

Management Guide
ES1008VL

Management Guide
ES1008VL

Management Guide
ES1008VL

Management Guide
ES1008VL

Management Guide
ES1008VL

Management

ES1008VL
Management Guide

Management

ES1008VL

Management Guide
ES1008VL

Management Guide
ES1008VL

Management Guide
ES1008VL

Management Guide
ES1008VL

Management Guide
ES1008VL

Management Guide

本マニュアルについて

- 本マニュアルでは、ES1008VL の各種設定およびシステムの監視手順について説明します。
- 本マニュアルに記載している機能は、ファームウェアバージョン 1.0.3 以降の製品に対応して

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

◆ 下記事項は、安全のために必ずお守りください。



- 安全のための注意事項を守る
注意事項をよくお読みください。製品全般の注意事項が記載されています。
 - 故障したら使わない
すぐに販売店まで修理をご依頼ください。
 - 万一異常が起きたら
 - ◆ 煙が出たら
 - ◆ 異常な音、においがしたら
 - ◆ 内部に水・異物が入ったら
 - ◆ 製品を高所から落としたり、破損したとき
 - ①電源を切る（電源コードを抜く）
 - ②接続ケーブルを抜く
 - ③販売店に修理を依頼する
-

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



- 電源ケーブルや接続ケーブルを傷つけない
 - ◆ 電源ケーブルを傷つけると火災や感電の原因となります。
 - ◆ 重いものをのせたり、引っ張ったりしない。
 - ◆ 加工したり、傷つけたりしない。
 - ◆ 熱器具の近くに配線したり、加熱したりしない。
 - ◆ 電源ケーブルを抜くときは、必ずプラグを持って抜く。
 - 内部に水や異物を入れない
 - ◆ 火災や感電の原因となります。
 - ◆ 万一、水や異物が入ったときは、すぐに電源を切り（電源ケーブルを抜き）、販売店に点検・修理をご依頼ください。
 - 内部をむやみに開けない

本体及び付属の機器（ケーブル含む）をむやみに開けたり改造したりすると、火災や感電の原因となります。
 - 落雷が発生したらさわらない

感電の原因となります。また、落雷の恐れがあるときは、電源ケーブルや接続ケーブルを事前に抜いてください。本機が破壊される原因となります。
 - 油煙、湯気、湿気、ほこりの多い場所には設置しない

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

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



- めれた手で電源プラグやコネクタに触らない
感電の原因となります。
- 指定された電源コードや接続ケーブルを使う
マニュアルに記載されている電源ケーブルや接続ケーブルを使わないと、火災や感電の原因となります。
- 指定の電圧で使う
マニュアルに記されている電圧の範囲で使わないと、火災や感電の原因となります。
- コンセントや配線器具の定格を超えるような接続はしない
発熱による火災の原因となります。
- 通風孔をふさがない
 - ◆ 通風孔をふさいでしまうと、内部に熱がこもり、火災や故障の原因となります。また、風通しをよくするために次の事項をお守りください。
 - ◆ 毛足の長いジュウタンなどの上に直接設置しない。
 - ◆ 布などでくるまない。
- 移動させるときは、電源ケーブルや接続ケーブルを抜く
接続したまま移動させると、電源ケーブルが傷つき、火災や感電の原因となります。

1. コンソール接続による基本設定	1
1.1 初期設定	2
1.2 CLI コマンド	3
1.2.1 ? コマンド	3
1.2.2 default コマンド	3
1.2.3 help コマンド	3
1.2.4 Logout コマンド	4
1.2.5 Ping コマンド	4
1.2.6 Reset コマンド	4
1.2.7 set コマンド	5
1.2.8 show network コマンド	5
2. Web コンソール	6
2.1 設定	7
2.1.1 システム情報の表示と設定	7
2.1.2 ポート設定	9
2.1.3 MAC テーブル	11
2.1.4 VLAN	13
VLAN の追加	13
VLAN メンバー設定画面	13
VLAN の追加と削除	14
VLAN ポート設定	15
設定例	16
2.1.5 Private VLAN	18
Private VLAN 設定画面	18
設定例	19
2.1.6 ポートアグリゲーション	23
2.1.7 動的ポートアグリゲーション	24
LACP プロトコル設定	24
2.1.8 RSTP	25
RSTP システム設定	25
RSTP ポート設定	26
2.1.9 802.1x ユーザ認証	27
802.1X 設定	27
802.1X パラメータ	29
2.1.10 ループ検知機能	30
ループ検知機能の設定	30
ループ検知機能を解除する場合	31
2.1.11 ミラーリング	32
2.1.12 ストームコントロール	33

2.1.13	QoS	34
	QoS 設定	34
	QoS 設定 (802.1p)	35
	QoS 設定 (DSCP)	36
	QoS 設定 (キューの処理方法)	37
2.2	メンテナンス	38
2.2.1	設定ファイル	38
2.2.2	工場出荷時設定	38
2.2.3	ソフトウェアアップロード	39
2.2.4	再起動	39
2.2.5	ログアウト	39
2.3	モニタリング	40
2.3.1	ポートトラフィック	40
2.3.2	統計詳細	41
2.3.3	LACP ステータス	43
2.3.4	RSTP ステータス	44
2.3.5	VeriPHY(ケーブル診断)	45
2.3.6	Ping	46

1. コンソール接続による基本設定

この度は、ES1008VL をお買い上げ頂き誠にありがとうございます。

お使いになる前に、本書をよくお読みください。また、お読みになった後は、後日お役に立つこともありますので必ず保管してください。

本書は、本製品を正しくご利用頂く上で必要な機能説明および操作方法について記述してある本機はマネージメント端末を接続してマネージメント機能の設定をおこないます。

主な設定は、イーサネットポート経由で PC から Web ブラウザにておこないますが、最初に RS-232C シリアルポート経由でマネージメント機能にログインし、本機に適切な IP アドレス、サブネットマスク、デフォルトゲートウェイを割り当てる必要があります。

コンソール接続による基本設定

初期設定

1.1 初期設定

以下の手順で、コンソールのハードウェア接続を行ってください。

- (1) 同梱のコンソールケーブルでスイッチ本体と PC を接続します。
- (2) PC のターミナルエミュレータ（Windows98/2000/XP ハイパーターミナル等の VT100/ANSI に対応した）を起動し、ターミナルエミュレータを下表のとおり設定します。

設定項目	設定
通信速度	9600bps
データビット	8bit
パリティ	なし
ストップビット	1bit
フロー制御	なし

- (3) スwitchの電源を投入します。

全ての設定が正しく行われていれば、スイッチの電源投入後、ターミナルプログラムに起動画面が表示されます。

初期化メッセージが表示された後、以下の画面で停止しますので、パスワードを入力してください。初期設定のパスワードは「admin」になります。

```
Booting ...image 0
S/W Version: ES1008VL V1.0.3

Password:
```

[注意] 現在本機ではシングルユーザ管理のみサポートしています。

1.2 CLI コマンド

1.2.1 ? コマンド

"?" と入力することで、コマンドリストを表示することができます。

```
ES1008VL>?  
[Commands at top level]  
?..... Help commands  
default..... Restore to factory default setting  
help..... Help commands  
logout..... Logout  
ping..... Ping a specified host with IP address  
reset..... Reset system  
set..... Set commands  
show..... Show commands  
ES1008VL>
```

1.2.2 default コマンド

設定を工場出荷時の状態に戻します。また、IP address、Subnetmask、Gateway IP address の設定を除きすべての設定情報をクリアし工場出荷時の状態に戻すことも可能です。

文法

default

default keepip

- ・ keepip — IP address、Subnetmask、Gateway IP address 設定を保持し、工場出荷時の状態に戻します。

例

```
ES1008VL>default keepip  
*** Restoring to default configuration...
```

1.2.3 help コマンド

"? " コマンドと同様に、コマンドリストを表示します。

例

```
ES1008VL>help  
[Commands at Top level]  
?..... Help commands  
default..... Restore to factory default setting  
help..... Help commands  
logout..... Logout  
ping..... Ping a specified host with IP address  
reset..... Reset system  
set..... Set commands  
show..... Show commands  
ES1008VL>
```

1.2.4 Logout コマンド

ログアウトをおこないます。

例

```
ES1008VL>logout  
  
Password:
```

1.2.5 Ping コマンド

他のネットワークデバイスに対して Ping を送信することができます。

文法

`ping { -t < -n count > < -w timeout > } ipaddress`

-t : 連続して PING を送信 (Ctrl キーを押しながら C を押す事で終了)。

-n *count* : 送信する Echo リクエストの回数

-w *timeout* : リプライが戻ってくるまでの待ち時間 (単位 : 秒)

ipaddress : 送信先 IP アドレス

例

ノード 192.168.1.99 へ 5 回、タイムアウト 5 秒で PING を送信しています。

```
ES1008VL>ping -n 5 -w 5 192.168.1.99  
Reply from 192.168.1.99, packet      1, time      6 ms  
Reply from 192.168.1.99, packet      2, time      6 ms  
Reply from 192.168.1.99, packet      3, time      7 ms  
Reply from 192.168.1.99, packet      4, time      6 ms  
Reply from 192.168.1.99, packet      5, time      7 ms  
ES1008VL>
```

1.2.6 Reset コマンド

本機の再起動を行います。

例

```
ES1008VL>reset  
  
Booting ...image 0  
S/W Version: ES1008VL V1.0.3  
  
Password:
```

1.2.7 set コマンド

スイッチの IP 設定および、ログインパスワードの設定をおこないます。

文法

set password *password*

ログインパスワードの設定をおこないます。

- *password* : 任意のパスワードを入力します。

(Password は半角英数字もしくは半角記号で 1 桁以上 16 桁以内で設定ください。)

set ip DHCP { enable | disable }

DHCP モードの有効 / 無効

set ip static < *ipaddress* > { < *ipmask* > < *ipgateway* > < *vid* > }

スイッチの IP アドレス設定をおこないます。

- *ipaddress* : IP アドレス

- *ipmask* : サブネットマスク

- *ipgateway* : ゲートウェイ IP アドレス

- *vid* : 管理 VLAN の ID

本機は DHCP クライアント機能をサポートしています。

DHCP を有効にした場合、スイッチは起動時に、IP 設定を DHCP サーバから取得します。

"show network" コマンドにて DHCP 設定および現在の IP 設定を確認することができます。

DHCP の無効時、手動で IP 設定 (IP アドレス、ネットマスク、ゲートウェイ、VID) をおこなえます。例えば、以下の例のように入力することで、IP アドレスを 192.168.1.250 ネットマスクを 255.255.255.0、ゲートウェイを 192.168.1.155、VLAN ID を 1 に設定することができます。

[注意] DHCP 及び手動で IP を設定した場合は DHCP で取得した IP が有効となります。例

```
ES1008VL>set ip static 192.168.1.250 255.255.255.0 192.168.1.155 1
ES1008VL>
```

1.2.8 show network コマンド

スイッチの IP 設定情報を表示します。

```
ES1008VL>show network
IP Configuration:
  Address: 192.168.1.250
  Subnet Mask: 255.255.255.0
  Gateway: 192.168.1.155
  VID: 1
  Mode: enabled
  Gatewaymac: 00-00-00-00-00-00
  Static_gatewaymac: disabled
  dhcp: disabled
ES1008VL>
```

2. Web コンソール

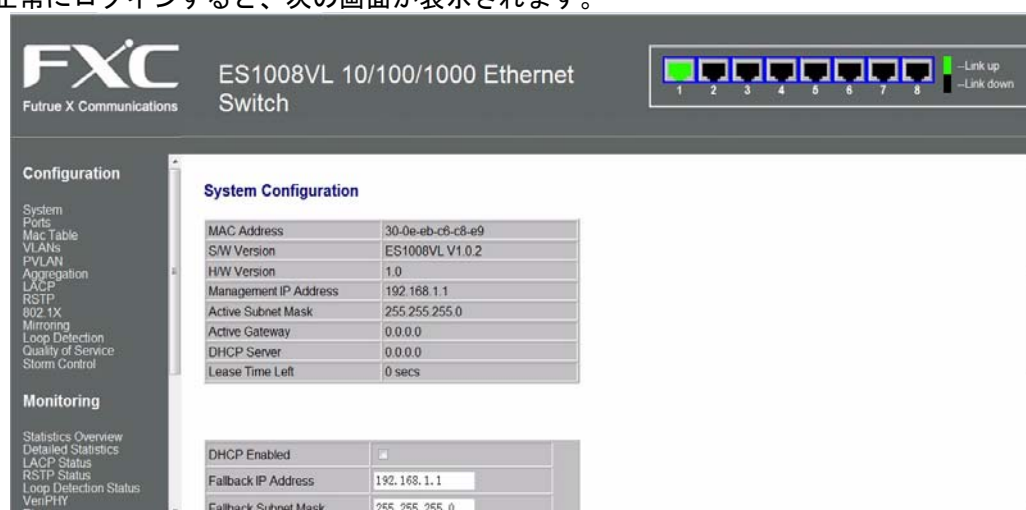
イーサネットポート経由でマネージメント機能に接続する前に、シリアルポート経由で本機にログインし、適切な IP アドレス、サブネットマスク、デフォルトゲートウェイを本機に設定する必要があります。（1.2.7 項「set コマンド」を参照してください）

Web ブラウザを起動し、設定したアドレスバーに IP アドレスを入力します。
以下のようにホームページが表示されます。



ログイン画面が表示されるのでパスワードを入力します。
初期設定のパスワードは「admin」になります。

正常にログインすると、次の画面が表示されます。



左側がファンクションリストになります。設定を行いたいメニューを選択します。
上部はスイッチのリンク状態を表示しています。
中央が各機能のオペレーションを行う場所になります。

2.1 設定

2.1.1 システム情報の表示と設定

スイッチのシステム情報の表示と設定を行います。

設定・表示項目

MAC Address

本機の MAC アドレスを表示。

S/W Version

ソフトウェアバージョンを表示。

H/W Version

ハードウェアバージョンを表示。

Management IP Address

管理 IP アドレスを表示。

Active Subnet Mask

サブネットマスクを表示。

Active Gateway

デフォルトゲートウェイを表示。

DHCP Server

DHCP サーバ IP アドレスを表示。

Lease Time Left

リース残り時間を表示。

DHCP Enabled

DHCP 機能の有効 / 無効を設定。チェックを入れることで有効になります。

Fallback IP Address

フォールバック IP アドレスを設定。

Fallback Subnet Mask

フォールバックサブネットマスクを設定。

Fallback Gateway

フォールバックゲートウェイを設定。

Fallback Gateway MAC

フォールバックゲートウェイ MAC アドレスを設定。

Management VLAN

設定に使用する管理 VLAN ID を設定します。

Password

ログインパスワードを設定します。

Inactivity Timeout (secs)

操作を行わなかった際に、自動でログアウトするまでの時間（秒）を設定。
"0" を入力すると自動ログアウトを行いません。

※フォールバックとは、DHCPで管理IPアドレスその他が取得出来なかった際に使用するアドレスです。

設定方法

上段の項目は全て閲覧のみとなります。

下段の必要な項目の設定変更を行い、＜ Apply ＞をクリックします。＜ Refresh ＞をクリックすることで、最新の情報に更新します。

System Configuration

MAC Address	00-17-2e-17-fb-47
S/W Version	ES1008VL V1.0.3
H/W Version	1.0
Management IP Address	192.168.1.1
Active Subnet Mask	255.255.255.0
Active Gateway	0.0.0.0
DHCP Server	0.0.0.0
Lease Time Left	0 secs

DHCP Enabled	☐
Fallback IP Address	192.168.1.1
Fallback Subnet Mask	255.255.255.0
Fallback Gateway	0.0.0.0
Fallback Gateway MAC	00-00-00-00-00-00 ☐
Management VLAN	1
Password	●●●●●
Inactivity Timeout (secs)	300

Apply

Refresh

2.1.2 ポート設定

ポートの各種設定を行います。また、ジャンボフレームの有効 / 無効、パワーセービングモードに関する設定もこのページで行えます。

設定・表示項目

Enable Jumbo Frames

ジャンボフレームの有効 / 無効を設定。チェックを入れることで有効になります。

(有効時 : 9,600byte 初期設定 : 無効)

Power Saving Mode

(初期設定 : 無効)

パワーセービングモードを選択します。

パワーセービングモードを使用した場合、使用されていないイーサネットポートを自動的に検出し、供給電力の削減やスタンバイ動作への切り替えを行うとともに、機器が接続されていた場合も LAN ケーブル長に応じた必要な電力レベルを動的に調節し消費電力を大幅に削減します。

- ・ Disable : 全てのパワーセービングモードは無効になります。
- ・ Link-Up : ACTiPHY モードのみを有効にします。
- ・ Link-down : LPI (Low Power Idle) モードのみを有効にします。
- ・ Full : 全てのパワーセービングモードが有効になります。

Link

現在のリンク状態を表示。

Mode

接続モードを選択。

- ・ Auto Speed : 対向機に合わせ、速度・Duplex を自動で設定します。
- ・ 10 Half : 10M 半二重接続。
- ・ 10 Full : 10M 全二重接続。
- ・ 100 Half : 100M 半二重接続。
- ・ 100 full : 100M 全二重接続。
- ・ 1000 full : 1000M 全二重接続。
- ・ Disable : ポートを無効にします。

Flow Control

フローコントロールの有効 / 無効を設定。チェックを入れることでフローコントロールが有効になります。

(初期設定 : 無効)

Drop frames after excessive collisions

再送回数が 16 回以上のコリジョン「excessive collisions」(過度のコリジョン) 発生の場合、発生後のフレームを破棄する場合に、チェックをいれます。

(初期設定 : 無効)

設定方法

必要な設定項目のドロップダウンリストから選択もしくはチェックボックスをチェックし
< Apply >をクリック、設定を反映させてください。

Power Saving Mode: Disable ▾

Port	Link	Mode	Flow Control
1	Down	Auto Speed ▾	☐
2	Down	Auto Speed ▾	☐
3	Down	Auto Speed ▾	☐
4	Down	Auto Speed ▾	☐
5	100FDX	Auto Speed ▾	☐
6	Down	Auto Speed ▾	☐
7	Down	Auto Speed ▾	☐
8	Down	Auto Speed ▾	☐

Drop frames after excessive collisions ☐

Apply

Refresh

2.1.3 MAC テーブル

エージングタイムの設定、静的アドレスの追加等、MAC アドレステーブルに関する各種設定を行います。

設定・表示項目

● Aging Time Setting

MAC アドレスに登録された動的エントリのエージングタイムを設定します。

ARL Aging Time

スイッチは、MAC アドレスを ARL テーブルへ自動的に学習します。

ある一定期間、同じ MAC アドレスが再度受信されることがない場合、これらのアドレスはテーブルから消去されます。このオペレーションはエージングと呼ばれます。

エージングオペレーションを行う間隔の設定ができます。

(初期値：300 範囲：10-65535 秒 0 はエージング無効)

● Static Address Table

本機はスタティック MAC アドレスの登録をサポートしています。

VID

静的アドレステーブルへ登録するエントリの VLAN ID。

MAC Address

静的アドレステーブルへ登録するエントリの MAC アドレス。

Destination Port

静的アドレステーブルへ登録するエントリのポート。

● Address Table

現在テーブルに登録されているエントリを表示します。「Delete」をクリックすることで、そのエントリを削除します。

設定方法

静的 MAC アドレステーブルの設定

- (1) 「VID」で VLAN エントリを入力します。
- (2) 「MAC Address」へ MAC アドレスを入力します。
- (3) 「Destination Port」で送信先ポートにチェックを入れます。
- (4) < Add > をクリックします。

Address Table

Previous Page		Next Page		
VID	MAC Address	Destination Port	Type	
1	aa-bb-cc-dd-ee-ff	1	static	Delete
1	aa-bb-cc-dd-ee-f0	3	static	Delete
1	aa-bb-cc-dd-ee-a1	2	static	Delete

2.1.4 VLAN

VLAN の追加

設定方法

- (1) VLAN ID を入力し、ドロップダウンリストから VLAN の種類を選択します。
 - Normal
 - Primary
 - Secondary
- (2) 「Add」をクリックすると、「VLAN Setup」の画面が表示されます。

Port Segmentation (VLAN) Configuration
Add a VLAN

VLAN ID		Normal v
----------------	----------------------	---

VLAN メンバー設定画面

設定方法

Port Segmentation (VLAN) Configuration 画面で Add a VLAN から新しい VLAN を作成するか、「Modify」をクリックします。VLAN Setup メニューで VLAN のメンバーポートを選択し、< Apply >をクリックします。

VLAN Setup

VLAN ID: 888 (TYPE: Normal)

Port	Member	Port	Member
Port 1	☐	Port 5	☐
Port 2	☒	Port 6	☐
Port 3	☐	Port 7	☐
Port 4	☐	Port 8	☒

VLAN の追加と削除

設定・表示項目

Modify

選択した VLAN のポートメンバーを修正します。

Delete

選択した VLAN を削除します。

Refresh

VLAN リストを更新します。

Port Config

「VLAN Per Port Configuration」の画面へ入ります。

PVLAN Mapping

PVLAN 設定画面へ入ります。詳細は P18 「Private VLAN」を参照してください。

設定方法

編集を行うには、VLAN を選択し Modify をクリックします。

削除するには VLAN を選択し Delete をクリックします。

Port Config をクリックすると、VLAN Per Port Configuration 画面が開き、Pvlan Mapping をクリックすると、Primary VLAN (PVLAN) Configuration 画面が開きます。

VLAN Configuration List							
Modify Delete Refresh Port Config Pvlan Mapping							
1	2	1003	1005	1007			
☐	☐	☐	☐	☒			

VLAN ポート設定

本システムは VLAN タグをサポートしており、ポートはタグ付きフレームを送信します。
初期設定では無効になっています。

設定・表示項目

Ingress Filtering Enabled

イングレスフィルタリング機能を有効にします。

本機能を有効にした場合、入力されたフレームに対して VLAN ID のチェックを行い、その入力フレームがポートに設定された VLAN グループの VLAN と異なる場合、このフレームを破棄します。

(初期値 : 無効)

Packet Type

タグ付フレームのみを受信または転送し、すべてのフレームを受信し転送するかを選択します。

(初期値 : 無効)

Pvid

ポートのデフォルトの UntagVID を設定します。

VLAN aware Enabled

IEEE802.1q VLAN のタグ付フレームを送受信します。このポートで送信されるフレームはポートが所属する PVID のタグが付けられ、受信するフレームからはタグが取り除かれ転送されます。

設定方法

Port Segmentation (VLAN) Configuration 画面で、「Port Config」をクリックします。

VLAN Per Port Configuration 画面が開きます。

ポートごとに VLAN の設定を行い、< Apply >をクリックします。

Port	VLAN aware Enabled	Ingress Filtering Enabled	Packet Type	Pvid
Port 1	☒	☐	☒ All ☐ Tagged Only	22
Port 2	☒	☐	☒ All ☐ Tagged Only	22
Port 3	☒	☐	☒ All ☐ Tagged Only	22
Port 4	☒	☐	☒ All ☐ Tagged Only	22
Port 5	☒	☐	☒ All ☐ Tagged Only	5
Port 6	☒	☐	☒ All ☐ Tagged Only	22
Port 7	☒	☐	☒ All ☐ Tagged Only	22
Port 8	☒	☐	☒ All ☐ Tagged Only	22

Apply

Cancel

設定例

ここでは、802.1QVLAN の設定を行います。

VLAN200 では VLAN タグを用いた通信を行う場合の設定例について説明します。

- (1) Port Segmentation (VLAN) Configuration 画面にて、「200」と入力して、< Add >をクリックします。

Port Segmentation (VLAN) Configuration

Add a VLAN

VLAN ID	200	Normal
---------	-----	--------

Add

- (2) ポート 7 および 8 を選択し、< Apply >をクリックします。

VLAN Setup

VLAN ID: 200 (TYPE: Normal)			
Port	Member	Port	Member
Port 1	☐	Port 5	☐
Port 2	☐	Port 6	☐
Port 3	☐	Port 7	☒
Port 4	☐	Port 8	☒

Apply

Refresh

- (3) 「Port Config」をクリックし、VLAN Per Port Configuration へ入ります。

VLAN Configuration List

Modify Delete Refresh Port Config Pvlan Mapping

1	2	200	300				
☐	☐	☐	☒				

(4) ポート 7, 8 の PVID をクリックして 200 を指定します。

Port	VLAN aware Enabled	Ingress Filtering Enabled	Packet Type	Pvid
Port 1	☐	☐	☒ All ☐ Tagged Only	1
Port 2	☐	☐	☒ All ☐ Tagged Only	1
Port 3	☐	☐	☒ All ☐ Tagged Only	1
Port 4	☐	☐	☒ All ☐ Tagged Only	1
Port 5	☐	☐	☒ All ☐ Tagged Only	1
Port 6	☐	☐	☒ All ☐ Tagged Only	1
Port 7	☐	☐	☒ All ☐ Tagged Only	200
Port 8	☐	☐	☒ All ☐ Tagged Only	200

Apply Cancel

None
1
2
200

(5) ポート 7, 8 に対して「VLAN aware Enabled」にチェック、＜ Apply ＞をクリックしてください。これで 802.1Q VLAN の設定は完了です。

Port 7	☒	☐	☒ All ☐ Tagged Only	200
Port 8	☒	☐	☒ All ☐ Tagged Only	200

Apply Cancel

2.1.5 Private VLAN

Private VLAN 設定画面

プライベート VLAN について

PVLAN (Private VLAN) とは、同じ VLAN 内のポートのブロードキャストドメインを分割できる VLAN のことです。

PVLAN により 1 つの VLAN 内でブロードキャストドメインを分割できるので、同じサブネット上でのセキュリティが 確保されます。また PVLAN の導入により、セキュリティ確保のための IP サブネットの分割が必要なくなります。

設定方法

プライマリ VLAN とセカンダリ VLAN は、システムでそれらが設定されている時のみ表示されます。本設定を行う前に Port Segmentation (VLAN) Configuration 画面から Primary VLAN と Secondary VLAN を作成しポートをアサインしてください。

- 1) VLAN Per Port Configuration からアサインした Primary VLAN Secondary VLAN の Pvid を選択します。

VLAN Per Port Configuration

Port	VLAN aware Enabled	Ingress Filtering Enabled	Packet Type	Pvid
Port 1	☐	☐	☒ All ☐ Tagged Only	1 ▼
Port 2	☐	☐	☒ All ☐ Tagged Only	6 ▼
Port 3	☐	☐	☒ All ☐ Tagged Only	9 ▼
Port 4	☐	☐	☒ All ☐ Tagged Only	10 ▼
Port 5	☐	☐	☒ All ☐ Tagged Only	3 ▼
Port 6	☐	☐	☒ All ☐ Tagged Only	1 ▼
Port 7	☐	☐	☒ All ☐ Tagged Only	1 ▼
Port 8	☐	☐	☒ All ☐ Tagged Only	1 ▼

Apply

Cancel

- (2) セカンダリ VLAN を選択します。

(3) < Confirm >をクリックし、VLAN マッピングを終了します。

Primary VLAN(PVLAN) Configuration

Primary Vlan: ▼

Secondary Vlan List

vlan 10	vlan 6	vlan 9
☒	☐	☐

設定例

この設定例では Primary VLAN100 を作成し Port8 をアサイン、Secondary VLAN101 ~ 107 を作成し Port1 ~ 7 に各々アサインしています。

- Primary VLAN100 は Secondary VLAN101 ~ 107 いずれとも通信が可能。
- Secondary VLAN101 ~ 107 は Primary VLAN100 と通信が可能。
- Secondary VLAN 間では組み合わせを問わず通信は不可。

(1) PrimaryVLAN100 を作成し Port8 をアサインします。

PortSegmentation(VLAN)Configuration 画面の Add a VLAN メニューから、VLANID100 を入力します。” Primary” を選択し、< Add >をクリックします。

Port Segmentation (VLAN) Configuration

Add a VLAN

VLAN ID	100	Primary ▼
		Normal
		Primary
		Secondary

VLAN Configuration List

(2) VLAN Setup 画面で Port8 を選択し、他のポートのチェックをはずします。

VLAN Setup

VLAN ID: 100 (TYPE: Primary)			
Port	Member	Port	Member
Port 1	☐	Port 5	☐
Port 2	☐	Port 6	☐
Port 3	☐	Port 7	☐
Port 4	☐	Port 8	☒

Apply

Refresh

(3) VLAN101 ~ 107 を SecondaryVLAN として作成します。

各 Secondary VLAN に任意ポートを (2) と同じ手順でアサインします。

次の例では Secondary VLAN104 を入力して < Add > をクリックし、Port4 をアサインしています。

Port Segmentation (VLAN) Configuration

Add a VLAN

VLAN ID	104	Secondary ▼
		Normal
		Primary
		Secondary

Add

VLAN Configuration List

Modify

Delete

Refresh

Port Config

Pvlan Mapping

1	100	101	102	103			
☐	☐	☐	☐	☒			

VLAN Setup

VLAN ID: 104 (TYPE: Secondary)			
Port	Member	Port	Member
Port 1	☐	Port 5	☐
Port 2	☐	Port 6	☐
Port 3	☐	Port 7	☐
Port 4	☒	Port 8	☐

Apply

Refresh

- (4) Port1 ~ 7 を Secondary VLAN101 ~ 107 に、Port8 を PrimaryVLAN100 を VLAN Per Port Configuration 画面で Pvid を選択します。

VLAN Per Port Configuration

Port	VLAN aware Enabled	Ingress Filtering Enabled	Packet Type	Pvid
Port 1	☐	☐	☒ All ☐ Tagged Only	101 ▼
Port 2	☐	☐	☒ All ☐ Tagged Only	102 ▼
Port 3	☐	☐	☒ All ☐ Tagged Only	103 ▼
Port 4	☐	☐	☒ All ☐ Tagged Only	104 ▼
Port 5	☐	☐	☒ All ☐ Tagged Only	105 ▼
Port 6	☐	☐	☒ All ☐ Tagged Only	106 ▼
Port 7	☐	☐	☒ All ☐ Tagged Only	107 ▼
Port 8	☐	☐	☒ All ☐ Tagged Only	100 ▼

None

1

100

デフォルトの Management VLAN は VLAN1 となります。

Pvid 変更の際は、Management VLAN を考慮し変更ください。

- (5) Primary VLAN(PVLAN)Configuration 画面で Pvlan Mapping をクリックし、Primary VLAN と Secondary VLAN のマッピング設定をします。

例では Primary VLAN100 に Secondary VLAN101 ~ 107 をマッピングしています。

Secondary Vlan List

vlan 101	vlan 102	vlan 103	vlan 104	vlan 105	vlan 106	vlan 107
☒	☒	☒	☒	☒	☒	☒

- (6) VLANs メニューから Port Segmentation(VLAN) Configuration 画面に戻り、各 Port から必要に応じてデフォルト VLAN1 を削除してください。

Port Segmentation (VLAN) Configuration

Add a VLAN

VLAN ID		Normal ▼
---------	----------------------	----------

Add

VLAN Configuration List

[Modify](#) [Delete](#) [Refresh](#) [Port Config](#) [Pvlan Mapping](#)

1 ☒	100 ☐	101 ☐	102 ☐	103 ☐	104 ☐	105 ☐	106 ☐
107 ☐							

VLAN Setup

VLAN ID: 1 (TYPE: Normal)			
Port	Member	Port	Member
Port 1	☐	Port 5	☐
Port 2	☐	Port 6	☐
Port 3	☐	Port 7	☐
Port 4	☐	Port 8	☐

[Apply](#) [Refresh](#)

2.1.6 ポートアグリゲーション

リンクアグリゲーションは複数の物理的なイーサネットポートを集約し、ES1008VL 間で論理的なアグリゲーションを形成します。

リンクアグリゲーションは、アグリゲーショングループ内の entry/exit 負荷が、全てのメンバー間でシェアされることで帯域幅の増加を可能にします。同時に、同じアグリゲーショングループポートの全てのメンバーは、接続信頼性の向上のため、相互に動的なバックアップを行います。

デフォルトでアグリゲーショングループは設定されていません。
本機器では 4 アグリゲーショングループをサポートしています。

設定方法

アグリゲーショングループに参加させるポートを選択し、＜ Apply ＞をクリックします。

Aggregation/Trunking Configuration

Group\Port	1	2	3	4	5	6	7	8
Normal	☐	☐	☒	☒	☐	☐	☐	☐
Group 1	☒	☒	☐	☐	☐	☐	☐	☐
Group 2	☐	☐	☐	☐	☒	☒	☒	☒
Group 3	☐	☐	☐	☐	☐	☐	☐	☐
Group 4	☐	☐	☐	☐	☐	☐	☐	☐

2.1.7 動的ポートアグリゲーション

LACP プロトコル設定

LACP（IEEE 802.3ad Link Aggregation Protocol）は、規格に準拠したスイッチ間の自動アグリゲーション方式を提供します。
デフォルトで LACP 設定されていません。

設定・表示項目

Protocol Enabled

チェックを入れたポートで LACP を有効にします。

Key Value

2 つの Key Value は同一にしてください。（範囲：1-255 推奨：auto）
ポートが同じアグリゲーションに参加するには同じ値が設定されている必要があります。

設定方法

LACP プロトコルを適用するポートの、「Protocol Enabled」チェックボックスにチェックを入れます。

LACP Port Configuration

Port	Protocol Enabled	Key Value
1	☒	auto
2	☒	auto
3	☐	auto
4	☐	auto
5	☐	auto
6	☐	auto
7	☒	128
8	☒	128

Apply

Refresh

2.1.8 RSTP

RSTP はネットワーク内の経路冗長化のためのプロトコルです。

主経路が使用不可になった場合、他の経路でフレームを転送を行うために自動的に再設定されます。

RSTP システム設定

設定・表示項目

System Priority

システムプライオリティ（範囲：0-61440 4096 毎 初期設定：32768）

Hello Time

本機がスパニングツリーのルートデバイスの場合に、スパニングツリー管理パケットを送信する間隔を設定します。（範囲：1-10 初期設定：2）

Max Age

スパニングツリー管理パケットを受信していない場合のスパニングツリーのエージングタイムを設定します。これはスパニングツリーの再作成を行います（範囲：6-40 初期設定：20）

Forward Delay

スパニングツリーの状態を変更（リスニング状態からラーニング状態への移行）する前の最大待ち時間を設定します。この設定が必要とされるのは、すべてのデバイスがフレームの転送を始める前にトポロジの変更についての情報を受信する必要があるからです。加えて、各ポートはブロッキング状態に再び戻るような障害情報（一時的なデータループの発生など）を検知するための時間が必要です。（範囲：4-30 初期設定：15）

Force Version

"Normal" 選択時、RSTP（Rapid Spanning Tree）で動作します。

"Compatible" 選択時には、旧 Spanning Tree モードで動作します。

設定方法

必要な項目の設定を行い、＜ Apply ＞をクリックします。

Hello Time、Forward Delay、Max Age の値は、以下の式で示される範囲内で設定してください。

- $2 \times (\text{Forward Delay} - 1 \text{ second}) \geq \text{Max Age}$
- $\text{Max Age} \geq 2 \times (\text{Hello Time} + 1 \text{ second})$

RSTP System Configuration	
System Priority	32768 ▼
Hello Time	2
Max Age	20
Forward Delay	15
Force version	Normal ▼

RSTP ポート設定

設定・表示項目

Protocol Enabled

チェックを入れたポートで RSTP を有効にします。

Edge

チェックを入れたポートをエッジにします。

Path Cost

デバイス間のパスコストを設定します。

設定方法

各ポートの、Protocol Enabled、Edge の設定を行います。

Path Cost を入力し、< Apply >をクリックします。

装置のポートは自動的にデフォルトパスコストを計算します。また、コストを手動で設定することも可能です。設定可能な範囲は 1 ～ 200000000 です。

Link rate	802.1t
10/half	2000000
10/full	2000000
100/half	200000
100/full	200000
1000/full	20000

Port	Protocol Enabled	Edge	Path Cost
Aggregations	☐		
1	☐	☒	auto
2	☐	☒	auto
3	☐	☒	auto
4	☐	☒	auto
5	☐	☒	auto
6	☐	☒	auto
7	☐	☒	auto
8	☐	☒	auto

Apply

Refresh

2.1.9 802.1X ユーザ認証

802.1X ユーザ認証を設定します。802.1X のモードの選択、RADIUS サーバー関連の設定、各ポートの設定およびステータスを確認できます。＜ Parameters ＞ボタンをクリックすることで、802.1X の各種パラメータ設定画面が表示されます。

802.1X 設定

802.1X 設定を行います。

設定・表示項目

● 802.1X 設定

Mode

802.1X 認証の有効 / 無効を選択。

RADIUS IP

RADIUS サーバ IP アドレスを設定。

RADIUS UDP Port

RADIUS サーバが使用する UDP ポート番号を設定 (初期値 : 1812) 。

RADIUS Secret

RADIUS サーバシークレットキー (15 文字以内)

802.1X Configuration	
Mode:	Disabled ▼
RADIUS IP	0.0.0.0
RADIUS UDP Port	1812
RADIUS Secret	

● ポート設定

Admin State

- ・ Auto : ポートは、認証サーバとサブリカントでやり取りされる認証結果に基づき認証状態または非認証状態に設定されます。
- ・ Force Authorized : ポートは、常に認証状態に設定されます。
- ・ Force Unauthorized : ポートは、常に非認証状態に設定されます。

Port State

現在のポートの状態を表示します。

Parameters

802.1X パラメータ設定画面を開きます。

設定方法

必要な項目を入力し、＜ Apply ＞をクリックします。＜ Refresh ＞をクリックすることで、最新の情報へ更新します。＜ Parameters ＞ボタンをクリックすることで 802.1X Parameters 設定画面が開きます。

Port	Admin State	Port State			
1	Force Authorized ▼	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
2	Force Authorized ▼	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
3	Force Authorized ▼	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
4	Force Authorized ▼	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
5	Force Authorized ▼	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
6	Force Authorized ▼	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
7	Force Authorized ▼	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
8	Force Authorized ▼	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
			Re-authenticate All	Force Reinitialize All	

Parameters

Apply

Refresh

802.1X パラメータ

802.1X Configuration 画面にて < Parameters > ボタンをクリックすることで 802.1X Parameters 設定画面が開きます。

設定・表示項目

Reauthentication Enabled

再認証の有効 / 無効を設定。

Reauthentication Period

再認証を行う間隔を設定。(1-3600 秒)

EAP timeout

認証タイムアウトを設定。(1-255 秒)

設定方法

- (1) Reauthentication Enabled にチェックを入れ、Reauthentication Period、EAP timeout の値を入力します。
- (2) < Apply > をクリックします。

802.1X Parameters	
Reauthentication Enabled	☐ Enabled
Reauthentication Period [1-3600 seconds]	3600
EAP timeout [1 - 255 seconds]	30
Apply Refresh	

2.1.10 ループ検知機能

ポートのループ検知機能の設定を行います。

ループ検知機能の設定

選択項目をチェックし、ループ検知機能を有効にします。

Loopback Detection Configuration

Port	LoopBack	Percentage
1	☒	LOW
2	☒	MIDDLE
3	☒	HIGH
4	☐	Unset
5	☐	Unset
6	☐	Unset
7	☐	Unset
8	☐	Unset

Apply

上の画面のように、指定するポート番号を選択し、＜ Apply ＞をクリックします。

- ・ 設定したポートから、ループ検知フレームを送信します。
(送信アドレス : 01:80:c2:00:00:10)
- ・ 上記の送信フレームを受信した場合ループ発生と判断し、該当ポートをシャットダウンします (ループ検知の LED が赤く点滅します)。

Percentage

ブロードキャスト (BC) またはマルチキャスト (MC) の、送受信の閾値を設定します。

設定した閾値を超えた場合、ループとみなし自動的にポートをシャットダウンします。

- ・ LOW : 該当ポートのスピードの 10% の BC,MC の送受信の閾値。
- ・ MIDDLE : 該当ポートのスピードの 40% の BC,MC の送受信の閾値。
- ・ HIGH : 該当ポートのスピードの 70% の BC,MC の送受信の閾値。

ループ検知機能を解除する場合

選択項目をチェックし、指定したポートのループ検知機能を解除します。

LoopBack Detection Status

Port	In Shutdown	In Loopback
1	☐	
2	☐	
3	☒	In Loopback
4	☐	
5	☐	
6	☐	
7	☐	
8	☐	

Apply

Loop Detection Status

ループ検知の確認と選択しているポートを解除します。

チェックをはずし、< Apply >をクリックしてください。

ポートをシャットダウンした場合、手動でのみ復帰が可能です。

- ・ In Shutdown

自動ポートシャットダウンした場合、チェック表示されポートがシャットダウンします。

- ・ In Loopback

ループを検知した場合、該当ポートに表示されます。

2.1.11 ミラーリング

ポートミラーリングの設定を行います。ミラーソースポートで受信したデータを、ミラーポートで監視することが可能です。

初期設定で、ポートミラーリングは設定されていません。

設定・表示項目

Mirror Source

被監視ポートにチェックを入れます。

Mirror Port

監視を行うポートをプルダウンメニューから選択します。

受信フレームのミラーリングのみサポートとなります。

設定方法

下の欄から、Mirror Port を選択し、その後に Mirror source を選択します。
< Apply >をクリックすることでポートモニタリング設定が終了します。

Mirroring Configuration

Port	Mirror Source
1	☐
2	☐
3	☐
4	☐
5	☐
6	☐
7	☒
8	☒

Mirror Port	1 ▼
-------------	-----

Apply

Refresh

2.1.12 ストームコントロール

ストームコントロールの設定を行います。本機では様々なタイプのフレームに対するストームコントロールをサポートしています。

全てのレートは、No Limit（リミット無し）または 1982k、3964k、5946k、7928k、32k、9910k、11892k、13874k、15856k、17838k、19820k、21802k、23874k、25766k、27748k、29730k、31712 k から選択が可能です。

設定・表示項目

Broadcast Rate

ブロードキャストレート

Multicast Rate

マルチキャストレート

Flooded unicast Rate

あて先不明でフラッドされたユニキャストレート

設定方法

各レートを選択し、＜ Apply ＞をクリックしてください。

Storm Control Configuration

Storm Control Number of frames per second	
Broadcast Rate	3964 ▼
Multicast Rate	1982 ▼
Flooded unicast Rate	No Limit ▼

Apply

Refresh

2.1.13 QoS

本機は 802.1p、DSCP の優先制御をサポートしています。

QoS 設定

設定・表示項目

QoS Mode

キューの処理方法を選択します。

- ・ Strict 絶対優先で、High キューから処理します。
- ・ WRR キューの重み付けに応じて処理します。

QoS モードを選択します。

- ・ QoS Disabled : QoS 無効
- ・ 802.1P プライオリティ機能の有効
- ・ DSCP : DSCP (Differential Service Code Point) プライオリティの有効

設定方法

QoS モードを選択し、「Apply」をクリックします。

QoS Configuration

Queue Mode	☒ Strict ☐ WRR
Note : WRR is not supported in Jumbo Frame mode.	
QoS Mode	QoS Disabled ▼ QoS Disabled 802.1p DSCP
APPLY CANCEL	

QoS 設定 (802.1p)

設定・表示項目

Prioritize Traffic

優先順位付けを行うトラフィック

- ・ custom : 任意に設定。
- ・ All Low Priority : すべての値を Low プライオリティに設定
- ・ All Normal Priority : すべての値を Normal プライオリティに設定
- ・ All Medium Priority : すべての値を Medium プライオリティに設定
- ・ All High Priority : すべての値を High プライオリティに設定

Priority

プライオリティを選択 (low、normal、medium、high)

設定方法

Prioritize Traffic を選択し、各 802.1p Value ごとの Priority を選択し < Apply > をクリックします。

QoS Configuration

Queue Mode	☒ Strict WRR
Note : WRR is not supported in Jumbo Frame mode.	
QoS Mode	802.1p ▼
Prioritize Traffic	Custom ▼

802.1p Configuration							
802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority
0	normal ▼	1	low ▼	2	low ▼	3	normal ▼
4	medium ▼	5	medium ▼	6	high ▼	7	high ▼

APPLY

CANCEL

QoS 設定 (DSCP)

設定・表示項目

Prioritize Traffic

優先順位付けを行うトラフィック

- ・ custom : 任意に設定。
- ・ All Low Priority : すべての値を Low プライオリティに設定
- ・ All Normal Priority : すべての値を Normal プライオリティに設定
- ・ All Medium Priority : すべての値を Medium プライオリティに設定
- ・ All High Priority : すべての値を High プライオリティに設定

DSCP Value

DSCP 値を入力 (0-63)

Priority

プライオリティを選択 (low、normal、medium、high)

設定方法

Prioritize Traffic を選択し、DSCP Value を入力します。Priority を low、normal、medium、high を選択し、< Apply >をクリックします

QoS Configuration

Queue Mode	☒ Strict ☐ WRR Note : WRR is not supported in Jumbo Frame mode.
QoS Mode	DSCP
Prioritize Traffic	Custom

DSCP Configuration	
DSCP Value(0..63)	Priority
0	low
24	medium
64	high
	high
	high
	high
	high
All others	high

APPLY

CANCEL

QoS 設定（キューの処理方法）

設定・表示項目

Queue Mode

キューの処理方法を設定

- ・ Strict : 絶対優先処理。キュー #1 が全て処理されてから #2 の処理を開始する。
(工場出荷時)
- ・ WRR : キューに重みづけを設定し、その値により処理する。

WRR Weight

キュー処理比率の設定

Queue Mode で、「WRR」を選択すると表示される。

設定方法

Queue Mode で「WRR」を選択します。

ドロップダウンリストから、処理比率を選択し、<Apply> をクリックします。

QoS Configuration

Queue Mode	☐ Strict ☒ WRR Note : WRR is not supported in Jumbo Frame mode.						
WRR Weight	The ratio of Low/Normal/Medium/High queue 1:2:3:4 ▼						
QoS Mode	1:1:1:5 ▼ 1:1:2:4 ▼						
Prioritize Traffic	1:1:2:6 ▼ 1:1:3:3 ▼ 1:1:3:5 1:2:2:3 1:2:2:5 1:2:3:4 1:3:3:3 2:2:2:2 2:2:2:4						

802.1p Configuration							
802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority
0	normal ▼	1	low ▼	2	low ▼	3	normal ▼
4	medium ▼	5	medium ▼	6	high ▼	7	high ▼

2.2 メンテナンス

2.2.1 設定ファイル

設定ファイルのアップロード、およびダウンロードを行います。

設定・表示項目

Configuration Upload

既に保存されている設定ファイルを、当機器にロードします。

「参照」ボタンで保存された設定ファイル名を選択し、Upload をクリックしてください。

Configuration Download

現行の設定を Download をクリックすることで、外部のパソコンなどにセーブします。

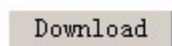
ファイル名は任意に設定できますが、設定しない場合は「swithc_config.cfg」になります。

Configuration Upload



The interface for Configuration Upload. It features a text input field for the file name, followed by a button labeled "参照..." (Reference...). Below this, there is a button labeled "Upload".

Configuration Download

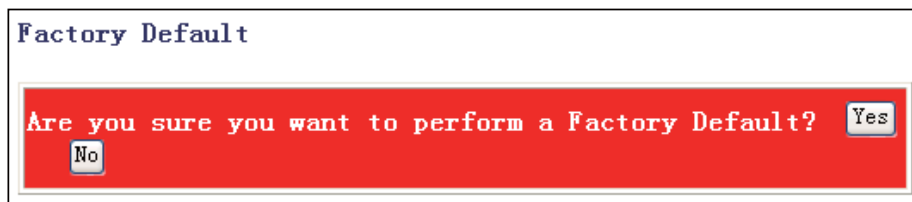


The interface for Configuration Download. It features a button labeled "Download".

2.2.2 工場出荷時設定

本機の設定を工場出荷時状態に戻します。

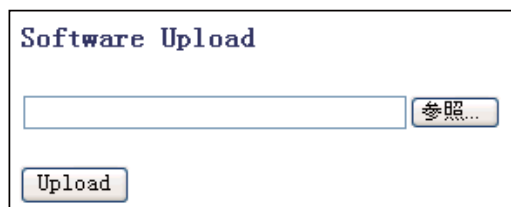
[注意] WEB GUI から Factory Default を行った場合、IP アドレスは設定されたままになります。



The Factory Default confirmation dialog. It has a title bar "Factory Default". The main area has a red background with the text "Are you sure you want to perform a Factory Default?". There are two buttons: "No" and "Yes".

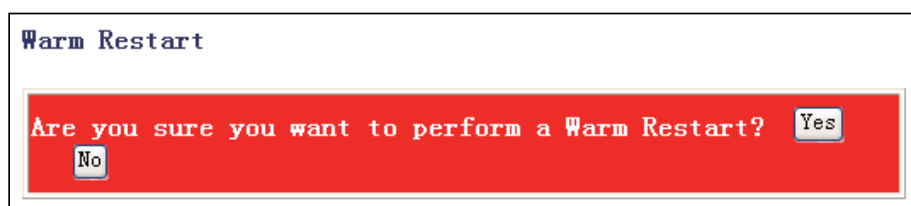
2.2.3 ソフトウェアアップロード

ソフトウェアをアップロードします。
「参照」ボタンでソフトウェアのファイル名を選択し、「Upload」をクリックします。



Software Upload

2.2.4 再起動

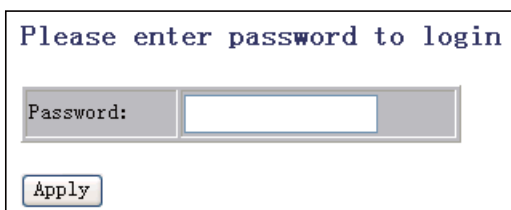


Warm Restart

Are you sure you want to perform a Warm Restart?

2.2.5 ログアウト

ログアウトをします。クリックすると、ログイン画面が表示されます。



Please enter password to login

Password:

2.3 モニタリング

2.3.1 ポートトラフィック

ポートの統計の概要を表示します。
「Clear」をクリックすると、統計をクリアします。
「Refresh」をクリックすると、最新の情報に更新します。

設定・表示項目

Tx Bytes

各ポートごとの送信バイトの合計

Tx Frames

各ポートごとの送信フレームの合計

Rx Bytes

各ポートごとの受信バイトの合計

Rx Frames

各ポートごとの受信フレームの合計

Tx Errors

各ポートごとの送信 CRC 異常フレームの合計

Rx Errors

各ポートごとの受信 CRC 異常フレームの合計

表示例

Statistics Overview for all ports

Clear

Refresh

Port	Tx Bytes	Tx Frames	Rx Bytes	Rx Frames	Tx Errors	Rx Errors
1	1289076688	14747410	2762944	43171	0	27
2	1289113168	14747980	2762304	43161	0	27
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	1721771	11973	213106906	1647891	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	5521792	86278	1310808446	15086946	0	30

2.3.2 統計詳細

各ポートごとの統計の詳細情報を表示します。
「Clear」をクリックすると、統計をクリアします。
「Refresh」をクリックすると、最新の情報に更新します。

設定・表示項目

● Receive Total, Transmit Total

各ポートごとの Rx Packets, Tx Packets
受信 / 送信されたメッセージの合計数

Rx Octets, Tx Octets

各ポートごとの受信 / 送信されたバイトの合計数

Rx Broad / Multicast, Tx Broad / Multicast

各ポートごとの送信 / 受信されたブロードキャスト / マルチキャストフレームの合計数

Rx Error Packets, Tx Error Packets

各ポートごとの送信 / 受信されたエラーフレームの合計数

● Receive Error Counters, Transmit Error Counters

Rx Fragments

各ポートごとのフラグメントした受信フレームの数

Rx Jabber

各ポートごとの受信されたジャンボフレームのフォーマット

Tx Drops

各ポートごとのドロップされたメッセージの数

Tx Overflow

各ポートごとのオーバーフローメッセージの数

[注意] Receive Size Counters、Transmit Size Counters はサポートされていません。

表示例

Statistics for Port 1

Clear

Refresh



Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8
Receive Total				Transmit Total			
Rx Packets	43171			Tx Packets	14747413		
Rx Octets	2762644			Tx Octets	1289076688		
Rx High Priority Packets	-			Tx High Priority Packets	-		
Rx Low Priority Packets	-			Tx Low Priority Packets	-		
Rx Broadcast	-			Tx Broadcast	-		
Rx Multicast	-			Tx Multicast	-		
Rx Broad- and Multicast	0			Tx Broad- and Multicast	14224136		
Rx Error Packets	27			Tx Error Packets	9		
Receive Size Counters				Transmit Size Counters			
Rx 64-Bytes	-			Tx 64-Bytes	-		
Rx 65-127-Bytes	-			Tx 65-127-Bytes	-		
Rx 128-255-Bytes	-			Tx 128-255-Bytes	-		
Rx 256-511-Bytes	-			Tx 256-511-Bytes	-		
Rx 512-1023-Bytes	-			Tx 512-1023-Bytes	-		
Rx 1024-Bytes	-			Tx 1024-Bytes	-		
Receive Error Counters				Transmit Error Counters			
Rx CRC Alignment	-			Tx Collisions	-		
Rx Undersize	-			Tx Drops	-		
Rx Oversize	-			Tx Overflow	-		
Rx Fragments	-						
Rx Jabber	-						
Rx Drops	-						

2.3.3 LACP ステータス

この画面で、現在の LACP のステータスを確認することができます。LACP トランクが作成されている場合、ポートグループメッセージが表示されます。

"Refresh" をクリックすることで最新の情報にアップデートできます。

設定・表示項目

● LACP Aggregation Overview

各ポートの動作状況を表示します。

● LACP Port Status

Protocol Active

ポートでプロトコルが有効化されているかを確認する

Partner Port Number

パートナーポート番号

Operetational Port Key

動作ポートキー

表示例

LACP Aggregation Overview

Group/Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Normal																

Legend

	Down	Port link down
0	Blocked	Port Blocked by RSTP. Number is Partner port number if other switch has LACP enabled
0	Learning	Port Learning by RSTP
	Forwarding	Port link up and forwarding frames
0	Forwarding	Port link up and forwarding by RSTP. Number is Partner port number if other switch has LACP enabled

Refresh

LACP Port Status

Port	Protocol Active	Partner Port Number	Operational Port Key
1	no		
2	no		
3	no		
4	no		
5	no		

2.3.4 RSTP ステータス

RSTP の概要およびポートステータスを表示します。

設定・表示項目

VLAN ID

VLAN ID

Bridge Id

ブリッジ ID

Hello Time

本機がスパニングツリーのルートデバイスの場合に、スパニングツリー管理パケットを送信する間隔を設定します。

Max Age

スパニングツリー管理パケットを受信していない場合のスパニングツリーのエージングタイムを設定します。これはスパニングツリーの再作成を引き起こします。

Fwd Delay

スパニングツリーの状態を変更（リスニング状態からラーニング状態への移行）する前の最大待ち時間を設定します。この設定が必要とされるのは、すべてのデバイスがフレームの転送を始める前にトポロジの変更についての情報を受信する必要があるからです。加えて、各ポートはブロッキング状態に再び戻るような衝突情報（一時的なデータループの発生など）を検知するための時間が必要です。

Topology

遷状態を表示

Root Id

ルートブリッジ ID

表示例

RSTP VLAN Bridge Overview

VLAN Id	Bridge Id	Hello Time	Max Age	Fwd Delay	Topology	Root Id
3	32771:00-11-f7-10-00-01	2	20	15	Steady	This switch is Root!
2	32770:00-11-f7-10-00-01	2	20	15	Steady	This switch is Root!
1	32769:00-11-f7-10-00-01	2	20	15	Steady	This switch is Root!

Refresh

RSTP Port Status

Port/Group	Vlan Id	Path Cost	Edge Port	P2p Port	Protocol	Port State
Port 1						Non-STP
Port 2						Non-STP
Port 3						Non-STP
Port 4						Non-STP
Port 5						Non-STP

2.3.5 VeriPHY(ケーブル診断)

VeriPHY(ケーブル損傷診断機能)

この VeriPHY(ケーブル損傷診断機能) を実行する事によって接続された LAN ケーブルのケーブル長や接続端子のペアの状態、短絡の有無を診断することが可能です。

設定・表示項目

Port

診断を行うポートを選択します。

Mode

診断モードを選択します。

- ・ Full : ケーブル実長チェックと全ての異常チェック
- ・ Anomaly : 全ての異常チェック
- ・ Anomaly w/o X-pair : w/o X-pair 異常チェック

表示例

VeriPHY Cable Diagnostics

Port

Port 1

Mode

Anomaly

Apply

Cable Status		
Pair	Length [m]	Status
A	—	—
B	—	—
C	—	—
D	—	—

2.3.6 Ping

ネットワーク内の他のノードへ ICMP echo リクエストパケットを送信することができます。

設定・表示項目

● Ping Parameters

Target IP address

PING 送信先 IP アドレス

Count

PING 送信回数（1、5、10、20 回）

Time Out

タイムアウト（1、5、10、30 秒）

● Ping Results

Status

PING の状態

Received replies

受信したリプライ数

Request timeouts

リクエストがタイムアウトした回数

Average Response Time

平均返答時間（ms）

表示例

Ping Parameters

Target IP address	
Count	1 ▼
Time Out (in secs)	1 ▼

Apply

Ping Results

Target IP address	0.0.0.0
Status	Test complete
Received replies	0
Request timeouts	0
Average Response Time (in ms)	0

ES1008VL Management Guide (FXC12-DC-200003-R1.1)

初版	2012 年 5 月
第 2 版	2012 年 6 月

- ◆ 本ユーザマニュアルは、FXC 株式会社が制作したもので、全ての権利を弊社が所有します。弊社に無断で本書の一部、または全部を複製 / 転載することを禁じます。
 - ◆ 改良のため製品の仕様を予告なく変更することがありますが、ご了承ください。
 - ◆ 予告なく本書の一部または全体を修正、変更することがありますが、ご了承ください。
 - ◆ ユーザマニュアルの内容に関しましては、万全を期しておりますが、万一ご不明な点がございましたら、弊社サポートセンターまでご相談ください。
-

Management Guide
ES1008VL

Management Guide
ES1008VL

Management Guide
ES1008VL

Management Guide
ES1008VL

Management Guide
ES1008VL

Management Guide
ES1008VL

Management Guide
ES1008VL

Management Guide
ES1008VL

Management Guide
ES1008VL

Management Guide
ES1008VL

Management Guide
ES1008VL

Management Guide
ES1008VL

Management Guide
ES1008VL