーについて設定します。

QoS Ingress Queue Policers



Port …… 本製品のポート番号が表示されます。

Queue 0～7 Enable(E) …… キューポリサーを有効にするとき、ボックスにチェックマークを入れます。
※キューポリサーを有効にすると、[Rate]欄と[Unit]欄が表示されます。

Rate …… キューポリサーを有効にしたとき、レートを設定します。
[Unit]欄で「kbps」を選択したとき、設定できる範囲は「100～3276700」です。
[Unit]欄で「Mbps」を選択したとき、設定できる範囲は「1～3276」です。
※キューポリサーが対応しているレートのうち、最も近い値に自動で切り上げられます。

Unit …… キューポリサーを有効にしたとき、レートの単位を、「kbps」、「Mbps」から選択します。

〈Save〉 …… 設定した内容を保存するボタンです。

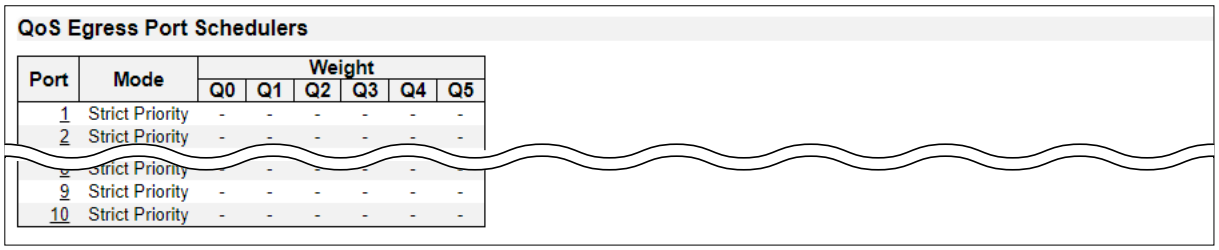
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Port Scheduler」画面

Configuration > QoS > Port Scheduler

送信ポートごとに、スケジューラの設定が表示されます。

QoS Egress Port Schedulers



QoS Egress Port Schedulers

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-

Port …… 本製品のポート番号が表示されます。
各ポート番号のリンクをクリックすると、「Port Scheduler and Shapers」画面へ移動します。（P.2-188）

Mode …… スケジューリングのモードが表示されます。

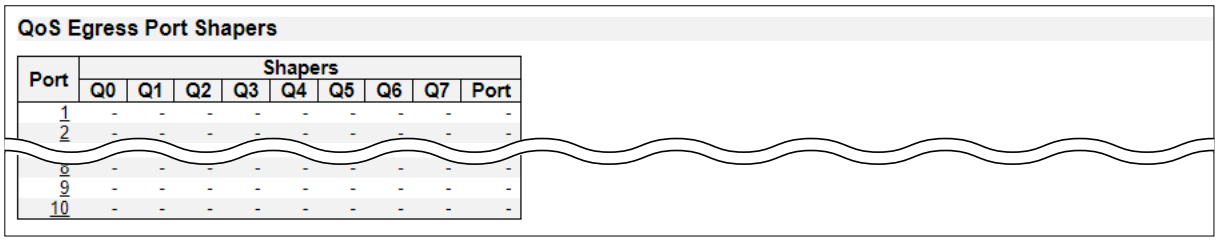
Weight
Q0～5 …… 各キューの重みが表示されます。

「Port Shaping」画面

Configuration > QoS > Port Shaping

送信ポートごとに、シェーパーの設定が表示されます。

QoS Egress Port Shapers



Port …… 本製品のポート番号が表示されます。
各ポート番号のリンクをクリックすると、「Port Scheduler and Shapers」画面へ移動します。(P.2-188)

Shapers

Q0～7 …… キューシェーパーのレートが表示されます。
キューシェーパーが無効のときは、「-」が表示されます。

Port …… ポートシェーパーのレートが表示されます。
ポートシェーパーが無効のときは、「-」が表示されます。

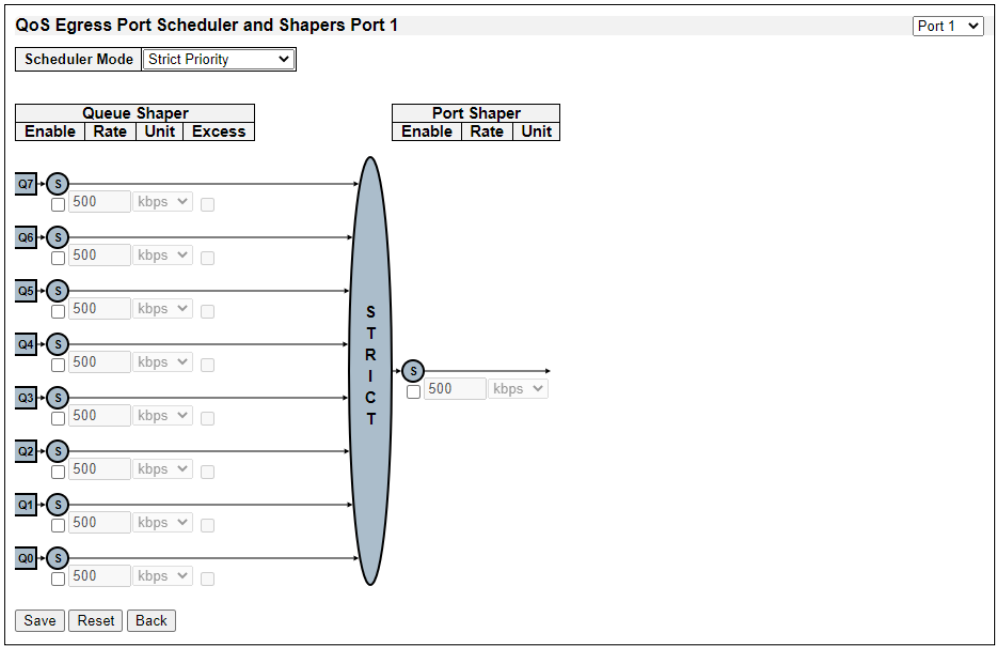
「Port Scheduler and Shapers」画面

Configuration > QoS > Port Scheduler/Port Shaping

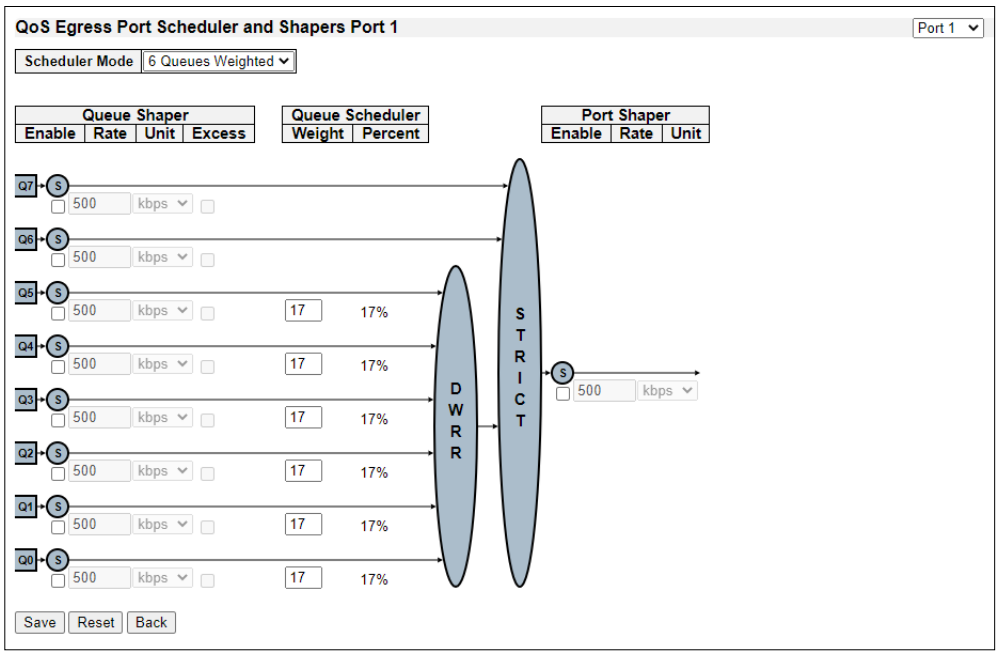
送信ポートごとに、スケジューラとシェーパーについて設定します。

QoS Egress Port Scheduler and Shapers Port 1～10

Scheduler Mode：Strict Priority



Scheduler Mode：6 Queues Weighted



「Port Scheduler and Shapers」画面

Configuration > QoS > Port Scheduler/Port Shaping

QoS Egress Port Scheduler and Shapers Port 1～10

Scheduler Mode ……
スケジューラのモードを選択します。

Strict Priority：
キューの優先度に応じて厳格にスケジューリングします。

6 Queues Weighted：
キューごとに設定された重み(Scheduler Weight)に応じてスケジューリングします。

Queue Shaper

Enable ……
キューシェーパーを有効にするとき、ボックスにチェックマークを入れます。

Rate ……
キューシェーパーを有効にしたとき、レートを設定します。
[Unit]欄で「kbps」を選択したとき、設定できる範囲は「100～3281943」です。
[Unit]欄で「Mbps」を選択したとき、設定できる範囲は「1～3281」です。
※キューシェーパーが対応しているレートのうち、最も近い値に自動で切り上げられます。

Unit ……
キューシェーパーを有効にしたとき、レートの単位を「kbps」、「Mbps」から選択します。

Excess ……
キューが余分な帯域幅を使用できるようにするときに、ボックスにチェックマークを入れます。

Queue Scheduler

Weight ……
[Scheduler Mode]欄で「6 Queues Weighted」を選択したとき、キューごとの重みを設定します。
設定できる範囲は、「1～100」です。

Percent ……
[Scheduler Mode]欄で「6 Queues Weighted」を選択したとき、キューごとの重みの比率がパーセントで表示されます。

Port Shaper

Enable ……
ポートシェーパーを有効にするとき、ボックスにチェックマークを入れます。

Rate ……
ポートシェーパーを有効にしたとき、レートを設定します。
[Unit]欄で「kbps」を選択したとき、設定できる範囲は「100～3281943」です。
[Unit]欄で「Mbps」を選択したとき、設定できる範囲は「1～3281」です。
※ポートシェーパーが対応しているレートのうち、最も近い値に自動で切り上げられます。

Unit ……
ポートシェーパーを有効にしたとき、レートの単位を「kbps」、「Mbps」から選択します。

〈Save〉 ……
設定した内容を保存するボタンです。

〈Reset〉 ……
設定内容を変更したとき、変更前の状態に戻すボタンです。

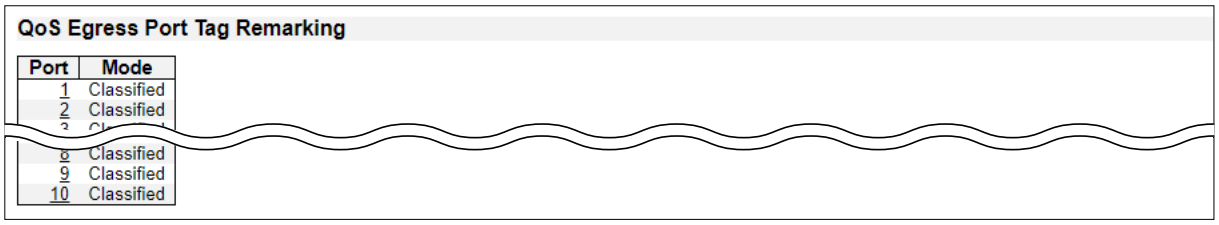
〈Back〉 ……
設定内容を変更したとき、変更前の状態に戻し、「Port Scheduler」画面に戻るボタンです。

「Port Tag Remarking」画面

Configuration > QoS > Port Tag Remarking

送信ポートごとに、VLANタグのリマーキングについて表示されます。

QoS Egress Port Tag Remarking



Port ……

本製品のポート番号が表示されます。
各ポート番号のリンクをクリックすると、「Tag Remarking」画面へ移動します。

Mode ……

リマーキングのモードが表示されます。

Classified：
分類されたPCP値/DEI値を使用します。

Default：
「Tag Remarking」画面で設定したデフォルトのPCP値とDEI値を使用します。

Mapped：
「Tag Remarking」画面でマッピング設定をしたCoS値とDPL値を使用します。

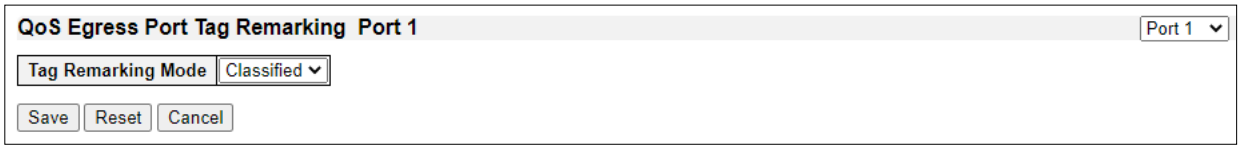
「Tag Remarking」画面

Configuration > QoS > Port Tag Remarking

送信ポートごとに、VLANタグのリマーキングについて設定します。

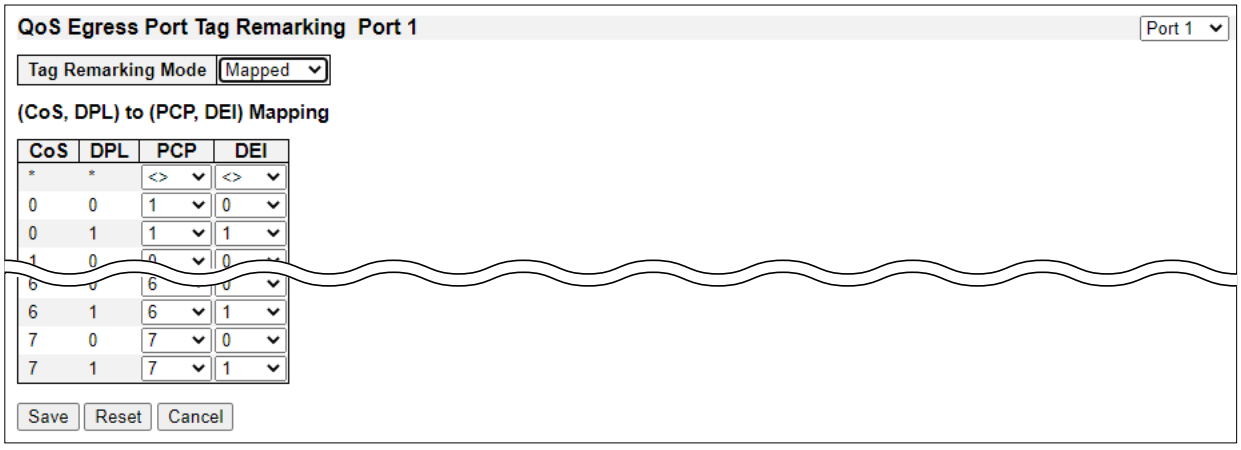
QoS Egress Port Tag Remarking Port 1～10

Tag Remarking Mode : Classified



Tag Remarking Mode : Default

Tag Remarking Mode : Mapped



「Tag Remarking」画面

Configuration > QoS > Port Tag Remarking

QoS Egress Port Tag Remarking Port 1～10

Tag Remarking Mode …… リマーキングのモードを設定します。

Classified：
分類されたPCP値とDEI値を使用します。

Default：
デフォルトのPCP値とDEI値を使用します。

Mapped：
マッピング設定をしたCoS値とDPL値を使用します。

PCP/DEI Configuration …… [Mode]欄で「Default」を選択したとき、デフォルトのPCP値とDEI値を設定します。

(CoS, DPL) to (PCP, DEI) Mapping …… [Mode]欄で「Mapped」を選択したとき、PCP値/DEI値からCoS値/DPL値へのマッピングについて設定します。

〈Save〉 …… 設定した内容を保存するボタンです。

〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

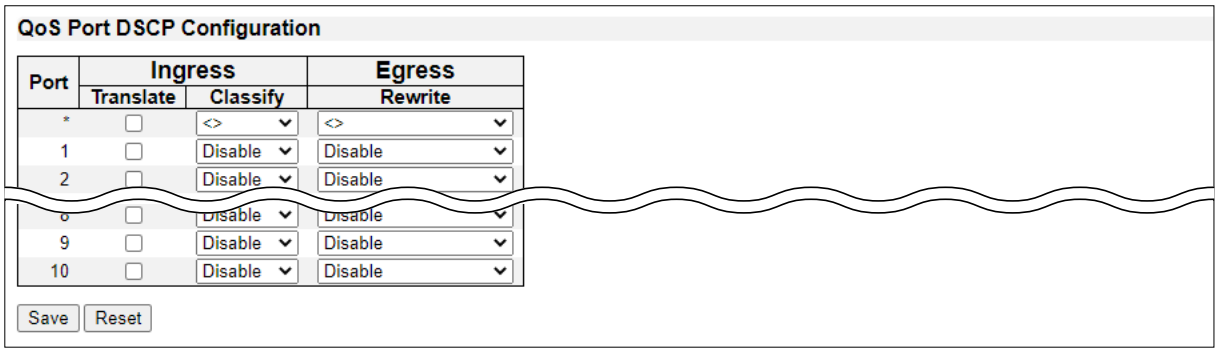
〈Cancel〉 …… 設定内容を変更したとき、変更前の状態に戻し、「Port Tag Remarking」画面に戻るボタンです。

「Port DSCP」画面

Configuration > QoS > Port DSCP

基本のポートDSCP(Differentiated Services Code Point)について設定します。

QoS Port DSCP Configuration



Port …… 本製品のポート番号が表示されます。

Ingress Translate …… 受信ポートでの変換機能を有効にするとき、ボックスにチェックマークを入れます。

Ingress Classify …… 受信ポートでの分類について設定します。

Disable ：DSCP分類を無効にします。

DSCP=0 ：受信したパケット、または変換済みパケットのDSCP値が0の場合に分類します。

Selected ：「DSCP Translation」画面で[Ingress Classify]欄を有効に設定しているDSCPだけを分類します。

All ：すべてのDSCPを分類します。

Egress Rewrite …… 送信ポートの書き換え機能について設定します。

Disable：
書き換え機能を無効にします。

Enable：
再マッピングなしの書き換え機能を有効にします。

Remap DP Unaware：
アナライザーからのDSCPが再マッピングされ、再マッピングされたDSCP値でフレームをマーキングします。
再マッピングされるDSCP値は、「DSCP Translation」画面の[Egress Remap DP0]欄から取得します。

Remap DP Aware：
アナライザーからのDSCPが再マッピングされ、再マッピングされたDSCP値でフレームをマーキングします。
再マッピングされるDSCP値は、フレームのDPLに応じて「DSCP Translation」画面の[Egress Remap DP0]欄、または[Egress Remap DP1]欄から取得します。

〈Save〉 …… 設定した内容を保存するボタンです。

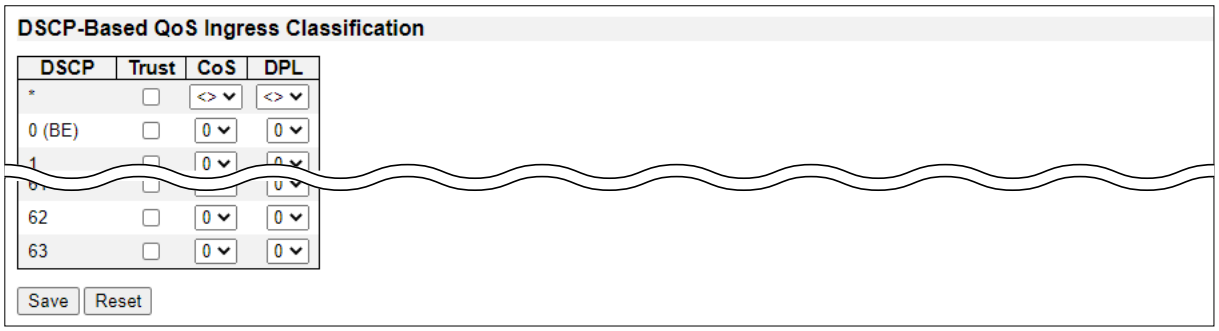
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「DSCP-Based QoS」画面

Configuration > QoS > DSCP-Based QoS

基本となるDSCPベースのQoS受信分類について設定します。

DSCP-Based QoS Ingress Classification



DSCP …… DSCP値が表示されます。
サポートしているDSCP値は最大64個です。

Trust …… 信頼できるDSCP値に設定するとき、ボックスにチェックマークを入れます。
信頼できるDSCP値を持つフレームは、設定したCoS値とDPL(Drop Precedence Level)値にマッピングされます。
信頼できないDSCP値を持つフレームは、non-IPフレームとして扱われます。

CoS …… CoS値を設定します。
設定できる範囲は、「0」～「7」です。

DPL …… DPL(Drop Precedence Level)値を「0」か「1」から選択します。

〈Save〉 …… 設定した内容を保存するボタンです。

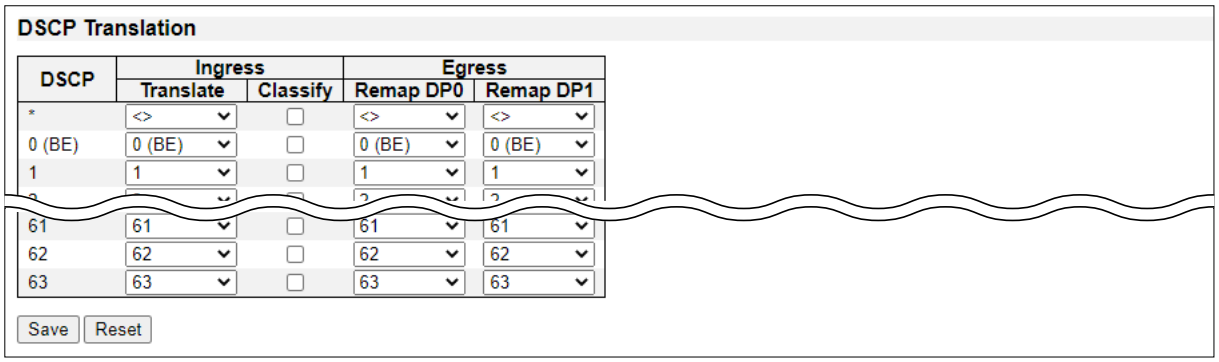
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「DSCP Translation」画面

Configuration > QoS > DSCP Translation

基本となるDSCP変換機能について設定します。

DSCP Translation



DSCP …… DSCP値が表示されます。
サポートしているDSCP値は0から63までの最大64個です。

Ingress Translate …… 受信ポートで変換するDSCP値を設定します。
設定できる範囲は、「0」～「63」です。

Ingress Classify …… 受信ポートでの分類を有効にするとき、ボックスにチェックマークを入れます。

Egress Remap DP0 …… 送信ポートでDPLが0のフレームを再マッピングするDSCP値を選択します。
設定できる範囲は、「0」～「63」です。

Egress Remap DP1 …… 送信ポートでDPLが1のフレームを再マッピングするDSCP値を選択します。
設定できる範囲は、「0」～「63」です。

〈Save〉 …… 設定した内容を保存するボタンです。

〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「DSCP Classification」画面

Configuration > QoS > DSCP Classification

DSCP値とCoS値、DPL値 のマッピングについて設定します。

DSCP Classification

CoS …… CoS値が表示されます。

DSCP DP0 …… DPLが0のときに分類されるDSCP値を設定します。
設定できる範囲は、「0」～「63」です。

DSCP DP1 …… DPLが1のときに分類されるDSCP値を設定します。
設定できる範囲は、「0」～「63」です。

〈Save〉 …… 設定した内容を保存するボタンです。

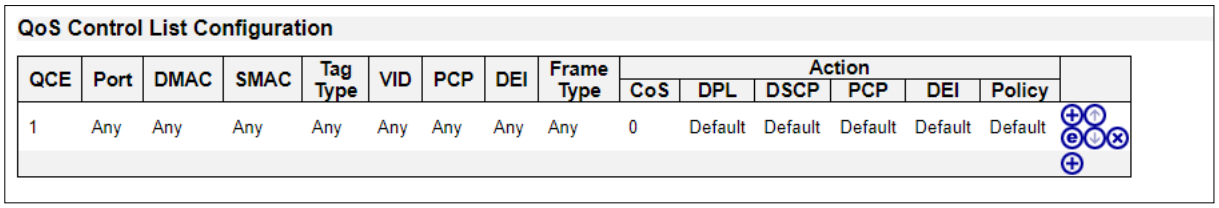
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「QoS Control List」画面

Configuration > QoS > QoS Control List

QoSコントロールリスト(QCL)を構成するQoSコントロールエントリ(QCE)が表示されます。
QCEは最大256件まで登録できます。

QoS Control List Configuration



QCE …… QCE IDが表示されます。

Port …… QCEを適用するポートが表示されます。

DMAC …… 条件となる宛先MACアドレスが表示されます。

Any：
宛先MACアドレスではフィルタリングしません。

Unicast：
宛先MACアドレスがユニキャストのフレームをフィルタリングします。

Multicast：
宛先MACアドレスがマルチキャストのフレームをフィルタリングします。

Broadcast：
宛先MACアドレスがブロードキャストのフレームをフィルタリングします。

SMAC …… 条件とする送信元MACアドレスが表示されます。
「Port Classification」画面で[Address Mode]欄を「Destination」に設定しているポートの場合、設定したアドレスが宛先MACアドレスと一致するかが条件になります。

Tag Type…… タグフレームかどうかを条件に含むかが表示されます。

Any：
VLANタグではフィルタリングしません。

Untagged：
タグなしフレームをフィルタリングします。

Tagged：
タグ付きフレームをフィルタリングします。

VID…… 条件とする特定のVID(VLAN ID)、またはVIDの範囲が表示されます。

PCP …… 条件とするPCP(Priority Code Point)値が表示されます。

DEI…… 条件とするDEI(Drop Eligible Indicator)値が表示されます。

「QoS Control List」画面

Configuration > QoS > QoS Control List

QoS Control List Configuration

Frame Type ……

条件となるフレームタイプが表示されます。

Any ：フレームタイプではフィルタリングしません。
Ethernet ：イーサネットタイプのフレームをフィルタリングします。
LLC ：LLCフレームをフィルタリングします。
SNAP ：SNAPフレームをフィルタリングします。
IPv4 ：IPv4フレームをフィルタリングします。
IPv6 ：IPv6フレームをフィルタリングします。

Action

CoS ……

QCEに一致するフレームを受信したとき、表示されているCoS(Class of Service)値に分類します。

DPL ……

QCEに一致するフレームを受信したとき、表示されているDPL(Drop Precedence Level)値に分類します。

DSCP ……

QCEに一致するフレームを受信したとき、表示されているDSCP値に分類します。

PCP ……

QCEに一致するフレームを受信したとき、表示されているPCP値に分類します。

DEI ……

QCEに一致するフレームを受信したとき、表示されているDEI値に分類します。

Policy ……

QCEに一致するフレームを受信したとき、表示されているACLポリシー番号に分類します。

 ……

1つ前にQCEを追加するボタンです。
一番下に表示されているボタンをクリックすると、リストの最後にQCEが追加されます。

 ……

QCEを編集するボタンです。
「QCE Configuration」画面に移動します。

 ……

1つ上に移動するボタンです。

 ……

1つ下に移動するボタンです。

 ……

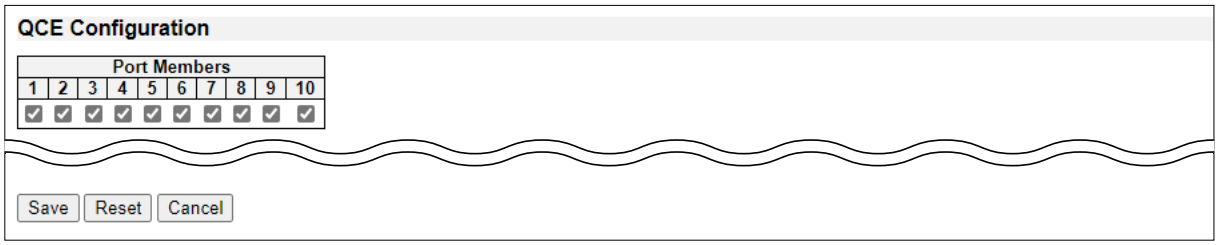
QCEを削除するボタンです。

「QCE Configuration」画面

Configuration > QoS > QoS Control List

QoSコントロールエントリ(QCE)を設定します。
設定できる項目は、[Frame Type]欄の設定によって異なります。
フレームタイプを選択すると、選択したフレームタイプに応じた設定項目が表示されます。

QCE Configuration



Port Members 1～10 …… QCEを適用するポートのボックスにチェックマークを入れます。

〈Save〉 …… 設定した内容を保存するボタンです。

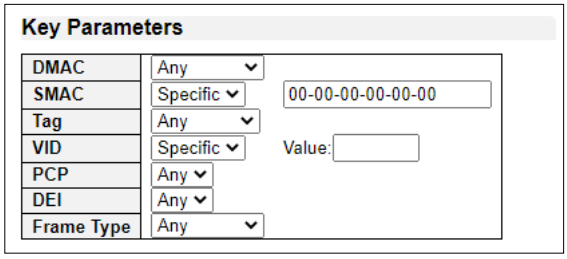
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

〈Cancel〉 …… 設定内容を変更したとき、変更前の状態に戻し、「QoS Control List」画面に戻るボタンです。

「QCE Configuration」画面

Configuration > QoS > QoS Control List

Key Parameters



DMAC ……

宛先MACアドレスでフィルタリングするかを設定します。

Any：
宛先MACアドレスではフィルタリングしません。

Unicast：
宛先MACアドレスがユニキャストのフレームをフィルタリングします。

Multicast：
宛先MACアドレスがマルチキャストのフレームをフィルタリングします。

Broadcast：
宛先MACアドレスがブロードキャストのフレームをフィルタリングします。

SMAC ……

送信元MACアドレスでフィルタリングするかを設定します。
「Port Classification」画面で[Address Mode]欄を「Destination」に設定したポートの場合、設定したアドレスが宛先MACアドレスと一致するかが条件になります。

Any　：ポリシー番号ではフィルタリングしません。

Specific　：設定したアドレスでフィルタリングします。
アドレスの設定欄が表示されます。

Tag……

VLANタグでフィルタリングするかを設定します。

Any　：VLANタグではフィルタリングしません。

Untagged：タグなしフレームをフィルタリングします。

Tagged　：タグ付きフレームをフィルタリングします。

C-Tagged：C-Tag付きフレームをフィルタリングします。

S-Tagged：S-Tag付きフレームをフィルタリングします。

VID……

VID（VLAN ID）でフィルタリングするかを設定します。
特定のVID、またはVID範囲を指定するとき、設定できる範囲は「1～4095」です。

Any　：VIDではフィルタリングしません。

Specific　：設定したVIDでフィルタリングします。
VIDの設定欄が表示されます。

Range　：設定したVID範囲でフィルタリングします。
VID範囲の設定欄が表示されます。

「QCE Configuration」画面

Configuration > QoS > QoS Control List

Key Parameters

PCP ……

PCP(Priority Code Point)値でフィルタリングするかを設定します。

Any：
PCP値ではフィルタリングしません。

0、1、2、3、4、5、6、7：
選択したPCP値のフレームをフィルタリングします。

0-1、2-3、4-5、6-7、0-3、4-7：
選択した範囲のPCP値のフレームをフィルタリングします。

DEI ……

DEI(Drop Eligible Indicator)値でフィルタリングするかを設定します。

Any ：DEI値ではフィルタリングしません。
0、1 ：選択したPCP値のフレームをフィルタリングします。

Frame Type ……

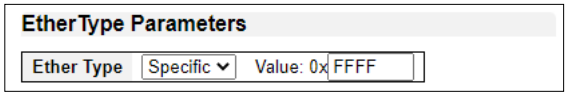
フレームタイプでフィルタリングするかを設定します。

Any ：フレームタイプではフィルタリングしません。
EtherType ：イーサネットタイプのフレームをフィルタリングします。
LLC ：LLCフレームをフィルタリングします。
SNAP ：SNAPフレームをフィルタリングします。
IPv4 ：IPv4フレームをフィルタリングします。
IPv6 ：IPv6フレームをフィルタリングします。

「QCE Configuration」画面

Configuration > QoS > QoS Control List

EtherType Parameters



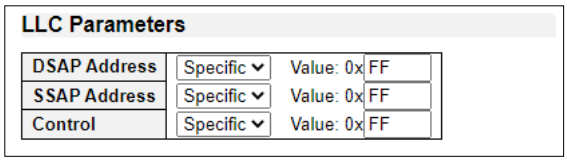
Ether Type ……

[Frame Type]欄で「Ethernet Type」を選択したときに、フレームのEtherTypeフィールドでフィルタリングするかを選択します。

Any ：EtherTypeフィールドではフィルタリングしません。

Specific ：設定したEtherTypeフィールド値でフィルタリングします。
EtherType値の設定欄が表示されます。
設定できる範囲は、0x800(IPv4)、0x86DD(IPv6) を除く「0x600～0xFFFF」です。

LLC Parameters



DSAP Address ……

DSAP(宛先サービスアクセスポイント)でフィルタリングするかを設定します。

Any ：DSAPではフィルタリングしません。

Specific ：設定したDSAPでフィルタリングします。
DSAPの設定欄が表示されます。
設定できる範囲は、「0x00～0xFF」です。

SSAP Address ……

SSAP(送信元サービスアクセスポイント)でフィルタリングするかを設定します。

Any ：SSAPではフィルタリングしません。

Specific ：設定したSSAPでフィルタリングします。
SSAPの設定欄が表示されます。
設定できる範囲は、「0x00～0xFF」です。

Control ……

Control(制御)フィールドでフィルタリングするかを設定します。

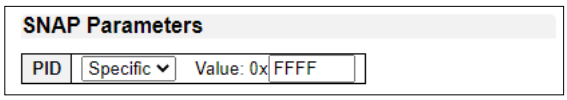
Any ：Controlフィールドではフィルタリングしません。

Specific ：設定したControlフィールド値でフィルタリングします。
Controlフィールド値の設定欄が表示されます。
設定できる範囲は、「0x00～0xFF」です。

「QCE Configuration」画面

Configuration > QoS > QoS Control List

SNAP Parameters



PID……

PID(プロトコル識別子)でフィルタリングするかを設定します。
※PIDは、EtherTypeと同じコードを使用します。

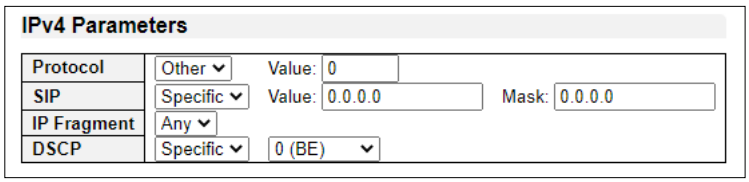
Any ：PIDではフィルタリングしません。

Specific ：設定したPIDでフィルタリングします。
PIDの設定欄が表示されます。
設定できる範囲は、「0x0000～0xFFFF」です。

「QCE Configuration」画面

Configuration > QoS > QoS Control List

IPv4 Parameters



Protocol ……

IPプロトコルでフィルタリングするかを選択します。

Any ：DSAPではフィルタリングしません。

UDP ：UDPプロトコルのIPv4フレームをフィルタリングします。
UDPパラメーターを設定するための設定項目が表示されます。
(P.2-206)

TCP ：TCPプロトコルのIPv4フレームをフィルタリングします。
TCPパラメーターを設定するための設定項目が表示されます。
(P.2-206)

Other ：指定したIPプロトコルでフィルタリングします。
IPプロトコルの設定欄が表示されます。
設定できる範囲は、「0～255」です。

SIP ……

送信元IPアドレスでフィルタリングするかを設定します。
「Port Classification」画面で[Address Mode]欄を「Destination」に設定したポートの場合、設定したアドレスが宛先IPアドレスと一致するかが条件になります。

Any ：送信元IPアドレスではフィルタリングしません。

Specific ：設定した送信元IPアドレスでフィルタリングします。
IPアドレスとサブネットマスクの設定欄が表示されます。

IP Fragment ……

IPv4フレームのMF(More Fragment)ビットとFRAG OFFSET(フラグメントオフセット)フィールドの値でフィルタリングするかを設定します。

Any ：MFビットとFRAG OFFSETフィールドの値ではフィルタリングしません。

Yes ：MFビットが1、またはFRAG OFFSETフィールド値が0より大きいIPv4フレームをフィルタリングします。

No ：MFビットが0かつFRAG OFFSETフィールド値が0のIPv4 フレームをフィルタリングします。

DSCP ……

DSCP(Diffserv Code Point)値でフィルタリングするかを設定します。
特定のDSCP、またはDSCP範囲を指定するとき、設定できる範囲は「0」～「63」(BE、CS1～CS7、EF、AF11～AF43含む)です。

Any ：DSCP値ではフィルタリングしません。

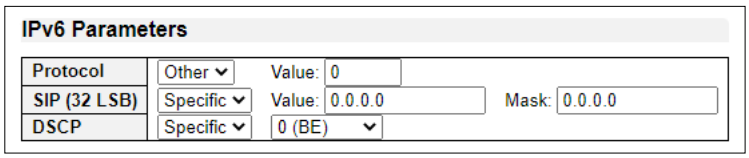
Specific ：設定したDSCP値でフィルタリングします。
DSCP値の設定欄が表示されます。

Range ：設定したDSCP値の範囲でフィルタリングします。
DSCP範囲の設定欄が表示されます。

「QCE Configuration」画面

Configuration > QoS > QoS Control List

IPv6 Parameters



Protocol ……

IPプロトコルでフィルタリングするかを選択します。

Any ：DSAPではフィルタリングしません。

UDP ：UDPプロトコルのIPv6フレームをフィルタリングします。
UDPパラメーターを設定するための設定項目が表示されます。
（P.2-206）

TCP ：TCPプロトコルのIPv6フレームをフィルタリングします。
TCPパラメーターを設定するための設定項目が表示されます。
（P.2-206）

Other ：指定したIPプロトコルでフィルタリングします。
IPプロトコルの設定欄が表示されます。
設定できる範囲は、「0～255」です。

SIP (32 LSB) ……

送信元IPv6アドレスの下位32ビットでフィルタリングするかを設定します。
「Port Classification」画面で「Address Mode」欄を「Destination」に設定したポートの場合、設定したアドレスが宛先IPアドレスと一致するかが条件になります。

Any ：送信元IPアドレスではフィルタリングしません。

Specific ：設定した送信元IPアドレスでフィルタリングします。
IPアドレスとサブネットマスクの設定欄が表示されます。

DSCP ……

DSCP（Diffserv Code Point）値でフィルタリングするかを設定します。
特定のDSCP、またはDSCP範囲を指定するとき、設定できる範囲は「0」～「63」（BE、CS1～CS7、EF、AF11～AF43含む）です。

Any ：DSCP値ではフィルタリングしません。

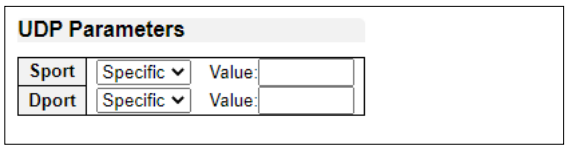
Specific ：設定したDSCP値でフィルタリングします。
DSCP値の設定欄が表示されます。

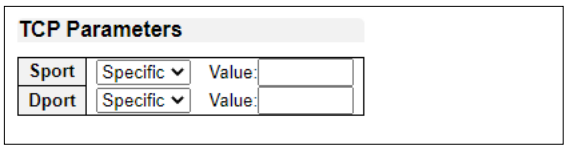
Range ：設定したDSCP値の範囲でフィルタリングします。
DSCP範囲の設定欄が表示されます。

「QCE Configuration」画面

Configuration > QoS > QoS Control List

UDP Parameters/TCP Parameters





Sport……

TCP/UDPフレームの送信元ポート番号フィールドでフィルタリングするかを設定します。
特定の送信元ポート番号、またはポート番号範囲を指定するとき、設定できる範囲は「0～65535」です。

Any ：送信元ポート番号ではフィルタリングしません。

Specific ：設定した送信元ポート番号でフィルタリングします。
送信元ポート番号の設定欄が表示されます。

Range ：設定した送信元ポート番号範囲でフィルタリングします。
送信元ポート番号範囲の設定欄が表示されます。

Dport……

TCP/UDPフレームの宛先ポート番号フィールドでフィルタリングするかを設定します。
特定の宛先ポート番号、またはポート番号範囲を指定するとき、設定できる範囲は「0～65535」です。

Any ：宛先ポート番号ではフィルタリングしません。

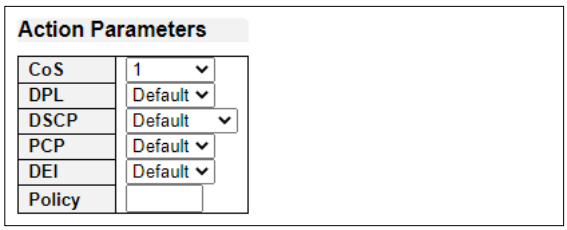
Specific ：設定した宛先ポート番号でフィルタリングします。
宛先ポート番号の設定欄が表示されます。

Range ：設定した宛先ポート番号範囲でフィルタリングします。
宛先ポート番号範囲の設定欄が表示されます。

「QCE Configuration」画面

Configuration > QoS > QoS Control List

Action Parameters



CoS ……

QCEに一致するフレームを受信したときに、分類するCoS値を設定します。
設定できる範囲は、「0」～「7」です。
「Default」を選択したときは、QCEに一致するフレームを受信してもCoS値を変更しません。

DPL ……

QCEに一致するフレームを受信したときに、分類するDPL値を「0」か「1」から設定します。
「Default」を選択したときは、QCEに一致するフレームを受信してもDPL値を変更しません。

DSCP ……

QCEに一致するフレームを受信したときに、分類するDSCP値を設定します。
設定できる範囲は、「0」～「63」(BE、CS1～CS7、EF、AF11～AF43含む)です。
「Default」を選択したときは、QCEに一致するフレームを受信してもDSCP値を変更しません。

PCP ……

QCEに一致するフレームを受信したときに、分類するPCP値を設定します。
設定できる範囲は、「0」～「7」です。
「Default」を選択したときは、QCEに一致するフレームを受信してもPCP値を変更しません。
※[DEI]欄で「Default」を選択した場合は、「Default」に設定してください。
[DEI]欄で「Default」以外を選択した場合は、「Default」以外に設定してください。

DEI ……

QCEに一致するフレームを受信したときに、分類するDEI値を「0」か「1」から設定します。
「Default」を選択したときは、QCEに一致するフレームを受信してもDEI値を変更しません。
※[PCP]欄で「Default」を選択した場合は、「Default」に設定してください。
[PCP]欄で「Default」以外を選択した場合は、「Default」以外に設定してください。

Policy ……

QCEに一致するフレームを受信したときに、分類するACLポリシー番号を設定します。
設定できる範囲は、「0～255」です。
空白(Default)に設定したときは、QCEに一致するフレームを受信してもACLポリシーを変更しません。

「Storm Policing」画面

Configuration > QoS > Storm Policing

システム全体のストームポリサーについて設定します。
ユニキャストストームポリサー、マルチキャストストームポリサー、ブロードキャストストームポリサーの3種類あり、フラッディングされたフレーム（MACアドレステーブルに存在しないVLAN IDと宛先MACアドレスの組み合わせを持つフレーム）にだけ有効な機能です。

Global Storm Policer Configuration

Frame Type …… 対応するフレームの種類が表示されます。

Enable …… システム全体でストームポリサーを有効にするとき、ボックスにチェックマークを入れます。

Rate …… ストームポリサーのレートを設定します。
[Unit]欄で「fps」を選択したとき、設定できる範囲は「1～1024000」です。
[Unit]欄で「kfps」を選択したとき、設定できる範囲は「1～1024」です。
※ストームポリサーが対応しているレートのうち、最も近い値に自動で切り上げられます。

Unit …… ストームポリサーのレートの単位を、「fps」、「kfps」から選択します。

〈Save〉 …… 設定した内容を保存するボタンです。

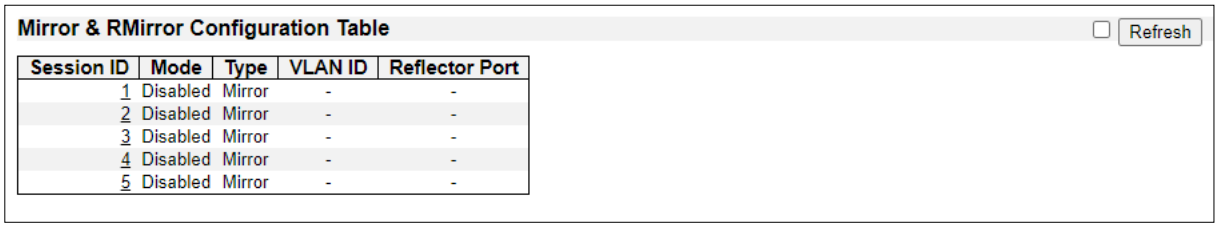
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「Mirroring」画面

Configuration > Mirroring

ミラーリング設定の一覧が表示されます。
ミラーリングは、スイッチのポートに接続したネットワークアナライザーのための機能です。
ネットワークアナライザーが接続されたポートにトラフィックをミラーリング(コピー)することで、ネットワークトラフィックを分析し、ネットワークの問題をデバッグできます。
リモートミラーリングは、ミラーリングの拡張機能です。
別のスイッチへトラフィックを転送したり、別のスイッチのネットワークトラフィックを分析したりできます。
トラフィックのタグ情報が必要な場合は、リフレクターポートの[Egress Tagging]を「Tag All」に設定してください。
トラフィックのタグ情報が不要な場合は、リフレクターポートの[Egress Tagging]を「Untag All」に設定してください。
[Egress Tagging]は、「Configuraion」→「VLANs」画面で設定できます。

Mirror & RMirror Configuration Table



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

Session ID ……　セッションIDが表示されます。
各セッションIDのリンク先をクリックすると、「Mirror Configuration」画面へ移動します。

Mode ……　ミラーリング機能が有効かが表示されます。

Type ……　使用するミラーリング機能の種類が表示されます。

Mirror：
ミラーリングモードを使用します。
本製品のポートがモニターポートとミラーポートになります。

RMirror source：
本製品のポートのトラフィックを監視します。
本製品のポートが、モニターポートとリフレクターポートになります。

RMirror destination：
トラフィックを監視するためのデバイスとして使用します。
本製品のポートがミラーポートになります。

VLAN ID ……　パケットのコピー先VLAN IDが表示されます。

「Mirroring」画面

Configuration > Mirroring

Mirror & RMirror Configuration Table

Reflector Port ……

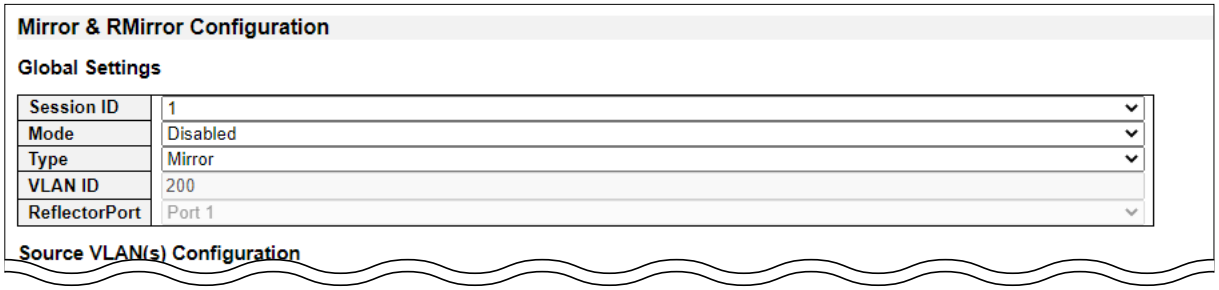
リフレクターポートは、トラフィックをリモートミラーリング用VLANに転送するためのポートです。
リフレクターポートとして設定されたポートに接続したデバイスは、リモートミラーリングが無効になるまで切断されます。
シャットダウン状態のポートは、リフレクターポートに設定できません。
リフレクターポートに設定したポートをシャットダウンすると、リモートミラーリング機能が動作しなくなります。

ご注意
◎リフレクターポートは、[Type]欄が「RMirror source」のときだけ設定する必要があります。
◎リフレクターポートは、MACアドレス学習とSTPを無効にしてください。
◎光ファイバーケーブル用ポートは、リフレクターポートとして使用できません。

「Mirroring」画面

Configuration > Mirroring

Mirror & RMirror Configuration



Global Settings

Session ID …… 設定を変更するセッションのIDを選択します。

Mode …… ミラーリング機能を使用するかどうかを選択します。

Type …… 使用するミラーリング機能の種類を選択します。

Mirror：
ミラーリングモードを使用します。
本製品のポートがモニターポートとミラーポートになります。

RMirror source：
本製品のポートのトラフィックを監視します。
本製品のポートが、モニターポートとリフレクターポートになります。

RMirror destination：
トラフィックを監視するためのデバイスとして使用します。
本製品のポートがミラーポートになります。

VLAN ID …… パケットのコピー先VLAN IDを設定します。

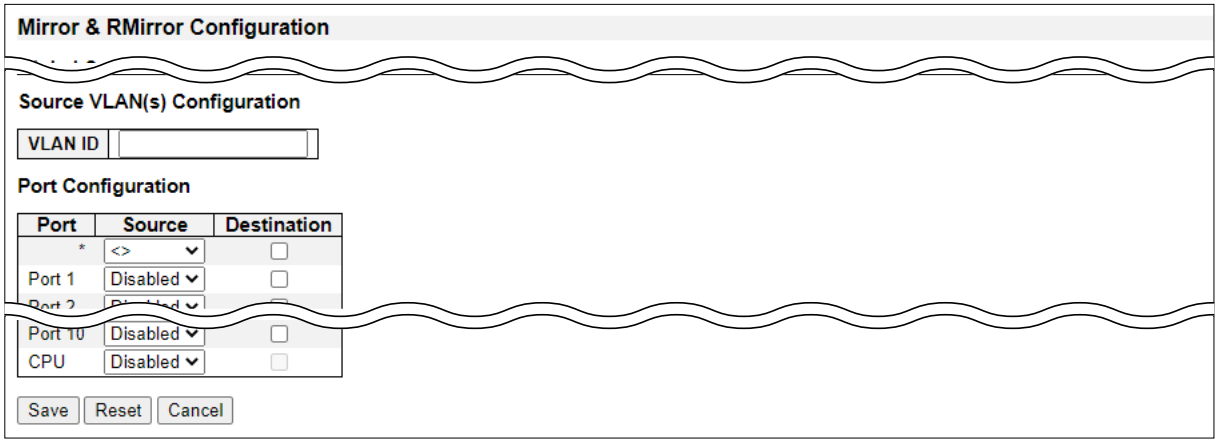
ReflectorPort …… リフレクターポートは、トラフィックをリモートミラーリング用VLANに転送するためのポートです。
リフレクターポートとして設定されたポートに接続したデバイスは、リモートミラーリングが無効になるまで切断されます。
シャットダウン状態のポートは、リフレクターポートに設定できません。
リフレクターポートに設定したポートをシャットダウンすると、リモートミラーリング機能が動作しなくなります。

ご注意
◎リフレクターポートは、[Type]欄が「RMirror source」のときだけ設定する必要があります。
◎リフレクターポートは、MACアドレス学習とSTPを無効にしてください。
◎光ファイバーケーブル用ポートは、リフレクターポートとして使用できません。

「Mirroring」画面

Configuration > Mirroring

Mirror & RMirror Configuration



Source VLAN(s) Configuration

VLAN ID ……

VLANベースのミラーリング機能を使用する場合に、トラフィックを監視するVLANを設定します。
※ポートとVLANの両方を同時にミラーリングすることはできません。

Port Configuration

Port ……

本製品のポート番号が表示されます。

Source ……

ミラーリングのモードを選択します。

Disabled：
送信したフレームも受信したフレームもミラーリングしません。

Both：
受信したフレームと送信したフレームを、ミラーポートにミラーリングします。

Rx only：
受信したフレームをミラーポートにミラーリングし、送信したフレームはミラーリングしません。

Tx only：
送信したフレームをミラーポートにミラーリングし、受信したフレームはミラーリングしません。

Destination……

[Type]欄で「Mirror」、または「Rmirror destination」を選択したときに、ミラーポートとして使用するポートのボックスにチェックマークを入れます。
ミラーポートは、モニターポートからトラフィックのコピーを受信するポートです。
※[Type]欄で「Mirror」を選択したとき、ミラーポートとして使用できるポートは1つです。
※ミラーポートはMACアドレス学習を無効に設定してください。

〈Save〉 ……

設定した内容を保存するボタンです。

〈Reset〉 ……

設定内容を変更したとき、変更前の状態に戻すボタンです。

〈Cancel〉 ……

設定内容を変更したとき、変更前の状態に戻し、「Mirroring」画面に戻るボタンです。

「Mirroring」画面

Configuration > Mirroring

Mirror & RMirror Configuration

リモートミラーリング使用時の各機能の設定について
リモートミラーリング機能を使用する場合、管理者はほかの機能が有効か無効かを確認する必要があります。
たとえば、リフレクターポートのMSTPを無効にしないと、すべてのモニタートラフィックは、リフレクターポートでブロックされます。
下記のように設定することを推奨します。

	Impact	source port（モニターポート）	reflector port	intermediate port	destination port（ミラーポート）	Remote Mirroring VLAN
arp_inspection	High		* disabled	* disabled		
acl	Critical		* disabled	* disabled	* disabled	
dhcp_relay	High		* disabled	* disabled		
dhcp_snooping	High		* disabled	* disabled		
ip_source_guard	Critical		* disabled	* disabled	* disabled	
ipmc/igmpsnp	Critical					un-conflict
ipmc/mldsnp	Critical					un-conflict
lacp	Low				o disabled	
lldp	Low				o disabled	
mac learning	Critical		* disabled	* disabled	* disabled	
mstp	Critical		* disabled		o disabled	
mvr	Critical					un-conflict
nas	Critical		* authorized	* authorized	* authorized	
psec	Critical		* disabled	* disabled	* disabled	
qos	Critical		* unlimited	* unlimited	* unlimited	
upnp	Low				o disabled	
mac-based vlan	Critical		* disabled	* disabled		
protocol-based vlan	Critical		* disabled	* disabled		
vlan_translation	Critical		* disabled	* disabled	* disabled	
voice_vlan	Critical		* disabled	* disabled		
mrp	Low				o disabled	
mvrp	Low				o disabled	

* ：必ず設定してください。
o ：設定は任意です。

Impact
Critical ：5パケット→0パケット
High ：5パケット→4パケット
Low ：5パケット→6パケット

「UPnP」画面

Configuration > UPnP

UPnP(Universal Plug and Play)について設定します。

UPnP Configuration

Mode……　UPnPを有効にするかどうかを選択します。

TTL……　UPnP使用時、SSDPパケットのTTL(Time to Live)値が表示されます。
※設定は変更できません。

Advertising Duration……　スイッチがSSDPメッセージを送信する頻度を、コントロールポイントへ通知するために使用します。
コントロールポイントは、期間内にメッセージを受信しなかったときに、スイッチは存在しないとみなします。
UDPの信頼性が低いため、[Advertising Duration]欄で設定した半分未満の期間内に、新たなSSDPメッセージを送信することが推奨されます。
本製品は、[Advertising Duration]－30秒の間隔で、SSDPメッセージを定期的に送信します。
設定できる範囲は、「100～86400」(秒)です。

IP Addressing Mode……　IPアドレッシングのモードを選択します。

Dynamic　：使用可能なシステムIPアドレスから自動で選択します。

Static　：本製品のIPアドレスを選択するためのVLAN IDを指定します。

Static VLAN Interface ID……　本製品のIPアドレスを選択するためのVLAN IDを設定します。
設定できる範囲は、「1～4095」です。
[IP Addressing Mode]欄で「Static」を選択したときに有効な設定です。

〈Save〉……　設定した内容を保存するボタンです。

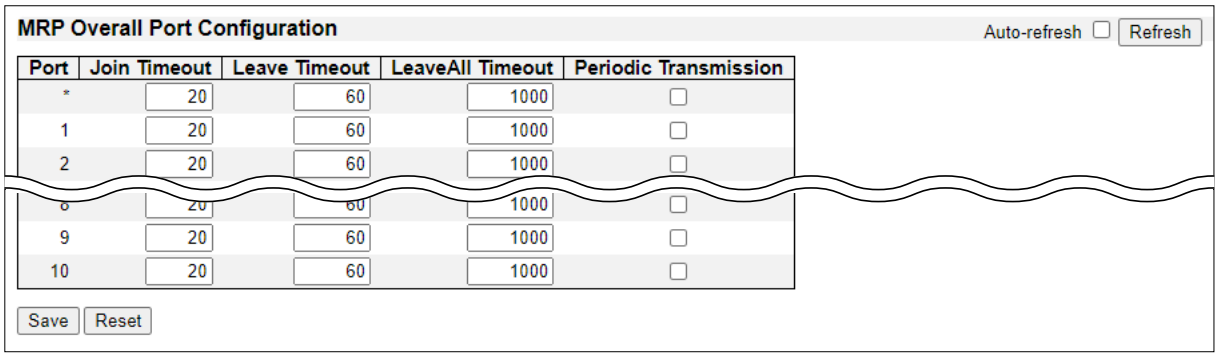
〈Reset〉……　設定内容を変更したとき、変更前の状態に戻すボタンです。

「Ports」画面

Configuration > MRP > Ports

MRP(Multiple Registration Protocol)について設定します。

MRP Overall Port Configuration



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。
※設定内容を変更したときは、変更前の状態に戻ります。

Port ……　本製品のポート番号が表示されます。

Join Timeout ……　Joinメッセージを送信してから、応答を待機する時間を設定します。
設定できる範囲は、「1～ 20」(×0.01秒)です。

Leave Timeout ……　Leaveメッセージを受信してから登録を解除するまでの時間を設定します。
設定できる範囲は、「60～300」(×0.01秒)です。

LeaveAll Timeout ……　LeaveAllメッセージを送信するまでの時間を設定します。
設定できる範囲は、「1000～5000」(×0.01秒)です。

Periodic Transmission ……　定期的にMRPメッセージを送信するかどうかを設定します。

〈Save〉 ……　設定した内容を保存するボタンです。

〈Reset〉 ……　設定内容を変更したとき、変更前の状態に戻すボタンです。

「MVRP」画面

Configuration > MRP > MVRP

MVRP(Multiple Vlan Registration Protocol)について設定します。

MVRP Global Configuration

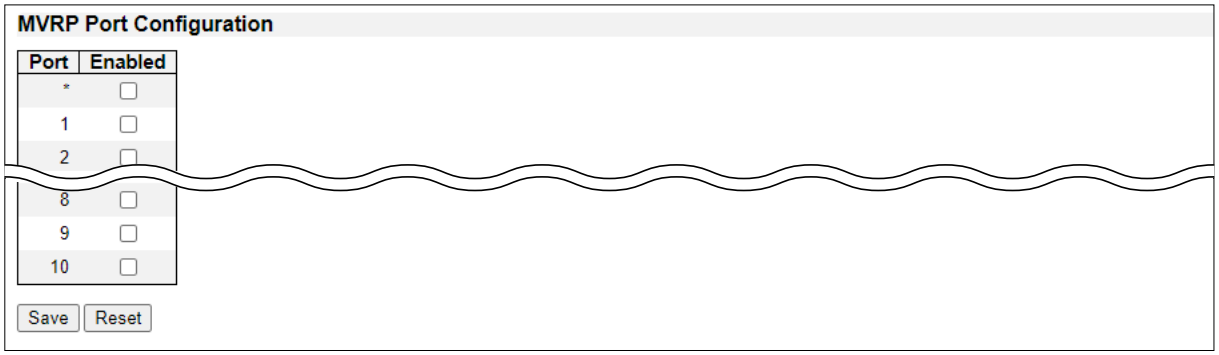
Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。
※設定内容を変更したときは、変更前の状態に戻ります。

Global State ……　システム全体で、MVRPを有効にするかどうかを設定します。

Managed VLANs ……　MVRPが動作するVLANのVLAN IDを入力します。
VLANは単数(xx)、または範囲(xx-yy)で指定できます。
複数指定する場合は、それぞれをコンマかスペースで区切ってください。
たとえば、「1,10-13,200,300」と入力した場合、VLAN ID 1、10、11、12、13、200、300が対象になります。

MVRP Port Configuration



Port ……　本製品のポート番号が表示されます。

Enabled ……　ポートごとにMVRPを有効にするかどうかを設定します。
[Global State]欄で「Enabled」を選択したときに、ボックスにチェックマークを入れたポートでMVRPが有効になります。

〈Save〉 ……　設定した内容を保存するボタンです。

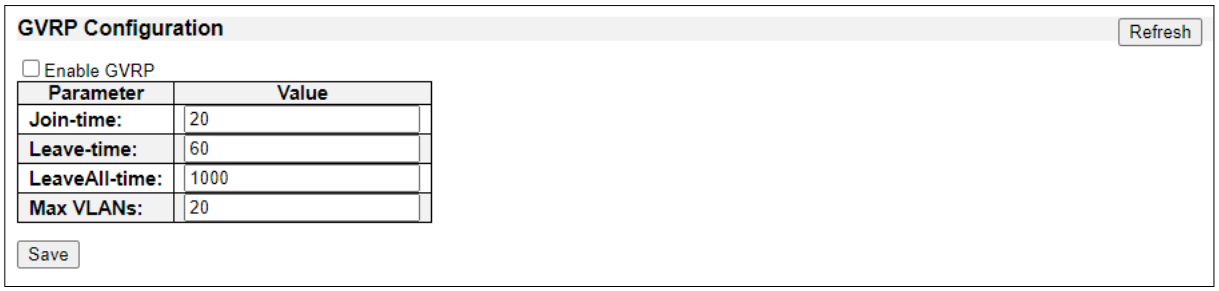
〈Reset〉 ……　設定内容を変更したとき、変更前の状態に戻すボタンです。

「Global config」画面

Configuration > GVRP > Global Config

GVRP(GARP VLAN Registration Protocol)について設定します。
※すべての GVRP対応ポートに適用されます。

GVRP Configuration



〈Refresh〉 …… 最新の状態に更新するボタンです。
※設定内容を変更したときは、変更前の状態に戻ります。

Enable GVRP …… システム全体でGVRPを有効にするかどうかを設定します。

Join-time …… Joinメッセージの送信間隔を設定します。
設定できる範囲は、「1～20」(×0.01秒)です。

Leave-time …… GARP状態でなくなるまで待つ時間を設定します。
設定できる範囲は、「60～300」(×0.01秒)です。

LeaveAll-time …… LeaveAllメッセージの送信間隔を設定します。
設定できる範囲は、「1000～5000」(×0.01秒)です。

Max VLANs …… GVRP が有効な場合に、GVRPがサポートする VLAN の最大数を指定します。
※設定を変更するときは、[Enable GVRP]欄を無効にしてください。

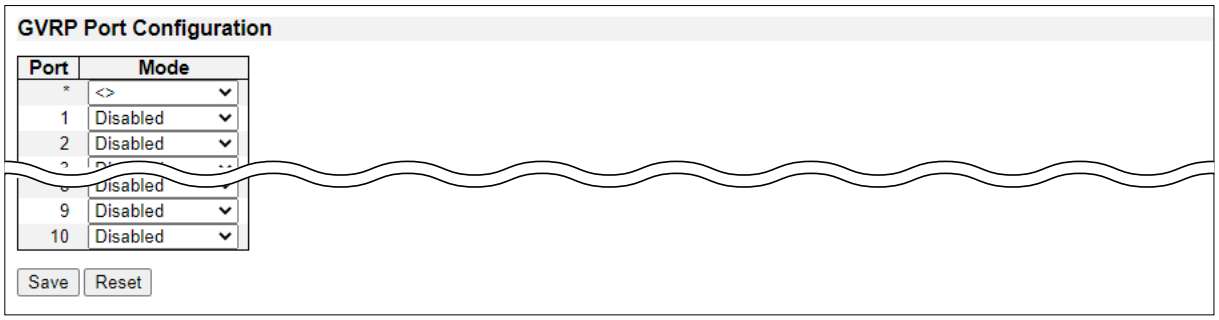
〈Save〉 …… 設定した内容を保存するボタンです。

「Port config」画面

Configuration > GVRP > Port Config

ポートごとに、GVRPについて設定します。

GVRP Port Configuration



Port …… 本製品のポート番号が表示されます。

Mode …… ポートごとに、GVRPを有効にするかどうかを設定します。

〈Save〉 …… 設定した内容を保存するボタンです。

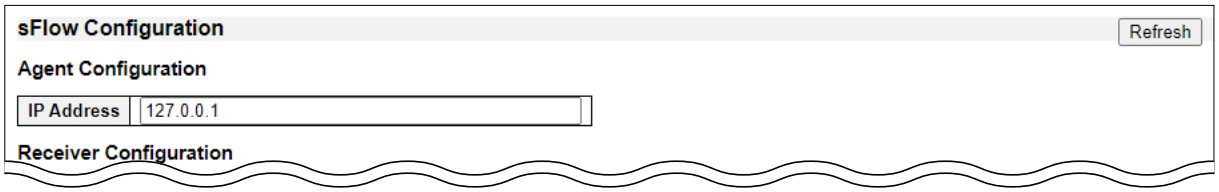
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「sFlow」画面

Configuration > sFlow

sFlowについて設定します。
sFlowレシーバー(sFlowコレクター)の設定と、ポートごとのフロー、およびカウンターサンプラーの設定があります。
sFlow設定は不揮発性メモリーに保存されないため、本製品を再起動するとsFlowサンプリングが無効になります。

sFlow Configuration



〈Refresh〉 …… 最新の状態に更新するボタンです。
※設定内容を変更したときは、変更前の状態に戻ります。

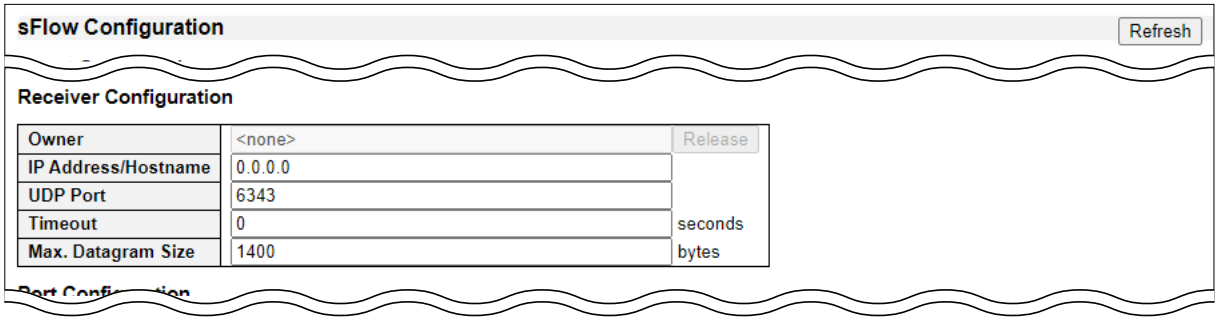
Agent Configuration

IP Address …… sFlowデータグラムに含まれるsFlowエージェントのIPアドレス(IPv4/IPv6)を設定します。
sFlowエージェントを識別するためのキーとして使用されます。

「sFlow」画面

Configuration > sFlow

sFlow Configuration



Receiver Configuration

Owner ……

sFlowはWebやCLIを使用したローカル管理、またはSNMPを使用する2つの方法で設定できます。
[Owner]欄には、現在のsFlowの所有者名が表示されます。

<none>：
sFlowを使用していない場合に表示されます。

<Configured through local management>：
Web、またはCLIを使用して設定されている場合に表示されます。

※SNMPを使用して設定されていると、sFlowコレクターを識別する文字列が表示されます。
SNMPを使用して設定されている場合は、不注意による再設定を避けるために、〈Release〉以外のすべての操作が無効になります。
※〈Release〉をクリックすると、現在の所有者を解放し、sFlowサンプリングを無効にできます。
sFlowを使用していない場合はクリックできません。
SNMPを使用して設定する前に、現在の所有者を確認してください。

IP Address/Hostname …… sFlowレシーバーのIPアドレス(IPv4/IPv6)、またはホスト名を設定します。

UDP Port…… sFlowレシーバーのsFlowデータグラム待ち受け用UDPポートの番号を設定します。
「0」に設定したときは、デフォルトのポート「6343」を使用します。

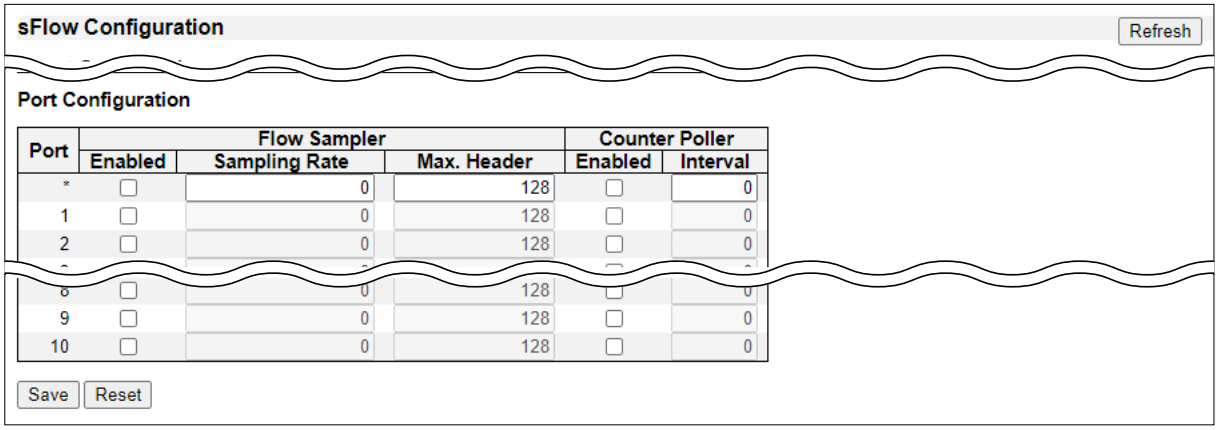
Timeout …… サンプリングを停止し、現在のsFlow所有者を解放するまでの残り時間が表示されます。
〈Refresh〉をクリックすると、残り時間の表示を更新できます。
ローカル管理の場合、動作中でも他の設定に影響を与えることなく残り時間を変更できます。
表示される範囲は、「0～2147483647」(秒)です。

Max. Datagram Size …… 1つのsFlowデータグラムで送信できるデータの最大サイズを設定します。
設定できる範囲は、「200～1468」(バイト)です。
※sFlowデータグラムがフラグメント化されない、十分な値に設定してください。

「sFlow」画面

Configuration > sFlow

sFlow Configuration



Port Configuration

Port …… 本製品のポート番号が表示されます。

Flow Sampler Enabled …… ポートで送受信されるデータをサンプリングするかどうかを設定します。

Flow Sampler Sampling Rate… データをサンプリングするときのサンプリングレートを設定します。
Nに設定すると、ポートで送受信されるパケットのうち平均Nパケットごとに1パケットがサンプリングされます。
設定できる範囲は、「1～4096」です。
※一部のサンプリングレートには対応していません。
対応していない値を設定すると、対応しているサンプリングレートのなかで最も近い値に自動調整されます。

Flow Sampler Max. Header…… サンプリングされたパケットからsFlowデータグラムにコピーするデータの最大サイズを設定します。
設定できる範囲は、「14～200」(バイト)です。
※フレームに十分なスペースを確保するために、[Max. Datagram Size]欄の設定を[Flow Sampler Max. Header]欄の設定より約100バイト大きくしてください。
[Max. Datagram Size]欄の設定が小さすぎると、サンプリングされたデータが破棄される場合があります。

Counter Poller Enabled…… カウンターポーリングを有効にするかどうかを設定します。

Counter Poller Interval…… カウンターポーリングを使用するときに場合、ポーリング間隔を設定します。
設定できる範囲は、「1～3600」(秒)です。

〈Save〉 …… 設定した内容を保存するボタンです。
※sFlow設定は不揮発性メモリーに保存されないため、本製品を再起動するとsFlowサンプリングが無効になります。

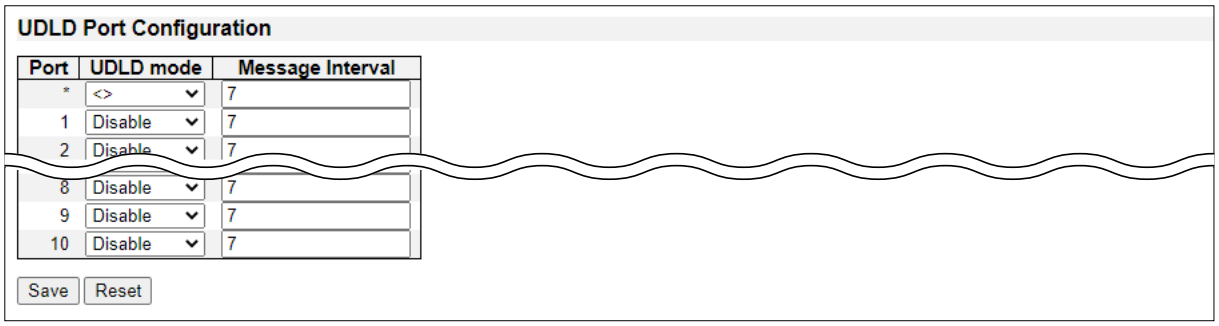
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「UDLD」画面

Configuration > UDLD

UDLD(Uni Directional Link Detection)について設定します。

UDLD Port Configuration



Port ……　本製品のポート番号が表示されます。

UDLD mode ……　UDLDモードを設定します。

Disable：
UDLDを無効にします。

Normal：
単一方向リンクを検出しても場合、ポートの状態を変更しません。

Aggressive：
単一方向リンクを検出したポートをシャットダウンします。
ポートを再起動するには、そのポートでUDLDを無効にしてください。

Message Interval ……　advertisementフェーズに移行して双方向リンク状態と判断されたポートの、UDLDプローブメッセージの送信間隔を設定します。
設定できる範囲は、「7～90」(秒)です。

〈Save〉 ……　設定した内容を保存するボタンです。

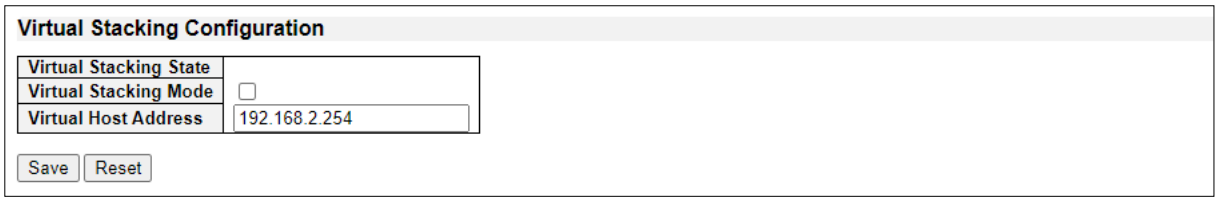
〈Reset〉 ……　設定内容を変更したとき、変更前の状態に戻すボタンです。

「Virtual Stack」画面

Configuration > Virtual Stack

Virtual Stacking機能について設定します。

Virtual Stacking Configuration



Virtual Stacking State …… 現在の状態が表示されます。

Virtual Stacking Mode …… Virtual Stacking機能を有効にするかどうかを設定します。

Virtual Host Address …… Virtual Stacking機能使用時に使用するIPアドレスを設定します。

〈Save〉 …… 設定した内容を保存するボタンです。

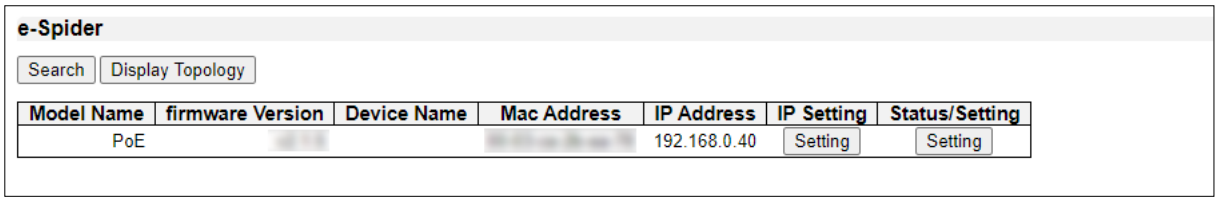
〈Reset〉 …… 設定内容を変更したとき、変更前の状態に戻すボタンです。

「e-Spider」画面

Configuration > e-Spider

本製品や接続されている装置の状態を一覧表示できます。

e-Spider



〈Search〉 …… ネットワーク検索を開始するボタンです。

〈Display Topology〉…… 現在のネットワークトポロジーを表示するボタンです。
「Display Topology」画面に移動します。

Model Name …… モデル名が表示されます。

firmware Version…… ファームウェアバージョンが表示されます。

Device Name…… デバイスの名称が表示されます。

Mac Address…… デバイスのMACアドレスが表示されます。

IP Address …… デバイスのIPアドレスが表示されます。

IP Setting …… 〈Setting〉をクリックすると、「IP Setting」画面に移動します。

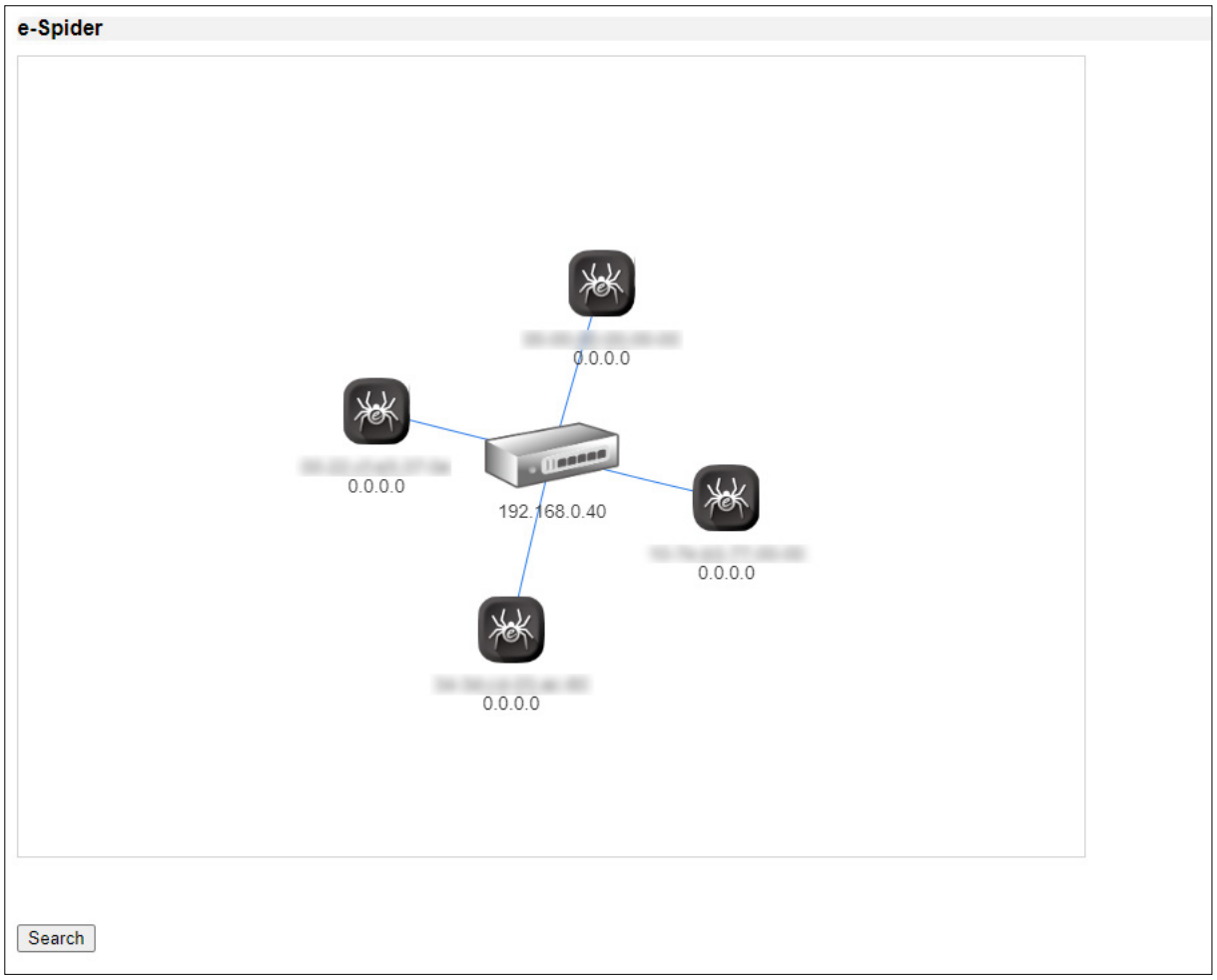
Status/Setting…… 〈Setting〉をクリックすると、「Status/Setting」画面に移動します。

「Display Topology」画面

Configuration > e-Spider

現在のネットワークトポロジーが表示されます。

e-Spider



〈Search〉 …… ネットワークトポロジーを更新するボタンです。

「IP Setting」画面

Configuration > e-Spider

IPアドレスについて設定します。

e-Spider

MAC Address …… MACアドレスが表示されます。

IP Address …… IPアドレスを設定します。

NetMask …… サブネットマスクを設定します。

Gateway …… デフォルトゲートウェイを設定します。

〈Save〉 …… 設定した内容を保存するボタンです。

〈Cancel〉 …… 設定内容を変更したとき、変更前の状態に戻し、「e-Spider」画面に戻るボタンです。

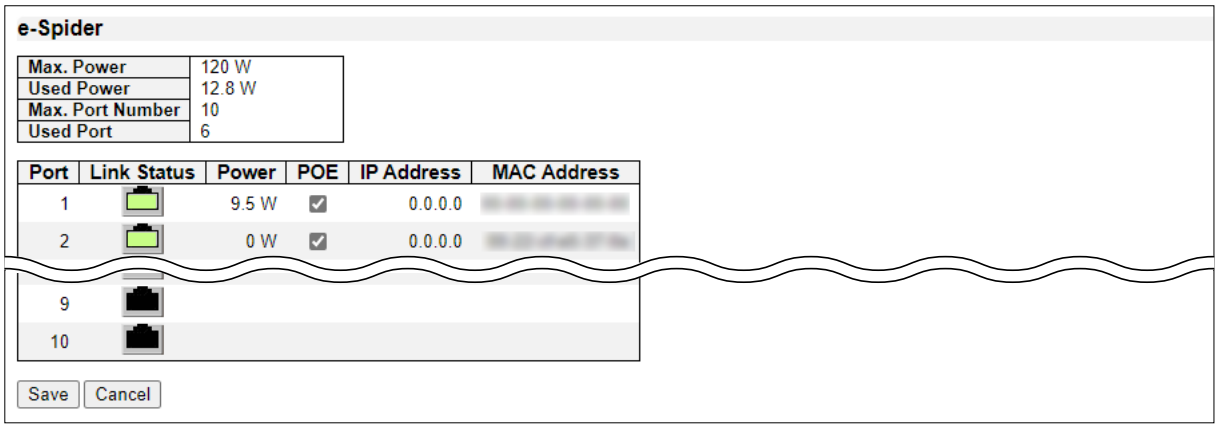
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Status/Setting」画面

Configuration > e-Spider

ポートのPoE状態について確認したり、設定したりします。

e-Spider



Max. Power ……　電源装置の最大供給電力が表示されます。

Used Power ……　接続している機器全体の消費電力が表示されます。

Max. Port Number ……　PoE非対応ポートを含む、本製品で使用できるポート数が表示されます。

Used Port ……　使用中のポート数が表示されます。

Port ……　本製品のポート番号が表示されます。

Link Status ……　ポートの状態が表示されます。

Power ……　PoE機能使用時に、接続している機器の消費電力が表示されます。

POE ……　PoE機能が有効か無効かが表示されます。
クリックして設定を変更できます。

IP Address ……　接続している機器のIPアドレスが表示されます。

MAC Address ……　接続している機器のMACアドレスが表示されます。

〈Save〉 ……　設定した内容を保存するボタンです。

〈Cancel〉 ……　設定内容を変更したとき、変更前の状態に戻し、「e-Spider」画面に戻るボタンです。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

3章 Monitorメニュー

「Information」画面 …… 3-5
System Information …… 3-5

「CPU Load」画面 …… 3-6
CPU Load …… 3-6

「IP Status」画面 …… 3-7
IP Interfaces …… 3-7
IP Routes …… 3-7
Neighbour cache …… 3-8

「Log」画面 …… 3-9
System Log Information …… 3-9

「Detailed Log」画面 …… 3-10
Detailed System Log Information …… 3-10
Message …… 3-10

「Port Power Savings」画面 …… 3-11
Port Power Savings Status …… 3-11

「Traffic Overview」画面 …… 3-12
Port Statistics Overview …… 3-12

「QoS Statistics」画面 …… 3-13
Queuing Counters …… 3-13

「QCL Status」画面 …… 3-14
QoS Control List Status …… 3-14

「Detailed Statistics」画面 …… 3-15
Detailed Port Statistics Port 1～10 …… 3-15

「Statistics」画面 …… 3-17
DHCP Server Statistics …… 3-17

「Binding」画面 …… 3-19
DHCP Server Binding IP …… 3-19

「Declined IP」画面 …… 3-20
DHCP Server Declined IP …… 3-20

「Snooping Table」画面 …… 3-21
Dynamic DHCP Snooping Table …… 3-21

「Relay Statistics」画面 …… 3-22
DHCP Relay Statistics …… 3-22

「Detailed Statistics」画面 …… 3-24
DHCP Detailed Statistics Port 1～10 …… 3-24

「Snooping Table」画面 …… 3-26
DHCPv6 Snooping Table …… 3-26

「Snooping Statistics」画面 …… 3-27
DHCPv6 Snooping Statistics …… 3-27

「Relay」画面 …… 3-28
DHCPv6 Relay Status and Statistics …… 3-28

「Access Management Statistics」画面 …… 3-29
Access Management Statistics …… 3-29

「Overview」画面 …… 3-30
Port Security Switch Status …… 3-30

「Details」画面 …… 3-33

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

下記は、前ページからのつづきです。

Port Security Port Status Port 1～10 …… 3-33
「Switch」画面 …… 3-34
Network Access Server Switch Status …… 3-34
「Port」画面 …… 3-35
NAS Statistics Port 1～10 …… 3-35
「ACL Status」画面 …… 3-41
ACL Status …… 3-41
「ARP Inspection」画面 …… 3-43
Dynamic ARP Inspection Table …… 3-43
「IP Source Guard」画面 …… 3-44
Dynamic IP Source Guard Table …… 3-44
「IPv6 Source Guard」画面 …… 3-45
IPv6 Source Guard Dynamic Table …… 3-45
「RADIUS Overview」画面 …… 3-46
RADIUS Server Status Overview …… 3-46
「RADIUS Details」画面 …… 3-47
RADIUS Authentication Statistics for Server #1～5 …… 3-47
RADIUS Accounting Statistics for Server #1～10 …… 3-50
「Statistics」画面 …… 3-52
RMON Statistics Status Overview …… 3-52
「Detailed RMON Statistics」画面 …… 3-54
Detailed RMON Statistics ID n …… 3-54
「History」画面 …… 3-56
RMON History Overview …… 3-56
「Detailed RMON History」画面 …… 3-58
Detailed RMON History ID n …… 3-58
「Alarm」画面 …… 3-59
RMON Alarm Overview …… 3-59
「Detailed RMON Alarm」画面 …… 3-60
Detailed RMON Alarm ID n …… 3-60
「Event」画面 …… 3-61
RMON Event Overview …… 3-61
「Detailed RMON Event」画面 …… 3-62
Detailed RMON Event ID n …… 3-62
「Status」画面 …… 3-63
Aggregation Status …… 3-63
「System Status」画面 …… 3-64
LACP System Status …… 3-64
「Internal Status」画面 …… 3-65
LACP Internal Port Status …… 3-65
「Neighbor Status」画面 …… 3-66
LACP Neighbor Port Status …… 3-66
「Port Statistics」画面 …… 3-68
LACP Statistics …… 3-68

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

下記は、前ページからのつづきです。

「Loop Protection」画面 …… 3-69
Loop Protection Status …… 3-69
「Bridge Status」画面 …… 3-70
STP Bridges …… 3-70
「STP Detailed Bridge Status」画面 …… 3-71
STP Detailed Bridge Status …… 3-71
「Port Status」画面 …… 3-73
STP Port Status …… 3-73
「Port Statistics」画面 …… 3-74
STP Statistics …… 3-74
「Statistics」画面 …… 3-75
MVR Statistics …… 3-75
「MVR Channel Groups」画面 …… 3-76
MVR Channels (Groups) Information …… 3-76
「MVR SFM Information」画面 …… 3-77
MVR SFM Information …… 3-77
「Status」画面 …… 3-78
IGMP Snooping Status …… 3-78
「Groups Information」画面 …… 3-79
IGMP Snooping Group Information …… 3-79
「IPv4 SFM Information」画面 …… 3-80
IGMP SFM Information …… 3-80
「Status」画面 …… 3-81
MLD Snooping Status …… 3-81
「Groups Information」画面 …… 3-82
MLD Snooping Group Information …… 3-82
「IPv6 SFM Information」画面 …… 3-83
IGMP SFM Information …… 3-83
「Neighbors」画面 …… 3-84
LLDP Neighbor Information …… 3-84
「LLDP-MED Neighbors」画面 …… 3-85
LLDP-MED Neighbor Information …… 3-85
「PoE」画面 …… 3-89
LLDP Neighbor Power Over Ethernet Information …… 3-89
「EEE」画面 …… 3-90
LLDP Neighbors EEE Information …… 3-90
「Port Statistics」画面 …… 3-92
LLDP Global Counters …… 3-92
LLDP Statistics Local Counters …… 3-93
「PoE」画面 …… 3-94
Power Over Ethernet Status …… 3-94
「MAC Table」画面 …… 3-96
MAC Address Table …… 3-96
「Membership」画面 …… 3-97
VLAN Membership Status for Combined users …… 3-97

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

下記は、前ページからのつづきです。

「Ports」画面…… 3-98
VLAN Port Status for Combined users …… 3-98
「MVRP」画面 …… 3-99
MVRP Statistics …… 3-99
「sFlow」画面 …… 3-100
sFlow Statistics …… 3-100
「UDLD」画面 …… 3-102
Detailed UDLD Status for Port 1～10 …… 3-102
Neighbour Status …… 3-102

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Information」画面

Monitor > System > Information

本製品のシステム情報が表示されます。

System Information

Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

System

Contact ……　管理対象ノードの連絡先が表示されます。
※「Configuration」→「System」→「Information」画面の[System Contact]欄で設定した内容が表示されます。

Name ……　管理対象ノードのシステム名称が表示されます。
※「Configuration」→「System」→「Information」画面の[System Name]欄で設定した内容が表示されます。

Location ……　管理対象ノードの場所が表示されます。
※「Configuration」→「System」→「Information」画面の[Location]欄で設定した内容が表示されます。

Hardware

MAC Address ……　本製品のMACアドレスが表示されます。

Time

System Date ……　本製品に設定されている時刻(GMT：グリニッジ標準時)が表示されます。
時刻は、本製品に登録されたタイムサーバーから取得します。

System Uptime ……　本製品の運用時間が表示されます。

Software

Software Version ……　本製品のソフトウェアバージョンが表示されます。

Software Date ……　本製品のソフトウェアの作成日が表示されます。

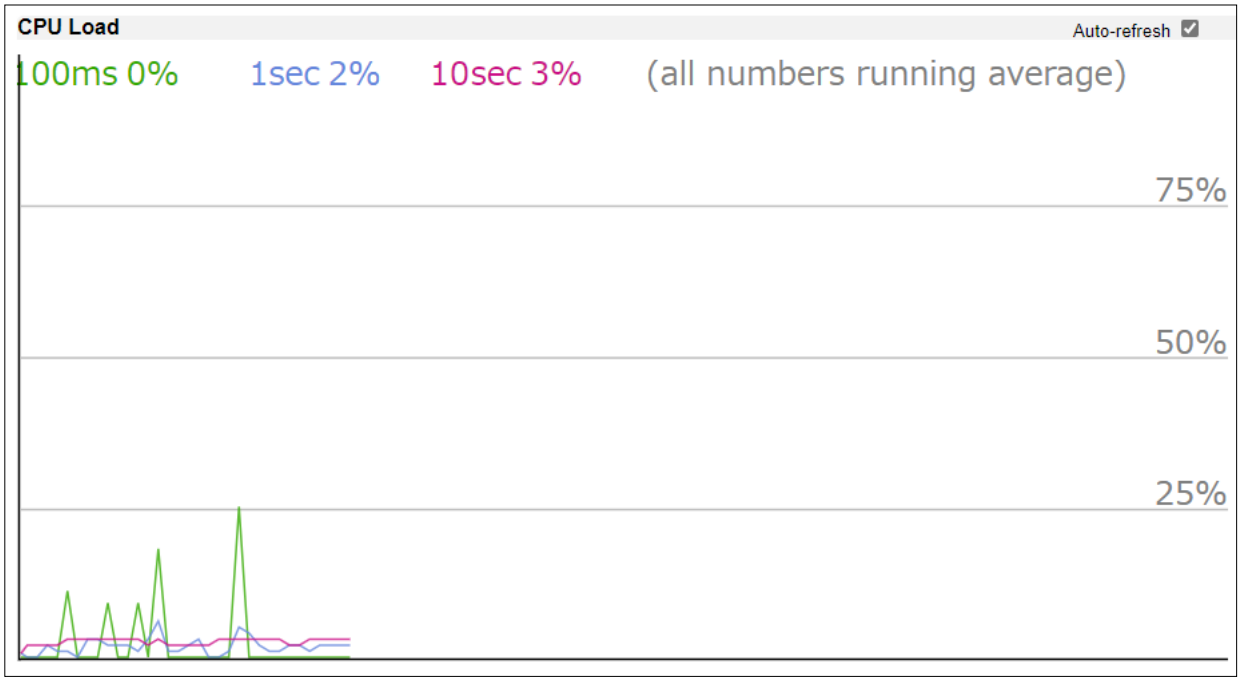
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「CPU Load」画面

Monitor > System > CPU Load

CPU負荷率が表示されます。
CPU負荷率は、過去100ミリ秒、1秒、10秒の平均を測定しています。
直近120個のサンプルがグラフ化され、直近の数値もテキストで表示されます。
※CPU負荷率の表示には、SVGグラフを使用しています。
　SVGグラフを表示するには、ご使用になるWWWブラウザーがSVG形式をサポートしている必要があります。

CPU Load



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

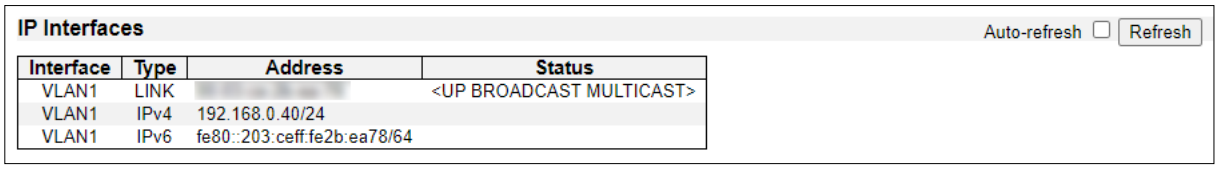
三和システムサービス株式会社
〒330-0854　埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211　FAX 048-653-2217

「IP Status」画面

Monitor > System > IP Status

IPプロトコル層のステータス(IPインターフェース、IPルート、ネイバーキャッシュ(ARPキャッシュ)ステータス)が表示されます。

IP Interfaces



Auto-refresh ····· 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ····· 最新の状態に更新するボタンです。

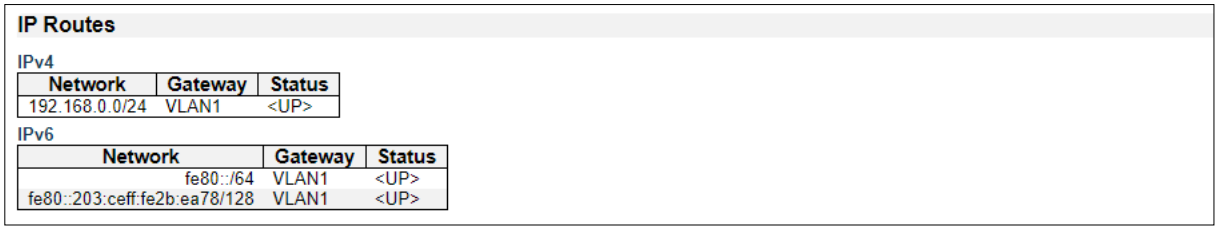
Interface ····· インターフェース名が表示されます。

Type ····· アドレスの種類が表示されます。

Address ····· インターフェースのアドレスが表示されます。

Status ····· インターフェース(アドレス)の状態が表示されます。

IP Routes



Network ····· IPルートの宛先IPネットワークアドレス、またはホストアドレスが表示されます。

Gateway ····· IPルートのゲートウェイアドレスが表示されます。

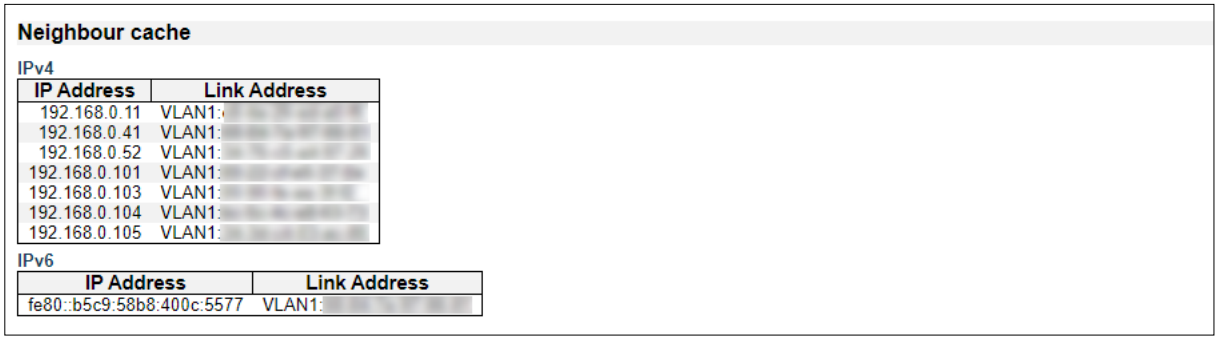
Status ····· IPルートの状態が表示されます。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「IP Status」画面

Monitor > System > IP Status

Neighbour cache



IP Address…… ネイバーのIPアドレスが表示されます。

Link Address…… IPアドレスにバインドされたリンクアドレス(MACアドレス)が表示されます。

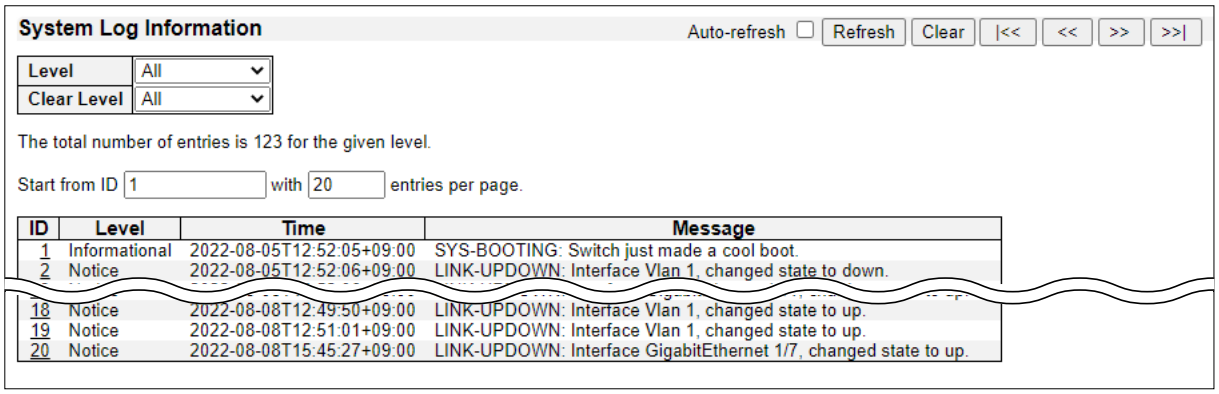
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Log」画面

Monitor > System > Log

システムログ情報が表示されます。

System Log Information



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈Clear〉 ……　[Clear Level]欄で選択した種類のログを削除するボタンです。

〈|<<〉 ……　最初のページに戻るボタンです。

〈<<〉 ……　前のページに戻るボタンです。

〈>>〉 ……　次のページに進むボタンです。

〈>>|〉 ……　最後のページに進むボタンです。

Level ……　表示するログの種類を選択します。

Clear Level ……　〈Clear〉をクリックしたときに、削除するログの種類を選択します。

Start from ID [ID] with [表示数] entries per page.
……　ページの表示設定です。
システムログのうち、IDの一番小さいエントリがはじめに表示されます。
[ID]欄で、はじめに表示するシステムログのIDを指定できます。
[表示数]欄で1ページあたりの表示数を指定できます。（最大999件まで）

ID ……　システムログのIDが表示されます。
各IPのリンク先をクリックすると、「Detailed Log」画面へ移動します。

Level ……　システムログの重大度コードが表示されます。

Time ……　システムログの発生日時が表示されます。

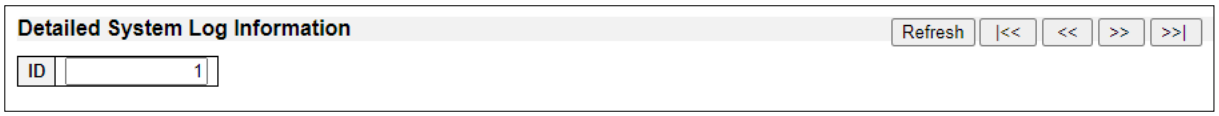
Message ……　システムログの詳細メッセージが表示されます。

「Detailed Log」画面

Monitor > System > Detailed Log

システムログの詳細情報が表示されます。

Detailed System Log Information



〈Refresh〉 …… 最新の状態に更新するボタンです。

〈|<<〉 …… 最初のシステムログを表示するボタンです。

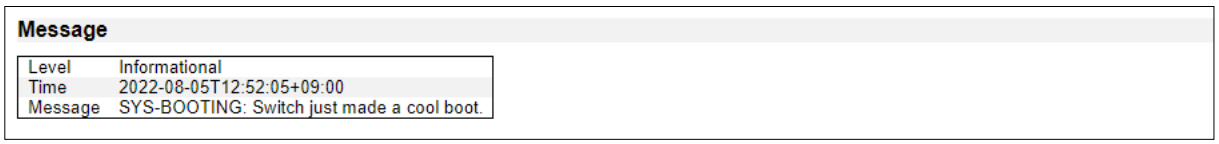
〈<<〉 …… 1つ前のシステムログを表示するボタンです。

〈>>〉 …… 1つ次のシステムログを表示するボタンです。

〈>>|〉 …… 最後のシステムログを表示するボタンです。

ID …… 表示するシステムログのIDを入力します。
〈Refresh〉をクリックすると、入力したIDのシステムログが表示されます。

Message



Level …… システムログの重大度コードが表示されます。

Time …… システムログの発生日時が表示されます。

Message …… システムログの詳細メッセージが表示されます。

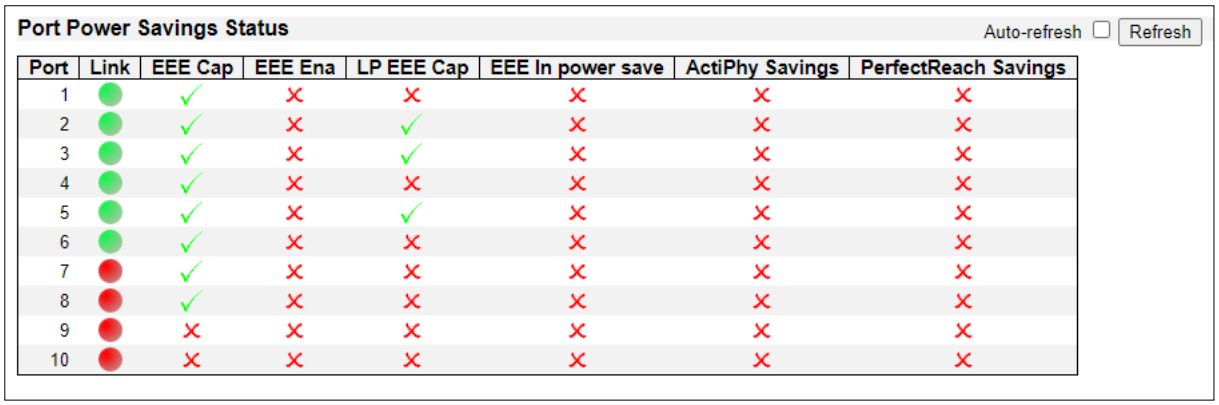
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Port Power Savings」画面

Monitor > Green Ethernet > Port Power Savings

EEE機能の使用状況が表示されます。

Port Power Savings Status



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

Port ……　本製品のポート番号が表示されます。

Link ……　現在のリンク状態が表示されます。
緑：リンク中
赤：リンクダウン

EEE Cap ……　EEE機能に対応しているかが表示されます。

EEE Ena ……　EEE機能が有効かどうかが表示されます。
※EEE機能については、「Port Power Saving」画面で設定します。

LP EEE Cap ……　接続する機器がEEE機能に対応しているかが表示されます。

EEE In power save ……　EEE機能によって、省電力モードになっているかが表示されます。
EEE機能を使用している場合、5マイクロ秒間フレームの送受信がなかったときに省電力モードに切り替わります。

ActiPhy Savings ……　AntiPHY機能によって、省電力モードになっているかが表示されます。

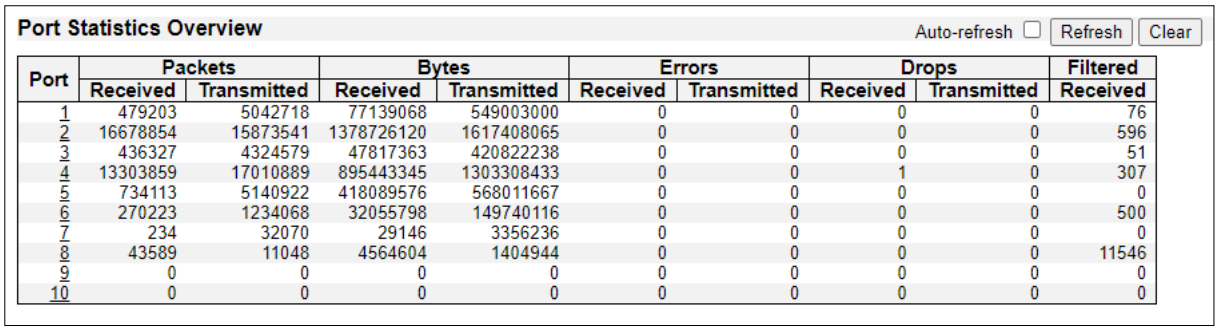
PerfectReach Savings ……　PerfectReach機能によって、省電力モードになっているかが表示されます。

「Traffic Overview」画面

Monitor > Ports > Traffic Overview

本製品のポートのトラフィック統計が表示されます。

Port Statistics Overview



Port Statistics Overview

Auto-refresh ☐ Refresh Clear

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	479203	5042718	77139068	549003000	0	0	0	0	76
2	16678854	15873541	1378726120	1617408065	0	0	0	0	596
3	436327	4324579	47817363	420822238	0	0	0	0	51
4	13303859	17010889	895443345	1303308433	0	0	1	0	307
5	734113	5140922	418089576	568011667	0	0	0	0	0
6	270223	1234068	32055798	149740116	0	0	0	0	500
7	234	32070	29146	3356236	0	0	0	0	0
8	43589	11048	4564604	1404944	0	0	0	0	11546
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0

Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈Clear〉 ……　すべてのポートのカウンター値を0にするボタンです。

Port ……　本製品のポート番号が表示されます。
各ポート番号のリンク先をクリックすると、「Detailed Statistic」画面へ移動します。（P.3-15）

Packets Received/Transmitted …　受信パケット数と送信パケット数が表示されます。

Bytes Received/Transmitted ……　受信バイト数と送信バイト数が表示されます。

Errors Received/Transmitted ……　受信エラーのフレーム数と送信エラーのフレーム数が表示されます。

Drops Received/Transmitted ……　受信時、または送信時に輻輳（ふくそう）が原因で破棄されたフレーム数が表示されます。

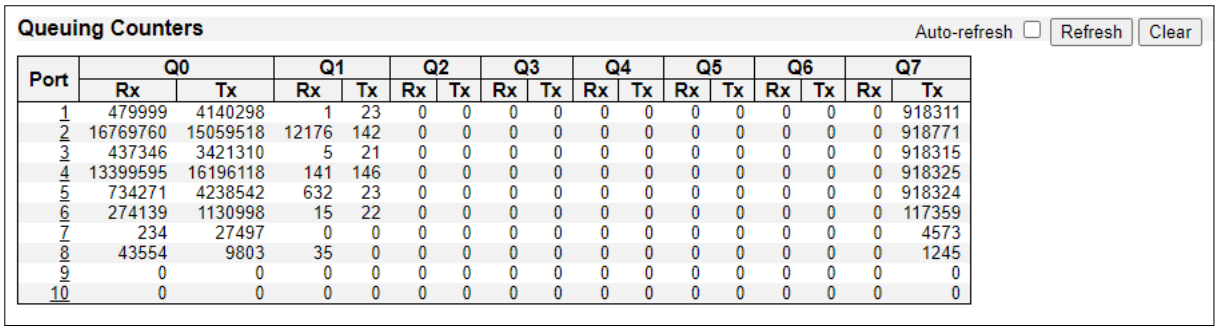
Filtered Received ……　転送時にフィルタリングされた受信フレーム数が表示されます。

「QoS Statistics」画面

Monitor > Ports > QoS Statistics

すべてのポートのキューについて、統計情報が表示されます。

Queuing Counters



Queuing Counters　Auto-refresh ☐ Refresh Clear

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	479999	4140298	1	23	0	0	0	0	0	0	0	0	0	0	0	918311
2	16769760	15059518	12176	142	0	0	0	0	0	0	0	0	0	0	0	918771
3	437346	3421310	5	21	0	0	0	0	0	0	0	0	0	0	0	918315
4	13399595	16196118	141	146	0	0	0	0	0	0	0	0	0	0	0	918325
5	734271	4238542	632	23	0	0	0	0	0	0	0	0	0	0	0	918324
6	274139	1130998	15	22	0	0	0	0	0	0	0	0	0	0	0	117359
7	234	27497	0	0	0	0	0	0	0	0	0	0	0	0	0	4573
8	43554	9803	35	0	0	0	0	0	0	0	0	0	0	0	0	1245
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈Clear〉 ……　すべてのポートのカウンター値を0にするボタンです。

Port ……　本製品のポート番号が表示されます。
各ポート番号のリンク先をクリックすると、「Detailed Statistic」画面へ移動します。（P.3-15）

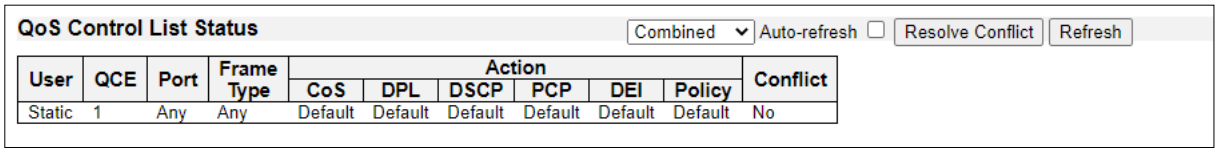
Q0～7 Rx/Tx ……　QoSキューごとに送受信パケット数が表示されます。
※Q0は優先順位が最も低いキューです。

「QCL Status」画面

Monitor > Ports > QCL Status

ドロップダウンリストで選択したQCLユーザーの、QCL状態が表示されます。
各行には、QoSコントロールリスト(QCL)を構成するQoSコントロールエントリ(QCE)が表示されます。
QCEは最大256件まで登録できます。
ハードウェアの制限が原因で、特定のQCEが適用できない場合があります。(競合)

QoS Control List Status



Auto-refresh ····· 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Resolve Conflict〉 ····· QCEの追加に必要なリソースを解放するボタンです。
[Conflict]欄が「Yes」の場合に有効です。

〈Refresh〉 ····· 最新の状態に更新するボタンです。

User ····· QCLユーザーが表示されます。

QCE ····· QCE IDが表示されます。

Port ····· QCEを適用するポートが表示されます。

Frame Type ····· 条件となるフレームの種類が表示されます。

Action

CoS ····· QCEに一致するフレームを受信したとき、表示されているCoS(Class of Servise)値に分類します。

DPL ····· QCEに一致するフレームを受信したとき、表示されているDPL(Drop Precedence Level)値に分類します。

DSCP ····· QCEに一致するフレームを受信したとき、表示されているDSCP値に分類します。

PCP ····· QCEに一致するフレームを受信したとき、表示されているPCP値に分類します。

DEI ····· QCEに一致するフレームを受信したとき、表示されているDEI値に分類します。

Policy ····· QCEに一致するフレームを受信したとき、表示されているACLポリシー番号に分類します。

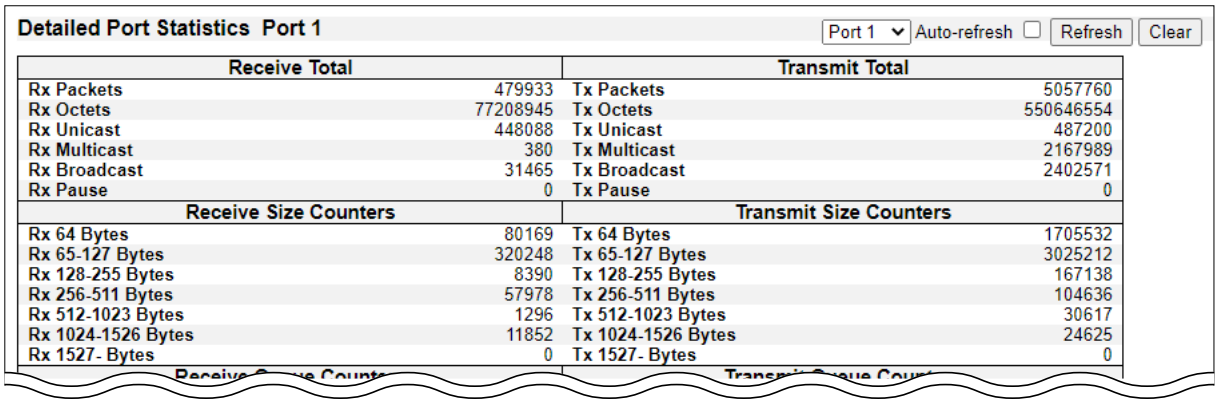
Conflict ····· QCEが競合しているかどうかが表示されます。
ハードウェアリソースを複数のアプリケーションで共有しているため、QCEの追加に必要なリソースが使用できない場合があります。(競合)
競合が発生している場合は「Yes」と表示され、それ以外の場合は「No」と表示されます。
〈Resolve Conflict〉をクリックすると、QCEを追加するために必要なハードウェアリソースが解放され、競合を解決できます。

「Detailed Statistics」画面

Monitor > Ports > Detailed Statistics

ドロップダウンリストから選択したポートの、詳細なトラフィック統計が表示されます。

Detailed Port Statistics Port 1～10



Detailed Port Statistics Port 1

Port 1 Auto-refresh Refresh Clear

Receive Total		Transmit Total	
Rx Packets	479933	Tx Packets	5057760
Rx Octets	77208945	Tx Octets	550646554
Rx Unicast	448088	Tx Unicast	487200
Rx Multicast	380	Tx Multicast	2167989
Rx Broadcast	31465	Tx Broadcast	2402571
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	80169	Tx 64 Bytes	1705532
Rx 65-127 Bytes	320248	Tx 65-127 Bytes	3025212
Rx 128-255 Bytes	8390	Tx 128-255 Bytes	167138
Rx 256-511 Bytes	57978	Tx 256-511 Bytes	104636
Rx 512-1023 Bytes	1296	Tx 512-1023 Bytes	30617
Rx 1024-1526 Bytes	11852	Tx 1024-1526 Bytes	24625
Rx 1527- Bytes	0	Tx 1527- Bytes	0

Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈Clear〉 ……　表示されているポートのカウンター値を0にするボタンです。

Receive Total/Transmit Total

Rx Packets/Tx Packets ……　受信パケット数と送信パケット数が表示されます。

Rx Octets/Tx Octets ……　受信バイト数と送信バイト数が表示されます。
FCSフィールドは含まれますが、フレーミングビットは含まれません。

Rx Unicast/Tx Unicast……　受信したユニキャストパケット数と送信したユニキャストパケット数が表示されます。

Rx Multicast/Tx Multicast ……　受信したマルチキャストパケット数と送信したマルチキャストパケット数が表示されます。

Rx Broadcast/Tx Broadcast …　受信したブロードキャストパケット数と送信したブロードキャストパケット数が表示されます。

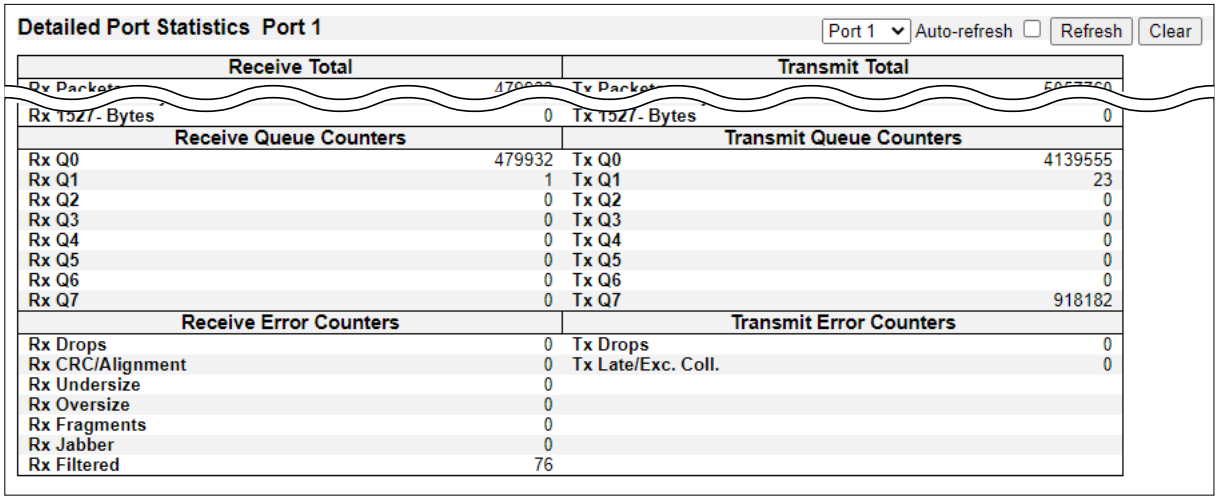
Rx Pause/Tx Pause ……　送受信したMAC制御フレームのうち、PAUSEコマンドが含まれるフレームの数が表示されます。

Receive Size Counters/Transmit Size Counters
……　送受信したパケットの数がフレーム長ごとに表示されます。

「Detailed Statistics」画面

Monitor > Ports > Detailed Statistics

Detailed Port Statistics Port 1～10



Detailed Port Statistics Port 1

Port 1 | Auto-refresh | Refresh | Clear

Receive Total		Transmit Total	
Rx Packets	479932	Tx Packets	5063760
Rx 1527 - Bytes	0	Tx 1527 - Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	479932	Tx Q0	4139555
Rx Q1	1	Tx Q1	23
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	918182
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	76		

Receive Queue Counters/Transmit Queue Counters

……　送受信したパケットの数がキューごとに表示されます。

Receive Error Counters

Rx Drops……　受信バッファーの不足、または輻輳(ふくそう)が原因で破棄されたフレームの数が表示されます。

Rx CRC/Alignment……　CRCエラー、またはアライメントエラーが検出された受信フレーム数が表示されます。

Rx Undersize……　有効なCRCを含む64バイト未満の受信フレーム数が表示されます。

Rx Oversize ……　有効なCRCを含み、ポートに設定された最大フレーム長よりも長い受信フレーム数が表示されます。

Rx Fragments ……　無効なCRCを含む64バイト未満の受信フレーム数が表示されます。

Rx Jabber ……　無効なCRCを含み、ポートに設定された最大フレーム長よりも長い受信フレーム数が表示されます。

Rx Filtered ……　転送時にフィルタリングされた受信フレーム数が表示されます。

Transmit Error Counters

Tx Drops……　送信バッファーの輻輳(ふくそう)が原因で破棄されたフレーム数が表示されます。

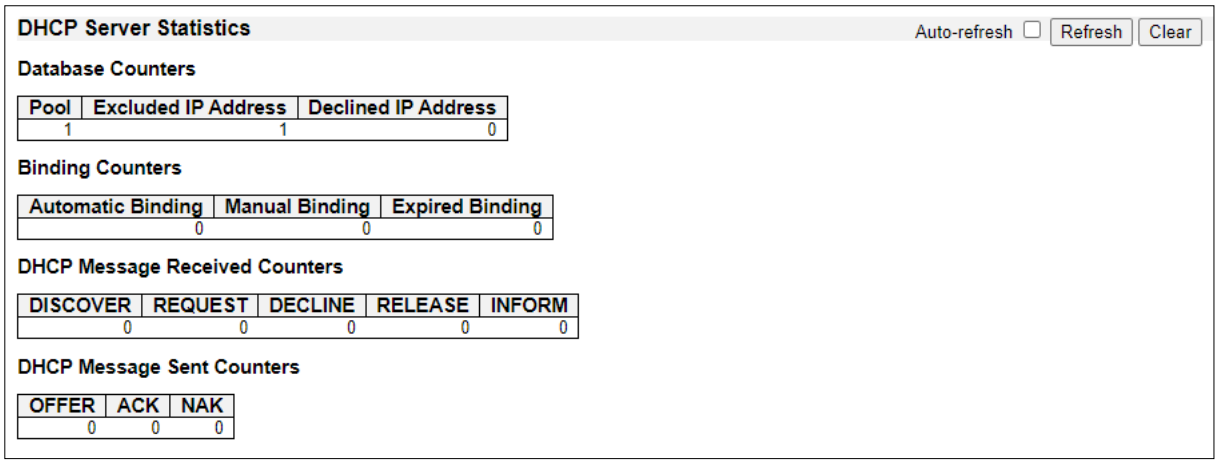
Tx Late/Exc. Coll. ……　過度の衝突、または遅延が原因で破棄されたフレーム数が表示されます。

「Statistics」画面

Monitor > DHCPv4 > Server > Statistics

DHCPデータベースカウンターと、DHCPサーバーが送受信するDHCPメッセージのカウンターが表示されます。

DHCP Server Statistics



Auto-refresh …… 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 …… 最新の状態に更新するボタンです。

〈Clear〉 …… 「DHCP Message Received Counters」と「DHCP Message Sent Counters」を0にするボタンです。

Database Counters

Pool …… 登録したDHCPアドレスプールの数が表示されます。

Excluded IP Address …… 登録した割り当てを除外するIPアドレス範囲の数が表示されます。

Declined IP Address …… DHCPクライアントから拒否されたIPアドレスの数が表示されます。

Binding Counters

Automatic Binding …… NetworkタイプのDHCPプールにバインディングされたクライアント数が表示されます。

Manual Binding …… HostタイプのDHCPプールにバインディングされたクライアント数が表示されます。
※HostタイプのDHCPプールは、特定のクライアントにIPアドレスを割り当てるときに使用します。

Expired Binding …… リース期間切れや、自動バインディングや手動バインディングから削除されたクライアント数が表示されます。

「Statistics」画面

Monitor > DHCPv4 > Server > Statistics

DHCP Server Statistics

DHCP Message Received Counters

DISCOVER …… 受信したDHCP DISCOVERメッセージ数が表示されます。

REQUEST …… 受信したDHCP REQUESTメッセージ数が表示されます。

DECLINE …… 受信したDHCP DECLINEメッセージ数が表示されます。

RELEASE …… 受信したDHCP RELEASEメッセージ数が表示されます。

INFORM …… 受信したDHCP INFORMメッセージ数が表示されます。

DHCP Message Sent Counters

OFFER …… 送信したDHCP OFFERメッセージ数が表示されます。

ACK …… 送信したDHCP ACKメッセージ数が表示されます。

NAK …… 送信したDHCP NAKメッセージ数が表示されます。

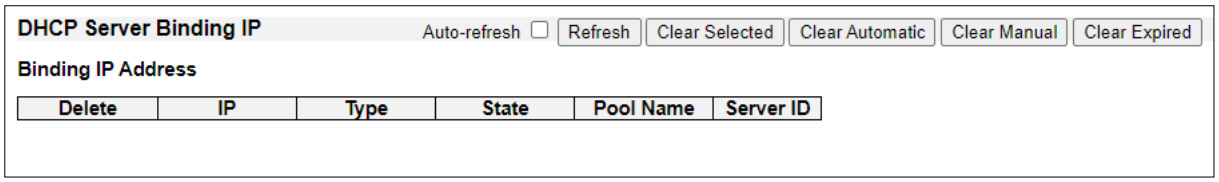
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Binding」画面

Monitor > DHCPv4 > Server > Binding

DHCPクライアントのバインディング状態が表示されます。

DHCP Server Binding IP



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈Clear Selected〉 ……　選択したバインディングを削除するボタンです。
自動バインディングと手動バインディングは期限切れに変更されます。
期限切れのバインディングはデータベースから削除されます。

〈Clear Automatic〉 ……　すべての自動バインディングを削除し、期限切れに変更するボタンです。

〈Clear Manual〉 ……　すべての手動バインディングを削除し、期限切れに変更するボタンです。

〈Clear Expired〉 ……　すべての期限切れのバインディングをデータベースから削除するボタンです。

Binding IP Address

Delete ……　登録された内容を削除するとき、ボックスにチェックマークを入れます。

IP ……　DHCPクライアントに割り当てられたIPアドレスが表示されます。

Type ……　バインディングタイプが「Automatic」(自動)、「Manual」(手動)、「Expired」(期限切れ)で表示されます。

State ……　バインド状態が「Committed」(コミット済み)、「Allocated」(割り当て済み)、「Expired」(期限切れ)で表示されます。

Pool Name ……　DHCPクライアントに使用しているDHCPプールが表示されます。

Server ID ……　DHCPバインディングを処理するサーバーのIPアドレスが表示されます。

「Declined IP」画面

Monitor > DHCPv4 > Server > Declined IP

DHCPクライアントから拒否されたIPアドレスが表示されます。

DHCP Server Declined IP

Auto-refresh …… 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 …… 最新の状態に更新するボタンです。

Declined IP Address

Declined IP…… DHCPクライアントから拒否されたIPアドレスが表示されます。

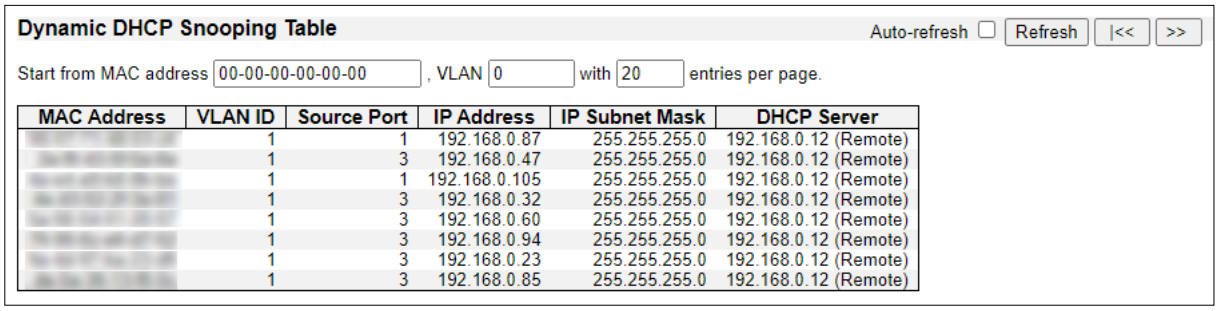
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Snooping Table」画面

Monitor > DHCPv4 > Snooping Table

DHCPv4スヌーピングテーブルが表示されます。
テーブルには、DHCPサーバーから動的IPアドレスを取得したすべてのDHCPクライアントが表示されます。（ローカルVLANインターフェースIPアドレスを除く）

Dynamic DHCP Snooping Table



MAC Address	VLAN ID	Source Port	IP Address	IP Subnet Mask	DHCP Server
[illegible]	1	1	192.168.0.87	255.255.255.0	192.168.0.12 (Remote)
[illegible]	1	3	192.168.0.47	255.255.255.0	192.168.0.12 (Remote)
[illegible]	1	1	192.168.0.105	255.255.255.0	192.168.0.12 (Remote)
[illegible]	1	3	192.168.0.32	255.255.255.0	192.168.0.12 (Remote)
[illegible]	1	3	192.168.0.60	255.255.255.0	192.168.0.12 (Remote)
[illegible]	1	3	192.168.0.94	255.255.255.0	192.168.0.12 (Remote)
[illegible]	1	3	192.168.0.23	255.255.255.0	192.168.0.12 (Remote)
[illegible]	1	3	192.168.0.85	255.255.255.0	192.168.0.12 (Remote)

Start from MAC address[MAC address], VLAN [VLAN ID] with[表示数] entries per page. ……
ページ表示の設定です。
[MAC Address]欄と[VLAN ID]欄で、DHCPスヌーピングテーブルの表示開始位置を指定できます。
[表示数]欄で1ページあたりの表示数を指定できます。（最大99件まで）

Auto-refresh …… 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 …… 最新の状態に更新するボタンです。

〈|<<〉 …… 最初のページに戻るボタンです。

〈>>〉 …… 次のページに進むボタンです。

MAC Address …… ユーザーMACアドレスが表示されます。

VLAN ID …… DHCPトラフィックが許可されているVLAN IDが表示されます。

Source Port …… 本製品の送信元ポート番号が表示されます。

IP Address …… ユーザーIPアドレスが表示されます。

IP Subnet Mask …… ユーザーIPアドレスのサブネットマスクが表示されます。

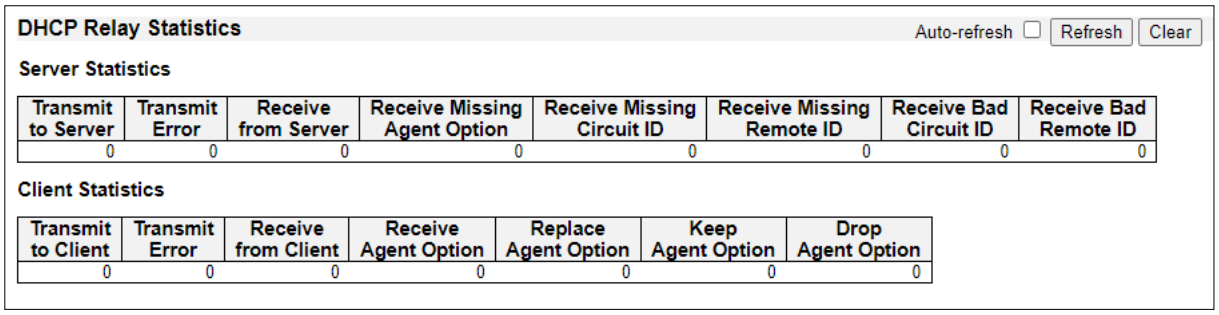
DHCP Server …… クライアントにIPアドレスを割り当てたDHCPサーバーのアドレスが表示されます。

「Relay Statistics」画面

Monitor > DHCPv4 > Relay Statistics

DHCPリレーの統計情報が表示されます。

DHCP Relay Statistics



Auto-refresh ····· 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ····· 最新の状態に更新するボタンです。

〈Clear〉 ····· すべての統計情報を削除するボタンです。

Server Statistics

Transmit to Server····· クライアントからサーバーに中継されたパケット数が表示されます。

Transmit Error ····· クライアントへの送信中にエラーが発生したパケット数が表示されます。

Receive from Server ····· サーバーから受信したパケット数が表示されます。

Receive Missing Agent Option··· 受信パケットのうち、リレーエージェント情報オプションを含まないパケット数が表示されます。

Receive Missing Circuit ID ····· 受信パケットのうち、Circuit IDオプションを含まないパケット数が表示されます。

Receive Missing Remote ID ··· 受信パケットのうち、Remote IDオプションを含まないパケット数が表示されます。

Receive Bad Circuit ID ····· Circuit IDオプションが、既知のCircuit IDと一致しなかったパケット数が表示されます。

Receive Bad Remote ID ····· Remote IDオプションが、既知のRemote IDと一致しなかったパケット数が表示されます。

「Relay Statistics」画面

Monitor > DHCPv4 > Relay Statistics

DHCP Relay Statistics

Client Statistics

Transmit to Client …… サーバーからクライアントに中継されたパケット数が表示されます。

Transmit Error …… サーバーへの送信中にエラーが発生したパケット数が表示されます。

Receive from Client …… クライアントから受信したパケット数が表示されます。

Receive Agent Option …… リレーエージェント情報オプション付きの受信パケット数が表示されます。

Replace Agent Option …… リレーエージェント情報オプションが置き換えられたパケット数が表示されます。

Keep Agent Option …… リレーエージェント情報が保持されたパケット数が表示されます。

Drop Agent Option …… リレーエージェント情報付きの受信パケットのうち、破棄されたパケット数が表示されます。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Detailed Statistics」画面

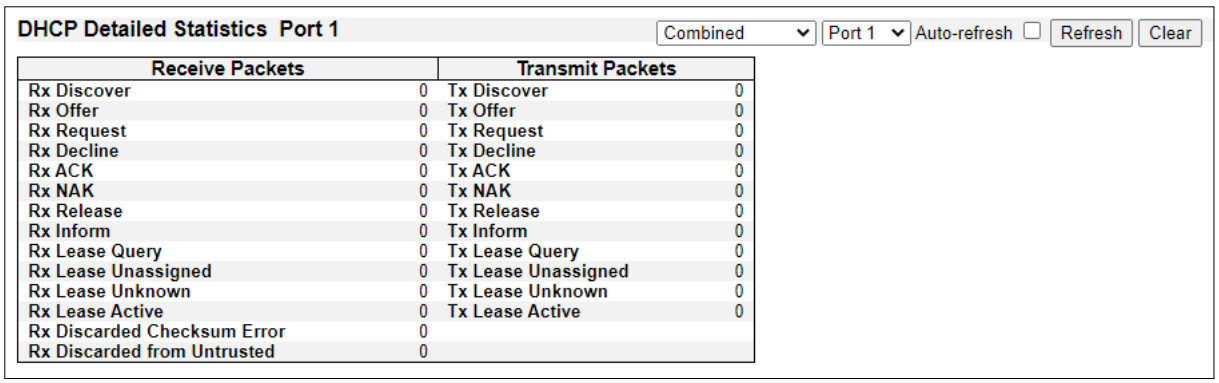
Monitor > DHCPv4 > Detailed Statistics

ドロップダウンリストで選択したDHCPユーザーとポート番号の、DHCPスヌーピングに関する詳細な統計情報が表示されます。

※L3転送メカニズムを使用して受信したDHCPパケットを転送処理した場合、ポートごとの通常の送信パケット統計には含まれません。

※特定のポートの統計情報をクリアしても、異なるレイヤーの情報を収集しているため、システム全体の統計は変更されない場合があります。

DHCP Detailed Statistics Port 1～10



Auto-refresh …… 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 …… 最新の状態に更新するボタンです。

〈Clear〉 …… 表示されているポートのカウンター値を0にするボタンです。

Receive Packets/Transmit Packets

Rx Discover/Tx Discover …… 送受信したDISCOVERパケット(DHCPオプション53の値が1)のパケット数が表示されます。

Rx Offer/Tx Offer …… 送受信したOFFERパケット(DHCPオプション53の値が2)のパケット数が表示されます。

Rx Request/Tx Request …… 送受信したREQUESTパケット(DHCPオプション53の値が3)のパケット数が表示されます。

Rx Decline/Tx Decline …… 送受信したDECLINEパケット(DHCPオプション53の値が4)のパケット数が表示されます。

Rx ACK/Tx ACK …… 送受信したACKパケット(DHCPオプション53の値が5)のパケット数が表示されます。

Rx NAK/Tx NAK …… 送受信したNAKパケット(DHCPオプション53の値が6)のパケット数が表示されます。

Rx Release/Tx Release …… 送受信したRELEASEパケット(DHCPオプション53の値が7)のパケット数が表示されます。

「Detailed Statistics」画面

Monitor > DHCPv4 > Detailed Statistics

DHCP Detailed Statistics Port 1～10

Rx Inform/Tx Inform …… 送受信したINFORMパケット(DHCPオプション53の値が8)のパケット数が表示されます。

Rx Lease Query/Tx Lease Query …… 送受信したLEASEQUERYパケット(DHCPオプション53の値が10)のパケット数が表示されます。

Rx Lease Unassigned/Tx Lease Unassigned …… 送受信したLEASEUNASSIGNEDパケット(DHCPオプション53の値が11)のパケット数が表示されます。

Rx Lease Unknown/Tx Lease Unknown …… 送受信したLEASEUNKNOWNパケット(DHCPオプション53の値が12)のパケット数が表示されます。

Rx Lease Active/Tx Lease Active …… 送受信したLEASEACTIVEパケット(DHCPオプション53の値が13)のパケット数が表示されます

Rx Discarded Checksum Error… IP/UDPチェックサムがエラーで廃棄されたパケット数が表示されます。

Rx Discarded from Untrusted … DHCPサーバーから受信したパケットのうち、untrustedポートで破棄されたパケット数が表示されます。

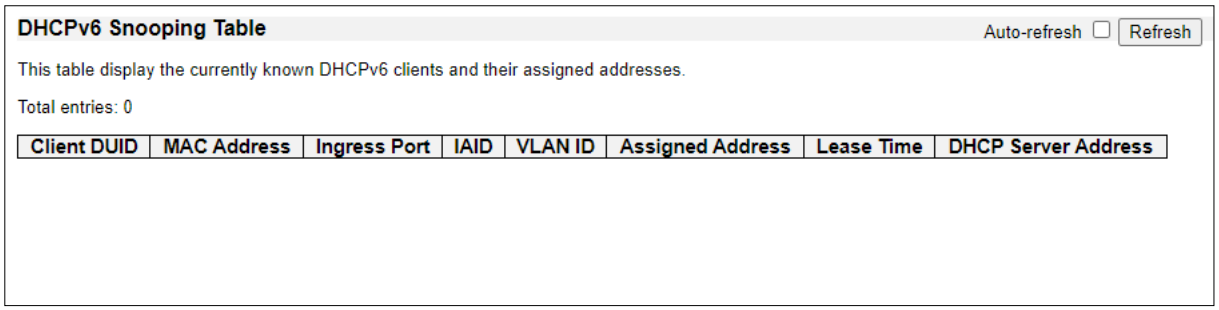
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Snooping Table」画面

Monitor > DHCPv6 > Snooping Table

DHCPv6スヌーピングテーブルが表示されます。

DHCPv6 Snooping Table



Auto-refresh ····· 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ····· 最新の状態に更新するボタンです。

Client DUID ····· クライアントのDUID(DHCP Unique Identifier)が表示されます。
DHCPv4ではMACアドレスを使用してクライアントインターフェースを識別しますが、DHCPv6ではDUIDを使用してクライアントのシステムを識別します。

MAC Address ····· DHCPv6メッセージを送信したクライアントのMACアドレスが表示されます。

Ingress Port ····· クライアントメッセージを受信するスイッチのポート番号が表示されます。

IAID ····· クライアントインターフェースのIAID(Identity Association Identifier)が表示されます。
1つのクライアントに複数のインターフェースが含まれる場合、同じDHCPv6メッセージで各インターフェースのアドレスを要求できます。
IAID値は、クライアントのシステム内のインターフェースを識別するために使用します。

VLAN ID ····· クライアントメッセージに使用されているVLAN IDが表示されます。

Assigned Address ····· IAID値によって識別されるクライアントインターフェースに割り当てられたアドレスが表示されます。

Lease Time ····· 割り当てられたアドレスのリース時間(秒)が表示されます。

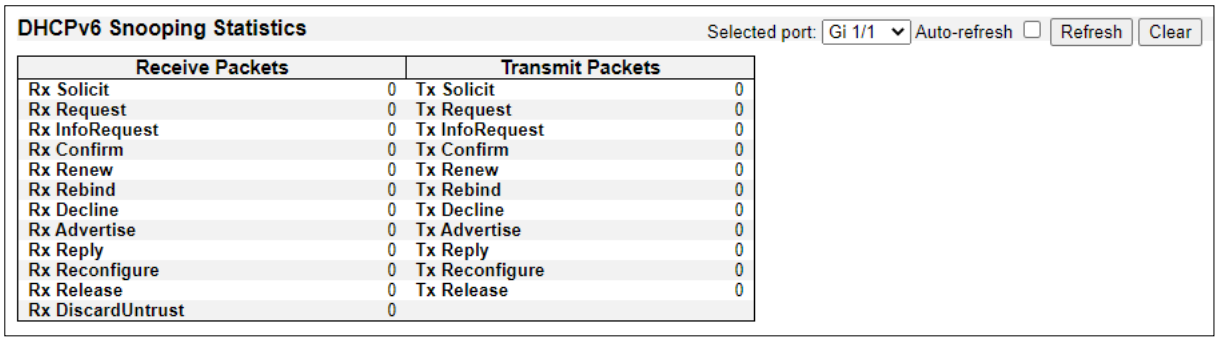
DHCP Server Address ····· クライアントにIPアドレスを割り当てたDHCPサーバーのIPv6アドレスが表示されます。

「Snooping Statistics」画面

Monitor > DHCPv6 > Snooping Statistics

ドロップダウンリストから選択したポートの、DHCPv6スヌーピングに関する詳細な統計情報が表示されます。

DHCPv6 Snooping Statistics



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈Clear〉 ……　表示されているポートのカウンター値を0にするボタンです。

Receive Packets/Transmit Packets ……　DHCPv6メッセージタイプごとに、送受信したパケット数が表示されます。
DHCPv6メッセージタイプについては、RFC3315を参照してください。

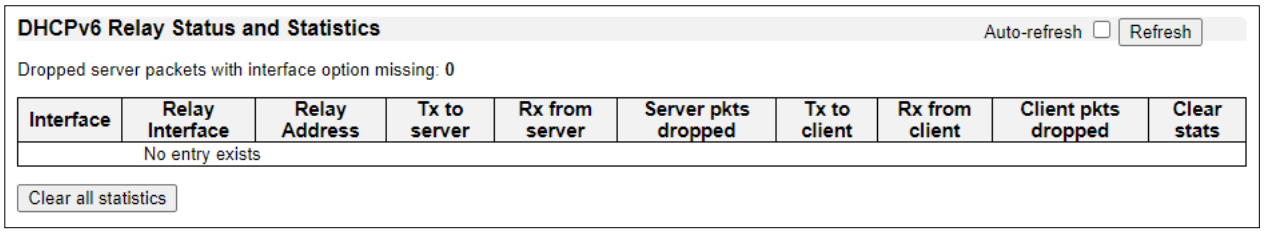
Rx DiscardUntrust ……　DHCPサーバーから受信したパケットのうち、untrustedポートで破棄されたパケット数が表示されます。

「Relay」画面

Monitor > DHCPv6 > Relay

DHCPv6リレーエージェントの状態が表示されます。

DHCPv6 Relay Status and Statistics



Auto-refresh …… 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 …… 最新の状態に更新するボタンです。

Interface …… インターフェースIDが表示されます。

Relay Interface …… 中継に使用するインターフェースのIDが表示されます。

Relay Address …… 中継に使用するインターフェースのアドレスが表示されます。

Tx to server …… クライアントからサーバーに中継されたパケット数が表示されます。

Rx from server …… サーバーから受信したパケット数が表示されます。

Server pkts dropped …… サーバーから受信したパケットのうち、破棄されたパケット数が表示されます。

Tx to client …… サーバーからクライアントに中継されたパケット数が表示されます。

Rx from client …… クライアントから受信したパケット数が表示されます。

Client pkts dropped …… クライアントから受信したパケットのうち、破棄されたパケット数が表示されます。

Clear stats …… 統計情報を削除するとき、ボックスにチェックマークを入れます。

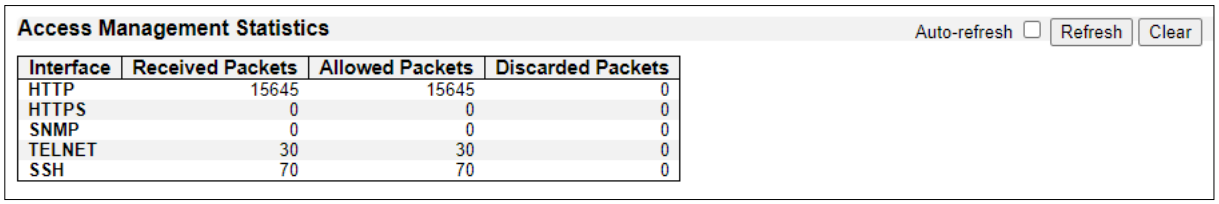
〈Clear all statistics〉 …… すべての統計情報を削除するボタンです。

「Access Management Statistics」画面

Monitor > Security > Access Management Statistics

本製品の各種情報にアクセスできるユーザーを制限しているとき、アクセス管理に関する統計情報が表示されます。
※アクセス制限は、「Configuration」→「Security」→「Switch」→「Access Management」画面で設定します。

Access Management Statistics



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈Clear〉 ……　すべてのカウンター値を0にするボタンです。

Interface ……　ユーザーが使用しているインターフェースが表示されます。

Received Packets ……　ユーザーから受信したパケット数が表示されます。

Allowed Packets ……　ユーザーから受信したパケットのうち、アクセスを許可したパケット数が表示されます。

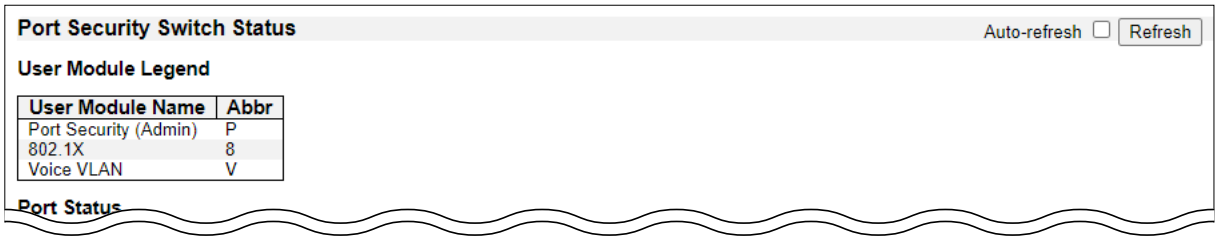
Discarded Packets……　ユーザーから受信したパケットのうち、破棄されたパケット数が表示されます。

「Overview」画面

Monitor > Security > Network > Port Security > Overview

ポートセキュリティーの状態が表示されます。
ポートセキュリティーは、他のソフトウェア機能(ユーザーモジュール)を介して管理、および間接的に設定できます。
ユーザーモジュールがポートセキュリティーを有効にしている場合、ポートはソフトウェアベースの学習用にセットアップされます。
このモードでは、不明なMACアドレスからのフレームがポートセキュリティーモジュールに渡され、ポートセキュリティーモジュールは、フレームの転送を許可するかブロックするかをユーザーモジュールに問い合わせます。
フレームの転送を許可するには、有効なすべてのユーザーモジュールが、MACアドレスの転送を許可する必要があります。
ユーザーモジュールが1つでもブロックすることを選択した場合、そのユーザーモジュールが許可するまでフレーム転送はブロックされます。

Port Security Switch Status



Auto-refresh …… 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 …… 最新の状態に更新するボタンです。

User Module Legend

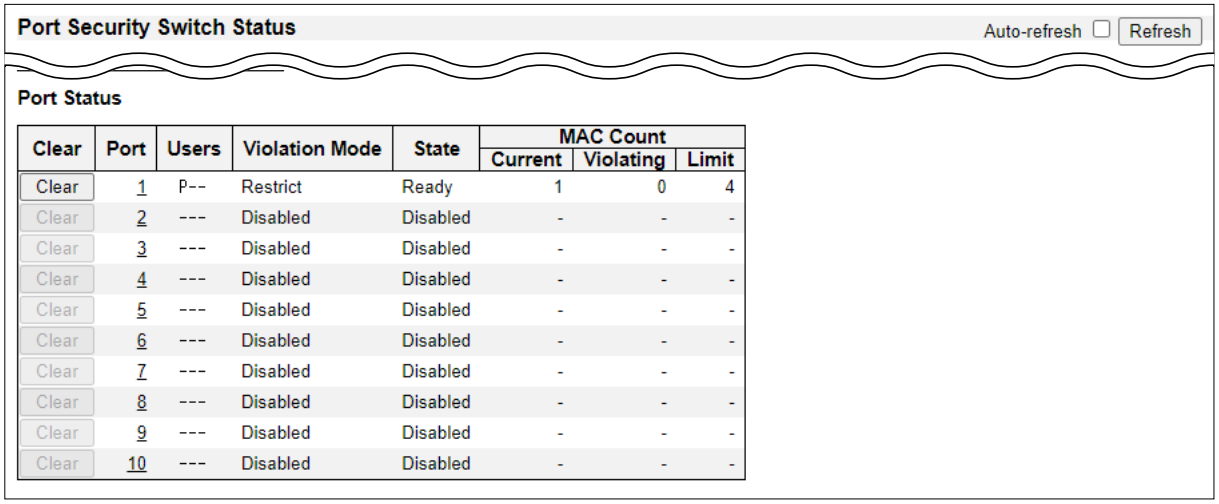
User Module Name…… ポートセキュリティーに対応した機能(ユーザーモジュール)のフルネームが表示されます。

Abbr …… ユーザーモジュール名の省略形が表示されます。
「Port Status」の[Users]欄に表示されます。

「Overview」画面

Monitor > Security > Network > Port Security > Overview

Port Security Switch Status



Port Status

〈Clear〉 ……

VLAN上のすべてのMACアドレスを削除するボタンです。
セキュアMACアドレスがない場合はクリックできません。

Port ……

本製品のポート番号が表示されます。
各ポート番号のリンク先をクリックすると、「Details」画面へ移動します。

Users ……

ポートセキュリティーに対応した各ユーザーモジュールが有効かどうかが表示されます。
対応するユーザーモジュールが無効の場合は、「-」が表示されます。
有効になっているユーザーモジュールは、「User Module Legend」の[Abbr]欄に設定されている文字が表示されます。

Violation Mode ……

セキュリティー違反が発生したときの動作が表示されます。

Disabled ：ポートセキュリティーは無効になっています。
Protect ：新しいMACアドレスの転送をブロックします。
Restrict ：違反MACアドレスとしてマークします。
Shutdown：ポートをシャットダウンします。

「Overview」画面

Monitor > Security > Network > Port Security > Overview

Port Security Switch Status

State……

ポートの状態が表示されます。

Disabled：
すべてのユーザーモジュールでポートセキュリティーが無効になっています。

Ready：
1つ以上のユーザーモジュールでポートセキュリティーが有効で、不明なMACアドレスからのフレームの受信待ち状態です。

Limit Reached：
1つ以上のユーザーモジュールでポートセキュリティーが有効で、セキュリティー上限に達しています。

Shut down：
1つ以上のユーザーモジュールでポートセキュリティーが有効で、ポートがシャットダウン状態です。
ポートがシャットダウンすると、「Configuration」→「Ports」画面で再起動するまで、MACアドレスを学習できません。
本製品を再起動するか、ポートセキュリティー設定を変更しても、ポートを再起動できます。

MAC Count Current ……

学習されているMACアドレス数(転送およびブロック)が表示されます。
※すべてのユーザーモジュールが無効になっている場合、「-」が表示されます。

MAC Count Violating……

違反MACアドレス数が表示されます。
※[Violation Mode]欄が「Restrict」のポートでカウントされます。
※ポートセキュリティーが無効になっている場合、「-」が表示されます。

MAC Count Limit……

ポートで学習できるMACアドレスの最大数が表示されます。
※ポートセキュリティーが無効になっている場合、「-」が表示されます。

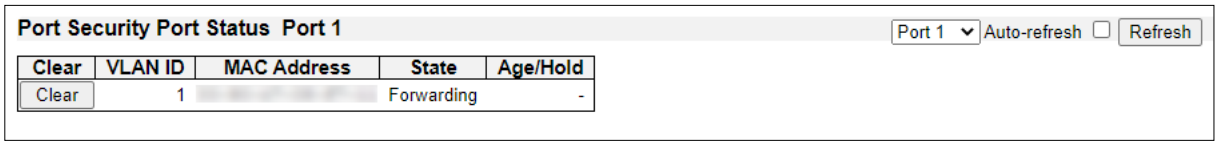
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Details」画面

Monitor > Security > Network > Port Security > Details

ドロップダウンリストから選択したポートのポートセキュリティーモジュールで保護されたMACアドレス(セキュアMACアドレス)が表示されます。
※MACアドレス学習が無効の場合は、「No MAC addresses attached」が表示されます。

Port Security Port Status Port 1～10



Auto-refresh …… 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 …… 最新の状態に更新するボタンです。

〈Clear〉 …… MACアドレスをMACアドレステーブルから削除するボタンです。

VLAN ID …… VLAN IDが表示されます。

MAC Address …… MACアドレスが表示されます。

State …… MACアドレスの状態が「Violating」(違反)、「Blocked」(ブロック)、「Forwarding」(転送中)で表示されます。
※「Violating」は、「Restrict」モードのポートで、MACアドレスをブロックしているときに表示されます。

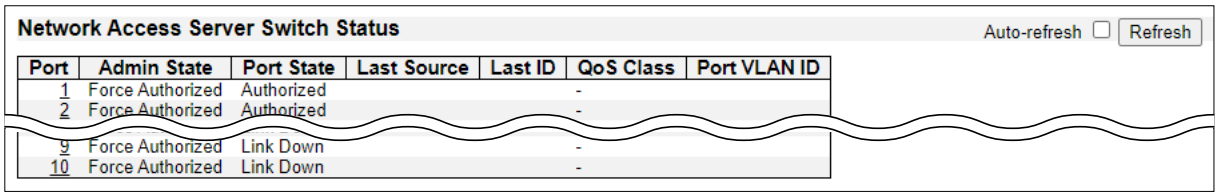
Age/Hold …… 1つ以上のユーザーモジュールがMACアドレスをブロックした場合、ホールド時間(秒)が表示されます。
ホールド時間が経過するまで、ブロック状態のままになります。
すべてのユーザーモジュールが転送を許可し、エージングが有効になっている場合、エージング期間(秒)が表示されます。
ポートセキュリティーモジュールは、MACアドレスがまだトラフィックを転送していることをエージング期間間隔でチェックします。
エージング期間経過後、フレームが転送されていない場合、MACテーブルから削除されます。
エージングが無効になっている場合、またはユーザーモジュールがMACアドレスを無期限に保持する場合、「−」が表示されます。

「Switch」画面

Monitor > Security > Network > NAS > Switch

現在のNASポートの状態が表示されます。

Network Access Server Switch Status



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

Port ……　本製品のポート番号が表示されます。
各ポート番号のリンク先をクリックすると、「Port」画面へ移動します。

Admin State ……　ポートの管理状態が表示されます。
表示される状態は、「Configuration」→「Security」→「Network」→「NAS」画面の[Admin State]欄をご確認ください。

Port State ……　ポートの状態が表示されます。
表示される状態は、「Configuration」→「Security」→「Network」→「NAS」画面の[Port State]欄をご確認ください。

Last Source ……　EAPOLベース認証の場合は、最後に受信したEAPOLフレームに含まれる送信元MACアドレスが表示されます。
MACベース認証の場合は、新しいクライアントから最後に受信したフレームが表示されます。

Last ID ……　EAPOLベース認証の場合は、最後に受信したEAP-Response/Identityフレームに含まれるユーザー名（サプリカント ID）が表示されます。
MACベース認証の場合は、新しいクライアントから最後に受信したフレームの送信元MACアドレスが表示されます。

QoS Class ……　RADIOUS QoS割り当てが有効な場合、RADIUSサーバーによってポートに割り当てられるQoSクラスが表示されます。

Port VLAN ID ……　動的VLAN割り当てが有効な場合、NASがポートに割り当てたVLAN IDが表示されます。
動的VLAN割り当てが無効の場合は空白になります。
VLAN IDがRADIUSサーバーによって割り当てられている場合は、VLAN IDのあとに「(RADIUS-assigned)」が表示されます。
RADIUSサーバーによる動的VLAN割り当てについては、「Configuration」→「Security」→「Network」→「NAS」画面の[RADIUS-Assigned VLAN Enabled]欄をご確認ください。
ポートをゲストVLANに割り当てると、VLAN IDのあとに「(Guest)」が表示されます。
ゲストVLANの詳細については、「Configuration」→「Security」→「Network」→「NAS」画面の[Guest VLAN Enabled]欄をご確認ください。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Port」画面

Monitor > Security > Network > NAS > Port

ドロップダウンリストで選択したポートでEAPOLベースのIEEE 802.1X認証を使用している場合、詳細なNAS統計情報が表示されます。
MACベース認証を使用している場合、選択したバックエンド・サーバー(RADIUS認証サーバー)の統計情報だけが表示されます。

NAS Statistics Port 1～10

Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈Clear〉 ……　表示されているポートのカウンター値を0にするボタンです。
[Admin State]欄が下記の状態のときに使用できます。
◎Force Authorized
◎Force Unauthorized
◎Port-based 802.1X
◎Single 802.1X

〈Clear All〉 ……　表示されているポートの「port counters」とすべてのクライアントの「Selected counters」を0にするボタンです。
[Admin State]欄が下記の状態のときに使用できます。
◎Multi 802.1X
◎MAC-based Auth.X
※「Last Client」は削除されません。

〈Clear This〉 ……　選択したクライアントの「Selected counters」を0にするボタンです。
[Admin State]欄が下記の状態のときに使用できます。
◎Multi 802.1X
◎MAC-based Auth.X
※「Last Client」は削除されません。

「Port」画面

Monitor > Security > Network > NAS > Port

NAS Statistics Port 1～10

Port State

Admin State ……

ポートの管理状態が表示されます。
表示される状態は、「Configuration」→「Security」→「Network」→「NAS」画面の[Admin State]欄をご確認ください。

Port State ……

ポートの状態が表示されます。
表示される状態は、「Configuration」→「Security」→「Network」→「NAS」画面の[Port State]欄をご確認ください。

QoS Class ……

RADIOUS QoS割り当てが有効な場合、RADIUSサーバーがポートに割り当てたQoSクラスが表示されます。

Port VLAN ID ……

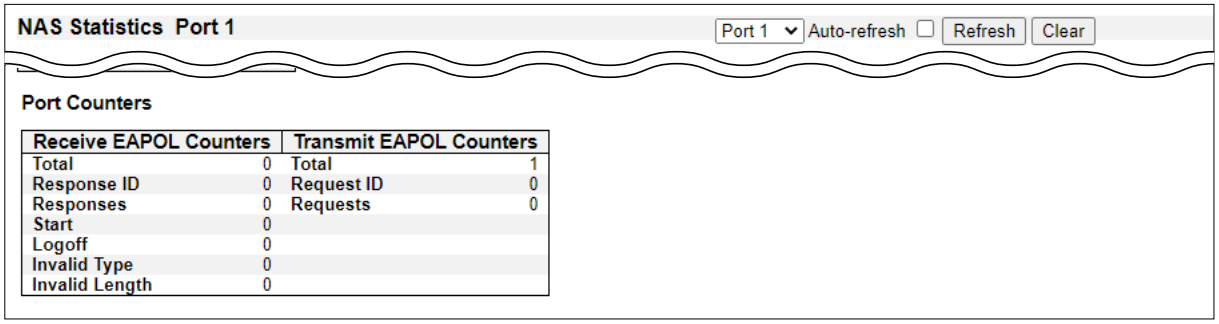
動的VLAN割り当てが有効な場合、NASがポートに割り当てたVLAN IDが表示されます。
動的VLAN割り当てが無効の場合は空白になります。
VLAN IDがRADIUSサーバーによって割り当てられている場合は、VLAN IDのあとに「(RADIUS-assigned)」が表示されます。
RADIUSサーバーによる動的VLAN割り当てについては、「Configuration」→「Security」→「Network」→「NAS」画面の[RADIUS-Assigned VLAN Enabled]欄をご確認ください。
ポートをゲストVLANに割り当てると、VLAN IDのあとに「(Guest)」が表示されます。
ゲストVLANの詳細については、「Configuration」→「Security」→「Network」→「NAS」画面の[Guest VLAN Enabled]欄をご確認ください。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Port」画面

Monitor > Security > Network > NAS > Port

NAS Statistics Port 1～10



Port Counters

Receive EAPOL Counters/Transmit EAPOL Counters

……　[Admin State]欄が下記の状態のときに使用できます。
◎Force Authorized
◎Force Unauthorized
◎Port-based 802.1X
◎Single 802.1X
◎Multi 802.1X

Rx/Tx	項目名	IEEE名	概要
Rx	Total	dot1xAuthEapolFramesRx	受信した有効なEAPOLフレーム数
	Response ID	dot1xAuthEapolRespIdFramesRx	受信した有効なEAPOL Response Identityフレーム数
	Responses	dot1xAuthEapolRespFramesRx	受信した有効なEAPOL Responseフレーム数（Response Identityフレームを除く）
	Start	dot1xAuthEapolStartFramesRx	受信した有効なEAPOL Startフレーム数
	Logoff	dot1xAuthEapolLogoffFramesRx	受信フレームのなかで、フレームタイプが認識できなかったフレーム数
	Invalid Type	dot1xAuthInvalidEapolFramesRx	受信フレームのなかで、Packet Body Lengthフィールドの値が無効なフレーム数
	Invalid Length	dot1xAuthEapLengthErrorFramesRx	受信した有効なEAPOL Response IDフレーム数
Tx	Total	dot1xAuthEapolFramesTx	送信したEAPOLフレーム数
	Request ID	dot1xAuthEapolReqIdFramesTx	送信したEAPOL Request Identityフレーム数
	Requests	dot1xAuthEapolReqFramesTx	送信したEAPOL Requestフレーム数（Request Identityフレームを除く）

「Port」画面

Monitor > Security > Network > NAS > Port

NAS Statistics Port 1～10

Backend Server Counters …… [Admin State]欄が下記の状態のときに使用できます。
◎Port-based 802.1X
◎Single 802.1X
◎Multi 802.1X
◎MAC-based Auth.

Rx/Tx	項目名	IEEE名	概要
Rx	Access Challenges	dot1xAuthBackendAccessChallenges	**802.1X-based：** サプリカントからの最初の応答につづいて、バックエンドサーバーから最初の要求を受信した回数 ※バックエンドサーバーと通信しているときに表示されます。 **MAC-based：** ポート(左端のテーブル)、またはクライアント(右端のテーブル)がバックエンドサーバーから受信したすべてのアクセスチャレンジの回数
	Other Requests	dot1xAuthBackendOtherRequestsToSupplicant	**802.1X-based：** 最初の要求パケットにつづいて、EAP Requestパケットをサプリカントに送信した回数 ※バックエンドサーバーがEAP方式を選択したときに表示されます。 **MAC-based：** 表示されません。
	Auth. Successes	dot1xAuthBackendAuthSuccesses	**802.1X-based/MAC-based：** 認証成功メッセージを受信した回数 ※バックエンドサーバーがサプリカント/クライアントを正常に認証したときに表示されます。
	Auth. Failures	dot1xAuthBackendAuthFails	**802.1X-based/MAC-based：** 認証失敗メッセージを受信した回数 ※バックエンドサーバーがサプリカント/クライアントを認証していないときに表示されます。
Tx	Responses	dot1xAuthBackendResponses	**802.1X-based：** サプリカントの最初の応答パケットをバックエンドサーバーに送信しようとした回数 ※バックエンドサーバーと通信しようとしたときに表示されます。 再送信はカウントされません。 **MAC-based：** ポート(左端のテーブル)、またはクライアント(右端のテーブル)について、バックエンドサーバーに送信されたすべてのパケット数 ※再送信はカウントされません。

「Port」画面

Monitor > Security > Network > NAS > Port

NAS Statistics Port 1～10

Last Supplicant/Client Info…… 認証を試行した直近のサプリカント/クライアント情報が表示されます。
[Admin State]欄が下記の状態のときに使用できます。
◎Port-based 802.1X
◎Single 802.1X
◎Multi 802.1X
◎MAC-based Auth.

項目名	IEEE名	概要
MAC Address	dot1xAuthLastEapolFrameSource	サプリカント/クライアントのMACアドレス
VLAN ID	―	サプリカント/クライアントのVLAN ID
Version	dot1xAuthLastEapolFrameVersion	**802.1X-based：** EAPOLフレームに含まれるプロトコルバージョン **MAC-based：** 表示されません。
Identity	―	**802.1X-based：** EAPOL Response Identityフレームに含まれるユーザー名(supplicant identity) **MAC-based：** 表示されません。

「Port」画面

Monitor > Security > Network > NAS > Port

NAS Statistics Port 1～10

Selected Counters

Selected Counters …… 「Attached MAC Addresses」で選択したサプリカントについての統計情報が表示されます。

Attached MAC Addresses

Identity…… EAPOL Response Identityフレームで受信したサプリカントのIDが表示されます。
各IDのリンク先をクリックすると、サプリカントのEAPOLカウンターとバックエンドサーバーカウンターが「Selected Counters」に表示されます。
サプリカントが接続されていない場合は、「No supplicants attached.」が表示されます。
※MACベース認証では表示されません。

MAC Address …… 「Multi 802.1X」の場合、接続されたサプリカントのMACアドレスが表示されます。
「MAC-based Auth.」の場合、この列には接続されたクライアントのMACアドレスが表示されます。
各MACアドレスのリンク先をクリックすると、クライアントのバックエンドサーバーカウンターが「Selected Counters」に表示されます。
クライアントが接続されていない場合は、「No clients attached」と表示されます。

VLAN ID …… クライアントが所属しているVLAN IDが表示されます。

State…… クライアントの状態が「authenticated」(認証済み)、または「unauthenticated」(認証されていない)で表示されます。
認証済みの状態では、ポート上のフレーム転送が許可され、認証されていない状態ではブロックされます。
バックエンドサーバーからの認証が失敗した場合、一定期間クライアントは認証されていない状態になります。
※認証が失敗したときの待機時間は、「Configuration」→「Security」→「Network」→「NAS」画面の[Hold Time]欄で設定します。

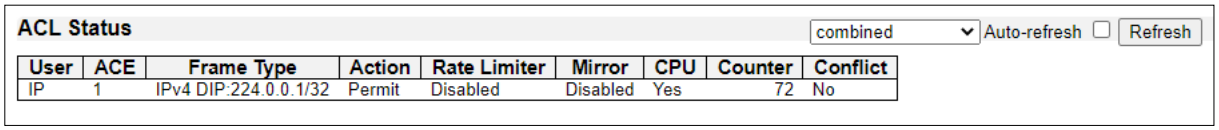
Last Authentication …… クライアントが最後に認証を試行した日時が表示されます。

「ACL Status」画面

Monitor > Security > Network > ACL Status

ドロップダウンリストで選択したACLユーザーの、ACLステータスが表示されます。
各行には、ACLを構成するACEが表示されます。
ACEは最大256件まで登録できます。
ハードウェアの制限が原因で、特定のACEが適用できない場合があります。（競合）

ACL Status



Auto-refresh ····· 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ····· 最新の状態に更新するボタンです。

User ····· ACLユーザーが表示されます。

ACE ····· ACE IDが表示されます。

Frame Type ····· 条件となるフレームタイプが表示されます。

Any：
フレームタイプでフィルタリングしません。

Etype：
イーサネットタイプのフレームをフィルタリングします。
※ARP、IPv4、IPv6フレームは、ACEに一致しないと判断されます。

ARP：
ARP/RARPフレームをフィルタリングします。

IPv4：
すべてのIPv4フレームをフィルタリングします。

IPv4/ICMP：
ICMPプロトコルのIPv4フレームをフィルタリングします。

IPv4/UDP：
UDPプロトコルのIPv4フレームをフィルタリングします。

IPv4/TCP：
TCPプロトコルのIPv4 フレームをフィルタリングします。

IPv4/Other：
ICMP/UDP/TCPプロトコル以外のIPv4フレームをフィルタリングします。

IPv6：
IPv6フレームをフィルタリングします。

「ACL Status」画面

Monitor > Security > Network > ACL Status

ACL Status

Action …… ACEに一致するフレームを受信したときの動作が表示されます。

Permit：
ACEに一致するフレームを転送、学習します。

Deny：
ACEに一致するフレームを破棄します。

Filter：
ACEに一致するフレームをフィルタリングします。

Rate Limiter …… ACEのレートリミッター番号が0～16で表示されます。
レートリミッターが無効の場合は、「Disabled」と表示されます。

Mirror …… ACEに一致するフレームを受信したとき、ミラーポートにミラーリングするかが表示されます。

Enabled：
ポートで受信したフレームをミラーリングします。

Disabled：ポートで受信したフレームをミラーリングしません。

CPU …… ACEに一致したパケットをCPUに転送するかどうかが表示されます。

Counter …… フレームがACEに一致した回数が表示されます。

Conflict …… ACEが競合しているかどうかが表示されます。

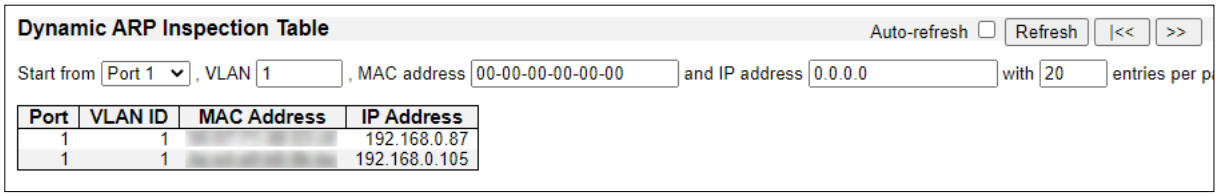
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「ARP Inspection」画面

Monitor > Security > Network > ARP Inspection

動的ARPインスペクションテーブルが表示されます。
動的ARPインスペクションテーブルにはMACアドレスとIPアドレスの組み合わせが最大256件まで登録され、ポート番号、VLAN ID、MACアドレス、IPアドレスでソートされます。
すべてのエントリは、DHCPスヌーピング機能を使用して学習します。

Dynamic ARP Inspection Table



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈|<<〉……　最初のページに戻るボタンです。

〈>>〉 ……　次のページに進むボタンです。

Start from［ポート番号］, VLAN［VLAN ID］, MAC address［MACアドレス］and IP address［IPアドレス］with［表示数］entries per page.
……　ページの表示設定です。
［ポート番号］、［VLAN ID］、［MACアドレス］、［IPアドレス］欄で、テーブルの開始位置を指定できます。
［表示数］欄で1ページあたりの表示数を指定できます。（最大99件まで）

Port ……　本製品のポート番号が表示されます。

VLAN ID ……　ARPトラフィックが許可されたVLAN IDが表示されます。

MAC Address ……　ユーザーからARPリプライで通知されたMACアドレスが表示されます。

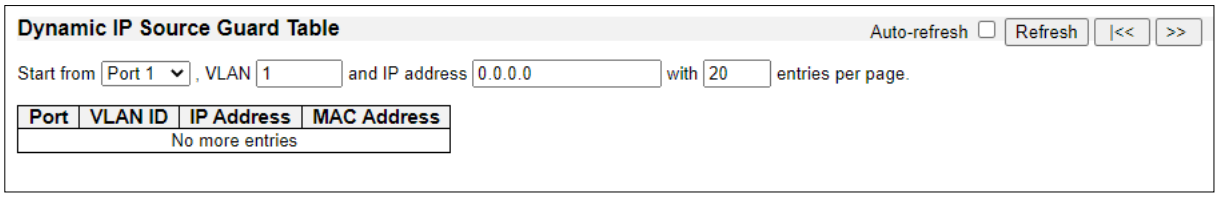
IP Address……　ユーザーIPアドレスが表示されます。

「IP Source Guard」画面

Monitor > Security > Network > IP Source Guard

動的IPソースガードテーブルが表示されます。
動的IPソースガードテーブルは、ポート番号、VLAN ID、MACアドレス、IPアドレスでソートされます。

Dynamic IP Source Guard Table



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈|<<〉 ……　最初のページに戻るボタンです。

〈>>〉 ……　次のページに進むボタンです。

Start from［ポート番号］, VLAN［VLAN ID］and IP address［IPアドレス］with［表示数］entries per page.
……　ページの表示設定です。
［ポート番号］、［VLAN ID］、［IPアドレス］欄で、テーブルの開始位置を指定できます。
［表示数］欄で1ページあたりの表示数を指定できます。（最大99件まで）

Port ……　本製品のポート番号が表示されます。

VLAN ID ……　IPトラフィックが許可されたVLAN IDが表示されます。

IP Address ……　ユーザーIPアドレスが表示されます。

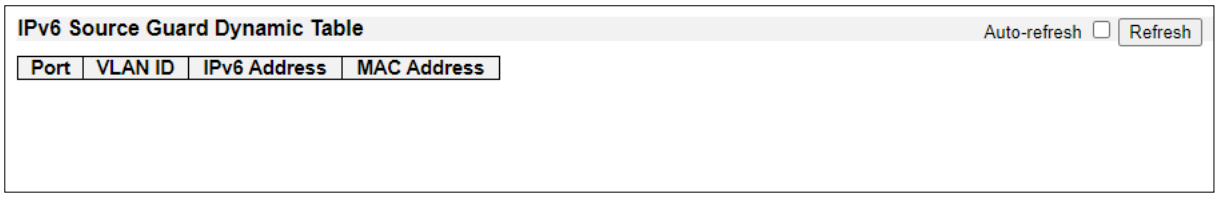
MAC Address ……　送信元MACアドレスが表示されます。

「IPv6 Source Guard」画面

Monitor > Security > Network > IPv6 Source Guard

動的IPv6ソースガードテーブルが表示されます。

IPv6 Source Guard Dynamic Table



Auto-refresh ····· 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ····· 最新の状態に更新するボタンです。

Port ····· 本製品のポート番号が表示されます。

VLAN ID ····· IPトラフィックが許可されたVLAN IDが表示されます。
VLAN IDが割り当てられていない場合、「0」が表示されます。

IPv6 Address ····· 送信元IPv6アドレスが表示されます。

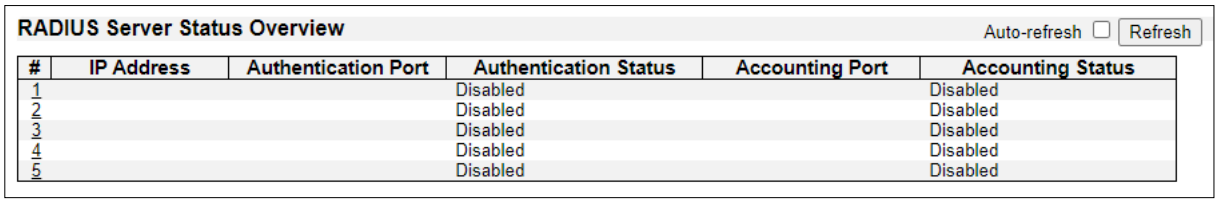
MAC Address ····· 送信元MACアドレスが表示されます。

「RADIUS Overview」画面

Monitor > Security > AAA > RADIUS Overview

設定したRADIUSサーバーの状態が表示されます。
※RADIUSサーバーは、「Configuration」→「Security」→「AAA」→「RADIUS」画面で設定します。

RADIUS Server Status Overview



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

……　RADIUSサーバーの番号が表示されます。
各番号のリンク先をクリックすると、「RADIUS Details」画面に移動します。

IP Address ……　サーバーのIPアドレスが表示されます。

Authentication Port ……　認証に使用するUDPポート番号が表示されます。

Authentication Status ……　サーバーの認証状態が表示されます。

Disabled：
サーバーは使用できません。

Not Ready：
サーバーは使用できますが、サーバーと通信できません。

Ready：
RADIUSモジュールがアクセス試行待ちです。

Dead (X seconds left)：
サーバーへのアクセスが試行されましたが、タイムアウト時間に応答がなかったため、一時的に無効になっています。
カッコ内に表示された時間が経過後、ふたたび有効になります。
※複数のRADIUSサーバーが登録されているときに表示されます。

Accounting Port ……　アカウンティングに使用するUDPポート番号が表示されます。

Accounting Status ……　サーバーのアカウンティング状態が表示されます。

Disabled：
サーバーは使用できません。

Not Ready：
サーバーは使用できますが、サーバーと通信できません。

Ready：
RADIUSモジュールがアクセス試行待ちです。

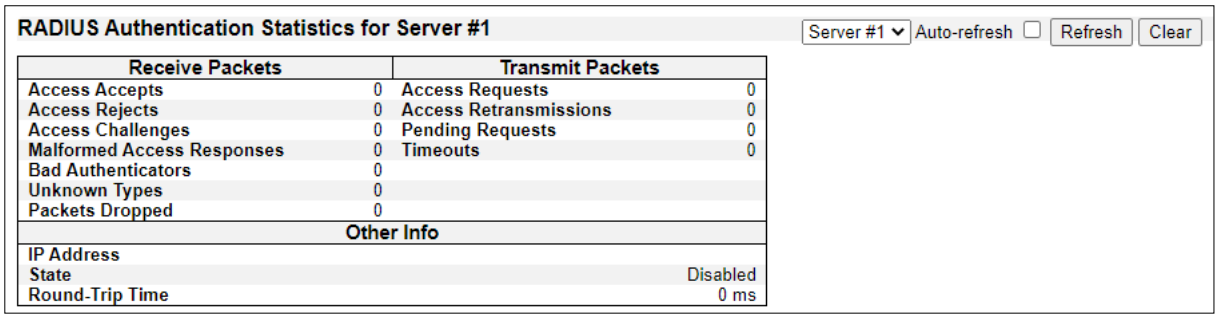
Dead (X seconds left)：
サーバーへのアクセスが試行されましたが、タイムアウト時間に応答がなかったため、一時的に無効になっています。
カッコ内に表示された時間が経過後、ふたたび有効になります。
※複数のRADIUSサーバーが登録されているときに表示されます。

「RADIUS Details」画面

Monitor > Security > AAA > RADIUS Details

ドロップダウンリストで選択したRADIUSサーバーの、詳細な統計情報が表示されます。

RADIUS Authentication Statistics for Server #1～5



Auto-refresh …… 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 …… 最新の状態に更新するボタンです。

〈Clear〉 …… 表示しているサーバーのカウンター値を0にするボタンです。
※[Pending Requests]欄は0になりません。

「RADIUS Details」画面

Monitor > Security > AAA > RADIUS Details

RADIUS Authentication Statistics for Server #1～5

Receive Packets/Transmit Packets

RADIUS認証サーバーのパケットカウンターです。

Rx/Tx	項目名	RFC4668名	概要
Rx	Access Accepts	radiusAuthClientExtAccessAccepts	サーバーから受信したRADIUS Access-Acceptパケット数
	Access Rejects	radiusAuthClientExtAccessRejects	サーバーから受信したRADIUS Access-Rejectパケット数
	Access Challenges	radiusAuthClientExtAccessChallenges	サーバーから受信したRADIUS Access-Challengeパケット数
	Malformed Access Responses	radiusAuthClientExtMalformedAccessResponses	サーバーから受信した不正なRADIUS Access-Responseパケット数 ※無効な長さのパケットも含みます。 不正なオーセンティケータ、メッセージオーセンティケータ属性、または不明なタイプは含まれません。
	Bad Authenticators	radiusAuthClientExtBadAuthenticators	サーバーから受信した無効なオーセンティケータ、またはメッセージ認証属性を含むRADIUS Access-Responseパケット数
	Unknown Types	radiusAuthClientExtUnknownTypes	サーバーから受信し破棄された、不明なタイプのRADIUSパケット数
	Packets Dropped	radiusAuthClientExtPacketsDrop	サーバーから受信し、破棄されたRADIUSパケット数
Tx	Access Requests	radiusAuthClientExtAccessRequests	サーバーに送信したRADIUS Access-Requestパケット数 ※再送信は含まれません。
	Access Retransmissions	radiusAuthClientExtAccessRetransmissions	サーバーに再送信したRADIUS Access-Requestパケット数
	Pending Requests	radiusAuthClientExtpendingRequests	サーバーに送信したRADIUS Access-Requestパケットのうち、タイムアウトしていないか、応答を受信していないパケットの数 ※Access-Requestが送信されるとインクリメントされ、Access-Accept、Access-Reject、Access-Challenge、タイムアウト、または再送信の受信でデクリメントされます。
	Timeouts	radiusAuthClientExtTimeouts	サーバーに対する認証タイムアウトの回数 ※タイムアウト後、クライアントは同じサーバーに再試行したり、別のサーバーに送信したり、認証を断念したりします。 同じサーバーへの再試行は、タイムアウトだけでなく再送信としてもカウントされます。 別のサーバーへの送信は、タイムアウトだけでなく送信としてもカウントされます。

「RADIUS Details」画面

Monitor > Security > AAA > RADIUS Details

RADIUS Authentication Statistics for Server #1～5

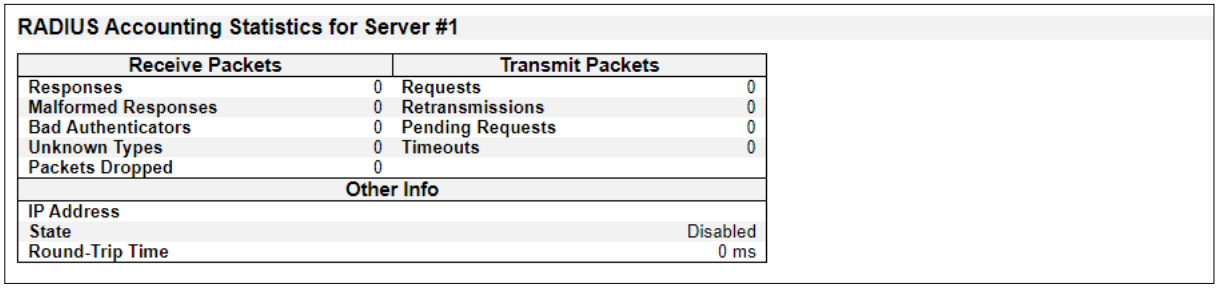
Other Info ……　サーバーの状態と最新のラウンドトリップ時間に関する情報が表示されます。

項目名	RFC4668名	概要
IP Address	—	認証サーバーのIPアドレスとUDPポート番号
State	—	認証サーバーの状態 **Disabled :** サーバーは使用できません。 **Not Ready :** サーバーは使用できますが、サーバーと通信できません。 **Ready :** RADIUSモジュールがアクセス試行待ちです。 **Dead (X seconds left) :** サーバーへのアクセスが試行されましたが、タイムアウト時間に応答がなかったため、一時的に無効になっています。 カッコ内に表示された時間が経過後、ふたたび有効になります。 ※複数のRADIUSサーバーが登録されているときに表示されます。
Round-Trip Time	radiusAuthClientExtRoundTripTime	Access-Requestパケットを送信してから、RADIUS認証サーバーからのAccess-Reply/Access-Challengeパケットを受信するまでにかかった時間(ミリ秒、100ミリ秒刻み) ※サーバーと一度も通信していない場合は、「0」が表示されます。

「RADIUS Details」画面

Monitor > Security > AAA > RADIUS Details

RADIUS Accounting Statistics for Server #1～10



RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address			
State			Disabled
Round-Trip Time			0 ms

Receive Packets/Transmit Packets

RADIUS認証サーバーのパケットカウンターです。

Rx/Tx	項目名	RFC4670名	概要
Rx	Responses	radiusAccClientExtResponses	サーバーから受信したRADIUSパケット数
	Malformed Responses	radiusAccClientExtMalformedResponses	サーバーから受信した不正なRADIUSパケット数 ※無効な長さのパケットも含まれます。 不正なオーセンティケータや不明なタイプのパケットは含まれません。
	Bad Authenticators	radiusAcctClientExtBadAuthenticators	サーバーから受信した不正なオーセンティケーターを含むRADIUSパケット数
	Unknown Types	radiusAccClientExtUnknownTypes	サーバーから受信した不明なタイプのRADIUSパケット数
	Packets Dropped	radiusAccClientExtPacketsDropped	サーバーから受信し、破棄されたRADIUSパケット数
Tx	Requests	radiusAccClientExtRequests	サーバーに送信したRADIUSパケット数 ※再送信は含まれません。
	Retransmissions	radiusAccClientExtRetransmissions	サーバーに再送信したRADIUSパケット数
	Pending Requests	radiusAccClientExtPendingRequests	サーバーに送信したRADIUSパケットのうち、タイムアウトしていないか、応答を受信していないパケットの数 ※Accounting-Requestが送信されるとインクリメントされ、Accounting-Response、タイムアウト、または再送信の受信でデクリメントされます。
	Timeouts	radiusAccClientExtTimeouts	サーバーに対するアカウンティングタイムアウトの回数 ※タイムアウト後、クライアントは同じサーバーに再試行したり、別のサーバーに送信したり、アカウンティングを断念したりします。 同じサーバーへの再試行は、タイムアウトだけでなく再送信としてもカウントされます。 別のサーバーへの送信は、タイムアウトだけでなく送信としてもカウントされます。

「RADIUS Details」画面

Monitor > Security > AAA > RADIUS Details

RADIUS Accounting Statistics for Server #1 ～ 10

Other Info …… サーバーの状態と最新のラウンドトリップ時間に関する情報が表示されます。

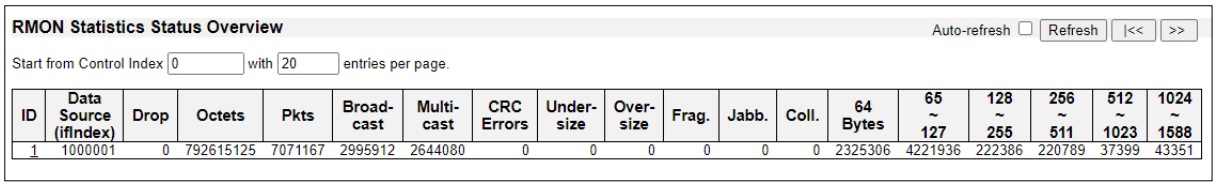
項目名	RFC4670名	概要
IP Address	—	アカウンティングサーバーのIPアドレスとUDPポート番号
State	—	アカウンティングサーバーの状態 **Disabled :** サーバーは使用できません。 **Not Ready :** サーバーは使用できますが、サーバーと通信できません。 **Ready :** RADIUSモジュールがアカウンティング試行待ちです。 **Dead (X seconds left) :** サーバーへアカウンティングが試行されましたが、タイムアウト時間に応答がなかったため、一時的に無効になっています。 カッコ内に表示された時間が経過後、ふたたび有効になります。 ※複数のRADIUSサーバーが登録されているときに表示されます。
Round-Trip Time	radiusAccClientExtRoundTripTime	Requestパケットを送信してから、RADIUS認証サーバーからのResponseパケットを受信するまでにかかった時間(ミリ秒、100ミリ秒刻み) ※サーバーと一度も通信していない場合は、「0」が表示されます。

「Statistics」画面

Monitor > Security > Switch > RMON > Statistics

RMONの統計情報が表示されます。

RMON Statistics Status Overview


RMON Statistics Status Overview

Auto-refresh ☐ Refresh |<< >>

Start from Control Index 0 with 20 entries per page.

ID	Data Source (ifIndex)	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
1	1000001	0	792615125	7071167	2995912	2644080	0	0	0	0	0	0	2325306	4221936	222386	220789	37399	43351

Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈|<<〉……　最初のページに戻るボタンです。

〈>>〉 ……　次のページに進むボタンです。

Start from Control Index [ID] with [表示数] entries per page.
……　ページの表示設定です。
IDの一番小さいエントリがはじめに表示されます。
[ID]欄で、はじめに表示するIDを指定できます。
[表示数]欄で1ページあたりの表示数を指定できます。（最大99件まで）

ID ……　IDが表示されます。
各IDのリンク先をクリックすると、「Detailed RMON Statistics」画面に移動します。

Data Source (ifIndex) ……　監視しているポートIDが表示されます。

Drop ……　リソース不足のためにプローブによってパケットが破棄されたイベントの数が表示されます。

Octets ……　受信したデータのバイト数が表示されます。
※不正なデータのパケットも含まれます。

Pkts ……　受信したパケット数が表示されます。
※不正なデータのパケット、ブロードキャストパケット、マルチキャストパケットも含まれます。

Broad-cast ……　ブロードキャストアドレス宛ての有効な受信パケット数が表示されます。

Multi-cast ……　マルチキャストアドレス宛ての有効な受信パケット数が表示されます。

CRC Errors……　フレーミングビットを除き、フレームチェックシーケンス(FCS)を含むパケット長が64～1518バイトのパケットのうち、FCSエラー、またはアライメントエラーと判断された受信パケット数が表示されます。
※FCSが整数個のオクテットを持つとき、FCSエラーと判断されます。
※FCSのオクテット数が整数でないとき、アライメントエラーと判断されます。

Under-size ……　64バイト未満の受信パケットの数が表示されます。

「Statistics」画面

Monitor > Security > Switch > RMON > Statistics

RMON Statistics Status Overview

Over-size…… 1518バイトを超える受信パケットの数が表示されます。

Frag. …… 64バイト未満でCRCが無効な受信フレームの数が表示されます。

Jabb.…… 64バイト以上でCRCが無効な受信フレームの数が表示されます。

Coll. …… イーサネットセグメントでの推定のコリジョン(衝突)回数が表示されます。

64 Bytes…… 64バイトの受信パケットの数が表示されます。
※不正なデータのパケットも含まれます。

65～127 …… 65～127バイトの受信パケットの数が表示されます。
※不正なデータのパケットも含まれます。

128～255…… 128～255バイトの受信パケットの数が表示されます。
※不正なデータのパケットも含まれます。

256～511…… 256～511バイトの受信パケットの数が表示されます。
※不正なデータのパケットも含まれます。

512～1023 …… 512～1023バイトの受信パケットの数が表示されます。
※不正なデータのパケットも含まれます。

1024～1588 …… 1024～1588バイトの受信パケットの数が表示されます。
※不正なデータのパケットも含まれます。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Detailed RMON Statistics」画面

Monitor > Security > Switch > RMON > Statistics

ドロップダウンリストで選択したIDの、RMON統計情報が表示されます。

Detailed RMON Statistics ID n

Auto-refresh …… 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 …… 最新の状態に更新するボタンです。

Receive Total

Port …… 監視しているポートIDが表示されます。

Drops …… リソース不足のためにプローブによってパケットが破棄されたイベントの数が表示されます。

Octets …… 受信したデータのバイト数が表示されます。
※不正なデータのパケットも含まれます。

Pkts …… 受信したパケット数が表示されます。
※不正なデータのパケット、ブロードキャストパケット、マルチキャストパケットも含まれます。

Broadcast …… ブロードキャストアドレス宛ての有効な受信パケット数が表示されます。

Multicast …… マルチキャストアドレス宛ての有効な受信パケット数が表示されます。

CRC/Alignment …… フレーミングビットを除き、フレームチェックシーケンス(FCS)を含むパケット長が64～1518バイトのパケットのうち、FCSエラー、またはアライメントエラーと判断された受信パケット数が表示されます。
※FCSが整数個のオクテットを持つとき、FCSエラーと判断されます。
※FCSのオクテット数が整数でないとき、アライメントエラーと判断されます。

Undersize …… 64バイト未満の受信パケットの数が表示されます。

Oversize …… 1518バイトを超える受信パケットの数が表示されます。

Fragments …… 64バイト未満でCRCが無効な受信フレームの数が表示されます。

「Detailed RMON Statistics」画面

Monitor > Security > Switch > RMON > Statistics

Detailed RMON Statistics ID n

Jabber …… 64バイト以上でCRCが無効な受信フレームの数が表示されます。

Collisions…… イーサネットセグメントでの推定のコリジョン(衝突)回数が表示されます。

64 Bytes…… 64バイトの受信パケットの数が表示されます。
※不正なデータのパケットも含まれます。

65-127 Bytes …… 65～127バイトの受信パケットの数が表示されます。
※不正なデータのパケットも含まれます。

128-255 Bytes …… 128～255バイトの受信パケットの数が表示されます。
※不正なデータのパケットも含まれます。

256-511 Bytes …… 256～511バイトの受信パケットの数が表示されます。
※不正なデータのパケットも含まれます。

512-1023 Bytes …… 512～1023バイトの受信パケットの数が表示されます。
※不正なデータのパケットも含まれます。

1024-1588 Bytes…… 1024～1588バイトの受信パケットの数が表示されます。
※不正なデータのパケットも含まれます。

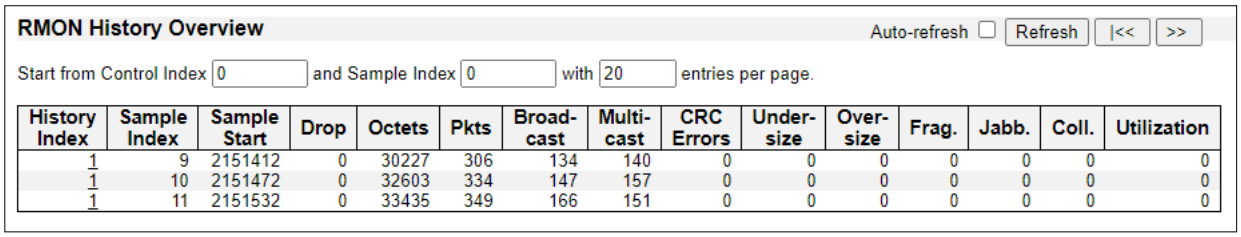
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「History」画面

Monitor > Security > Switch > RMON > History

RMON履歴が表示されます。

RMON History Overview


RMON History Overview

Auto-refresh ☐ Refresh |<< >>

Start from Control Index 0 and Sample Index 0 with 20 entries per page.

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
1	9	2151412	0	30227	306	134	140	0	0	0	0	0	0	0
1	10	2151472	0	32603	334	147	157	0	0	0	0	0	0	0
1	11	2151532	0	33435	349	166	151	0	0	0	0	0	0	0

Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈|<<〉 ……　最初のページに戻るボタンです。

〈>>〉 ……　次のページに進むボタンです。

Start from Control Index [History ID] and Sample Index [Sample ID] with [表示数] entries per page. ……　ページの表示設定です。
IDの一番小さいエントリがはじめに表示されます。
[History ID]欄と[Sample ID]欄で、はじめに表示する履歴を指定できます。
[表示数]欄で1ページあたりの表示数を指定できます。（最大99件まで）

History Index ……　「Configuration」→「Security」→「Switch」→「RMON」→「History」画面で設定した、履歴制御用エントリのIDが表示されます。
各IDのリンク先をクリックすると、「Detailed RMON History」画面に移動します。

Sample Index ……　履歴制御用エントリごとに、履歴データのIDが表示されます。

Sample Start ……　履歴が記録されたときのsysUpTime値が表示されます。

Drop ……　リソース不足のためにプローブによってパケットが破棄されたイベントの数が表示されます。

Octets ……　受信したデータのバイト数が表示されます。
※不正なデータのパケットも含まれます。

Pkts ……　受信したパケット数が表示されます。
※不正なデータのパケット、ブロードキャストパケット、マルチキャストパケットも含まれます。

Broad-cast ……　ブロードキャストアドレス宛ての有効な受信パケット数が表示されます。

Multi-cast ……　マルチキャストアドレス宛ての有効な受信パケット数が表示されます。

「History」画面

Monitor > Security > Switch > RMON > History

RMON History Overview

CRC Errors…… フレーミングビットを除き、フレームチェックシーケンス(FCS)を含むパケット長が64～1518バイトのパケットのうち、FCSエラー、またはアライメントエラーと判断された受信パケット数が表示されます。
※FCSが整数個のオクテットを持つとき、FCSエラーと判断されます。
※FCSのオクテット数が整数でないとき、アライメントエラーと判断されます。

Under-size …… 64バイト未満の受信パケットの数が表示されます。

Over-size…… 1518バイトを超える受信パケットの数が表示されます。

Frag. …… 64バイト未満でCRCが無効な受信フレームの数が表示されます。

Jabb. …… 64バイト以上でCRCが無効な受信フレームの数が表示されます。

Coll. …… イーサネットセグメントでの推定のコリジョン(衝突)回数が表示されます。

Utilization …… 物理層でのネットワーク使用率の推定値(×0.01%)が表示されます。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Detailed RMON History」画面

Monitor > Security > Switch > RMON > History

ドロップダウンリストで選択したHistory IDとSample IDのRMON統計情報が表示されます。

Detailed RMON History ID n

Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

Receive Total

Sample Start……　履歴が記録されたときのsysUpTime値が表示されます。

Drops ……　リソース不足のためにプローブによってパケットが破棄されたイベントの数が表示されます。

Octets ……　受信したデータのバイト数が表示されます。
※不正なデータのパケットも含まれます。

Pkts ……　受信したパケット数が表示されます。
※不正なデータのパケット、ブロードキャストパケット、マルチキャストパケットも含まれます。

Broadcast ……　ブロードキャストアドレス宛ての有効な受信パケット数が表示されます。

Multicast……　マルチキャストアドレス宛ての有効な受信パケット数が表示されます。

CRC/Alignment ……　フレーミングビットを除き、フレームチェックシーケンス(FCS)を含むパケット長が64～1518バイトのパケットのうち、FCSエラー、またはアライメントエラーと判断された受信パケット数が表示されます。
※FCSが整数個のオクテットを持つとき、FCSエラーと判断されます。
※FCSのオクテット数が整数でないとき、アライメントエラーと判断されます。

Undersize ……　64バイト未満の受信パケットの数が表示されます。

Oversize ……　1518バイトを超える受信パケットの数が表示されます。

Fragments ……　64バイト未満でCRCが無効な受信フレームの数が表示されます。

Jabber ……　64バイト以上でCRCが無効な受信フレームの数が表示されます。

Collisions……　イーサネットセグメントでの推定のコリジョン(衝突)回数が表示されます。

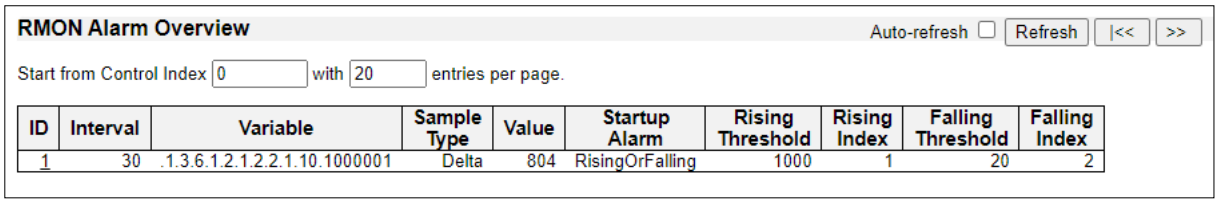
Utilization ……　物理層でのネットワーク使用率の推定値(×0.01%)が表示されます。

「Alarm」画面

Monitor > Security > Switch > RMON > Alarm

RMONアラームテーブルが表示されます。

RMON Alarm Overview



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈|<<〉……　最初のページに戻るボタンです。

〈>>〉 ……　次のページに進むボタンです。

Start from Control Index [ID] with [表示数] entries per page.
……　ページの表示設定です。
IDの一番小さいエントリがはじめに表示されます。
[ID]欄ではじめに表示するエントリを指定できます。
[表示数]欄で1ページあたりの表示数を指定できます。（最大99件まで）

ID ……　「Configuration」→「Security」→「Switch」→「RMON」→「Alarm」画面で設定した、アラーム制御用エントリのIDが表示されます。
各IDのリンク先をクリックすると、「Detailed RMON Alarm」画面に移動します。

Interval……　監視対象の値を取得し、しきい値と比較する間隔（秒）が表示されます。

Variable ……　監視対象のOIDが表示されます。

Sample Type ……　指定したOIDの値をしきい値と比較する方法が表示されます。

Value……　最後に取得した値が表示されます。

Startup Alarm ……　比較するしきい値が表示されます。

Rising Threshold ……　上昇しきい値が表示されます。

Rising Index ……　上昇しきい値を上回ったときのイベントIDが表示されます。

Falling Threshold……　下降しきい値が表示されます。

Falling Index ……　下降しきい値を下回ったときのイベントIDが表示されます。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Detailed RMON Alarm」画面

Monitor > Security > Switch > RMON > Alarm

ドロップダウンリストで選択したIDのRMONアラーム設定が表示されます。

Detailed RMON Alarm ID n

Auto-refresh …… 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 …… 最新の状態に更新するボタンです。

Receive Total

Interval…… 監視対象の値を取得し、しきい値と比較する間隔(秒)が表示されます。

Variable …… 監視対象のOIDが表示されます。

Sample Type …… 指定したOIDの値をしきい値と比較する方法が表示されます。

Value…… 最後に取得した値が表示されます。

Startup…… 比較するしきい値が表示されます。

RisingThreshold …… 上昇しきい値が表示されます。

RisingIndex …… 上昇しきい値を上回ったときのイベントIDが表示されます。

FallingThreshold …… 下降しきい値が表示されます。

FallingIndex …… 下降しきい値を下回ったときのイベントIDが表示されます。

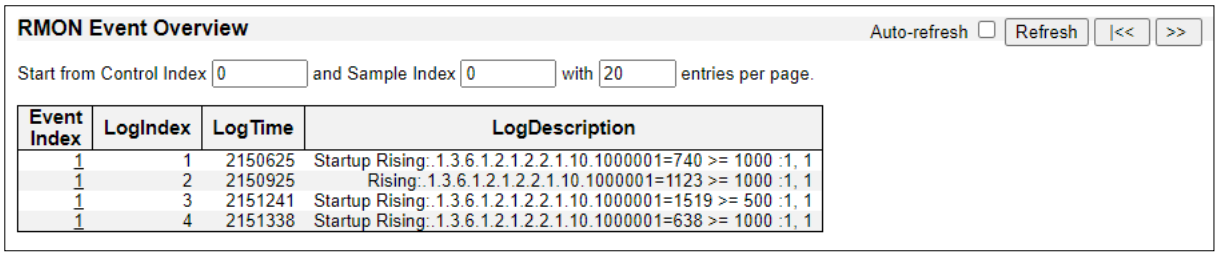
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Event」画面

Monitor > Security > Switch > RMON > Event

RMONイベントのログが表示されます。

RMON Event Overview



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈|<<〉……　最初のページに戻るボタンです。

〈>>〉 ……　次のページに進むボタンです。

Start from Control Index [Event ID] and Sample Index [Log ID] with [表示数] entries per page.
……　ページの表示設定です。
IDの一番小さいエントリがはじめに表示されます。
[Event ID]欄と[Log ID]欄ではじめに表示するイベントを指定できます。
[表示数]欄で1ページあたりの表示数を指定できます。（最大99件まで）

Event Index ……　「Configuration」→「Security」→「Switch」→「RMON」→「Event」画面で設定した、イベント制御用エントリのIDが表示されます。
各IDのリンク先をクリックすると、「Detailed RMON Event」画面に移動します。

LogIndex ……　イベントログのIDが表示されます。

LogTime ……　イベントが発生した時間が表示されます。

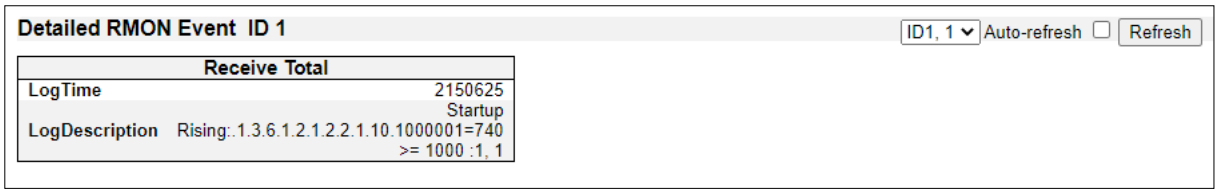
LogDescription……　イベントの詳細が表示されます。

「Detailed RMON Event」画面

Monitor > Security > Switch > RMON > Event

ドロップダウンリストで選択したEvent IDとLog IDのRMONイベントの情報が表示されます。

Detailed RMON Event ID n



Auto-refresh …… 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 …… 最新の状態に更新するボタンです。

LogTime …… イベントが発生した時間が表示されます。

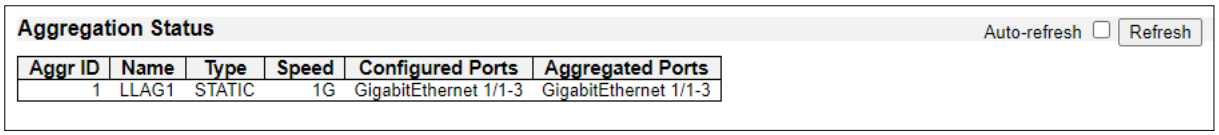
LogDescription…… イベントの詳細が表示されます。

「Status」画面

Monitor > Aggregation > Status

リンクアグリゲーショングループの状態が表示されます。

Aggregation Status



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

Aggr ID ……　リンクアグリゲーションのグループIDが表示されます。

Name ……　リンクアグリゲーションのグループ名が表示されます。

Type ……　アグリゲーショングループの動作が、「Static」か「LACP」で表示されます。

Speed ……　アグリゲーショングループの速度が表示されます。

Configured Ports……　アグリゲーショングループに所属しているポートが表示されます。

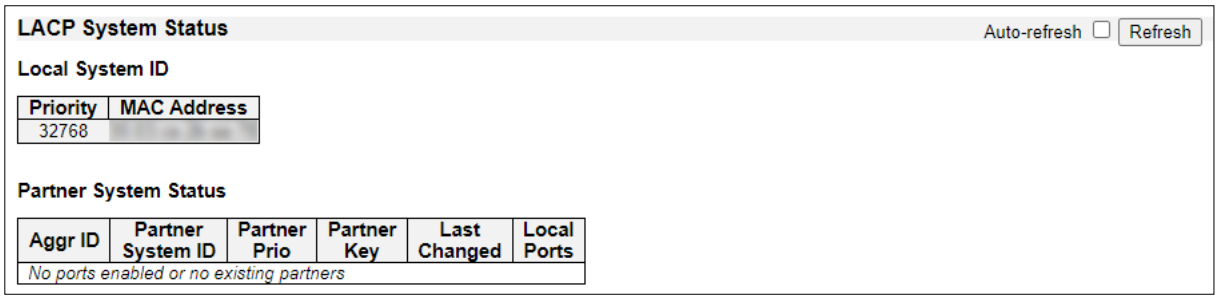
Aggregated Ports ……　アグリゲーショングループに所属しているポートで、実際に集約されているポートが表示されます。

「System Status」画面

Monitor > Aggregation > LACP > System Status

LACPの状態が表示されます。

LACP System Status



Auto-refresh ····· 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ····· 最新の状態に更新するボタンです。

Local System ID

Priority ····· 本製品の優先度が表示されます。

MAC Address ····· 本製品のLACPシステムID(MACアドレス)が表示されます。

Partner System Status

Aggr ID ····· リンクアグリゲーションのグループIDが表示されます。

Partner System ID ····· LACPパートナーのシステムID(MACアドレス)が表示されます。

Partner Prio ····· LACPパートナーの優先度が表示されます。

Partner Key ····· LACPパートナーのキーが表示されます。

Last Changed ····· アグリゲーション状態が変更されてからの時間が表示されます。

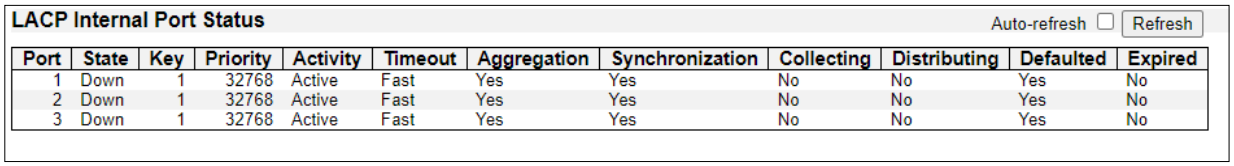
Local Ports ····· 集約されている本製品のポート番号が表示されます。

「Internal Status」画面

Monitor > Aggregation > LACP > Internal Status

本製品のポート(ローカルシステム)のLACP状態が表示されます。
LACPグループに所属するポートだけが表示されます。
※詳細は、IEEE 802.1AX-2014を参照してください。

LACP Internal Port Status


LACP Internal Port Status

Auto-refresh Refresh

Port	State	Key	Priority	Activity	Timeout	Aggregation	Synchronization	Collecting	Distributing	Defaulted	Expired
1	Down	1	32768	Active	Fast	Yes	Yes	No	No	Yes	No
2	Down	1	32768	Active	Fast	Yes	Yes	No	No	Yes	No
3	Down	1	32768	Active	Fast	Yes	Yes	No	No	Yes	No

Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

Port ……　本製品のポート番号が表示されます。

State……　ポートの状態が表示されます。

Down　：LACPが無効です。

Active　：LACPが有効です。

Standby　：スタンバイ状態です。

Key ……　ポートに割り当てられたキーが表示されます。
同じキーのポートだけが集約されます。

Priority……　アグリゲーショングループの優先度が表示されます。

Activity ……　アグリゲーショングループのLACPモードが「Active」、または「Passive」で表示されます。

Timeout ……　設定されたBPDU(Bridge Protocol Data Unit)の送信間隔が「Fast」、または「Slow」で表示されます。

Aggregation ……　アグリゲーショングループで集約できるかどうかが表示されます。

Synchronization ……　同期している(SynchronizationフラグがIN_SYNC)かどうかが表示されます。
同期の条件は下記のとおりです。
◎正しいLAGが割り当てられている。
◎グループは互換性のあるアグリゲーターにひもづいている。
◎送信されたシステムID、キー情報がLAG IDと一致している。

Collecting ……　受信フレームを収集するかどうかが表示されます。

Distributing ……　送信フレームを配信するかどうかが表示されます。

Defaulted ……　Actor(自分自身)のReceive machineがデフォルトのパートナー情報を使用しているかどうかが表示されます。

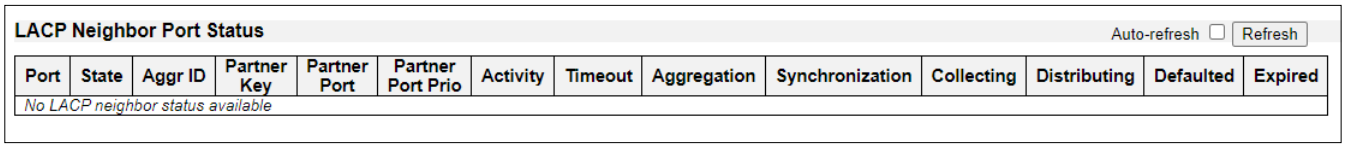
Expired……　Actor(自分自身)のReceive machineがEXPIRED状態かどうかが表示されます。

「Neighbor Status」画面

Monitor > Aggregation > LACP > Neighbor Status

LACPネイバーの状態が表示されます。
LACPグループに所属するポートだけが表示されます。
※詳細は、IEEE 802.1AX-2014を参照してください。

LACP Neighbor Port Status



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

Port ……　本製品のポート番号が表示されます。

State……　ポートの状態が表示されます。
Down　：LACPが無効です。
Active　：LACPが有効です。
Standby　：スタンバイ状態です。

Aggr ID ……　ポートに割り当てられているアグリゲーショングループのIDが表示されます。

Partner Key ……　パートナーからポートに割り当てられたキーが表示されます。

Partner Port ……　パートナーのポート番号が表示されます。

Partner Port Prio ……　パートナーポートの優先度が表示されます。

Activity ……　アグリゲーショングループのLACPモードが「Active」、または「Passive」で表示されます。

Timeout ……　パートナーポートに設定されたBPDU（Bridge Protocol Data Unit）の送信間隔が「Fast」、または「Slow」で表示されます。

Aggregation ……　アグリゲーショングループで集約できるとパートナーに判断されたかどうかが表示されます。

「Neighbor Status」画面

Monitor > Aggregation > LACP > Neighbor Status

LACP Neighbor Port Status

Synchronization …… 同期している(SynchronizationフラグがIN_SYNC)とパートナーに判断されたかどうかが表示されます。
同期の条件は下記のとおりです。
◎正しいLAGが割り当てられている。
◎グループは互換性のあるアグリゲーターにひもづいている。
◎送信されたシステムID、キー情報がLAG IDと一致している。

Collecting …… 受信フレームを収集するかどうかが表示されます。

Distributing …… 送信フレームを配信するかどうかが表示されます。

Defaulted …… パートナーのReceive machineがデフォルトのパートナー情報を使用しているかどうかが表示されます。

Expired…… パートナーのReceive machineがEXPIRED状態かどうかが表示されます。

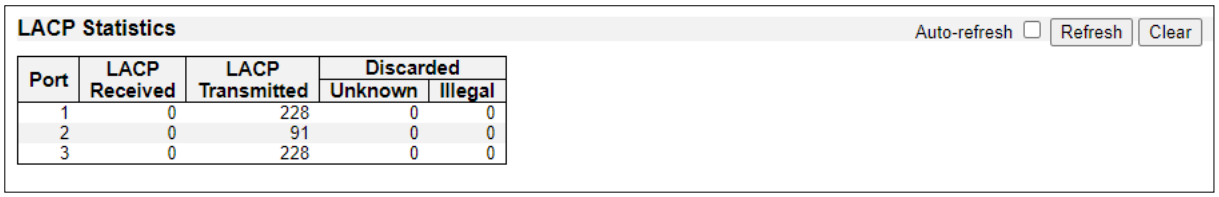
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Port Statistics」画面

Monitor > Aggregation > LACP > Port Statistics

各ポートのLACP統計情報が表示されます。

LACP Statistics



Auto-refresh ····· 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ····· 最新の状態に更新するボタンです。

〈Clear〉 ····· すべてのポートのカウンター値を0にするボタンです。

Port ····· 本製品のポート番号が表示されます。

LACP Received ····· 受信したLACPフレーム数が表示されます。

LACP Transmitted ····· 送信したLACPフレーム数が表示されます。

Discarded Unknown ····· 破棄された不明なLACPフレーム数が表示されます。

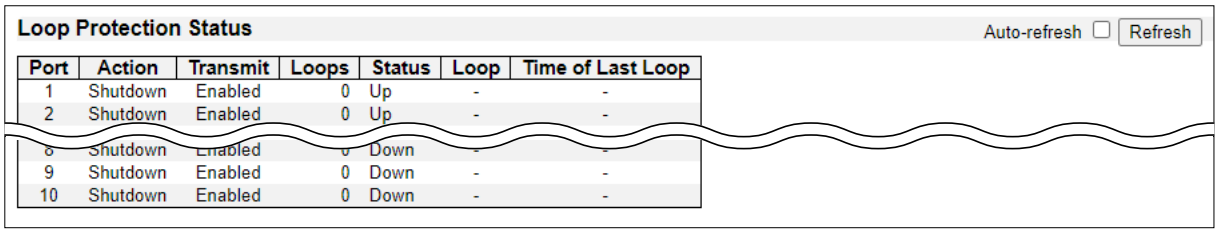
Discarded Illegal ····· 破棄された不正なLACPフレーム数が表示されます。

「Loop Protection」画面

Monitor > Loop Protection

ループプロテクションの状態が表示されます。

Loop Protection Status



Auto-refresh ····· 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ····· 最新の状態に更新するボタンです。

Port ····· 本製品のポート番号が表示されます。

Action ····· ポートでループが検出されたときの動作が表示されます。

Transmit ····· ポートの送信動作が表示されます。

Loops ····· ループが検出された回数が表示されます。

Status ····· ポートの状態が表示されます。

Loop ····· 現時点でループが検出されているかどうかが表示されます。

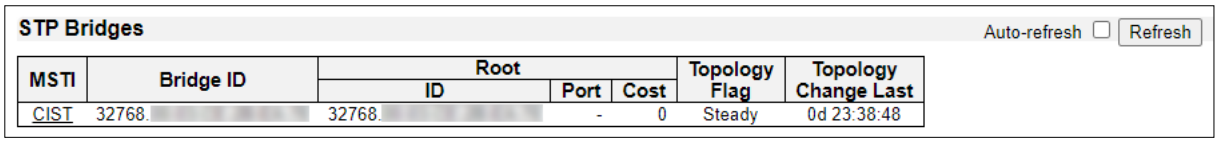
Time of Last Loop ····· 最後にループが検出された時刻が表示されます。

「Bridge Status」画面

Monitor > Spanning Tree > Bridge Status

STPブリッジインスタンスの状態が表示されます。

STP Bridges



Auto-refresh ····· 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ····· 最新の状態に更新するボタンです。

MSTI ····· ブリッジインスタンスが表示されます。
各インスタンスのリンク先をクリックすると、「STP Detailed Bridge Status」画面に移動します。

Bridge ID ····· ブリッジインスタンスのブリッジIDが表示されます。

Root ID ····· ルートブリッジのブリッジIDが表示されます。

Root Port ····· ルートポートとして使用しているポートの番号が表示されます。

Root Cost ····· ルートパスコストが表示されます。
ルートブリッジの場合は「0」が表示されます。
その他のブリッジでは、ルートブリッジまでの最小パスコストの合計が表示されます。

Topology Flag ····· Topology Changeフラグの状態が表示されます。

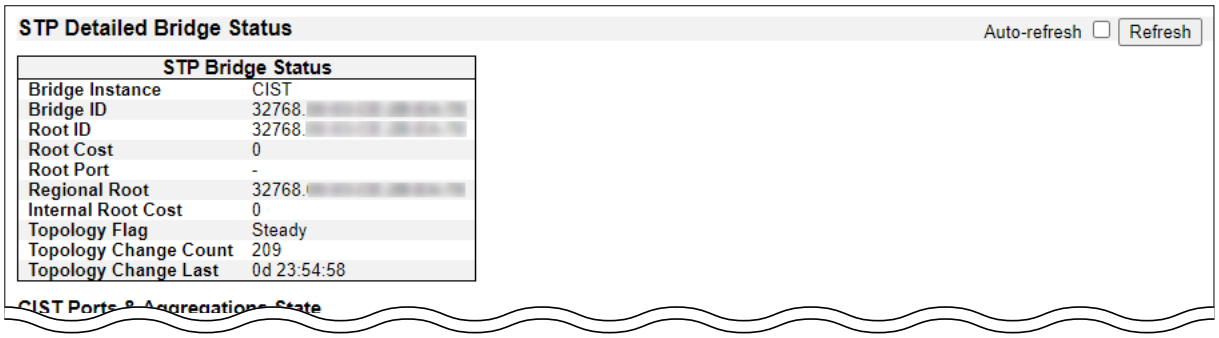
Topology Change Last ····· 最後にトポロジーが変更されてから経過した時間が表示されます。

「STP Detailed Bridge Status」画面

Monitor > Spanning Tree > Bridge Status

特定のSTPブリッジインスタンスの詳細情報が表示されます。

STP Detailed Bridge Status



Auto-refresh ····· 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ····· 最新の状態に更新するボタンです。

STP Bridge Status

Bridge Instance ····· ブリッジインスタンスが表示されます。

Bridge ID ····· ブリッジインスタンスのブリッジIDが表示されます。

Root ID ····· ルートブリッジのブリッジIDが表示されます。

Root Cost ····· ルートパスコストが表示されます。
ルートブリッジの場合は「0」が表示されます。
その他のブリッジでは、ルートブリッジまでの最小パスコストの合計が表示されます。

Root Port ····· ルートポートとして使用しているポートの番号が表示されます。

Regional Root ····· MSTPリージョン内の、リージョナルルートブリッジのブリッジIDが表示されます。
※CISTインスタンスのときだけ表示されます。

Internal Root Cost ····· リージョナルルートパスコストが表示されます。
リージョナルルートブリッジの場合は「0」が表示されます。
MSTPリージョン内のその他のCISTインスタンスでは、内部ルートブリッジまでの最小パスコストの合計が表示されます。
※CISTインスタンスのときだけ表示されます。

Topology Flag ····· Topology Changeフラグの状態が表示されます。

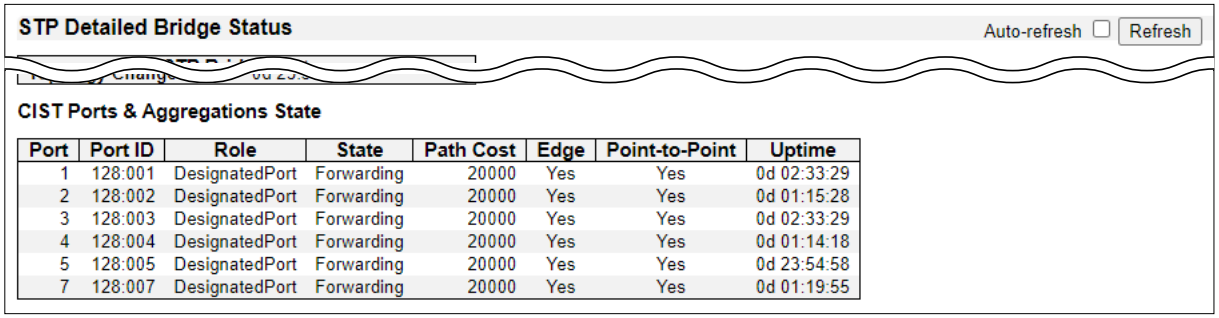
Topology Change Count ····· トポロジーを変更した回数が表示されます。
※1秒間隔でカウントされます。

Topology Change Last ····· 最後にトポロジーが変更されてから経過した時間が表示されます。

「STP Detailed Bridge Status」画面

Monitor > Spanning Tree > Bridge Status

STP Detailed Bridge Status



CIST Ports & Aggregations State

Port ……

STPポートのポート番号が表示されます。

Port ID ……

STPプロトコルで使用されるポートIDが表示されます。
ポートIDはブリッジポートの優先度とポート番号で構成されています。

Role ……

ポートの役割が表示されます。

State……

ポートの状態が表示されます。

Path Cost ……

ポートのパスコストが表示されます。
パスコストを自動で計算するかどうかは、設定によって異なります。

Edge ……

エッジポートかどうかが表示されます。
エッジポートは、ブリッジが取り付けられておらず、直接エッジデバイスに接続しているポートです。
エッジポートを自動で判別するかどうかは、設定によって異なります。
エッジポートはループしないため、すぐにForwarding状態に移行します。

Point-to-Point ……

ポートがポイントツーポイントリンク(直接機器が接続されている)かが表示されます。
ポイントツーポイントリンクを自動で判別するかどうかは、設定によって異なります。
シェアードリンク(HUBなどで複数の機器が接続されている)よりもポイントツーポイントリンクの方が速くForwarding状態へ移行します。

Uptime ……

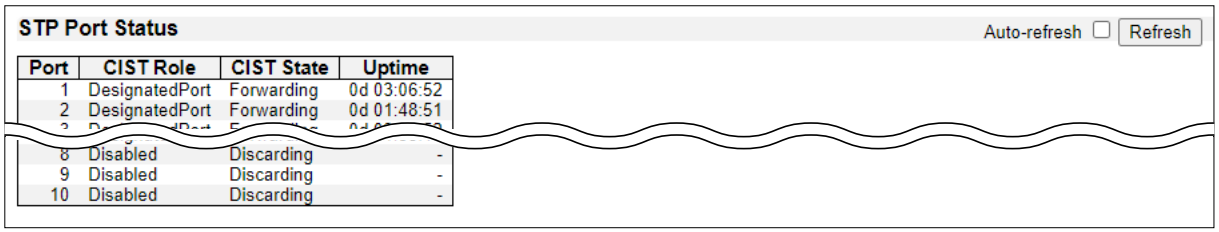
最後にポートが初期化されてから経過した時間が表示されます。

「Port Status」画面

Monitor > Spanning Tree > Port Status

STP CISTポートの状態が表示されます。

STP Port Status



Auto-refresh ····· 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ····· 最新の状態に更新するボタンです。

Port ····· 本製品のポート番号が表示されます。

CIST Role ····· CISTポートの役割が表示されます。

CIST State ····· CISTポートの状態が表示されます。

Uptime ····· 最後にポートが初期化されてから経過した時間が表示されます。

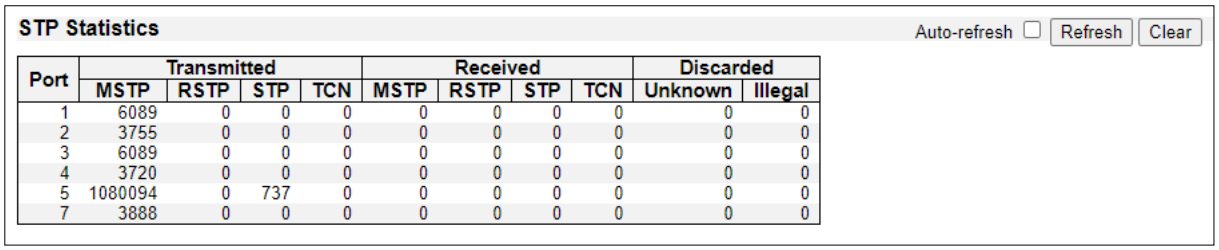
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Port Statistics」画面

Monitor > Spanning Tree > Port Statistics

STPポートの統計情報が表示されます。

STP Statistics



Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1	6089	0	0	0	0	0	0	0	0	0
2	3755	0	0	0	0	0	0	0	0	0
3	6089	0	0	0	0	0	0	0	0	0
4	3720	0	0	0	0	0	0	0	0	0
5	1080094	0	737	0	0	0	0	0	0	0
7	3888	0	0	0	0	0	0	0	0	0

Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈Clear〉 ……　すべてのポートのカウンター値を0にするボタンです。

Port ……　本製品のポート番号が表示されます。

Transmitted/Received

MSTP ……　送受信したMSTP BPDUの数が表示されます。

RSTP……　送受信したRSTP BPDUの数が表示されます。

STP ……　送受信したレガシーSTP Configuration BPDUの数が表示されます。

TCN ……　送受信したレガシートトポロジー変更通知(TCN)BPDUの数が表示されます。

Discarded

Unknown……　受信、または破棄した不明なスパニングツリーのBPDUの数が表示されます。

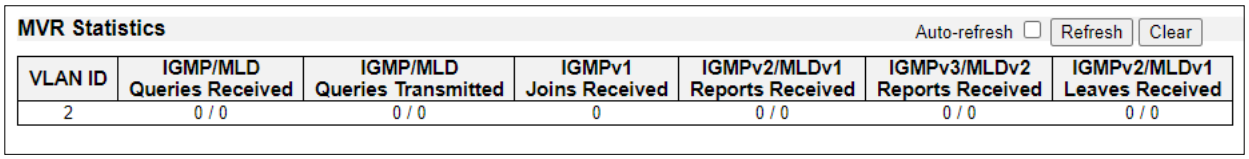
Illegal ……　受信、または破棄した不正なスパニングツリーのBPDUの数が表示されます。

「Statistics」画面

Monitor > MVR > Statistics

MVRの統計情報が表示されます。

MVR Statistics



Auto-refresh ····· 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ····· 最新の状態に更新するボタンです。

〈Clear〉 ····· すべてのカウンター値を0にするボタンです。

VLAN ID ····· マルチキャストVLAN IDが表示されます。

IGMP/MLD Queries Received ····· 受信したIGMP QueryメッセージとMLD Queryメッセージの数が表示されます。

IGMP/MLD Queries Transmitted··· 送信したIGMP QueryメッセージとMLD Queryメッセージの数が表示されます。

IGMPv1 Joins Received ····· 受信したIGMPv1 Joinメッセージの数が表示されます。

IGMPv2/MLDv1 Reports Received 受信したIGMPv2 JoinメッセージとMLDv1 Reportメッセージの数が表示されます。

IGMPv3/MLDv2 Reports Received 受信したIGMPv1 JoinメッセージとMLDv2 Reportメッセージの数が表示されます。

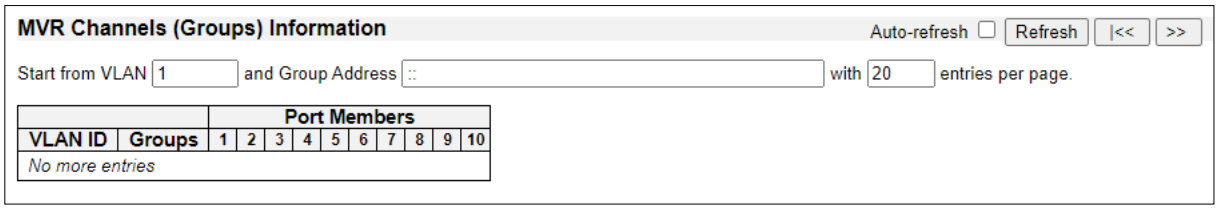
IGMPv2/MLDv1 Leaves Received 受信したIGMPv2 LeaveメッセージとMLDv1 Doneメッセージの数が表示されます。

「MVR Channel Groups」画面

Monitor > MVR > MVR Channel Groups

MVRチャンネル(グループ)の情報が表示されます。
MVRチャンネル(グループ)の情報は、VLAN IDとグループでソートされます。

MVR Channels (Groups) Information



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈|<<〉……　最初のページに戻るボタンです。

〈>>〉 ……　次のページに進むボタンです。

Start from VLAN [VLAN ID] and Group Address [グループアドレス] with [表示数] entries per page.
……　ページの表示設定です。
IDの一番小さいエントリがはじめに表示されます。
[VLAN ID]欄と[グループアドレス]欄ではじめに表示するイベントを指定できます。
[表示数]欄で1ページあたりの表示数を指定できます。(最大99件まで)

VLAN ID ……　グループのVLAN IDが表示されます。

Groups ……　グループのグループIDが表示されます。

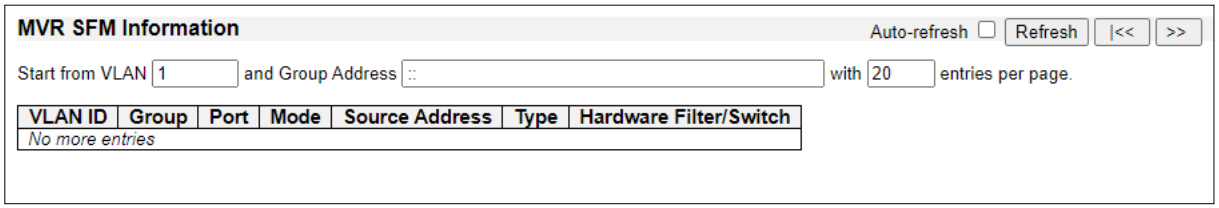
Port Members ……　グループに所属しているポートが表示されます。

「MVR SFM Information」画面

Monitor > MVR > MVR SFM Information

MVR SFM(Source-Filtered Multicast)の情報が表示されます。
SSM(Source-Specific Multicast)情報も含まれています。
MVR SFMの情報は、VLAN ID、グループアドレス、ポートでソートされます。
同じグループに所属する異なる送信元アドレスのエントリは、1つのエントリとして扱われます。

MVR SFM Information



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈|<<〉 ……　最初のページに戻るボタンです。

〈>>〉 ……　次のページに進むボタンです。

Start from VLAN [VLAN ID] and Group Address [グループアドレス] with [表示数] entries per page. ……
ページの表示設定です。
IDの一番小さいエントリがはじめに表示されます。
[VLAN ID]欄と[グループアドレス]欄ではじめに表示するイベントを指定できます。
[表示数]欄で1ページあたりの表示数を指定できます。(最大99件まで)

VLAN ID ……　グループのVLAN IDが表示されます。

Groups ……　グループのグループアドレスが表示されます。

Port ……　グループに所属しているポートが表示されます。

Mode ……　フィルタリングのモードが表示されます。

Source Address ……　送信元IPアドレスが表示されます。
使用できる送信元IPアドレスは、グループごとに最大8個までです。
送信元IPアドレスがない場合は、「None」が表示されます。

Type ……　動作タイプが表示されます。

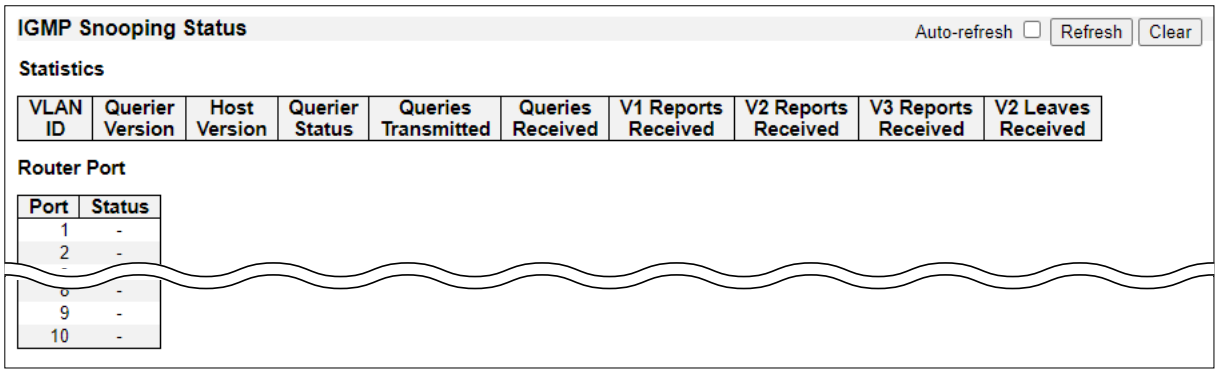
Hardware Filter/Switch ……　送信元IPv4/IPv6アドレスから特定のグループアドレス宛てのデータをハードウェアで処理するかどうかが表示されます。

「Status」画面

Monitor > IPMC > IGMP Snooping > Status

IGMPスヌーピングの状態が表示されます。

IGMP Snooping Status



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈Clear〉 ……　すべてのカウンター値を0にするボタンです。

Statistics

VLAN ID ……　VLAN IDが表示されます。

Querier Version ……　クエリアのバージョンが表示されます。

Host Version ……　ホストのバージョンが表示されます。

Querier Status ……　クエリアの状態が「ACTIVE」、または「IDLE」で表示されます。
インターフェースが無効の場合、「DISABLE」が表示されます。

Queries Transmitted ……　送信したQueryメッセージの数が表示されます。

Queries Received ……　受信したQueryメッセージの数が表示されます。

V1 Reports Received ……　受信したV1 Reportメッセージの数が表示されます。

V2 Reports Received ……　受信したV2 Reportメッセージの数が表示されます。

V3 Reports Received ……　受信したV3 Reportメッセージの数が表示されます。

V2 Leaves Received ……　受信したV2 Leaveメッセージの数が表示されます。

Router Port

Port ……　本製品のポート番号が表示されます。

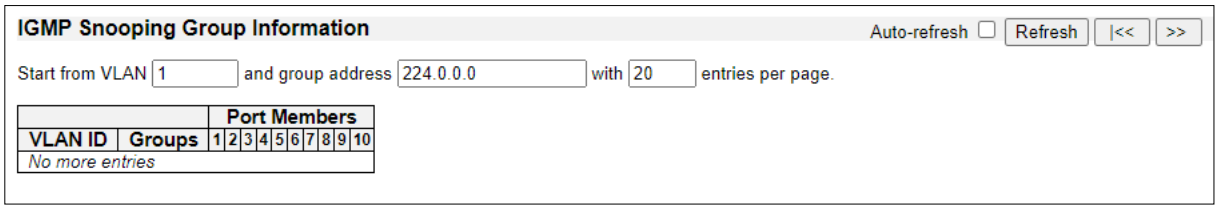
Status ……　ルーターポートとして使用されているかどうかが表示されます。
ルーターポートは、レイヤー3 マルチキャストデバイス、またはIGMPクエリアが接続されているポートです。
特定のポートをルーターポートに設定している場合は、「Static」が表示されます。
自動でルーターポートを学習している場合は、「Dynamic」が表示されます。
「Static」と「Dynamic」の両方を使用している場合は、「Both」が表示されます。

「Groups Information」画面

Monitor > IPMC > IGMP Snooping > Groups Information

IGMPグループテーブルが表示されます。
IGMPグループテーブルは、VLAN ID、グループアドレスでソートされます。

IGMP Snooping Group Information



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈|<<〉……　最初のページに戻るボタンです。

〈>>〉 ……　次のページに進むボタンです。

Start from VLAN [VLAN ID] and group address [グループアドレス] with [表示数] entries per page.
……　ページの表示設定です。
IDの一番小さいエントリがはじめに表示されます。
[VLAN ID]欄と[グループアドレス]欄ではじめに表示するイベントを指定できます。
[表示数]欄で1ページあたりの表示数を指定できます。(最大99件まで)

VLAN ID ……　グループのVLAN IDが表示されます。

Groups ……　グループのグループアドレスが表示されます。

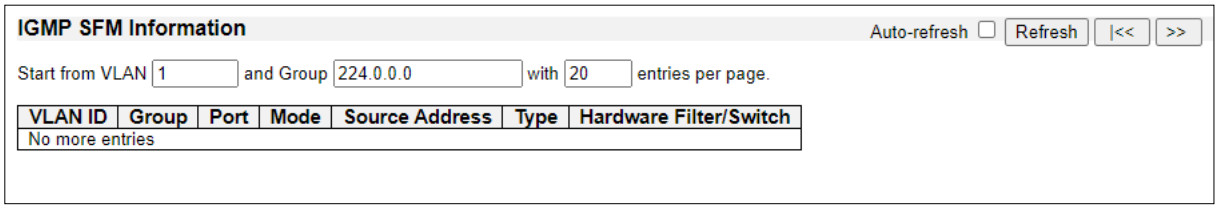
Port Members ……　グループに所属しているポートが表示されます。

「IPv4 SFM Information」画面

Monitor > IPMC > IGMP Snooping > IPv4 SFM Information

IGMP SFM(Source-Filtered Multicast)の情報が表示されます。
IGMP SSM(Source-Specific Multicast)情報も含まれています。
IGMP SFMの情報は、VLAN ID、グループアドレス、ポートでソートされます。
同じグループに所属する異なる送信元アドレスのエントリは、1つのエントリとして扱われます。

IGMP SFM Information



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈|<<〉……　最初のページに戻るボタンです。

〈>>〉 ……　次のページに進むボタンです。

Start from VLAN [VLAN ID] and Group [グループアドレス] with [表示数] entries per page.
……　ページの表示設定です。
IDの一番小さいエントリがはじめに表示されます。
[VLAN ID]欄と[グループアドレス]欄ではじめに表示するイベントを指定できます。
[表示数]欄で1ページあたりの表示数を指定できます。(最大99件まで)

VLAN ID ……　グループのVLAN IDが表示されます。

Group ……　グループのグループアドレスが表示されます。

Port ……　グループに所属しているポートが表示されます。

Mode……　フィルタリングのモードが表示されます。

Source Address ……　送信元IPv4アドレスが表示されます。
使用できる送信元IPアドレスは、グループごとに最大8個までです。
送信元IPアドレスがない場合は、「None」が表示されます。

Type ……　動作タイプが表示されます。

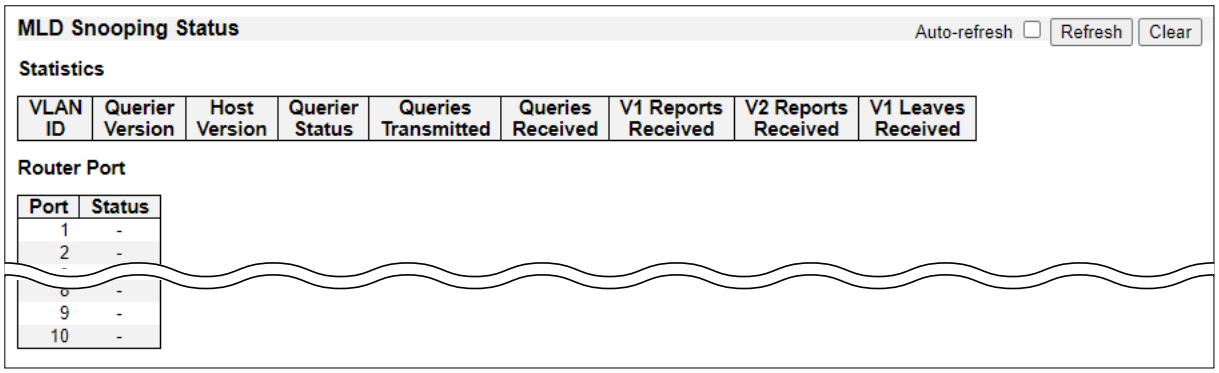
Hardware Filter/Switch ……　送信元IPv4アドレスから特定のグループアドレス宛てのデータをハードウェアで処理するかどうかが表示されます。

「Status」画面

Monitor > IPMC > MLD Snooping > Status

MLDスヌーピングの状態が表示されます。

MLD Snooping Status



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈Clear〉 ……　すべてのカウンター値を0にするボタンです。

Statistics

VLAN ID ……　VLAN IDが表示されます。

Querier Version ……　クエリアのバージョンが表示されます。

Host Version ……　ホストのバージョンが表示されます。

Querier Status ……　クエリアの状態が「ACTIVE」、または「IDLE」で表示されます。
インターフェースが無効の場合、「DISABLE」が表示されます。

Queries Transmitted ……　送信したQueryメッセージの数が表示されます。

Queries Received ……　受信したQueryメッセージの数が表示されます。

V1 Reports Received ……　受信したV1 Reportメッセージの数が表示されます。

V2 Reports Received ……　受信したV2 Reportメッセージの数が表示されます。

V1 Leaves Received ……　受信したV2 Leaveメッセージの数が表示されます。

Router Port

Port ……　本製品のポート番号が表示されます。

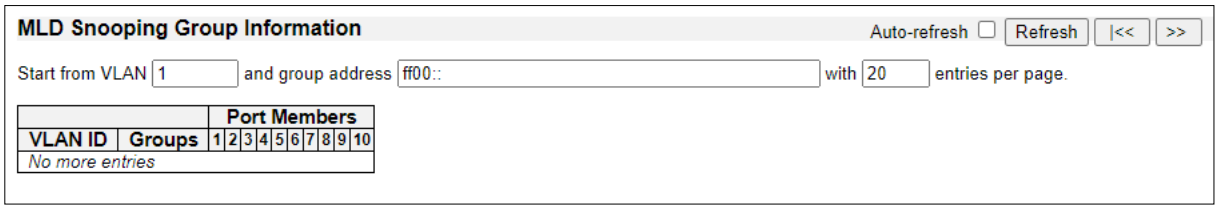
Status ……　ルーターポートとして使用されているかどうかが表示されます。
ルーターポートは、レイヤー3 マルチキャストデバイス、またはMLDクエリアが接続されているポートです。
特定のポートをルーターポートに設定している場合は、「Static」が表示されます。
自動でルーターポートを学習している場合は、「Dynamic」が表示されます。
「Static」と「Dynamic」の両方を使用している場合は、「Both」が表示されます。

「Groups Information」画面

Monitor > IPMC > MLD Snooping > Groups Information

MLDグループテーブルが表示されます。
MLDグループテーブルは、VLAN ID、グループアドレスでソートされます。

MLD Snooping Group Information



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈|<<〉……　最初のページに戻るボタンです。

〈>>〉 ……　次のページに進むボタンです。

Start from VLAN [VLAN ID] and group address [グループアドレス] with [表示数] entries per page.
……　ページの表示設定です。
IDの一番小さいエントリがはじめに表示されます。
[VLAN ID]欄と[グループアドレス]欄ではじめに表示するイベントを指定できます。
[表示数]欄で1ページあたりの表示数を指定できます。(最大99件まで)

VLAN ID ……　グループのVLAN IDが表示されます。

Groups ……　グループのグループアドレスが表示されます。

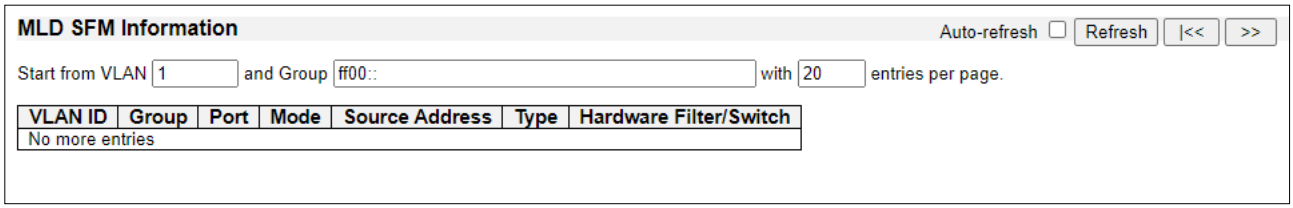
Port Members ……　グループに所属しているポートが表示されます。

「IPv6 SFM Information」画面

Monitor > IPMC > IGMP Snooping > IPv6 SFM Information

MLD SFM(Source-Filtered Multicast)の情報が表示されます。
MLD SSM(Source-Specific Multicast)情報も含まれています。
MLD SFMの情報は、VLAN ID、グループアドレス、ポートでソートされます。
同じグループに所属する異なる送信元アドレスのエントリは、1つのエントリとして扱われます。

IGMP SFM Information



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈|<<〉 ……　最初のページに戻るボタンです。

〈>>〉 ……　次のページに進むボタンです。

Start from VLAN [VLAN ID] and Group [グループアドレス] with [表示数] entries per page.
……　ページの表示設定です。
IDの一番小さいエントリがはじめに表示されます。
[VLAN ID]欄と[グループアドレス]欄ではじめに表示するイベントを指定できます。
[表示数]欄で1ページあたりの表示数を指定できます。(最大99件まで)

VLAN ID ……　グループのVLAN IDが表示されます。

Group ……　グループのグループアドレスが表示されます。

Port ……　グループに所属しているポートが表示されます。

Mode ……　フィルタリングのモードが表示されます。

Source Address ……　送信元IPv6アドレスが表示されます。
使用できる送信元IPアドレスは、グループごとに最大8個までです。
送信元IPアドレスがない場合は、「None」が表示されます。

Type ……　動作タイプが表示されます。

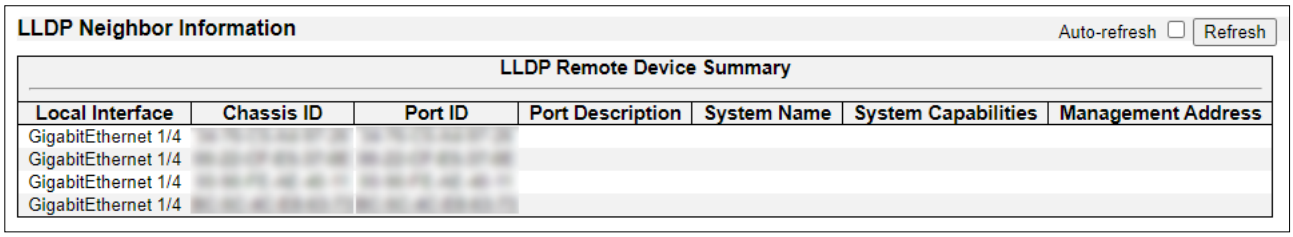
Hardware Filter/Switch ……　送信元IPv6アドレスから特定のグループアドレス宛てのデータをハードウェアで処理するかどうかが表示されます。

「Neighbors」画面

Monitor > LLDP > Neighbors

LLDP機能を使用しているときに、隣接しているデバイス(ネイバー)の一覧が表示されます。

LLDP Neighbor Information



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

LLDP Remote Device Summary

Local Interface ……　LLDPフレームを受信したインターフェースが表示されます。

Chassis ID ……　LLDPフレームに含まれるChassis IDが表示されます。
Chassis IDは、ネイバーのMACアドレスなどの情報です。

Port ID ……　LLDPフレームに含まれるPort IDが表示されます。
Port IDは、ネイバーがLLDPを送信したインターフェースの情報です。

Port Description ……　LLDPフレームに含まれるPort Descriptionが表示されます。
Port Descriptionは、ネイバーが設定したポートの説明です。

System Name ……　LLDPフレームに含まれるSystem Nameが表示されます。
System Nameは、ネイバーが設定したデバイスの名前です。

System Capabilities ……　LLDPフレームに含まれるSystem Capabilitiesが表示されます。
System Capabilitiesは、ネイバーが使用できる機能です。

1. Other
2. Repeater
3. Bridge
4. WLAN Access Point
5. Router
6. Telephone
7. DOCSIS cable device
8. Station only
9. Reserved

※有効になっている機能には「(+)」が、無効になっている機能には「(-)」が表示されます。

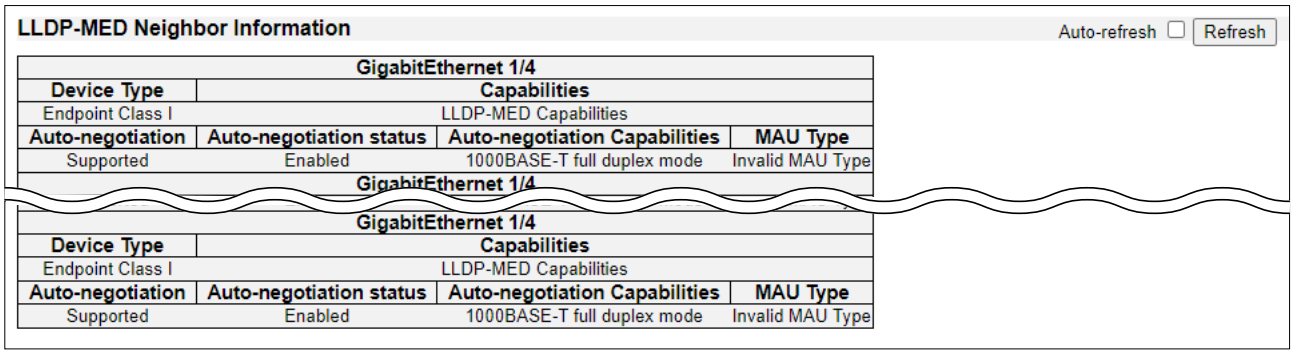
Management Address ……　LLDPフレームに含まれるManagement Addressが表示されます。
Management Addressは、上位層のエンティティがネットワーク管理のために使用するネイバーのIPアドレスやMACアドレスなどです。

「LLDP-MED Neighbors」画面

Monitor > LLDP > LLDP-MED Neighbors

LLDP-MEDネイバーの情報が表示されます。
※LLDP-MED対応のVoIPデバイスに適用されます。

LLDP-MED Neighbor Information



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

Interface ……　LLDPフレームを受信したインターフェースが表示されます。

Device Type ……　デバイスの種類が表示されます。
LLDP-MEDデバイスの種類は、TIA-1057で定義されたネットワーク接続デバイス、または特定のクラスのエンドポイントデバイスに分類されます。

LLDP-MEDネットワーク接続デバイス：
ネットワーク接続デバイスは、LLDP-MEDエンドポイントデバイスにIEEE802ベースLANインフラストラクチャへのアクセスを提供するLLDP-MEDデバイスです。
LLDP-MEDネットワーク接続デバイスは、次のどれかのテクノロジーに基づくLANアクセスデバイスです。

1. LAN スイッチ/ルーター
2. IEEE 802.1 ブリッジ
3. IEEE 802.3 レピータ（歴史的な理由から含まれています。）
4. IEEE 802.11 ワイヤレスアクセスポイント
5. IEEE 802.1ABとTIA-1057で定義されたMED拡張機能に対応し、任意の方法でIEEE 802フレームを中継できるデバイス。

「LLDP-MED Neighbors」画面

Monitor > LLDP > LLDP-MED Neighbors

LLDP-MED Neighbor Information

Device Type(つづき) ……

LLDP-MEDエンドポイントデバイス：
エンドポイントデバイスはネットワークの終端に位置し、IEEE 802 LANテクノロジーベースのIP通信サービスを提供するLLDP-MEDデバイスです。
LLDP-MEDエンドポイントデバイスカテゴリに属するLLDP-MEDスキームは、さらにエンドポイントデバイスクラスで分類されます。
LLDP-MEDエンドポイントデバイスクラスは、下位のエンドポイントデバイスクラスで定義された機能をサポートするように定義されています。
たとえば、Media Endpoint(クラス II)のLLDP-MEDエンドポイントデバイスは、Generic Endpoints(クラス I)に適用されるTIA-1057のすべての機能もサポートし、Communication Device(クラス III)のLLDP-MEDエンドポイントデバイスは、Media Endpoint(クラス II)とGeneric Endpoints(クラス I)の両方に適用されるTIA-1057のすべての機能もサポートします。

LLDP-MED Generic Endpoint(クラス I)：
TIA-1057で定義されているLLDP検出サービスを必要とするすべてのエンドポイントデバイスに適用できますが、IPメディア機能をサポートしたり、エンドユーザー通信アプライアンスとして機能したりしません。
このようなデバイスには、IP通信コントローラー、その他の通信関連サーバー、またはTIA-1057で定義されている基本サービスを必要とするデバイスが含まれます。
クラス Iで定義される検出サービスには、LAN構成、デバイスの場所、ネットワークポリシー、電源管理、およびインベントリ管理が含まれます。

LLDP-MED Media Endpoint(クラス II)：
IPメディア機能をサポートするすべてのエンドポイントデバイスに適用できますが、特定のエンドユーザーに関連付けられている場合と、関連付けられていない場合があります。
Generic Endpoints(クラス I)に対して定義されたすべての機能が含まれており、メディアストリーミングに関連する機能を含むように拡張されています。
クラス IIに準拠することが望ましい製品には、音声/メディアゲートウェイ、会議ブリッジ、メディアサーバーなどがあります。
クラス IIで定義される検出サービスには、メディアタイプ固有のネットワーク層ポリシー検出が含まれます。

LLDP-MED Communication Endpoint(クラス III)
IPメディア機能をサポートするエンドユーザー通信アプライアンスとして機能するすべてのエンドポイントデバイスに適用されます。
Media Endpoint(クラス II)とGeneric Endpoints(クラス I)に対して定義されたすべての機能が含まれており、エンドユーザーデバイスに関連する機能を含むように拡張されています。
クラス IIIに準拠することが望ましい製品には、IP電話、パソコンベースのソフトフォン、またはエンドユーザーを直接サポートするその他の通信機器などのエンド ユーザー通信機器などがあります。
クラス IIIで定義される検出サービスには、位置情報識別子(ECS/E911情報を含む)の提供、組み込みL2スイッチのサポート、インベントリ管理が含まれます。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「LLDP-MED Neighbors」画面

Monitor > LLDP > LLDP-MED Neighbors

LLDP-MED Neighbor Information

Capabilities ……

ネイバーが対応しているLLDP-MED機能が表示されます。
1. LLDP-MED capabilities
2. Network Policy
3. Location Identification
4. Extended Power via MDI - PSE
5. Extended Power via MDI - PD
6. Inventory
7. Reserved

Application Type ……

エンドポイントデバイス、またはネットワーク接続デバイスからアドバタイズされた、ネットワークポリシーに関連付けられたアプリケーションタイプが表示されます。

Voice：
専用のIP電話端末や対話型音声サービスに対応した類似機器に使用します。
これらのデバイスは、切り離されたVLAN上に設置しデータアプリケーションと分離することで、設置を簡単にし、セキュリティーを強化します。

Voice Signalling：
ボイスメディアとは異なるボイスシグナリング用のポリシーを必要とするネットワークトポロジーに使用します。

Guest Voice：
独自のIP電話装置や対話型音声サービスに対応した類似機器を使用して、ゲストユーザーやビジター向けに機能が制限された音声サービスをサポートします。

Guest Voice Signalling：
ゲストボイスメディアとは異なるゲストボイスシグナリング用のポリシーを必要とするネットワークトポロジーに使用します。

Softphone Voice：
デスクトップパソコンやノートパソコンなど、一般的なデータ処理用デバイス上のソフトフォンアプリケーションに使用します。

Video Conferencing：
ビデオ会議専用の機器や、リアルタイムのインタラクティブビデオ/オーディオサービスに対応した類似機器で使用します。

Streaming Video：
ブロードキャストやマルチキャストでのビデオコンテンツ配信、および特定のネットワークポリシー処理を必要とするストリーミングビデオサービスに対応した類似のアプリケーションで使用します。
バッファリングでTCPに依存するビデオアプリケーションでの使用は想定していません。

Video Signalling：
ビデオメディアと異なるビデオシグナリング用のポリシーを必要とするネットワークトポロジーに使用します。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「LLDP-MED Neighbors」画面

Monitor > LLDP > LLDP-MED Neighbors

LLDP-MED Neighbor Information

Policy ……

ネットワークポリシーが定義されているかどうかが表示されます。

Unknown：
ネットワークポリシーは不明です。

Defined：
ネットワークポリシーが定義されています。

TAG ……

使用しているVLANの種類が表示されます。

Untagged：
タグなしフレーム形式を使用しています。

Tagged：
IEEE 802.1Qタグ付きフレーム形式を使用しています。

VLAN ID ……

IEEE 802.1Q-2003で定義されている、インターフェースのVLAN ID(VID)が表示されます。
優先タグ付きフレームを使用している場合、「0」が表示されます。
優先タグ付きフレームを使用している場合は、IEEE 802.1D優先度だけが重要で、入力インターフェースのデフォルトのPVIDが代わりに使用されます。

Priority……

Layer 2 Priority値が表示されます。

DSCP ……

IETF RFC 2474で定義されている、Diffserv使用時のDSCP値が表示されます。

Auto-negotiation ……

リンクパートナーがMAC/PHYオートネゴシエーションに対応しているかどうかが表示されます。

Auto-negotiation status ……

リンクパートナーのオートネゴシエーションが有効になっているかが表示されます。
オートネゴシエーションに対応していて無効になっている場合、802.3 PMDの動作モードはMAU typeフィールドの値によって決定します。

Auto-negotiation Capabilities…

リンクパートナーのMAC/PHYの能力が表示されます。

MAU Type ……

MAU typeフィールドの値が表示されます。

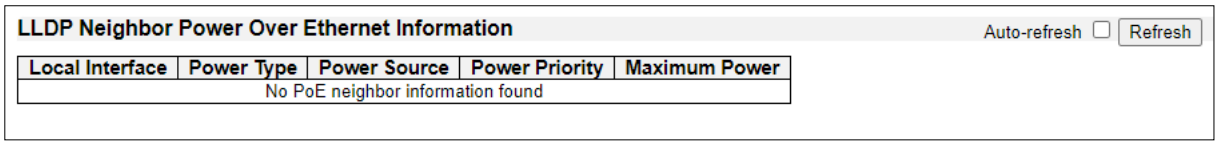
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「PoE」画面

Monitor > LLDP > PoE

LLDP PoEネイバーの状態が表示されます。

LLDP Neighbor Power Over Ethernet Information



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

Local Interface ……　LLDPフレームを受信したインターフェースが表示されます。

Power Type ……　デバイスの種類が「PSE」(Power Sourcing Entity)、または「PD」(Power Device)で表示されます。
※デバイスの種類が不明な場合は、「Reserved」と表示されます。

Power Source ……　デバイスが使用している電源が表示されます。
PSEデバイスの場合、プライマリ電源、またはバックアップ電源を使用します。
PDデバイスの場合、ローカル電源かPSEを使用するか、または両方を電源として使用します。
※使用している電源が不明な場合は、「Unknown」と表示されます。

Power Priority ……　PDデバイスの優先度、または電力を供給しているPSEデバイスのインターフェースに設定された電力優先度が「Critical」、「High」、「Low」表示されます。
※優先度が不明な場合は、「Unknown」と表示されます。

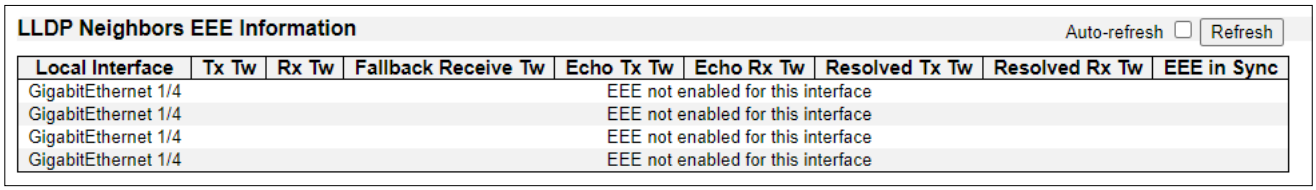
Maximum Power ……　PDデバイスがPSEデバイスに要求している最大電力(W)、または現在の設定に基づく最大長のケーブル経由でPSEデバイスが供給できる最小電力が表示されます。
表示される最大値は102.3Wです。
※電力が102.3Wよりも高い場合、「reserved」と表されます。

「EEE」画面

Monitor > LLDP > EEE

LLDPで交換されたEEE情報が表示されます。
EEEを使用すると、消費電力を削減できますが、トラフィックの遅延が発生します。
トラフィック使用率が低いときやデータが流れていないときに一部の回路を停止するため、トラフィックを送信する前に回路の通電にかかる時間(ウェイクアップ時間)がトラフィックの遅延につながります。
遅延を最少にするために、LLDPを使用して送受信時のウェイクアップ時間情報を交換できます。
※インターフェースがEEEに対応していない場合、「EEE not supported for this interface」と表示されます。
※インターフェースでEEEが無効になっている場合、「EEE not enabled for this interface」と表示されます。
※リンクパートナーがEEEに対応していない場合、「Link partner is not EEE capable」と表示されます。

LLDP Neighbors EEE Information


LLDP Neighbors EEE Information

Auto-refresh ☐ Refresh

Local Interface	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE in Sync
GigabitEthernet 1/4	EEE not enabled for this interface							
GigabitEthernet 1/4	EEE not enabled for this interface							
GigabitEthernet 1/4	EEE not enabled for this interface							
GigabitEthernet 1/4	EEE not enabled for this interface							

Auto-refresh …… 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 …… 最新の状態に更新するボタンです。

Local Interface …… LLDPを送受信するインターフェースが表示されます。

Tx Tw …… LPI(Low Power Idle)モードに移行後に、リンクパートナーがデータの送信を保留できる最大時間が表示されます。

Rx Tw …… リンクパートナーのレシーバーがスリープ状態から復帰するために、レシーバーがトランスミッターに送信停止を要求する時間が表示されます。

Fallback Receive Tw …… リンクパートナーのFallback receive Twの値が表示されます。
受信側のリンクパートナーは、送信側に別のTw sys txを通知する場合があります。
受信側のリンクパートナーは節電のために個別のレベルを持っている可能性が高いため、より効率的な割り当てに使用できる追加情報をトランスミッターに通知します。
このオプションを実装していないシステムのデフォルト値は、Receive Tw sys txの値になります。

Echo Tx Tw …… リンクパートナーのEcho Tx Twの値が表示されます。
Echo Tx TwとEcho Rx Twは、リモートリンクパートナーがローカルリンクパートナーへ返送(エコー)してきた値です。
ローカルリンクパートナーは、リモートリンクパートナーからエコーされた値を受信すると、リモートリンクパートナーが最新の値を受信、登録、および処理したかどうかを判断できます。
たとえば、ローカルリンクパートナーがローカルMIBの値と一致しないエコー値を受信した場合、ローカルリンクパートナーは、リモートリンクパートナーの要求が古い情報に基づいていると推測します。

「EEE」画面

Monitor > LLDP > EEE

LLDP Neighbors EEE Information

Echo Rx Tw …… リンクパートナーのEcho Rx Twの値が表示されます。

Resolved Tx Tw …… リンクのResolved Tx Twの値が表示されます。
Resolved Tx Twは、LLDPで交換したEEE情報に基づく実際の送信時のウェイクアップ時間です。
※リンクパートナーの値ではありません。

Resolved Rx Tw …… リンクのResolved Rx Twの値が表示されます。
Resolved Rx Twは、LLDPで交換したEEE情報に基づく実際の受信時のウェイクアップ時間です。
※リンクパートナーの値ではありません。

EEE in Sync …… 本製品とリンクパートナーでウェイクアップ時間がネゴシエートされたかどうかが表示されます。

赤：本製品とリンクパートナーでウェイクアップ時間がネゴシエートされていません。

緑：本製品とリンクパートナーでウェイクアップ時間がネゴシエートされています。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Port Statistics」画面

Monitor > LLDP > Port Statistics

LLDPトラフィックの統計情報が表示されます。
「LLDP Global Counters」にはスイッチ全体の統計情報が、「LLDP Statistics Local Counters」にはインターフェースごとの統計情報が表示されます。

LLDP Global Counters

Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈Clear〉 ……　[Clear]欄のボックスにチェックマークが入っているカウンターの値を0にするボタンです。

Global Counters

Clear global counters ……　〈Clear〉をクリックしたときに、「LLDP Global Counters」のカウンター値を0にするとき、ボックスにチェックマークを入れます。

Neighbor entries were last changed…　エントリが最後に削除、または追加された日時と、最後に変更されてから経過した時間が表示されます。

Total Neighbors Entries Added …　本製品が起動してから追加されたエントリの数が表示されます。

Total Neighbors Entries Deleted …　本製品が起動してから削除されたエントリの数が表示されます。

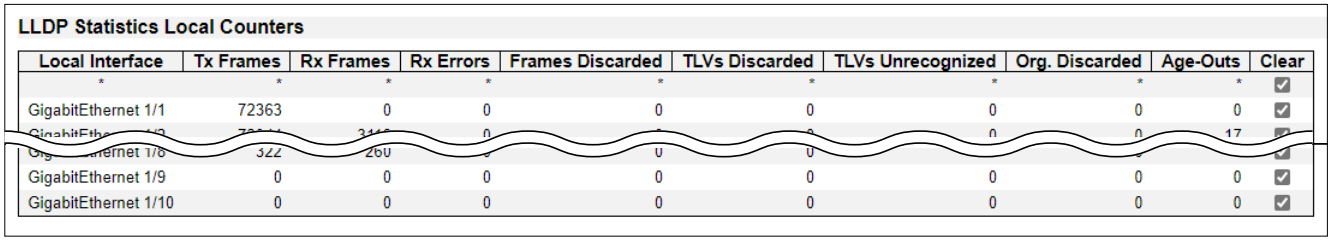
Total Neighbors Entries Dropped…　テーブルがいっぱいで破棄されたLLDPフレームの数が表示されます。

Total Neighbors Entries Aged Out…　Time-To-Live期限切れで削除されたエントリの数が表示されます。

「Port Statistics」画面

Monitor > LLDP > Port Statistics

LLDP Statistics Local Counters



LLDP Statistics Local Counters

Local Interface	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs	Clear
*	*	*	*	*	*	*	*	*	☑
GigabitEthernet 1/1	72363	0	0	0	0	0	0	0	☑
GigabitEthernet 1/9	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/10	0	0	0	0	0	0	0	0	☑

Local Interface…… LLDPフレームを送受信するインターフェースが表示されます。

Tx Frames …… 送信したLLDPフレームの数が表示されます。

Rx Frames …… 受信したLLDPフレームの数が表示されます。

Rx Errors…… 受信したLLDPフレームのうちエラーを含むフレームの数が表示されます。

Frames Discarded …… インターフェースでLLDPフレームを受信したとき、テーブルがいっぱいで破棄されたLLDPフレームの数が表示されます。(Too Many Neighbors)
Chassis ID、またはRemote Port IDがテーブルに登録されていない場合、テーブルにエントリの登録が必要です。
インターフェースのリンクがダウンしたとき、LLDP shutdownフレームを受信したとき、またはエントリが期限切れになったときに、テーブルからエントリが削除されます。

TLVs Discarded …… 不正な形式のTLV(Type Length Value)情報が含まれるために破棄されたLLDPフレームの数が表示されます。

TLVs Unrecognized …… 不明なタイプのTLV情報が含まれるLLDPフレームの数が表示されます。

Org. Discarded…… LLDPフレームを受信したインターフェースがTLVに対応していないために破棄されたTLVの数が表示されます。

Age-Outs…… LLDPフレームに含まれるエージング期間内に新しいLLDPフレームを受信しなかったために削除されたLLDP情報の数が表示されます。

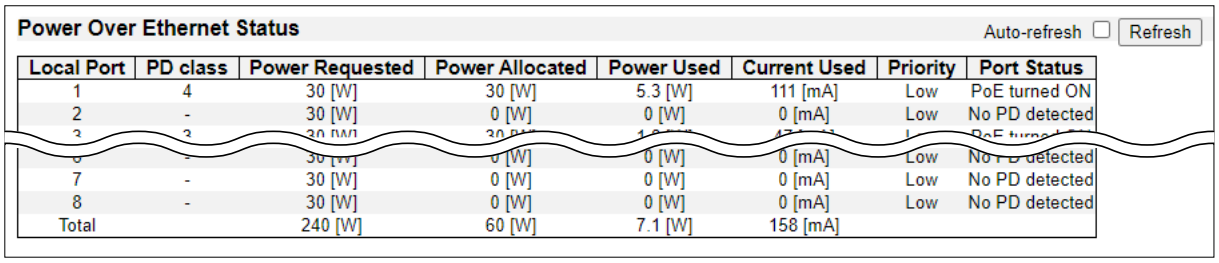
Clear …… 〈Clear〉をクリックしたときにカウンター値を0にするとき、ボックスにチェックマークを入れます。

「PoE」画面

Monitor > PoE

PoEポートの状態が表示されます。

Power Over Ethernet Status



Auto-refresh …… 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 …… 最新の状態に更新するボタンです。

Local Port …… 本製品のポート番号が表示されます。

PD class …… ポートに接続されたPDの電力クラスが表示されます。
クラスによって最大電力量が異なります。

Class 0：15.4 W
Class 1：4.0 W
Class 2：7.0 W
Class 3：15.4 W
Class 4：30.0 W

Power Requested …… PDから要求されている電力量が表示されます。

Power Allocated …… PDに割り当てられた電力量が表示されます。

Power Used …… PDの消費電力が表示されます。

Current Used …… PDの消費電流が表示されます。

Priority …… 設定されている優先度が表示されます。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「PoE」画面

Monitor > PoE

Power Over Ethernet Status

Port Status ……

ポートの状態が表示されます。

PoE not available - No PoE chip found：
ポートがPoEに対応していません。

PoE turned OFF - PoE disabled：
PoEが無効に設定されています。

PoE turned OFF - Power budget exceeded：
PDに供給される電力の合計が、本製品が供給できる電力量を越えたため、優先度の低いポートの電源が切れています。

No PD detected：
ポートでPDが検出されていません。

PoE turned OFF - PD overload：
供給できる電力以上の電力が必要なため、PDの電源が切れています。

PoE turned OFF：
PDの電源が切れています。

Invalid PD：
PDが検出されましたが、正常に動作していません。

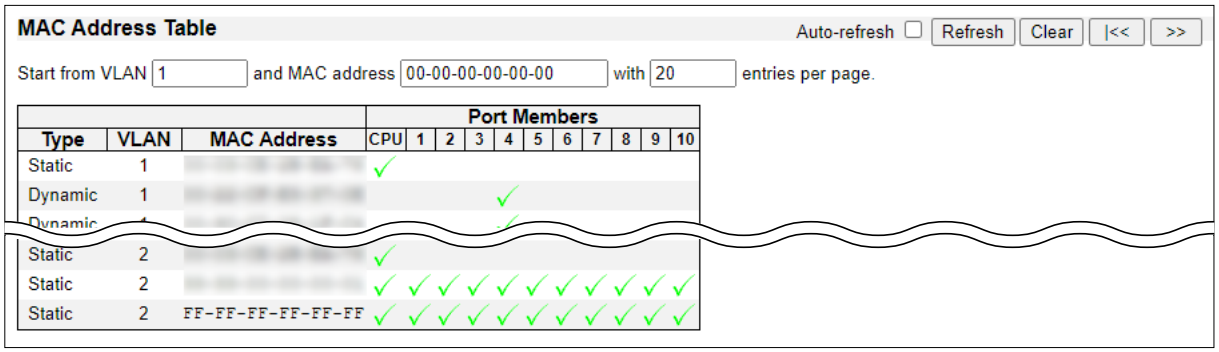
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「MAC Table」画面

Monitor > MAC Table

MACアドレステーブルが表示されます。
最大で8192件登録されます。
MACアドレステーブルは、VLAN ID、MACアドレスでソートされます。

MAC Address Table



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈Clear〉 ……　すべての動的エントリを削除するボタンです。

〈|<<〉 ……　最初のページに戻るボタンです。

〈>>〉 ……　次のページに進むボタンです。

Start from VLAN [VLAN ID] and MAC address [MACアドレス] with [表示数] entries per page.
……　ページの表示設定です。
[VLAN ID]欄と[MACアドレス]欄で、MACアドレステーブルの表示開始位置を指定できます。
[表示数]欄で1ページあたりの表示数を指定できます。(最大999件まで)

Type ……　静的エントリ(Static)か動的エントリ(Dynamic)かが表示されます。

VLAN ……　VLAN IDが表示されます。

MAC Address ……　MACアドレスが表示されます。

Port Members ……　所属しているポートが表示されます。

「Membership」画面

Monitor > VLANs > Membership

ドロップダウンリストで選択した機能の、VLANメンバーシップの状態が表示されます。
選択した機能がVLANメンバーシップを上書きしていない場合、「No data exists for the selected user」が表示されます。

VLAN Membership Status for Combined users

Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

Start from VLAN [VLAN ID] with [表示数] entries per page.
……　ページの表示設定です。
[VLAN ID]欄で、VLANメンバーシップの表示開始位置を指定できます。
[表示数]欄で1ページあたりの表示数を指定できます。（最大99件まで）

〈|<<〉……　最初のページに戻るボタンです。

〈>>〉 ……　次のページに進むボタンです。

VLAN ID ……　VLAN IDが表示されます。

Port Members ……　ポートの状態が表示されます。

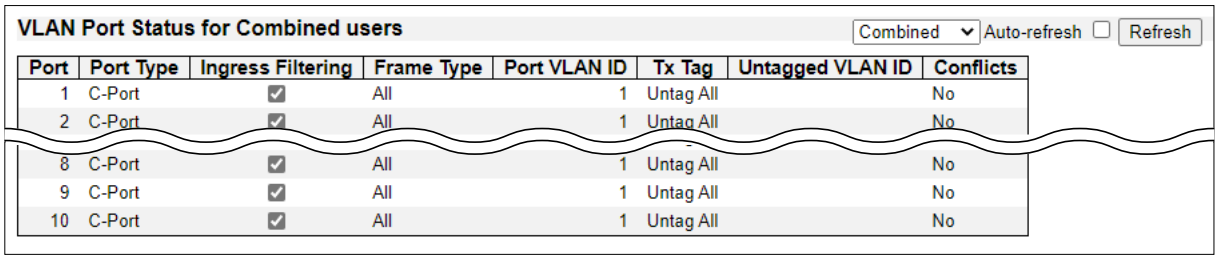
- ：VLANに所属しています。
- ：VLANへの所属が禁止されています。
- ：VLANへの所属が禁止されているポートを所属させようとしたときに表示されます。

「Ports」画面

Monitor > VLANs > Ports

ドロップダウンリストで選択した機能の、VLANポートの状態が表示されます。
選択した機能がVLANポートの設定を上書きしていない場合、「No data exists for the selected user」が表示されます。

VLAN Port Status for Combined users



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

Port ……　本製品のポート番号が表示されます。

Port Type ……　ポートタイプが「Unaware」、「C-Port」、「S-Port」、「S-Custom-Port」で表示されます。
選択した機能が設定を上書きしていないときは空白になります。

Ingress Filtering ……　受信時のフィルタリングが有効かどうかが表示されます。
選択した機能が設定を上書きしていないときは空白になります。

Frame Type ……　受信できるフレームの種類が、「All」、「Tagged」、「Untagged」で表示されます。
選択した機能が設定を上書きしていないときは空白になります。

Port VLAN ID ……　ポートVLAN ID(PVID)が表示されます。
選択した機能が設定を上書きしていないときは空白になります。

Tx Tag ……　送信時のタグ設定が、「Tag All」、「Tag PVID」、「Tag UVID」、「Untag All」、「Untag PVID」、「Untag UVID」表示されます。
選択した機能が設定を上書きしていないときは空白になります。

Untagged VLAN ID……　[Tx Tag]設定が選択した機能で「Tag UVID」、「Untag UVID」に変更されたとき、送信時にタグ付け、またはタグを削除するVLAN IDが表示されます。
選択した機能が設定を上書きしていないときは空白になります。

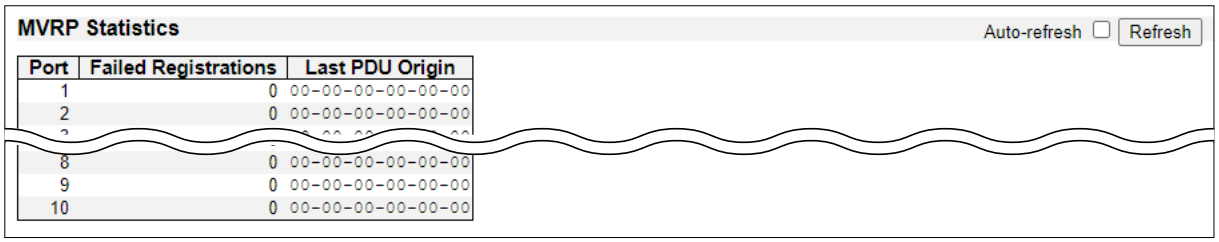
Conflicts ……　送信時にすべてのフレームをタグ付けするように設定された機能と、送信時にすべてのフレームにタグ付けしないように設定された機能があるなど、競合が発生しているかどうかが表示されます。
競合が発生した場合、「Admin」の優先度が最も低くなります。
その他の機能は、ドロップダウンリストに表示されている順番に優先度が低くなります。
競合が発生しているときは、「Combined」と競合が発生している機能で「Yes」が表示されます。

「MVRP」画面

Monitor > MVRP

MVRP(Multiple Vlan Registration Protocol)の状態が表示されます。

MVRP Statistics



Auto-refresh …… 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 …… 最新の状態に更新するボタンです。

Port …… 本製品のポート番号が表示されます。

Failed Registrations …… VLANの登録に失敗した回数が表示されます。
MVRPが有効なポートでVLAN登録要求を受信したときに、フィルタリングデータベースのスペース不足が原因でVLANの登録に失敗した回数をカウントします。

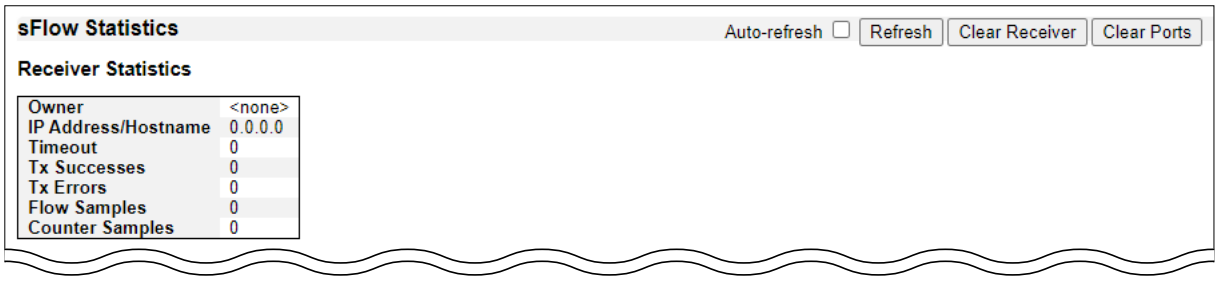
Last PDU Origin …… 最後に受信したMVRP PDUのMACアドレスが表示されます。
MVRPが無効、またはMVRP PDUを受信していない場合、「00-00-00-00-00-00」が表示されます。

「sFlow」画面

Monitor > sFlow

sFlowレシーバー(sFlowコレクター)とポートごとにsFlowの状態が表示されます。

sFlow Statistics



Auto-refresh ……　3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ……　最新の状態に更新するボタンです。

〈Clear Receiver〉 ……　「Receiver Statistics」のカウンター値を0にするボタンです。

〈Clear Ports〉 ……　「Port Statistics」のカウンター値を0にするボタンです。

Receiver Statistics

Owner ……　現在のsFlowの所有者名が表示されます。

<none>：
sFlowを使用していない場合に表示されます。

<Configured through local management>：
Web、またはCLIを使用して設定されている場合に表示されます。

※SNMPを使用して設定されていると、sFlowコレクターを識別する文字列が表示されます。

IP Address/Hostname ……　sFlowレシーバーのIPアドレス(IPv4/IPv6)、またはホスト名が表示されます。

Timeout ……　サンプリングを停止し、現在のsFlow所有者を解放するまでの残り時間が表示されます。

Tx Successes ……　sFlowレシーバーへの送信に成功したUDPデータグラムの数が表示されます。

Tx Errors……　sFlowレシーバーへの送信に失敗したUDPデータグラムの数が表示されます。
送信に失敗する場合は、設定したsFlowレシーバーのIPアドレス、またはホスト名が正しいか確認してください。
※「Diagnostics」→「Ping (IPv4)」画面、または「Ping (IPv6)」画面を使用すると、sFlowレシーバーに到達できるか確認できます。

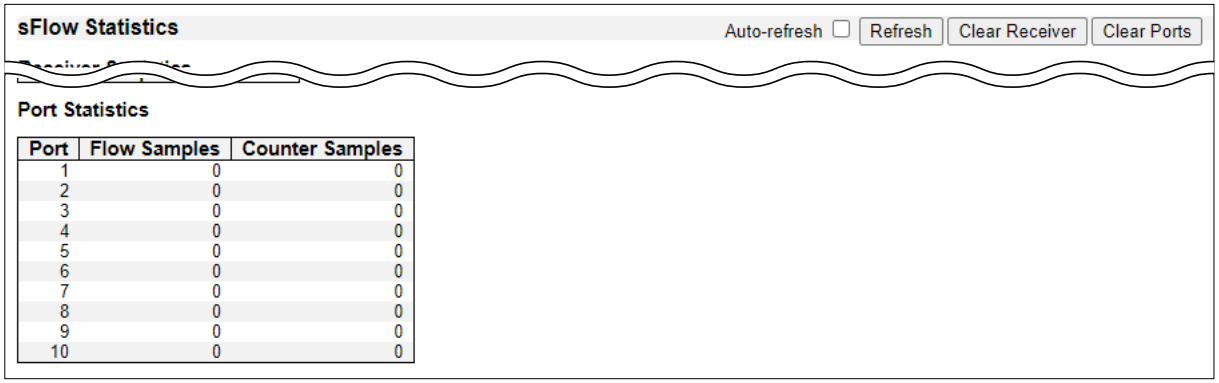
Flow Samples ……　sFlowレシーバーへ送信したフローサンプルの総数が表示されます。

Counter Samples ……　sFlowレシーバーへ送信したカウンターサンプルの総数が表示されます。

「sFlow」画面

Monitor > sFlow

sFlow Statistics



Port Statistics

Port …… 本製品のポート番号が表示されます。

Flow Samples …… sFlowレシーバーへ送信したフローサンプルの数が表示されます。

Counter Samples …… sFlowレシーバーへ送信したカウンターサンプルの総数が表示されます。

「UDLD」画面

Monitor > UDLD

ドロップダウンリストで選択したポートのUDLDの状態が表示されます。

Detailed UDLD Status for Port 1～10

Auto-refresh ····· 3秒ごとに自動で最新の状態に更新するとき、ボックスにチェックマークを入れます。

〈Refresh〉 ····· 最新の状態に更新するボタンです。

UDLD status

UDLD Admin state ····· ポートのUDLDモードが表示されます。

Device ID(local) ····· デバイスのIDが表示されます。

Device Name(local) ····· デバイスの名称が表示されます。

Bidirectional State ····· ポートの状態が表示されます。

Neighbour Status

Port ····· ネイバーのポートが表示されます。

Device Id ····· ネイバーのIDが表示されます。

Link Status ····· ネイバーのポートのリンク状態が表示されます。

Device Name ····· ネイバーのデバイスの名称が表示されます。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

4章 Diagnosticメニュー

「Ping (IPv4)」画面 …… 4-2
Ping (IPv4) …… 4-2
「Ping (IPv6)」画面 …… 4-4
Ping (IPv6) …… 4-4
「Traceroute (IPv4)」画面 …… 4-6
Traceroute (IPv4) …… 4-6
「Traceroute (IPv6)」画面 …… 4-8
Traceroute (IPv6) …… 4-8
「VeriPHY」画面 …… 4-10
VeriPHY Cable Diagnostics …… 4-10

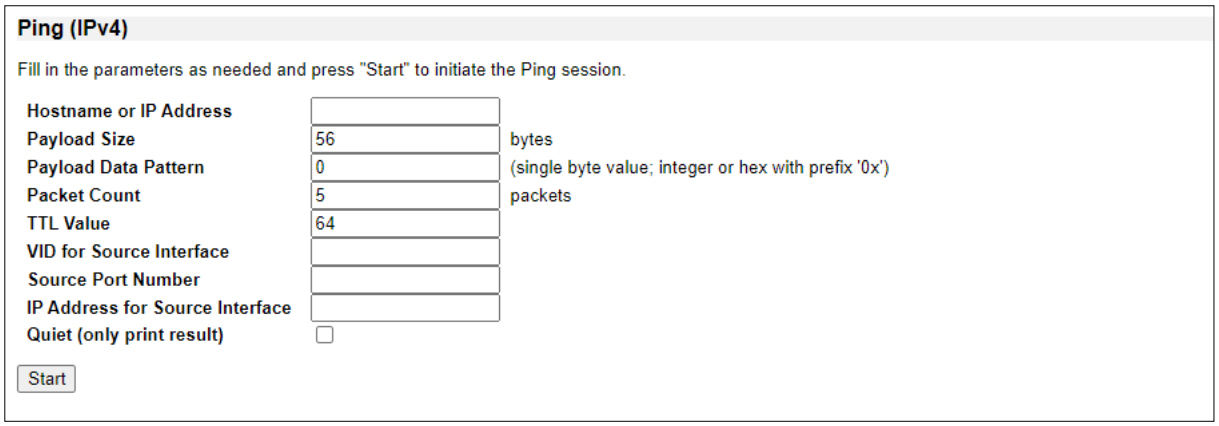
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Ping (IPv4)」画面

Diagnostics > Ping (IPv4)

本製品からICMP(IPv4) PINGパケットを送出し、ネットワークの疎通確認テストをします。

Ping (IPv4)



Hostname or IP Address…… PINGパケットを送出する対象ホストのIPアドレス、またはホスト名を入力します。

Payload Size …… イーサネット、IP、ICMPヘッダー部分を除く、ICMPパケットのペイロード長を設定します。
設定できる範囲は、「2～1452」(バイト)です。

Payload Data Pattern …… ICMPペイロードのパターンを設定します。
設定できる範囲は、「0～255」です。

Packet Count …… PINGパケットを送出する回数を設定します。
設定できる範囲は、「1～60」です。

TTL Value …… IPv4ヘッダーに含まれるTTL(Time-To-Live)フィールドの値を設定します。
設定できる範囲は、「1～255」です。

VID for Source Interface …… 特定のローカルVLANインターフェースを送信元インターフェースとして使用するときに、使用するインターフェースのVID、またはIPアドレスを設定します。
ルーティング構成に基づいて自動的に選択する場合は、空白のままにしてください。

Source Port Number …… 特定のポート番号のローカルインターフェースを送信元インターフェースとして使用するときに、使用するインターフェースの送信元ポート番号、またはIPアドレスを設定します。
指定したポートには、適切なIPアドレスを設定してください。
ルーティング構成に基づいて自動的に選択する場合は、空白のままにしてください。

IP Address for Source Interface… 特定のIPアドレスのローカルインターフェースを送信元インターフェースとして使用するときに、使用するインターフェースのVID、またはIPアドレスを設定します。
ローカルインターフェースのIPアドレスを設定してください。
ルーティング構成に基づいて自動的に選択する場合は、空白のままにしてください。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Ping (IPv4)」画面

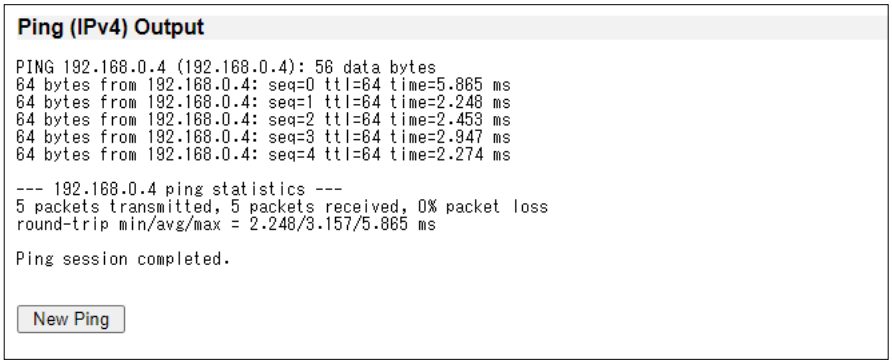
Ping (IPv4)

Quiet (only print result) ……

各ping要求の結果を表示せずに、最終結果だけを表示するとき、ボックスにチェックマークを入れます。

〈Start〉 ……

PINGテストを実行するボタンです。
クリックすると、「Ping (IPv4) Output」表示に切り替わり、応答を受信するとシーケンス番号とラウンドトリップ時間が表示されます。



受信したICMP echo replyパケットのペイロード長は、設定したペイロード長にICMPヘッダー長(8バイト)を加えた値になります。
すべての応答を受信するか、タイムアウトが発生するまでページは自動で更新されます。
〈New Ping〉をクリックすると、「Ping (IPv4)」表示に戻ります。

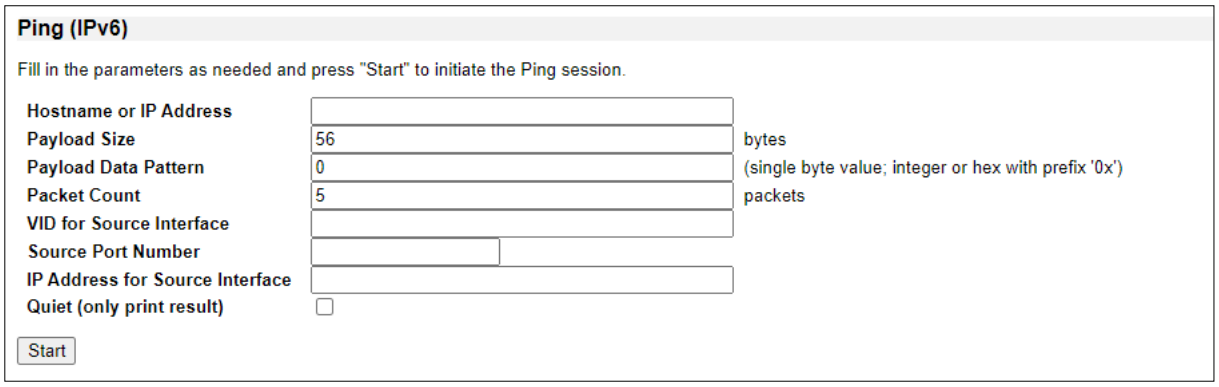
4 Diagnosticメニュー

「Ping (IPv6)」画面

Diagnostics > Ping (IPv6)

本製品からICMPv6 PINGパケットを送出し、ネットワークの疎通確認テストをします。

Ping (IPv6)



Hostname or IP Address…… PINGパケットを送出する対象ホストのIPアドレス、またはホスト名を入力します。

Payload Size …… イーサネット、IP、ICMPヘッダー部分を除く、ICMPパケットのペイロード長を設定します。
設定できる範囲は、「2～1452」(バイト)です。

Payload Data Pattern …… ICMPペイロードのパターンを設定します。
設定できる範囲は、「0～255」です。

Packet Count …… PINGパケットを送出する回数を設定します。
設定できる範囲は、「1～60」です。

VID for Source Interface …… 特定のローカルVLANインターフェースを送信元インターフェースとして使用するときに、使用するインターフェースのVID、またはIPアドレスを設定します。
ルーティング構成に基づいて自動的に選択する場合は、空白のままにしてください。

Source Port Number …… 特定のポート番号のローカルインターフェースを送信元インターフェースとして使用するときに、使用するインターフェースの送信元ポート番号、またはIPアドレスを設定します。
指定したポートには、適切なIPアドレスを設定してください。
ルーティング構成に基づいて自動的に選択する場合は、空白のままにしてください。

IP Address for Source Interface… 特定のIPアドレスのローカルインターフェースを送信元インターフェースとして使用するときに、使用するインターフェースのVID、またはIPアドレスを設定します。
ローカルインターフェースのIPアドレスを設定してください。
ルーティング構成に基づいて自動的に選択する場合は、空白のままにしてください。

Quiet (only print result) …… 各ping要求の結果を表示せずに、最終結果だけを表示するとき、ボックスにチェックマークを入れます。

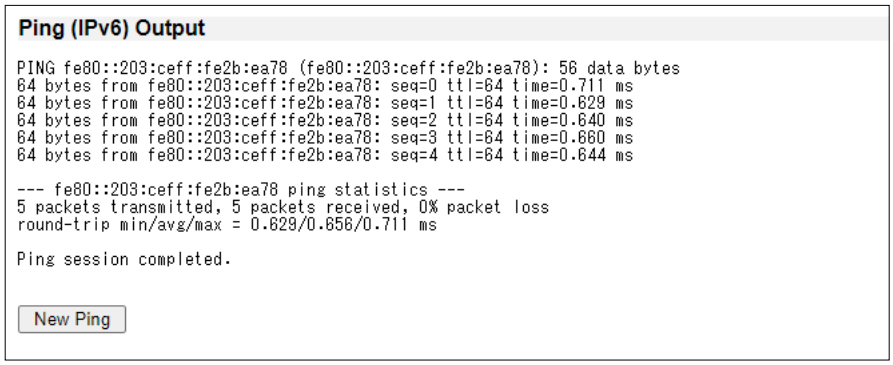
「Ping (IPv6)」画面

Diagnostics > Ping (IPv6)

Ping (IPv6)

〈Start〉 ……

PINGテストを実行するボタンです。
クリックすると、「Ping (IPv6) Output」表示に切り替わり、応答を受信するとシーケンス番号とラウンドトリップ時間が表示されます。



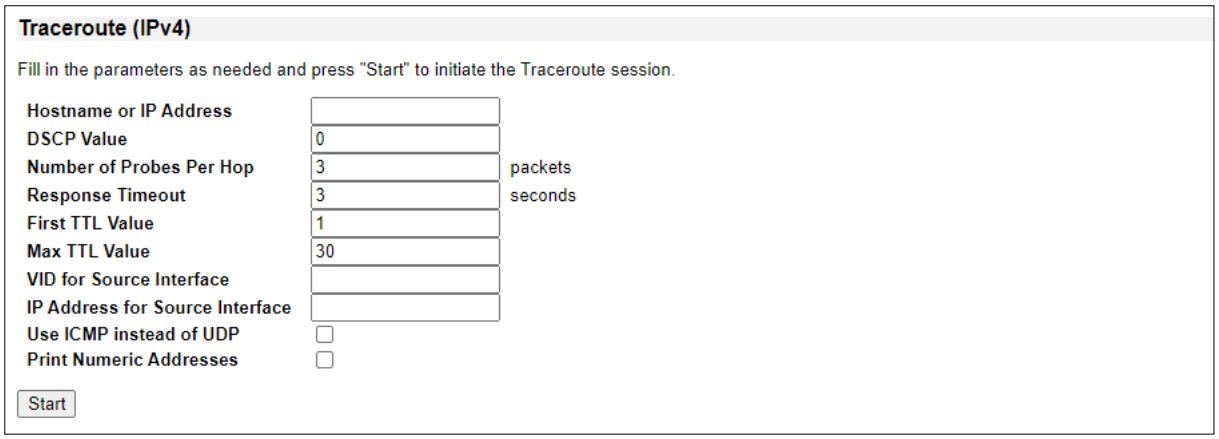
受信したICMP echo replyパケットのペイロード長は、設定したペイロード長にICMPヘッダー長(8バイト)を加えた値になります。
すべての応答を受信するか、タイムアウトが発生するまでページは自動で更新されます。
〈New Ping〉をクリックすると、「Ping (IPv6)」表示に戻ります。

「Traceroute (IPv4)」画面

Diagnostics > Traceroute (IPv4)

本製品から特定のノードに対しての経路テスト(traceroute)をします。

Traceroute (IPv4)



Hostname or IP Address…… 経路テストをする対象ノード(機器)のIPアドレス、またはホスト名を入力します。

DSCP Value …… IPv4ヘッダーに含まれるDSCP値を設定します。
設定できる範囲は、「0～63」です。

Number of Probes Per Hop … 1ホップあたりに送信するパケット数を設定します。
設定できる範囲は、「1～60」です。

Response Timeout …… テスト開始後、応答を待つ時間を設定します。
設定できる範囲は、「1～86400」(秒)です。

First TTL Value…… はじめに送信するパケットのIPv4ヘッダーに含まれるTTL(Time-To-Live)フィールドの値を設定します。
設定できる範囲は、「1～30」です。

Max TTL Value …… IPv4ヘッダーに含まれるTTL(Time-To-Live)フィールドの最大値を設定します。
設定できる範囲は、「1～255」です。
指定したリモートホストに到達する前に経由したホップ数(中継設備数)がTTL値を超えると、経路テストが停止します。

VID for Source Interface …… 特定のローカルVLANインターフェースを送信元インターフェースとして使用するときに、使用するインターフェースのVID、またはIPアドレスを設定します。
ルーティング構成に基づいて自動的に選択する場合は、空白のままにしてください。

IP Address for Source Interface… 特定のIPアドレスのローカルインターフェースを送信元インターフェースとして使用するときに、使用するインターフェースのVID、またはIPアドレスを設定します。
ローカルインターフェースのIPアドレスを設定してください。
ルーティング構成に基づいて自動的に選択する場合は、空白のままにしてください。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Traceroute (IPv4)」画面

Diagnostics > Ping (IPv6)

Traceroute (IPv4)

Use ICMP instead of UDP …… 経路テストにICMP echoパケットを使用するときは、ボックスにチェックマークを入れます。
デフォルトでは、経路テストにUDPデータグラムを使用します。

Print Numeric Addresses …… リバースDNSルックアップを使用せずIPアドレスでホップ情報を表示するときに、ボックスにチェックマークを入れます。
デフォルトでは、取得したホストIPアドレスでリバースDNSルックアップを使用してホップ情報を表示しますが、DNS情報が利用できない場合に、表示が遅くなることがあります。

〈Start〉 …… 経路テストを実行するボタンです。
クリックすると、「Traceroute (IPv4) Output」表示に切り替わり、テスト結果が表示されます。
〈New Traceroute〉をクリックすると、「Traceroute (IPv4)」表示に戻ります。

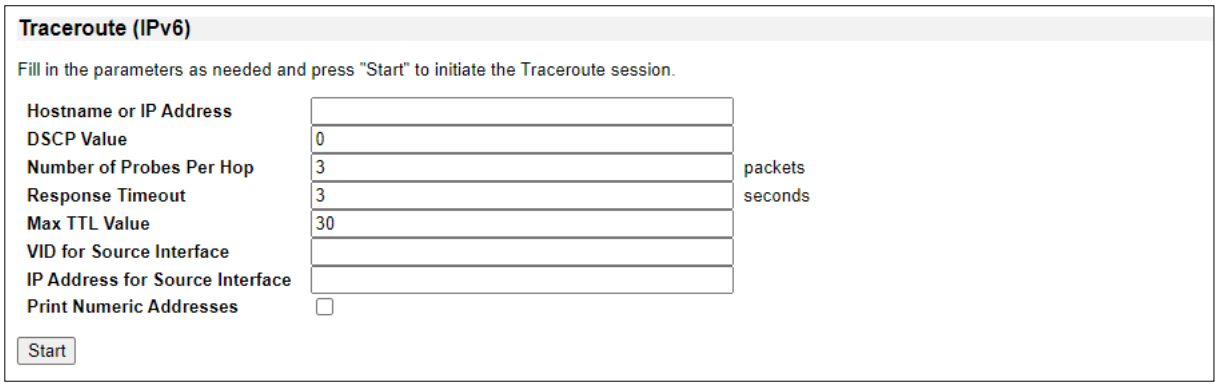
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Traceroute (IPv6)」画面

Diagnostics > Traceroute (IPv6)

本製品から特定のノードに対しての経路テスト(traceroute)をします。

Traceroute (IPv6)



Hostname or IP Address…… 経路テストをする対象ノード(機器)のIPアドレス、またはホスト名を入力します。

DSCP Value …… IPv6ヘッダーに含まれるDSCP値を設定します。
設定できる範囲は、「0～255」です。

Number of Probes Per Hop … 1ホップあたりに送信するパケット数を設定します。
設定できる範囲は、「1～60」です。

Response Timeout …… テスト開始後、応答を待つ時間を設定します。
設定できる範囲は、「1～86400」(秒)です。

Max TTL Value …… IPv6ヘッダーに含まれるTTL(Time-To-Live)フィールドの最大値を設定します。
設定できる範囲は、「1～255」です。
指定したリモートホストに到達する前に経由したホップ数(中継設備数)がTTL値を超えると、経路テストが停止します。

VID for Source Interface …… 特定のローカルVLANインターフェースを送信元インターフェースとして使用するときに、使用するインターフェースのVID、またはIPアドレスを設定します。
ルーティング構成に基づいて自動的に選択する場合は、空白のままにしてください。

IP Address for Source Interface… 特定のIPアドレスのローカルインターフェースを送信元インターフェースとして使用するときに、使用するインターフェースのVID、またはIPアドレスを設定します。
ローカルインターフェースのIPアドレスを設定してください。
ルーティング構成に基づいて自動的に選択する場合は、空白のままにしてください。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Traceroute (IPv6)」画面

Diagnostics > Ping (IPv6)

Traceroute (IPv6)

Print Numeric Addresses …… リバースDNSルックアップを使用せずIPアドレスでホップ情報を表示するときに、ボックスにチェックマークを入れます。
デフォルトでは、取得したホストIPアドレスでリバースDNSルックアップを使用してホップ情報を表示しますが、DNS情報が利用できない場合に、表示が遅くなることがあります。

〈Start〉 …… 経路テストを実行するボタンです。
クリックすると、「Traceroute (IPv6) Output」表示に切り替わり、テスト結果が表示されます。
〈New Traceroute〉をクリックすると、「Traceroute (IPv6)」表示に戻ります。

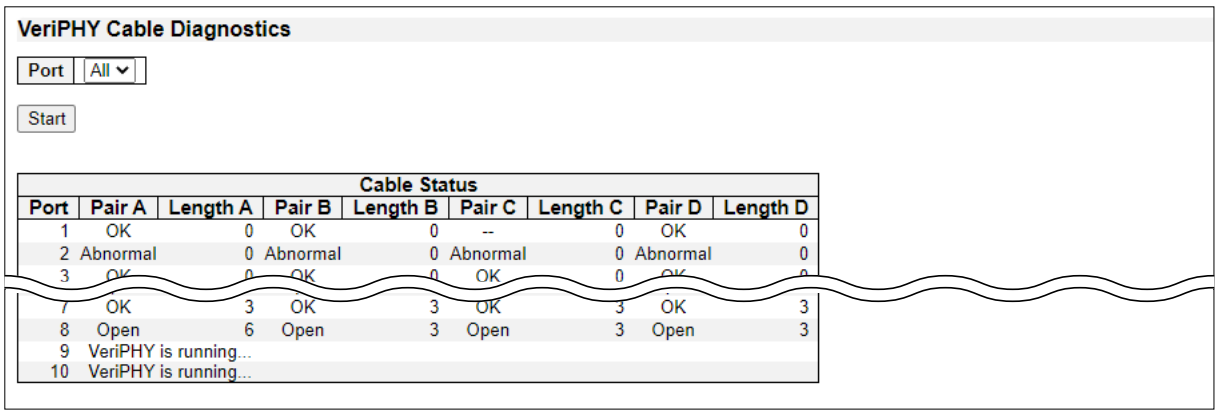
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「VeriPHY」画面

Diagnostics > VeriPHY

10/100/1Gのメタルケーブル用ポートで、VeriPHYケーブル診断をします。
〈Start〉をクリックしてから、特定のポートだけの場合は約5秒後に、すべてのポートの場合は約15秒後に診断結果が表示されます。
※正確に診断できるのは、7～140mのケーブルだけです。
※診断中は、10Mbpsと100Mbpsポートがリンクダウンします。
　10、または100Mbpsの管理ポートで診断を開始すると、診断が完了するまで本製品は応答しなくなります。

VeriPHY Cable Diagnostics



Port …… VeriPHYケーブル診断を実行するポートを選択します。

〈Start〉 …… VeriPHYケーブルを実行するボタンです。
クリックすると、「Cable Status」に診断結果が表示されます。

Cable Status

Port …… 本製品のポート番号が表示されます。

Pair A～D …… ツイストペアケーブルの各ペアの状態が表示されます。

- **OK** ：正しく終端されています。
- **Open** ：オープン状態です。
- **Short** ：ショートしています。
- **Short A** ：クロスペアがペアAにショートしています。
- **Short B** ：クロスペアがペアBにショートしています。
- **Short C** ：クロスペアがペアCにショートしています。
- **Short D** ：クロスペアがペアDにショートしています。
- **Cross A** ：ペアAと間違ったクロス結線をしています。
- **Cross B** ：ペアBと間違ったクロス結線をしています。
- **Cross C** ：ペアCと間違ったクロス結線をしています。
- **Cross D** ：ペアDと間違ったクロス結線をしています。

Length A～D …… ツイストペアケーブルの各ペアの長さ(メートル)が3メートル刻みで表示されます。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

5章 Maintenanceメニュー

「Restart Device」画面 …… 5-2
Restart Device …… 5-2
「Factory Defaults」画面 …… 5-3
Factory Defaults …… 5-3
「Upload」画面 …… 5-4
Software Upload …… 5-4
「Image Select」画面 …… 5-5
Software Image Selection …… 5-5
「Save startup-config」画面 …… 5-6
Save Running Configuration to startup-config …… 5-6
「Download」画面 …… 5-7
Download Configuration …… 5-7
「Upload」画面 …… 5-8
Upload Configuration …… 5-8
「Activate」画面 …… 5-9
Activate Configuration …… 5-9
「Delete」画面 …… 5-10
Delete Configuration File …… 5-10

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Restart Device」画面

Maintenance > Restart Device

本製品を再起動します。

Restart Device

〈Yes〉 …… 本製品を再起動するボタンです。

〈No〉 …… 再起動せずに、「Information」画面に戻るボタンです。

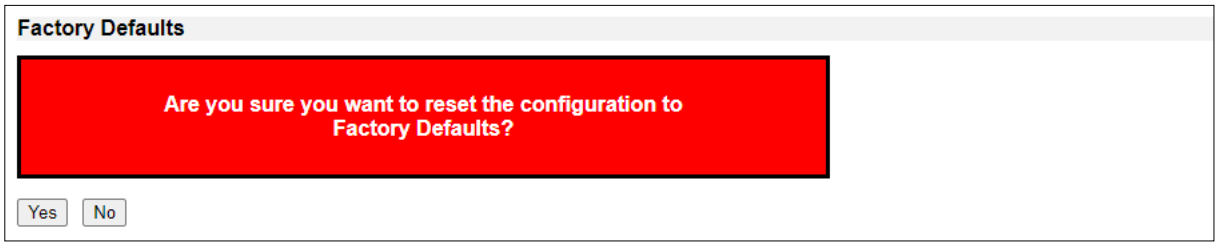
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Factory Defaults」画面

Maintenance > Factory Defaults

本製品の設定内容を初期化します。
※IP設定は初期化されません。
※IPアドレスと管理者用のパスワードが不明な場合などの初期化については、6章も併せてご覧ください。

Factory Defaults



〈Yes〉 …… 本製品を初期化するボタンです。

〈No〉 …… 初期化せずに、「Information」画面に戻るボタンです。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Upload」画面

ファームウェアの更新についてのご注意
◎ファームウェアの更新中は、前面部のランプが緑色で点滅します。
　故障の原因になるため、ファームウェアの更新が完了するまで、本製品の電源を切らないでください。
◎更新中(約1分間)は、すべての接続が切断されます。
※更新によって追加や変更になる機能、注意事項については、あらかじめ弊社ホームページでご確認ください。

Maintenance > Software > Upload

本製品のファームウェアを更新します。

Software Upload

〈Select File ...〉…… ファームウェアのイメージファイルを選択するボタンです。

〈Start Upgrade〉…… ファームウェアの更新を開始するボタンです。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Image Select」画面

Maintenance > Software > Image Select

本製品に内蔵のファームウェア情報が表示されます。
動作中のファームウェア(Active Image)と、バックアップ用のファームウェア(Alternate Image)があります。

Software Image Selection

Active Image/Alternate Image

Image …… ファームウェアイメージのファイル名が表示されます。

Version…… ファームウェアのバージョンが表示されます。

Date …… ファームウェアの作成日が表示されます。

〈Activate Alternate Image〉 … バックアップ用ファームウェアに切り替えるボタンです。

〈Cancel〉 …… バックアップ用ファームウェアの使用を中止し、「Information」画面に戻るボタンです。

ご注意
◎バックアップ用ファームウェアで動作中は、「Alternate Image」は表示されず、〈Activate Alternate Image〉ボタンも無効になります。
◎プライマリファームウェアの破損、または手動切り替えによって、バックアップ用ファームウェアで動作中にファームウェアを更新すると、プライマリファームウェアが書き換わり、アップロードしたファームウェアで動作します。
◎ファームウェアによっては、[Version]欄と[Date]欄が空白になる場合があります。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Save startup-config」画面

本製品の設定ファイルについて
本製品の設定は、CLI形式の複数のテキストファイルに保存されます。
設定ファイルは、仮想(RAMベース)、または本製品のフラッシュメモリーにも保存されます。
設定ファイルは、次の3種類があります。

running-config :
現在の設定が保存された仮想ファイルです。
揮発性メモリーに保存されます。

startup-config :
本製品が起動したときに読み込まれる設定ファイルです。
startup-configファイルがない場合は、default-configの設定で起動します。

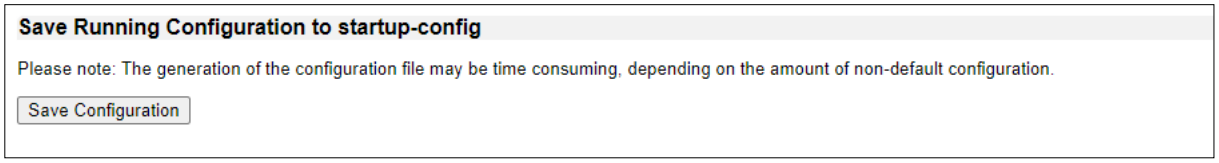
default-config :
ベンダーごとに固有の設定ファイルです。(読み取り専用)
本製品を初期化したときに読み込まれます。

そのほかに、設定のバックアップや代替用のファイルを最大31個まで保存できます。

Maintenance > Configuration > Save startup-config

本製品が現在の設定で起動するように設定します。

Save Running Configuration to startup-config



〈Save Configuration〉 …… running-configファイルをstartup-configファイルにコピーするボタンです。
本製品を再起動したときに、現在の設定で起動します。

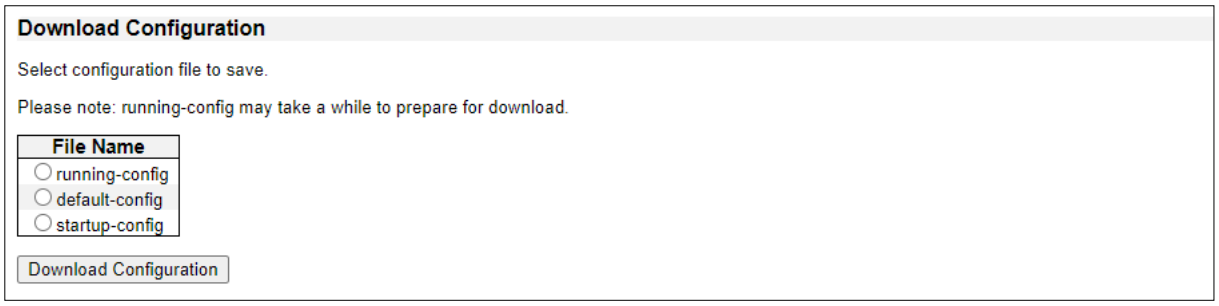
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Download」画面

Maintenance > Configuration > Download

設定ファイルをダウンロードします。

Download Configuration



File Name …… ダウンロードする設定ファイルを選択します。
※ファイルの種類については、5-6ページをご覧ください。
※running-configを選択した場合、ダウンロードに時間がかかることがあります。

〈Download Configuration〉 …… 選択した設定ファイルをダウンロードするボタンです。

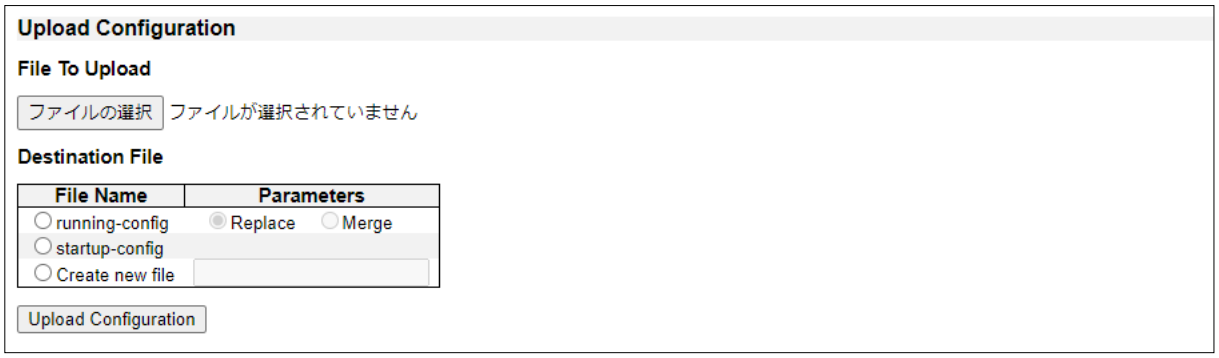
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Upload」画面

Maintenance > Configuration > Upload

ダウンロードした設定ファイルを本製品に書き込みます。
※default-configファイルは上書きできません。

Upload Configuration



File To Upload

〈ファイルの選択〉…… 本製品に書き込む設定ファイルを選択します。

Destination File

File Name …… 設定ファイルの書き込み先を選択します。
※ファイルの種類については、5-6ページをご覧ください。
※default-config、startup-configを含めて32個の設定ファイルが保存されているときは、新しい設定ファイルを作成できません。
既存のファイルに上書きするか、不要な設定ファイルを削除してください。

Parameters …… 「running-config」を選択したときは、書き込むモードを設定します。

Replace：
現在の設定を上書きします。
※書き込む前の設定内容は消去されます。

Merge：
現在の設定と結合します。

「Create new file」を選択したときは、本製品に設定ファイルを保存するときの名称を入力します。

〈Upload Configuration〉…… 選択した設定ファイルを本製品に書き込むボタンです。

設定ファイルについてのご注意
本製品以外の機器へ書き込み、改変による障害、および書き込みに伴う本製品の故障、誤動作、不具合、破損、データの消失、または停電などの外部要因により通信、通話などの機会を失ったために生じる損害や逸失利益、または第三者からのいかなる請求についても当社は一切その責任を負いかねますのであらかじめご了承ください。

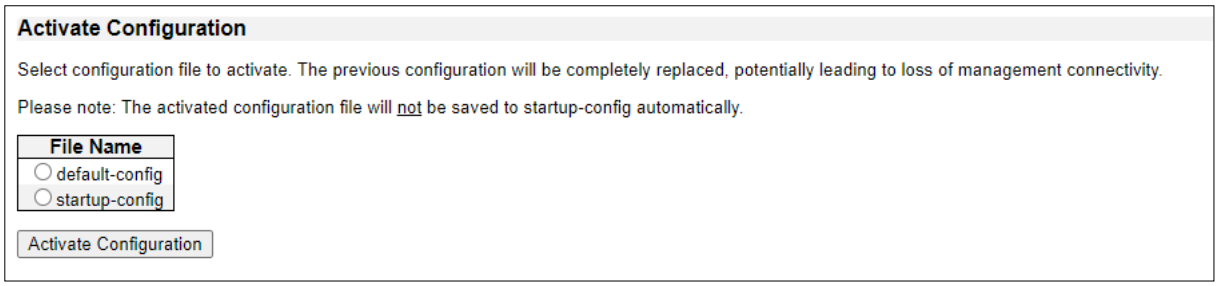
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Activate」画面

Maintenance > Configuration > Activate

本製品に保存された設定ファイルの設定内容を復元します。

Activate Configuration



File Name …… 復元する設定ファイルを選択します。
※復元前の設定内容は消去されます。

〈Activate Configuration〉…… 選択した設定ファイルを復元するボタンです。

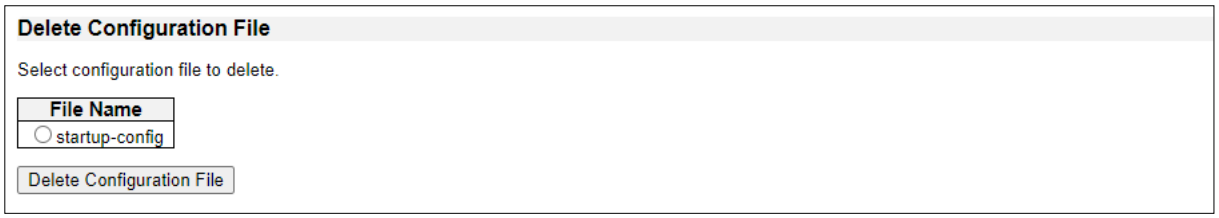
三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

「Delete」画面

Maintenance > Configuration > Delete

本製品に保存された設定ファイルを削除します。

Delete Configuration File



File Name …… 削除する設定ファイルを選択します。
※startup-configファイルを削除した場合、新しくstartup-configを保存せずに本製品を再起動すると、初期化された状態で起動します。

〈Delete Configuration File〉…… 選択した設定ファイルを削除するボタンです。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

6章 ご参考に

困ったときは…… 6-2

Telnet/SSHで接続するには …… 6-3
Telnet/SSHコマンドについて …… 6-3
[CONSOLE]ポートを使用する …… 6-4

設定内容の保存…… 6-5

保存された設定の書き込み(復元)…… 6-6

設定を出荷時の状態に戻すには…… 6-7
製品本体で初期化する…… 6-7
設定画面で初期化する…… 6-7

光ファイバーケーブルの接続について…… 6-8
取り付けかた…… 6-8
取りはずしかた…… 6-8

定格…… 6-9

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

6 ご参考に

困ったときは

下記のような現象は、故障ではありませんので、修理を依頼される前にもう一度お調べください。
それでも異常があるときは、弊社サポートセンターまでお問い合わせください。

POWERランプが点灯しない

●電源ケーブルが本製品に接続されていない
→ 本製品の電源ケーブル、およびACプラグの接続を確認する

●電源ケーブルをパソコンなどの電源と連動したコンセントに接続している
→ 本製品の電源ケーブルを壁などのコンセントに直接接続する

LINK/ACTランプが点灯しない

●LANケーブルが本製品と正しく接続されていない
→ 本製品やパソコンの[LAN]ポート、またはLANケーブルを確認する

●パソコン、またはHUBの電源が入っていない
→ パソコンとHUBの電源が入っていることを確認する

本製品の設定画面が正しく表示されない

●WWWブラウザーのJavaScript機能、およびCookieを無効に設定している
→ JavaScript機能、およびCookieを有効に設定する

本製品の設定画面にアクセスできない

●パソコンのIPアドレスを設定していない
→ 本製品の初期設定では、DHCPサーバー機能が無効のため、パソコンのIPアドレスを固定IPアドレスに設定する

●IPアドレスのネットワーク部が、本製品とパソコンで異なっている
→ パソコンに設定されたIPアドレスのネットワーク部を本製品と同じにする

●ご使用のWWWブラウザーにプロキシサーバーが設定されている
→ 〈スタート〉(ロゴボタン)→[設定]→[ネットワークとインターネット]にある[プロキシ]で、設定を確認する

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

6 ご参考に

Telnet/SSHで接続するには

Telnet/SSHでの接続について説明します。
ご使用のOSやTelnet/SSHクライアントが異なるときは、それぞれの使用方法をご確認ください。
※説明では、System Name(本体名称)が「VE-SW8」に設定されている場合を例にしています。
※出荷時の設定ではSystem Nameが未設定のため、Telnet/SSHでログインすると、「#」だけが表示されます。
（Configuration > System > Information > System Name）

【ログインについて】
① 下記を入力して、ログインします。
Username ：admin(固定)
Password ：admin
※「Users」画面で設定したパスワードを入力します。
出荷時や全設定初期化時のpasswordは、adminです。
② ログインに成功すると、プロンプト VE-SW8# が表示されます。

【設定の保存について】
設定変更後、「save」を入力して[Enter]キーを押します。
※コマンド入力で保存をしていない場合、本体再起動後、設定の変更が失われます。

【ログアウトについて】
「quit」、「exit」、「logout」コマンドを実行すると、ログアウトします。

Telnet/SSHコマンドについて

使用できるTelnet/SSHコマンドの表示方法と、コマンド入力について説明します。

コマンド一覧……　[Tab]キーを押すと、使用できるコマンドの一覧が表示されます。
コマンド名の入力につづいて[Tab]キーを押すと、サブコマンドの一覧が表示されます。

コマンドヘルプ……　コマンドの意味を知りたいときは、コマンド名につづいて、「？」を入力するとコマンドのヘルプが表示されます。
例）VE-SW8# copy ？ （copyコマンドのヘルプを表示する場合）
※「help」を入力して[Enter]キーを押すと、全ヘルプの一覧が表示されます。

コマンド名の補完……　コマンド名を先頭から数文字入力し[Tab]キーを押すと、コマンド名が補完されます。
入力した文字につづくコマンドが1つしかないときは、コマンド名を最後まで補完します。
例）a[Tab]→alarm
複数のコマンドがあるときは、1回目の押下でビープ音コマンドを送出し、2回目以降の押下でコマンド候補を表示します。
例）s[Tab]→send show
※ビープ音は、お使いのターミナルソフトウェアやOSの設定により、音の有無、音色が異なります。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

6 ご参考に

Telnet/SSH で接続するには

[CONSOLE]ポートを使用する

本製品の[CONSOLE]ポートとパソコンの[USB]ポートを、市販のUSBコンソールケーブル(RJ-45タイプ)で接続すると、ターミナルソフトウェアから設定できます。

◎[接続方法]の選択　：USBケーブルを接続しているCOMポートの番号を指定します。
◎通信速度　：115200(ビット/秒)
◎データビット　：8
◎パリティー　：なし
◎ストップビット　：1
◎フロー制御　：なし

※設定後、何も入力せずに[Enter]キーを押すと、「Username:」と表示されます。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

6 ご参考に

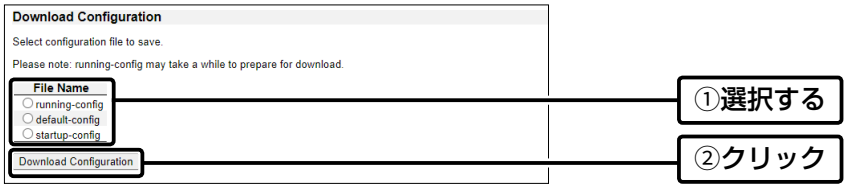
設定内容の保存

Maintenance > Configuration > Download

本製品の設定画面で変更された内容を設定ファイルとしてパソコンに保存できます。
※保存した設定ファイルは、本製品以外の製品では使用できません。
※設定を保存しておくと、誤って設定内容が失われたときなどに利用できます。

1 「Maintenance」→「Configuration」→「Download」の順でクリックします。
「Download」画面が表示されます。

2 保存したい条件を選択して、〈Download Configuration〉をクリックします。



保存される設定内容
◎running-config：各画面の〈Save〉が押され、再起動するまで有効な設定
◎default-config：工場出荷時の設定
◎startup-config：「Save startup-config」画面の〈Save Configuration〉が押され、再起動後も有効な設定

設定ファイルの保存場所
Microsoft Edge（Chromiumベース）の場合、デフォルトの設定では、「ダウンロード」フォルダーにファイルが保存されます。
必要に応じて、WWWブラウザーの設定で、デスクトップなど任意の場所に変更してください。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

保存された設定の書き込み(復元)

Maintenance > Configuration > Upload

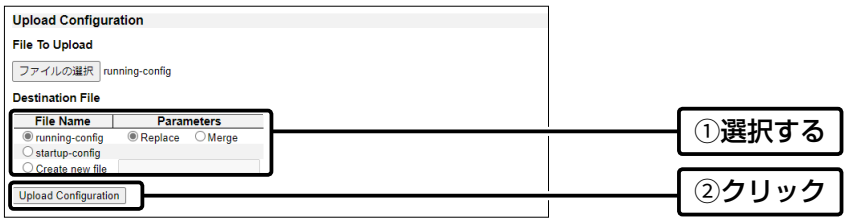
本製品の設定画面からパソコンに保存した設定ファイル(P.6-5)を本製品に書き込む手順を説明します。

1 「Maintenance」→「Configuration」→「Upload」の順でクリックします。
「Upload」画面が表示されます。

2 [File To Upload]項目の〈ファイルの選択〉をクリックします。
ファイルの選択画面(別画面)が表示されます。

3 設定ファイルを指定して、〈開く(O)〉をクリックします。
〈ファイルの選択〉の横に、書き込む設定ファイルが表示されます。

4 [Destination File]項目で書き込む条件を選択し、〈Upload Configuration〉をクリックします。
設定ファイルの内容が反映されます。
※running-configだけ、Replace(置換)かMerge(結合)を選択できます。



設定ファイルについてのご注意
本製品以外の機器へ書き込み、改変による障害、および書き込みに伴う本製品の故障、誤動作、不具合、破損、データの消失、または停電などの外部要因により通信、通話などの機会を失ったために生じる損害や逸失利益、または第三者からのいかなる請求についても当社は一切その責任を負いかねますのであらかじめご了承ください。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

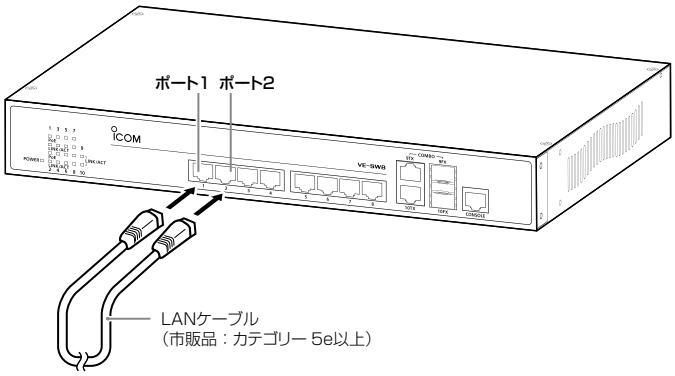
6 ご参考に

設定を出荷時の状態に戻すには

ネットワーク構成を変更するときなど、既存の設定データをすべて消去して、設定をはじめからやりなおすときは、本製品の設定内容を出荷時の状態に戻せます。
そのときの状況に応じて、製品本体、または設定画面の2とおりがあります。

製品本体で初期化する

本製品に設定されたIPアドレスやパスワードが不明な場合など、設定画面にアクセスできないときは、すべての機器を取りはずし、図のようにPoEポートの1番と2番をLANケーブルで接続してから、本製品の電源を入れなおしてください。
※再起動後、約1分で出荷時の設定(192.168.2.1)に戻ります。初期化後は、必要に応じて再設定してください。



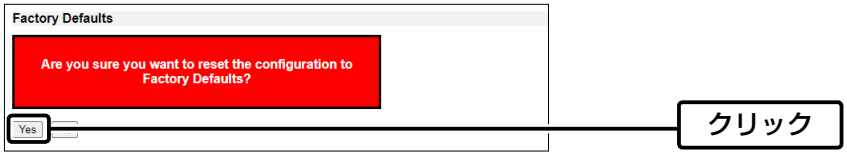
Maintenance > Factory Defaults

本製品に設定されたIPアドレスと管理者パスワードがわかっていて、そのIPアドレスで設定画面にアクセスできるときは、本製品の設定画面からIPアドレスを除く、すべての設定を出荷時の状態に戻せます。

設定画面で初期化する

1 「Maintenance」→「Factory Defaults」の順でクリックします。
「Factory Defaults」画面が表示されます。

2 [Factory Defaults]項目の〈Yes〉をクリックします。
出荷時の状態に戻ります。



三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

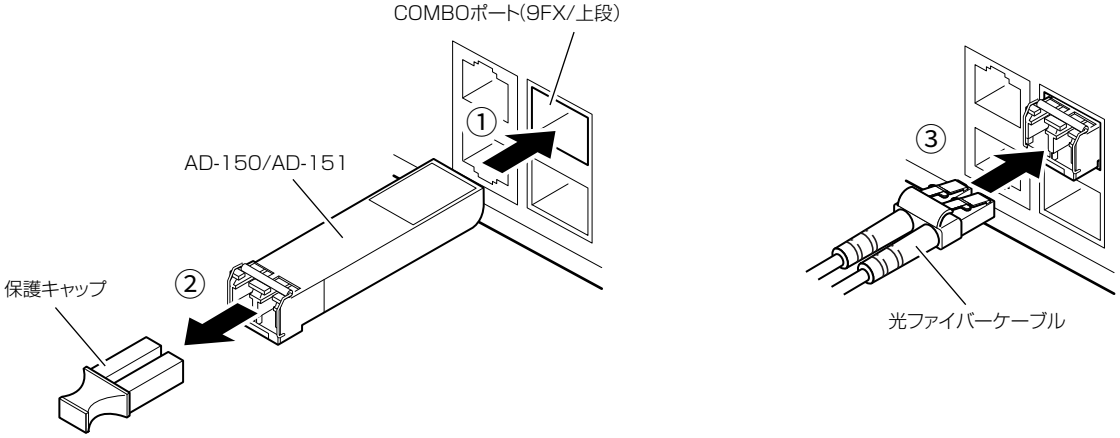
6 ご参考に

光ファイバーケーブルの接続について

光ファイバーケーブル(市販品)を接続するときは、SFPトランシーバー(別売品AD-150、AD-151)を本製品のCOMBOポート(9FX/10FX)に取り付けます。
※ホットスワップ対応のため、取り付けや取りはずしの際に、本製品の電源を切る必要はありません。

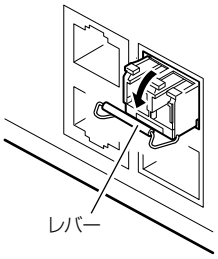
取り付けかた

① 本製品のCOMBOポートに、SFPトランシーバーを差し込みます。
② SFPトランシーバーの保護キャップを取りはずします。
③ 光ファイバーケーブルをSFPトランシーバーのコネクターに接続します。



取りはずしかた

① 光ファイバーケーブルを取りはずします。
② SFPトランシーバーのレバーを下げます。
③ SFPトランシーバーを引き抜きます。
※破損の原因になることがありますので、レバーを下げないまま無理に引き抜かないでください。



AD-150

トランシーバー種別	伝送速度	最大伝送距離	対応規格	ファイバ種別	コネクタータイプ
SFP	1Gbps	220m、550m	Fibre Channel 100-M5-SN-I	MMF	DLC(デュアルLC)
			Fibre Channel 100-M6-SN-I	MMF	
			1000Base-SX	MMF	

AD-151

トランシーバー種別	伝送速度	最大伝送距離	対応規格	ファイバ種別	コネクタータイプ
SFP	1Gbps	10km	Fibre Channel 100-SM-LC-L	SMF	DLC(デュアルLC)
			1000Base-LX	MMF/SMF	

別売品についてのご注意
弊社製別売品は、本製品の性能を十分に発揮できるように設計されていますので、必ず弊社指定の別売品をお使いください。
弊社指定以外の別売品とのご使用が原因で生じる無線機の破損、故障、または動作や性能については、保証対象外とさせていただきますので、あらかじめご了承ください。

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

6 ご参考に

定格

定格・仕様・外観等は、改良のため予告なく変更する場合があります。

寸法		約330(W)x44(H)x210(D)mm(突起物を含まず)	
重量		約2.35kg(本体のみ)	
電源		AC100～240V	
消費電力	PoE使用時	132W(最大)	
PoE	給電方式	Bタイプ給電方式	
	最大給電電力	30W(1ポートあたり)	
		120W(装置全体)	
動作温度		0～50℃	
動作湿度		10～90%（結露状態を除く）	
適合規格		クラスA情報技術装置(VCCI)	
インターフェース		PoEポート(RJ-45)	ポート1～8
			・オート MDI/MDI-X
			・オートネゴシエーション
			・10/100/1000BASE-T
			・フローコントロール
			・PoE+(Power over Ethernet)
		COMBOポート(RJ-45/SFP)	ポート9TX～10TX(LANポート)
			・1000BASE-T
			・オートネゴシエーション
			・オート MDI/MDI-X
			・フローコントロール
			ポート9FX～10FX(SFPポート)
			・100BASE-FX/1000BASE-X
			・オートネゴシエーション
			・オート MDI/MDI-X
			・フローコントロール
		CONSOLEポート(RJ-45)	

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

6 ご参考に

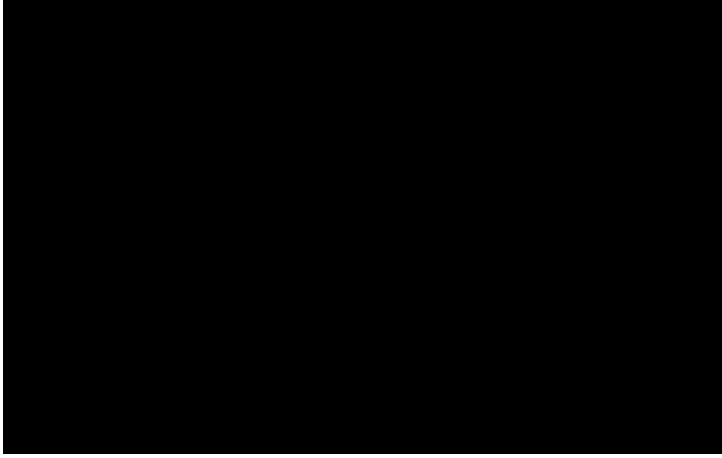
定格

規格	IEEE802.3 10BASE-T
	IEEE802.3u 100BASE-TX
	IEEE802.3ab 1000BASE-T
	IEEE802.3z 1000BASE-SX/LX (SFP)
	IEEE802.3af/at Power over Ethernet (PoE/PoE+)
	IEEE802.3az Energy Efficient Ethernet (EEE)
	IEEE802.3x Flow Control
	IEEE802.3ad Link Aggregation Control Protocol (LACP)
	IEEE802.1Q VLAN
	IEEE802.1v Protocol VLAN
	IEEE802.1p Class of Service
	IEEE802.1D Spanning Tree Protocol (STP)
	IEEE802.1w Rapid Spanning Tree Protocol (RSTP)
	IEEE802.1s Multiple Spanning Tree Protocol (MSTP)
	IEEE802.1AB Link Layer Discovery Protocol (LLDP)
	IEEE802.1X Port-Based Network Access Control
処理能力	14.88Mpps
スイッチング容量	20Gbps
パケットバッファ	4Mbits
MACアドレス登録数	8000
フローコントロール	IEEE802.3x (全二重)
	バックプレッシャー(半二重)
最大フレーム長	9600byte(VLAN Tagを含む)

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217

How the World Communicates

～コミュニケーションで世界をつなぐ～



アイコム株式会社
547-0003 大阪市平野区加美南1-1-32

三和システムサービス株式会社
〒330-0854 埼玉県さいたま市大宮区桜木町2-477 福島ビル3F
TEL 048-653-2211 FAX 048-653-2217