Modicon

MCSESM, MCSESM-E, MCSESP マネージドスイッチ
コンフィグレーション用ユーザーマニュアル

QGH59056.01

www.schneider-electric.com

Schneider Electric

本文書には、製品の性能に関する一般的な説明および技術的特性が記載されています。本書は、お客様の特定の用途に対する本製品の適合性または信頼性を確約するために作成されたものではありません。お客様またはインテグレーター様は自らの責任で、関連する特定の用途またはその使用に関する本製品のリスク分析、評価、および試験を完全かつ適切に行なってください。シュナイダーエレクトリック社あるいは系列会社は、本書に記載された情報の誤用に対して一切の責任を負いかねますので、あらかじめご了承ください。本書の内容について改善点や修正点の提案がある場合、また何らかの誤りを発見した場合には、弊社までご連絡ください。

本製品を設置して使用する際には、関連する都道府県、地域、地区の安全規定をすべて順守する必要があります。安全上の理由から、また立証済みのシステムデータに確実に準拠するため、部品の修理は製造業者にお任せください。

機器を技術的な安全要件がある用途に使用する場合、関連する指示に従ってください。

シュナイダーエレクトリック製のソフトウェアまたは承認されたソフトウェアを使用されない場合、傷害、損害、または不適切な動作が生じる可能性があります。

この情報に従わない場合、人的損害や装置の損傷を招くおそれがあります。

目次

安全上のご注意

注記：本書をよくお読みいただき、装置の正しい取り扱いと機能を十分ご理解いただいた上で、取り付け、操作、保守を行ってください。本書および装置には以下の表示が使われています。これらは、潜在的な危険を警告したり、手順を明確化あるいは簡素化する情報について注意を呼びかけたりするものです。

この記号が「危険」または「警告」安全ラベルに追加されると、電気的な危険が存在し、指示に従わないと人身傷害の危険があることを示します。

安全警告記号です。人的傷害の危険性があることを警告します。この記号の後に記載された安全に関する情報に従って、人的傷害や死亡の危険性を回避してください。

⚠ 危険

危険は、緊急で危険な状況を示しています。回避しないと、死亡や重傷を招きます。

⚠ 警告

警告は、危険が生じる可能性のある状況を示します。回避しないと、死亡や重傷を招くおそれがあります。

⚠ 注意

注意は、危険が生じる可能性のある状況を示します。回避しないと、軽症または中程度の傷害を招くおそれがあります。

注記

注記は、指示に従わないと物的損害を負う可能性があることを示します。

注記：電気装置の設置、操作、サービス、および保守は有資格者のみが行うことができます。定められた範囲外の使用によって生じた結果については、シュナイダーエレクトリックは一切の責任を負いかねます。

有資格者とは、電気装置の構造および操作ならびに設置に関する技術と知識を持ち、関連する危険性を認識して回避するための安全トレーニングを受けた人を指します。

本書について

有効性に関する注意

本書のデータや説明等の記載事項は拘束力があるものではありません。シュナイダーエレクトリックの方針である継続的な製品開発に従い、当社の製品を改良する権利はシュナイダーエレクトリックが有するものとします。本書に記載の情報は予告なく変更されることがあり、シュナイダーエレクトリックによる誓約として解釈されるべきものではありません。

お客様のフィードバック

本書に対するお客様のフィードバックを歓迎いたします。当社へのご連絡は右記メールアドレスを宛先としてください。techpub@schneider-electric.com

関連図書

この「コンフィグレーション用」ユーザーマニュアルには、デバイスのオペレーション開始に必要な情報が含まれています。使用環境でオペレーションするための初期スタートアップから基本設定までが、段階ごとに説明されています。

「インストール」マニュアルには、デバイスの説明、安全事項、ディスプレーの説明、その他インストールに必要な情報等が記載されています。

「グラフィカルユーザーインターフェース」参考マニュアルには、デバイスの個々の機能オペレーションに関する詳細情報が記載されています。

「コマンドラインインターフェース」参考マニュアルには、デバイスの個々の機能オペレーションに関する詳細情報が記載されています。

ネットワーク管理ソフトウェア ConneXium Network Manager では、円滑なコンフィグレーションやモニタリングの為の追加オプションが提供されています。
- オート・トポロジーディスカバリー
- ブラウザ・インターフェース
- クライアントサーバシステム構成
- イベントハンドリング
- イベントログ
- 複数デバイスの同時コンフィグレーション
- グラフィカルユーザーインターフェース及びそのネットワークレイアウト
- SNMP OPC ゲートウェイ

記号・注記

本書で使用する記号・注記等の意味は以下の通りです。

➢	リスト
☐	作業手順
Link	リンクとの相互参照
注記：	重要事項を強調する他、ユーザーの注意を促す
`Courier`	CLIコマンド又はグラフィカルユーザーインターフェース内フィールドのコンテンツ

グラフィカルユーザーインターフェース内での実行

コマンドラインインターフェース内での実行

不具合デバイスの交換

このデバイスは、元の不具合デバイスを同タイプのものと交換する際のプラグアンドプレイに関わるソリューションを提供するものです。

- 交換したデバイスのコンフィグレーションプロファイルは、外部メモリを通して新規のデバイス側にロードされます。
  102ページの「外部メモリからコンフィグレーションプロファイルを読み込む」をご参照ください。
- DHCP *Option 82* により、新規デバイスがIPアドレスを取得します。
  290ページの「DHCP L2 リレー」をご参照ください。
  333ページの「Option 82 によるDHCPサーバーのセットアップ」をご参照ください。

これら各ソリューションにより元デバイスのIP設定は、リブート時に新規デバイス側が取得します。

- このデバイスからHTTPSを利用したデバイスマネジメントにアクセスする際は、デジタル証明書が使用されています。ユーザー独自のデジタル証明書をデバイスにインポートすることも可能です。
  339ページの「HTTPS デジタル証明書の管理」をご参照ください。
- このデバイスからSSHを利用したデバイスマネジメントにアクセスする際は、RSAホストキーが使用されています。ユーザー独自のホストキーを、PEM形式でデバイスにインポートすることも可能です。
  336ページの「ユーザーのキーをデバイスにロードする」をご参照ください。

1 ユーザーインターフェース

以下のユーザーインターフェースを使用してデバイス設定を指定することができます。

表1 デバイス管理にアクセスするためのユーザーインターフェース

ユーザーインターフェース	アクセス経路	条件
グラフィカルユーザーインターフェース	イーサネット（インバンド）	ウェブブラウザ
コマンドラインインターフェース	イーサネット（インバンド） シリアルインターフェース（アウトバンド）	端末エミュレータ
システムモニター	シリアルインターフェース（アウトバンド）	端末エミュレータ

1.1 グラフィカルユーザーインターフェース

システム要件

グラフィカルユーザーインターフェースを開くには、HTML5がサポートされたウェブブラウザを使用できるデスクトップが必要となります。

注記：ウェブブラウザ等のサードパーティー製ソフトウェアは、有効期限やクリプトグラフィーによるパラメーター推奨値等を基準として証明書を認証しています。従って、有効期限が切れた場合やクリプトグラフィーによる推奨値が変更された場合などは、古い証明書ではエラーとなることがあります。このように、サードパーティー製ソフトウェアによる認証エラーを解決するには、ユーザーの最新証明書をデバイスに移行させるか、或いは最新のファームウェアで証明書を再度作成してください。

グラフィカルユーザーインターフェースを開始する

グラフィカルユーザーインターフェースを開始するための前提条件として、デバイスにIPパラメーターが設定されていなければなりません。43ページの「IPパラメーターの指定」をご参照ください。

以下の手順を実行します。

- ☐ ウェブブラウザを開きます。
- ☐ ウェブブラウザのアドレス入力フィールドに、デバイスのIPアドレスを入力します。右記の形式で入力してください。`https://xxx.xxx.xxx.xxx`
  ウェブブラウザからデバイスへの接続が設定され、ログインのダイアログボックスが表示されます。
- ☐ グラフィカルユーザーインターフェースの言語を変更する場合、ログインダイアログボックスの右上にある任意のリンクをクリックします。
- ☐ ユーザー名を入力します。
- ☐ パスワードを入力します。
- ☐ *Login* ボタンをクリックします。
  ウェブブラウザがグラフィカルユーザーインターフェースを表示します。

1.2 コマンドラインインターフェース

コマンドラインインターフェースにより、ローカル接続及びリモート接続にてデバイスの機能を使用することができます。

一般的に、IT機器のコンフィグレーションをする上でIT専門家が慣れ親しんだ環境が、コマンドラインインターフェースを通して提供されます。従って経験豊かなユーザー又は管理者であり、シュナイダーエレクトリックのデバイスの基本を理解していることが求められます。

1.2.1 データ接続の準備

デバイスの取付け及びスタートアップするために必要な情報は、「インストール」マニュアルをご参照ください。

- ☐ デバイスをネットワークに接続します。円滑なデータ接続を行うには、ネットワークパラメーターを正しく設定することが前提となります。

コマンドラインインターフェースのユーザーインターフェースは、*PuTTY*などのフリーウェアを使用してアクセスすることができます。

- ☐ PCに*PuTTY* のプログラムをインストールします。

1.2.2 Telnetによるコマンドラインインターフェースへのアクセス

WindowsでのTelnet接続

Telnetは、Windows Vista以前のバージョンのみに標準インストールされています。

以下の手順を実行します。

- ☐ PCの*Command Prompt*を開始します。
- ☐ コマンド`telnet <IP_address>`を入力します。

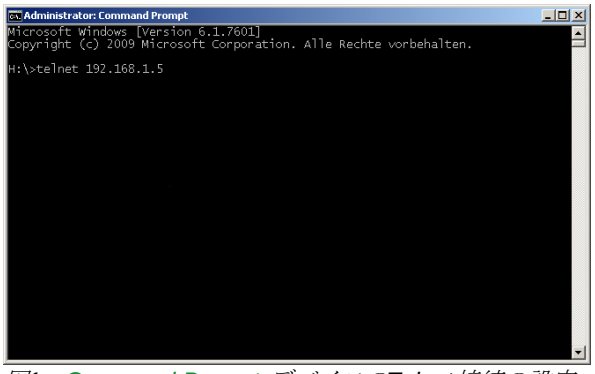


図1 Command Prompt: デバイスのTelnet接続の設定

PuTTYによるTelnet接続

以下の手順を実行します。

☐ PCの*PuTTY* プログラムを開始します。

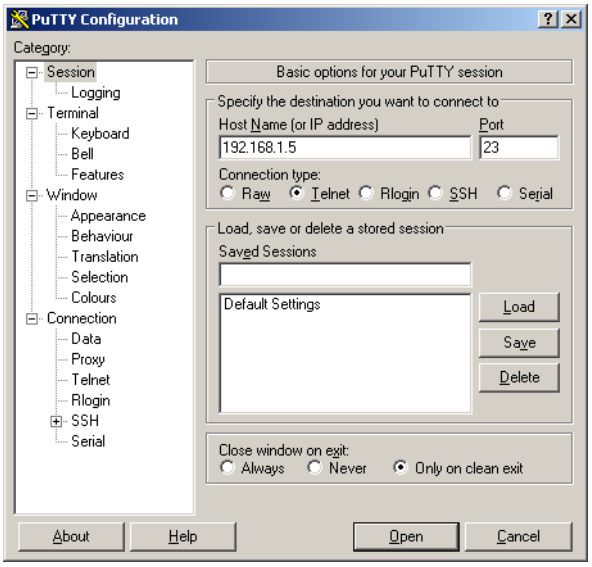


図2 PuTTY 入力画面

☐ *Host Name (or IP address)* フィールドに、使用デバイスのIPアドレスを入力します。
IPアドレスは0から255までの10進数4つで構成されています。これら4つの10進数はドットで分けられています。

☐ *Connection type* のオプションリストから、*Telnet* のラジオボタンを選択します。

☐ *Open* ボタンをクリックし、デバイスのデータ接続をセットアップします。
コマンドラインインターフェースと共にユーザー名入力ウィンドウが画面に表示されます。このデバイスでは、5名のユーザーまでが同時にコマンドラインインターフェースにアクセスすることができます。

注記：このデバイスはセキュリティ関連製品となっています。初期スタートアップ手順を進める際にパスワードを変更してください。

以下の手順を実行します。

☐ ユーザー名を入力します。
デフォルトのユーザー名はadminです。

☐ ＜Enter＞キーを押します。

- パスワードを入力します。
  デフォルトのパスワードはprivateとなっています。
- ＜Enter＞キーを押します。

```
                    Copyright (c) 2011-2021 Schneider

                      Electric All rights reserved

                        MCSESM-E Release 08.7.00

                       (Build date 2021-06-22 09:28)


                  System Name   :MCSESM-646038d5e836
                  Management IP :192.168.1.5
                  Subnet Mask   :255.255.255.0 Base
                  MAC           :64:60:38:01:02:03
                  USB IP        :91.0.0.100
                  USB Mask      :255.255.255.0
                  System Time   :2021-06-24 12:39:43


NOTE:Enter '?' for Command Help.Command help displays all
     options that are valid for the particular mode.
     For the syntax of a particular command form,
     please consult the documentation.

MCSESM-E>
```

図3　　コマンドラインインターフェースのスタート画面

1.2.3 SSH（Secure Shell）によるコマンドラインインターフェースへのアクセス

以下の例では、*PuTTY* プログラムを使用します。また、SSHを使用してデバイスにアクセスする他の方法として、OpenSSHスイートがあります。

以下の手順を実行します。

- PCの*PuTTY* プログラムを開始します。

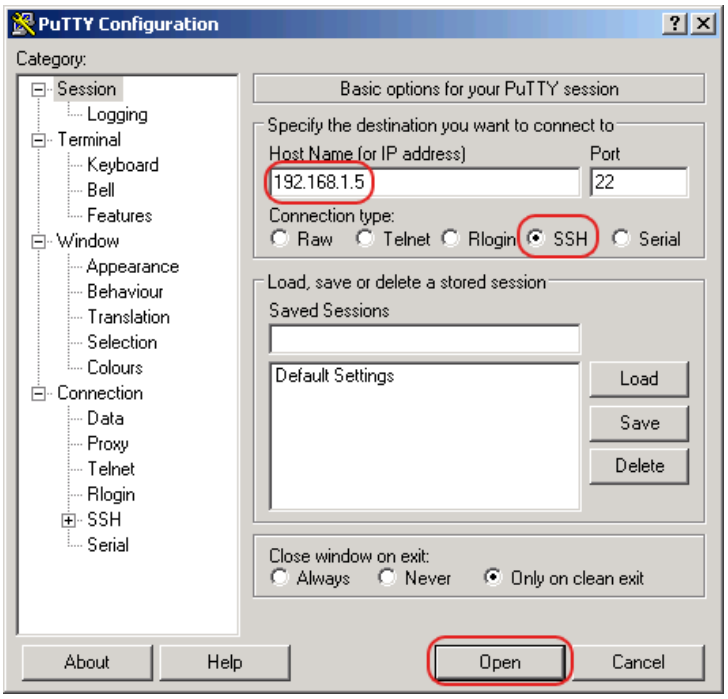


図4 PuTTY 入力画面

- *Host Name (or IP address)* フィールドに、使用デバイスのIPアドレスを入力します。
  IPアドレスは0から255までの10進数4つで構成されています。これら4つの10進数はドットで分けられています。
- 接続の種別（connection type）を選択するには、*Connection type* のオプションリストから、*SSH*のラジオボタンを選択します。選択後、要件に従いパラメーターを設定すると、SSHを通してデバイスとのデータ接続が確立します。

- ☐ *Open* ボタンをクリックし、デバイスのデータ接続をセットアップします。
  デバイス及びSSHのコンフィグレーションを行った時間によっては、接続の確立に1分程かかります。
  初期ログイン時、接続セットアップの終了が近くなると、*PuTTY* がセキュリティ警報メッセージを表示しますので、この時にキーのフィンガープリントを確認します。

図5　　フィンガープリントのセキュリティ警報プロンプト

- ☐ フィンガープリントを確認します。
  これにより、不要なゲストの侵入から保護します。
- ☐ このフィンガープリントがデバイスのフィンガープリントと一致した場合、*Yes* ボタンをクリックします。
  デバイスのフィンガープリントは、コマンド`show ssh`、又は*Device Security > Management Access > Server*ダイアログボックスの*SSH*タブに表示されます。
  コマンドラインインターフェースと共にユーザー名入力ウィンドウが画面に表示されます。このデバイスでは、5名のユーザーまでが同時にコマンドラインインターフェースにアクセスすることができます。
- ☐ ユーザー名を入力します。
  デフォルトのユーザー名は`admin`です。
- ☐ ＜Enter＞キーを押します。
- ☐ パスワードを入力します。
  デフォルトのパスワードは`private`となっています。
- ☐ ＜Enter＞キーを押します。

注記：このデバイスはセキュリティ関連製品となっています。初期スタートアップ手順を進める際にパスワードを変更してください。

```
login as: admin
admin@192.168.1.5's
password:


                              Copyright (c) 2011-2021 Schneider

                                Electric All rights reserved

                                  MCSESM-E Release 08.7.00

                                 (Build date 2021-06-22 09:28)


                        System Name   :MCSESM-646038d5e836
                        Management IP :192.168.1.5
                        Subnet Mask   :255.255.255.0 Base
                        MAC           :64:60:38:01:02:03
                        USB IP        :91.0.0.100
                        USB Mask      :255.255.255.0
                        System Time   :2021-06-24 12:39:43


NOTE:Enter '?' for Command Help.Command help displays all
      options that are valid for the particular mode.
      For the syntax of a particular command form,
      please consult the documentation.

MCSESM-E>
```

図6　　コマンドラインインターフェースのスタート画面

1.2.4 シリアルインターフェースを使用したコマンドラインインターフェースへのアクセス

外部のネットワーク管理ステーション（VT100端末又は端末エミュレータのあるPC）にローカルで接続するために、シリアルインターフェースを使用します。このインターフェースにより、コマンドラインインターフェース及びシステムモニターへのデータ接続が確立されます。

VT100端末設定	
速度	9600 bit/s
データ長	8 bit
ストップビット	1 bit
ハンドシェイク	off
パリティ	無し

以下の手順を実行します。

- シリアルインターフェースを使用し、デバイスを端末に接続します。他の方法としては、VT100用の端末エミュレータを使用したPCのCOMポートにデバイスを接続し、不特定のキーどれかを押します。
- その他*PuTTY*を使ったシリアルインターフェースとなるデバイスに、シリアルデータ通信を確立させる方法もあります。＜Enter＞キーを押します。

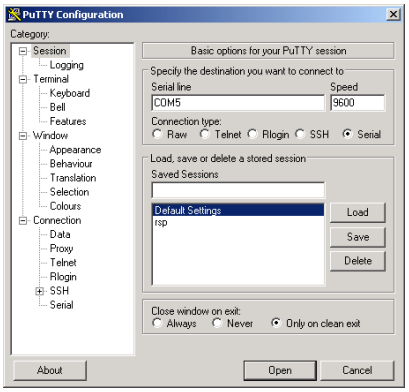


図7PuTTYを使ったシリアルインターフェースによるシリアルデータ通信

- ログイン画面にCLIモードが表示されるまで、端末キーボードの不特定のキーどれかを数回押します。
- ユーザー名を入力します。
  デフォルトのユーザー名は`admin`です。
- Enterキーを押します。
- パスワードを入力します。
  デフォルトのパスワードは`private`となっています。
- ＜Enter＞キーを押します。

注記：このデバイスはセキュリティ関連製品となっています。初期スタートアップ手順を進める際にパスワードを変更してください。

```
                    Copyright (c) 2011-2021 Schneider

                      Electric All rights reserved

                        MCSESM-E Release 08.7.00

                       (Build date 2021-06-22 09:28)


              System Name   :MCSESM-646038d5e836
              Management IP :192.168.1.5
              Subnet Mask   :255.255.255.0 Base
              MAC           :64:60:38:01:02:03
              USB IP        :91.0.0.100
              USB Mask      :255.255.255.0
              System Time   :2021-06-24 12:39:43


NOTE:Enter '?' for Command Help.Command help displays all
     options that are valid for the particular mode.
     For the syntax of a particular command form,
     please consult the documentation.

MCSESM-E>
```

図8　　コマンドラインインターフェースのスタート画面

1.2.5 モードに基づくコマンド階層

コマンドラインインターフェースでは、コマンドの種別によってそれぞれのコマンドが関連したモードとグループ化されています。全てのコマンドモードは、シュナイダーエレクトリック製ソフトウェアの特定コマンドをサポートしています。

ユーザーとして使用可能なコマンドは、ユーザーレベル（administrator/operator/guest/auditor）により異なります。更に、現在の使用モードによっても使用可能コマンドが異なります。特定のモードに切り替えた際は、そのモードで有用なコマンドが使用できるようになります。

これらコマンドのうち、User Exec modeのものは例外になります。コマンドラインインターフェースはこれらコマンドをPrivileged Exec modeでも実行させてくれます。

コマンドラインインターフェースのモードを下図に示します。

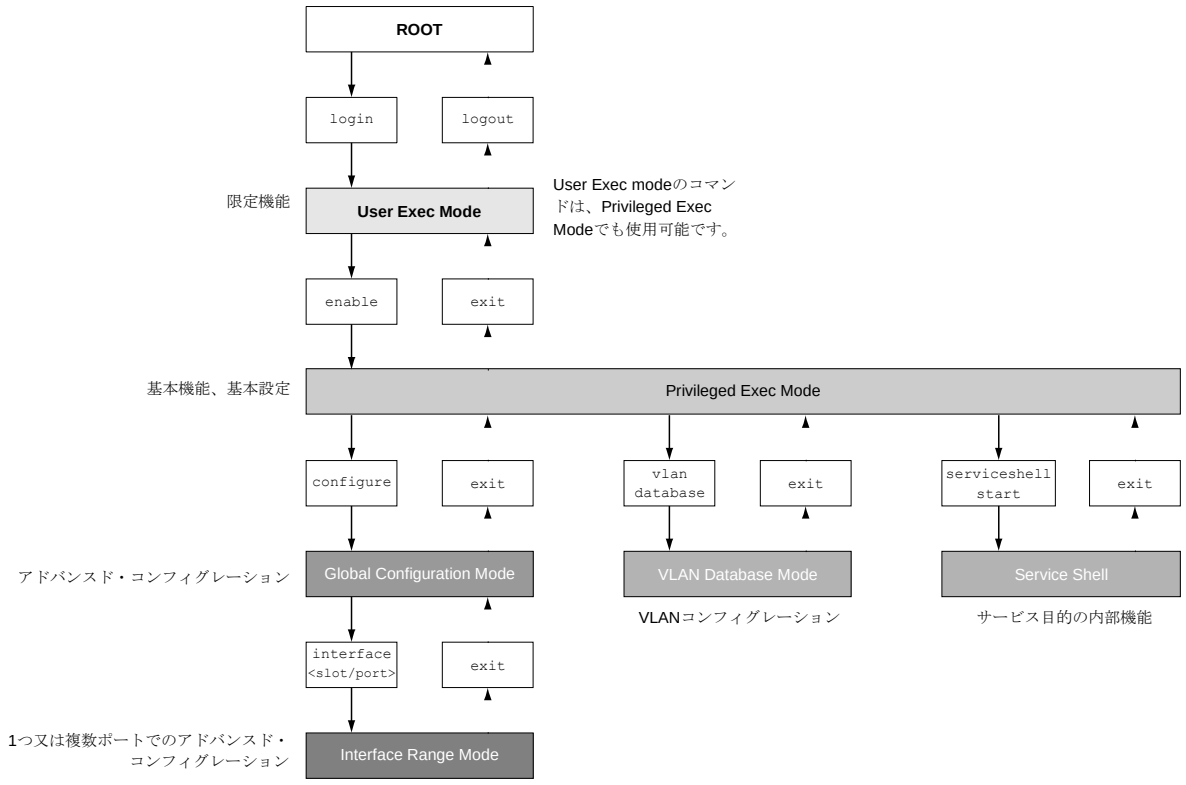


図9　　コマンドラインインターフェースの構造

コマンドラインインターフェースは、ユーザーレベルにより以下のモードをサポートします。

- User Exec mode
  コマンドラインインターフェースでログインの際は、User Exec modeでのログインとなります。User Exec modeでのコマンドには限りがあります。
  Command prompt: `(MCSESM-E) >`
- Privileged Exec mode
  コマンドの全てを利用するには、Privileged Exec modeでログインしなければなりません。特権ユーザーとしてログインすれば、Privileged Exec modeに入ることができます。Privileged Exec modeでは、User Exec modeのコマンドも実行可能です。
  Command prompt: `(MCSESM-E) #`
- VLAN mode
  VLAN modeでは、VLANに関連するコマンドが含まれます。Command prompt: `(MCSESM-E) (VLAN)#`
- Service Shell
  Service Shellはサービスのみが目的になります。Command prompt: `/mnt/fastpath #`

- Global Config mode
  Global Config modeでは、現在のコンフィグレーションに修正を加えることができます。このモードでは、一般のセットアップコマンドをグループ化します。
  Command prompt:`(MCSESM-E) (config)#`
- Interface Range mode
  Interface Range modeでは、デバイスの特定のポート、複数の選択されたポートのグループ、全てのポート、いずれにもコマンドが可能です。これらのコマンドは、単一ポート又は複数ポートの値を変更するか、或いはON/OFFの切り替えが可能です。
  - デバイスの物理ポート全て
    Command prompt:`(MCSESM-E) ((interface) all)#`
    例：Global Config modeからInterface Range modeに切り替えた場合、コマンドプロンプトは以下のように変わります。
    ```
    (MCSESM-E) (config)#interface all
    (MCSESM-E) ((Interface)all)#
    ```
  - インターフェース1つの単一ポート
    Command prompt:`(MCSESM-E) (interface <slot/port>)#`
    例：Global Config modeからInterface Range modeに切り替えた場合、コマンドプロンプトは以下のように変わります。
    ```
    (MCSESM-E) (config)#interface 2/1
    (MCSESM-E) (interface 2/1)#
    ```
  - インターフェース1つの、一定範囲のポート
    Command prompt:`(MCSESM-E) (interface <interface range> )#`
    例：Global Config modeからInterface Range modeに切り替えた場合、コマンドプロンプトは以下のように変わります。
    ```
    (MCSESM-E) (config)#interface 1/2-1/4
    (MCSESM-E) ((Interface)1/2-1/4)#
    ```
  - 単一ポートのリスト
    Command prompt:`(MCSESM-E) (interface <interface list>)#`
    例：Global Config modeからInterface Range modeに切り替えた場合、コマンドプロンプトは以下のように変わります。
    ```
    (MCSESM-E) (config)#interface 1/2,1/4,1/5
    (MCSESM-E) ((Interface)1/2,1/4,1/5)#
    ```
  - ポート範囲及び単一ポートのリスト
    Command prompt:`(MCSESM-E) (interface <complex range>)#`
    例：Global Config modeからInterface Range modeに切り替えた場合、コマンドプロンプトは以下のように変わります。
    ```
    (MCSESM-E) (config)#interface 1/2-1/4,1/6-1/9
    (MCSESM-E) ((Interface)1/2-1/4,1/6-1/9)
    ```

コマンドモード、対象モードで表示されるコマンドプロンプト（要求された入力文字）、どちらで当該モードを終了するかの選択、これらについて下表に記載されています。

表2　　コマンドモード

コマンドモード	アクセス方法	終了又は次のモードを開始

User Exec mode	初期アクセスレベル。基本タスクの実行及びシステム情報のリスティング	終了するには以下を入力
		`logout`:`(MCSESM-E) >logout`
		`Are you sure (Y/N) ?y`

Privileged Exec mode	User Exec modeから、以下コマンドを入力`enable`:
	`(MCSESM-E) >enable`
	`(MCSESM-E) #`
		Privileged Exec modeを終了しUser Exec modeへ戻るには、以下を入力
		`exit`:
		`(MCSESM-E) #exit`
		`(MCSESM-E) >`

表2　　コマンドモード

コマンドモード	アクセス方法	終了又は次のモードを開始
VLAN mode	Privileged Exec modeの状態で以下コマンドを入力：vlan database: (MCSESM-E) #vlan database (MCSESM-E) (Vlan)#	VLAN modeを終了してPrivileged Exec modeに戻るには、exit 又はCtrl + Z を押す (MCSESM-E) (Vlan)#exit (MCSESM-E) #
Global Config mode	Privileged Exec modeの状態で以下コマンドを入力：configure: (MCSESM-E) #configure (MCSESM-E) (config)# User Exec modeから、コマンドenableを入力し、 Privileged Exec modeで以下のコマンドを入力するConfigure: (MCSESM-E) >enable (MCSESM-E) #configure (MCSESM-E) (config)#	Global Config modeを終了してPrivileged Exec modeにPrivileged Exec modeに戻るには、以下を入力exit: (MCSESM-E) (config)#exit (MCSESM-E) # ここからPrivileged Exec modeを終了しPrivileged Exec modeに戻るには、再度exitを入力する: (MCSESM-E) #exit (MCSESM-E) >
Interface Range mode	Global Config modeの時、以下のコマンドを入力するinterface {all|<slot/port>|<interface range>|<interface list>|<complex ange>}. (MCSESM-E) (config)#interface <slot/ port> (MCSESM-E) (interface slot/port)#	Interface Range modeを終了してGlobal Config modeに戻るには再度exitを入力する。Privileged Exec modeに戻るには、Ctrl + Z を押す (MCSESM-E) (interface slot/port)#exit

プロンプトの最後にはてなマーク(?)を入力すると、コマンドラインインターフェースは有用なコマンドリスト及び各コマンドの簡単な説明を表示します。

```
(MCSESM-E)>
  cli             Set the CLI preferences.
  enable          Turn on privileged commands.
  help            Display help for various special keys.
  history         Show a list of previously run commands.
  logout          Exit this session.
  ping            Send ICMP echo packets to a specified IP address.
  show            Display device options and settings.
  telnet          Establish a telnet connection to a remote host.

(MCSESM-E)>
```

図10　　User Exec mode で使用可能なコマンド

1.2.6 コマンドの実行

シンタックス解析

コマンドラインインターフェースでログインの際は、User Exec modeでのログインとなります。コマンドラインインターフェースにより画面にプロンプト(MCSESM-E)> が表示されます。

コマンド入力後に＜Enter＞キーを押すと、コマンドラインインターフェースによりシンタックス解析が開始されます。コマンドラインインターフェースは、入力されたコマンドをツリーから検索します。

コマンドがコマンドラインインターフェースの域外にある場合は、エラーが検知され、メッセージ表示されます。

例：

show system info のコマンドを実行したいところ、info のf のアルファベットを入力せずに＜Enter＞キーを押した場合、

以下のメッセージがコマンドラインインターフェースにより表示されます。

```
(MCSESM-E)>show system ino
Error:Invalid command 'ino'
```

コマンドツリー構造

コマンドラインインターフェース内のコマンドは、ツリー状に整理されています。コマンド及びそれらに関連するパラメーターが存在するものは、コマンドが確実に定義されるまでツリーの枝が分岐しているために実行が可能です。コマンドラインインターフェースによって入力が確認されます。コマンド及びそのパラメーターを正確且つ完全に入力し、＜Enter＞キーを押してコマンドを実行します。

コマンド及び当該コマンドに求められるパラメーターを入力したら、入力されたその他のパラメーターはオプションパラメーターとして扱われます。いずれかのパラメーターが不明の場合、コマンドラインインターフェースがシンタックス形式のメッセージを表示します。

コマンドに求められるパラメーターがツリー構造の最後の枝に到達するまで、ツリーは分岐されています。

オプションパラメーターについても、コマンドに求められるパラメーターがツリー構造の最後の枝に到達するまで、ツリーは分岐されています。

1.2.7 コマンドの実行

この項ではシンタックス、規則、用語について記述し、これらの代表例も示します。

コマンドフォーマット

コマンドの殆どにはパラメーターが含まれています。

コマンドパラメーターが抜けている場合、不正確なコマンドシンタックスを検知したことをコマンドラインインターフェースが通知します。

なお、コマンドやパラメーターに関し、本書では`Courier`フォントで記載されています。

パラメーター

パラメーターのシーケンスは正確なシンタックスコマンドと関連しています。

パラメーターには値、オプション値、選択肢、又はこれらの組合せを要します。表記はパラメーターの種別を意味します。

表3: パラメーター及びコマンドシンタックス

`<command>`	山括弧(`<>`)内のコマンドは必須です。
`[command]`	ブラケット (`[]`) 内のコマンドは任意です。
`<parameter>`	山括弧 (`<>`) 内のパラメーターは必須です。
`[parameter]`	ブラケット (`[]`) 内のパラメーターは任意です。
`...`	エレメントの後に3点リーダ（ドット3つ、スペース無し）が続く場合、このエレメントを繰り返して良いことを意味します。
`[Choice1 | Choice2]`	ブラケット内のバーティカルバーは、選択オプションを意味します。値を一つ選択します。 ブラケット内のエレメントでバーティカルバーで区分されている場合、任意で選択可能であることを意味します（Option 1、Option 2、又はいずれも選択しない）。
`{list}`	ブレース (`{}`) は、このリストのオプションからパラメーターを選択することを意味します。
`{Choice1 | Choice2}`	ブレース (`{}`) に囲まれたエレメントでバーティカルバーで区分されたものは、オプションの選択が必須であることを意味します。
`[param1 {Choice1 | Choice2}]`	この場合、選択必須のオプションパラメーターであることを意味します。
`<a.b.c.d>`	小文字はワイルドカードを意味します。この場合、パラメーターをドットと共に a.b.c.d を入力します（例　IPアドレス）。
`<cr>`	Enterキーを押してキャリッジリターン（改行）します。

以下の表に、コマンドラインインターフェースで設定可能なパラメーター値を示します。

表4　　コマンドラインインターフェースのパラメーター値

値	概要
IP address	有効な IPv4 アドレスのパラメーター。アドレスは0から255までの10進数4つで構成されています。 これら4つの10進数はドットで分けられています。IPアドレスとして`0.0.0.0` も有効です。
MAC address	有効な MACアドレスのパラメーター。アドレスは0からFFまでの16進数6つで構成されています。これら数字はコロンで分けられています。例 `00:F6:29:B2:81:40`。
string	ユーザー定義された特定の長さのテキスト（最大で32文字）。
character string	文字ストリングを表現するには、"システム名と空白文字"のように、ダブルクォーテーションを使用。
number	特定の長さの整数、例えば`0..999999`。
date	`YYYY-MM-DD`形式の日付。
time	時刻の形式は`HH:MM:SS`。

ネットワークアドレス

ネットワークアドレスは遠隔ワークステーション、サーバー、その他ネットワーク等へのデータ接続を確立するために必要です。IPアドレスとMACアドレスとを区別しなければなりません。

IPアドレスは、ネットワーク管理者が割り当てるアドレスです。また、IPアドレスは一つのネットワークエリアで固有のものでなければなりません。

MACアドレスはハードウェアメーカー側で決定されています。MACアドレスは全世界で固有のものです。

アドレスの表記及びアドレス種別の範囲を下表に記載します。

表5　　ネットワークアドレスの形式及び範囲

アドレス種別	形式	範囲	例
IP アドレス	nnn.nnn.nnn.nnn	nnn:0～255 (10進数)	192.168.11.110
MACアドレス	mm:mm:mm:mm:mm:mm	mm:00～ff (16進数の組合せ)	A7:C9:89:DD:A9:B3

ストリング

ストリングは、ダブルクォーテーションで表記します。例として、`"システム名と空白文字"`。空白文字は有効なユーザー定義ストリングではありません。空白文字は、クォーテーションに囲まれたパラメーター内に入力します。

例：

```
*(MCSESM-E)#cli prompt Device name
Error:Invalid command 'name'

*(MCSESM-E)#cli prompt 'Device name'
```

```
*(Device name)#
```

1.2.8 コマンドの参考例

例1：clear arp-table-switch

キャッシュ管理エージェントのARPテーブルの削除コマンドは次の通りです。

コマンド名は、clear arp-table-switch となります。このコマンドは、他のパラメーターがなくても＜Enter＞キーを押すことで実行されます。

例2：radius server timeout

RADIUSサーバーの応答タイムアウト値の設定コマンドは次の通りです。

コマンド名は、(MCSESM-E) (config)#radius server timeout

```
 <1..30>          Timeout in seconds (default: 5). radius server timeout
```

がコマンド名となります。

パラメーターが必須となり、その範囲は1..30となります。

例3：radius server auth modify <1..8>

RADIUS認証サーバー1のパラメーター設定コマンドは次の通りです。

コマンド名は、(MCSESM-E) (config)#radius server auth modify 1

```
 [name]               RADIUS authentication server name.
 [port]               RADIUS authentication server port.
                      (default: 1812).
 [msgauth]            Enable or disable the message authenticator
                      attribute for this server.
 [primary]            Configure the primary RADIUS server.
 [status]             Enable or disable a RADIUS authentication server entry.
 [secret]             Configure the shared secret for the RADIUS authentication server.
 [encrypted]          Configure the encrypted shared secret.
  <cr>                Press Enter to execute the command.
```

radius server auth modify がコマンド名になります。

パラメーター<1..8> （RADIUSサーバーインデックス）が必須となり、その範囲は1..8 integer（整数）となります。

次のパラメーターは任意となります。[name], [port], [msgauth], [primary], [status], [secret] , [encrypted]

1.2.9 入力プロンプト

コマンドモード

入力プロンプトでは、3つのモードのうちどのモードにあるかをコマンドラインインターフェースが表示します。

- `(MCSESM-E) >`
  User Exec mode
- `(MCSESM-E) #`
  Privileged Exec mode
- `(MCSESM-E) (config)#`
  Global Config mode
- `(MCSESM-E) (Vlan)#`
  VLAN Database mode
- `(MCSESM-E) ((Interface)all)#`
  Interface Range mode / デバイスの全ポート
- `(MCSESM-E) ((Interface)2/1)#`
  Interface Range mode / 一つインターフェースの単一ポート
- `(MCSESM-E) ((Interface)1/2-1/4)#`
  Interface Range mode / 一つのインターフェースの一定範囲のポート
- `(MCSESM-E) ((Interface)1/2,1/4,1/5)#`
  Interface Range mode / 単一ポートのリスト
- `(MCSESM-E) ((Interface)1/1-1/2,1/4-1/6)#`
  Interface Range mode / ポート範囲及び単一ポートのリスト

アスタリスク、番号記号、感嘆符

- アスタリスク`*`
  入力プロンプトの先頭または二番目の位置のアスタリスク`*` は、揮発性メモリ内の設定及び不揮発性メモリの設定が異なることを意味します。これはデバイスがコンフィグレーションの際に保存されていない変更を検知したためです。
  `*(MCSESM-E)>`
- 番号記号`#`
  入力プロンプトの先頭の番号記号`#` は、ブートパラメーター及びブート中のパラメーターが異なることを意味します。
  `*#(MCSESM-E)>`
- 感嘆符`!`
  入力プロンプトの銭湯の感嘆符`!` は、`user`又は`admin` ユーザーアカウントがデフォルト設定と一致することを意味します。
  `!(MCSESM-E)>`

ワイルドカード

当デバイスでは、コマンドラインプロンプトの変更が可能です。

コマンドラインインターフェースでは以下のワイルドカードがサポートされます。

表6　コマンドラインインターフェースの入力プロンプトでのワイルドカードの使用

ワイルドカード	意味
`%d`	システム日付
`%t`	システム時刻

表6　コマンドラインインターフェースの入力プロンプトでのワイルドカードの使用

ワイルドカード	意味
%i	デバイスのIPアドレス
%i	デバイスのMACアドレス
%p	デバイスの製品名

```
!(MCSESM-E)>enable

!(MCSESM-E)#cli prompt %i

!192.168.1.5#cli prompt (MCSESM-E)%d

!*(MCSESM-E)2021-06-24#cli prompt (MCSESM-E)%d%t

!*(MCSESM-E)2021-06-24 12:39:43#cli prompt %m

!*AA:BB:CC:DD:EE:FF#
```

1.2.10 ショートカットキー

以下のショートカットキーを使用することでコマンドラインインターフェースの作業が便利になります。

表7　コマンドラインインターフェースでのショートカットキー

ショートカットキー	用途
<CTRL> + <H>, <Backspace>	1つ前の文字を消去
<CTRL> + <A>	行の先頭に移動
<CTRL> + <E>	行の末尾に移動
<CTRL> + <F>	1つ前の文字に移動
<CTRL> + <B>	1つ後ろの文字に移動
<CTRL> + <D>	選択中の文字を消す
<CTRL> + <U>, <X>	行の先頭までを消去
<CTRL> + <K>	行の末尾までを消去
<CTRL> + <W>	1つ前の単語を消去
<CTRL> + <P>	ヒストリーバッファにある1つ前の行に移動
<CTRL> + <R>	行の上書き又はペースト
<CTRL> + <N>	ヒストリーバッファにある1つ後ろの行に移動
<CTRL> + <Z>	rootコマンドプロンプトに戻る
<CTRL> + <G>	tcpdumpのセッションを中止
<Tab>, <SPACE>	コマンドライン完成
Exit	次の下にあるコマンドプロンプトに移動
<?>	リスト選択肢

HELPコマンドは、画面のコマンドラインインターフェース内で使用可能なショートカットキーを表示します。

```
(MCSESM-E) #help

HELP:
Special keys:

  Ctrl-H, BkSp delete previous character
  Ctrl-A .... go to beginning of line
  Ctrl-E .... go to end of line
  Ctrl-F .... go forward one character
  Ctrl-B .... go backward one character
  Ctrl-D .... delete current character
  Ctrl-U, X .. delete to beginning of line
  Ctrl-K .... delete to end of line
  Ctrl-W .... delete previous word
  Ctrl-P .... go to previous line in history buffer
  Ctrl-R .... rewrites or pastes the line
  Ctrl-N .... go to next line in history buffer
  Ctrl-Z .... return to root command prompt
  Ctrl-G .... aborts running tcpdump session
  Tab, <SPACE> command-line completion
  Exit    .... go to next lower command prompt
  ?       .... list choices (MCSESM-E) #

  (MCSESM-E) #
```

図11　Helpコマンドによるショートカットキーのリスト

1.2.11 データ入力のエレメント

コマンドの完了

コマンドのタイピングを簡略化するために、コマンドラインインターフェースではコマンド補完（タブ補完）の使用ができます。これにより、キーワード入力を省略することができます。

- まず、キーワードの入力を開始します。コマンドラインインターフェースが入力された文字からキーワードを検知すると、Tabキー又はスペースキーを押した後にキーワードを補完します。入力補完の選択肢が複数ある場合、キーワードを検出するに要する特有の文字（1文字以上）を入力します。再度Tabキー又はスペースキーを押します。その後、システム側でコマンド又はパラメーターの入力を補完します。
- 固有でない文字を入力し＜Tab＞又は＜スペース＞キーを2度押すと、コマンドラインインターフェースから選択肢のリストが表示されます。
- 固有でない文字を入力し＜Tab＞又は＜スペース＞キーを押すと、固有のコマンドに到達するまでコマンドラインインターフェース側で補完します。複数のコマンド候補がある場合で＜Tab＞又は＜スペース＞キーを再度押すと、コマンドラインインターフェースから選択肢のリストが表示されます。

  例：

  ```
  (MCSESM-E) (Config)#lo
  (MCSESM-E) (Config)#log
  logging logout
  ```

  ここで`lo` と入力し＜Tab＞又は＜スペース＞キーを押すと、固有のコマンドに到達するまでコマンドラインインターフェース側で補完します。
  ＜Tab＞又は＜スペース＞キーを再度押すと、コマンドラインインターフェースから選択肢のリスト (`logging logout`)が表示されます。

コマンドやパラメーターの候補

コマンドやパラメーターの候補リストを表示するには`help` 又は `?`を入力します。例：`(MCSESM-E) >show ?`

表示されたコマンドを入力すると、当該コマンドで可能なパラメーターのリストが表示されます。
`show.`

コマンドとクエスチョンマークの間に空白文字を入れないで入力した場合、当デバイスからコマンドそのものに対するヘルプテキストを表示します。

```
!*#(MCSESM-E)(Config)#show?

   show          Display device options and settings.
```

1.2.12 ユースケース

コンフィグレーションの保存

デバイスのリセット時又は停電後にもパスワード設定やその他変更したコンフィグレーションを確実に残すためには、コンフィグレーションを保存してください。以下の手順を実行します。

☐ `enable` を入力し、Privileged Exec modeへ移行します。
☐ 以下コマンドを入力します。
`save [profile]`
☐ ＜Enter＞キーを押すことで実行されます。

„radius server auth add“ コマンドのシンタックス

上記コマンドでRADIUS認証サーバーを追加します。

- モード：`Global Config` mode
- ユーザー認証レベル：Administrator
- フォーマット：`radius server auth add <1..8> ip <a.b.c.d> [name <string>] [port <1..65535>]`
  - `[name]`:RADIUS認証サーバー名。
  - `[port]`:RADIUS認証サーバーポート（デフォルト値：`1813`）。

パラメーター	意味	数値候補
`<1..8>`	RADIUS認証サーバーインデックス。	`1..8`
`<a.b.c.d>`	RADIUSアカウンティングサーバーの	IPアドレス
`<string>`	最大32文字の、ユーザー定義されたテキスト。	
`<1..65535>`	1～65535の間のポート番号を入力。	`1..65535`

モード及びユーザー認証レベル：

- コマンドの実行には条件があります。Global Config modeでなければなりません。25ページの「モードに基づくコマンド階層」をご参照ください。
- コマンドの実行には条件があります。Administratorとしてのアクセス権が必須です。

コマンド及びパラメーターのシンタックスは、 29ページの「コマンドの構造」をご参照ください。

実行可能コマンドの例：

- `radius server auth add 1 ip 192.168.30.40`
- `radius server auth add 2 ip 192.168.40.50 name radiusserver2`
- `radius server auth add 3 ip 192.168.50.60 port 1813`
- `radius server auth add 4 ip 192.168.60.70 name radiusserver4 port 1814`

1.2.13 Service Shell

Service Shellはサービスのみが目的になります。

ユーザーはService Shellにより、デバイスの内部機能へのアクセスが可能となります。デバイスに関するサポートが必要な場合は、サービス技師に、内部状況をモニターするのにService Shellを使用してもらわなければなりません（例：スイッチやCPUのレジスター）。

サービス技師の指示なく内部機能を実行しないでください。不揮発性メモリ（*NVM*）のコンテンツ消去などの内部機能の実行により、**デバイスが操作不能となる可能性があります**。

Service Shellの開始

条件としては、User Exec modeでなければなりません：`(MCSESM-E) >`

以下の手順を実行します。

- ☐ `enable` を入力し、＜Enter＞キーを押します。
  次の方法でタイピングの手間を省くことができます。
  - `e` を入力し、＜Tab＞キーを押します。
- ☐ `serviceshell start` を入力し、＜Enter＞キーを押します。
  次の方法でタイピングの手間を省くことができます。
  - `ser` を入力し、＜Tab＞キーを押します。
  - `s` を入力し、＜Tab＞キーを押します。

```
!MCSESM-E >enable

!*MCSESM-E #serviceshell start
 WARNING!The service shell offers advanced diagnostics and functions.
 Proceed only when instructed by a service technician.

 You can return to the previous mode using the 'exit' command.

 BusyBox v1.31.0 (2021-06-24 12:39:43 UTC) built-in shell (ash)
 Enter 'help' for a list of built-in commands.

!/mnt/fastpath #
```

Service Shellの作業

Service Shellがアクティブの時、コマンドラインインターフェースのタイムアウトは非アクティブです。コンフィグレーションの矛盾を防ぐため、他のユーザーがデバイスに対して新たなコンフィグレーションを行う前にService Shellを終了してください。

Service Shellコマンドの表示

条件として、既にService Shellが開始されてなければなりません。以下の手順を実行します。
☐ `help` を入力し、＜Enter＞キーを押します。

```
/mnt/fastpath # help

Built-in commands:
------------------
        . : [ [[ alias bg break cd chdir command continue echo eval exec
        exit export false fg getopts hash help history jobs kill let local
        pwd read readonly return set shift source test times trap true
        type ulimit umask unalias unset wait
/mnt/fastpath #
```

Service Shellの終了

以下の手順を実行します。
☐ `exit` を入力し、＜Enter＞キーを押します。

デバイスでService Shellを恒久的に無効化する

Service Shellを無効化しても、デバイスの設定は可能です。但し、サービス技師が使用できるシステム診断プログラムの内容に制限がかかります。デバイスの内部機能にサービス技師がアクセス出来なくなります。

なお、一度無効化したものは戻すことができません。Service Shellは恒久的に無効となります。**Service Shellを再度アクティブにするには、メーカーでデバイスを分解しなければなりません。**

以下が条件となります。
- Service Shellが開始されていない。
- モードがUser Exec modeであること。`(MCSESM-E) >`

以下の手順を実行します。
☐ `enable` を入力し、＜Enter＞キーを押します。
次の方法でタイピングの手間を省くことができます。
– `e` を入力し、＜Tab＞キーを押します。

☐ `serviceshell deactivate` を入力し、＜Enter＞キーを押します。
次の方法でタイピングの手間を省くことができます。
– `ser` を入力し、＜Tab＞キーを押します。
– `dea` を入力し、＜Tab＞キーを押します。

☐ **これを行うと、元に戻すことはできません！**
＜Y＞キーを押します。

```
!MCSESM-E >enable

!*MCSESM-E #serviceshell deactivate
Notice:If you continue, then the Service Shell is permanently deactivated.
This step is irreversible!
For details, refer to the Configuration Manual.
Are you sure (Y/N) ?
```

1.3 システムモニター

システムモニターにより、オペレーティングシステムの開始前に基本のオペレーションパラメーターを設定することが可能です。

1.3.1 機能の範囲

システムモニターにより実行可能なタスクの一例を以下に示します。
- オペレーティングシステムの管理及びソフトウェアイメージの確認
- オペレーティングシステムのアップデート
- オペレーティングシステムの起動
- コンフィグレーションプロファイルの削除、デバイスを出荷設定へリセット
- ブートコードの情報の確認

1.3.2 システムモニターの開始

条件：
- デバイスをPCに接続する端子ケーブル（アクセサリーとして入手可能）。
- VT100端末エミュレータ（PuTTY のような）又はシリアルターミナルのあるPC

以下の手順を実行します。

- ☐ デバイスのシリアルインターフェースとPCのCOMポートを、端子ケーブルで接続します。
- ☐ PCの端末エミュレータを起動します。
- ☐ 以下の伝送パラメーターを指定します。

VT100端末設定	
速度	9600 bit/s
データ長	8 bit
ストップビット	1 bit
ハンドシェイク	off
パリティ	無し

- ☐ デバイスを接続します。
- ☐ デバイスをONにします。デバイスが既にONであれば、リブートします。
  リブート後、以下のメッセージが画面に表示されます。
  `System Monitor 1を入力するには<1>キーを押します。`
- ☐ <1>キーを3秒以内に押します。
  デバイスがシステムモニターを起動します。以下の画面が表示されます。

```
System Monitor 1
(Selected OS: ...-8.7 (2021-06-22 09:28))

1  Manage operating system
2  Update operating system
3  Start selected operating system
4  Manage configurations
5  Show boot code information
q  End (reset and reboot)




sysMon1>
```

図12　System Monitor 1 画面表示

- ☐ 数字を入力してメニュー項目を選択します。
- ☐ サブメニューから離れてSystem Monitor 1 のメインメニューに戻るには、<ESC>キーを押します。

2 IPパラメーターの指定

当デバイスを初期インストールする際、IPパラメーターを入力します。

デバイスの初期インストール時にIPパラメーターを入力する時には、以下の選択肢があります。

- コマンドラインインターフェースを使用した入力。
  デバイスの作動環境外でプリコンフィグレーションを行う場合、或いはネットワークアクセス（インバンド）を復旧する場合、この「アウトバンド」法を使用します。
- Ethernet Switch Configuratorプロトコルを使用した入力。
  既にインストール済みのネットワークデバイスがあるか、PCとデバイス間が別のイーサネットで接続されている場合は、この「インバンド」法を使用します。
- 外部メモリを使用したコンフィグレーション。
  デバイスを同種のデバイスと交換する際にコンフィグレーションを外部メモリに保存済みであれば、この方法を使用します。
- BOOTPの使用。
  インストールしたデバイスをBOOTPで設定する場合、この「インバンド」法を使用します。この方法ではBOOTPサーバーが必要となります。BOOTPサーバーは、デバイスのMACアドレスを使用してコンフィグレーションデータを割り当てます。なお、DHCP modeは参照コンフィグレーションデータのデフォルトモードです。
- DHCPを使用したコンフィグレーション。
  インストールしたデバイスをDHCPで設定する場合、この「インバンド」法を使用します。この方法ではDHCPサーバーが必要となります。BOOTPサーバーは、デバイスのMACアドレス又はシステム名を使用してコンフィグレーションデータを割り当てます。
- グラフィカルユーザーインターフェースを使用したコンフィグレーション。
  デバイスにIPアドレスが既にあり、ネットワークを利用してアクセスできる場合、グラフィカルユーザーインターフェースはIPパラメーターを設定する上でその他のオプションを提示します。

2.1 IPパラメーターの基本

2.1.1 IPv4

IPアドレス

IPアドレスは4バイトで構成されています。これら4バイトを、小数点で区分けした10進数で入力します。

1992年に決定したRFC1340では、IPアドレスで5つのクラスがあります。

表8　IPアドレスのクラス

クラス	ネットワークアド	ホストアドレス	アドレスの範囲
A	1 Byte	3 Bytes	0.0.0.0 から 127.255.255.255 まで
B	2 Bytes	2 Bytes	128.0.0.0 から 191.255.255.255 まで
C	3 Bytes	1 Byte	192.0.0.0 から 223.255.255.255 まで
D			224.0.0.0 から 239.255.255.255 まで
E			240.0.0.0 から 255.255.255.255 まで

IPアドレスの最初のバイトは、ネットワークアドレスになっています。全世界のネットワークは、IANA（Internet Assigned Numbers Authority：インターネット番号割当機関）と呼ばれる規制機関で割当てられています。IPアドレスブロックが必要であれば、ご利用のISP（インターネットサービスプロバイダー）にご連絡してください。そのISPに、現地で上位の組織からIPアドレスブロックを予約してもらいます。

- APNIC (Asia Pacific Network Information Center)
  アジア太平洋地域
- ARIN (American Registry for Internet Numbers)
  メキシコ除く北米及びサブサハラアフリカ
- LACNIC (Regional Latin-American and Caribbean IP Address Registry)
  ラテンアメリカ及び一部カリブ諸島
- RIPE NCC (Réseaux IP Européens)
  ヨーロッパ及び周辺地域

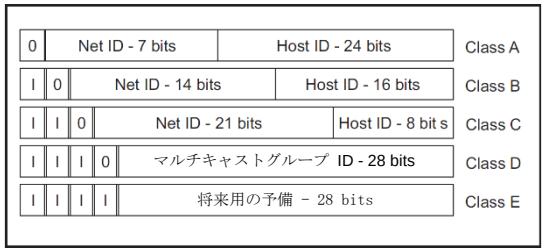


図13 IPアドレスのビット数

IPアドレスの最初のビットが0で、例えばそれがClass Aである場合は、最初のオクテットは128より小さくなります。

IPアドレスの最初のビットが1、そして2番目のビットが0で、例えばそれがClass Bある場合は、最初のオクテットは128から191の間となります。

IPアドレスの最初と2番目のビットが1で、例えばそれがClass Cある場合は、最初のオクテットは191より大きくなります。

ホストアドレス（host ID）の割当ては、ネットワークオペレーターの責任となります。ネットワークオペレーターが唯一、割当てたIPアドレスの固有性の責任を負います。

ネットマスク

ルーターやゲートウェイは、大きなネットワークをサブネットワークへと細分化します。ネットマスクは各デバイスのIPアドレスを特定のサブネットワークへ割当てます。

ネットマスクを使用したサブネットワークの分割は、ネットワークアドレス（net id）のクラスをA～Cに分割するのと同じような方法で行います。

ホストアドレス（host id）のビットを、サブネットマスクを1になるよう設定します。残りのホストアドレスのビットを0（以下例を参照）に設定します。

サブネットマスク例：

10進数
255.255.192.0

2進数
11111111.11111111.11000000.00000000
サブネットワークマスク・ビット
Class B

サブネットマスクを、サブネットワーク割当てのためIPアドレスに適用する例を以下に示します。

10進数
129.218.65.17
└──── 128 < 129 191 › Class B

2進数
10000001.11011010.01000001.00010001
サブネットワーク1
ネットワークアドレス

10進数
129.218.129.17
└──── 128 < 129 191 › Class B

2進数
10000001.11011010.10000001.00010001
サブネットワーク2
ネットワークアドレス

ネットマスクの使用例

大きなネットワークｋでは、ゲートウェイ及びルーターが管理エージェントをネットワーク管理ステーションから分けることがあります。このような場合、どのようにアドレス指定を行うのでしょうか。

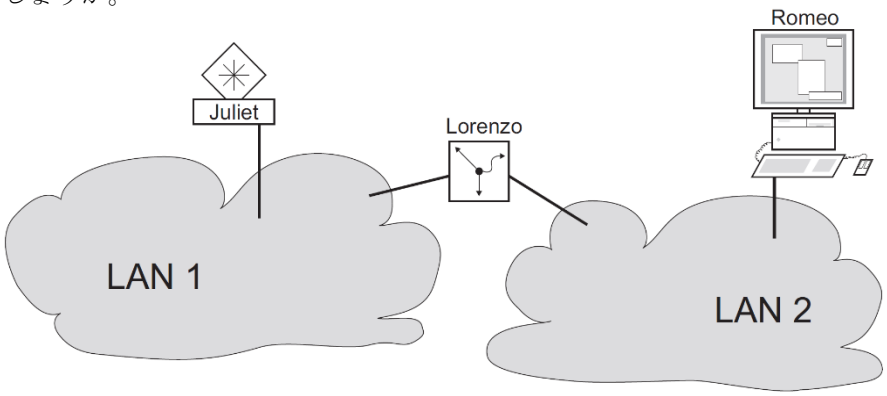


図14　管理エージェントはルーターによってネットワーク管理ステーションから分けられる

ネットワーク管理ステーション「Romeo」が、管理エージェント「Juliet」にデータを送りたい、とします。RomeoはJulietのIPアドレスを知っていると同時に、ルーター「Lorenzo」はJulietへの道順を知っています。

従って、Romeoは自身のメッセージを封筒に入れ、宛先にJulietのIPアドレスを記入し、封筒の差出人アドレスには自分のIPアドレスを記入します。

ここでRomeoは二つ目の封筒にLorenzoのMACアドレスを宛先、自分のMACアドレスを差出人として記入し、前述の封筒をそれに入れます。このプロセスは、ISO/OSI基本参照モデルのレイヤー3から2へ移行するのと同等です。

レイヤー2から1への移行と同じように、最終的にRomeoはデータパケットの全てを郵便ポストに投函しました。即ち、イーサネット上でデータパケットを送ったことを意味します。

Lorenzoは手紙を受け取ると外封筒を開封し、内封筒を見てそれがJuliet宛てだと理解します。彼は内封筒を新たな外封筒に入れ、アドレス帳（ARPテーブル）でJulietのMACアドレスを検索し、そのMACアドレスを宛先として外封筒の宛先に記入し、自分のMACアドレスを差出人として記入します。そして、データパケット全てを郵便ポストに投函します。

Julietは手紙を受け取り、外封筒を開封します。そこで、RomeoのIPアドレスの書かれた内封筒を見つけます。内封筒を開封してその手紙を読むことは、即ちISO/OSIレイヤーモデルの上位プロトコルレイヤーにメッセージを転送することに相当します。

今度は、JulietはRomeoに返信したいと考えています。彼女は封筒にRomeoのIPアドレスを宛先に記入し、自分のIPアドレスを差出人に記入します。それでは、彼女はどこに返信を送るのでしょうか。というのも、彼女はRomeoのMACアドレスは受け取っていません。Lorenzoが外封筒を入れ替えてしまったため、失われてしまいました。

JulietのMIBでは、LorenzoはRomeoと通信する手段としての可変`NetGatewayIPAddr` としてリスティングされています。従って、彼女はそれぞれのIPアドレスが記入された封筒を、LorenzoのMACアドレスを宛先とした別の封筒に納めます。

これにより、最初にRomeoからJulietに手紙が渡ったのと同じ方法で、今度は手紙がLorenzoを通してRomeoまで届けられます。

クラスレス・インタードメインルーティング

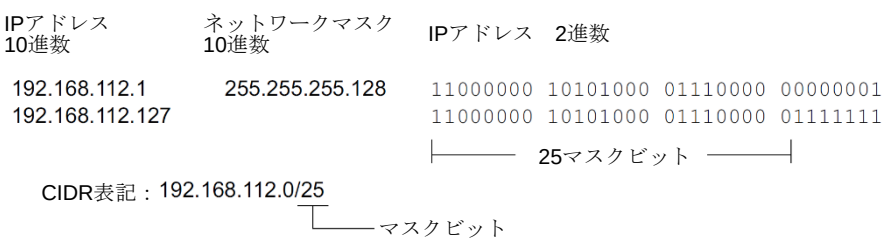
殆どのユーザーにとって、最大254個のアドレスのClass Cは少なすぎますし、最大65534個のアドレスのClass Bは多すぎます。結果として、Class Bで可用なアドレスを非効率的に使用することとなります。

Class Dには、予備のマルチキャストアドレスがあります。Class Eは実験的な目的です。参加していないゲートウェイは、これらの宛先アドレスが含まれる実験的なデータグラムを無視します。

1993年以降にRFC1519で使用されているクラスレス・インタードメインルーティング（CIDR）が解決策をもたらしました。CIDRはクラスによる境界をなくし、クラスレスでアドレスを一定範囲でサポートするようになっています。

CIDRを使用する場合、ＩＰアドレスの範囲を決定するビット数を入力します。IPアドレスの範囲を2進数形式で表記すれば、ネットマスクを決定するマスクビットがカウントされます。マスクビットにより、サブネットで使用されたビット数を任意のIPアドレス範囲に均等に振り分けられます。

例：



「スーパーネッティング」とは、一定範囲のClass C アドレスを組み合わせることを意味します。スーパーネッティングにより、一定範囲のClass B アドレスをかなり細かく分割することができます。

2.1.2 IPv6

IPパラメーターの基本

IPv6（Internet Protocol version 6）とは、IPv4（Internet Protocol version 4）の新たなバージョンとなります。近年のインターネットの成長によりIPv4では不十分となってしまった背景により、必要に迫られIPv6が実現しました。IPv6 のプロトコルはRFC 8200に記載されています。

IPv6 と IPv4 の違いについて、例を示します。
- アドレス表記及び長さ
- ブロードキャストアドレスの種別がない
- ヘッダーの構造の簡略化
- 断片化は送信元ホストが実行
- ネットワーク内のパケットフロー識別能力の強化

IPv4 及び IPv6 のプロトコルはいずれもデバイス内で同時に作動します。これはデュアルスタック（又はデュアルIPレイヤーテクニック）と呼ばれる技術により可能となっています。

注記：デバイスでIPv4の機能のみを使用したい場合、デバイスのIPv6機能は無効化します。

デバイス内では、IPv6の機能には以下の制限があります。
- IPv6のユニキャストアドレスを最大8個まで、以下の方法で指定できます。
  - マニュアルコンフィグレーションにてIPv6アドレス4個
  - *Auto* ラジオボタン選択状態でIPv6アドレス2個
  - DHCPv6サーバーを使用してIPv6アドレス1個
  - リンクローカルアドレス1個
- IPv6 の機能は、管理インターフェースのみから有効化することができます。構成可能なIPv6アドレスの総数は、インターフェース上で同時に使用することができます。
- IPv6アドレスは、デバイスの管理IPアドレスを設定するのに使用することも可能です。その他IPv6アドレスを使用できるサービスとして、SNTP、SYSLOG、DNS、LDAP等があります。

アドレス表記

IPv6アドレスは128ビット構成です。表記は16進数を4桁で8グループ、各グループがヘクステット（hextet）と呼ばれる16ビットで表記されます。ヘクステットはコロン記号（:）で分割されます。IPv6アドレスは大文字・小文字の区別はないため、大文字・小文字のどちらでも入力できます。

RFC 4291に従い、IPv6アドレスの表記フォーマットは x:x:x:x:x:x:x:x が好ましいとされます。各「x」は16進数4桁で構成されるヘクステットとします。Ipv6の理想的なフォーマットの例を下図に示します。

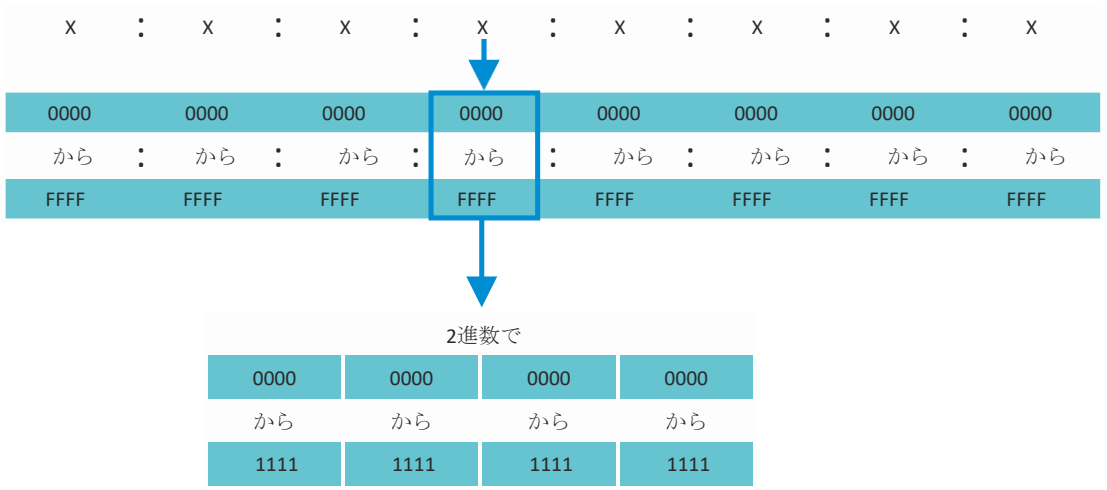


図15　IPv6アドレスの表記

通常、上の図に示すように、IPv6アドレスには多くの 0 が含まれます。0ビットを含むIPv6アドレスを短くするには、2つの入力ルールに従います。

- 第1のルールとして、ヘクステット全てから頭の 0 を除くことです。但しこのルールは頭の 0 に関してであって、ヘクステットの末尾の 0 には適用されません。末尾の 0 を抜くと、出来上がったアドレスが曖昧になってしまいます。
- 第2のルールでは、0 を圧縮するために特殊なシンタックスを使用します。連続したヘクステットで 0 のみで構成されるストリングを入れ替えるのに、連続2つのコロン記号「::」を使用することができます。この記号「::」は1つのアドレスで一度しか使えません。もしも「::」記号を1つのアドレスで複数回使うと、この表記から導かれるアドレスが複数に増える可能性があります。

これら2つのルールを適用したものを、一般的には圧縮フォーマットとしています。以下に2つのルールを適用したアドレスの例を示します。

表9　IPv6アドレスの圧縮

理想	CC03:0000:0000:0000:0001:AB30:0400:FF02
頭の0 抜き	CC03: 0: 0: 0: 1:AB30:400:FF02
圧縮	CC03::1:AB30:400:FF02
理想	2008:00B7:0000:DEF0:DDDD:0000:E604:0001
頭の0 抜き	2008: B7: 0:DEF0:DDDD: 0:E604: 1
圧縮	2008:B7::DEF0:DDDD:0:E604:1

プレフィックス長

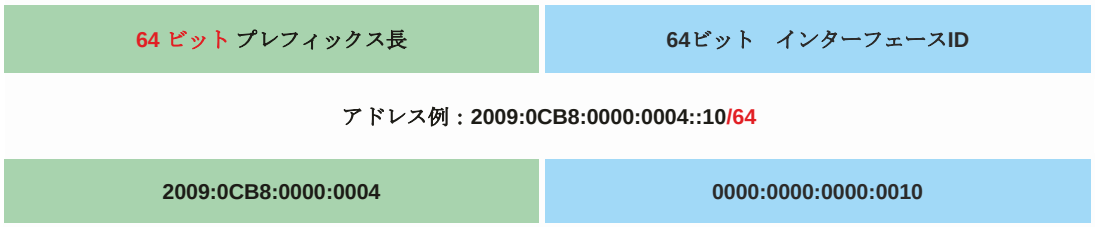
Ipv4アドレスとは違い、IPv6アドレスはサブネットマスクを使用してアドレスがネットワーク構成部を検知することはありません。IPv6のプロトコルは、サブネットマスクの代わりにプレフィックス長を使用します。

IPv6アドレスのプレフィックス表記は、CIDR（クラスレス・インタードメインルーティング）でのIPv4アドレスのプレフィックス表記に類似しています。

```
<ipv6-address>/<prefix-length>
```

プレフィックス長の幅は`0..128`となります。LANや他種ネットワークの典型的なIPv6プレフィックス長は /64となります。つまり、アドレスのネットワーク構成部の長さは64ビットあることになります。残りの64ビット分は、IPv4アドレスのホスト構成部と同様に、インターフェースIDを表します。

プレフィックス長のビット割当ての例を下図に示します。



アドレスの種別

IPv6アドレスの種別はRFC 4291に記載されています。

下表に示す通り、IPv6アドレスの種別は、アドレスの上位ビットから認識されています。

表10　IPv6アドレス種別

アドレスの種別	2進数プレフィックス	IPv6表記
未指定	00...0 (128 bits)	::/128
ループバック	00...1 (128 bits)	::1/128
マルチキャスト	11111111	FF00::/8
リンクローカルユニキャスト	1111111010	FE80::/10
グローバルユニキャスト	（その他全て）	

未指定アドレス

全ビットが 0 となっているIPv6アドレスは未指定アドレス（Unspecified address）と呼ばれ、IPv4アドレスでは0.0.0.0に相当します。
未指定アドレスは、アドレスが無いことを表示する目的で使用します。一般的に、固有のアドレスがまだ決定していない時に送信元アドレスとして使用されます。

注記：未指定アドレスは、インターフェースへ割当てることはできず、宛先アドレスとして使用することもできません。

ループバックアドレス

ユニキャストアドレス 0:0:0:0:0:0:0:1 は、ループバックアドレスと呼ばれます。デバイスが、IPv6パケットをデバイス自身に送ることができるアドレスです。なお、物理インターフェースにも割当てることはできません。

マルチキャストアドレス

IPv6には、IPv4のようにブロードキャストアドレスがありません。但し、原則的に同等の結果を得られる全ノードマルチキャストアドレスがIPv6にあります。

IPv6マルチキャストアドレスは、複数の宛先にIPv6パケットを送信するのに使用されます。マルチキャストアドレスの構造は次の通りです。後ろの4ビットはマルチキャストの範囲（どこまでパケットを送信するか）を決定します。

- 最初の8ビットは FFに設定されています。
- 次の4ビットは、アドレスの有効期間です。0 は恒久的で、1は一時的です。
- 次の4ビットはマルチキャストの範囲を指し、ネットワークを通してどこまでパケットを送信するかを決定します。

リンクローカルアドレス

リンクローカルアドレスは、同リンクにある他デバイスとの通信に使用します。ここでいう「リンク」とは、サブネットを意味します。ルーターは、リンクローカルにある送信元アドレスから他リンクにある宛先アドレスへとパケットを送信することはできません。

リンクローカルアドレスは、例えば自動アドレス設定、近隣探索、ルーターが無い場合などの範囲の単一リンクにパケットを送信するのに使用します。フォーマットは以下の通りです。

図11　リンクローカルアドレスのフォーマット

10 bits	54 bits	64 bits
1111111010	0	インターフェースID

リンクローカルアドレスは常時設定されていて、変更はできません。

グローバルユニキャストアドレス

グローバルユニキャストアドレスは全世界で固有のもので、インターネット上を経由するものです。この種のアドレスは、パブリックIPv4アドレスと同等と扱われます。現在、最初の3ビットが001 又は2000::/3 のものしか割当てられていません。

グローバルユニキャストアドレスは3部で構成されています。

- グローバルルーティングプレフィックス
- サブネットID
- インターフェースID

グローバルルーティングプレフィックスは、アドレスのネットワーク部にあたります。

サブネットIDは、そのサブネットを識別するために組織で使用され、ビット長は16ビットまであります。サブネットIDのビット長は、グローバルルーティングプレフィックスの長さにより決定します。

インターフェースIDは、特定ノードのインターフェースを識別します。インターフェースIDという用語の意図は、ホストが複数のインターフェースを持ち、それぞれが1つ又は複数のIPv6アドレスを持つことができるためです。

IPv6グローバルユニキャストアドレスの基本形式は、以下の図に示す通りです。

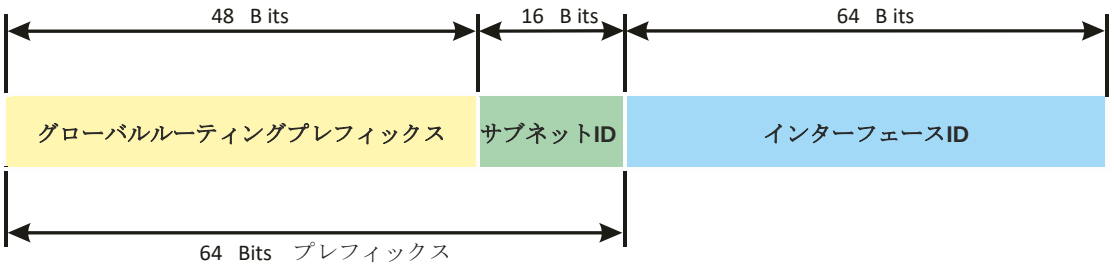


図16 IPv6グローバルユニキャストアドレスの基本形式

2.2 コマンドラインインターフェースを使用したIPパラメーターの指定

2.2.1 IPv4

IPパラメーターを入力するには、以下の方法があります。
- BOOTP/DHCP
- Ethernet Switch Configuratorプロトコル
- 外部メモリ
- シリアル接続を使用したコマンドラインインターフェース

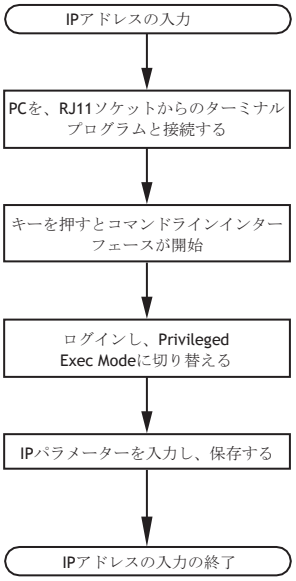
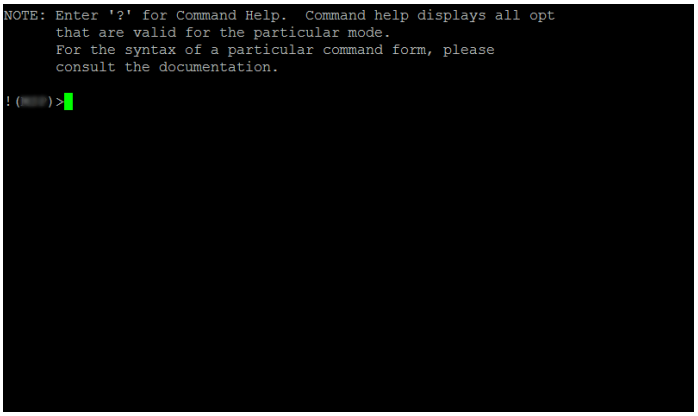


図17 IPアドレス入力のフローチャート

注記：インストールする場所の近辺に端末又は端末エミュレータに接続したPCがない場合、ユーザーのワークステーションでデバイス設定をし、最終的にインストールする場所へ移動することが可能です。

以下の手順を実行します。
☐ デバイスを接続します。
スタート画面が現れます。



☐ DHCPを無効化します。

☐ IPパラメーターを入力します。
- ➢ ローカルIPアドレス
  デフォルトのローカルIPアドレスは、0.0.0.0です。
- ➢ ネットマスク
  ネットワークをサブネットワークへと分割した際にこれらをネットマスク有りとして識別された場合、ここでネットマスクを入力します。デフォルトのネットマスクは、0.0.0.0です。
- ➢ ゲートウェイのIPアドレス
  デバイス及びネットワーク管理ステーション又はTFTPサーバーが異なるサブネットワークにある場合に限り、入力します（45ページの「ネットマスクの使用例」を参照）。
  デバイスのサブネットワーク及びネットワーク管理ステーションへのパス間のゲートウェイの、IPアドレスを指定します。
  デフォルトのIPアドレスは、0.0.0.0です。

☐ copy config running-config nvmで、指定したコンフィグレーションを保存します。

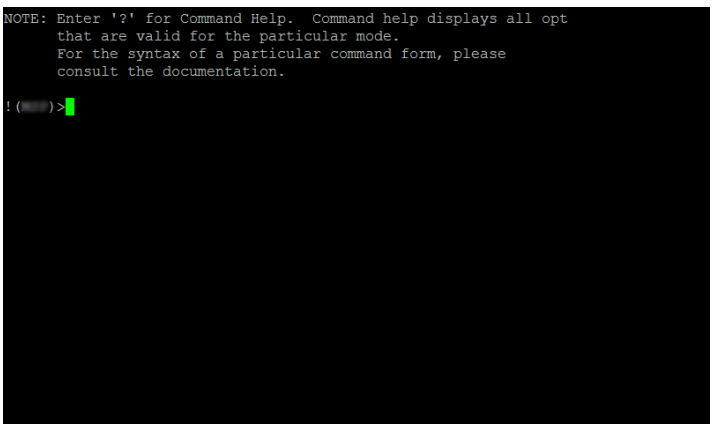
enable	Privileged Exec Modeに切り替えます。
network protocol none	DHCPを無効化します。
network parms 10.0.1.23 255.255.255.0	デバイスにIPアドレス 10.0.1.23 及びネットマスクに 255.255.255.0 を割当てます。また、ゲートウェイアドレスを割当てるという選択肢もあります。
copy config running-config nvm	不揮発性メモリ（nvm）にある現状の設定を「選択」したコンフィグレーションプロファイルに保存します。

IPパラメーターの入力後、グラフィカルユーザーインターフェースを使用してデバイスの設定が簡単に行えます。

2.2.2 IPv6

当デバ当デバイスではIPv6パラメーターを、シリアルインターフェース上のコマンドラインインターフェースを使用して指定することができます。その他の方法として、IPv4管理アドレスを使用したSSH接続を利用してコマンドラインインターフェースにアクセスすることでも可能です。

以下の手順を実行します。
☐ デバイスを接続します。スタート画面が現れます。



- ☐ プロトコルが無効な場合は、IPv6プロトコルを有効化します。
- ☐ IPv6パラメーターを入力します。
  - ➢ IPv6 アドレス
    有効なIPv6アドレス。IPv6アドレスは、圧縮形式で表示されます。
  - ➢ プレフィックス長
    Ipv4アドレスとは違い、IPv6アドレスはサブネットマスクを使用してアドレスがネットワーク構成部を識別することはありません。このタスクは、IPv6がプレフィックス長をもとに実行します(49ページの「プレフィックス長」 を参照)。
  - ➢ *EUI option* 機能
    EUI option 機能を使用することで、IPv6アドレスのインターフェースIDを自動的に構成することができます。当デバイスが自身のインターフェースのMACアドレスを使い、バイインターフェースの間に追加された `ff` 及び `fe` の値から、64ビットのインターフェースIDを作成します。
    このオプションは、`64`相当のプレフィックス長のあるIPv6アドレスのみに対して選択できます。
  - ➢ IPv6 ゲートウェイアドレス
    IPv6のゲートウェイアドレスは、デバイスがネットワーク外のネットワークにアクセスされているルーターのアドレスになります。
    IPv6のアドレスは、ループバック及びマルチキャストアドレス以外であれば指定できます。
    デフォルトのIPv6ゲートウェイアドレスは、`::`です。

`enable`	Privileged Exec Modeに切り替えます。
`network ipv6 operation`	プロトコルが無効な場合は、IPv6プロトコルを有効化します。デフォルトでは、IPv6プロトコルは有効です。
`network ipv6 address add 2001::1 64 eui-64`	IPv6アドレス `2001::1` 及びプレフィックス長`64`を指定します。`eui-64` パラメーターはオプションです。また、ゲートウェイアドレスを割当てるという選択肢もあります。
`copy config running-config nvm`	不揮発性メモリ（`nvm`）にある現状の設定を「選択」したコンフィグレーションプロファイルに保存します。

IPv6パラメーターの入力後、グラフィカルユーザーインターフェースを使用してデバイスの設定が簡単に行えます。URLにIPv6アドレスを使用するには、次のURL形式に従います。syntax: `https:// [<ipv6_address>]`

2.3 Ethernet Switch Configuratorを使用したIPパラメーターの指定

Ethernet Switch Configuratorプロトコルにより、イーサネットを使用してデバイスにIPパラメーターを指定することが可能です。

他のパラメーターは、グラフィカルユーザーインターフェースを使用して簡単に設定することができます。

PCにEthernet Switch Configuratorソフトウェアをインストールします。

以下の手順を実行します。
- ☐ Ethernet Switch Configuratorプログラムを開始します。

Ethernet Switch Configuratorが開始されると、Ethernet Switch Configuratorプログラムが自動でネットワーク上のEthernet Switch Configuratorプロトコルをサポートするデバイスを検索します。

Ethernet Switch Configuratorプログラムは、最初に検知したPCのネットワークインターフェースを使用します。PCに複数のネットワークカードがある場合、Ethernet Switch Configuratorツールバーから任意のカードを選択することができます。

Ethernet Switch Configuratorプログラムは、Ethernet Switch Configuratorプロトコルの探索に応答した全てのデバイスをライン上に表示します。

Ethernet Switch Configuratorプログラムにより、表示したデバイスが識別可能となります。
- ☐ デバイスのラインを選択します。
- ☐ 選択したデバイスのLEDを点滅させるには、ツールバーの*Signal* ボタンをクリックします。点滅を停止するには、再度*Signal* ボタンをクリックします。
- ☐ ラインをダブルクリックすると、デバイス名およびIPパラメーターを指定するウィンドウが開きます。

注記：デバイスにIPパラメーターを指定した後、デバイスのEthernet Switch Configurator機能を無効化します。

注記：入力データが再起動後も残るよう、設定を保存します。

2.4 グラフィカルユーザーインターフェースを使用したIPパラメーターの指定

2.4.1 IPv4

以下の手順を実行します。

☐ *Basic Settings > Network > Global* ダイアログボックスを開きます。

このダイアログでデバイス管理にアクセスし、Ethernet Switch Configuratorでの構成が可能なVLANを指定します。

☐ *VLAN ID* のカラムで、ネットワーク上でデバイス管理にアクセスできるVLANを指定します。

ここでは関連するVLANを構成するポートを使用したデバイス管理のみアクセス可能であることにご留意ください。

MAC address フィールドは、ネットワーク上でデバイスにアクセスするデバイスのMACアドレスが表示されます。

☐ *Ethernet Switch Configurator protocol v1/v2* のフレームでは、Ethernet Switch Configuratorソフトウェアを使用したデバイスにアクセスするための設定を指定します。

☐ Ethernet Switch Configuratorプロトコルにより、デバイスのMACアドレスをもとにしたIPアドレスを割当てることができます。PCのEthernet Switch Configuratorソフトウェアを使用してデバイスにIPアドレスを割当てたい場合、Ethernet Switch Configuratorプロトコルのアクティベーションを行います。

☐ *Basic Settings > Network > IPv4* ダイアログボックスを開きます。

このダイアログで、起動後にデバイスがIPパラメーターを取得するソースを指定します。

☐ *Management interface* フレームで、下記いずれかの、デバイスのIPパラメーター取得先を最初に指定します。

➢ *BOOTP* モードでは、デバイスのMACアドレスをもとにしたBOOTP又はDHCPサーバーをコンフィグレーションに使用します。

➢ *DHCP* モードでは、デバイスのMACアドレス又はデバイス名をもとにしたDHCPサーバーをコンフィグレーションに使用します。

➢ *Local* モードでは、デバイスは内部デバイスメモリから得たネットワークパラメーターを使用します。

注記：IPアドレスの割当てモードを変更する場合、☑ ボタンをクリックすると、デバイスは直ちに新規モードのアクティベーションを行います。

☐ 必要な場合、IPアドレス、ネットマスク、ゲートウェイを*IP parameter*のフレームに入力してください。

☐ ☑ ボタンをクリックし、変更を一時的に保存します。

2.4.2 IPv6

以下の手順を実行します。

- ☐ *Basic Settings > Network > IPv6* ダイアログボックスを開きます。
- ☐ デフォルトでは、IPv6プロトコルは有効です。*Operation* フレームで、*On* のラジオボタンが選択されていることを確認します。
- ☐ *Configuration* フレームで、下記いずれかの、デバイスのIPv6パラメーター取得先を指定します。
  - ➢ *None* ラジオボタンが選択されている場合、デバイスはIPv6パラメーターをマニュアルで取得します。最大4つのIPv6アドレスを手動で指定することができます。ループバック、リンクローカル、マルチキャストのアドレスを静的IPv6アドレスとして指定することはできません。
  - ➢ *Auto* ラジオボタンが選択されている場合、デバイスは、例えばradvd（Router Advertisement Daemon：ルーター告知デーモン）などを使用して動的にIPv6パラメーターを取得します。デバイスは、最大2つのIPv6アドレスを取得します。
  - ➢ *DHCPv6* ラジオボタンが選択されている場合、デバイスはIPv6パラメーターをDHCPv6サーバーより取得します。
    デバイスは、DHCPv6サーバーから1つのIPv6アドレスしか取得することはできません。
  - ➢ *All* ラジオボタンが選択されている場合、デバイスはIPv6パラメーターを、動的及びマニュアルの割当てに代わる全ての方法で取得します。

注記：IPv6アドレスの割当てモードを変更する場合、☑ ボタンをクリックすると、デバイスは直ちに新規モードのアクティベーションを行います。

- ☐ 必要な場合、*IP parameter*のフレームに*Gateway address* を入力してください。

注記：▶ *Auto* ラジオボタンが選択されている時にradvd（Router Advertisement Daemon：ルーター告知デーモン）を使用すると、デバイスは手動で設定した*Gateway address* よりも高いメトリックのリンクローカル*Gateway address* を自動取得します。

- ☐ *Duplicate Address Detection* フレームでは、デバイスが*Duplicate Address Detection* 機能に送信した連続する*Neighbor Solicitation*メッセージ数を指定できます（63ページの「重複アドレス検出」をご参照ください。
- ☑ ボタンをクリックし、変更を一時的に保存します。

IPv6アドレスを手動で指定します。以下の手順を実行します。

- ☐ *Basic Settings > Network > IPv6* ダイアログボックスを開きます。
- ☐ ⊞ ボタンをクリックします。
  ダイアログが*Create* ウィンドウを表示します。
- ☐ *IP address* フィールドに、IPv6アドレスを入力します。
- ☐ *PrefixLength* フィールドに、IPv6アドレスのプレフィックス長を入力します。
- ☐ *Ok* ボタンをクリックします。
  デバイスは、新規のテーブルエントリーを追加します。

2.5 BOOTPを使用したIPパラメーターの指定

BOOTP 機能がアクティベートされていれば、デバイスはBOOTPサーバーにブートリクエストメッセージを送信します。ブートリクエストメッセージには、*Basic Settings > Network > IPv4* ダイアログボックスで設定されたクライアントIDが含まれています。BOOTPサーバーはクライアントIDをデータベースに書込み、IPアドレスを割当てます。サーバーはブートリプライメッセージにより応答します。ブートリプライメッセージには指定されたIPアドレスが含まれています。

2.6 DHCPを使用したIPパラメーターの指定

2.6.1 IPv4

DHCP（Dynamic Host Configuration Protocol）はBOOTPから更に開発したものであり、現在では置換えられています。DHCPは更に、MACアドレスを使用する代わりにDHCPクライアントの名前を使ってコンフィグレーションを行います。

DHCPでは、この名前をRFC 2131に従い「クライアント識別子（Client Identifier）」とされています。

当デバイスは、MIB IIのシステムグループ内のsysNameで入力された名前をクライアント識別子として使用します。グラフィカルユーザーインターフェース（*Basic Settings > System*参照）、コマンドラインインターフェース、SNMPのいずれからもシステム名を変更できます。

デバイスは、自身のシステム名をDHCPサーバーに送信します。次に、DHCPサーバーはMACアドレスの代替として、システム名を使ってIPアドレスを割当てます。

また、DHCPサーバーはIPアドレスの他、以下も送信します。

- ネットマスク
- デフォルトゲートウェイ（該当する場合）
- コンフィグレーションファイルのTFTP URL（該当する場合）

デバイスはコンフィグレーションデータを適切なパラメーターに適用します。DHCPサーバーがIPアドレスを割合てた時、当デバイスはコンフィグレーションデータを不揮発性メモリに恒久的に保存します。

表12　デバイスが要求するDHCPオプション

オプション	意味
1	サブネットマスク
2	タイムオフセット
3	ルーター
4	タイムサーバー
12	ホスト名
42	NTPサーバー
61	クライアント識別子
66	TFTPサーバー名
67	ブートファイル名

BOOTPの代わりにDHCPを使用する利点は、DHCPサーバーはコンフィグレーションパラメーターの有効性を一定時間、制限できる（「リース」）ためです（dynamic address allocation：動的アドレスの割当てと呼ばれる）。この期間（「リース期間」）が経過する前に、DHCPクライアントはこのリースを更新しようとします。他には、クライアントから新規のリースを交渉することもできます。すると、DHCPサーバーは無作為の未使用アドレスを割当てます。

これを防ぐため、DHCPサーバーはハードウェアの固有IDをもとにしたIPアドレスと同じアドレスを特定のクライアントに指定するという、明白なコンフィグレーションオプションを提供しています（static address allocation：静的アドレスの割当てと呼ばれる）。

デフォルトでは、DHCPは有効です。DHCPが有効であれば、デバイスはIPアドレスの取得を試みてくれます。再起動後にもデバイスがDHCPサーバーを見つけることができなければ、IPアドレスが無いことになります。*Basic Settings > Network > IPv4* のダイアログボックスで、DHCPのアクティベーション及びディアクティベーションを行えます。

注記：ネットワーク管理ソフトウェア ConneXium Network Manager を使用の際、DHCPが全てのデバイスに固有のIPアドレスを割当てます。

本書付録にBOOTP/DHCPサーバー設定の参考例が記載されています。

DHCPコンフィグレーションファイルの例：

```
# /etc/dhcpd.conf for DHCP Daemon
#
subnet 10.1.112.0 netmask 255.255.240.0 {
option subnet-mask 255.255.240.0;
option routers 10.1.112.96;
}
#
# Host berta requests IP configuration
# with her MAC address
#
host berta {
hardware ethernet 00:80:63:08:65:42;
fixed-address 10.1.112.82;
}
#
# Host hugo requests IP configuration
# with his client identifier.
#
host hugo {
#
option dhcp-client-identifier "hugo";
option dhcp-client-identifier 00:68:75:67:6f;
fixed-address 10.1.112.83;
server-name "10.1.112.11";
filename "/agent/config.dat";
}
```

先頭に# 記号のある行は、コメントが含まれます。

リストされた各デバイスより前にある行は、そのデバイスに適用される設定となります。

fixed-addressと書かれた行は、デバイスの恒久的IPアドレスを指定します。

詳細については、DHCPサーバーマニュアルをご参照ください。

2.6.2 IPv6

DHCPv6（Dynamic Host Configuration Protocol version 6）とはネットワークプロトコルで、IPv6アドレスを動的に指定します。このプロトコルは、IPv4用DHCPプロトコルに相当するIPv6となります。DHCP IPv6プロトコルはRFC 8415に記載されています。

当デバイスは固有の識別子「DUID」 (DHCP Unique Identifier：ユニークアイデンティファイア)を使用してDHCPv6 サーバーにリクエストを送信します。当デバイス内でDUIDとは、DHCPv6サーバーがIPv6アドレスをリクエストしたデバイスを識別するための*Client ID* に相当します。

Client ID は、*DHCP* フレーム内の*Basic Settings > Network > IPv6* ダイアログボックスに表示されています。

デバイスは、DHCPv6サーバーから*PrefixLength* が128のIPv6アドレス1つしか取得することができません。*Gateway address* 情報は提供されません。必要であれば、*Gateway address* 情報をマニュアルで指定します。

デフォルトでは、DHCPv6プロトコルは無効です。プロトコルのアクティベーション・ディアクティベーションは*Basic Settings > Network > IPv6* ダイアログボックスで行います。*Configuration* フレームの*DHCPv6* のラジオボタンが選択されていることを確認します。

プレフィックス長*PrefixLength* が128以外のIPv6アドレスを動的に取得する場合は、*Auto* ラジオボタンを選択します。ここでは、radvd（Router Advertisement Daemon：ルーター告知デーモン）の使用例を記載します。radvdは*Router Solicitation*（ルーター要請）及びRouter Advertisement（ルーター告知）メッセージを使用し、自動でIPv6アドレスを構成します。

デフォルトでは、*Auto* ラジオボタンが選択されています。この*Auto* ラジオボタンは、*Basic Settings > Network > IPv6* ダイアログボックスの*Configuration* フレーム内で選択・解除が可能です。

All ラジオボタンが選択されている場合、デバイスはIPv6パラメーターを、動的及びマニュアルの割当てに代わる全ての方法で取得します。

2.7 管理アドレス競合検出

デバイスに様々な異なる方法でIPアドレスを割当てます。この機能では、ブート後にネットワーク上のIPアドレスの競合をデバイスが検出し、作動中に同様の監視を定期的に行います。当機能については、RFC 5227に記載されています。

有効な場合、デバイスはSNMPトラップを送信し、競合のIPアドレスが検知されたことを知らせます。

この機能のデフォルト設定の一部は以下リストの通りです。

- *Operation*:`On`
- *Detection mode*: `active and passive`
- *Send periodic ARP probes*: `marked`
- *Detection delay [ms]*:`200`
- *Release delay [s]*:`15`
- *Address protections*:`3`
- *Protection interval [ms]*:`200`
- *Send trap*: `marked`

2.7.1 アクティブ及びパッシブ検出

ネットワークのアクティブな監視は、デバイスが重複したIPアドレスと接続してしまうことを防ぎます。デバイスをネットワークに接続した後やIPアドレスを構成した後、デバイスはネットワーク内に自身のIPアドレスが存在するか監視を行います。ネットワーク内でのアドレス競合の監視目的で、デバイスはARPプローブ4つを、200msの検出遅延でネットワークに送り込みます。IPアドレスが存在する場合、デバイスは以前のコンフィグレーションに戻ろうとし、設定後の解除遅延時間が経過したら再度監視を開始します。

アクティブ検出を無効にすると、デバイスから2秒間隔をおいてGARP（Gratuitous ARP）通知を2つ送信します。パッシブ検出が有効な時にARP通知を使用すると、デバイスはネットワークのポーリングを実行し、アドレス競合の有無を検出します。アドレス競合が解消された或いは解除遅延時間の経過後、デバイスはネットワークに再接続します。競合を10個検出し、設定後の解除遅延時間の間隔が60秒に満たない場合、デバイスは解除遅延時間の間隔を60秒に設定します。

デバイスがアクティブ検出を行うか、ユーザーがアクティブ検出機能を無効化すると、パッシブ検出が有効であればデバイスはネットワークのリスニングを行い、同IPアドレスのデバイスの有無を確認します。重複IPアドレスを検知した場合、最初にデバイスはパッシブ検出モード内のACD（アドレス競合検出）機能により自身のアドレスを保護し、GARPを送信します。デバイス保護で送信するGARP数及びその時間の間隔は、設定可能です。アドレス競合を解決する上で、リモートのデバイスをネットワークに接続したままにすると、ローカルデバイスのネットワークインターフェースをネットワークから切断されます。

DHCPサーバーがデバイスにIPアドレスを割当ててアドレス競合が発生した場合、DHCPからdecline message（拒否メッセージ）が送られます。

当デバイスはARPプローブを使用します。この方式には以下の利点があります。

- ➢ 他デバイスのARPキャッシュが変更されない
- ➢ この方式は、複数のARPプローブ伝送でも安定する

2.8 重複アドレス検出

Duplicate Address Detection （重複アドレス検出）機能は、インターフェース上のIPv6ユニキャストアドレスの固有性を判断します。IPv6アドレスをマニュアル、*DHCPv6*、*Auto* で設定した場合に上記機能が実行されます。また、下から上へとリンクステータスを変更した場合などの、リンクステータス変更がトリガーとなります。

Duplicate Address Detection （重複アドレス検出）機能は、*Neighbor Solicitation* （近隣要請）及び*Neighbor Advertisement* （近隣告知）メッセージを使用します。ユーザーは、デバイスが連続で送信する複数の*近隣要請*メッセージを設定できます。以下の手順を実行します。

- ☐ *Basic Settings > Network > IPv6* ダイアログボックスを開きます。
- ☐ *Duplicate Address Detection* フレームの*Number of neighbor solicitants* フィールドに必要な値を設定します。
  数値候補：
  - `0`
    この機能を無効化します。
  - `1..5` (デフォルト： `1`)
- ☐ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`network ipv6 dad-transmits <0..5>`	デバイスから送信する *Neighbor Solicitation* メッセージ数を設定します。 数値を`0` にすると機能が無効化されます。

注記：*Duplicate Address Detection* がリンク上のIPv6アドレスが固有でないと検知した場合、デバイスはこのイベントをlogファイル（System Log）に記録しません。

3 デバイスへのアクセス

3.1 アクセスロール

ユーザーとして使用できる当デバイスの機能は、アクセスロールにより異なります。特定のアクセスロールとしてログインしている場合は、当該アクセスロールの機能が使用できます。

ユーザーとして使用可能なコマンドは、現在操作しているコマンドラインインターフェースのモードによっても異なります。25ページの「モードに基づく コマンド階層」をご参照ください。

当デバイスには以下のアクセスロールがあります。

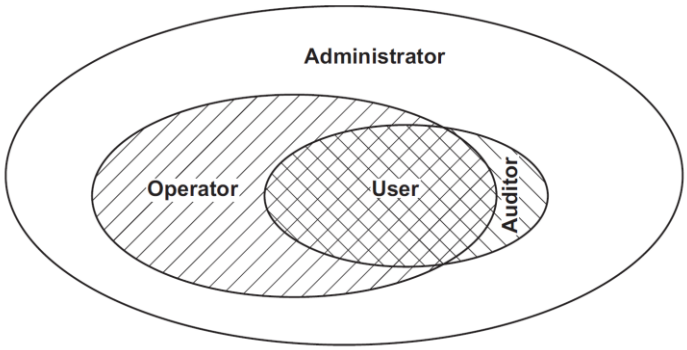


表 13　アクセスロール及びユーザーの権限範囲

アクセスロール	ユーザーの権限
User	アクセスロールが User としてログインしたユーザーは、デバイスの監視が許可されます。
Auditor	アクセスロールが Auditorとしてログインしたユーザーは、デバイスの監視の他、*Diagnostics > Report > Audit Trail* ダイアログボックスにログファイルを保存することが許可されます。
Operator	アクセスロールが Operator としてログインしたユーザーは、デバイスの監視の他、設定の変更が許可されますが、デバイスアクセスに関わるセキュリティ設定はこの限りではありません。
Administrator	アクセスロールが Administrator としてログインしたユーザーは、デバイスの監視の他、設定の変更が許可されます。
Unauthorized	Unauthorized （無許可）ユーザーはブロックされ、デバイスからログインを拒否されます。ユーザーアカウントを一時的にロックするには、この値を使用します。アクセスロールの変更中にエラーが発生すると、デバイスはこのアクセスロールをユーザーアカウントに割当てます。

3.2 初期ログイン（パスワードの変更）

デバイスへの不正なアクセスを防ぐには、初期セットアップ時にデフォルトパスワードを変更することが不可欠です。

以下の手順を実行します。

- ☐ 初期ログイン時、グラフィカルユーザーインターフェース、SE View application、コマンドラインインターフェースのいずれかを開きます。
- ☐ デフォルトのパスワードでログインします。
  デバイスは、新規のパスワードを入力するよう促します。
- ☐ 新規のパスワードを入力します。
  安全性を向上させるために、大文字、小文字、数字、特殊文字を含む少なくとも8文字のパスワードを作成します。
- ☐ コマンドラインインターフェースでログインの際は、新規のパスワードを確認するようデバイスが促します。
- ☐ 新規パスワードで再度ログインします。

注記：パスワードを忘れてしまった場合は、現地サポートまでご連絡をしてください。

3.3 認証リスト

ユーザーが特定の接続からデバイスにアクセスする場合、デバイスはログインするユーザーの認証情報を、デバイスが認証に適用した方針が含まれる認証リストから確認を行います。

デバイス管理へのユーザーのアクセス条件は、アクセスを行うアプリケーションの認証リストに、少なくとも1つの方針が割当てられていることです。

3.3.1 アプリケーション

当デバイスは、誰かがデバイスにアクセスする際の各種接続方法に関わるアプリケーションを提供することができます。

- シリアル接続によるコマンドラインインターフェースへのアクセス`Console(V.24)`
- SSHによるコマンドラインインターフェースへのアクセス`SSH`
- Telnetによるコマンドラインインターフェースへのアクセス`Telnet`
- グラフィカルユーザーインターフェースへのアクセス`WebInterface`

また、デバイスはポートベースのネットワークアクセスコントロールを使用したエンドデバイスからネットワークアクセスを管理するためのアプリケーションも提供しています。`8021x`

3.3.2 方針

ユーザーが有効なログインデータでログインする場合、デバイスはユーザーのデバイス管理へのアクセスを許可します。当デバイスは、以下の方針に従いユーザーを認証します。

- デバイスのユーザー管理
- LDAP
- RADIUS

エンドデバイスから有効なログインデータでログインする場合、IEEE 802.1Xの規定に従い、当デバイスは接続されたエンドデバイスがポートベースのネットワークアクセスコントロールでアクセスすることを許可します。当デバイスは、以下の方針に従いエンドデバイスを認証します。

- RADIUS
- IAS (Integrated Authentication Server)

当デバイスは、フォールバックソリューションのオプションを備えています。これにより、ユーザーは複数の方針を認証リストから指定することができます。現在ある方針で認証に失敗した場合、デバイスは次点に指定した方針を適用します。

3.3.3 認証リストの管理

グラフィカルユーザーインターフェース又はコマンドラインインターフェース内の認証リストを管理します。以下の手順を実行します。

☐ *Device Security > Authentication List* ダイアログボックスを開きます。
設定された認証リストをダイアログボックスが表示します。

`show authlists`	設定された認証リストを表示します。

☐ 例えば`8021x`などの、デバイスへのアクセス方法がないアプリケーションの認証リストを無効化します。

☐ 認証リストの*Active* カラムの`defaultDot1x8021AuthList`から、チェックボックスのチェックを外します。

☐ ボタンをクリックし、変更を一時的に保存します。

`authlists disable defaultDot1x8021AuthList`	認証リストを無効化します。`defaultDot1x8021AuthList`.

3.3.4 設定の調整

例：`WebInterface` アプリケーションにはデフォルトに含まれる認証リスト`defaultLoginAuthList`とは別途の認証リストを設定します。

デバイスは、ネットワーク上のRADIUSサーバーに対して認証リクエストを転送します。フォールバックソリューションとして、デバイスはローカルユーザー管理を使用しているユーザーを認証します。以下の手順を実行します。

☐ 認証リスト`loginGUI`を作成します。

☐ *Device Security > Authentication List* ダイアログボックスを開きます。

☐  ボタンをクリックします。
ダイアログが*Create* ウィンドウを表示します。

☐ *Name* フィールドに分かりやすい名前を入力します。
ここの例では、`loginGUI`を名前として入力します。

☐ *Ok* ボタンをクリックします。
デバイスは、新規のテーブルエントリーを追加します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`authlists add loginGUI`	認証リスト`loginGUI`が作成されます。

☐ 認証リスト`loginGUI`の方針を選択します。

☐ *Policy 1* カラムに、値*`radius`*を選択します。

☐ *Policy 2* カラムに、値*`local`*を選択します。

☐ *Policy 3* から *Policy 5* カラムまでは、値 *`reject`* を選択して更なるフォールバックを防止します。

☐ *Active* カラムのチェックボックスにチェックを入れます。

☐ ボタンをクリックし、変更を一時的に保存します。

`authlists set-policy loginGUI radius local reject reject reject`	`loginGUI`に、方針`radius`、`local` 、`reject` を割当てます。
`show authlists`	設定された認証リストを表示します。
`authlists enable loginGUI`	認証リスト`loginGUI`を有効化します。

☐ `loginGUI`にアプリケーションを設定します。

☐ *Device Security > Authentication List* ダイアログボックスにある認証リスト`loginGUI`にハイライトをつけます。

☐ ボタンに続き、 *Allocate applications* の項目をクリックします。ダイアログが*Allocate applications* ウィンドウを表示します。

☐ 左カラムのアプリケーション`WebInterface`にハイライトをつけます。

☐ ボタンをクリックします。
これで、右カラムにアプリケーション`WebInterface`が表示されます。

☐ *Ok* ボタンをクリックします。
ダイアログボックスに更新された設定が表示されます。
- 認証リスト`loginGUI` の*Dedicated applications* カラムには、アプリケーション`WebInterface`が表示されます。
- 認証リスト`defaultLoginAuthList` の*Dedicated applications* カラムは、アプリケーション`WebInterface`をこれ以降表示しなくなります。

☐ ボタンをクリックし、変更を一時的に保存します。

`show applists`	アプリケーション及び割当てられたリストを表示します。
`applists set-authlist WebInterface loginGUI`	アプリケーション`loginGUI` を、認証リスト`WebInterface`に割当てます。

3.4 ユーザー管理

ユーザーが有効なログインデータでログインする場合、デバイスはユーザーのデバイス管理へのアクセスを許可します。デバイスは、ローカルユーザー管理又はネットワーク上のRADIUSサーバーのいずれかを使用し、ユーザーを認証します。デバイスにユーザー管理を使用させるには、認証リストに`local` 方針を割当てます（*Device Security > Authentication List* ダイアログボックスを参照）。

ローカルユーザー管理内でユーザーアカウントを管理します。通常、一人のユーザーに対してアカウントは1つです。

3.4.1 アクセスロール

ユーザーはとりわけデバイス管理へのアクセスをコントロールしたい場合、ロールベースの認証モデルを使用することができます。特殊な認証プロファイルが割当られたユーザーは、下位の同じ認証プロファイルで使用できるコマンドや機能を使用することが認められます。

当デバイスは、デバイス管理でアクセス可能な全てのアプリケーションで認証プロファイルを使用します。

ユーザーアカウントは全て、デバイスの各機能へのアクセスを制限するアクセスロールとリンクされています。各ユーザーがどのような操作を予定しているかにより、事前定義したアクセスロールをユーザーに割当てます。デバイスは、以下のアクセスロールをそれぞれに区別しています。

表14　ユーザーアカウント用アクセスロール

ユーザーロール	解説	以下の操作を許可
Administrator	ユーザーはデバイスの監視及び管理が許可されます。	読込み・書込みアクセス、以下のAdministrator用の操作を含む全ての操作 ➢ ユーザーアカウントの追加、変更、削除 ➢ ユーザーアカウントのアクティベーション、ディアクティベーション、アンロック ➢ 全てのパスワードの変更 ➢ パスワード管理のコンフィグレーション ➢ システム時計の設定又は変更 ➢ デバイスへのファイルロード、例えばデバイスコンフィグレーション、証明書又はソフトウェアイメージ ➢ 設定やセキュリティ関連設定を初期設定へとリセット ➢ RADIUSサーバー及び認証リストの設定 ➢ コマンドラインインターフェースを使用したスクリプトの適用 ➢ CLIロギング及びSNMPロギングの有効化・無効化 ➢ 外部メモリのアクティベーション・ディアクティベーション ➢ システムモニターのアクティベーション・ディアクティベーション ➢ デバイス管理へのアクセスサービスの有効化・無効化（例：SNMP）。 ➢ IPアドレスをもとにしたグラフィカルユーザーインターフェース又はコマンドラインインターフェースのアクセス制限の設定
Operator	ユーザーはセキュリティ関連の設定を除く、デバイスの監視及び管理が許可されます。	アドミニストレーター専用の上記操作を除く、読込み・書込みアクセスを含む操作全て。
Auditor	ユーザーはデバイスの監視の他、*Diagnostics > Report > Audit Trail* ダイアログボックスにログファイルを保存することが許可されます。	読込みアクセスを含む監視操作
Guest	ユーザーはセキュリティ関連の設定を除く、デバイスの監視が許可されます。	読込みアクセスを含む監視操作
Unauthorized	デバイスへのアクセスはできません。 ➢ Administratorであれば、このアクセスロールを指定し、一時的にユーザーアカウントをロックします。 ➢ Administratorがユーザーアカウントに別のアクセスロールを指定するとエラーが発生し、デバイスはこのアクセスロールをユーザーアカウントに割当てます。	如何なる操作も不許可

3.4.2 ユーザーアカウントの管理

グラフィカルユーザーインターフェース又はコマンドラインインターフェース内のユーザーアカウントを管理します。以下の手順を実行します。

□ *Device Security > User Management* ダイアログボックスを開きます。
設定されたユーザーアカウントをダイアログボックスが表示します。

`show users` 設定されたユーザーアカウントを表示します。

3.4.3 デフォルト設定

初期設定では、ユーザーアカウント`admin` 及び`user` はデバイス内に設定済みです。

表15 ユーザーアカウントの出荷設定のデフォルト

パラメーター	デフォルト設定	
User name	`admin`	`user`
Password	`private`	`public`
Role	`administrator`	`guest`
User locked	`unmarked`	`unmarked`
Policy check	`unmarked`	`unmarked`
SNMP auth type	`hmacmd5`	`hmacmd5`
SNMP encryption type	`des`	`des`

デバイスをネットワーク内で有効にする前に、`admin` ユーザーアカウントのパスワードを変更してください。

3.4.4 デフォルトパスワードの変更

不正なアクセスを防止するために、デフォルトのユーザーアカウントのパスワードを変更します。以下の手順を実行します。
□ `admin` 及び `user` のユーザーアカウントのパスワードの変更手順

□ *Device Security > User Management* ダイアログボックスを開きます。
設定されたユーザーアカウントをダイアログボックスが表示します。
□ パスワードをより複雑なレベルにするには、*Policy check* カラムのチェックボックスにチェックを入れます。
保存する前に、デバイスは*Password policy* フレームに指定された方針を確認します。

注記：パスワード確認が実行されると、*Basic Settings > System* ダイアログボックスの *Security status* フレームにメッセージが表示されることがあります。このメッセージ表示を出すための設定は*Basic Settings > System* ダイアログボックスにあります。

☐ *Password* フィールド内の、対象のユーザーアカウントが表示された行をクリックします。
少なくとも6文字のパスワードを入力します。
最大で英数字64文字まで可能です。
- ➢ デバイスは大文字・小文字を区別します。
- ➢ パスワードの最小長は、*Configuration* フレームで指定されています。デバイスは、常時パスワードの最小長を確認しています。

☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`users password-policy-check <user> enable`	指定した方針でのユーザーアカウント`<user>` のパスワード確認のアクティベーションを行います。 この方法でパスワードをより複雑なレベルにすることができます。

注記：Security statusを表示すると、パスワード確認がでメッセージ「`show security-status all`」が表示されることがあります。このメッセージ表示を出すための指定コマンドは`security-status monitor pwd-policy-inactive`となります。

`users password <user> SECRET`	ユーザーアカウント`<user>`のパスワードを`SECRET` と指定します。 少なくとも6文字を入力します。
`save`	揮発性メモリ（`nvm`）にある設定を「選択」したコンフィグレーションプロファイルに保存します。

3.4.5 新規ユーザーアカウントの設定

デバイス管理にアクセスする各ユーザーに、個別のユーザーアカウントを割当てます。これによって、アクセスに関わる認証も個別に管理することができます。

以下の例では、`operator`ロールを担うユーザー名`USER` の、ユーザーアカウントを設定します。`operator` ロールのユーザーはセキュリティ関連の設定を除く、デバイスの監視及びコンフィグレーションが許可されます。以下の手順を実行します。

☐ 新規ユーザーアカウントを作成します。

☐ *Device Security > User Management* ダイアログボックスを開きます。

☐ ボタンをクリックします。
ダイアログが*Create* ウィンドウを表示します。

☐ *User name* フィールドに名前を入力します。
ここの例では、ユーザーアカウント名を`USER`とします。

☐ *Ok* ボタンをクリックします。

☐ パスワードをより複雑なレベルにするには、*Policy check* カラムのチェックボックスにチェックを入れます。
保存する前に、デバイスは*Password policy* フレームに指定された方針をもとにパスワードを確認します。

- ☐ *Password* フィールドに、少なくとも6文字のパスワードを入力します。最大で英数字64文字まで可能です。
  - ➢ デバイスは大文字・小文字を区別します。
  - ➢ パスワードの最小長は、*Configuration* フレームで指定されています。デバイスは、常時パスワードの最小長を確認しています。
- ☐ *Role* カラムの、ユーザーロールを選択します。
  ここの例では、operatorを選択します。
- ☐ このユーザーアカウントを有効にするには、*Active* カラムのチェックボックスにチェックを入れます。
- ☐ ✔ ボタンをクリックし、変更を一時的に保存します。 設定されたユーザーアカウントをダイアログボックスが表示します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`users add USER`	ユーザー名`USER` のアカウントを追加します。
`users password-policy-check USER enable`	指定した方針でのユーザーアカウント`USER` のパスワード確認のアクティベーションを行います。この方法でパスワードをより複雑なレベルにすることができます。
`users password USER SECRET`	ユーザーアカウント`USER` のパスワードをSECRETと指定します。少なくとも6文字を入力します。
`users access-role USER operator`	ユーザーアカウント`USER`にユーザーロール`operator` を割当てます。
`users enable USER`	ユーザーアカウント`USER`を有効にします。
`show users`	設定されたユーザーアカウントを表示します。
`save`	不揮発性メモリ（`nvm`）にある設定を「選択」したコンフィグレーションプロファイルに保存します。

注記：コマンドラインインターフェースに新規ユーザーアカウントを設定する際にパスワードの設定を必ず行ってください。

3.4.6 ユーザーアカウントの無効化

ユーザーアカウントが無効化されると、当該ユーザーがデバイス管理にアクセスすることをデバイスが拒否します。完全にアカウントを削除するのとは違い、ユーザーアカウントを無効化した場合はその設定を保存し、将来再利用することが可能です。以下の手順を実行します。

☐ ユーザーアカウント設定を保存し将来再利用するには、一時的にユーザーアカウントを無効化します。

- ☐ *Device Security > User Management* ダイアログボックスを開きます。設定されたユーザーアカウントをダイアログボックスが表示します。
- ☐ 対象のユーザーアカウントが表示された行の*Active* カラムから、チェックボックスのチェックを外します。
- ☐ ✔ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`users disable <user>`	ユーザーアカウントを無効化します。
`show users`	設定されたユーザーアカウントを表示します。
`save`	不揮発性メモリ（nvm）にある設定を「選択」したコンフィグレーションプロファイルに保存します。

☐ ユーザーアカウントを恒久的に無効化したい場合は、ユーザーアカウントを削除します。

☐ 対象のユーザーアカウントが表示された行にハイライトを入れます。

☐  ボタンをクリックします。

`users delete <user>`	ユーザーアカウント`<user>`を削除します。
`show users`	設定されたユーザーアカウントを表示します。
`save`	不揮発性メモリ（`nvm`）にある設定を「選択」したコンフィグレーションプロファイルに保存します。

3.4.7 パスワード変更の方針

ユーザーアカウントの方針が指定した方針と一致するかを、デバイス側からユーザーへ促します。パスワードが方針と一致していれば、パスワードがより複雑なレベルを得ることができています。

各ユーザーアカウントについて、個別アカウントのパスワード方針確認はデバイスのユーザー管理で有効化・無効化することができます。チェックボックスのチェックを入れ、新規のパスワードが方針要件を満たせば、デバイスはパスワードの変更を許可します。

実用的な方針については、デバイスのデフォルトで設定済みです。但しユーザーの要件を満たすよう方針を変更することができます。以下の手順を実行します。

□ 要件を満たすためにパスワードの方針を変更する手順は次の通りです。

□ *Device Security > User Management* ダイアログボックスを開きます。

Configuration フレームで、ユーザーがロックされてしまうまでのログイン試行回数を指定します。また、パスワードを定義する最小文字数を指定できます。

注記：当デバイスでは、ロック解除の権限は`administrator` レベルのユーザーのみとなります。

ログイン試行回数及びユーザーのロックは、以下のデバイス管理にアクセスしようとした場合に適用されます。

- グラフィカルユーザーインターフェース
- SSHプロトコル
- Telnetプロトコル

注記：シリアル接続からコマンドラインインターフェースを使用してデバイス管理にアクセスする場合、ログイン試行回数は無制限です。

□ 要件を満たす値を指定する方法

- *Login attempts* （ログイン試行）フィールドで、ログイン試行可能な回数を指定します。
  このフィールドの範囲は`0..5`です。
  上記の例では、数値を`0` にすると機能が無効化されます。
- *Min. password length* フィールドの範囲は `1..64`です。

ダイアログボックスの*Password policy* フレームに設定した方針が表示されます。

□ 要件を満たす値を指定します。

- 値の範囲は`1` から `16` までです。値`0` で対象の方針を無効化できます。

Configuration 及び *Password policy* フレームで指定したエントリーを適用するには、対象ユーザーの*Policy check* カラムのチェックボックスにチェックを入れます。

□ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`passwords min-length 6`	パスワード最小長の方針を指定します。
`passwords min-lowercase-chars 1`	パスワードに使用する小文字の最小数の方針を指定します。
`passwords min-numeric-chars 1`	パスワードに使用する数文字の最小数の方針を指定します。
`passwords min-special-chars 1`	パスワードに使用する特殊文字の最小数の方針を指定します。
`passwords min-uppercase-chars 1`	パスワードに使用する大文字の最小数の方針を指定します。
`show passwords`	設定された方針を表示します。
`save`	不揮発性メモリ（`nvm`）にある設定を「選択」したコンフィグレーションプロファイルに保存します。

3.5 LDAP

オフィス環境で使用のアプリケーション用ユーザーログイン認証情報を含むアクティブディレクトリは、サーバーアドミニストレーターが管理します。アクティブディレクトリは階層構造であり、ユーザー名、パスワード、各ユーザーのレベルに応じた読込み・書込み許可が含まれます。

当デバイスはLDAP（Lightweight Directory Access Protocol）を使用してユーザーログイン情報及び許可レベルを、アクティブディレクトリから読み出します。これにより、ネットワークデバイスにSSO（シングルサインオン）を提供します。アクティブディレクトリより認証情報を読み出すことで、ユーザーはオフィス環境で使用されるものと同じログイン認証情報でログインができます。

LDAPのセッションは、デバイスがDSA（Directory System Agent：ディレクトリシステムエージェント）を通してLDAPサーバーのアクティブディレクトリを検索することで開始されます。サーバーがアクティブディレクトリにユーザーのエントリーを複数確認すると、サーバーは検索された上位の認証レベルを送信します。DSAは情報リクエストをリッスンし、LDAPのTCPポート389又はLDAPS（LDAP over SSL）のTCPポート636 に応答を送信します。クライアントやサーバーはLDAPSリクエストをエンコードした後にBER（Basic Encoding Rules：基本符号化規則）で応答します。デバイスはリクエスト全てに対して新規接続を開き、サーバーから応答を受信した後に接続を遮断します。

SSL（Secure Socket Layer：セキュア・ソケット・レイヤー）及びTLS（Transport Layer Security：トランスポート・レイヤー・セキュリティ）セッションに対するサーバーの検証用に、当デバイスは、ユーザーにCA証明書のアップロードを許可します。従って、証明書はTLSセッションに対しては任意です。

デバイスは、ログイン認証情報を、メモリ内に1024ユーザー分までキャッシュすることができます。アクティブディレクトリサーバーにアクセスが届かなくても、ユーザーはオフィスログイン認証情報でログインすることができます。

3.5.1 サーバーアドミニストレーターとの連携

LDAP 機能の設定には、ネットワークアドミニストレーターがサーバーアドミニストレーターから以下の情報をリクエストしなければなりません。

- サーバー名又はIPアドレス
- サーバー上のアクティブディレクトリの位置
- 接続方法
- TCPリスニングポート
- 必要な場合、CA証明書の位置
- ユーザーログイン名を含むアトリビュート名
- ユーザー認証レベルを含むアトリビュート名

サーバーアドミニストレーターは、個別に`description`などのアトリビュートを使用するか、又はグループに対して`memberOf` などのアトリビュートを使用して認証レベルを割当てることができます。*Device Security > LDAP > Role Mapping* ダイアログボックスで、どのアトリビュートがどの種の認証レベルを受けられるかを指定できます。

また、JXplorer や SofterraなどのLDAPブラウザーを使用すれば、ユーザーログイン名や認証レベルを含むアトリビュート名を取得することもできます。

3.5.2 コンフィグレーション例

当デバイスは暗号リンクをサーバー名のみでローカルサーバー、又はIPアドレスを使用して別ネットワークのサーバーに構築することができます。サーバーアドミニストレーターはユーザーのログイン認証情報の識別にアトリビュートを使用し、個別及びグループの認証レベルを割当てることができます。

サーバーアドミニストレーターから受信した情報を使用し、アクティブディレクトリの、どのアトリビュートがユーザーログイン認証情報及び認証レベルを含めるかを指定します。すると、デバイス自身で指定されているユーザーログイン認証情報を認証レベルと比較し、指定された認証レベルでユーザーのログインを許可します。

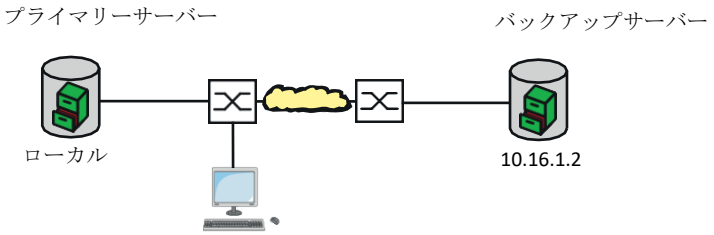


図18 LDAPコンフィグレーション例

この例では、サーバーアドミニストレーターは以下の情報を送信します。

情報	プライマリーサーバー	バックアップサーバー
サーバー名又はIPアドレス	ローカルサーバー	10.16.1.2
サーバー上のアクティブディレクトリの位置	Country/City/User	Country/Company/User
接続の種別	TLS （証明書あり）	SSL
サーバーアドミニストレーターはemailでCA証明書を送信	プライマリーサーバーのCA証明書はローカル保存	バックアップサーバーのCA証明書はローカル保存
TCPリスニングポート	389 (tls)	636 (ssl)
ユーザー名を含んだアトリビュート名	userPrincipalName	userPrincipalName
ユーザー認証レベルを含んだアトリビュート名	ADMINISTRATOR	ADMINISTRATOR

以下の手順を実行します。

- ☐ *Device Security > Authentication List* ダイアログボックスを開きます。
- ☐ デバイスの設定を実行しユーザーログイン認証情報を読み出すには、最初にアクティブディレクトリのグラフィカルユーザーインターフェースを使用したログイン中に、defaultLoginAuthList リストの*Policy 1* カラムにldap を指定します。
- ☐ *Device Security > LDAP > Configuration* ダイアログボックスを開きます。
- ☐ ユーザーログイン認証情報のキャッシュ保存期間は、ユーザーが指定できます。ユーザーログイン認証情報のキャッシュを1日保存したい場合、*Configuration* フレームの *Client cache timeout [min]* フィールドに、1440を入力します。
- ☐ *Bind user* のエントリーは任意です。指定した場合、ユーザーはログインする際に自分のユーザー名のみを入力します。サービスユーザーは*User name attribute* カラムにリストされたアクティブディレクトリの、どのログイン認証情報でも問題ありません。*Bind user* カラムにユーザー名及びドメインを入力します。

- ☐ *Base DN* とは、DC（Domain component：ドメイン・コンポーネント）及びOU（Organizational Unit：オーガニゼーショナル・ユニット）を組み合わせたものです。*Base DN* は、ドメイン（DC）にサーバーの位置を決定し、アクティブディレクトリ（OU）を検索します。アクティブディレクトリの位置を指定するには、*Base DN* カラムに値`ou=Users,ou=City,ou=Country,dc=server,dc=local`を指定します。
- ☐ サーバーアドミニストレーターがユーザーをどのアトリビュートにリストするかを指定するには、*User name attribute* カラムに値`userPrincipalName` を入力します。

デバイスはCA証明書でサーバーを確認します。

- ☐ 証明書がPC内又はネットワークドライブにある場合は、証明書を  エリア内にドラッグ&ドロップします。もしくは、エリア内をクリックして証明書を選択します。
- ☐ CA証明書をデバイスに移動させる場合、*Start* ボタンをクリックします。
- ☐ テーブルエントリーを追加するには、  ボタンをクリックします。
- ☐ 説明文を指定するには、*Description* カラムに値`Primary AD Server` を入力します。
- ☐ プライマリーサーバーのサーバー名及びドメインを指定するには、*Address* カラムに値`local.server`を入力します。
- ☐ プライマリーサーバーはTCPポート`389`で通信を行いますが、これは*Destination TCP port* のデフォルト値となっています。
- ☐ プライマリーサーバーは通信の暗号化にTLSを、サーバー検証にCA証明書を使用します。*Connection security* カラムに、値`startTLS`を指定します。
- ☐ このエントリーを有効にするには、*Active* カラムのチェックボックスにチェックを入れます。
- ☐ バックアップサーバー用にサーバーアドミニストレーターから受信した情報を使用し、行の追加及び設定を行い、有効化します。

- ☐ *Device Security > LDAP > Role Mapping* ダイアログボックスを開きます。
- ☐ テーブルエントリーを追加するには、  ボタンをクリックします。

LDAPが構成・有効化されている状態でユーザーがログインすると、デバイスはユーザーのログイン認証情報をアクティブディレクトリから検索します。デバイスがユーザー名及びパスワードが正しいと判断すると、デバイスは*Type* カラムに指定した値を検索します。デバイスがアトリビュートを発見し、*Parameter* カラムのテキストがアクティブディレクトリのテキストと一致していれば、デバイスはユーザーに指定された認証レベルでのログインを許可します。値`attribute` が*Type* カラムに指定されている場合、*Parameter* カラムに次の値を入力します。`attributeName=attributeValue`

- ☐ *Role* カラムに値`operator` を入力してユーザーロールを指定します。
- ☐ このエントリーを有効にするには、*Active* カラムのチェックボックスにチェックを入れます。
- ☐  ボタンをクリックします。
  ダイアログが*Create* ウィンドウを表示します。
  サーバーアドミニストレーターから受信した`administrator` ロールの値を入力します。
  このエントリーを有効にするには、*Active* カラムのチェックボックスにチェックを入れます。
- ☐ *Device Security > LDAP > Configuration* ダイアログボックスを開きます。
- ☐ 機能を有効化するには*Operation* フレームの*On* のラジオボタンを選択します。

以下の表は、コマンドラインインターフェースを使用してデバイス内のLDAP機能の設定するための手順を示したものです。表は`Index 1`のコマンドが示されています。`Index 2`の設定を行うには、同じコマンドを使用しますが、適切な情報で代替しなければなりません。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`ldap cache-timeout 1440`	デバイスに1日後に不揮発性メモリのフラッシングするよう指定します。

`ldap client server add 1 local.server port 389`	ホスト名`local.server` 及びUDPポート`389`でリモート認証クライアントサーバーの接続を追加します。
`ldap client server modify 1 security startTLS`	接続に使用するセキュリティの種類を指定します。
`ldap client server modify 1 description Primary_AD_Server`	エントリーのコンフィグレーション名を指定します。
`ldap basedn ou=Users,ou=City,ou=Country, dc=server, dc=local`	サーバーのアクティブディレクトリを検索するに使用するベースドメイン名を指定します。
`ldap search-attr userPrincipalName`	ユーザーのログイン認証情報の含まれるアクティブディレクトリで、検索するアトリビュートを指定します。
`ldap bind-user user@company.com`	サービスユーザーの名前及びドメインを指定します。
`ldap bind-passwd Ur-123456`	サービスユーザーのパスワードを指定します。
`ldap client server enable 1`	リモート認証クライアントサーバーの接続を有効化します。
`ldap mapping add 1 access-role operator mapping-type attribute mapping- parameter OPERATOR`	`Operator` ロールの、リモート認証ロールマッピングのエントリーを追加します。`Operator` ロールを`OPERATOR`のワードを含むアトリビュートにマッピングします。
`ldap client server enable 1`	リモート認証ロールマッピングのエントリーを有効化します。
`ldap operation`	リモート認証機能を有効化します。

3.6 SNMP access

SNMPにより、ユーザーはネットワーク管理システムを使ってネットワーク上のデバイスを監視し、その設定を変更することが可能です。

3.6.1 SNMPv1/v2 アクセス

デバイス通信を暗号化しない状態で、ネットワーク管理システムにSNMPv1又はSNMPv2を使用します。SNMPパケットは全て、プレーンテキストでのコミュニティ名と送信元のIPアドレスを含みます。

読込みアクセス用のコミュニティ名`user` 及び書込みアクセスの`admin` は、デバイスにプリセット済みです。SNMPv1/v2が有効であれば、コミュニティ名を知っているユーザーであれば、誰でもアクセスすることができます。

デバイスへの不正なアクセスをより難しくします。以下の手順を実行します。

- ☐ デバイス内のコミュニティ名をデフォルトから変更します。コミュニティ名は慎重に扱うようにします。
  書込みアクセスを持つコミュニティ名を知るユーザーは、誰でもデバイスの設定を変更することができます。
- ☐ アクセスが「読込み・書込み」と「読込み」のみのコミュニティでは、異なる名前を指定します。
- ☐ SNMPv1又はSNMPv2は、傍受から保護された環境でのみ使用してください。これらプロトコルは暗号化されていません。
- ☐ SNMPv3を使用し、デバイスのSNMPv1及びSNMPv2でのアクセスを無効化することをお勧めします。

3.6.2 SNMPv3 アクセス

デバイス通信を暗号化した状態で、ネットワーク管理システムにSNMPv3を使用します。ネットワーク管理システムは、ユーザーのログイン認証情報を使用してシステム自身が認証を行います。SNMPv3の条件として、ネットワーク管理システムがデバイスで定義された設定と同じ定義でなければなりません。

デバイスは、ユーザーに*SNMP auth type* 及び*SNMP encryption type* パラメーターを各ユーザーアカウントに対して個別に使用させてくれます。

デバイスに新規ユーザーアカウントを作成すると、ネットワーク管理システムConneXium Network Managerが瞬時にデバイスにアクセスできるようプリセットされています。

デバイスに設定されたユーザーアカウントは、グラフィカルユーザーインターフェース、コマンドラインインターフェース、SNMPv3で使用されるパスワードと同じものを使用しています。

ユーザーアカウント設定のSNMPv3パラメーターをネットワーク管理システムの設定に適応させるには、以下の手順を実行します。

- ☐ *Device Security > User Management* ダイアログボックスを開きます。
  設定されたユーザーアカウントをダイアログボックスが表示します。

- ☐ *SNMP auth type* フィールド内の、対象のユーザーアカウントが表示された行をクリックします。任意の設定を選択します。
- ☐ *SNMP encryption type* フィールド内の、対象のユーザーアカウントが表示された行をクリックします。任意の設定を選択します。
- ☐ ✔ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`users snmpv3 authentication <user> md5 | sha1`	ユーザーアカウント`<user>`の認証リクエストに、HMAC-MD5 又は HMACSHAプロトコルを指定します。
`users snmpv3 encryption <user> des | aescfb128 | none`	ユーザーアカウント`<user>`に、DES 又は AES-128 アルゴリズムを指定します。 このアルゴリズムは、デバイスは認証リクエストを暗号化します。 値`none` を選択すると暗号化が取り除かれます。
`show users`	設定されたユーザーアカウントを表示します。
`save`	不揮発性メモリ（`nvm`）にある設定を「選択」したコンフィグレーションプロファイルに保存します。

3.7 アウトオブバンド・アクセス

当デバイスには、デバイス管理へアウトオブバンドでアクセスするための別ポートが備わっています。スイッチポートに高いインバンド負荷がかかる場合、この別ポートを使用してデバイス管理へアクセスすることができます。

条件として、USBポートから直接管理ステーションに接続する必要があります。Microsoft Windowsを使用している場合は、必要に応じてRNDISドライバーをインストールします。管理ステーションに接続したら、バーチャルネットワークによる接続でデバイス管理と通信できるようになります。

デフォルトでは、このポートを通した以下のIPパラメーターを使用してデバイス管理にアクセスするようになっています。
- *IP address* `91.0.0.100`
- *Netmask* `255.255.255.0`

デバイス管理にアクセスするには、以下のプロトコルを使用できます。
- SNMP
- Telnet
- SSH
- HTTP
- HTTPS
- FTP
- SCP
- TFTP
- SFTP

3.7.1 IPパラメーターの指定

USBポートを通して管理ステーションに接続する場合、デバイスはUSBネットワークインターフェースに、1を足したIPアドレスを管理ステーションに割当てます（デフォルトでは `91.0.0.101` ）。デバイスはユーザーにIPパラメーターを変更し、使用環境要件を満たせるようデバイス側に適応させることを許可します。

このネットワークインターフェースのIPサブネットが、デバイスの他のインターフェースと繋がったサブネットと重複しないことを確認してください。
- 管理インターフェース

管理ステーションがUSBポートを通してデバイス管理へアクセスし、ユーザーが変更を終了すると、デバイスは瞬時にグラフィカルユーザーインターフェース及びコマンドラインインターフェースの接続を遮断します。

以下の手順を実行します。

- ☐ *Basic Settings > Out of Band over USB* ダイアログボックスを開きます。
- ☐ *IP parameter* の*IP address* フィールドに、IPアドレスを上書きします。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

```
enable
```
Privileged Exec Modeに切り替えます。

```
network usb parms 192.168.1.1
255.255.255.0
```
USBネットワークインターフェースのIPアドレスに192.168.1.1を、ネットマスクに255.255.255.0を指定します。

```
show network usb
```
USBネットワークインターフェースの設定を表示します。

```
Out-of-band USB management settings
-----------------------------------
Management operation.....................enabled
IP address. .............................192.168.1.1
Subnet mask. ............................255.255.255.0
Host MAC address.........................64:60:38:1f:85:85
Device MAC address.......................64:60:38:1f:85:86
```

```
save
```
不揮発性メモリ（nvm）にある設定を「選択」したコンフィグレーションプロファイルに保存します。

3.7.2 USBネットワークインターフェースの無効化

デフォルトでは、USBネットワークインターフェースは有効です。USBポートから誰にもデバイス管理へアクセスしてほしくない場合、USBネットワークインターフェースを無効化することができます。

管理ステーションがUSBポートを通してデバイス管理へアクセスし、ユーザーが変更を終了すると、デバイスは瞬時にグラフィカルユーザーインターフェース及びコマンドラインインターフェースの接続を遮断します。

以下の手順を実行します。

- ☐ *Basic Settings > Out of Band over USB* ダイアログボックスを開きます。
- ☐ USBネットワークインターフェースを無効化するには*Operation* フレームの*Off* のラジオボタンを選択します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

```
enable
```
Privileged Exec Modeに切り替えます。

```
no network usb operation
```
USBネットワークインターフェースを無効化します。

```
Out-of-band USB management settings
-----------------------------------
Management operation.....................disabled
IP address. .............................192.168.1.1
Subnet mask. ............................255.255.255.0
Host MAC address.........................64:60:38:1f:85:85
Device MAC address.......................64:60:38:1f:85:86
```

```
save
```
不揮発性メモリ（nvm）にある設定を「選択」したコンフィグレーションプロファイルに保存します。

4 ネットワーク内でシステム時刻を同期させる

多くのアプリケーションは時刻機能に依存しているため、時刻はできるだけ正確でなければなりません。必要とされる精度及び実際の時刻とのずれは、アプリケーションエリアにより異なります。

アプリケーションエリアは、以下の例を含みます。
- ログのエントリー
- 製造データのタイムスタンプ
- プロセス管理

当デバイスでは、以下のオプションを使ってネットワークの時刻と同期させることができます。
- SNTP（Simple Network Time Protocol）は、精度要件が低いときに利用できる簡単な方法です。
  好ましい条件下であれば、SNTPからミリ秒単位の精度を得ることができます。精度は信号の遅延具合によります。
- IEEE 1588 PTP（Precision Time Protocol）は、マイクロ秒以下の精度を得ることができます。この方法は、プロセスコントロールを含む厳しい環境にも適切です。

対象のデバイスがPTPプロトコルをサポートしている場合は、ＰＴＰがより好ましいといえます。PTPはより精度があり、誤差の修正にもより高度な方法が使われ、ネットワークの負荷も低くなっています。また、PTPを実装するほうが比較的簡単でもあります。

注記：PTP及びSNTPの規格によれば、いずれのプロトコルも同ネットワークで同時に機能します。但し、いずれのプロトコルもデバイスのシステム時刻に影響を及ぼすため、プロトコル同士で一致しない状況が発生することもあります。

4.1 基本設定

Time > Basic Settings ダイアログボックスで、時刻の基本設定を行います。

4.1.1 時刻設定

ソースとなる基準時刻にアクセスできない場合、デバイス内で時刻設定することもできます。

コールドスタート又はリブート後にリアルタイムの時計がない或いはリアルタイム時計の時刻が誤っている場合、デバイスの時刻が初期値のJanuary 1, 00:00hとなります。電源を落とした後でも、デバイスはリアルタイム時計の設定を24時間ほどバッファします。

また、PTP時計又はSNTPサーバーから現在時刻を自動取得するようデバイスを設定することもできます。

その他、SNTPサーバーから現在時刻を自動取得するようデバイスを設定することもできます。

以下の手順を実行します。

☐ *Time > Basic Settings* ダイアログボックスを開きます。

➢ *System time (UTC)* フィールドは、デバイスの現在のUTC（Universal Time Coordinated：協定世界時）を表示します。UTCは協定世界時の測定と同期しています。UTCは世界共通で、地域の時差は考慮しません。

➢ *System time* フィールドの時刻は*System time (UTC)* に*Local offset [min]*（現地オフセット）の値を加えたもので、サマータイム導入の場合はその分の時差も考慮されます。

注記：PTPはTAI（International Atomic Time：国際原子時）を送信します。2020年7月1日次点で、TAI時刻はUTCよりも37秒進んでいます。PTPの基準時刻となるUTCオフセットが正しく設定されていれば、デバイスはこの時差を*System time (UTC)* フィールドに自動修正して表示します。

☐ お使いのPCの時刻をデバイスに適用させるには、*System time* フィールドの*Set time from PC* ボタンをクリックします。
Local offset [min] フィールドの値をもとに、デバイスは*System time (UTC)* フィールドの時刻を計算します。 *System time (UTC)* の時刻は*System time (UTC)* から*Local offset [min]*の値を引いたもので、サマータイム導入の場合はその分の時差も考慮されます。

➢ *Time source* フィールドは、時刻データの発信元を表示します。デバイスは、最も精度のある発信元を自動で選択します。
初期の発信元は`local`です。
SNTPが有効でデバイスが有効なSNTPパケットを受信すると、デバイスは時刻ソースを`sntp`と設定します。
PTPが有効でデバイスが有効なPTPメッセージを受信すると、デバイスは時刻ソースを`ptp`と設定します。
なお、デバイスはPTPをSNTPに優先します。

➢ *Local offset [min]* 値は現地時刻と*System time (UTC)*の時差を指定したものです。

☐ デバイスにお使いのPCのタイムゾーンを特定させるには、*Set time from PC* ボタンをクリックします。デバイスはUTCからの現地時刻の時差を計算し、*Local offset [min]* フィールドに時差を入力してくれます。

注記：当デバイスでは、DHCPサーバーからlocal offsetを取得することもできます。

☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`clock set <YYYY-MM-DD> <HH:MM:SS>`	デバイスのシステム時刻を設定します。
`clock timezone offset <-780..840>`	現地時刻と受信したUTC時刻との時差を、分単位で入力します。
`save`	不揮発性メモリ（`nvm`）にある設定を「選択」したコンフィグレーションプロファイルに保存します。

4.1.2 サマータイムによる時刻の切替え

サマータイムが導入されているタイムゾーンでデバイスをご利用の場合、*Daylight saving time*（サマータイム）タブでサマータイム時刻切替えを設定します。

Daylight saving timeが有効な場合、デバイスはサマータイム開始時に現地時刻を1時間進めます。サマータイム終了時、デバイスは現地時刻を再び1時間戻します。以下の手順を実行します。

- ☐ *Time > Basic Settings* ダイアログボックスの*Daylight saving time* タブを開きます。
- ☐ サマータイムの開始・終了のプリセットプロファイルを選択するには、*Operation* フレームの*Profile...*ボタンをクリックします。
- ☐ 一致するサマータイムのプロファイルがない場合、時刻切替のタイミングを*Summertime begin*（開始）及び*Summertime end*（終了）フィールドで指定します。
  いずれのフィールドも、その月、月内のどの週、平日、時刻を設定します。
- ☐ 機能を有効化するには*Operation* フレームの*On* のラジオボタンを選択します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`clock summer-time mode <disable|recurring|eu|usa>`	自動でサマータイムの時刻切替を設定するには、プロファイルでenable/disable又はactivateを実行します。
`clock summer-time recurring start`	切替の開始時刻を入力します。
`clock summer-time recurring end`	切替の終了時刻を入力します。
`save`	不揮発性メモリ（nvm）にある設定を「選択」したコンフィグレーションプロファイルに保存します。

4.2 SNTP

SNTP（Simple Network Time Protocol）により、ネットワーク上のシステム時刻の同期が可能です。当デバイスではSNTPクライアント及びSNTPサーバー機能がサポートされています。

SNTPサーバーではUTC（Universal Time Coordinated：協定世界時）が使用できます。UTCは協定世界時の測定と同期しています。UTCは世界共通のため、現地時刻による時差は考慮されません。

SNTPは、NTP（Network Time Protocol）を簡略化したものです。SNTPとNTPのデータパケットは同一のものです。従って、NTP、SNTPのいずれのサーバーもSNTPクライアントの時刻ソースとして機能します。

注記：本章のに記載する外部SNTPサーバーの事項は、NTPサーバーにも適用します。

SNTPは時間を転送する上で、以下のオペレーションモードを認識しています。

- *Unicast*
  Unicast operation modeは、SNTPクライアントはSNTPサーバーにリクエストを送信し、サーバーからの応答を待ちます。
- *Broadcast*
  Broadcast operation modeは、SNTPサーバーはSNTPメッセージを指定した間隔でネットワークに送信します。SNTPクライアントはこれらSNTPメッセージを受信し、評価します。

Broadcast operation modeは、IPv6環境下では以下のオペレーションを実行します。

- SNTPクライアントは、IPv6の宛先アドレスとして`ff05::101` に設定したIPv6マルチキャストアドレスのあるSNTPサーバーメッセージのみを待機します。
- SNTPサーバーは、マルチキャストアドレス`ff05::101`にSNTPメッセージのみを送信します。SNTPサーバーは、IPv6の送信元アドレスとしてのリンクローカルアドレスのあるSNTPメッセージは送信しません。

表16　Broadcast operation modeのターゲットIPv4アドレスクラス

IPv4宛先アドレス	SNTPパケット送信先
`0.0.0.0`	対象無し
`224.0.1.1`	SNTPメッセージのマルチキャストアドレス
`255.255.255.255`	ブロードキャストアドレス

注記：*Broadcast* operation mode にあるSNTPサーバーは、SNTPクライアントからのユニキャストのダイレクトリクエストにも応答します。
一方、SNTPクライアントは*Unicast* 又は*Broadcast* の、いずれのoperation modeでも機能します。

4.2.1 準備

以下の手順を実行します。

☐ 時間がどのように転送されていくのかの概要を理解するために、SNTPに関わる機器類のネットワーク計画図を描いてください。
計画時は、SNTPメッセージの遅延によって時刻の精度が左右されることを意識してください。遅延時間やその偏差を最小限にするには、SNTPサーバーを各ネットワークセグメントに配置してください。これら個々のSNTPサーバーは、SNTPクライアントとメインSNTPサーバーをカスケード接続したシステム時刻と同期します。カスケード接続の最上位にあるメインSNTPサーバーは、基準時刻のソースに最も直接アクセスをしやすくなっています。

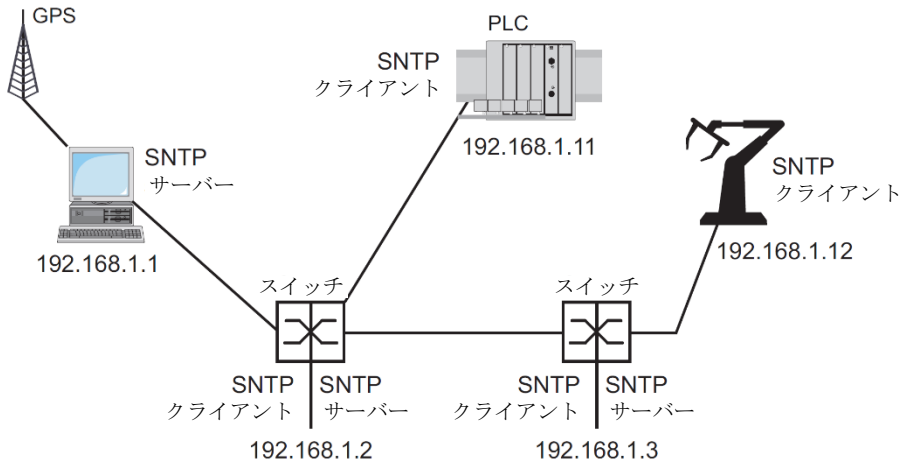


図19　SNTPのカスケード接続例

注記：正確な時刻の分配のため、SNTPサーバー及びSNTPクライアントの間に、SNTPパケットを低損失で均一な転送時間（レイテンシー）で転送できるネットワーク機器（ルーターやスイッチ）を使用することが好ましいといえます。

➢ SNTPクライアントは、設定されたSNTPサーバー4つまでリクエストを送信できます。最初のSNTPサーバーから応答がない場合、SNTPクライアントは2番目のSNTPサーバーへリクエストを送信します。このリクエストでも失敗する場合は3番目、最終的には4番目のSNTPサーバーへリクエストを送信します。これらのSNTPサーバーのいずれも応答しな場合、SNTPクライアントは同期を失います。SNTPクライアントは定期的に、いずれかのSNTPサーバーから有効な時間を受信するまでリクエストを送信します。

注記：当デバイスには、DHCPサーバーからSNTPサーバーのIPアドレスリストを取得できるオプションもあります。

☐ 基準時刻のソースが得られない場合は、SNTPサーバーのあるデバイス1つを、基準時刻のソースとして指定してください。このソースとなるシステム時刻は定期的に調整が必要です。

4.2.2 SNTPクライアントの設定

デバイスは、SNTPクライアントとしてSNTPサーバー又はNTPサーバーから時刻情報を取得し、自身のシステム時計を同期させます。以下の手順を実行します。

☐ *Time > SNTP > Client* ダイアログボックスを開きます。
☐ SNTPオペレーションモードの設定。
Configuration フレームの*Mode* フィールドで、以下いずれかの値を選択します。
➢ `unicast`
デバイスはSNTPサーバーにリクエストを送信し、サーバーからの応答を待ちます。
➢ `broadcast`
デバイスはネットワーク上のSNTPサーバーから、*Broadcast* 又は *Multicast* メッセージを待機します。
☐ 時刻を1度だけ同期するには、*Disable client after successful sync* のチェックボックスにチェックを入れます。同期後、デバイスは*SNTP Client* 機能を無効化します。
➢ テーブルには*Unicast* operation modeでリクエストを送信するSNTPクライアントが対象のSNTPサーバーを表示します。
このテーブルにはSNTPサーバー定義4つが含まれます。
☐ テーブルエントリーを追加するには、  ボタンをクリックします。
☐ SNTPサーバーの接続データを指定します。
☐ 機能を有効化するには*Operation* フレームの`On` のラジオボタンを選択します。
☐  ボタンをクリックし、変更を一時的に保存します。
➢ *State* フィールドには*SNTP Client* 機能の現在のステータスが表示されます。

表17　上記例のSNTPクライアント設定

情報	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
SNTP Client 機能	`Off`	`On`	`On`	`On`	`On`
Configuration:*Mode*	`unicast`	`unicast`	`unicast`	`unicast`	`unicast`
Request interval [s]	`30`	`30`	`30`	`30`	`30`
SNTP Server アドレス	–	`192.168.1.1`	`192.168.1.2` `192.168.1.1`	`192.168.1.2` `192.168.1.1`	`192.168.1.3` `192.168.1.2` `192.168.1.1`

4.2.3 SNTPサーバーの設定

デバイスがSNTPサーバーとしてのオペレーションを行う場合、ネットワークのUTC（協定世界時）をシステムの時刻とします。以下の手順を実行します。

- ☐ *Time > SNTP > Server* ダイアログボックスを開きます。
- ☐ 機能を有効化するには*Operation* フレームの*On* のラジオボタンを選択します。
- ☐ *Broadcast* operation modeを有効にする場合、*Configuration* フレームの*Broadcast admin mode* ラジオボタンを選択します。

  Broadcast operation modeは、SNTPサーバーはSNTPメッセージを指定した間隔でネットワークに送信します。また、SNTPサーバーはSNTPクライアントのリクエストに*Unicast* operation modeで応答します。
- ☐ *Broadcast destination address* フィールドに、SNTPサーバーがSNTPパケットを送信するIPv4アドレスを設定します。*Broadcast* アドレス又は *Multicast* アドレスを設定します。

  IPv6環境では、SNTPサーバーがSNTPパケットを送信するIPv6アドレスを設定することはできません。SNTPサーバーはマルチキャストアドレス`ff05::101`をIPv6の宛先アドレスとして使用します。
- ☐ *Broadcast UDP port* フィールドに、SNTPサーバーが*Broadcast* operation modeでSNTPパケットを送信するUDPポートの番号を指定します。
- ☐ *Broadcast VLAN ID* フィールドに、SNTPサーバーが*Broadcast* operation modeでSNTPパケットを送信するVLANのIDを指定します。
- ☐ *Broadcast send interval [s]* フィールドに、デバイスのSNTPサーバーがSNTP *Broadcast* パケットを送信するインターバルを入力します。

注記：*Broadcast destination address* フィールドを除き、残りの設定はIPv4及びIPv6 SNTPサーバーの両方に適用できます。

- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

➢ *State* フィールドには*SNTP Server* 機能の現在のステータスが表示されます。

表18　上記例の設定

デバイス	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
SNTP Server 機能	*On*	*On*	*On*	*Off*	*Off*
UDP port	123	123	123	123	123
Broadcast admin mode	unmarked	unmarked	unmarked	unmarked	unmarked
Broadcast destination address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Broadcast UDP port	123	123	123	123	123
Broadcast VLAN ID	1	1	1	1	1
Broadcast send interval [s]	128	128	128	128	128
Disable server at local time source	unmarked	unmarked	unmarked	unmarked	unmarked

4.3 PTP

LAN制御されたアプリケーションをレイテンシーなく作動させるには、正確な時間管理が必須です。IEEE 1588では、PTP（Precision Time Protocol）はネットワーク上の時計の正確な同期を実現する方法としています。

PTPの同期精度は数百ナノ秒となっています。PTPは同期メッセージにマルチキャストを使用することでネットワークの負荷を低減しています。

4.3.1 時計の種類

PTPはネットワーク上の時計に「マスター」「スレイブ」のロールを定義しています。
- マスタークロック（基準時間ソース）はその時間を分配します。
- スレイブクロックはマスターより受信したタイミング信号に自身の時刻を同期します。

バウンダリークロック（境界クロック）

ルーター及びスイッチの伝達時間（レイテンシー）は、時刻伝達の精度に明確な影響を及ぼします。このような誤差は、PTPではバウンダリークロック（境界クロック）として定義しています。

ネットワークセグメントでは、バウンダリークロックは基準時刻ソース（マスタークロック）であり、下位にあるスレイブ時計はマスターに時刻を同期します。通常、ルーターやスイッチがバウンダリークロックとしての役目を果たします。

代わりに、バウンダリークロックはより上位の基準時刻ソース（Grandmaster：グランドマスター）から時刻を取得します。

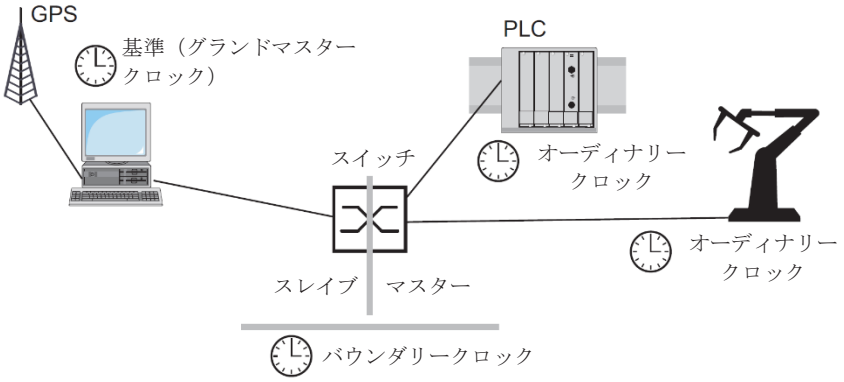


図20　ネットワーク上のバウンダリークロックの位置

トランスペアレントクロック（透過クロック）

スイッチは一般的にトランスペアレントクロックの役目を担うことでカスケード接続上に高い精度を発揮します。トランスペアレントクロックは、受信した同期メッセージを転送する際に、自身の伝送時間を修正するスレイブクロックです。

Ordinary Clock（オーディナリークロック）

PTPは、エンドクロックを「Ordinary Clock」（オーディナリークロック）と定義します。オーディナリークロックは、マスタークロック又はスレイブクロックのいずれとしても機能します。

4.3.2 Best Master Clock algorithm

PTPに関連するデバイス類は、ネットワーク上のデバイスを基準時刻ソース（グランドマスター）と定義しています。ここではネットワーク上の時計全ての精度を決定する、BMCA（Best Master Clock Algorithm：ベスト・マスタークロック・アルゴリズム）を使用します。

BMCAは、以下の基準を評価するアルゴリズムです。
- *Priority 1*
- *Clock class*
- *Clock accuracy*
- *Clock variance*
- *Priority 2*

アルゴリズムが最初に評価する値は、関連デバイスの*Priority 1* フィールドです。*Priority 1* フィールドの値が最も小さいデバイスが基準時刻ソース（グランドマスター）となります。
複数デバイスで同じ値の場合は、アルゴリズムは次の基準を評価します。こでも同じ値であれば、更に次の基準を評価します。これらの値が複数のデバイスで同じであれば、*Clock identity* フィールドの最も小さい値のものが、どのデバイスが基準時刻ソース（グランドマスター）となるかを決定します。

当デバイスでは、バウンダリークロックの設定で*Priority 1* 及び*Priority 2*の値をユーザーが個別に指定できます。このため、ネットワーク上のどのデバイスを基準時刻ソースとするか、ユーザーが決定することができます。

4.3.3 遅延測定

デバイス間の同期メッセージの遅延は、精度に影響を及ぼします。遅延測定により、各デバイスが平均遅延を考慮に入れることができるようになります。

PTP version 2 では、以下の遅延測定方法があります。
- *e2e* (End to End)
  スレイブクロックが、マスタークロックへの同期メッセージの遅延を測定します。
- *e2e-optimized*
  スレイブクロックが、マスタークロックへの同期メッセージの遅延を測定します。
  この方法は、トランスペアレントクロックのみ可能です。デバイスはマルチキャストで送信された同期メッセージをマスタークロックのみに転送し、ネットワークの負荷を軽減します。
  デバイスが別のマスタークロックから同期メッセージを受信すると、同期メッセージをこの新規のポートのみに転送します。
  デバイスがマスタークロックを認識していない場合、同期メッセージを全てのポートに転送します。
- *p2p* (Peer to Peer)
  スレイブクロックが、マスタークロックへの同期メッセージの遅延を測定します。
  また、マスタークロックはブロックされたポートも含め、各スレイブクロックへの遅延を測定します。但し、マスタークロック及びスレイブクロックがPeer-to-Peer（*p2p*）をサポートしていることが条件です。
  冗長リングによる遮断があった場合等は、例えばスレイブクロックがマスタークロックに、そしてマスタークロックがスレイブクロックになります。
  これらクロックは反対方向からの遅延を既に認識できているため、前述の切替えにより精度を失うことはありません。

4.3.4 PTPドメイン

デバイスは、同期メッセージを同一PTPドメインのデバイス間のみに伝送します。ユーザーは、バウンダリークロック及びトランスペアレントクロックのドメインを個別に設定することができます。

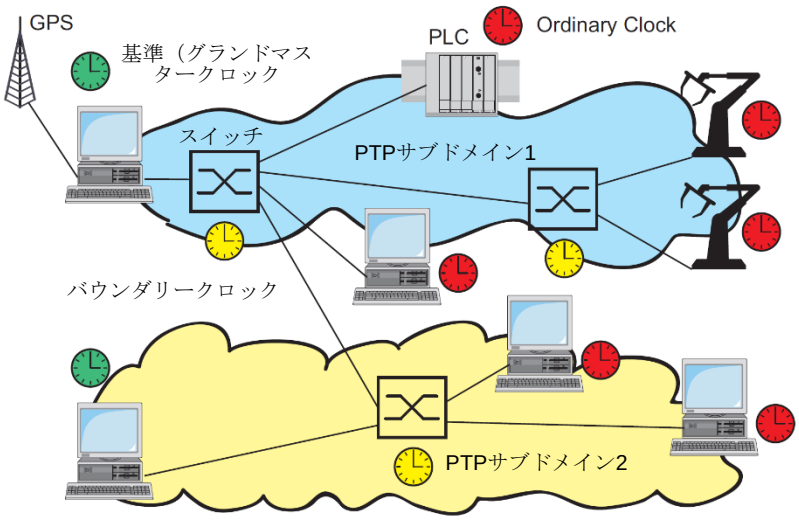


図21　PTPドメインの例

4.3.5 PTPの使用

時計を正確にPTPで同期するには、バウンダリークロック又はトランスペアレントクロックをノードとするスイッチのみ使用します。

以下の手順を実行します。

- ☐ 時計の分配の全体図を把握するために、PTPに関連するデバイス類を含めたネットワーク計画を描きます。
- ☐ 関連するスイッチ（バウンダリークロック又はトランスペアレントクロック）のロールを指定します。この設定を、当デバイスでは*PTP mode*としています。

表19　PTPモードの設定例

PTP mode	用途
v2-boundary-clock	デバイスはバウンダリークロックとして同期メッセージを下位ネットワークセグメントにあるスレイブクロックに分配します。 代わりに、バウンダリークロックはより上位の基準時刻ソース（Grandmaster：グランドマスター）から時刻を取得します。
v2-transparent-clock	デバイスはトランスペアレントクロックとして、 受信した同期メッセージの遅延をトランスペアレントクロックが修正した後に転送します。

- ☐ 関連する各スイッチのPTPを有効にします。
  これでPTPは概ね自動化されます。
- ☐ エンドデバイスのPTPを有効にします。
- ☐ ネットワーク上のどのデバイスを基準クロック（グランドマスター）とするか、ユーザーが決定することができます。従って、*Boundary Clock* の*Priority 1* 及び*Priority 2* フィールドのデフォルト値を変更します。

5 コンフィグレーションプロファイルの管理

作動中にデバイスの設定を変更すると、デバイスはこれら変更をメモリ（*RAM*）に保存します。リブート後、この設定は失われます。

リブート後もこれら変更を維持するには、不揮発性メモリ（*NVM*）にコンフィグレーションプロファイルの設定を保存します。素早く他の設定に切り替えられるよう、不揮発性メモリには複数のコンフィグレーションプロファイルを保存するスペースが確保されています。

外部メモリが接続されている場合は、その外部メモリ（*ENVM*）内のコンフィグレーションプロファイルのコピーが自動で保存されます。この機能は無効化することができます。

5.1 変更された設定の検知

当デバイスは、作動中に変更された設定を自身の揮発性メモリ（*RAM*）に保存します。不揮発性メモリ（*NVM*）内のコンフィグレーションプロファイルは、変更した設定を確実に保存するまで維持されます。それまでは、メモリ及び不揮発性メモリ内のコンフィグレーションプロファイルは異なります。デバイスは、ユーザーに変更した設定を気付かせてくれます。

5.1.1 揮発性メモリ (RAM) 及び不揮発性メモリ (NVM)

揮発性メモリ（*RAM*）内のコンフィグレーションプロファイルが「選択した」不揮発性メモリ（*NVM*）のコンフィグレーションプロファイルと異なる場合、ユーザーがそれに気付くことができます。以下の手順を実行します。

- ☐ メニュー上段のステータスバーを確認します。
  - – 点滅する  アイコンが表示されている場合、コンフィグレーションプロファイルは互いに異なります。
  - – アイコン  が表示されている場合、コンフィグレーションプロファイルは一致します。

又は...

- ☐ *Basic Settings > Load/Save* ダイアログボックスを開きます。
- ☐ *Information* フレームのチェックボックスの状態を確認します。
  - – チェックボックスにチェックが無い場合、コンフィグレーションプロファイルは互いに異なります。
  - – チェックボックスにチェックがある場合、コンフィグレーションプロファイルは一致します。

```
show config status

Configuration Storage sync State
--------------------------------
running-config to NV.......................out of sync
...
```

5.1.2 外部メモリ (EAM) 及び不揮発性メモリ (NVM)

外部メモリ（EAM）のコピーが不揮発性メモリ（*NVM*）内のコンフィグレーションプロファイルと異なる場合も、これに気付くことができます。以下の手順を実行します。

- ☐ *Basic Settings > Load/Save* ダイアログボックスを開きます。
- ☐ *Information* フレームのチェックボックスの状態を確認します。
  - チェックボックスにチェックが無い場合、コンフィグレーションプロファイルは互いに異なります。
  - チェックボックスにチェックがある場合、コンフィグレーションプロファイルは一致します。

```
show config status

Configuration Storage sync State
--------------------------------
...
NV to EAM.....................................out of sync
...
```

5.2 設定の保存

5.2.1 デバイスにコンフィグレーションプロファイルを保存する

作動中にデバイスの設定を変更すると、デバイスはこれら変更をメモリ（RAM）に保存します。リブート後もこれら変更を維持するには、不揮発性メモリ（*NVM*）にコンフィグレーションプロファイルの設定を保存します。

コンフィグレーションプロファイルの保存

当デバイスは、不揮発性メモリ(*NVM*)のコンフィグレーションプロファイル内に「選択」した設定を保存します。

以下の手順を実行します。

- ☐ *Basic Settings > Load/Save* ダイアログボックスを開きます。
- ☐ 必要なコンフィグレーションプロファイルが「選択」されたことを確認します。*Selected* カラムのチェックボックスにチェックが入っていれば、コンフィグレーションプロファイルが「選択」されていることを指します。
- ☐  ボタンをクリックします。

`show config profiles nvm`	不揮発性メモリ（nvm）内のコンフィグレーションプロファイルが表示されます。
`enable`	Privileged Exec Modeに切り替えます。
`save`	不揮発性メモリ（nvm）にある設定を「選択」したコンフィグレーションプロファイルに保存します。

コンフィグレーションプロファイルに設定をコピーする

上記の「選択」したコンフィグレーションプロファイルの他、メモリ（RAM）に保存された設定もコンフィグレーションプロファイルに保存することができます。この方法であれば、新規のコンフィグレーションプロファイルを不揮発性メモリ（*NVM*）に作成できる他、既存のものに上書きすることも可能です。

以下の手順を実行します。

- ☐ *Basic Settings > Load/Save* ダイアログボックスを開きます。
- ☐  ボタンに続き、 *Save as..* の項目をクリックします。ダイアログボックスに*Save as..* ウィンドウが表示されます。
- ☐ *Name* フィールドで、コンフィグレーションプロファイルの名前を変更します。推奨された名前のままで保存をすると、デバイスは既存の同名コンフィグレーションプロファイルに上書きします。
- ☐ *Ok* ボタンをクリックします。

これで新規コンフィグレーションプロファイルが、「選択」されたものと定義されます。

`show config profiles nvm`	不揮発性メモリ（nvm）内のコンフィグレーションプロファイルが表示されます。
`enable`	Privileged Exec Modeに切り替えます。
`copy config running-config nvm profile <string>`	不揮発性メモリ（`nvm`）内の`<string>` 名のコンフィグレーションプロファイルにある現在の設定を保存します。これがあれば、デバイスは既存の同名コンフィグレーションプロファイルに上書きします。これで新規コンフィグレーションプロファイルが、「選択」されたものと定義されます。

コンフィグレーションプロファイルの選択

不揮発性メモリ（*NVM*）に複数のコンフィグレーションプロファイルが含まれる場合、ユーザーはそこにある任意のコンフィグレーションプロファイルを選択することができます。当デバイスはコンフィグレーションプロファイル内に「選択」した設定を保存します。リブートの際、デバイスは「選択」したコンフィグレーションプロファイルの設定をメモリ（`RAM`）にロードします。

以下の手順を実行します。

- ☐ *Basic Settings > Load/Save* ダイアログボックスを開きます。

  テーブルにデバイス内にあるコンフィグレーションプロファイルが表示されます。*Selected* カラムのチェックボックスにチェックが入っていれば、コンフィグレーションプロファイルが「選択」されていることを指します。
- ☐ 揮発性メモリ（*NVM*）内に保存された必要となるコンフィグレーションプロファイルのエントリーを、テーブルで選択します。
- ☐ ☰ ボタンに続き、 *Select* の項目をクリックします。

これで*Selected* カラムにあるコンフィグレーションプロファイルのチェックボックスにチェックが入ります（`marked`）。

`enable`	Privileged Exec Modeに切り替えます。
`show config profiles nvm`	不揮発性メモリ（`nvm`）内のコンフィグレーションプロファイルが表示されます。
`configure`	Configuration modeに切り替えます。
`config profile select nvm 1`	コンフィグレーションプロファイルの識別子です。コンフィグレーションプロファイルに隣接している名前に注意してください。
`save`	不揮発性メモリ（`nvm`）にある設定を「選択」したコンフィグレーションプロファイルに保存します。

5.2.2 外部メモリにコンフィグレーションプロファイルを保存する

外部メモリが接続されている状態でコンフィグレーションプロファイルを保存する場合、デバイスは自動的に*Selected external memory*にコピーを保存します。この機能はデフォルトで有効です。この機能は無効化することができます。

以下の手順を実行します。

- ☐ *Basic Settings > External Memory* ダイアログボックスを開きます。
- ☐ *Backup config when saving* カラムのチェックボックスにチェックを入れることで、保存プロセス中にデバイスが自動的に外部メモリにも保存するようになります。
- ☐ この機能を無効化するには、*Backup config when saving* カラムのチェックボックスからチェックを外します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`config envm config-save usb`	機能を有効化します。 コンフィグレーションプロファイルを保存する際に、デバイスは外部メモリにコピーを保存します。 `usb` = 外部USBメモリ
`save`	不揮発性メモリ（`nvm`）にある設定を「選択」したコンフィグレーションプロファイルに保存します。

5.2.3 リモートサーバーにコンフィグレーションプロファイルのバックアップを保存する

当デバイスでは、リモートサーバーにコンフィグレーションプロファイルのバックアップを自動で保存することができます。
但しコンフィグレーションプロファイルを保存する前に、この機能を有効化しておく必要があります。

不揮発性メモリ（*NVM*）にコンフィグレーションプロファイルを保存後、デバイスは指定されたURLにコピーを送信します。

以下の手順を実行します。

- ☐ *Basic Settings > Load/Save* ダイアログボックスを開きます。
  Backup config on a remote server when saving フレームで、以下の手順を実行します。
- ☐ *URL*フィールドに、サーバー、パス、バックアップされたコンフィグレーションプロファイルのファイル名を指定します。
- ☐ *Set credentials* ボタンをクリックします。
  ダイアログボックスに*Credentials* ウィンドウが表示されます。
- ☐ リモートサーバーの認証に必要なログイン認証情報を入力します。
- ☐ *Operation* オプションリストで、機能を有効化します。
- ☐ ☑タンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`show config remote-backup`	機能のステータスを確認します。
`configure`	Configuration modeに切り替えます。
`config remote-backup destination`	コンフィグレーションプロファイルをバックアップするリンク先URLを入力します。
`config remote-backup username`	リモートサーバーで認証するユーザー名を入力します。
`config remote-backup password`	リモートサーバーで認証するパスワードを入力します。
`config remote-backup operation`	機能を有効化します。

リモートサーバーへの移行が成功すれば、デバイスはこのイベントをログファイル（システムログ）に記録します。

5.2.4 コンフィグレーションプロファイルのエクスポート

当デバイスでは、サーバーにコンフィグレーションプロファイルをXMLファイルで保存することができます。グラフィカルユーザーインターフェースを使用すれば、XMLファイルを直接PCに保存することもできます。

条件：
- ファイルをサーバーに保存するには、ネットワークに設定済みのサーバーが必要となります。
- ファイルをSCP又はSFTPサーバーに保存するには、このサーバーにアクセスできるユーザー名及びパスワードが必要となります。

以下の手順を実行します。

- ☐ *Basic Settings > Load/Save* ダイアログボックスを開きます。
- ☐ 必要となるコンフィグレーションプロファイルのエントリーを、テーブルで選択します。

コンフィグレーションプロファイルをPCにエクスポートします。以下の手順を実行します。

- ☐ *Profile name* カラムのリンクをクリックします。
- ☐ 保存先を選択し、ファイル名を指定します。
- ☐ *Ok* ボタンをクリックします。

これでコンフィグレーションプロファイルがXMLファイルとして指定の場所に保存されます。

リモートサーバーにコンフィグレーションプロファイルをエクスポートします。以下の手順を実行します。

- ☐ ボタンに続き、*Export...* の項目をクリックします。
  ダイアログボックスに*Export...* ウィンドウが表示されます。
- ☐ *URL* フィールドに、リモートサーバーのファイルURLを指定します。
  - ☐ ファイルをFTPサーバーに保存するには、以下の形式でファイルURLを指定します。
    `ftp://<user>:<password>@<IP address>:<port>/<file name>`
  - ☐ ファイルをTFTPサーバーに保存するには、以下の形式でファイルURLを指定します。
    `tftp://<IP address>/<path>/<file name>`
  - ☐ ファイルをSCP又はSFTPサーバーに保存するには、以下の形式でファイルURLを指定します。
    `scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>` `scp://` or `sftp://<IP address>/<path>/<file name>`
    Ok ボタンをクリックすると、デバイスは*Credentials* ウィンドウを表示します。ここに*User name* 及び*Password* を入力し、サーバーにログインします。
- ☐ *Ok* ボタンをクリックします。
  これでコンフィグレーションプロファイルがXMLファイルとして指定の場所に保存されます。

`show config profiles nvm`	不揮発性メモリ（`nvm`）内のコンフィグレーションプロファイルが表示されます。
`enable`	Privileged Exec Modeに切り替えます。
`copy config running-config remote tftp://<IP_address>/<path>/<file_name>`	現在の設定をTFTPサーバーに保存します。
`copy config nvm remote sftp://<user_name>:<password>@<IP_address>/<path>/<file_name>`	SFTPサーバー上の不揮発性メモリ（`nvm`）に選択したコンフィグレーションプロファイルを保存します。
`copy config nvm profile config3 remote tftp://<IP_address>/<path>/<file_name>`	FTPサーバー上の不揮発性メモリ（`nvm`）にコンフィグレーションプロファイル`config3` を保存します。
`copy config nvm profile config3 remote ftp://<IP_address>:<port>/<path>/<file_name>`	FTP サーバー上の不揮発性メモリ（`nvm`）にコンフィグレーションプロファイル`config3` を保存します。

5.3 設定のローディング

メモリに複数のコンフィグレーションプロファイルを保存されていれば、ユーザーは異なるコンフィグレーションプロファイルを選択してロードすることができます。

5.3.1 コンフィグレーションプロファイルのアクティベーション

デバイスの不揮発性メモリには、複数のコンフィグレーションプロファイルを保存ことができます。不揮発性メモリ（*NVM*）に保存されたコンフィグレーションプロファイルのアクティベーションをすると、デバイスの設定は瞬時に変更されます。デバイスのリブートは不要です。

以下の手順を実行します。

- ☐ *Basic Settings > Load/Save* ダイアログボックスを開きます。
- ☐ 必要となるコンフィグレーションプロファイルのエントリーを、テーブルで選択します。
- ☐ ☰ ボタンに続き、*Activate* の項目をクリックします。

デバイスはメモリ（RAM）に設定をコピーし、グラフィカルユーザーインターフェースから切断されます。デバイスは瞬時にコンフィグレーションプロファイルの設定を使用します。

- ☐ グラフィカルユーザーインターフェースをリロードします。
- ☐ 再度ログインします。

Selected カラムにある先にアクティベーションされたコンフィグレーションプロファイルのチェックボックスにチェックが入ります（marked）。

`show config profiles nvm`	不揮発性メモリ（nvm）内のコンフィグレーションプロファイルが表示されます。
`enable`	Privileged Exec Modeに切り替えます。
`copy config nvm profile config3 running-config`	不揮発性メモリ（nvm）内のコンフィグレーションプロファイルconfig3 の設定をアクティベートします。 デバイスは設定を揮発性メモリにコピーし、コマンドラインインターフェースとの接続を切断します。デバイスは瞬時にコンフィグレーションプロファイルconfig3の設定を使用します。

5.3.2 外部メモリからコンフィグレーションプロファイルを読み込む

外部メモリが接続されている場合は、デバイスは再起動時に外部メモリのコンフィグレーションプロファイルを自動でロードします。ユーザーはこれら設定を不揮発性メモリのコンフィグレーションプロファイルに保存できます。

外部メモリが同一デバイスのコンフィグレーションプロファイルを保存していた場合、片方のデバイスからもう片方へと設定を移すことが可能です。

以下の手順を実行します。

☐ 再起動時に、デバイスが外部メモリからコンフィグレーションプロファイルをロードすることを確認します。この機能はデフォルトで有効です。無効になっている場合は、以下の方法で有効化します。

☐ *Basic Settings > External Memory* ダイアログボックスを開きます。

☐ *Config priority* カラムで、値`first`を選択します。

☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`config envm load-priority usb first`	機能を有効にします。 リブート時に、デバイスが外部メモリからコンフィグレーションプロファイルをロードします。 `usb` = 外部USBメモリ
`show config envm settings`	外部メモリ（`envm`）の設定を表示します。

```
Type   Status      Auto Update  Save Config Config Load Prio
------ ----------- ----------- ----------- ----------------
usb    ok          [x]          [x]         first
```

`save`	デバイスの揮発性メモリ（`NVM`）にある設定をコンフィグレーションプロファイルに保存します。

当デバイスではコマンドラインインターフェースを使用し、外部メモリにある設定をコピーして直接不揮発性メモリ（*NVM*）に保存することができます。

`show config profiles nvm`	不揮発性メモリ（`nvm`）内のコンフィグレーションプロファイルが表示されます。
`enable`	Privileged Exec Modeに切り替えます。
`copy config envm profile config3 nvm`	外部メモリ（`envm`）から不揮発性メモリ（`nvm`）へとコンフィグレーションプロファイル`config3`をコピーします。

また、デバイスはブート中にスクリプトファイルからコンフィグレーションプロファイルを自動でロードすることもできます。

条件：

- デバイスの起動前に外部メモリが接続されていることを確認します。
- 外部メモリのルートディレクトリには、コンテンツ`script=<file_name>`とするテキストファイル `startup.txt` が含まれます。プレースホルダー`<file_name>` は、起動中にデバイスが実行するスクリプトファイルを指します。
- 外部メモリのルートディレクトリには、スクリプトファイルが含まれます。保存する際のスクリプト名はユーザーが指定できます。ファイル拡張子は`.cli`となります。

注記：外部メモリに保存したスクリプトが空でないことを確認してください。スクリプトが空の場合、デバイスはconfiguration priorityの優先順位に従い、次点のコンフィグレーションプロファイルをロードします。

スクリプトを適用したら、デバイスはスクリプトをXMLファイルとしてコンフィグレーションプロファイルを外部メモリに自動保存します。適切なコマンドをスクリプトファイルに入力すれば、この機能を無効化することができます。

☐ `no config envm config-save usb`
デバイスは外部USBメモリにコピーを保存しなくなります。

スクリプトファイルに不正確なコマンドが含まれると、デバイスは起動中にこのコマンドを適用しません。デバイスはこのイベントをログファイル（システムログ）に記録します。

5.3.3 コンフィグレーションプロファイルのインポート

当デバイスは、XMLファイルとして保存されたコンフィグレーションプロファイルをサーバーからインポートすることができます。グラフィカルユーザーインターフェースを使用すれば、XMLファイルを直接PCからインポートすることができます。

条件：
- ファイルをサーバーに保存するには、ネットワークに設定済みのサーバーが必要となります。
- ファイルをSCP又はSFTPサーバーに保存するには、このサーバーにアクセスできるユーザー名及びパスワードが必要となります。

以下の手順を実行します。

☐ *Basic Settings > Load/Save* ダイアログボックスを開きます。

☐ ☰ ボタンに続き、*Import...* の項目をクリックします。ダイアログボックスに*Import...* ウィンドウが表示されます。

☐ *Select source* ドロップダウンリストで、コンフィグレーションプロファイルのインポート元を選択します。
- *PC/URL*
  デバイスはローカルPC又はリモートサーバーからコンフィグレーションプロファイルをインポートします。
- *External memory*
  デバイスは外部メモリからコンフィグレーションプロファイルをインポートします。

ローカルPC又はリモートサーバーからコンフィグレーションプロファイルをインポートします。以下の手順を実行します。

☐ コンフィグレーションプロファイルのインポート：

☐ ファイルがFTPサーバーに保存されている場合、以下の形式でファイルURLを指定します。
`ftp://<user>:<password>@<IP address>:<port>/<file name>`

☐ ファイルがTFTPサーバーに保存されている場合、以下の形式でファイルURLを指定します。
`tftp://<IP address>/<path>/<file name>`

☐ ファイルがSCP又はSFTPサーバーに保存されている場合、以下の形式でファイルURLを指定します。
`scp://` or `sftp://<IP address>/<path>/<file name>`
Start ボタンをクリックすると、デバイスは*Credentials* ウィンドウを表示します。ここに*User name* 及び*Password* を入力し、サーバーにログインします。
`scp://` or `sftp://<user>:<password>@<IP address>/<path>/<file name>`

- *Destination* フレームに、デバイスがインポートされたコンフィグレーションプロファイルを保存する場所を指定します。
  - *Profile name* フィールドに、デバイスがコンフィグレーションプロファイルを保存するプロファイル名を指定します。
  - *Storage type* フィールドに、コンフィグレーションプロファイルの保存先を指定します。
- *Ok* ボタンをクリックします。

デバイスは指定したメモリにコンフィグレーションプロファイルをコピーします。

Destination フレームに値`ram` を指定した場合、デバイスはグラフィカルユーザーインターフェースを切断し、設定を瞬時に使用します。

外部メモリからコンフィグレーションプロファイルをインポートします。以下の手順を実行します。

- *Import profile from external memory* フレームの *Profile name* ドロップダウンリストで、インポートするコンフィグレーションプロファイルの名前を選択します。
  条件として外部メモリにエクスポートしたコンフィグレーションプロファイルがなければなりません。
- *Destination* フレームに、デバイスがインポートされたコンフィグレーションプロファイルを保存する場所を指定します。
  - *Profile name* フィールドに、デバイスがコンフィグレーションプロファイルを保存するプロファイル名を指定します。
- *Ok* ボタンをクリックします。

デバイスは不揮発性メモリ（*NVM*）にコンフィグレーションプロファイルをコピーします。

Destination フレームに値`ram` を指定した場合、デバイスはグラフィカルユーザーインターフェースを切断し、設定を瞬時に使用します。

```
enable
```

Privileged Exec Modeに切り替えます。

```
copy config remote ftp://
<IP_address>:<port>/<path>/
<file_name> running-config
```

FTPサーバーに保存したコンフィグレーションプロファイルの設定をインポートし、アクティベートします。
デバイスは設定を揮発性メモリにコピーし、コマンドラインインターフェースとの接続を切断します。デバイスは瞬時にインポートしたコンフィグレーションプロファイルの設定を使用します。

```
copy config remote tftp://
<IP_address>/<path>/<file_name>
running-config
```

TFTPサーバーに保存したコンフィグレーションプロファイルの設定をインポートし、アクティベートします。
デバイスは設定を揮発性メモリにコピーし、コマンドラインインターフェースとの接続を切断します。デバイスは瞬時にインポートしたコンフィグレーションプロファイルの設定を使用します。

`copy config remote sftp://<user name>:<password>@<IP_address>/ <path>/<file_name> running-config`	SFTPサーバーに保存したコンフィグレーションプロファイルの設定をインポートし、アクティベートします。 デバイスは設定を揮発性メモリにコピーし、コマンドラインインターフェースとの接続を切断します。デバイスは瞬時にインポートしたコンフィグレーションプロファイルの設定を使用します。
`copy config remote ftp:// <IP_address>:<port>/<path>/ <file_name> nvm profile config3`	FTPサーバーに保存されたコンフィグレーションプロファイルの設定をインポートし、不揮発性メモリ（`nvm`）にコンフィグレーションプロファイル`config3` を保存します。
`copy config remote tftp:// <IP_address>/<path>/<file_name> nvm profile config3`	TFTPサーバーに保存されたコンフィグレーションプロファイルの設定をインポートし、不揮発性メモリ（`nvm`）にコンフィグレーションプロファイル`config3` を保存します。

5.4 デバイスを出荷設定にリセットする

デバイスの設定を出荷設定にリセットすると、デバイスは揮発性メモリ及び不揮発性メモリのコンフィグレーションプロファイルを消去します。

外部メモリが接続されている場合は、デバイスは外部メモリ内に保存されたコンフィグレーションプロファイルも消去します。

その後デバイスはリブートし、出荷設定をロードします。

5.4.1 グラフィカルユーザーインターフェース又はコマンドラインインターフェースの使用

以下の手順を実行します。

- ☐ *Basic Settings > Load/Save* ダイアログボックスを開きます。
- ☐  ボタンをクリックし、*Back to factory...*を選択します。
  ダイアログボックスにメッセージが表示されます。
- ☐ *Ok* ボタンをクリックします。

デバイスはメモリ（RAM）及び不揮発性メモリ（*NVM*）のコンフィグレーションプロファイルを消去します。

外部メモリが接続されている場合は、デバイスは外部メモリ内に保存されたコンフィグレーションプロファイルも消去します。

しばらくするとデバイスは再起動し、出荷設定をロードします。

`enable`	Privileged Exec Modeに切り替えます。
`clear factory`	不揮発性メモリ及び外部メモリからコンフィグレーションプロファイルを消去します。 外部メモリが接続されている場合は、デバイスは外部メモリ内に保存されたコンフィグレーションプロファイルも消去します。 しばらくするとデバイスは再起動し、出荷設定をロードします。

5.4.2 システムモニターの使用

条件：
- PCとデバイスが端末ケーブルでシリアル接続されていなければなりません。

以下の手順を実行します。
- ☐ デバイスを再起動します。
- ☐ システムモニターに切り替えるには、リブート中にプロンプトが要求してから3秒以内に<1>キーを押します。
  デバイスがシステムモニターをロードします。
- ☐ メインメニューから`Manage configurations` へ切り替えるには、<4>キーを押します。
- ☐ `Clear configs and boot params` コマンドを実行するには、<1>キーを押します。

- 出荷設定をロードするには<Enter>キーを押します。
  デバイスはメモリ（RAM）及び不揮発性メモリ（*NVM*）のコンフィグレーションプロファイルを消去します。
  外部メモリが接続されている場合は、デバイスは外部メモリ内に保存されたコンフィグレーションプロファイルも消去します。
- メインメニューに切り替えるには、<q>キーを押します。
- デバイスを出荷設定状態でリブートするには<q>キーを押します。

6 ソフトウェアアップデートのローディング

シュナイダーエレクトリックは、自社ソフトウェアの改良及び開発を常時継続いたします。お客様に更に有益なアップデート版のソフトウェアがないか、定期的にご確認ください。製品情報やソフトウェアのダウンロードは、インターネット上の右記シュナイダーエレクトリック製品ページからお探しください。www.schneider-electric.com

当デバイスのソフトウェアをアップデートするには、次の方法から選択できます。
- PCからのソフトウェアアップデート
- サーバーからのソフトウェアアップデート
- 外部メモリからのソフトウェアアップデート
- 旧バージョンのソフトウェアのロード

注記：デバイスのソフトウェアをアップデート後も、デバイスの設定は維持されます。

インストールしたソフトウェアのバージョンは、グラフィカルユーザーインターフェースのログインダイアログで確認できます。

既にログインした状態からインストールしたソフトウェアのバージョンを表示するには、以下の手順を実行します。

☐ *Basic Settings > Load/Save* ダイアログボックスを開きます。
Running version フィールドには、バージョンの番号及びデバイスが最後の再起動時にロードし、現在稼働しているバージョンの作成日が表示されます。

```
enable
show system info
```

Privileged Exec Modeに切り替えます。

バージョンの番号及びデバイスが最後の再起動時にロードし、現在稼働しているバージョンの作成日などのシステム情報が表示されます。

6.1 PCからのソフトウェアアップデート

デバイスソフトウェアのイメージファイルが、PCからアクセス可能なデータ記憶媒体に保存されていることが条件となります。

以下の手順を実行します。

☐ デバイスソフトウェアのイメージファイルが保存されているフォルダまで移動します。
☐ *Basic Settings > Load/Save* ダイアログボックスを開きます。
☐ イメージファイルを  エリアにドラグ＆ドロップします。もしくは、エリア内をクリックしてファイルを選択します。
☐ アップデートを開始するには、*Start* ボタンをクリックします。
アップデートの手順が成功すると、デバイスはソフトウェアアップデートが成功したという情報を表示します。
再起動時、デバイスはインストールされたデバイスソフトウェアをロードします。

6.2 サーバーからのソフトウェアアップデート

SFTP又はSCPを使用してソフトウェアアップデートを行うには、デバイスソフトウェアのイメージファイルが保存されたサーバーが必要となります。

TFTP、SFTP、SCPのいずれかを使用してソフトウェアアップデートを行うには、デバイスソフトウェアのイメージファイルが保存されたサーバーが必要となります。

以下の手順を実行します。

- ☐ *Basic Settings > Software* ダイアログボックスを開きます。
- ☐ *Software update* フレームの *URL* フィールドで、以下の形式でイメージファイルのURLを入力します。
  - ➢ イメージファイルがFTPサーバーに保存されている場合：
    `ftp://<IP_address>:<port>/<path>/<image_file_name>.bin`
  - ➢ イメージファイルがTFTPサーバーに保存されている場合：
    `tftp://<IP_address>/<path>/<image_file_name>.bin`
  - ➢ イメージファイルがSCP又はSFTPサーバーに保存されている場合：
    `scp://` 又は `sftp://<IP_address>/<path>/<image_file_name>.bin`
    `scp://` 又は `sftp://<username>:<password>@<IP_address>/<path>/<image_file_name>.bin`
    ユーザー名及びパスワードが無いURLを入力すると、デバイスは*Credentials* ウィンドウを表示します。
    ここにログイン認証情報を入力し、サーバーにログインします。
- ☐ アップデートを開始するには、*Start* ボタンをクリックします。
  デバイスは、現在作動しているデバイスソフトウェアをバックアップメモリにコピーします。アップデートの手順が成功すると、デバイスはソフトウェアアップデートが成功したという情報を表示します。
  再起動時、デバイスはインストールされたデバイスソフトウェアをロードします。

```
enable

copy firmware remote tftp://
10.0.1.159/ product.bin system
```

Privileged Exec Modeに切り替えます。

TFTPサーバーからIPアドレス`10.0.1.159`の`product.bin` ファイルを、デバイスへ移します。

6.3 外部メモリからのソフトウェアアップデート

6.3.1 アドミニストレーターが手動で開始する

デバイスソフトウェアのアップデートは、マウスで数回クリックするだけで実行できます。デバイスソフトウェアのイメージファイルが、外部メモリに保存されていることが条件となります。

以下の手順を実行します。

- ☐ *Basic Settings > Software* ダイアログボックスを開きます。
- ☐ 外部メモリにある任意のイメージファイルの名前が表示されたテーブル内の行に印を入れます。
- ☐ 右クリックでコンテキストメニューを開きます。
- ☐ アップデートを開始するには、コンテキストメニュー内の*Update* をクリックします。
  デバイスは、現在作動しているデバイスソフトウェアをバックアップメモリにコピーします。アップデートの手順が成功すると、デバイスはソフトウェアアップデートが成功したという情報を表示します。
  再起動時、デバイスはインストールされたデバイスソフトウェアをロードします。

6.3.2 デバイスが自動で開始する

以下のファイルが再起動中に外部メモリにある場合、デバイスソフトウェアのアップデートは自動で開始します。

➢ デバイスソフトウェアのイメージファイル
➢ コンテンツ`autoUpdate=<Image_file_name>.bin`を含むテキストファイル`startup.txt`

Basic Settings > External Memory ダイアログボックスの、*Software auto update* カラムのチェックボックスにチェックが入っていることが条件となります。デフォルトではチェックが入っています。

以下の手順を実行します。

- ☐ 新しいデバイスソフトウェアのイメージファイルを、外部メモリのメインディレクトリにコピーします。デバイスに適応したイメージファイルのみを使用してください。
- ☐ 外部メモリのメインディレクトリに、テキストファイル`startup.txt` を作成します。
- ☐ テキストエディターで`startup.txt` を開き、以下のラインを追加します。
  `autoUpdate=<Image_file_name>.bin`
- ☐ デバイスに外部メモリをインストールします。

☐ デバイスを再起動します。
起動中、デバイスは自動的に以下の基準を満たしているかを確認しています。
- 外部メモリは接続されているか。
- `startup.txt` ファイルは外部メモリのメインディレクトリにあるか。
- `startup.txt` ファイルに指定されたイメージファイルは存在するか。
- イメージファイルのソフトウェアのバージョンは、現在作動しているソフトウェアのものよりも新しいか。

基準が満たされていれば、デバイスはアップデートを開始します。
デバイスは、現在作動しているデバイスソフトウェアをバックアップメモリにコピーします。
アップデートの手順が成功すると、デバイスはすぐに自動リブートし、新バージョンのソフトウェアをロードします。

☐ アップデートの結果を確認します。*Diagnostics > Report > System Log*ダイアログボックスのログファイルには以下いずれかのメッセージが表示されます。

- `S_watson_AUTOMATIC_SWUPDATE_SUCCESS`
  ソフトウェアアップデートは成功しました
- `S_watson_AUTOMATIC_SWUPDATE_ABORTED`
  ソフトウェアアップデートは中止しました
- `S_watson_AUTOMATIC_SWUPDATE_ABORTED_WRONG_FILE`
  ソフトウェアアップデートはイメージファイルが誤っていたために中止しました
- `S_watson_AUTOMATIC_SWUPDATE_ABORTED_SAVING_FILE`
  ソフトウェアアップデートはデバイスがイメージファイルを保存できなかったために中止しました

6.4 旧バージョンのソフトウェアをロードする

ユーザーは、デバイスソフトウェアを旧バージョンと入れ替えることができます。デバイスのソフトウェアを入れ替え後も、基本設定は維持されます。

注記：新しいバージョンのデバイスソフトウェアの機能設定のみが失われます。

7 ポートのコンフィグレーション

以下のポートコンフィグレーション機能が使用できます。
- ポートの有効化・無効化
- Operating modeの選択
- ポートのGigabit Ethernet mode

7.1 ポートの有効化・無効化

デフォルトでは、全てのポートが有効です。アクセスに対するセキュリティを高めるには、接続されていないポートを無効にします。以下の手順を実行します。

- ☐ *Basic Settings > Port* ダイアログボックスの *Configuration* タブを開きます。
- ☐ ポートを有効化するには、*Port on* カラムのチェックボックスにチェックを入れます。
- ☐ ポートを無効化するには、*Port on* カラムのチェックボックスのチェックを外します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`interface 1/1`	インターフェース`1/1`のInterface Configuration mode に変更します。
`no shutdown`	インターフェースを有効化します。

7.2 Operating modeの選択

デフォルトでは、ポートのOperating modeは*Automatic configuration* に設定されています。

注記：アクティブな自動コンフィグレーションは、手動コンフィグレーションに優先します。

以下の手順を実行します。

- ☐ *Basic Settings > Port* ダイアログボックスの *Configuration* タブを開きます。
- ☐ このポートに接続されたデバイスの設定を固定する必要がある場合、以下の手順を実行します。
  - ☐ 機能を無効化します。*Automatic configuration* カラムのチェックボックスのチェックを外します。
  - ☐ *Manual configuration* カラムに、任意の操作モード（transmission rate、duplex mode等）を入力します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`interface 1/1`	インターフェース`1/1`のInterface Configuration modeに変更します。
`no auto-negotiate`	自動Configuration modeを無効化します。
`speed 100 full`	ポート速度100 MBit/s、全二重

7.3 ポートのGigabit Ethernet mode

当デバイスは以下いずれかのSFPトランシーバーのうち1つで、複数のインターフェースを2.5Gbit/s でサポートします。

- M-SFP-2.5-MM/LC EEC
- M-SFP-2.5-SM-/LC EEC
- M-SFP-2.5-SM/LC EEC
- M-SFP-2.5-SM+/LC EEC

スロットにどの種のトランシーバーを挿入するかは、ポート速度によります。当デバイスは速度をマニュアルで設定することはできません。ポート速度が2.5Gbit/s では、100Mb/s のデータ伝送レートはサポートできません。

注記：トランシーバーのオーダー番号についての詳細情報は、「インストール」ユーザーマニュアルの「アクセサリー」の章をご参照ください。

7.3.1 例：

Gigabit Ethernet modeを使用してアップリンクの帯域幅をより高くすることができます。この機能は、対応可能なトランシーバーを適正なスロットで使用します。

以下の手順を実行します。

☐ *Basic Settings > Port* ダイアログボックスの *Configuration* タブを開きます。

Manual configuration カラムに表示の`2.5 Gbit/s FDX` は、2.5 Gbit/s のSFPトランシーバーが挿入されたポートを示しています。
速度の変更はできません。

```
show port 1/1
```

スロット`1` ポート`1`のパラメーターを表示します。Physical Mode リストエントリーは、2.5 Gbit/s のSFPトランシーバーが挿入されたポートの値 2500 full を表示します。

```
Interface.....................1/1
Name..........................My interface
--
Cable-crossing Setting........-
Physical Mode.................2500 full
Physical Status...............-
```

8 不正アクセスからの保護アシスト

当デバイスには、不正アクセスからデバイスを保護するアシスト機能があります。

デバイスのセットアップ後、以下手順を実施してデバイスへの不正アクセスのリスクを軽減させます。

- SNMPv1/v2 コミュニティの変更
- SNMPv1/v2の無効化
- HTTPの無効化
- ユーザーのHTTPS証明書を使用する
- ユーザーのSSHキーを使用する
- Telnetの無効化
- Ethernet Switch Configuratorの無効化
- IPアクセス制限
- セッションのタイムアウト時間の調整

8.1 SNMPv1/v2 コミュニティの変更

SNMPv1/v2 でのオペレーションは暗号化されます。SNMPパケットは全て、送信元のIPアドレスの他、送信元がデバイスにアクセスするためのプレーンテキストのコミュニティ名を含みます。SNMPv1/v2が有効であれば、コミュニティ名を知っているユーザーであれば、誰でもアクセスすることができます。

読込みアクセス用のコミュニティ名`user` 及び書込みアクセスの`admin` は、プリセット済みです。SNMPv1又はSNMPv2を使用している場合は、デフォルトコミュニティ名を変更してください。コミュニティ名は慎重に扱うようにします。以下の手順を実行します。

- ☐ *Device Security > Management Access > SNMPv1/v2 Community* ダイアログボックスを開きます。設定されたコミュニティ名をダイアログボックスが表示します。
- ☐ `Write` には、*Name* カラムにコミュニティ名を指定します。
  - 最大で英数字32文字まで可能です。
  - デバイスは大文字・小文字を区別します。
  - 読込みアクセスとは別のコミュニティ名を指定します。
- ☐ ✔ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`snmp community rw <community name>`	読込みアクセス・書込みアクセスのコミュニティを指定します。
`show snmp community`	設定されたコミュニティを表示します。
`save`	不揮発性メモリ（`nvm`）にある設定を「選択」したコンフィグレーションプロファイルに保存します。

8.2 SNMPv1/v2の無効化

SNMPv1又はSNMPv2が必要な場合は、傍受から保護された環境でのみ使用してください。SNMPv1及びSNMPv2は暗号化を行いません。SNMPパケットでは、コミュニティはクリアテキストとなっています。SNMPv3を使用し、デバイスのSNMPv1及びSNMPv2でのアクセスを無効化することをお勧めします。以下の手順を実行します。

- ☐ *Device Security > Management Access > Server* ダイアログボックスの*SNMP*タブを開きます。

ダイアログボックスがSNMPサーバーの設定を表示します。

- ☐ SNMPv1プロトコルを無効化するには、*SNMPv1* のチェックボックスからチェックを外します。
- ☐ SNMPv2プロトコルを無効化するには、*SNMPv2* のチェックボックスからチェックを外します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`no snmp access version v1`	SNMPv1プロトコルを無効化します。
`no snmp access version v1`	SNMPv2プロトコルを無効化します。
`show snmp access`	SNMPサーバーの設定を表示します。
`save`	不揮発性メモリ（`nvm`）にある設定を「選択」したコンフィグレーションプロファイルに保存します。

8.3 HTTPの無効化

ウェブサーバーは、グラフィカルユーザーインターフェースのプロトコルにHTTP又はHTTPSを使用します。HTTPSでの接続は暗号化されているのに対し、HTTPの接続は暗号化されていません。

デフォルトでは、HTTPプロトコルは有効です。HTTPを無効化すると、グラフィカルユーザーインターフェースに暗号化しないでもアクセスできるようになります。以下の手順を実行します。

- ☐ *Device Security > Management Access > Server* ダイアログボックスの*HTTP* タブを開きます。
- ☐ HTTPプロトコルを無効化するには*Operation* フレームの*Off* のラジオボタンを選択します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`no http server`	HTTPプロトコルを無効化します。

HTTPプロトコルが無効であれば、デバイスのグラフィカルユーザーインターフェースにはHTTPSのみでアクセスすることができます。ウェブブラウザのアドレスバーに、デバイスのIPアドレスの前にストリング`https://` を入力します。

HTTPSプロトコルが無効の時に更にHTTPSを無効化すると、、グラフィカルユーザーインターフェースにアクセスすることはできません。グラフィカルユーザーインターフェースで作業する場合、コマンドラインインターフェースを使用してHTTPSを有効にしてください。以下の手順を実行します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`https server`	HTTPSプロトコルを有効化します。

8.4 Telnetの無効化

当デバイスでは、Telnet又はSSHを使用してTelnetにリモートアクセスすることができます。Telnetでの接続は暗号化されていないのに対し、SSHの接続は暗号化されています。

Telnetサーバーはデフォルトで有効になっています。Telnetを無効化すると、リモートから暗号化無しでコマンドラインインターフェースにアクセスすることができなくなります。以下の手順を実行します。

- ☐ *Device Security > Management Access > Server* ダイアログボックスの*Telnet* タブを開きます。
- ☐ Telnetサーバーを無効化するには*Operation* フレームの*Off* のラジオボタンを選択します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`no telnet server`	Telnetサーバーを無効化します。

SSHサーバーが無効の時にTelnetも無効化すると、デバイスのシリアルインターフェースを通してのみコマンドラインインターフェースにアクセスすることができます。リモートでコマンドラインインターフェースを使用する場合、SSHを有効にしてください。以下の手順を実行します。

- ☐ *Device Security > Management Access > Server* ダイアログボックスの*SSH* タブを開きます。
- ☐ *SSH* サーバーを有効化するには*Operation* フレームの*On* のラジオボタンを選択します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`ssh server`	SSHサーバーを有効にします。

8.5 Ethernet Switch Configuratorアクセスの無効化

Ethernet Switch Configuratorにより、試運転中にネットワークからデバイスのIPパラメーターを指定することができます。Ethernet Switch Configuratorは、暗号化及び認証無しで、デバイス管理と通信することができます。

デバイスの試運転後、Ethernet Switch Configuratorをread-only（読込み専用）に設定するか、Ethernet Switch Configuratorのアクセスを完全に無効にすることをお勧めします。以下の手順を実行します。

- ☐ *Basic Settings > Network* ダイアログボックスを開きます。
- ☐ Ethernet Switch Configuratorソフトウェアからの書込み許可を取り消すには、*Ethernet Switch Configurator protocol v1/v2* のフレームの*Access* フィールドで、値`readOnly` を指定します。
- ☐ Ethernet Switch Configuratorのアクセスを完全に無効にするには、*Ethernet Switch Configurator protocol v1/v2* フレームの`Off` ラジオボタンを選択します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`network ethernet-switch-conf mode read- only`	Ethernet Switch Configuratorソフトウェアの書込み許可を無効化します。
`no network ethernet-switch-conf operation`	Ethernet Switch Configuratorアクセスを無効化します。

8.6 IPアクセス制限のアクティベーション

デフォルトでは、いずれものIPアドレス及びそれをサポートするプロトコルであれば、デバイス管理へアクセスすることができます。

IPアクセス制限をすると、指定したIPアドレス範囲及び指定したIPプロトコルでデバイス管理へアクセスすることが制限されます。

例：

デバイスは、グラフィカルユーザーインターフェースを使用して、社内ネットワークのみからアクセス可能とすべきです。アドミニストレーターは、SSHを使用したリモートアクセスも可能です。社内ネットワークはアドレス範囲が192.168.1.0/24 となり、モバイルネットワークからのリモートアクセスはアドレス範囲が109.237.176.0/24となります。SSHアプリケーションプログラムは、RSAキーのフィンガープリントを認識しています。

表20 IPアクセス制限のパラメーター

パラメーター	社内ネットワーク	モバイルネットワーク
ネットワークアドレス	192.168.1.0	109.237.176.0
ネットマスク	24	24
推奨プロトコル	https, snmp	ssh

以下の手順を実行します。

- ☐ *Device Security > Management Access > IP Access Restriction* ダイアログボックスを開きます。
- ☐ エントリーの*Active* カラムのチェックボックスからチェックを外します。
  このエントリーによりユーザーは、いずれものIPアドレス及びそれをサポートするプロトコルであれば、デバイスへアクセスすることができます。

社内ネットワークのアドレス範囲：

- ☐ テーブルエントリーを追加するには、  ボタンをクリックします。
- ☐ *IP address range* カラムに、社内ネットワークのアドレス範囲を指定します。
  192.168.1.0/24
- ☐ 社内ネットワークのアドレス範囲には、不要なプロトコルは無効化します。*HTTPS*、*SNMP*、*Active* それぞれのチェックボックスは、チェックを外したままとします。

モバイルスネットワークのアドレス範囲：

- ☐ テーブルエントリーを追加するには、  ボタンをクリックします。
- ☐ *IP address range* カラムに、モバイルネットワークのアドレス範囲を指定します。
  109.237.176.0/24
- ☐ モバイルネットワークのアドレス範囲には、不要なプロトコルは無効化します。*SSH*、*Active* それぞれのチェックボックスは、チェックを外したままとします。

機能を有効化する前に、テーブルのアクティブエントリーの少なくとも1つがアクセスを許可していることを確認します。これを怠ると、設定変更した場合にデバイスへの接続が遮断されます。デバイスのシリアルインターフェースを通してコマンドラインインターフェースを使用することが、デバイス管理へアクセスする唯一の方法です。

- ☐ IPアクセス制限を有効化するには*Operation* フレームの*On* のラジオボタンを選択します。
- ☐  ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`show network management access global`	IPアクセス制限が有効化又は無効化されたことを表示します。
`show network management access rules`	エントリーが設定されたことを表示します。
`no network management access operation`	IPアクセス制限を無効化します。
`network management access add 2`	社内ネットワークのアドレス範囲のエントリーを作成します。 ここの例で次点のインデックス数は、2となります。
`network management access modify 2 ip 192.168.1.0`	社内ネットワークのIPアドレスを指定します。社
`network management access modify 2 mask 24`	内ネットワークのネットマスクを指定します。
`network management access modify 2 ssh disable`	社内ネットワークのアドレス範囲のSSHを無効化します。 不要なプロトコルに対し、この作業を繰り返します。
`network management access add 3`	モバイルネットワークのアドレス範囲のエントリーを作成します。 ここの例で次点のインデックス数は、3となります。
`network management access modify 3 ip 109.237.176.0`	モバイルネットワークのIPアドレスを指定します。
`network management access modify 3 mask 24`	モバイルネットワークのネットマスクを指定します。
`network management access modify 3 snmp disable`	モバイルスネットワークのアドレス範囲のSNMPを無効化します。 不要なプロトコルに対し、この作業を繰り返します。
`no network management access status 1`	デフォルトのエントリーを無効化します。 このエントリーによりユーザーは、いずれものIPアドレス及びそれをサポートするプロトコルであれば、デバイスへアクセスすることができます。
`network management access status 2`	社内ネットワークのアドレス範囲のエントリーを有効化します。
`network management access status 3`	モバイルネットワークのアドレス範囲のエントリーを有効化します。
`show network management access rules`	エントリーが設定されたことを表示します。
`network management access operation`	IPアクセス制限を有効化します。

8.7 セッションのタイムアウト時間の調整

ログオンしたユーザーにアクティビティが無い場合、デバイスは自動的にセッションを遮断します。セッションタイムアウトは、最後のユーザーアクションからアクティビティのない期間を指します。

セッションタイムアウトは、以下の使用に指定することができます。
- SSH接続されたコマンドラインインターフェースのセッション
- Telnet接続されたコマンドラインインターフェースのセッション
- シリアル接続されたコマンドラインインターフェースのセッション
- グラフィカルユーザーインターフェース

SSH接続されたコマンドラインインターフェースのセッションタイムアウト

以下の手順を実行します。

- ☐ *Device Security > Management Access > Server* ダイアログボックスの*SSH* タブを開きます。
- ☐ *Configuration* フレームの*Session timeout [min]* フィールドに、タイムアウトの時間を分単位で指定します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`ssh timeout <0..160>`	SSH接続されたコマンドラインインターフェースのセッションタイムアウトの時間を分単位で指定します。

Telnet接続されたコマンドラインインターフェースのセッションタイムアウト

以下の手順を実行します。

- ☐ *Device Security > Management Access > Server* ダイアログボックスの*Telnet* タブを開きます。
- ☐ *Configuration* フレームの*Session timeout [min]* フィールドに、タイムアウトの時間を分単位で指定します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`telnet timeout <0..160>`	Telnet接続されたコマンドラインインターフェースのセッションタイムアウトの時間を分単位で指定します。

シリアル接続されたコマンドラインインターフェースのセッションタイムアウト

以下の手順を実行します。

- ☐ *Device Security > Management Access > CLI* ダイアログボックスの*Global* タブを開きます。
- ☐ *Configuration* フレームの*Serial interface timeout [min]*フィールドに、タイムアウトの時間を分単位で指定します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`cli serial-timeout <0..160>`	シリアル接続されたコマンドラインインターフェースのセッションタイムアウトの時間を分単位で指定します。

グラフィカルユーザーインターフェースのセッションタイムアウト

以下の手順を実行します。

- ☐ *Device Security > Management Access > Web* ダイアログボックスを開きます。
- ☐ *Configuration* フレームの*Web interface session timeout [min]* フィールドに、タイムアウトの時間を分単位で指定します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`network management access web timeout <0..160>`	グラフィカルユーザーインターフェースのセッションタイムアウトの時間を分単位で指定します。

9 データトラフィック制御

当デバイスは、定義されたルールに基づき転送するデータパケットを確認します。ルールが適用されるデータパケットは、デバイスにより転送されるか、或いはブロックされます。データパケットがいずれのルールにも適用されない場合、デバイスはパケットをブロックします。

何らルールが定義されていないルーテッドポートは、パケットを通過させます。ルールが定義されると即時に、定義されたルールが最初に処理されます。その後、デバイスに指定された標準アクションが有効となります。

当デバイスには、データストリームの制御する以下の機能があります。
- サービスリクエストの制御（DoS：Denial of Service）
- IPアドレス又はMACアドレスに基づきデバイスへのアクセスを拒否します（アクセスコントロールリスト）。

当デバイスは、データストリームを観察・監視します。デバイスは観察・監視の結果とネットワークセキュリティとを組み合わせ、「ステータステーブル」と呼ばれる状態テーブルを作成します。このステータステーブルを元に、デバイスはデータを受付ける・ドロップする・拒否する等を決定します。

データは以下の順に、デバイスのフィルター機能を通過します。
- DoS … `permit` 又は `accept`の場合、次のルールに進みます。
- ACL … `permit` 又は `accept`の場合、次のルールに進みます。

9.1 不正アクセスからの保護

デバイスはこの機能により、特定のサービス又はデバイスに不具合を起こさせることを目的とした無効な又は偽造されたデータパケットからの保護をサポートします。DoS攻撃に対して保護するため、ユーザーはフィルターを指定してデータストリームに制限をかけることができます。アクティブなフィルターは受信データパケットを確認し、フィルター規則に一致する場合は即時にそれを破棄します。

Network Security > DoS > Global ダイアログボックスには、2つの異なるフィルターを有効化することのできるフレームを含みます。これらを有効にするには、対応するチェックボックスにチェックを入れます。

TCP/UDP フレームでは、TCP及びUDPパケットのみに影響するフィルター4つを有効にします。このフィルターを使い、攻撃者がデバイスや対応サービスを認識するために行うポートスキャンを無効にすることができます。フィルターは以下のように作動します。

表21 TCPパケット用DoSフィルター

フィルター	効果
Activate Null Scan Filter	受信した以下の性質のTCPパケットを検知し、破棄します。 ➢ TCPフラグがない。 ➢ TCPシーケンス番号が0。

表21　TCPパケット用DoSフィルター

フィルター	効果
Activate Xmas Filter	受信した以下の性質のTCPパケットを検知し、破棄します。 ➢ *FIN*、*URG*、*PSH* のTCPフラグが同時にセットされている。 ➢ TCPシーケンス番号が0。
Activate SYN/FIN Filter	TCPパケットに*SYN*、*FIN*のTCPフラグが同時にセットされたTCPパケットの受信を検知し、破棄します。
Activate Minimal Header Filter	TCPヘッダーが短すぎるTCPパケットの受信を検知し、破棄します。

*ICMP*フレームにはICMPパケットのオプションが2つ提示されます。受信したICMPパケットが断片化されている場合は攻撃の予兆です。このフィルターを有効にすると、デバイスは断片化されたICMPパケットを検知し、破棄します。*Allowed payload size [byte]* パラメーターを使い、ICMPパケットペイロードの最大許容量を指定することもできます。デバイスはこのバイト数を超えたパケットを破棄します。

注記：フィルターは*Network Security > DoS > Global* ダイアログボックスで如何様にも組み合わせることができます。複数のフィルターを選択した場合は論理ORが適用されます。例えば1番目又は2番目（又は3番目等）のフィルターがデータパケットに適用されると、デバイスはそれを破棄します。

9.2 ACL

このメニューでは、ACL（Access Control Lists：アクセスコントロールリスト）にパラメーターを入力することができます。

当デバイスは、ACLを使いVLAN・単独ポート、複数ポートのデータパケットをフィルターすることができます。ACLではデバイスがデータパケットをフィルターするルールを指定することができます。データパケットにルールが適用されると、デバイスはパケットに対して当該ルールに基づいたアクションを実行します。使用可能なアクションは以下の通りです。

- 許可（`permit`）
- 拒否（`deny`）
- 特定ポートへリダイレクトする（*Redirection port* フィールド参照）
- ミラーリング（*Mirror port* フィールド参照）

以下のリストは、データパケットのフィルターに適用可能な基準になります。

- パケットの送信元又は宛先アドレス（MAC）
- データパケットの送信元又は宛先アドレス（IPv4）
- データパケットの送信元又は宛先ポート（IPv4）

以下の各種ACLを指定することができます。

- VLANのIP ACL
- ポートのIP ACL
- VLANのMAC ACL
- ポートのMAC ACL

同インターフェースにIP ACL及びMAC ACLの両方を指定すると、デバイスは最初にIP ACLを使用してデータストリームをフィルターします。デバイスはパケットがIP ACLを通してフィルターされた後でなければMAC ACLルールを適用しません。ACLの優先順位は、ルールのインデックスは考慮しません。

デバイスはACL内でルールの順位を処理しています。デバイスがデータストリームをフィルターする順番は、各ルールのインデックスにより決定します。ポート又はVLANにACLを指定した場合、優先順位をインデックスと合わせて指定することができます。数字が低いほど優先順位は高くなります。デバイスは優先順位の高いルールから処理を行います。

ACLに指定したルールのいずれもデータパケットに適用されない場合、暗黙の`deny` ルールが適用されます。結果として、デバイスは受信したデータパケットをドロップします。

デバイスが暗黙の`deny` ルールを直接実行することにご留意ください。

注記：使用可能なACL数はデバイスによります。ACLの値に関する詳細は、347ページの「技術データ」をご参照ください。

注記：単独のACLは、ポート又はVLANいくつでも指定することができます。*ACL*メニューには

以下のダイアログボックスが含まれます。

- *ACL IPv4 Rule*
- *ACL MAC Rule*
- *ACL Assignment*

これらダイアログは以下のオプションを提供します。

- 各種ACLのルールの指定
- 必要な優先順位でルールを提供
- ACLをポート又はVLANに指定

9.2.1 IPv4ルールの作成・編集

IPv4データパケットをフィルターする際、ユーザーは以下を実行できます。
- 新規グループやルールの作成
- 既存グループに新規ルールを追加
- 既存ルールの編集
- グループやルールのアクティベーション・ディアクティベーション
- 既存グループやルールの削除
- 既存ルールの順番の変更

以下の手順を実行します。

- ☐ *Network Security > ACL > IPv4 Rule* ダイアログボックスを開きます。
- ☐  ボタンをクリックします。
  ダイアログが*Create* ウィンドウを表示します。
- ☐ グループを作成するには、*Group name* フィールドに分かりやすい名前を入力します。1つのグループに複数のルールを組み合わせることができます。
- ☐ 既存のグループにルールを追加する場合、*Group name* フィールドのグループ名を選択します。
- ☐ *Index* フィールドで、ACL内のルール番号を指定します。この番号はルールの優先順位を決定するものです。
- ☐ *Ok* ボタンをクリックします。
  デバイスはルールをテーブルに追加します。グループ及びロールは即時に有効となります。
  グループ又はルールを無効化する場合、*Active* カラムのチェックボックスからチェックを外します。ルールを削除する場合、対象のテーブルエントリーにハイライトを入れ、  ボタンをクリックします。
- ☐ テーブルのルールパラメーターを編集します。
  値を変更するには、任意のフィールドをダブルクリックします。
- ☐  ボタンをクリックし、変更を一時的に保存します。

注記：*Source IP address* 及び *Destination IP address* パラメーターのワイルドカードを使用できます。例えば`192.168.?.?`と入力すると、デバイスは`192.168`で開始するアドレスを許可します。

注記：*Source TCP/UDP port* 及び*Destination TCP/UDP port* カラムの値を変更するには、*Protocol* カラムに値`tcp` 又は `udp` と指定しなければなりません。

注記：*Redirection port* 及び*Mirror port* カラムの値を変更するには、*Action* カラムに値`permit` と指定しなければなりません。

9.2.2 コマンドラインインターフェースを使用したIP ACLの作成・コンフィグレーション

以下の例では、コンピューターB・CからIP（TCP、UDP等）を介したコンピューターAへの通信をブロックするよう、ユーザーがACL設定を行います。

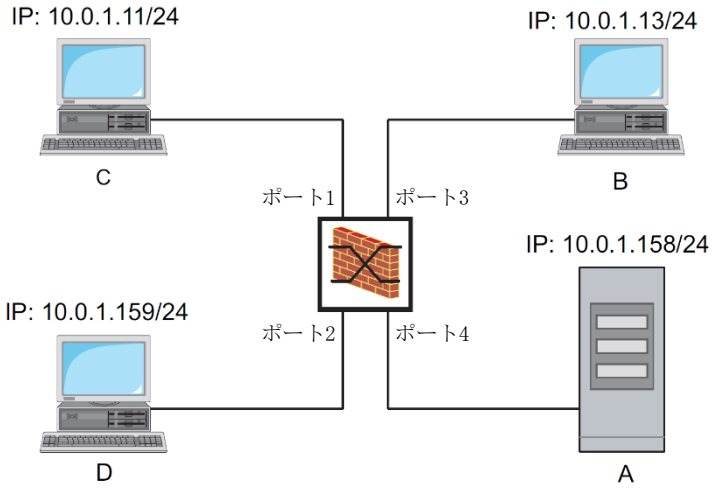


図22　IP ACLの例

以下の手順を実行します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`ip access-list extended name filter1 deny src 10.0.1.11-0.0.0.0 dst 10.0.1.158-0.0.0.0 assign-queue 1`	IP ACL を`filter1`の名で追加します。`10.0.1.11` から`10.0.1.158`までのIPデータパケットを拒否するルールを追加します。Priority `1` （最も高い優先順位）。
`ip access-list extended name filter1 permit src any dst any`	IPデータパケットを許可するルールをIP ACLに追加します。
`show access-list ip filter1`	IP ACL `filter1`のルールを表示します。
`ip access-list extended name filter2 deny src 10.0.1.13-0.0.0.0 dst 10.0.1.158-0.0.0.0 assign-queue 1`	IP ACL を`filter2`の名で追加します。`10.0.1.13` から`10.0.1.158`までのIPデータパケットを拒否するルールを追加します。Priority `1` （最も高い優先順位）。
`show access-list ip filter2`	IP ACL `filter2`のルールを表示します。

9.2.3 MACルールの作成・編集

MACデータパケットをフィルターする際、ユーザーは以下を実行できます。

- 新規グループやルールの作成
- 既存グループに新規ルールを追加
- 既存ルールの編集
- グループやルールのアクティベーション・ディアクティベーション
- 既存グループやルールの削除
- 既存ルールの順番の変更

以下の手順を実行します。

- ☐ *Network Security > ACL > MAC Rule* ダイアログボックスを開きます。
- ☐  ボタンをクリックします。
  ダイアログが*Create* ウィンドウを表示します。
- ☐ グループを作成するには、*Group name* フィールドに分かりやすい名前を入力します。1つのグループに複数のルールを組み合わせることができます。
- ☐ 既存のグループにルールを追加する場合、*Group name* フィールドのグループ名を選択します。
- ☐ *Index* フィールドで、ACL内のルール番号を指定します。この番号はルールの優先順位を決定するものです。
- ☐ *Ok* ボタンをクリックします。
  デバイスはルールをテーブルに追加します。グループ及びロールは即時に有効となります。
  グループ又はルールを無効化する場合、*Active* カラムのチェックボックスからチェックを外します。ルールを削除する場合、対象のテーブルエントリーにハイライトを入れ、
   ボタンをクリックします。
- ☐ テーブルのルールパラメーターを編集します。
  値を変更するには、任意のフィールドをダブルクリックします。
- ☐  ボタンをクリックし、変更を一時的に保存します。

注記： *Source MAC address* 及び *Destination MAC address* フィールドに、次の形式（`FF:??:??:??:??:??` 又は `??:??:??:??:00:01` ）でワイルドカードを使用することができます。ここでは大文字を使用します。

9.2.4 コマンドラインインターフェースを使用したMAC ACLの作成・コンフィグレーション

以下の例では、AppleTalk 及び IPX がネットワーク全体からフィルターで拒否されます。以下の手順を実行します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`mac acl add 1 macfilter`	MAC ACL を、ID `1` 及び名前 `macfilter`で追加します。
`mac acl rule add 1 1 deny src any any dst any any etype appletalk`	MAC ACL の Position `1` に ID `1` を追加し、EtherType `0x809B (AppleTalk)`のパケットを拒否します。
`mac acl rule add 1 2 deny src any any dst any any etype ipx-old`	MAC ACL の Position `2` に ID `1` を追加し、EtherType `0x8137 (IPX alt)`のパケットを拒否します。
`mac acl rule add 1 3 deny src any any dst any any etype ipx-new`	MAC ACL の Position `3` に ID `1` を追加し、EtherType `0x8138 (IPX)`のパケットを拒否します。
`mac acl rule add 1 4 permit src any any dst any any`	MAC ACLのPosition `4` に ID `1` を追加し、パケットを転送します。
`show acl mac rules 1`	ID `1`のMAC ACLのルールを表示します。
`interface 1/1,1/2,1/3,1/4,1/5,1/6`	`1/1` から `1/6`までのインターフェースのInterface Configuration mode に変更します。

`acl mac assign 1 in 1`	ID `1` のMAC ACLを、`1/6` から `in`までのインターフェースの受信データパケット（`1/1`）に割当てます。
`exit`	Interface modeから退出します。
`show acl mac assignment 1`	ID `1` のMAC ACLからインターフェース又はVLANへのアサインメントを表示します。

9.2.5 ACLをポート又はVLANに指定

ポート又はVLANにACLを指定した場合には以下のオプションがあります。
- ポート又はVALNを選択。
- ACLの優先順位の指定。
- グループ名を使ってACLを指定。

以下の手順を実行します。

- ☐ *Network Security > ACL > Assignment* ダイアログボックスを開きます。
- ☐  ボタンをクリックします。
  ダイアログが*Create* ウィンドウを表示します。
  - ☐ *Port/VLAN* フィールドに、任意のポート又はVLANを指定します。
  - ☐ *Priority* フィールドに、優先順位を指定します。
  - ☐ *Direction* フィールドに、デバイスにルールを適用させるデータパケットを指定します。
  - ☐ *Group name* フィールドに、デバイスがポート又はVLANに割当てるルールを指定します。
- ☐ *Ok* ボタンをクリックします。
- ☐  ボタンをクリックし、変更を一時的に保存します。

9.3 MAC認証バイパス

*MAC 認証バイパス*機能により、プリンターやFAX機等の802.1Xがサポートされていないクライアントでもデバイスを使ってネットワークを認証することができます。当デバイスでは、RADIUSサーバー上のクライアントを認証するMACアドレスのフォーマットを指定することができます。

例：

MACアドレスをそれぞれ2文字・6グループに分割します。大文字を使用し、セパレーターにはコロンを使用します。`AA:BB:CC:DD:EE:FF`

パスワードは`xY-45uM_e`です。以下の手順を実行します。

- ☐ *Network Security > 802.1X Port Authentication > Global* ダイアログボックスを開きます。*MAC authentication bypass format options* フレームで、以下の手順を実行します。
- ☐ *Group size* ドロップダウンリストで、値*2*を選択します。
  デバイスはMACアドレスをそれぞれ2文字・6グループに分割します。
- ☐ *Group separator* ドロップダウンリストで、記号*:* を選択します。
- ☐ *Upper or lower case* ドロップダウンリストで、*upper-case* 項目を選択します。
- ☐ *Password* フィールドに、パスワード`xY-45uM_e`を入力します。
  デバイスは、RADIUSサーバーを認証するクライアント全てにパスワードを使用します。フィールドが空のままだと、デバイスはフォーマットされたMACアドレスをパスワードに使用することもできます。
- ☐ ☑ ボタンをクリックし、設定を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`dot1x mac-authentication-bypass format group-size 2`	グループサイズ`2`を指定します。
`dot1x mac-authentication-bypass format group-separator :`	セパレーター`:`を指定します。
`dot1x mac-authentication-bypass format letter-case upper-case`	認証データは大文字フォーマットとするよう指定します。
`dot1x mac-authentication-bypass password xY-45uM_e`	パスワード`xY-45uM_e`を指定します。デバイスは、RADIUSサーバーの全クライアントにこのパスワードを使用します。

10 ネットワーク負荷の制御

当デバイスには、ネットワーク負荷を軽減するための様々な機能があります。
- パケットの直接通信分配
- マルチキャスト
- Rate limiter（レートリミッター）
- Prioritization - QoS （優先制御）
- フローコントロール

10.1 パケットの直接通信分配

当デバイスはパケットの直接通信分配によりネットワーク負荷を軽減します。

デバイスは各ポートで、受信したデータパケットの送信元MACアドレスを学習します。デバイスは「ポート及びMACアドレス」を組み合わせて自身のMACアドレステーブル（FDB）に保存します。

Store and Forward（保存して転送）法を適用することで、デバイスは受信データをバッファし、転送に先立ってその有効性を検証します。デバイスは無効及び不具合データパケットを拒否します。

10.1.1 MACアドレスの学習

デバイスがデータパケットを受信すると、送信元のMACアドレスがMACアドレステーブル（FDB）に保存されているかを確認します。送信元のMACアドレスが不明の場合、デバイスは新たなエントリーを作成します。次に、デバイスは宛先のMACアドレスと、MACアドレステーブル（FDB）に保存されているエントリーとを比較します。
- デバイスは既知の宛先MACアドレスを、このMACアドレスからデータパケットを過去に受信したことあるポートに転送します。
- デバイスは宛先アドレスが不明のデータパケットをフラッディングします。具体的には、デバイスがこれらデータパケットを全てのポートに転送します。

10.1.2 学習したMACアドレスのエージング

調整可能な一定期間内（エージングタイム）にデバイスが検知しなかったアドレスは、MACアドレステーブル（FDB）から削除されます。リブート又はMACアドレステーブルのリセットをすると、MACアドレステーブル（FDB）のエントリーが削除されます。

10.1.3 静的アドレスのエントリー

送信元のMACアドレスを学習することに加え、当デバイスではMACアドレスを手動で送信することもできます。これらMACアドレスは設定された状態を維持しつつ、MACアドレステーブル（FDB）のリセットやデバイスがリブートされた際も残されます。

静的アドレスのエントリーにより、デバイスが選択したポートに直接データパケットを送信することができます。宛先ポートを指定しないと、デバイスはそのデータパケットを破棄します。

グラフィカルユーザーインターフェース又はコマンドラインインターフェース内の静的アドレスエントリーを管理します。

以下の手順を実行します。
☐ 静的アドレスエントリーを作成します。

☐ *Switching > Filter for MAC Addresses* ダイアログボックスを開きます。
☐ ユーザー設定可能なMACアドレスを追加します。
➢ ボタンをクリックします。
ダイアログが*Create* ウィンドウを表示します。
➢ *Address* フィールドに、宛先MACアドレスを指定します。
➢ *VLAN ID* フィールドに、VLANのIDを指定します。
➢ *Port* リストには、デバイスがデータパケットを転送する、指定されたVLANの指定宛先MACアドレスのポートを選択します。
Address フィールドにユニキャストMACアドレスを指定したら、ポートは1つだけ選択します。
Address フィールドにマルチキャストMACアドレスを指定したら、ポートは1つ又は複数選択します。
デバイスに宛先がMACアドレスのデータパケットを破棄させたい場合、いずれのポートも選択してはなりません。
➢ *Ok* ボタンをクリックします。
☐ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`mac-filter <MAC address> <VLAN ID>`	MACアドレス及びVLAN IDを含むMACアドレスフィルターを作成します。
`interface 1/1`	インターフェース`1/1`のInterface Configuration mode に変更します。
`mac-filter <MAC address> <VLAN ID>`	先に作成したMACアドレスフィルターにポートを割当てます。
`save`	不揮発性メモリ（`nvm`）にある設定を「選択」したコンフィグレーションプロファイルに保存します。

☐ 学習したMACアドレスを静的アドレスエントリーに変換します。

☐ *Switching > Filter for MAC Addresses* ダイアログボックスを開きます。
☐ 学習したMACアドレスを静的アドレスエントリーに変換するには、*Status* カラムに値`permanent`を選択します。
☐ ボタンをクリックし、変更を一時的に保存します。

☐ 静的アドレスエントリーを無効化します。

☐ *Switching > Filter for MAC Addresses* ダイアログボックスを開きます。
☐ 静的アドレスエントリーに無効化するには、*Status* カラムに値`invalid` を選択します。
☐ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`interface 1/1`	インターフェース`1/1`のInterface Configuration mode に変更します。
`no mac-filter <MAC address> <VLAN ID>`	ポートに指定したMACアドレスフィルターをキャンセルします。
`exit`	Configuration modeに切り替えます。
`no mac-filter <MAC address> <VLAN ID>`	MACアドレス及びVLAN IDを含むMACアドレスフィルターを削除します。
`exit`	Privileged Exec Modeに切り替えます。
`save`	不揮発性メモリ（`nvm`）にある設定を「選択」したコンフィグレーションプロファイルに保存します。

☐ 学習したMACアドレスを削除します。

☐ 学習したアドレスをMACアドレステーブル（FDB）から削除するには、*Basic Settings > Restart* ダイアログボックスを開き、*Reset MAC address table* ボタンをクリックします。

`clear mac-addr-table`	学習したアドレスをMACアドレステーブル（FDB）から削除します。

10.2 マルチキャスト

デフォルトでは、デバイスはマルチキャストアドレスのデータパケットをフラッディングします。具体的には、デバイスがこのデータパケットを全てのポートに転送します。これにより、ネットワーク負荷が増加します。

IGMPスヌーピングを使用するとマルチキャストによるネットワーク負荷を軽減することができます。IGMPスヌーピングは、マルチキャストに「関心のある」デバイスが接続されたポートに対してのみ、マルチキャストデータパケットを送信させます。

10.2.1 マルチキャストの適用例

監視カメラは、画像を機械室及びモニター室のモニターに画像を伝送します。IPマルチキャスト伝送では、カメラはグラフィックデータをマルチキャストパケットとしてネットワークに伝送します。

IGMP（Internet Group Management Protocol）は、マルチキャストルーター及びモニター間のマルチキャストデータトラフィックを管理します。ネットワーク上のマルチキャストルーター及びモニター間のスイッチは、IGMPデータトラフィックを継続的に監視しています（「IGMPスヌーピング」）。

スイッチ類はマルチキャストストリームを受信すると、ログインを記録します（IGMPレポート）。すると、デバイスはMACアドレステーブル（FDB）にエントリーを作成し、過去にIGMPレポートを受信したことあるポートのみに対してマルチキャストパケットを転送します。

10.2.2 IGMPスヌーピング

IGMP（Internet Group Management Protocol）は、ルーターからレイヤー3の接続済みレシーバー間にマルチキャスト情報を配送します。IGMPスヌーピングは、スイッチが継続的にIGMPトラフィックを監視し、当該データトラフィックの伝送設定を最適化する機能のことです。

当デバイスでの*IGMPスヌーピング*機能は、RFC 4541の記載（Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches）に基づき作動します。

アクティブな*IGMP*機能のあるマルチキャストルーターは、関連するIPマルチキャストグループメンバーを決定するために、定期的にマルチキャストストリームの登録リクエスト（クエリー）を行います。IPマルチキャストグループメンバーは、レポートメッセージで返信します。レポートメッセージは、*IGMP*機能に要するパラメーターを含みます。マルチキャストルーターはルーティングテーブルに、レポートメッセージにあるIPマルチキャストグループアドレスを入力します。これにより、当該IPマルチキャストグループのデータパケットは、ルーティングテーブルに基づくアドレスフィールドの宛先に対し、データパケットが転送されます。

マルチキャストグループ（IGMP version2以降）を脱退すると、レシーバーは「Leave」メッセージをログし、これ以降レポートメッセージを送信しなくなります。一定時間（エイジングタイム）内にこのレシーバーからレポートメッセージを受信しないと、マルチキャストルーターはレシーバーのルーティングテーブルエントリーを削除します。

同ネットワーク上に複数のIGMPマルチキャストルーターがある場合、より小さいIPアドレスのデバイスがクエリー機能を引き継ぎます。ネットワーク上にマルチキャストルーターが無い場合、ユーザーは適正な装備のスイッチにクエリー機能を付すことができます。

マルチキャストレシーバー1つをマルチキャストルーターに繋ぐスイッチは、IGMPスヌーピングを使用してIGMP情報を分析します。

IGMPスヌーピングにより、スイッチが*IGMP*機能を使うことが可能となります。スイッチは、マルチキャストレシーバーのIPアドレスから生成したMACアドレスを、MACアドレステーブル（FDB）にある認識済みのマルチキャストアドレスとして保存します。また、スイッチは特定のマルチキャストアドレスからレポートを受信したポートを識別することもできます。これにより、スイッチはマルチキャストパケットを、マルチキャストレシーバーが接続されたポートのみに転送します。他のポートはこれらパケットを受信することはありません。

当デバイスの特殊な機能として、不明なマルチキャストアドレスのデータパケット処理を判定できる可能性があります。設定によっては、デバイスはこれらデータパケットを破棄するか、或いは全てのポートに転送します。デフォルトでは、データパケットを接続デバイスのあるポートのみに伝送し、これらポートがクエリーパケットを受信します。また、ユーザーは既知のマルチキャストパケットをクエリーされたポートに、追加で送信することも可能です。

IGMPスヌーピングの設定

以下の手順を実行します。

- ☐ *Switching > IGMP Snooping > Global* ダイアログボックスを開きます。
- ☐ 機能を有効化するには*Operation* フレームの*On* のラジオボタンを選択します。*IGMP Snooping* 機能が無効化されると、デバイスは以下のアクションを起こします。
  - ➢ 受信したクエリー及びレポートメッセージを無視します。
  - ➢ 受信したマルチキャストアドレスのデータパケットを、宛先アドレスを全ポートとして転送します。
- ☐ ボタンをクリックし、変更を一時的に保存します。

☐ ポートの設定を行います。

- ☐ *Switching > IGMP Snooping > Configuration* ダイアログボックスの*Port* タブを開きます。
- ☐ ポートの*IGMP Snooping*機能を有効化するには、当該ポートの*Active* カラムのチェックボックスにチェックを入れます。
- ☐ ボタンをクリックし、変更を一時的に保存します。

☐ VLANの設定を行います。

- ☐ *Switching > IGMP Snooping > Configuration* ダイアログボックスの*VLAN ID* タブを開きます。
- ☐ 特定のVLANの*IGMP Snooping*機能を有効化するには、当該VLANの*Active* カラムのチェックボックスにチェックを入れます。
- ☐ ボタンをクリックし、変更を一時的に保存します。

IGMPクエリア機能を設定する

デバイスは随意にアクティブなクエリーメッセージを自身で送信します。また、その代替としてクエリーメッセージに応答するか、ネットワーク上の他のマルチキャストクエリアを検知も行います（*IGMP Snooping Querier* 機能）。

条件：

IGMP Snooping 機能を全域で有効化します。

以下の手順を実行します。

- ☐ *Switching > IGMP Snooping > Querier*ダイアログボックスを開きます。
- ☐ *Operation* フレームで、*IGMP Snooping Querier* 機能をデバイス全域で有効化・無効化します。
- ☐ 特定のVLANの*IGMP Snooping Querier* 機能を有効化するには、当該VLANの*Active* カラムのチェックボックスにチェックを入れます。
  - ➢ デバイスは簡易な選定処理を実行します。もう片方のマルチキャストクエリアのIP送信元アドレスがこちらよちも小さい場合、デバイスはパッシブ状態へと切り替わるため、これ以降クエリーリクエストを送信しなくなります。
  - ➢ *Address* カラムに、生成されたクエリーリクエスト内の送信元アドレスとしてデバイスが挿入したIPマルチキャストアドレスを指定します。マルチキャストルーターのアドレスを使用してください。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

IGMPスヌーピングの拡張機能（テーブル）

Switching > IGMP Snooping > Snooping Enhancements ダイアログボックスでは、*IGMP Snooping* の拡張機能の設定にアクセスすることができます。VLAN内のポート毎の設定を、アクティベート・ディアクティベートすることができます。

以下の設定が可能となります。

- ➢ `Static`
  ポートを静的クエリーポートとして設定します。デバイスは、以前このポートでIGMPクエリーメッセージを受信したことがなくても、全てのIGMPメッセージを静的クエリーポートに転送します。静的（static）オプションが無効になっていても、デバイスが以前IGMPクエリーメッセージを受信したことがあれば、IGMPメッセージをこのポートに転送します。このケースでは、エントリーに`L` （Learned：学習済み）と表示されます。
- ➢ `Learn by LLDP`
  この設定のポートは他のシュナイダーエレクトリック製デバイスを、LLDP（Link Layer Discovery Protocol）を使用して自動検出することができます。すると、シュナイダーエレクトリック製デバイスからこのポートのIGMPクエリーステータスをデバイスが学習し、それに基づき*IGMP Snooping Querier* 機能の設定を行います。エントリー`ALA`は、`Learn by LLDP` 機能がアクティベートされたことを意味します。デバイスがVLANのこのポートに他のシュナイダーエレクトリック製デバイスを検知すると、エントリーに`A` （Automatic）が表示されます。
- ➢ `Forward All`
  この設定では、デバイスがマルチキャストアドレスを宛先とするデータパケットをそのポートに転送します。この設定は以下のような例では好ましいといえます。
  - – 診断目的。
  - – MRPリング上のデバイス類。リングを切り替えた後、マルチキャストを宛先アドレスとしたデータパケットのためにネットワークを再構成させてくれるのが、`Forward All` 機能です。全リングポートで`Forward All` 機能をアクティベートします。

条件：

IGMP Snooping 機能が全域で有効となっていなければなりません。

以下の手順を実行します。

- ☐ *Switching > IGMP Snooping > Snooping Enhancements* ダイアログボックスを開きます。
- ☐ 任意のVLANの、任意のポートをダブルクリックします。

☐ 更に1つ又は複数の機能をアクティベートするには、対応するオプションを選択します。
☐ *Ok* ボタンをクリックします。
☐ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`vlan database`	VLAN Configuration modeに切り替えます。
`igmp-snooping vlan-id 1 forward-all 1/1`	VLAN `1`のポート`1/1` の`Forward All` 機能をアクティベートします。

マルチキャストのコンフィグレーション

ユーザーは、マルチキャストデータパケットの交換について設定を行うことができます。データパケットを不明又は既知、いずれののマルチキャストレシーバーに送信するべきかによって、当デバイスは異なるオプションを提示します。

不明マルチキャストアドレスについての設定は、全デバイスで全域に渡ります。以下のオプションを選択することができます。
➢ 不明マルチキャストをデバイスが破棄します。
➢ 不明マルチキャストをデバイスが全ポートに転送します。

注記：不明マルチキャストアドレスの交換の設定は、Local Network Control Block（`224.0.0.0..224.0.0.255`）の予約IPアドレスにも適用することができます。このアクションは、高位のルーティングプロトコルにも影響します。

ユーザーは、既知のマルチキャストアドレスに対して個々にマルチキャストパケットを送信するよう、各VLANに指定できます。以下のオプションを選択することができます。
➢ デバイスは、既知のマルチキャストを過去にクエリーメッセージを受信したポート（クエリーポート）及び登録済みポートに転送します。登録済みポートとは、対応するマルチキャストグループのある登録済みマルチキャストレシーバーを意味します。このオプションにより、基本アプリケーションで更に設定されていないものにも伝送されます。
➢ デバイスは、既知のマルチキャストを登録済みポートのみに転送します。この設定の利点は、可能な帯域幅の範囲で最適な直接分配をすることです。

条件：

IGMP Snooping 機能が全域で有効となっていなければなりません。

以下の手順を実行します。

☐ *Switching > IGMP Snooping > Multicasts* ダイアログボックスを開きます。
☐ *Configuration* フレームで、デバイスがどのように不明マルチキャストアドレスにデータパケットを送信するかを指定します。
  ➢ *send to registered ports*
  不明マルチキャストアドレスのパケットを、デバイスが全クエリーポートに転送します。
☐ *Known multicasts* カラムで、デバイスがどのように対応するVLAN内の既知マルチキャストアドレスにデータパケットを送信するかを指定します。関連するフィールドをクリックし、任意の値を選択します。
☐ タンをクリックし、変更を一時的に保存します。

10.3 レート制限

レート制限（rate limiter）機能は、大量のデータトラフィック時でもポートのトラフィックを制限することで安定したオペレーションを実現します。レート制限は各ポートで個別に、また、インバウンド及びアウトバウンドトラフィックにも個別に実行されます。

ポートのデータ伝送レートが定義された制限を超過すると、デバイスはこのポートの過負荷分を破棄します。

レート制限はレイヤー2全域で実行されます。処理に際し、レート制限機能はIPやTCPなどの上位レベルのプロトコル情報は無視します。これはTCPトラフィックに影響を及ぼします。

この影響を最小化するには、以下のオプションを使用します。
- 例えばブロードキャスト、マルチキャスト、宛先アドレス不明のユニキャスト等、レート制限を一部の種類のパケットに限定します。
- インバウンドトラフィックではなく、アウトバウンドトラフィックを制限します。データパケットのデバイス内部バッファリングのため、アウトバウンドトラフィックのレート制限は、TCPフローコントロールと同時にすることで効果が向上します。
- 学習したユニキャストアドレスのエイジングタイムを増やします。

以下の手順を実行します。

☐ *Switching > Rate Limiter* ダイアログボックスを開きます。
- レートリミッターを有効にし、データ伝送レートの制限値を設定します。設定はポート毎を基本とし、トラフィックの種類によって細分化されます。
  - 受信したブロードキャストデータパケット
  - 受信したマルチキャストデータパケット
  - 受信した不明宛先アドレスのデータパケット

  ポートのレートリミッターを有効にするには、少なくとも1つのカテゴリーのチェックボックスにチェックを入れます。*Threshold unit* カラムで、デバイスが閾値をポート帯域幅のパーセンテージで解釈するか、又はパケット毎秒（pps）で解釈するかを、指定します。閾値`0` はレート制限を無効化します。

☐ ☑ ボタンをクリックし、変更を一時的に保存します。

10.4 QoS ・優先制御

QoS （Quality of Service）とは、IEEE 802.1Dに定義されたネットワークにリソースを分配するための手順です。QoSにより、必要となるアプリケーションのデータを優先させることができます。

ネットワーク負荷が高い場合には、遅延感度の高いデータトラフィックに低優先のデータトラフィックが干渉されるのを防ぐのに役立ちます。遅延感度の高いデータトラフィックには、例えば音声、動画、リアルタイムデータなどがあります。

10.4.1 優先制御

当デバイス内でデータトラフィックがクラス分けさることで、データトラフィックの優先制御が行われます。デバイスは高いトラフィックのクラスを低いトラフィックのクラスに優先します。トラフィックのクラス数はデバイスによります。

遅延感度の高いデータのデータフローを最適化するために、このようなデータは高いクラスのトラフィックを指定してください。遅延感度が低いデータであれば、低クラスのトラフィックを指定します。

データにトラフィッククラスを割当て

当デバイスは、インバウンドデータにトラフィックのクラスを定義しています（トラフィッククラス）。デバイスは以下のクラス分けを基準としています。

- デバイスが受信したデータパケットをトラフィッククラスに割当てるには、以下の方法に基づきます。
  - `trustDot1p`
    デバイスは、VLANタグ内のデータパケットの優先順位を使用します。
  - `trustIpDscp`
    デバイスは、IPヘッダー（ToS/DiffServ）内のQoS情報を使用します。
  - `untrusted`
    デバイスは、データパケット内にあり得る優先情報を無視し、直接受信ポートの優先順位を使用します。
- 受信ポートに割当てられた優先順位。

いずれのクラス分け基準を設定可能です。

トラフィックのクラス分け中、デバイスは以下のルールを適用しています。

- 受信ポートが`trustDot1p` （デフォルト）に設定されている場合、デバイスは、VLANタグ内のデータパケットの優先順位を使用します。データパケットにVLANタグが含まれない場合、デバイスは受信ポートの優先順位に導かれます。
- 受信ポートが`trustIpDscp`に設定されている場合、デバイスは、IPヘッダー（ToS/DiffServ）内のQoS情報を使用します。データパケットにIPパケットが含まれない場合、デバイスは受信ポートの優先順位に導かれます。
- 受信ポートが`untrusted`に設定されている場合、デバイスは受信ポートの優先順位に導かれます。

トラフィッククラスの優先制御

トラフィッククラスの優先制御に、デバイスは以下のルールを適用しています。

- `Strict`
  より高トラフィッククラスのデータ伝送がされていない場合や、データがまだキュー（queue）で待機している場合、デバイスは対応するトラフィッククラスのデータを送信します。どのトラフィッククラスも`Strict` 法によって優先制御されていて、ネットワークが高負荷にある場合は、デバイスが低クラスのトラフィックを恒久的にブロックします。
- `WFQ (Weighted Fair Queuing)`
  トラフィッククラスは、特定の帯域幅が割当てられています。これにより、高クラスのトラフィックに膨大なデータトラフィックがあったとしても、デバイスはこのトラフィッククラスのデータトラフィックを送信することができます。

10.4.2 受信した優先情報の取扱い

アプリケーション類は、データパケットに以下の優先情報のラベル付けをします。

- IEEE 802.1Q/ 802.1D （レイヤー2）に基づく VLAN 優先情報
- ToS（Type-of-Service）又は VLAN Management IPパケット（レイヤー3）用 DSCP（DiffServ）

ユーザーは以下のオプションを使用して優先情報を評価することができます。

- `trustDot1p`
  デバイスが、VLANタグが付いたデータパケットを、VLAN優先情報に基づき異なるトラフィッククラスに割当てます。これに付随する割当ては、設定可能です。デバイスは受信ポートの優先順位をVLANタグのないデータパケットに割当てます。
- `trustIpDscp`
  デバイスは、パケットにVLANタグが付いているにも関わらず、IPヘッダー内のDSCP値に基づいた異なるトラフィッククラスにIPパケットを割当てます。これに付随する割当ては、設定可能です。デバイスは受信ポートの優先情報に基づき、非IPパケットを優先します。
- `untrusted`
  デバイスは、データパケット内の優先情報を無視し、受信ポートの優先順位を割当てます。

10.4.3 VLANタグ付け

VLAN及び優先制御機能については、MACフレームとVLANタグの統合についてIEEE 802.1Qで定められています。VLANタグは4バイトで構成され、送信元アドレスフィールド（Source Address Field）及び種別フィールド（Length / Type Field）に間にあります。

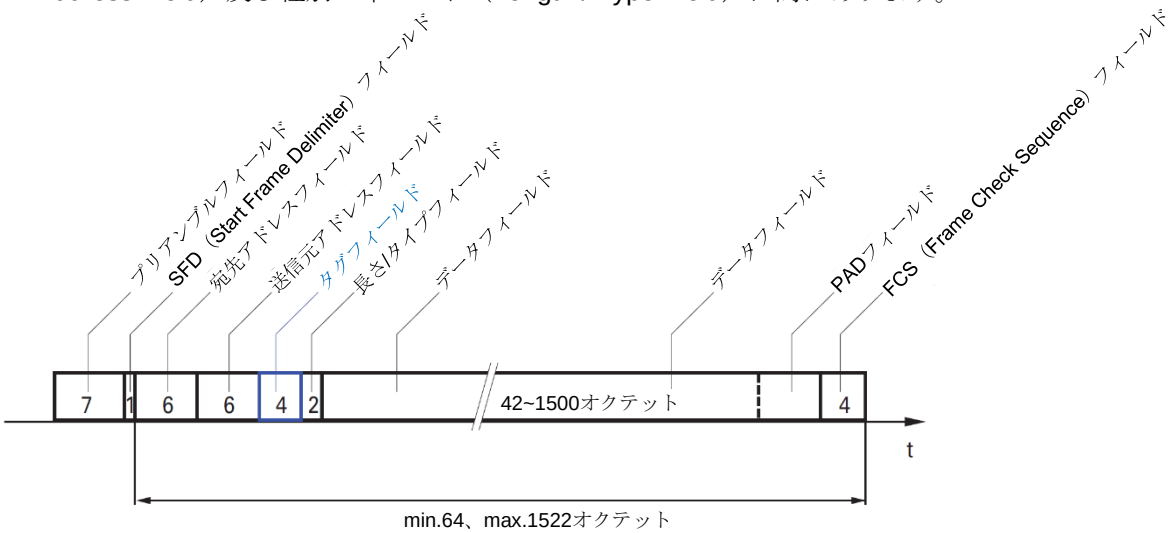


図23 イーサネット・タグ付きデータパケット

VLANタグが付いたデータパケットについて、デバイスは以下を検証します。
- ➢ 優先情報
- ➢ VLANが設定されていれば、VLANタグ付け

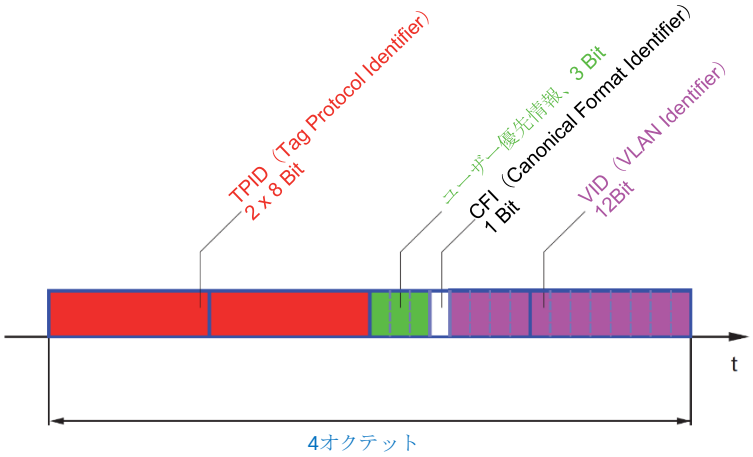


図24　VLANタグ付けの構造

優先情報を含むVLANタグの付いたデータパケットで、VLAN情報を持たないもの（VLAN ID =0）は、Priority Tagged Frames（優先順位タグ付けフレーム）と呼ばれます。

注記：ネットワークプロトコル及び冗長メカニズムは、最も高いトラフィッククラス7を使用します。従って、アプリケーションデータには他のトラフィッククラスを使用してください。

VLANを優先する場合、以下の特殊機能を考慮しなければなりません。
- ➢ End-to-end 優先制御は、VLANタグをネットワーク全域に伝送しなければなりません。全てのネットワーク機器がVLANに対応していることが条件となります。
- ➢ ルーターは、VLANをタグ付けしてポートベースのルーターインターフェースを介したパケットの送受信をすることはできません。

10.4.4 IP ToS (Type of Service)

IPヘッダー内のToS（Type of Service）フィールドは、当初よりIPプロトコルの一部で、IPネットワークの異なるサービスを区別するために使用します。限定的な帯域幅及び不安定な接続パス故に、その当初でさえIPパケットを区別して処理する案は存在していました。有用可能な帯域幅が広がり続けたため、今ではToSフィールドを使用する必要はなくなりました。

しかし、今現在のネットワークではリアルタイムでの要件があるため、再度ToSフィールドが重要になりました。IPヘッダーのToSバイトを選択することで、異なるサービスを区別することができます。但し、実際に広く使われているフィールドとはいえません。

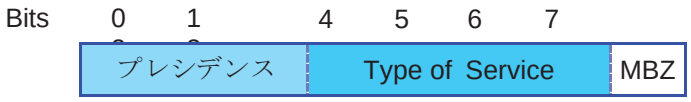


表22　IPヘッダー内のToSフィールド

Bits (0-2):IPプレシデンス　定義	Bits (3-6):Type of Service　定義	Bit (7)
111 - ネットワーク制御	0000 - [all normal]	0 - ゼロ
110 - インターネットワーク制御	1000 - [minimize delay]	
101 - CRITIC / ECP	0100 - [maximize throughput	

表22　*IPヘッダー内のToSフィールド*（続き）

Bits (0-2):IPプレシデンス　定義	Bits (3-6):Type of Service　定義　Bit (7)
100 – フラッシュオーバーライド	0010 – [maximize reliability]
011 – フラッシュ	0001 – [minimize monetary cost]
010 – 即時	
001 - 優先	
000 - ルーチン	

10.4.5　トラフィッククラスの取扱い

トラフィッククラスの取扱いに、デバイスは以下のオプションを提示します。
- SP (Strict Priority)
- WFQ (Weighted Fair Queuing)
- SPとWFQの組合せ
- Queue Management

Strict Priority

SP（Strict Priority：絶対優先）設定では、デバイスは最初に高クラスのトラフィック（高優先）のデータパケットを、次点の高クラストラフィックのデータパケットに先立って伝送します。キューに他のデータパケットが残っていない場合、デバイスは最も低いクラスのトラフィック（優先度最低）のデータパケットを伝送します。不運なケースとして、膨大な量の高優先トラフィックがこのポートで伝送を待機している場合、デバイスは優先度の低いパケットを伝送しません。

VoIPや動画などの遅延感度の高いアプリケーションでは、SPはデータを即時に伝送します。

Weighted Fair Queuing

WFQ（Weighted Fair Queuing：重み付き公平キューイング）、別名WRR（Weighted Round Robin）では、ユーザーは最小帯域幅又は予約帯域幅を各トラフィッククラスに割当てます。これは低優先のデータパケットも、ネットワークが渋滞していても伝送されるようアシストしています。

帯域幅の予約値は使用可能な帯域幅の0%から100%を1%で刻みます。
- 予約値0は、「帯域幅無し」（no bandwidth）設定に相当します。
- 個々の帯域幅の合計は100%までです。

WFQを全トラフィッククラスに割当てると、対応ポートの全帯域幅が使用可能になります。

SPとWFQの組合せ

WFQをSPと組み合わせる場合、WFQの高トラフィッククラスがSPの低トラフィッククラスよりも低いことを確認してください。

WFQとSPを組み合わせると、高負荷のSPネットワークがWFQが使用する帯域幅を大きく低減させてしまう可能性があります。

10.4.6 Queue Management

Queue Shaping

Queue Shaping（キューシェーピング）とは、キューがパケットを伝送するレートを調整することです。例えばQueue Shapingを使用すると、高位SPのキューのレートを制限することで、高優先パケットの伝送が可能なのにも関わらず、低位SPキューにパケットを伝送させることができます。当デバイスでは如何なるキューでもQueue Shapingが設定できます。使用可能な帯域幅のパーセンテージを、トラフィックがキューを通過する最大レートとするQueue Shapingを、ユーザーが指定することができます。

Queue Managementの設定

以下の手順を実行します。

- ☐ *Switching > QoS/Priority > Queue Management* ダイアログボックスを開きます。

Min. bandwidth [%] カラムの割当て帯域幅の合計は100%です。

- ☐ *Traffic class* = 0のWFQをアクティベートするには、以下の手順を進めます。
  - ➢ *Strict priority* カラムのチェックボックスのチェックを外します。
  - ➢ *Min. bandwidth [%]* カラムに値5を指定します
- ☐ *Traffic class* = 1のWFQをアクティベートするには、以下の手順を進めます。
  - ➢ *Strict priority* カラムのチェックボックスのチェックを外します。
  - ➢ *Min. bandwidth [%]* カラムに値20を指定します
- ☐ *Traffic class* = 2のWFQをアクティベートするには、以下の手順を進めます。
  - ➢ *Strict priority* カラムのチェックボックスのチェックを外します。
  - ➢ *Min. bandwidth [%]* カラムに値30を指定します
- ☐ *Traffic class* = 3のWFQをアクティベートするには、以下の手順を進めます。
  - ➢ *Strict priority* カラムのチェックボックスのチェックを外します。
  - ➢ *Min. bandwidth [%]* カラムに値20を指定します
- ☐ *Traffic class* = 4のWFQ及びQueue Shapingをアクティベートするには、以下の手順を進めます。
  - ➢ *Strict priority* カラムのチェックボックスのチェックを外します。
  - ➢ *Min. bandwidth [%]* カラムに値10を指定します
  - ➢ *Max. bandwidth [%]* カラムに値10を指定します

  特殊なトラフィッククラスにWFQ及びQueue Shapingを組み合わせて使用する場合、*Min. bandwidth [%]* カラムに指定した値よりも*Max. bandwidth [%]* カラムの値を高くします。
- ☐ *Traffic class* = 5のWFQをアクティベートするには、以下の手順を進めます。
  - ➢ *Strict priority* カラムのチェックボックスのチェックを外します。
  - ➢ *Min. bandwidth [%]* カラムに値5を指定します
- ☐ *Traffic class* = 6のWFQをアクティベートするには、以下の手順を進めます。
  - ➢ *Strict priority* カラムのチェックボックスのチェックを外します。
  - ➢ *Min. bandwidth [%]* カラムに値10を指定します
- ☐ *Traffic class* = 7のSP及びQueue Shapingをアクティベートするには、以下の手順を進めます。
  - ➢ *Strict priority* カラムのチェックボックスにチェックを入れます。
  - ➢ *Max. bandwidth [%]* カラムに値10を指定します
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

```
enable                                  Privileged Exec Modeに切り替えます。
configure                               Configuration modeに切り替えます。
cos-queue weighted 0                    トラフィッククラス0にWFQを有効化します。
cos-queue min-bandwidth:0 5             トラフィッククラス0に重量5 %を指定します。
cos-queue weighted 1                    トラフィッククラス1にWFQを有効化します。
cos-queue min-bandwidth:1 20            トラフィッククラス1に重量20 %を指定します。
cos-queue weighted 2                    トラフィッククラス2にWFQを有効化します。
cos-queue min-bandwidth:2 30            トラフィッククラス2に重量30 %を指定します。
cos-queue weighted 3                    トラフィッククラス3にWFQを有効化します。
cos-queue min-bandwidth:3 20            トラフィッククラス3に重量20 %を指定します。
show cos-queue
Queue Id Min. bandwidth Max. bandwidth Scheduler type
-------- -------------- -------------- --------------
                      0  5      0       weighted
                      1  20     0       weighted
                      2  30     0       weighted
                      3  20     0       weighted
                      4  0      0       strict
                      5  0      0       strict
                      6  0      0       strict
                      7  0      0       strict
```

WFQとQueue Shapingの組合せ

以下の手順を実行します。

```
enable                                  Privileged Exec Modeに切り替えます。
configure                               Configuration modeに切り替えます。
cos-queue weighted 4                    トラフィッククラス4にWFQを有効化します。
cos-queue min-bandwidth:4 10            トラフィッククラス4に重量10 %を指定します。
cos-queue max-bandwidth:4 10            トラフィッククラス4に重量10 %を指定します。
cos-queue weighted 5                    トラフィッククラス5にWFQを有効化します。
cos-queue min-bandwidth:5 5             トラフィッククラス5に重量5 %を指定します。
cos-queue weighted 6                    トラフィッククラス6にWFQを有効化します。
cos-queue min-bandwidth:6 10            トラフィッククラス6に重量10 %を指定します。
show cos-queue
Queue Id Min. bandwidth Scheduler type
-------- -------------- -------------- --------------
                      0  5      0       weighted
                      1  20     0       weighted
                      2  30     0       weighted
                      3  20     0       weighted
                      4  10     10      weighted
                      5  5      0       weighted
                      6  10     0       weighted
                      7  0      0       strict
```

Queue Shapingの設定

以下の手順を実行します。

```
enable                                  Privileged Exec Modeに切り替えます。
configure                               Configuration modeに切り替えます。
cos-queue max-bandwidth:7 10            トラフィッククラス7に重量10 %を指定します。
show cos-queue
Queue Id    Min. bandwidth   Scheduler type
--------    --------------   --------------   -------------
0           5                0                weighted
1           20               0                weighted
2           30               0                weighted
3           20               0                weighted
4           10               10               weighted
5           5                0                weighted
6           10               0                weighted
7           0                10               strict
```

10.4.7 パケット管理の優先制御

ユーザーがデバイス管理に常時アクセスできるよう、ネットワークが高負荷でもユーザーは管理パケットの優先制御を行えます。

管理パケットの優先制御の際には、デバイスから管理パケットの優先情報が送信されます。

- デバイスはレイヤー2のVLANタグ内の優先情報を変更します。
  この機能を使用する条件として、対応ポートがVLANタグ付けされたパケットを送信できるよう許可されていなければなりません。
- デバイスはレイヤー3のIP-DSCP値を変更します。

10.4.8 優先順位の設定

ポートの優先制御

以下の手順を実行します。

- ☐ *Switching > QoS/Priority > Port Configuration* ダイアログボックスを開きます。
- ☐ *Port priority* カラムに、VLANタグの無いデータパケットを受信したポートからデバイスがパケットを転送する優先順位を指定します。
- ☐ *Trust mode* カラムに、デバイスが受信したデータパケットにトラフィッククラスを割当てる際に使用する基準を指定します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`interface 1/1`	インターフェース`1/1`のInterface Configuration mode に変更します。
`vlan priority 3`	インターフェース `1/1` に port priority `3`を指定します。
`exit`	Configuration modeに切り替えます。

トラフィッククラスにVLAN優先順位を割当てる

以下の手順を実行します。

- ☐ *Switching > QoS/Priority > 802.1D/p Mapping*ダイアログボックスを開きます。
- ☐ トラフィッククラスにVLAN優先順位を割当てるには、*Traffic class*カラムに該当する値を挿入します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`classofservice dot1p-mapping 0 2`	トラフィッククラス`2`にVLAN優先順位`0` を指定します。
`classofservice dot1p-mapping 1 2`	トラフィッククラス`2`にVLAN優先順位`1` を指定します。
`exit`	Privileged Exec Modeに切り替えます。
`show classofservice dot1p-mapping`	割当てを表示します。

受信データパケットにポート優先順位を割当てる

以下の手順を実行します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`interface 1/1`	インターフェース`1/1`のInterface Configuration mode に変更します。
`classofservice trust untrusted`	インターフェースに`untrusted` mode を割当てます。
`classofservice dot1p-mapping 0 2` `classofservice dot1p-mapping 1 2`	トラフィッククラス`2`にVLAN優先順位`0` を指定します。トラフィッククラス`2`にVLAN優先順位`1` を指定します。
`vlan priority 1`	ポート優先順位に値`1` を指定します。
`exit`	Configuration modeに切り替えます。

```
exit
```
Privileged Exec Modeに切り替えます。

```
show classofservice trust
```
ポート・インターフェースのTrust modeを表示します。

```
 Interface Trust Mode
 --------- -------------
 1/1       untrusted
 1/2       dot1p
 1/3       dot1p
 1/4       dot1p
 1/5       dot1p
 1/6       dot1p
 1/7       dot1p
```

トラフィッククラスにDSCPを割当てる

以下の手順を実行します。

- ☐ *Switching > QoS/Priority > IP DSCP Mapping*ダイアログボックスを開きます。
- ☐ *Traffic class* カラムに任意の値を指定します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

```
enable
```
Privileged Exec Modeに切り替えます。

```
configure
```
Configuration modeに切り替えます。

```
classofservice ip-dscp-mapping cs1 1
```
トラフィッククラス1にDSCP値CS1 を割当てます。

```
show classofservice ip-dscp-mapping
```
IP DSCP の割当てを表示します。

```
    IP DSCP       Traffic Class
 -------------    -------------
   be                  2
   1                   2
   .                   .
   .                   .
   (cs1)               1
   .                   .
```

受信したIPデータパケットにDSCP優先順位を割当てる

以下の手順を実行します。

```
enable
```
Privileged Exec Modeに切り替えます。

```
configure
```
Configuration modeに切り替えます。

```
interface 1/1
```
インターフェース1/1のInterface Configuration mode に変更します。

```
classofservice trust ip-dscp
```
全域に trust ip-dscp mode を指定します。

```
exit
```
Configuration modeに切り替えます。

```
show classofservice trust
```
ポート・インターフェースのTrust modeを表示します。

```
 Interface    Trust Mode
 ----------   -------------
 1/1          ip-dscp
 1/2          dot1p
 1/3          dot1p
 .            .
 .            .
 1/5          dot1p
 .            .
```

ポートのトラフィックシェーピングのコンフィグレーション

以下の手順を実行します。

```
enable
```
Change to the Privileged EXEC mode.

```
configure
```
Configuration modeに切り替えます。

```
interface 1/2
```
インターフェース1/2のInterface Configuration mode に変更します。

```
traffic-shape bw 50
```
ポート1/2 の最大帯域幅を50%に制限します。

```
exit
```
Configuration modeに切り替えます。

```
exit
```
Privileged Exec Modeに切り替えます。

```
show traffic-shape
```
トラフィックシェーピングのコンフィグレーションを表示します。

```
Interface Shaping rate
--------- ------------
1/1       0 %
1/2       50 %
1/3       0 %
1/4       0 %
```

レイヤー2の管理優先順位のコンフィグレーション

以下の手順を実行します。

- ☐ *Switching > QoS/Priority > Global* ダイアログボックスを開きます。
- ☐ *VLAN priority for management packets* フィールドに、デバイスが管理データパケットを送信するVLANの優先順位を指定します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

```
enable
```
Privileged Exec Modeに切り替えます。

```
network management priority dot1p 7
```
管理パケットにVLAN優先順位 7 を割当てます。
デバイスは最優先の管理パケットを送信します。

```
show network parms
```
デバイス管理が配置されたVLANの優先順位を表示します。

```
Ipv4 Network
------------
…
Management VLAN priority. ..... 7
…
```

レイヤー3の管理優先順位のコンフィグレーション

以下の手順を実行します。

- ☐ *Switching > QoS/Priority > Global* ダイアログボックスを開きます。
- ☐ *IP DSCP value for management packets* フィールドに、デバイスが管理データパケットを送信するDSCP値を指定します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

```
enable
```
Privileged Exec Modeに切り替えます。

```
network management priority ip-dscp 56
```
管理パケットに値56 を割当てます。
デバイスは最優先の管理パケットを送信します。

```
show network parms
```
デバイス管理が配置されたVLANの優先順位を表示します。

```
Ipv4 Network
------------
…
Management IP-DSCP value. ..... 56
```

10.5 フローコントロール

大量のデータパケットを優先キューのポートで同時に受信すると、ポートのメモリーオーバーフローの原因となります。これが発生すると、例として、デバイスはギガビットポートでデータを受信してより低い帯域幅のポートに転送します。デバイスは余剰データパケットを破棄します。

フローコントロール・メカニズムはIEEE 802.3に定義されているように、ポートのメモリーオーバーフローによってデータパケットが失われないようサポートします。ポートのメモリーが満杯になる少し手前で、デバイスはこれ以上データパケットを受け付けていない接続デバイスに信号を送ります。

- Full-duplex modeでは、デバイスはPauseデータパケットを送信します。
- Half-duplex modeでは、デバイスはコリジョンのシミュレーションを実施します。

フローコントロールの仕組みを下図に表示します。Workstationの1・2・3は大量のデータをWorkstation 4に、同時に送信しようとしています。Workstation 1・2・3の帯域幅の合計は、Workstation 4のそれよりも大きくなります。これがポート4の受信キューにオーバーフローを起こします。左の漏斗がその状況を表現しています。

デバイスの、ポート1・2・3のフローコントロール機能が有効になっていれば、デバイスは漏斗がオーバーフローする前に反応することができます。右の漏斗はポート1・2・3が伝送デバイスにメッセージを送信して伝送速度を制御してる様を表現しています。結果として、受信ポートが対処できないような状況ではなくなり、受信トラフィックを処理できるようになります。

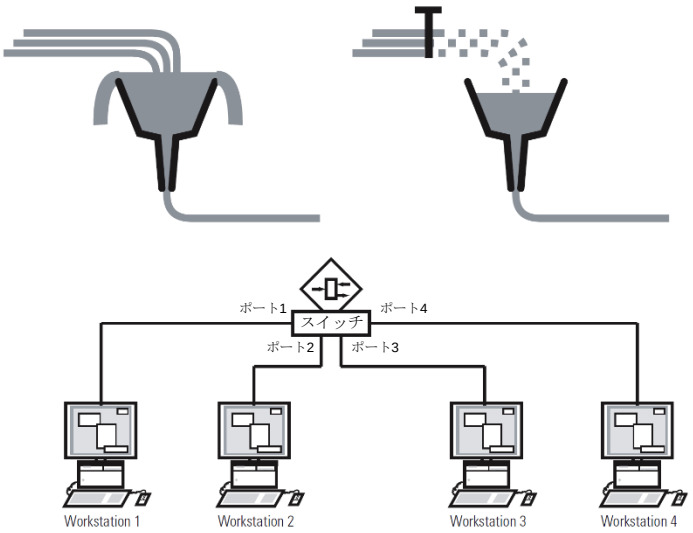


図25 フローコントロール例

10.5.1 全二重又は半二重リンク

半二重リンクのフローコントロール

上記の例で、Workstation 2とデバイスの間に半二重リンクがあると仮定します。

ポート2の送信キューがオーバーフローすると、デバイスはデータをWorkstation 2に返送します。Workstation 2はコリジョンを検知し、伝送を止めます。

全二重リンクのフローコントロール

上記の例で、Workstation 2とデバイスの間に全二重リンクがあると仮定します。

ポート2の送信キューがオーバーフローする前に、デバイスはWorkstation 2に、送信の間に短時間の中断を含めるようリクエストします。

10.5.2 フローコントロールの設定

以下の手順を実行します。

- ☐ *Switching > Global* ダイアログボックスを開きます。
- ☐ *Flow control* のチェックボックスにチェックを入れます。
  このように設定すると、デバイスのフローコントロールが有効となります。
- ☐ *Basic Settings > Port* ダイアログボックスの *Configuration* タブを開きます。
- ☐ ポートのフローコントロールを有効化するには、*Flow control* カラムのチェックボックスにチェックを入れます。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

注記：冗長機能を使用している場合、関連ポートのフローコントロールはディアクティベートします。フローコントロールと冗長機能が同時にアクティブな場合、冗長機能が意図したものと異なるオペレーションを行う可能性があります。

11 テンプレートに基づいたTSNのコンフィグレーション

11.1 基本事項

TSN 機能を使用すると、以下の基本条件が適用となります。

- デバイスはStore and Forward（保存して転送）法で稼働します。従って、デバイスが転送を決定するに先立ってデータパケットを完全に受信しなければなりません。
- Base time及びCycle timeを一度デバイス内で指定しなければなりません。いずれの設定も、TSNに関わる各ポートに対して有効です。
- ユーザーはセットアップを簡略化するために予め定義されたテンプレートに基づき、ポート毎のゲートコントロールリストを設定します。
- ゲートコントロールリストにあるエントリータイムの合計が、指定のサイクルタイムと同等又は小さいことを確認します。
- デバイスはガードバンドを使用して、高優先パケットのタイムスロットを、過去タイムスロットから「漏れた」パケットから保護します。ガードバンドのインターバル長の決定要素は、送信ポートの速度になります。

  ガードバンドのインターバル長として、以下を推奨します。数値はポート速度及びイーサネットパケットの最大許容サイズを基にしたものです。
  - 2.5 Gbit/s:5 µs
  - 1 Gbit/s:13 µs
  - 100 Mbit/s:124 µs
- サイクルタイムの幅は 50 000..10 000 000 ns です。
- ゲートコントロールリストのインターバル長の幅は 1 000..10000000ns です。
- サイクルタイム並びにゲートコントロールリストのインターバル長が、1 µs、2 µs、4 µs の倍数であることを確認します。

表23　サイクルタイムとデータ粒度間の依存性

サイクルタイム	データ粒度
50 µs..4 ms	1 µs
4.002 ms..8 ms	2 µs
8.004 ms..10 ms	4 µs

11.2 例：

ここの例では、デバイスを以下の条件シナリオでセットアップします。
- サイクルタイム=1ms
- 高優先パケットのタイムスロット=500µs
- 低優先パケットのタイムスロット=487µs

ここの例では、各デバイスはポート速度1 Gbit/s のネットワークに接続されています。

表24　サイクルの構造

タイムスロット	トラフィッククラス	継続時間
高優先パケット	7	500 µs
低優先パケット	0,1,2,3,4,5,6	487 µs
ガードバンド	–	13 µs

11.2.1 タイムの計算

デバイスは、低優先パケットのタイムスロットの継続時間を自動計算します。計算は以下のパラメーターに基づきます。
- サイクルタイム
- 高優先パケットのタイムスロット継続時間
- ガードバンドの継続時間

11.2.2 デバイスのセットアップ

既に指定されたタイムを使い、グラフィカルユーザーインターフェース又はコマンドラインインターフェースを使用してデバイスをセットアップします。関連する各デバイスに、以下の手順を実行します。

サイクルタイムを確認し、調整する

以下の手順を実行します。

- ☐ *Switching > TSN > Configuration* ダイアログボックスの*Port* タブを開きます。
- ☐ *Cycle time [ns]* フィールドの、*Configuration* フレームを確認します。
- ☐ 必要に応じ数値を調整します。

- ☐ ボタンをクリックし、変更を一時的に保存します。

```
enable                                  Privileged Exec Modeに切り替えます。
configure                               Configuration modeに切り替えます。
show tsn configuration
Port Status                 Conf. cycle time[ns]  Conf. base time
     Default gate states    Curr. cycle time[ns] Curr. base time
     Config change pending                       Time of last activation
---- -------------------- -------------------- ------------------------------

 1/1 [x]           disabled             1000000 1970-01-01  00:00:00.000000000
     7,6,5,4,3,2,1,0                    1000000 1970-01-01  00:00:00.000000000
     [ ]                                        2018-07-12  08:10:58.813000000

 1/2  [x]          disabled             1000000  1970-01-01  00:00:00.000000000
     7,6,5,4,3,2,1,0                    1000000  1970-01-01  00:00:00.000000000
     [ ]                                        2018-07-11  07:24:35.204000000

 1/3  [ ]          disabled             1000000  1970-01-01  00:00:00.000000000
     7,6,5,4,3,2,1,0                          0  1970-01-01  00:00:00.000000000
     [ ]                                        1970-01-01  00:00:00.000000000

 1/4  [ ]          disabled             1000000  1970-01-01  00:00:00.000000000
     7,6,5,4,3,2,1,0                          0  1970-01-01  00:00:00.000000000
     [ ]                                        1970-01-01  00:00:00.000000000

tsn cycle-time 1000000                  必要に応じ数値を調整します。
```

テンプレートを選択し、ゲートコントロールリストをセットアップする

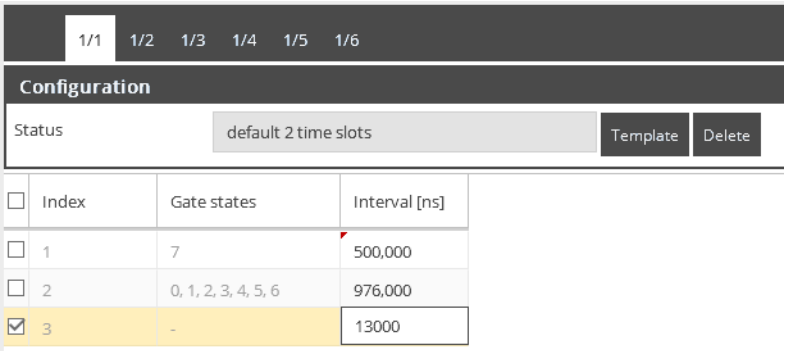
ゲートコントロールリストのセットアップのアシストとして、デバイスには予め定義されたテンプレートがあります。ここの例では、テンプレート*default 2 time slots*を使用します。テンプレートを選択したら、タイムスロットの継続時間を調整することができます。*TSN* 機能を使用したい各ポートに以下の手順を実行します。

以下の手順を実行します。

- ☐ *Switching > TSN > Gate Control List > Configured* ダイアログボックスを開きます。
- ☐ 設定したいポートのタブを選択します。

☐ *Configuration* フレームのテンプレートを選択します。以下の手順を実行します。
- *Template* ボタンをクリックします。
- *default 2 time slots* の項目を選択します。
- *Ok* ボタンをクリックします。

☐ *Interval [ns]* カラムの数値を調整します。
- 高優先パケットの行には 500000を入力します。
- ガードバンドの行には 13000 を入力します。
- 変更を保存する時に、3番目の数値をデバイスが自動で計算します。



☐ ✔ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`interface 1/1`	インターフェース 1/1 の Interface Configuration mode に変更します。
`tsn gcl modify 1 interval 500000`	高優先パケットには、タイムスロットの継続時間をナノ秒単位で調整します。
`tsn gcl modify 3 interval 13000`	ガードバンドには、タイムスロットの継続時間をナノ秒単位で調整します。 デバイスは、低優先パケットのタイムスロットの継続時間を自動計算します。ユーザーは低優先パケットのタイムスロットを設定することはできません。

12 VLAN

最も簡単なケースでは、バーチャルLAN（VLAN）は、1つのネットワークセグメント上のグループで個別のLANに属していいても、互いに通信できるネットワーク参加者で構成されています。

より複雑なVLANは、ネットワーク参加者間で論理的に（物理的である代わりに）複数のネットワークセグメントに展張したものです。VLANは柔軟なネットワークデザインの一要素となっています。ケーブル同士を接続させるよりも、一元的に論理的な接続を再構成する方が簡単になります。

VLAN 機能を定義したIEEE 802.1Qの規定に則り、当デバイスは独立したVLANラーニングをサポートします。

VLANを使用することで様々な利点があります。以下のリストに最も大きな利点を示します。

- ネットワーク負荷の制限
  バーチャルLAN内のみでデバイスが不明の（未学習の）宛先アドレスのブロードキャスト、マルチキャスト、ユニキャストパケットを伝送しつつも、VLANはネットワーク負荷を大幅に軽減することができます。その他データネットワークは、トラフィックを通常通りに転送します。
- 柔軟性
  ユーザーは、ネットワーク参加者の機能に基づいたユーザーグループを構築することができますが、参加者の物理的な位置や媒体はその限りではありません。
- 明確な構造
  VLANはネットワークの構造を明確にするため、保守性も上がります。

12.1 VLANの例

以下はVLAN構造の実例の概略です。

注記：VLANを設定する際、デバイス管理にアクセス可能な、変更することのないインターフェースを使用してください。ここの例では、インターフェース1/6又はシリアル接続でVLANの設定を行います。

12.1.1 例1

ここの例では、最小のVLANコンフィグレーション（ポートベースのVLAN）を示します。アドミニストレーターは複数のエンドデバイスを伝送デバイスに接続し、2つのVLANに割当てます。これはグループのVLANのみで通信するVLAN間のあらゆるデータ伝送を効果的に抑止します。

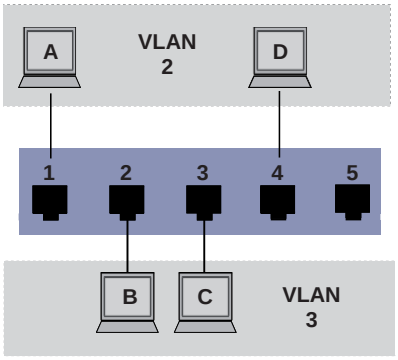


図26　簡易なポートベースのVLAN例

VLANをセットアップする際、各ポートに通信ルールとしてingress（イングレス＝上り）・egress（エグレス＝下り）テーブルを作成します。

Ingressテーブルは、ポートが受信データパケットにどのVLAN IDを割当てるかを指定するものです。従って、ユーザーはエンドデバイスのポートアドレスをVLANの割当てに使用します。

Egressテーブルは、デバイスがこのVLANからのパケットにどのポートを割当てるかを指定するものです。

- T = Tagged（タグ付け）　（タグフィールドあり、マーキングあり）
- U = Untagged（タグ無し）（タグフィールド無し、マーキング無し）

ここの例では、データパケットのタグフィールドのステータスは無関係の為、設定Uを使用します。

表25　Ingressテーブル

端末	ポート	PVID (Port VLAN Identifier)
A	1	2
B	2	3
C	3	3
D	4	2
	5	1

表26　Egressテーブル

VLAN ID	ポート				
	1	2	3	4	5
1					U
2	U			U	
3		U	U		

以下の手順を実行します。

☐ VLANのセットアップ

☐ *Switching > VLAN > Configuration* ダイアログボックスを開きます。

☐  ボタンをクリックします。
ダイアログが*Create* ウィンドウを表示します。

☐ *VLAN ID* フィールドに、値2を指定します。

☐ *Ok* ボタンをクリックします。

☐ VLANには、名前VLAN2を指定します。
Name カラムをダブルクリックし、名前を指定します。
VLAN 1について、*Name* カラムの値Default をVLAN1に変更します。

☐ これらの手順を繰り返してVLAN 3 をVLAN3の名前で作成します。

`enable`	Privileged Exec Modeに切り替えます。
`vlan database`	VLAN Configuration modeに切り替えます。
`vlan add 2`	VLAN ID 2で新規のVLANを作成します。
`name 2 VLAN2`	VLAN VLAN2に名前2 を指定します。
`vlan add 3`	VLAN ID 3で新規のVLANを作成します。
`name 3 VLAN3`	VLAN VLAN3に名前3 を指定します。
`name 1 VLAN1`	VLAN VLAN1に名前1 を指定します。
`exit`	Privileged Exec Modeに切り替えます。
`show vlan brief`	現在のVLANコンフィグレーションを表示します。

```
Max.VLAN ID….................................4042
Max. supported VLANs. ....................... 128
Number of currently configured VLANs. ....... 3
vlan unaware mode….............................disabled
VLAN ID VLAN Name                    VLAN Type VLAN Creation Time
---- -------------------------------- --------- -------------------
1       VLAN1            default              0 days, 00:00:05
2       VLAN2            static               0 days, 02:44:29
3       VLAN3            static               0 days, 02:52:26
```

☐ ポートのセットアップ

☐ *Switching > VLAN > Port* ダイアログボックスを開きます。

☐ ポートをVLANに割当てるには、対応するカラムに任意の値を入力します。数値候補：
- T = ポートはVLANのメンバーです。このポートはタグ付けしたデータパケットを伝送します。
- U = ポートはVLANのメンバーです。このポートはタグの無いデータパケットを伝送します。
- F = ポートはVLANのメンバーではありません。*GVRP* 機能を使用した変更は無効となっています。
- – = ポートはVLANのメンバーではありません。*GVRP* 機能を使用した変更は許可されます。

通常、エンドデバイスはタグ無しのデータパケットを解釈できるため、値Uを指定します。

☐  ボタンをクリックし、変更を一時的に保存します。

☐ *Switching > VLAN > Port* ダイアログボックスを開きます。

☐ *Port-VLAN ID* カラムに、関連するVLANのVLAN IDを指定します。
2 又は3

- 通常、エンドデバイスはタグ無しのデータパケットを解釈できるため、全てのエンドデバイスポートに対し、*Acceptable packet types* カラムに値`admitAll` を指定します。
- ☑ ボタンをクリックし、変更を一時的に保存します。

Ingress filtering カラムの値はここでの例の機能に影響はありません。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`interface 1/1`	インターフェース`1/1`のInterface Configuration mode に変更します。
`vlan participation include 2`	ポート`1/1` がVLAN `2`のメンバーになり、VLANタグ無しでデータパケットを伝送します。
`vlan pvid 2`	VLAN ID `1/1` をポート`2`に割当てます。
`exit`	Configuration modeに切り替えます。
`interface 1/2`	インターフェース`1/2`のInterface Configuration mode に変更します。
`vlan participation include 3`	ポート`1/2` がVLAN `3`のメンバーになり、VLANタグ無しでデータパケットを伝送します。
`vlan pvid 3`	VLAN ID `1/2` をポート`3`に割当てます。
`exit`	Configuration modeに切り替えます。
`interface 1/3`	インターフェース`1/3`のInterface Configuration mode に変更します。
`vlan participation include 3`	ポート`1/3` がVLAN `3`のメンバーになり、VLANタグ無しでデータパケットを伝送します。
`vlan pvid 3`	VLAN ID `1/3` をポート`3`に割当てます。
`exit`	Configuration modeに切り替えます。
`interface 1/4`	インターフェース`1/4`のInterface Configuration mode に変更します。
`vlan participation include 2`	ポート`1/4` がVLAN `2`のメンバーになり、VLANタグ無しでデータパケットを伝送します。
`vlan pvid 2`	VLAN ID `1/4` をポート`2`に割当てます。
`exit`	Configuration modeに切り替えます。
`exit`	Privileged Exec Modeに切り替えます。
`show vlan id 3`	VLAN `3`の詳細を表示します。

```
VLAN ID           :3
VLAN Name         :VLAN3
VLAN Type         :Static
Interface   Current   Configured   Tagging
----------- -------- ----------- --------
1/1           -      Autodetect   Tagged
1/2         Include   Include     Untagged
1/3         Include   Include     Untagged
1/4           -      Autodetect   Tagged
1/5           -      Autodetect   Tagged
```

12.1.2 例2

例2では、更に複雑な3つのVLAN（1～3）のコンフィグレーションを示します。例1のスイッチと、2つ目のスイッチ（ここの例では右側）を使用します。

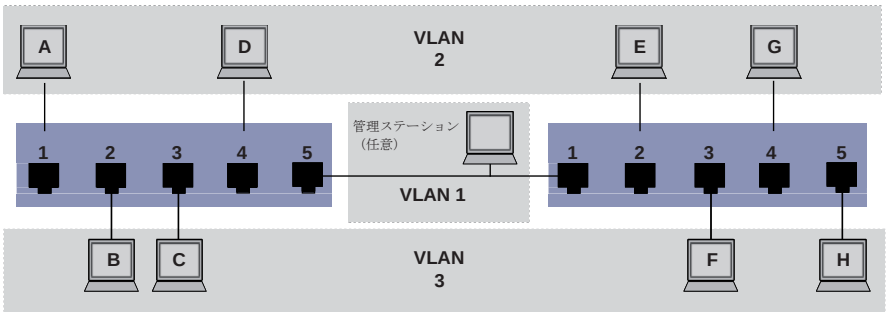


図27　更に複雑なVLANコンフィグレーション例

個々のVLANの端末デバイス（A～H）は、2つの伝送デバイス（スイッチ）上に展開されています。このようなVLANは、Distributed VLAN（分散VLAN）と呼ばれます。VLANが正しく構成されていれば、全てのネットワーク機器にアクセスを実現する任意のネットワーク管理ステーションが表示されます。

注記：このケースでは、VLAN 1はエンドデバイスの通信には重要でない一方で、いわゆる管理VLANを介した伝送デバイスの管理には必要となります。

先の例で示したように、ポートとそれに接続された端末デバイスをVLANに割当てます。2つの伝送デバイス（アップリンク）間の直接接続により、ポートは両VLANにパケットを伝送します。これらアップリンクを区別するために、データパケットを適切に処理する「VLANタグ付け」を使用します。従って、ユーザーは各VLANのアサインメントを維持しなければなりません。

以下の手順を実行します。
- ☐ アップリンクポート5を例1のIngressテーブル及びEgressテーブルに追加します。
- ☐ 新規Ingressテーブル及びEgressテーブルを、例1で示した右側スイッチ用に作成します。

Egressテーブルは、デバイスがこのVLANからのパケットにどのポートを割当てるかを指定するものです。
- ➢ T = Tagged（タグ付け）（タグフィールドあり、マーキングあり）
- ➢ U = Untagged（タグ無し）（タグフィールド無し、マーキング無し）

ここの例でタグ付けパケットは、異なるVLANのパケットはこれらポートで区別されるため、伝送デバイス（アップリンク）間の通信に使用されます。

表27　左側デバイスのIngressテーブル

端末	ポート	PVID (Port VLAN Identifier)
A	1	2
B	2	3
C	3	3
D	4	2
アップリンク	5	1

表28　右側デバイスのIngressテーブル

端末	ポート	PVID (Port VLAN Identifier)
アップリンク	1	1
E	2	2
F	3	3
G	4	2
H	5	3

表29　左側デバイスのEgressテーブル

VLAN ID	ポート				
	1	2	3	4	5
1					U
2	U			U	T
3		U	U		T

表30　右側デバイスのEgressテーブル

VLAN ID	ポート				
	1	2	3	4	5
1	U				
2	T	U		U	
3	T		U		U

ここでの通信関係は次の通りです。左側デバイスのポート1及びポート4のエンドデバイスと、右側デバイスのポート2及びポート4は、VLAN2のメンバーであるため、互いに通信することができます。この動作は左側デバイスのポート2及びポート3のエンドデバイス、更には右側デバイスのポート3及びポート5でも同じです。これらはVLAN3に属します。

これらエンドデバイスは、個々のネットワークを「見る」ことができます。このVLANに属さない参加者は、アクセスできません。デバイスが不明の（未学習の）宛先アドレスのブロードキャスト、マルチキャスト、ユニキャストパケットを、VLAN内のみに送信します。

ここでは、デバイスはID 1（アップリンク）のVLAN内で、VLANタグ付け（IEEE 801.1Q）を使用します。ポートのEgressテーブルの文字T は、VLANタグ付けを意味します。

この例のコンフィグレーションは、右側デバイスでも同じです。上記で作成したIngressテーブル及びEgressテーブルを使用して前述と同じ手順で進め、先に構築した左側デバイスの新しい環境に適応させてください。

以下の手順を実行します。
☐ VLANのセットアップ

☐ *Switching > VLAN > Configuration* ダイアログボックスを開きます。

☐  ボタンをクリックします。
ダイアログが*Create* ウィンドウを表示します。

☐ *VLAN ID* フィールドに、VLANのIDを指定します（例えば、2）。

☐ *Ok* ボタンをクリックします。

☐ VLANには、名前VLAN2を指定します。
Name カラムをダブルクリックし、名前を指定します。
VLAN 1について、*Name* カラムの値Default をVLAN1に変更します。

☐ これらの手順を繰り返してVLAN 3 をVLAN3の名前で作成します。

```
enable                          Privileged Exec Modeに切り替えます。
vlan database                   VLAN Configuration modeに切り替えます。
vlan add 2                      VLAN ID 2で新規のVLANを作成します。
name 2 VLAN2                    VLAN VLAN2に名前2 を指定します。
vlan add 3                      VLAN ID 3で新規のVLANを作成します。
name 3 VLAN3                    VLAN VLAN3に名前3 を指定します。
name 1 VLAN1                    VLAN VLAN1に名前1 を指定します。
exit                            Privileged Exec Modeに切り替えます。
show vlan brief                 現在のVLANコンフィグレーションを表示します。
Max.VLAN ID….................................   4042
Max. supported VLANs.                          128
Number of currently configured VLANs. ........ 3
vlan unaware mode….............................  disabled
VLAN ID VLAN Name                    VLAN Type VLAN Creation Time
---- -------------------------------- --------- ------------------
1       VLAN1                        default   0 days, 00:00:05
2       VLAN2                        static    0 days, 02:44:29
3       VLAN3                        static    0 days, 02:52:26
```

☐ ポートのセットアップ

☐ *Switching > VLAN > Port* ダイアログボックスを開きます。

☐ ポートをVLANに割当てるには、対応するカラムに任意の値を入力します。数値候補：
- T = ポートはVLANのメンバーです。このポートはタグ付けしたデータパケットを伝送します。
- U = ポートはVLANのメンバーです。このポートはタグの無いデータパケットを伝送します。
- F = ポートはVLANのメンバーではありません。*GVRP* 機能を使用した変更は無効となっています。
- - = ポートはVLANのメンバーではありません。*GVRP* 機能を使用した変更は無効となっています。

エンドデバイスはタグ無しのデータパケットを解釈できることが通常のため、値Uを指定します。VLANが互いに通信を行うアップリンクポートの設定にT を指定します。

☐ ☑ ボタンをクリックし、変更を一時的に保存します。

☐ *Switching > VLAN > Port* ダイアログボックスを開きます。

☐ *Port-VLAN ID* カラムに、関連するVLANのVLAN IDを指定します。
1、2 、3いずれか

☐ 通常、エンドデバイスはタグ無しのデータパケットを解釈できるため、全てのエンドデバイスポートに対し、*Acceptable packet types* カラムに値admitAll を指定します。

- アップリンクポートの*Acceptable packet types* に、値`admitOnlyVlanTagged`を指定します。
- アップリンクポートがこのポートのVLANタグを検証するよう、*Ingress filtering* カラムのチェックボックスにチェックを入れます。
- ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`interface 1/1`	インターフェース`1/1`のInterface Configuration mode に変更します。
`vlan participation include 1`	ポート`1/1` がVLAN`1`のメンバーになり、VLANタグ無しでデータパケットを伝送します。
`vlan participation include 2`	ポート`1/1` がVLAN `2`のメンバーになり、VLANタグ無しでデータパケットを伝送します。
`vlan tagging 2 enable`	ポート`1/1` がVLAN`2`のメンバーになり、VLANタグ付けでデータパケットを伝送します。
`vlan participation include 3`	ポート`1/1` がVLAN`3`のメンバーになり、VLANタグ無しでデータパケットを伝送します。
`vlan tagging 3 enable`	ポート`1/1` がVLAN`3`のメンバーになり、VLANタグ付けでデータパケットを伝送します。
`vlan pvid 1`	VLAN ID `1` をポート`1/1`に割当てます。
`vlan ingressfilter`	ポート`1/1`のIngressフィルタリングをアクティベートします。
`vlan acceptframe vlanonly`	ポート`1/1` は、VLANタグ付けたデータパケットのみ転送します。
`exit`	Configuration modeに切り替えます。
`interface 1/2`	インターフェース`1/2`のInterface Configuration mode に変更します。
`vlan participation include 2`	ポート`1/2` がVLAN`2`のメンバーになり、VLANタグ無しでデータパケットを伝送します。
`vlan pvid 2`	VLAN ID `2` をポート`1/2`に割当てます。
`exit`	Configuration modeに切り替えます。
`interface 1/3`	インターフェース`1/3`のInterface Configuration mode に変更します。
`vlan participation include 3`	ポート`1/3` がVLAN `3`のメンバーになり、VLANタグ無しでデータパケットを伝送します。
`vlan pvid 3`	VLAN ID `3` をポート`1/3`に割当てます。
`exit`	Configuration modeに切り替えます。
`interface 1/4`	インターフェース`1/4`のInterface Configuration mode に変更します。
`vlan participation include 2`	ポート`1/4` がVLAN `2`のメンバーになり、VLANタグ無しでデータパケットを伝送します。
`vlan pvid 2`	VLAN ID `2` をポート`1/4`に割当てます。
`exit`	Configuration modeに切り替えます。
`interface 1/5`	インターフェース`1/5`のInterface Configuration mode に変更します。
`vlan participation include 3`	ポート`1/5` がVLAN`3`のメンバーになり、VLANタグ無しでデータパケットを伝送します。
`vlan pvid 3`	VLAN ID `3` をポート`1/5`に割当てます。
`exit`	Configuration modeに切り替えます。

```
exit                                                    Privileged Exec Modeに切り替えます。
show vlan id 3                                          VLAN 3の詳細を表示します。
VLAN ID. ..................... 3
VLAN Name….....................VLAN3
VLAN Type….....................Static
VLAN Creation Time….........0 days, 00:07:47 (System Uptime)
VLAN Routing….................disabled

Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1         Include   Include      Tagged
1/2         -         Autodetect   Untagged
1/3         Include   Include      Untagged
1/4         -         Autodetect   Untagged
1/5         Include   Include      Untagged
```

12.2 ゲストVLAN / 未認証VLAN

ゲストVLANではデバイスが、802.1xが不能なサプリカントにポートベースのネットワークアクセスコントロール（IEEE 802.1x）を提供することができます。この機能は、ゲストが外部ネットワークのみにアクセスすることを許可するメカニズムとなっています。802.1xが不能なサプリカントをアクティブな未認証802.1xポートに接続すると、サプリカントは802.1xリクエストには応答を送信しません。サプリカントからの応答がないため、ポートは未認証状態のままとなります。サプリカントは外部ネットワークにもアクセスできません。

ゲストVLANサプリカントにはポート毎のコンフィグレーションとなります。ポートをゲストVLANとして構築し、802.1xが不能なサプリカントをこのポートに接続すると、デバイスはサプリカントをゲストVLANに割当てます。ゲストVLANにサプリカントを追加すると、ポートは認証済みのステータスに変わってサプリカントが外部ネットワークにアクセスできるようになります。

未認証VLANは、デバイスが802.1x可能なサプリカントにサービスを提供してしまい、誤った認証が行われます。この機能は未認証サプリカントにサービスのアクセスを限定するものです。未認証VLANを802.1xポート認証されたポートにGlobal Operationを有効にして構築すると、デバイスはポートを未認証VLANに配置します。802.1x可能なサプリカントがポートで誤った認証をしてしまった場合、デバイスはサプリカントを未認証VLANに追加します。また、ポートにゲストVLANを構築した場合、802.1x不能なサプリカントがゲストVLANを使用できるようになります。

ポートに未認証VLANが割当てられている場合、再認証タイマーがカウントダウンを実行します。*Reauthentication period [s]* カラムの時間が経過してサプリカントがまだポートに存在している場合、未認証VLANが再認証を実行します。サプリカントが不在の場合、デバイスはポートを構築済みVLANに配置します。

ゲストVLANの作成例を以下に示します。未認証VLANも同様の手順で先性します。

以下の手順を実行します。

- ☐ *Switching > VLAN > Configuration* ダイアログボックスを開きます。
- ☐  ボタンをクリックします。
  ダイアログが*Create* ウィンドウを表示します。
- ☐ *VLAN ID* フィールドに、値`10`を指定します。
- ☐ *Ok* ボタンをクリックします。
- ☐ VLANには、名前`Guest`を指定します。
  Name カラムをダブルクリックし、名前を指定します。
- ☐  ボタンをクリックします。
  ダイアログが*Create* ウィンドウを表示します。
- ☐ *VLAN ID* フィールドに、値`20`を指定します。
- ☐ *Ok* ボタンをクリックします。
- ☐ VLANには、名前`Not authorized`を指定します。*Name* カラムをダブルクリックし、名前を指定します。
- ☐ *Network Security > 802.1X Port Authentication > Global* ダイアログボックスを開きます。
- ☐ 機能を有効化するには*Operation* フレームの`On` のラジオボタンを選択します。
- ☐  ボタンをクリックし、変更を一時的に保存します。

- ☐ *Network Security > 802.1X Port Authentication > Port Configuration* ダイアログボックスを開きます。
- ☐ 1/4に以下を設定します。
  - *Port control* カラムに、値auto
  - *Guest VLAN ID* カラムに、値10
  - *Unauthenticated VLAN ID* カラムに、値20
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`vlan database`	VLAN Configuration modeに切り替えます。
`vlan add 10`	VLAN 10を作成します。
`vlan add 20`	VLAN 20を作成します。
`name 10 Guest`	VLAN10 の名前をGuestに変更します。
`name 20 Unauth`	VLAN20 の名前をUnauthに変更します。
`exit`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`dot1x system-auth-control enable`	*802.1X Port Authentication* 機能を全域で有効にします。
`dot1x port-control auto`	ポート1/4のポート制御を有効にします。
`interface 1/4`	インターフェース1/4のInterface Configuration mode に変更します。
`dot1x guest-vlan 10`	ゲストVLANをポート1/4に割当てます。
`dot1x unauthenticated-vlan 20`	未認証VLANをポート1/4に割当てます。
`exit`	Configuration modeに切り替えます。

12.3 RADIUS VLAN 割当て

RADIUS VLAN割当て機能は、RADIUS VLAN IDの属性を認証済みクライアントと紐付けることができます。クライアントが認証に成功してRADIUSサーバーがVLANのアトリビュートを送信すると、デバイスはクライアントをRADIUS認証したVLANを紐付けます。結果として、デバイスは物理ポートを適切なVLANのメンバーとして追加し、ポートVLAN ID（PVID）を与えられた値で設定します。ポートはVLANタグ無しでデータパケットを伝送します。

12.4 音声VLANを作成する

音声VLAN機能を使用して、ポートの音声及びデータトラフィックをVLAN及び（又は）優先順位に区分けします。音声VLANを使用する主な利点として、ポートのデータトラフィックが高い場合にIP電話の音声品質を保護することです。

当デバイスは送信元MACアドレスを使用して音声データのフローを識別し、優先化します。デバイスを識別するのにMACアドレスを使用することは、不正クライアントが同じポートに接続して音声トラフィックを劣化させるのを防ぐのに役立ちます。

音声VLAN機能の他の利点としては、VoIP電話がLLPD-MEDを使用してVLAN ID又は優先情報を取得できることです。その結果、VoIP電話は音声データを、タグ付け、優先タグ付け、タグ無しのいずれかで送信します。これは音声VLANインターフェースのコンフィグレーションにより決定します。

以下の音声VLANインタフェースモードが使用可能です。最初の3つのモードは音声及びデータトラフィックを分別し、優先付けします。トラフィックの分別は、トラフィック量が高い時間帯に音声トラフィックの品質を向上させることができます。

- `vlan` モードでポートのコンフィグレーションを行うと、デバイスがユーザー定義の音声VLAN IDのVoIP電話から来た音声データにタグ付けをします。デバイスは通常データをデフォルトのポートVLAN IDに割当てます。
- `dot1p-priority` モードでポートのコンフィグレーションを行うと、デバイスがユーザーが定義した優先順位の、VLAN 0のVoIP電話から来た音声データにタグ付けをします。デバイスは、通常データのポートにデフォルトの優先情報を割当てます。
- 音声VLAN ID及び優先順位を、`vlan/dot1p-priority` で設定します。このモードでは、VoIP電話はユーザー定義の音声VLAN ID及び優先情報で音声データを送信します。デバイスは、デフォルトPVID及びポートの優先順位を通常データに割当てます。
- `untagged`として設定した場合、電話はタグ無しのパケットを送信します。
- `none`として設定した場合、電話は自身のコンフィグレーションを使用して音声トラフィックを送信します。

13 冗長性

13.1 ネットワークトポロジー対冗長プロトコル

イーサネットを使用する際の重要な条件は、データパケットが送信者から受信者へ単一（固有の）パスを通ることです。以下のネットワークトポロジーはこの条件をサポートします。

- ライン型トポロジー
- スター型トポロジー
- ツリー型トポロジー

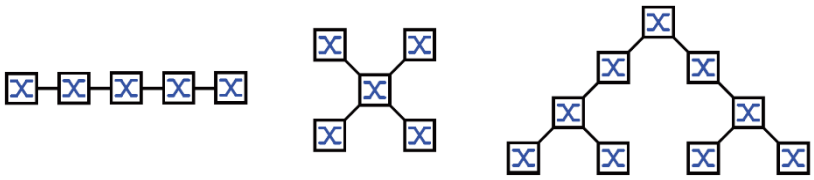


図28　ライン型、スター型、ツリー型トポロジーのネットワーク

接続に失敗しても通信を維持するために、追加の物理接続をネットワークのノード間に取り付けます。冗長プロトコルは、既存の接続が作動中に追加接続のスイッチを切るようにします。通信に失敗すると、冗長プロトコルが送信者から受信者へ、代替の接続を介して新しいパスを作ります。

ネットワークのレイヤー2を冗長化する場合、まずはどのネットワークトポロジーが必要かを判断します。選択したネットワークトポロジーによって、ここでどの冗長プロトコルが使用できるかを選択します。

13.1.1 ネットワークトポロジー

メッシュ型トポロジー

スター型又はツリー型トポロジーのネットワークには、冗長プロトコルは物理ループのある接続のみで可能です。これがメッシュ型トポロジーとなります。

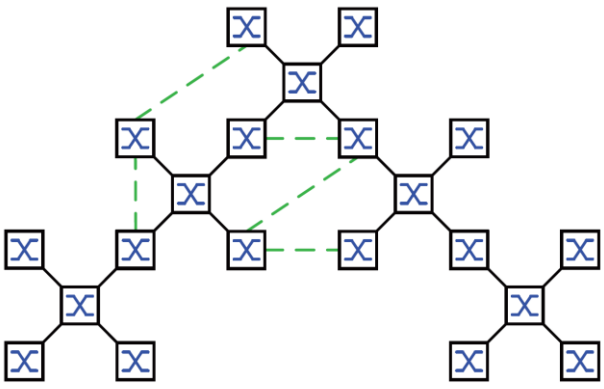


図29　メッシュ型トポロジー（物理ループを含んだツリー型トポロジー）

このネットワークトポロジーで作動するには、デバイスは以下の冗長プロトコルを提供します。
- RSTP（Rapid Spanning Tree Protocol：ラピッドスパニングツリープロトコル）

リング型トポロジー

ライン型トポロジーのネットワークでは、ラインの終端を接続することで冗長化することができます。これでリング型トポロジーが出来上がります。

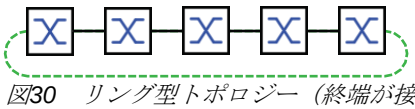


図30　リング型トポロジー（終端が接続されたライン型トポロジー）

このネットワークトポロジーで作動するには、デバイスは以下の冗長プロトコルを提供します。
- MRP（Media Redundancy Protocol：メディア冗長プロトコル）
- RSTP（Rapid Spanning Tree Protocol：ラピッドスパニングツリープロトコル）

13.1.2 冗長プロトコル

異なるネットワークトポロジーで作動するには、デバイスは以下の冗長プロトコルを提供します。

表31　冗長プロトコルの概要

冗長プロトコル	ネットワークトポロジー	備考
MRP	リング型	スイッチングタイムを選択することができ、デバイス数から実質的に独立しています。 MRPリングは、IEC 62439に基づき、MRPプロトコルをサポートするデバイス50個までで構成されます。 シュナイダーエレクトリック製デバイスのみを使用する場合、MRPリング内にデバイス100個までの使用が可能です。
サブリング	リング型	*Sub Ring* 機能では、簡単にネットワークセグメントを既存の冗長リングに連結することができます。
リングネットワークの連結型	リング型	
RSTP	ランダム構造	スイッチングタイムは、ネットワークトポロジー及びデバイス数によります。 ➢ typ. < 1 s with RSTP ➢ typ. < 30 s with STP
リンクアグリゲーション	ランダム構造	リンクアグリゲーショングループは、2つ以上の全二重ポイント・ツー・ポイント・リンクが同時に同レートで、単一スイッチで作動して帯域幅を増加させるものです。

表31　冗長プロトコルの概要（続き）

冗長プロトコル	ネットワークトポロジー	備考
リンクバックアップ	ランダム構造	デバイスが一次リンクにエラーを検知すると、デバイスはバックアップリンクにトラフィックを転送します。通常、リンクバックアップはサービスプロバイダーやエンタープライズネットワークで使用されます。
HiPER Ring Client	リング型	既存のHiPERリングを延長するか、或いはHiPERリング内でクライアントとして既に参加しているデバイスを交換します。
HiPER Ring over LAG	リング型	デバイス同士を、リンクアグリゲーショングループ（LAG）上でリンクさせます。リングのクライアント及び管理者は、LAGインスタンスが無いリングと同様の動作を行います。

フローコントロールと冗長機能が同時にアクティブな場合、冗長機能が意図したものと異なるオペレーションを行う可能性があります。

⚠ 警告

機器の誤操作

冗長機能を使用している場合、デバイス関連ポートのフローコントロールはディアクティベートします。

この指示に従わない場合、人的損害や装置の損傷を招くおそれがあります。

13.1.3 冗長化の組合せ

表32　冗長プロトコルの概要

	MRP	RSTP	リンクアグリゲーション	リンクバックアップ	サブリング	HiPERリング
MRP	▲	– – –	– – –	– – –	– – –	– – –
RSTP	▲1)	▲	– – –	– – –	– – –	– – –
リンクアグリゲーション	▲2)	▲2)	▲	– – –	– – –	– – –
リンクバックアップ	▲	▲	▲	▲	– – –	– – –
サブリング	▲	▲	▲2)	▲	▲	– – –
HiPERリング	▲	▲1)	▲2)	▲	▲	▲

▲　組合せ可

1)　これらネットワークトポロジーの冗長連結は、ループになる可能性があります。これらトポロジーを冗長的に連結する場合は、215ページのFuseNetの章をご参照ください。

2)　同ポートで組合せ可

13.2 MRP（Media Redundancy Protocol:メディア冗長プロトコル）

2008年5月以降、MRP（メディア冗長プロトコル）は、産業環境でのリング冗長化の標準ソリューションとされてきました。

MRPは冗長リング連結に適応し、VLANをサポートし、非常に短い再構成タイムのものとして別途の扱いをされています。

MRPリングは、IEC 62439によれば、MRPプロトコルをサポートするデバイス50個まで構成することができます。シュナイダーエレクトリック製デバイスのみを使用する場合、MRPリング内にデバイス100個までの使用が可能です。

固定MRP冗長化ポート（固定バックアップ）を使用の際に一時リングがエラーを起こすと、リングマネジャーはデータを二次リングのリンクに転送します。一次リンクが復旧すれば、二次リンクは継続して使用されます。

13.2.1 ネットワーク構造

冗長リングのコンセプトは、ユーザーがリング型の高可用性ネットワークを構築できることにあります。

RM（**R**ing**M**anager＝リングマネジャー）機能のサポートで、ライン構造の2つのバックボーン終端が冗長リングで閉じられます。リングマネジャーは、ライン構造が健全である限り、冗長ラインを開いた状態を維持します。セグメントが作動不能になると、リングマネジャーは即時に冗長ラインを閉じることで、再びライン構造が健全となります。

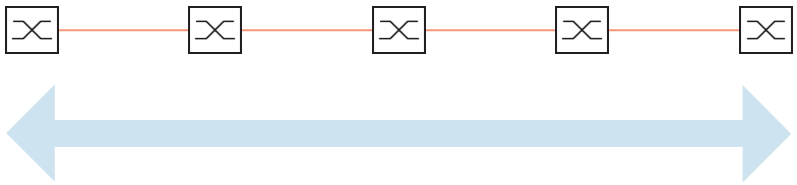


図31　ライン構造

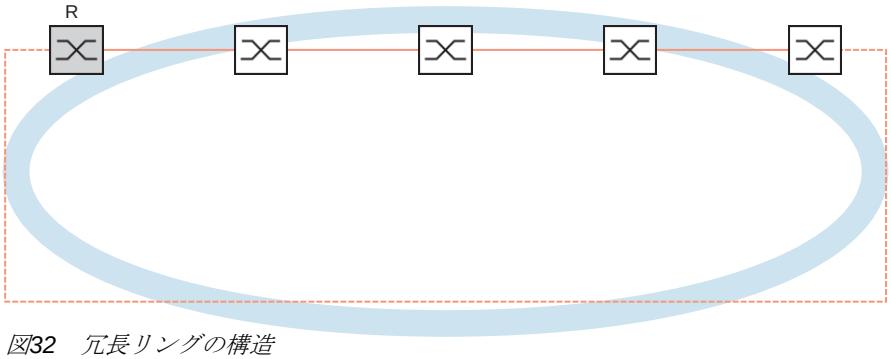


図32　冗長リングの構造
RM = Ring Manager（リングマネジャー）
—— 基幹ライン
- - - 冗長化ライン

13.2.2 再構成タイム

ラインの一部に不具合があると、リングマネジャーはMRPリングをライン構造に戻します。ユーザーはリングマネジャーのライン再構成の最大時間を設定します。

可能な最大遅延タイム：
- *500ms*
- *30ms*

注記：リング内の全デバイスは短い遅延タイムはサポートするので、ユーザーは*500ms*より少ない値の再構成タイムを設定することができます。

長い遅延タイムしかサポートしないデバイスでは、過負荷によりアクセスできない可能性があるためです。この結果、ループが出来てしまいます。

13.2.3 Advanced mode

指定した再構成タイムよりも短いタイムについては、当デバイスではAdvanced modeを使用します。リング参加者がリンクダウン通知によってリングマネジャーにリングの中断を通知すると、Advanced modeがリンク不具合の認識速度を上げます。

シュナイダーエレクトリック製デバイスはリンクダウン通知をサポートしています。従って、通常はリングマネジャーのAdvanced modeをアクティブにしておいてください。

リンクダウン通知をサポートしないデバイスを使用している場合、リングマネジャーは選択された最大再構成タイム内でラインを再構成します。

13.2.4 MRPの条件

MRPリングをセットアップする前に、以下の条件が満たされていることを確認します。
- ➢ リングの全参加者がMRPをサポートしている。
- ➢ リング参加者は、リングポートを介して相互に接続されている。デバイスの近隣者以外、他のリング参加者は個々のデバイスと接続されている。
- ➢ リングの全参加者は、リングマネジャーに指定された構成タイムをサポートしている。
- ➢ リング内にリングマネジャーは1つしか存在しない。

VLANを使用している場合、全リングポートを以下の通りに設定します。
- ☐ Ingressフィルタリングをディアクティベートします。*Switching > VLAN > Port* ダイアログボックスを参照。
- ☐ VLAN ID（PVID）を定義します。*Switching > VLAN > Port* ダイアログボックスを参照。
  - – デバイスがMRPデータパケットをタグ無し（*Switching > L2-Redundancy > MRP* ダイアログボックスで、VLAN ID＝0 ）で伝送する場合、PVID=1 。
    PVID = 1を設定することで、デバイスは受信したタグ無パケットをVLAN 1に割当てます。
  - – デバイスがMRPデータパケットをVLAN（*Switching > L2-Redundancy > MRP* ダイアログボックスで、VLAN ID≥1 ）で伝送する場合、PVID=any 。
- ☐ Egressルールを定義します。*Switching > VLAN > Configuration* ダイアログボックスを参照。
  - – デバイスがMRPデータパケットをタグ無し（*Switching > L2-Redundancy > MRP* ダイアログボックスで、VLAN ID＝0 、MRPリングはVLANに割当てられていない）で伝送する場合、VLAN 1のリングポートはU （タグ無し）。
  - – ユーザーがMRPリングを割当てたVLANのリングポートは、T （タグ付け）。デバイスがMRPデータパケットをVLAN（*Switching > L2-Redundancy > MRP* ダイアログボックスで、VLAN ID≥1 ）で伝送する場合、Tを選択。

13.2.5 コンフィグレーション例

バックボーンネットワークは、ライン構造にデバイス3つを含みます。ネットワークの可用性を上げるには、ライン構造を冗長リング構造に変換します。異なるメーカーのデバイスが使用されています。デバイスは全てMRPをサポートします。各デバイスのポート1.1及び1.2をリングポートと定義します。

一次リングに障害が起きると、リングマネジャーは二次リングのリンクにデータを送信します。一次リンクが復旧すれば、二次リンクはBackup modeに戻ります。

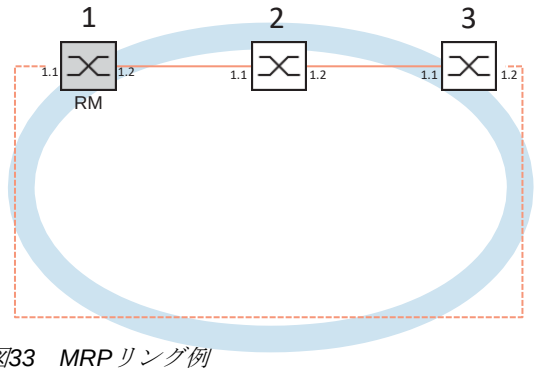


図33　MRPリング例
RM = Ring Manager（リングマネジャー）
—— 基幹ライン
- - - 冗長化ライン

以下のコンフィグレーションの例は、リングマネジャーデバイス（1）のコンフィグレーションを示したものです。もう2つのデバイス（2から3）を同様に、但し*Ring manager* 機能はアクティベートしないように設定します。ここの例ではVLANは使用しません。リングのリカバリータイムとして`30ms` を指定します。デバイスは全てリングマネジャーのAdvanced modeをサポートします。

- ☐ ユーザーの要件を満たすようネットワークを設定します。
- ☐ 全てのポートのコンフィグレーションを行い、伝送速度及びラインの二重（duplex）設定を以下の表と一致させます。

表33　リングポートのポート設定

ポート種別	ビットレート	ポートの状態	自動コンフィグレーション	手動コンフィグレーション
TX	100 Mbit/s	`marked`	`unmarked`	*`100 Mbit/s FDX`*
TX	1 Gbit/s	`marked`	`marked`	–
光	100 Mbit/s	`marked`	`unmarked`	*`100 Mbit/s FDX`*
光	1 Gbit/s	`marked`	`marked`	–
光	2.5 Gbit/s	`marked`	–	*`2.5 Gbit/s FDX`*

注記：ユーザーは、オートネゴシエーション（自動コンフィグレーション）をサポートしない光ポートを100 Mbit/s全二重（FDX）又は1000 Mbit/s全二重（FDX）に設定します。

注記：ユーザーは、オートネゴシエーション（自動コンフィグレーション）をサポートしない光ポートを100 Mbit/s全二重（FDX）に設定します。

注記：MRPリングの全デバイスを個別に設定します。冗長化ラインを接続する前に、MRPリングの全デバイスのコンフィグレーションを完了したことを確認します。これにより、コンフィグレーションの段階でループができるのを避けることができます。

⚠ 警告

機器の誤操作

コンフィグレーションの段階でループができるのを避けるには、*MRP* コンフィグレーションの各デバイスを個々に設定します。冗長化ラインを接続する前に、MRPリングの全デバイスのコンフィグレーションを完了させてください。

この指示に従わない場合、人的損害や装置の損傷を招くおそれがあります。

関連ポートのフローコントロールはディアクティベートします。

フローコントロールと冗長機能が同時にアクティブな場合、冗長機能が意図したものと異なるオペレーションを行う可能性があります。（デフォルトでは、フローコントロールは全域でディアクティベートされていて、全ポートでアクティベートされています。）

ネットワークの全デバイスの*Spanning Tree* 機能を無効化します。以下の手順を実行します。

- ☐ *witching > L2-Redundancy > Spanning Tree > Global* ダイアログボックスを開きます。
- ☐ 機能を無効化します。
  初期設定では、Spanning Treeはデバイス内で有効になっています。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`no spanning-tree operation`	Spanning TreeをOFFに切り替えます。
`show spanning-tree global`	確認用にパラメーターを表示します。

ネットワークの全デバイスのMRPを有効化します。以下の手順を実行します。

- ☐ *Switching > L2-Redundancy > MRP* ダイアログボックスを開きます。
- ☐ 任意のリングポートを指定します。

コマンドラインインターフェースで、最初に追加パラメーター（MRPドメインID）を定義します。リングの全参加者に同じMRPドメインIDを設定します。MRPドメインIDは、16個連続するブロックです（8ビット値）

グラフィカルユーザーインターフェースのコンフィグレーションの再、デバイスのデフォルトは `255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255`となっています。

`mrp domain add default-domain`	ID `default- domain`で新規MRPドメインを作成します。
`mrp domain modify port primary 1/1`	ポート*1/1* をリングポート`1`として指定します。
`mrp domain modify port secondary 1/2`	ポート*1/2* をリングポート`2`として指定します。

Fixed backup を有効化します。以下の手順を実行します。

- ☐ リングマネジャーを有効化します。
  リング内その他デバイスについては、*Off*設定のままとします。
- ☐ リングの修復後、デバイスを二次ポートにデータを送信させ続けるには、*Fixed backup* チェックボックスにチェックを入れます。

注記：デバイスが一次ポートに戻った場合、リングのリカバリータイムの最大値は超過することができます。

Fixed backup チェックボックスのチェックを外した場合、リングは修復され、リングマネジャーが二次ポートをブロック、一次ポートのブロックを解除します。

```
mrp domain modify port secondary
1/2 fixed-backup enable
```

二次ポートの*Fixed backup* 機能を有効化します。二次ポートはリングの修復後にデータを転送し続けます。

- ☐ リングマネジャーを有効化します。
  リング内その他デバイスについては、*Off*設定のままとします。

```
mrp domain modify mode manager
```

デバイスが*Ring manager*として作動することを指定します。リング内その他デバイスについては、デフォルトのままとします。

- ☐ *Advanced mode* フィールドのチェックボックスにチェックを入れます。

```
mrp domain modify  advanced-mode
enabled
```

Advanced modeをアクティベートします。

- ☐ *Ring recovery* フィールドに、値*30ms*を指定します。

```
mrp domain modify  recovery-delay
200ms
```

リングのコンフィグレーションの最大遅延時間を*30ms* と指定します。

注記：値*30ms* をリングの修復時間に選択した際に、ユーザーのネットワーク要件を満たすだけのリングの安定性が得られない場合、値*500ms*を選択します。

- ☐ MRPリングのオペレーションをONに切り替えます。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

```
mrp domain modify operation enable
```

MRPリングをアクティベートします。

全てのリング参加者のコンフィグレーションがされたら、ラインをリングで閉じます。これを行うには、ライン終端にリングポートを介してデバイスを接続します。

デバイスからのメッセージを確認します。以下の手順を実行します。

`show mrp` 確認用にパラメーターを表示します。

Operation フィールドは、リングポートの作動状況を表示します。

数値候補：
- `forwarding`
  ポートは有効で、接続が存在しています。
- `blocked`
  ポートはブロックされ、接続が存在しています。
- `disabled`
  ポートは無効です。
- `not-connected`
  接続は存在しません。

Information フィールドは、冗長化の設定用のメッセージや、エラーの原因を表示します。

デバイスがリングクライアント又はリングマネジャーとして作動しているのであれば、以下メッセージが出る可能性があります。
- *Redundancy available*
  冗長化設定ができています。リングのコンポーネントが故障すると、冗長化ラインがその機能を引継ぎます。
- *Configuration error:Error on ringport link.*
  リングポートのケーブルにエラーがあります。

デバイスがリングマネジャーとして作動しているのであれば、以下メッセージが出る可能性があります。
- *Configuration error:Packets from another ring manager received.*
  リング内に、リングマネジャーとして作動している別のデバイスが存在します。リング内で、1つだけのデバイスで*Ring manager* 機能をアクティベートします。
- *Configuration error:Ring link is connected to wrong port.*
  リング内のラインは、リングポートでなく別のポートと接続されています。デバイスは、1つのリングポートのみでテストデータパケットを受信します。

必要であれば、MRPリングをVLANと統合します。以下の手順を実行します。

- *VLAN ID* フィールドに、MRP VLAN IDを定義します。MRP VLAN IDとは、どの構成済みVLANにMRPパケットをデバイスが送信するかを決定するものです。
  MRP VLAN IDを設定するには、まず、VLAN及び対応するEgressルールを*Switching > VLAN > Configuration* ダイアログボックスで設定します。
  - ここでの例のように、MRPリングがVLANに割当てられていない場合、VLAN IDを`0`のままとします。
    Switching > VLAN > Configuration ダイアログボックスで、VLAN`1`のリングポートを、VLAN membership `U`（タグ無し）と指定します。
  - MRPリングがVLANに割当てられていれば、VLAN ID >`0`を入力します。
    Switching > VLAN > Configuration ダイアログボックスで、VLAN1のリングポートを、VLAN membership `T`（タグ付け）と指定します。

`mrp domain modify vlan <0..4042>` VLAN IDを割当てます。

13.2.6 MRP over LAG

シュナイダーエレクトリック製デバイスでは、LAG（Link Aggregation Groups）を組合せ、冗長性を提供するMRP（Media Redundancy Protocol）と共に帯域幅を増加させることができます。ユーザーはこの機能を使用して、個々のセグメント又はネットワーク全体の帯域幅を増加させることができます。

Link Aggregation 機能は個別のポートの帯域幅の制限を超えることができます。LAGでは、2つ以上のリンクを並列に組み合わせ、2つのデバイス間に1つの論理リンクを作成することができます。並列リンクは2つのデバイス間のデータストリーム用帯域幅を増加させます。

MRPリングは、IEC 62439によれば、MRPプロトコルをサポートするデバイス50個まで構成することができます。シュナイダーエレクトリック製デバイスのみを使用した場合、MRPリングを最大100デバイスまでプロトコルで構成することができます。

MRP over LAGは以下の場合に使用します。
- 特定のMRPリングのセグメントのみで帯域幅を増加させたい
- MRPリング全域で帯域幅を増加させたい

ネットワーク構造

MRPリングにLAGを構成したい場合、継続性を維持させるためにRM（リングマネジャー）は基幹回線網の両端を監視します。基幹回線網が健全である間は、RMは二次（冗長化）ポートのデータをブロックします。RMがデータストリームの中断をリングで検知すると、基幹回線網の継続性を修復する二次ポートにデータを転送するようになります。

帯域幅を増加だけのためにMRPリングにLAGのインスタンスを使用しますが、このケースではMRPは冗長性を与えます。

RMがリングの中断を検知できるようにするには、インスタンスのポートが停止している場合はLAGインスタンスの全ポートをデバイスがブロックするよう、MRPが要求します。

MRPリングの単一セグメント上のLAG

当デバイスでは、ユーザーがLAGインスタンスをMRPリングの特定セグメントに構成することができます。

MRPリング内のデバイスには、LAG Single Switch（単一スイッチ）法を使用します。Single Switch法は、物理ポートへ供給するセグメントの両端にデバイスを1つだけ使用することで、安価にネットワークを成長させることができます。デバイスのポートをLAGインスタンスにグループ化し、帯域幅を必要とする特定セグメントの帯域幅を増加させます。

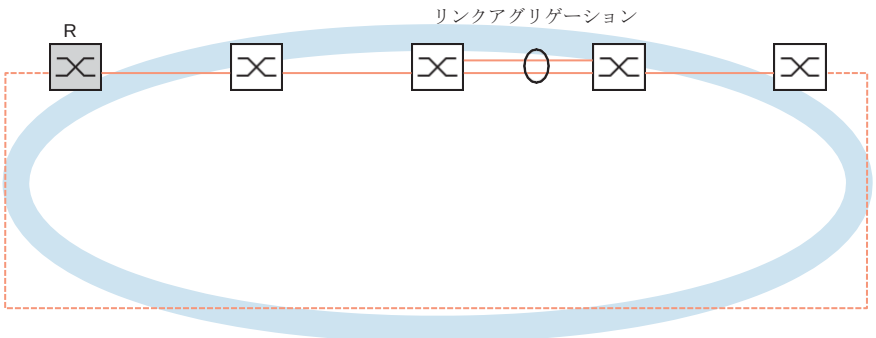


図34　MRPリングの単一リンク上のリンクアグリゲーション

MRPリング全域にLAG

LAGインスタンスをMRPリングの特定セグメントに構成できるのに加え、シュナイダーエレクトリック製デバイスでは、ユーザーが全セグメントにLAGインスタンスを構成できるため、MRP全域で帯域幅が増加します。

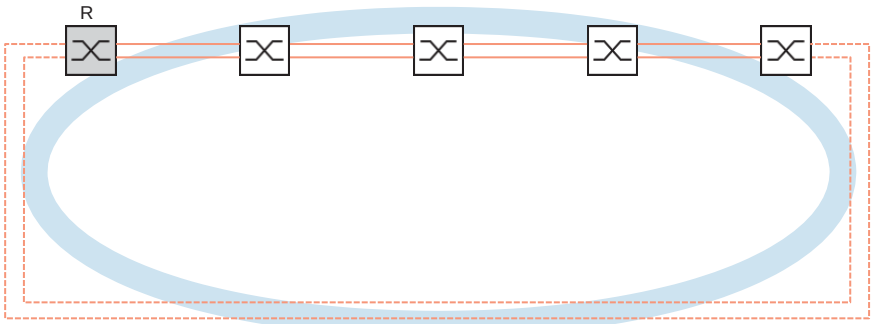


図35　MRPリング全域のリンクアグリゲーション

リングの中断の検知

LAGインスタンスを構成の際に、値*Active ports (min.)* をLAGインスタンスに使用されるポート数の合計と同等にします。デバイスがLAGインスタンスのポートで中断を検知すると、インスタンスの他ポートのデータをブロックします。全ポートのインスタンスがブロックされると、RMはリングがオープンであると検知し、二次ポートにデータを転送し始めます。これによりRMは中断されたセグメントの反対側デバイスへの継続性を修復することができます。

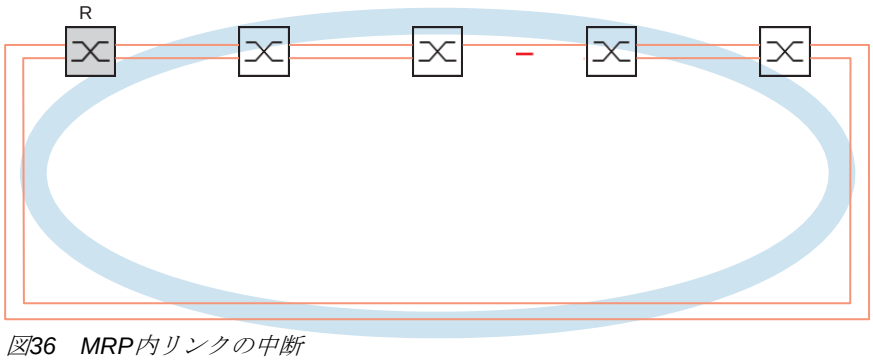


図36　MRP内リンクの中断

コンフィグレーション例

以下の例では、スイッチA及びスイッチBは2つのデパートメントをリンクさせるものです。これらデパートメントは、トラフィックが個々ポートの帯域幅では足りないくらい高くなっています。ユーザーはMRPリングの単一セグメントにLAGインスタンスを構成し、セグメントの帯域幅を増加させます。

この例を実行する条件は、作動可能なMRPリングからコンフィグレーションを開始することです。

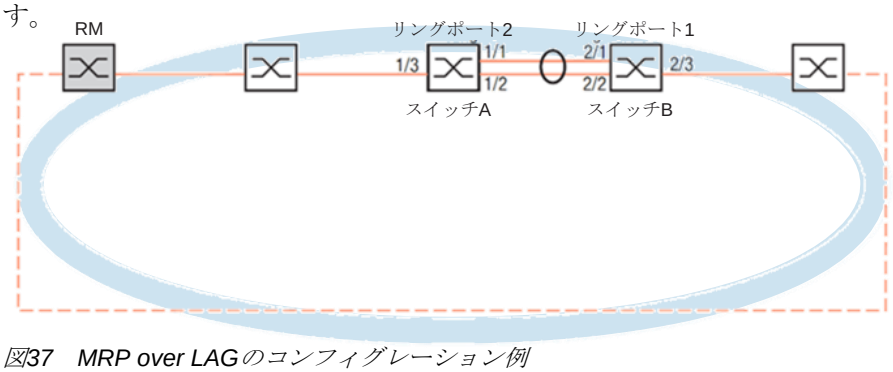


図37　MRP over LAGのコンフィグレーション例

最初にスイッチAのコンフィグレーションを実行します。以下の手順を実行します。次に同じ手順で、ポートやリングポート番号を適切に変えてスイッチBのコンフィグレーションを実行します。

- ☐ *Switching > L2-Redundancy > Link Aggregation* ダイアログボックスを開きます。
- ☐ ボタンをクリックします。
  ダイアログが*Create* ウィンドウを表示します。
- ☐ *Trunk port* ドロップダウンリストで、リンクアグリゲーショングループのインスタンス番号を選択します。
- ☐ *Port* ドロップダウンリストで、ポート*1/1*を選択します。
- ☐ *Ok* ボタンをクリックします。
- ☐ 前述の手順を繰り返いし、ポート*1/2*を選択します。
- ☐ *Ok* ボタンをクリックします。
- ☐ *Active ports (min.)* カラムに、このケースではインスタンス内のポート数合計である2を入力します。MRP及びLAGを組み合わせる場合、ポート数の合計を*Active ports (min.)*として指定します。デバイスがポートで中断を検知すると、インスタンスの他ポートのデータをブロックするため、リングが開きます。リングマネジャーがリングが開いていると検知すると、ネットワーク上の他デバイスとの接続を修復する二次ポートにデータを転送し始めます。
- ☐ ボタンをクリックし、変更を一時的に保存します。
- ☐ *Switching > L2-*Redundancy *> MRP* ダイアログボックスを開きます。
- ☐ *Ring port 2* フレームで、*Port* ドロップダウンリストのポートlag/1 を選択します。
- ☐ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`link-aggregation add lag/1`	Link Aggregation Group `lag/1`を作成します。
`link-aggregation modify lag/1 addport 1/1`	ポート *1/1* を Link Aggregation Groupに追加します。

`link-aggregation modify lag/1 addport 1/2`	ポート *1/2* を Link Aggregation Groupに追加します。
`mrp domain modify portsecondary lag/1`	ポート`lag/1` をリングポート`2`として指定します。
`copy config running-config nvm`	不揮発性メモリ（`nvm`）にある現状の設定を「選択」したコンフィグレーションプロファイルに保存します。

13.3 HiPER Ring Client

⚠ 警告

機器の誤操作

コンフィグレーションの段階でループができるのを避けるには、*HIPER Ring* コンフィグレーションの各デバイスを個々に設定します。冗長化ラインを接続する前に、MRPリングの全デバイスのコンフィグレーションを完了させてください。

この指示に従わない場合、人的損害や装置の損傷を招くおそれがあります。

HiPER Ring冗長化のコンセプトは、高可用性のリング型ネットワークの構築を可能にすることです。*HiPER Ring* Client 機能は、ネットワーク管理者に既存のHiPER Ringを延長させるか、又は既にHiPER Ringに参加しているクライアントデバイスと入れ替えさせます。

デバイスがリングポートのリンクが停止したと検知したら、デバイスはLinkDownパケットをRM（リングマネジャー）に送信し、FDBテーブルをフラッシュします。RMがLinkDownパケットを受信すると、RMは即時にデータストリームを一次及び二次リングポートに送信します。従って、RMはHiPER Ringの健全性を維持することができます。

当デバイスは、リングポートとしてはFast Ethernet及びGigabit Ethernetポートしかサポートしません。これらリングポートはLAGインスタンスに含めることができます。

デフォルトの状態では、HiPER Ring Clientは非アクティブであり、一次及び二次ポートは`no Port`と設定されています。

注記：STP と HiPER Ring では反応時間が異なるため、*Switching > L2- Redundancy > Spanning Tree > Port* ダイアログボックスのリングポートのSTP （Spanning Tree Protocol）をディアクティベートします。

表34　リングポートのポート設定

ポート種別	ビットレート	ポートの状態	自動コンフィグレーション	手動コンフィグレーション
TX	100 Mbit/s	`marked`	`unmarked`	*`100 Mbit/s FDX`*
TX	1 Gbit/s	`marked`	`marked`	–
光	100 Mbit/s	`marked`	`unmarked`	*`100 Mbit/s FDX`*
光	1 Gbit/s	`marked`	`marked`	–
光	2.5 Gbit/s	`marked`	–	*`2.5 Gbit/s FDX`*

13.3.1 HiPER Ring上のVLAN

当デバイスでは、VLANデータをHiPER Ring上に転送することができます。これにより、デバイスはVLANデータを冗長化することができます。リングデバイスがリングを回って管理データを転送します（例えば、VLAN 1上で）。データを管理ステーションに届かせるために、リングデバイスはタグ無しの管理データをリングポートに転送します。但し、リングポートをVLAN 1のメンバーとして指定します。

他のVLANがリングデバイスを横断している場合、リングデバイスは他のVLANデータをタグ付けとして転送します。

VLANを設定します。以下の手順を実行します。

- *Switching > VLAN > Configuration* ダイアログボックスを開きます。
- タグ無しのVLAN管理データをリングポートに転送します。
  VLAN 1の行で、リングポートに関連するカラムのドロップダウンリストから`U` 項目を選択します。
- 非リングポートに管理パケットが転送されないようブロックします。
  VLAN 1の行で、リングポートに関連**しない**カラムのドロップダウンリストから`-` 項目を選択します。
- リングデバイスにVLANデータをVLANメンバーのポートへ転送することを許可します。
  VLAN の行で、リングポートに関連するカラムのドロップダウンリストから`T` 項目を選択します。
- *Switching > VLAN > Port* ダイアログボックスを開きます。
- VLAN 1メンバーシップをリングポートに割当てます。
  リングポートの行で、*Port-VLAN ID* カラムに値`1` を入力します。
- VLAN メンバーシップを非リングポートに割当てます。
  非リングポートの行で、*Port-VLAN ID* カラムに適切なVLAN IDを入力します。

13.3.2 HIPER Ring over LAG

HIPER Ring 機能では、デバイス同士を、リンクアグリゲーショングループ（LAG）上でリンクさせることができます。リングのクライアント及び管理者は、LAGインスタンスが無いリングと同様の動作を行います。

LAGリンクが停止すると、インスタンス内の他リンクも停止し、リングが破損します。リングの破損を検知した後、影響を受けたポートはLinkDownパケットをリングマネジャーに送信します。リングマネジャーは二次ポートのブロックを解除し、リングの双方向にデータを送信し、Deleteパケットで返信します。Deleteパケットを受信する際に、リングはFDBのフラッシュに参加します。

13.4 スパニングツリー

注記：STP（Spanning Tree Protocol：スパニングツリープロトコル）はMACブリッジ用のプロトコルです。このため、以下ではデバイスの事を「ブリッジ」と記述します。

ローカルネットワークは日毎に大きくなっています。これは、地理的な拡大及びネットワーク参加者数の両者とも該当します。そのため、以下の例のように複数のブリッジを使う利点があります。

- サブエリアのネットワーク負荷を軽減するため
- 冗長接続を設定するため
- 距離により制限を克服するため

但し、複数のブリッジを複数の冗長接続でサブネットワーク間で使用することでループができてしまい、ネットワークを通して通信が中断します。これを避けるため、スパニングツリーを使用します。スパニングツリーは冗長接続を体系立ってディアクティベートすることを通し、ループフリースイッチングを有効にします。冗長化は個々の接続を必要に応じ、体系立って再アクティベートさせてくれます。

RSTPは、STP（スパニングツリープロトコル）を更に発展させたもので、STPと互換性もあります。接続又はブリッジが作動できなくなると、STPは最大30秒の再コンフィグレーションタイムを要求します。これは時間依存のアプリケーションには受け入れられないものです。RSTPでは再コンフィグレーションタイムを平均で1秒未満を達成できます。デバイス数が10から20あるリングトポロジーでRSTPを使用すると、再コンフィグレーションタイムをミリ秒単位で達成することもできます。

注記：RSTPは、レイヤー2の冗長パスを有するネットワークトポロジーを、これ以上の冗長パスを含まないツリー構造（スパニングツリー）内で減少させます。デバイスのうち1つがルートブリッジの役目を果たします。アクティブな枝（ルートブリッジから枝の先）に許可されるデバイスの最大数は、当該ルートブリッジの、可変*Max age* で指定されています。*Max age* のプリセット値は20で、最大40まで増やすことができます。

ルートの役目のデバイスが操作不能で、別デバイスがこの機能を引き継いだ場合、新規ルートブリッジの*Max age* 設定が枝に許容されたデバイス最大数を決定します。

注記：RSTP標準では、ネットワーク上の全デバイスが（ラピッド）スパニングツリーアルゴリズムで作動することが求められます。STP及びRSTPが同時に使用される場合、より速い再コンフィグレーションというRSTPの利点は、これらを組み合わせて作動するネットワークセグメントでは失われます。

RSTPのみをサポートするデバイスは、MSTリージョンを自身に割当る代わりにCST（Common Spanning Tree）を割当てることで、MSTPデバイスと使用することができます。

13.4.1 基本事項

RSTPはSTPを更に発展させたものであるため、以下のSTPに関する記述はRSTPにも適用されます。

STPの役目

スパニングツリーアルゴリズムは、ブリッジを有し、且つツリー構造に冗長リンクがあることでリング構造を含むネットワークのトポロジーを減少させます。これをするにあたり、冗長パスをディアクティベートすることで、プリセットルールに従いSTPがリング構造を開きます。ネットワークコンポーネントの故障のためにパスが中断されると、STPは過去にディアクティベートしたパスを再度アクティベートします。これによって、冗長リンクが通信の可用性を増加させます。

STPは、STP構造のベースとなるフリッジを決定します。このフリッジを、ルートブリッジと呼びます。

STPアルゴリズムの機能：
- ブリッジが作動不能になった場合やデータパスが中断した場合の、ツリー構造の自動再コンフィグレーション
- ツリー構造の安定化がネットワークサイズの最大サイズまで可能
- 短時間内でのトポロジーの安定化
- トポロジーを指定でき、アドミニストレーターであれば再作成することができる
- エンドデバイスの透明性
- 作成したツリー構造により、有用な伝送キャパシティがありネットワーク負荷が低い

ブリッジのパラメーター

各ブリッジとその接続は、スパニングツリーの観点から、以下固有のパラメーターがあります。
- ブリッジ識別子
- ブリッジポートのルートパスコスト
- ポート識別子

ブリッジ識別子

ブリッジ識別子は8バイトで構成されています。最大値のバイト2つは優先です。ネットワークをコンフィグレーションする際に、管理アドミニストレーターは優先のデフォルト値である32768 (8000H)を変更することができます。ブリッジ識別子の最小値のバイト6つは、ブリッジのMACアドレスです。MACアドレスは、各ブリッジに固有のブリッジ識別子を持たせます。

最も小さなブリッジ識別子の数字のブリッジが、最高位の優先となります。

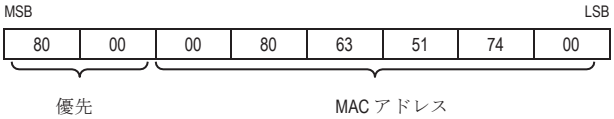


図38　ブリッジ識別子の例（数値は16進数）

ルートパスコスト

ブリッジ2つと接続する各パスは、伝送にコスト（パスコスト）が割当てられます。デバイスは、伝送速度を基にこの値を決定します（表35参照）。伝送速度が遅いほど、デバイスは高いパスコストを割当てます。

また、アドミニストレーターがパスコストを設定することもできます。デバイスと同様、アドミニストレーターは伝送速度が遅いほど、高いパスコストを割当てます。但し、アドミニストレーターがこの値を任意で選択できるため、冗長パスのうち特定のパスを優位にするツールが、アドミニストレーターにはあります。

ルートパスコストは、データパケットが接続されたブリッジのポートからルートブリッジへと横断しなければならないパスの、個々のコストの合計です。

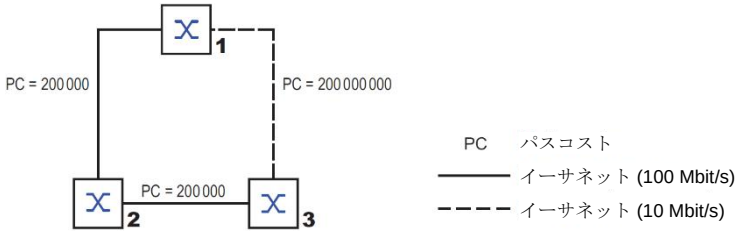


図39 パスコスト

表35 データ伝送レートを基にしたRSTPの推奨パスコスト

データ伝送レート	推奨値	推奨範囲	可能領域
≤100 kbit/s	200 0000001	20000000-200000000	1-200000000
1 Mbit/s	20000000a	2000000-200000000	1-200000000
10 Mbit/s	2000000a	200000-20000000	1-200000000
100 Mbit/s	200000a	20000-2000000	1-200000000
1 Gbit/s	20000	2000-200000	1-200000000
10 Gbit/s	2000	200-20000	1-200 000000
100 Gbit/s	200	20-2000	1-200000000
1 TBit/s	20	2-200	1-200000000
10 TBit/s	2	1-20	1-200000000

1. IEEE 802.1D 1998の規定を満たし、且つパスコストに16ビット値のみをサポートするブリッジは、パスコストに32ビット値をサポートするブリッジと連携している場合は、パスコストに65,535 (FFFFH) を使用するべきです。

ポート識別子

ポート識別子は2バイトで構成されています。そのうち、低いビット値の方は、物理ポート番号を含みます。これにより、このブリッジのポートに固有の識別子を与えます。もう片方の高いビット値はポートの優先順位で、アドミニストレーターが指定するものです（デフォルトは128）。また、最も小さなポート識別子の数字のポートが、最高位の優先となります。

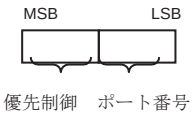


図40 ポート識別子

Max Age（最大経過時間）及び直径

最大経過時間（Max Age）及び直径（Diameter）の値は、スパニングツリーネットワークの拡大の最大値を決定します。

直径

ネットワークで最も遠く離れたデバイス間の接続数は、ネットワーク直径（Diameter）として知られています。

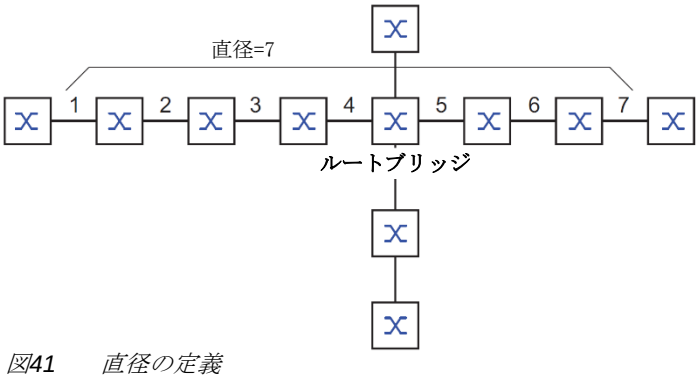


図41　直径の定義

ネットワークで可能なネットワーク直径は、MaxAge（最大経過時間）－1となっています。

出荷設定ではMaxAge=20、最大直径=19となっています。MaxAgeの最大値を40と設定すると、最大直径=39となります。

MaxAge（最大経過時間）

全てのSTP-BPDUには「MessageAge」カウンターが含まれます。ブリッジが通過されると、カウンターが1増えます。

STP-BPDUを転送する前に、ブリッジはデバイス内で指定された「MessageAge」カウンターと「MaxAge」値を比較します。

- MessageAge < MaxAge であれば、ブリッジはSTP-BPDUを次のブリッジに転送します。
- MessageAge = MaxAge であれば、ブリッジはSTP-BPDUを破棄します。

ルートブリッジ

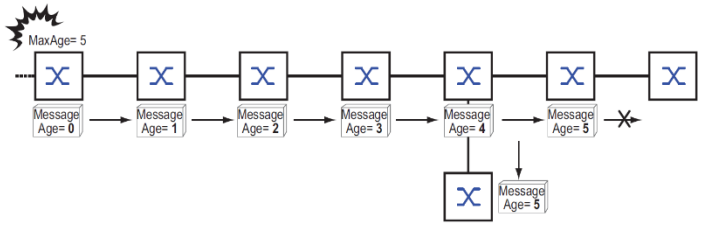


図42　MaxAgeによるSTP-BPDUの伝送

13.4.2　ツリー構造作成のルール

ブリッジ情報

ツリー構造を決定するには、ブリッジがネットワーク内の他のブリッジに関する更なる詳細情報を必要とします。

この情報を得る為に、各ブリッジはBPDU（Bridge Protocol Data Unit）を他のブリッジに送信します。

BPDUのコンテンツには以下を含みます。
- ブリッジ識別子
- ルートパスコスト
- ポート識別子

(IEEE 802.1D参照)

ツリー構造のセットアップ

最も小さなブリッジ識別子の数字のブリッジは、ルートブリッジと呼ばれます。この識別子がツリー（木）のルート（根）となっている、或いはこれからなる為です。

ツリーの構造は、ルートパスコストによります。スパニングツリーは個々のブリッジとルートブリッジ間のパスコストが最小限となる構造を選択します。

- 同じパスコストで複数のパスができる場合、ルートから最も離れたブリッジがどのポートをブロックするかを決定します。このため、よりルートに近いブリッジのブリッジ識別子が使われます。ブリッジは、高数値のID（理論上、数値が高いIDほど劣る）を持つブリッジへと導くポートをブロックします。優先順位が同じブリッジが2つある場合、高数値のMACアドレスが高数値のIDとなっており、理論上は劣る方となります。
- 一つのブリッジから同じルートパスコストの複数パスが同じブリッジへと繋がる場合、ルートから最も離れたブリッジが他方のブリッジのポート識別子を、最終的な判断基準とします（図40参照）。このプロセスにおいて、ブリッジは、高数値のID（理論上、数値が高いIDほど劣る）を持つポートへと導くポートをブロックします。優先順位が同じポートが2つある場合、高数値のIDを持つポートが高数値のIDとなっており、理論上は劣る方となります。

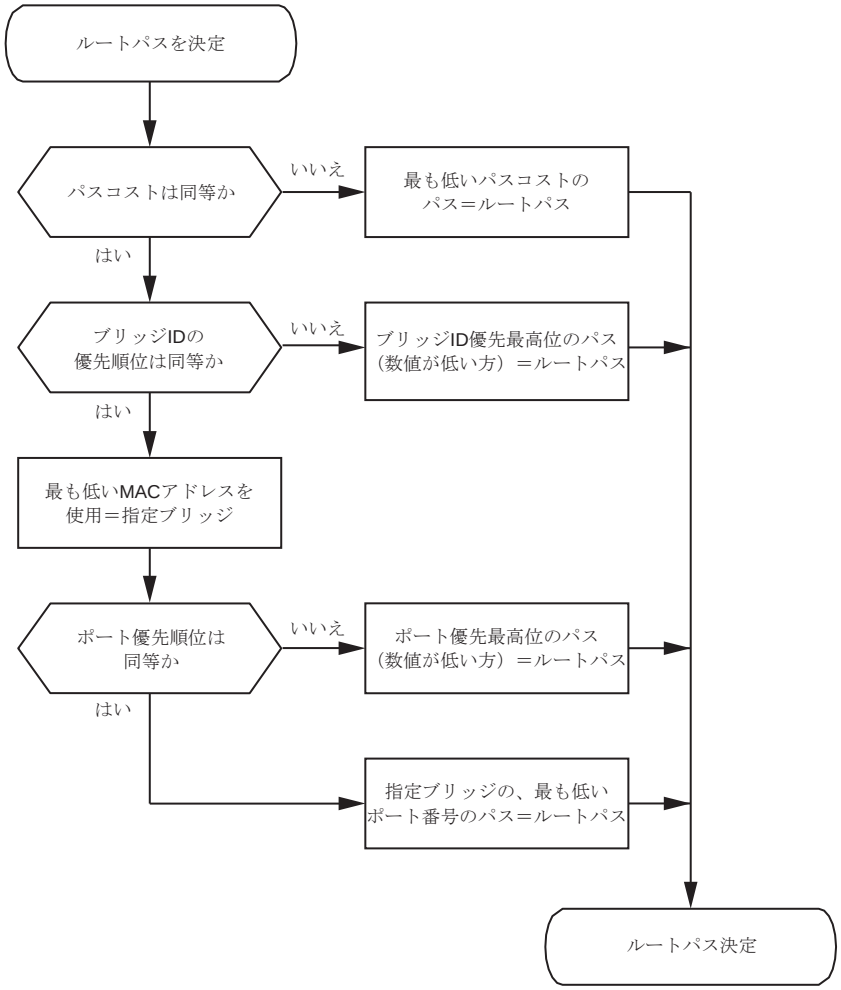


図43　ルートパス指定のフローチャート

13.4.3 例

ルートパス決定の参考例

ルートパスの決定には、ネットワーク計画（図44）を使用してフローチャート（図43）のフローを辿ります。アドミニストレーターは、各ブリッジのブリッジIDに優先順位を割当ててあります。最小値のブリッジIDのブリッジは、ルートブリッジの役割を担います（ここの例では、ブリッジ1）。ここでは、全てのサブパスは同等のパスコストとします。ブリッジ3からブリッジ2を介したルートブリッジへの接続はパスコストが高くなるため、ブリッジ2とブリッジ3の間のパスをプロトコルがブロックします。

ブリッジ6からルートブリッジへのパスは興味深いと言えます。
- ブリッジ5からブリッジ3へのパスは、ブリッジ4からブリッジ2へのパスと、同じルートパスコストになります。
- STPはブリッジIDで最も低いMACアドレスのブリッジを使用したパスを選択します（図ではブリッジ4）。
- また、ブリッジ6及びブリッジ4間には2つパスがあります。
  ここではポート識別子が決定要素です（ポート1＜ポート3）。

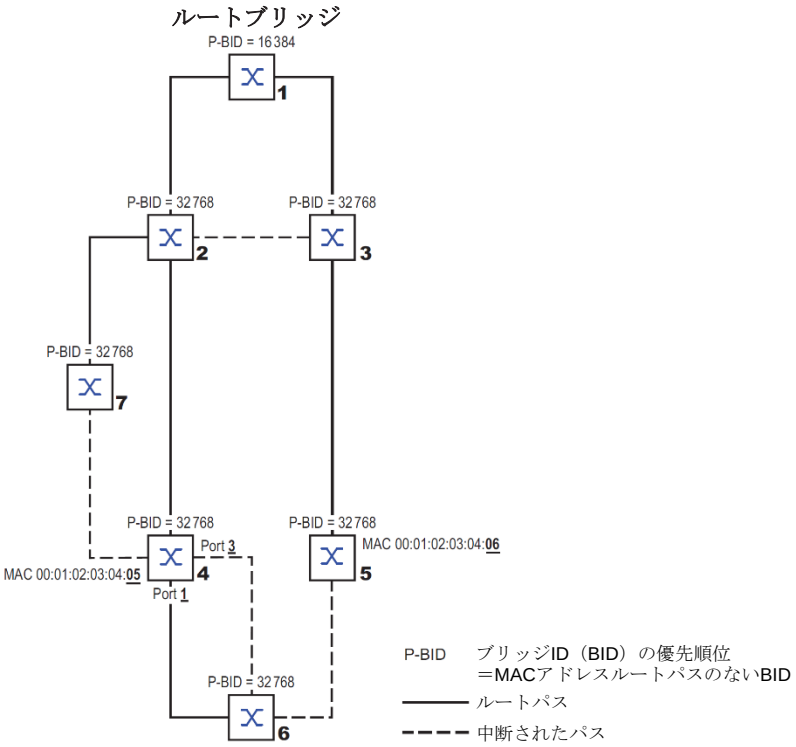


図44 ルートパス決定の参考例

注記：現在のルートブリッジに不具合が起こると、アドミニストレーターがブリッジ識別子のデフォルトブリッジ優先順位をルートブリッジの数値以外は変更しないため、ブリッジ識別子のMACアドレスが単独で、どのブリッジを新規ルートブリッジとするかを判断します。

ルートパス操作の参考例

ルートパスの決定には、ネットワーク計画（図45）を使用してフローチャート（図43）のフローを辿ります。アドミニストレーターは、以下を実行します。

- ブリッジ1及びブリッジ5を除く全てのブリッジにはデフォルト値32768 (8000H)を、
- ブリッジ1は値16384 (4000H)にすることで、ルートブリッジを作成します。
- ブリッジ5には、値28672 (7000H)を割当てます。

ブリッジ3からブリッジ2を介したルートブリッジへの接続はパスコストが高くなるため、ブリッジ2とブリッジ3の間のパスをプロトコルがブロックします。

ブリッジ6からルートブリッジへのパスは興味深いと言えます。

➢ ブリッジ識別子の優先順位の値28672は値32768よりも小さいため、それぞれのブリッジは、ブリッジは5を介したパスを選択します。

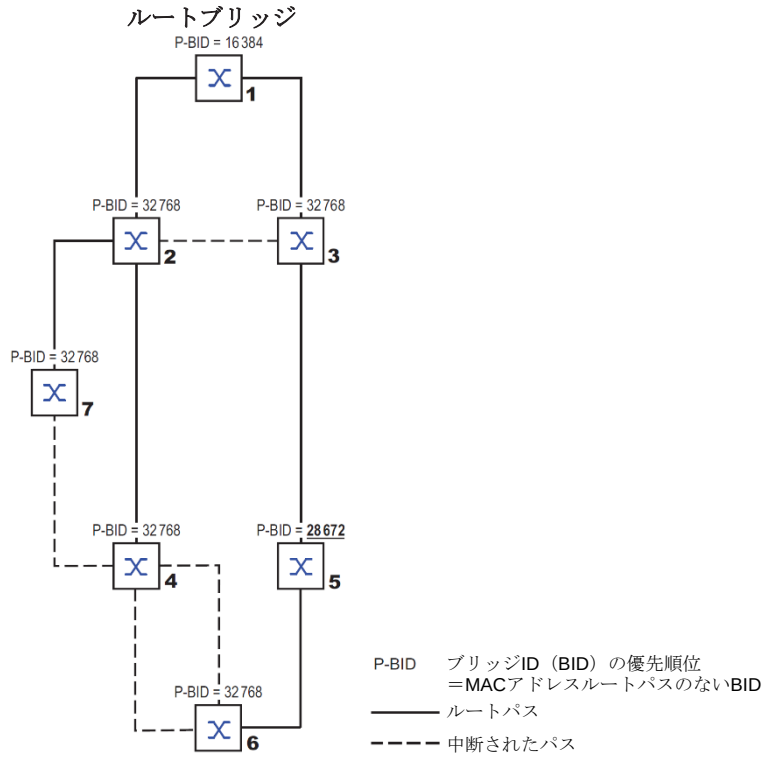


図45 ルートパス操作の参考例

ツリー構造の操作の参考例

管理アドミニストレーターは、ブリッジ1をルートブリッジとしたコンフィグレーションは無効だと気付いたとします。ブリッジ1からブリッジ2及びブリッジ3へのパス上は、ルートブリッジが他の全ブリッジへと送信するコントロールパケットが加算されます。

管理アドミニストレーターがブリッジ2をルートブリッジとして設定すると、コントロールパケットがサブネットワークにかける負荷は、より均等に配分されます。その結果としてできたコンフィグレーションが、図46です。殆どのブリッジからルートブリッジへのパスコストが軽減されました。

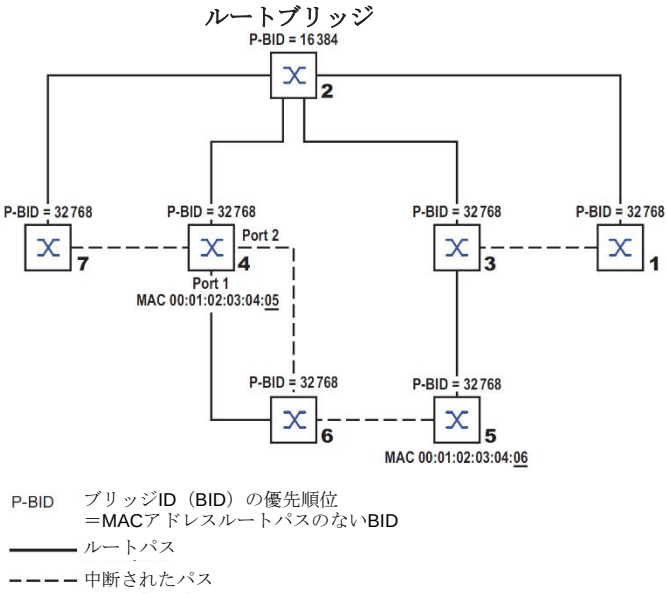


図46　ツリー構造操作の参考例

13.5 RSTP（Rapid Spanning Tree Protocol）

RSTPは、STPがツリーの構造を決定するアルゴリズムと同じアルゴリズムを使用します。リンク又はブリッジに障害が起きた場合、RSTPはパラメーターを変えただけで、再コンフィグレーションの速度を上げる新規パラメーターやメカニズムが追加されます。

この状況では、ポートが重要な役割を担います。

13.5.1 ポートの役割

RSTPは各ポートに以下のいずれかの役割を与えます鵜（図47参照）。

- ルートポート
  ルートポートとは、最も低いパスコストのデータパケットをブリッジがルートブリッジから受信するポートの事です。
  同程度の低いパスコストのポートが複数ある場合、ルートへ繋がるブリッジのブリッジID（指定ブリッジ）は、自身のポートのうちどのポートがルートから距離のあるブリッジ傍のルートポートの役割を担うかを決定します。
  同程度の低いパスコストのブリッジが複数ある場合、ルートへ繋がるブリッジのポートID（指定ブリッジ）を使い、どのポートをローカルのルートポートとして選択するかを、ブリッジが決定します（図43参照）。
  ルートブリッジそのものに、ルートポートはありません。
- 指定ポート
  ネットワークセグメントにあるブリッジで最も低いルートパスコストものが、指定ブリッジとなります。同等のルートパスコストのブリッジが1つ以上ある場合、ブリッジ識別子の数値が最も小さいものが指定ブリッジとなります。このブリッジの指定ポートは、ルートブリッジから離れていくネットワークセグメントと接続するポートとなります。ブリッジが1つ以上のポートを持つネットワークセグメントと接続している場合（例：ハブ経由等）、ブリッジはポートIDの優れたポートに、指定ポートの役割を与えます。
- エッジポート
  追加RSTPブリッジの無いネットワークセグメントは、全て指定ポート1つだけと接続されています。この場合、指定ポートはエッジポートでもあります。エッジポートの特質は、RST BPDU（Rapid Spanning Tree Bridge Protocol Data Units）を受信しない点です。
- オルタネートポート
  ルートブリッジへの接続が失われると、このブロックされたポートがルートポートの役目を引き受けます。オルタネートポートは、ルートポートへの接続のバックアップをするものです。

- バックアップポート
  バックアップポートとは、このネットワークセグメント（RSTPブリッジ無し）の指定ポートへの接続が失われた場合のバックアップをするものです。
- ディセーブルドポート
  ディセーブルドポートとは、スパニングツリーのオペレーションに参加しない、即ちスイッチが切られている又は接続されていないポートのことです。

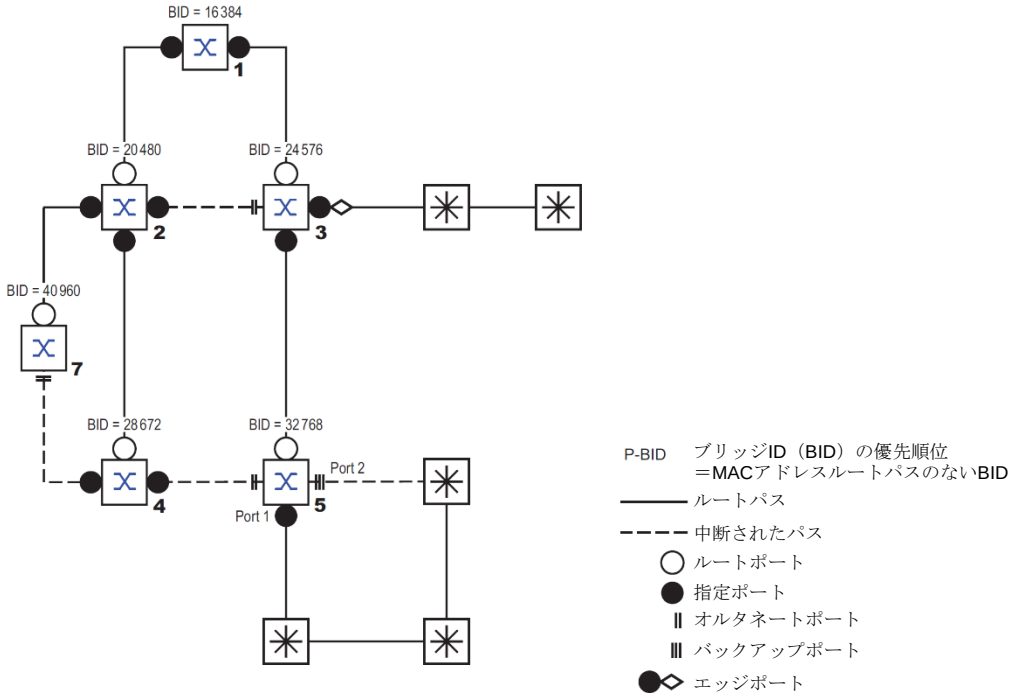


図47　ポートの役割

13.5.2 ポートステート

ツリーの構造及び選択した接続パスのステートによっては、RSTPはポートにそのポートのステートを割当てます。

表36　STP及びRSTPのポートステート値の関係

STPポートステート	管理ブリッジ・ポートステート	MAC オペレーション可否	RSTPポートステート	アクティブトポロジー（ポートロール）
DISABLED	Disabled	FALSE	Discarding[1]	Excluded (disabled)
DISABLED	Enabled	FALSE	Discarding[a]	Excluded (disabled)
BLOCKING	Enabled	TRUE	Discarding[2]	Excluded (alternate, backup)
LISTENING	Enabled	TRUE	Discarding[b]	Included (root, designated)
LEARNING	Enabled	TRUE	Learning	Included (root, designated)
FORWARDING	Enabled	TRUE	Forwarding	Included (root, designated)

1. dot1d-MIBはDisabledを表示
2. dot1d-MIBはBlockedを表示

RSTPポートステートの意味を以下に示します。
- Disabled:ポートはアクティブトポロジーに属しません。
- Discarding:FDBにアドレスラーニング無し、STP-BPDU以外のデータトラフィック無し。

- Learning:アドレスラーニングはアクティブ（FDB）、STP-BPDU以外のデータトラフィック無し。
- Forwarding:アドレスラーニングはアクティブ（FDB）、全パケットタイプの受信及び送信（STP-BPDUに限らず）

13.5.3 Spanning Tree Priority Vector（スパニングツリー・プライオリティベクトル）

ポートにロールを割当てるため、RSTPブリッジは互いにコンフィグレーション情報を交換します。この情報は、Spanning Tree Priority Vector（スパニングツリー・プライオリティベクトル）と呼ばれています。これはRSTP BPDUの一部で、以下の情報が含まれます。

- ルートブリッジのブリッジID
- 送信ブリッジのルートパスコスト
- 送信ブリッジのブリッジID
- メッセージが送信されたポートのポート識別子
- メッセージを受信したポートのポート識別子

上記の情報をもとに、RSTPに参加しているブリッジは自身でポートロールを決定することができ、自身のポートのポートステートを決定することができます。

13.5.4 Fast reconfiguration（ファスト・リコンフィグレーション）

RSTPは何故、ルートパス中断の際にSTPよりも素早く反応できるのでしょうか。

- エッジポートとは
  再コンフィグレーション中、RSTPはエッジポートを3秒後にTransmission （伝送）modeに切り替えます（デフォルト設定）。BPDUを送信しているブリッジが接続されていないことを確実にするために、RSTPはHello Time（ハロータイム）が経過するまで待機します。
  ユーザーはエンドデバイスがこのポートに接続されていて、接続が継続されると確認したら、再コンフィグレーションにおいてこのポートでの待機時間はありません。
- オルタネートポートとは
  通常オペレーションにおいてポートロールが既に分配されているため、ルートブリッジの接続が失われた後、ブリッジはルートポートからオルタネートポートへと即時に切り替えることができます。
- 近隣ブリッジとの通信（ポイント・ツー・ポイント接続）
  近隣ブリッジ間の分散型・直接通信では、スパニングツリートポロジーのステータス変更に待機時間なく反応することができます。
- アドレステーブル
  STPであれば、FDB内エントリーのエージングが通信のアップデートを決定します。再コンフィグレーションに影響されるこれらポートのエントリーを、RSTPは即時に削除します。
- イベントへの反応
  RSTPは如何なるタイム関連の設定に従うことなく、即時に通信の中断や復旧に反応することができます。

注記：RSTPトポロジーの再コンフィグレーション中、データパッケージは、複製及び（又は）受信者に誤った順番で到着することがあります。ユーザーは、STPを使用するか、本書に記載する別の冗長手段を選択することができます。

13.5.5 デバイスのコンフィグレーション

⚠ 警告

機器の誤操作

コンフィグレーションの段階でループができるのを避けるには、*Spanning Tree* コンフィグレーションの各デバイスを個々に設定します。冗長化ラインを接続する前に、*Spanning Tree* の全デバイスのコンフィグレーションを完了させてください。

この指示に従わない場合、人的損害や装置の損傷を招くおそれがあります。

RSTPはネットワークトポロジーを完全に、自律してコンフィグレーションを実行します。ブリッジ優先順位の最も低いデバイスは、自動的にルートブリッジとなります。但し、特定のネットワーク構造を定義するには、いずれかのデバイスをルートブリッジとして指定しなければなりません。通常、基幹回線のデバイスがルートブリッジの役割を担います。

以下の手順を実行します。
- ☐ ユーザーの要件を満たすようネットワークを、当初は冗長化ライン無しで構築します。
- ☐ 関連ポートのフローコントロールはディアクティベートします。
  フローコントロールと冗長機能が同時にアクティブな場合、冗長機能が意図したものと異なるオペレーションを行う可能性があります。（デフォルトでは、フローコントロールは全域でディアクティベートされていて、全ポートでアクティベートされています。）
- ☐ 全デバイスのMRPを無効化します。
- ☐ ネットワーク上の全デバイスのスパニングツリーを有効化します。
  初期設定では、Spanning Treeはデバイス内でスイッチがオンになっています。

以下の手順を実行します。

- ☐ *Switching > L2-Redundancy > Spanning Tree > Global* ダイアログボックスを開きます。
- ☐ 機能を有効化します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`spanning-tree operation`	スパニングツリーを有効化します。
`show spanning-tree global`	確認用にパラメーターを表示します。

ここで冗長化ラインを接続します。

ルートブリッジの役目を担うデバイスの設定を定義します。

以下の手順を実行します。

- ☐ *Priority*フィールドに、低い数字を入力します。
  最も低い数字のブリッジIDを持つブリッジは、優先順位が最高位となり、ネットワークのルートブリッジとなります。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`spanning-tree mst priority 0 <0..61440>` デバイスのブリッジ優先順位を指定します。

注記：ブリッジの優先順位を`0..61440` の範囲で、4096毎単位で指定します。

保存後、ダイアログボックスが以下の情報を表示します。
- *Bridge is root* のチェックボックスにチェックが入っている
- *Root port* フィールドの値が`0.0`を表示
- *Root path cost* フィールドの値が`0`を表示

`show spanning-tree global` 確認用にパラメーターを表示します。

- ☐ 必要であれば、*Forward delay [s]* 及び*Max age* フィールドの値を変更します。
  - ルートブリッジは変更した値を他デバイスへ伝送します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`spanning-tree forward-time <4..30>` ステータス変更の遅延時間を秒単位で指定します。

`spanning-tree max-age <6..40>` 最大許容ブランチ長を指定します（例：ルートブリッジに繋がるデバイス数等）

`show spanning-tree global` 確認用にパラメーターを表示します。

注記：*Forward delay [s]* 及び*Max age* のパラメーターは、以下の相関があります。

Forward delay [s] ≥ (*Max age*/2) + 1

この相関と矛盾する数値をフィールドに入力すると、デバイスはこの数値を、最後に使用した有効な値或いはデフォルト値と置換えます。

注記：可能であれば、Hello Timeフィールドの値は変更しないでください。他デバイスの、以下

数値を確認します。
- 対応するデバイス及びルートブリッジのブリッジID（ブリッジ優先順位及びMACアドレス）。
- ルートブリッジへ繋がるデバイスポートの数。
- デバイスのルートポートからルートブリッジへのパスコスト。

以下の手順を実行します。

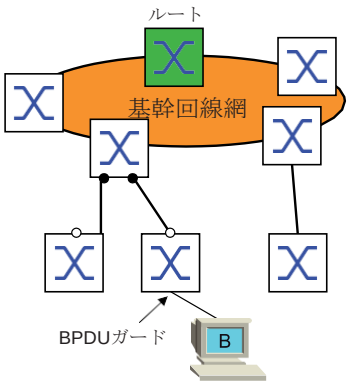
`show spanning-tree global` 確認用にパラメーターを表示します。

13.5.6 ガード（保護）

当デバイスでは、デバイスポートで様々な保護機能（ガード）をアクティベートすることができます。

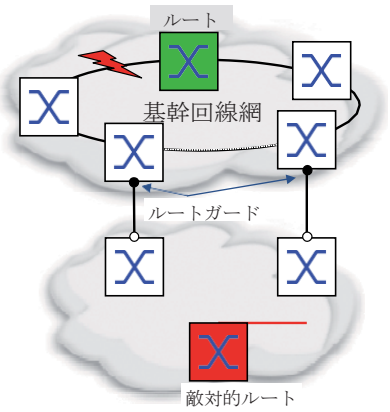
以下の保護機能は、ネットワークを不正確なコンフィグレーションやループ、STP-BPDU攻撃などから保護するものです。

- BPDU Guard：手動で割当てたエッジポート（エンドデバイスポート）。
  この保護機能は、デバイス全域でアクティベートしてください。



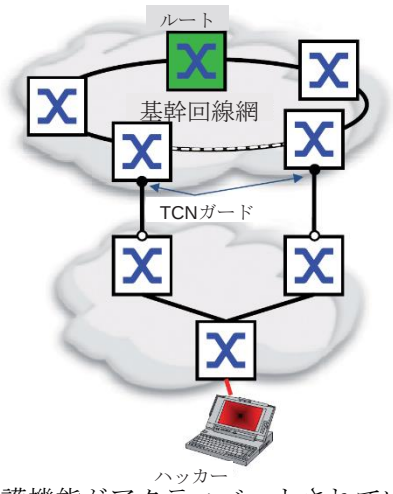
通常、端末デバイスポートは如何なるSTP-BPDUも受信しません。攻撃者がSTP-BPDU攻撃をこのポートに続けるようであれば、デバイスはデバイスポートをディアクティベートします。

- Root Guard：指定ポート用。
  この保護機能は、全デバイスポートで個別にアクティベートします。



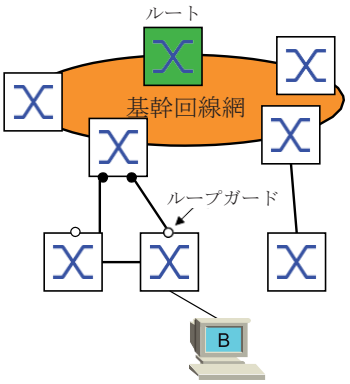
指定ポートがSTP-BPDUをルートブリッジへのより優れたパスで受信すると、デバイスはSTP-BPDUを破棄し、ポートの伝送ステートを`root`の代わりに`discarding`に設定します。ルートブリッジへのより優れたパスのSTP-BPDUが無い場合、*Hello time [s]* ×2回の後、デバイスはポートのステートをポートロールに基づいた値へとリセットします。

- TCN Guard：TCNフラグ付きSTP-BPDUを受信するポート。この保護機能は、全デバイスポートで個別にアクティベートします。



保護機能がアクティベートされていれば、デバイスは受信したSTP-BPDUのTCNフラグを無視します。これによって、デバイスポートのアドレステーブル（FDB）のコンテンツが変わることはありません。但し、トポロジーを変更させるBPDU内の追加情報はデバイスが処理しています。

- Loop Guard：オルタネートポート及びバックアップポート用。
この保護機能は、全デバイスポートで個別にアクティベートします。



ポートがこれ以上のSTP-BPDUを受信しなければ、この保護機能はポートが意図せずに伝送ステータスを`Forwarding`に変更されるのを防止します。このような状況が発生すると、デバイスはポートのループステータスをInconsistentと指定しますが、データパケットを転送することはありません。

BPDUガードのアクティベーション

以下の手順を実行します。

- ☐ *Switching > L2-Redundancy > Spanning Tree > Global* ダイアログボックスを開きます。
- ☐ *BPDU guard* のチェックボックスにチェックを入れます。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable` Privileged Exec Modeに切り替えます。

`configure`	Configuration modeに切り替えます。
`spanning-tree bpdu-guard`	BPDU Guardをアクティベートします。
`show spanning-tree global`	確認用にパラメーターを表示します。

- ☐ *Switching > L2-Redundancy > Spanning Tree > Port* ダイアログボックスを開きます。
- ☐ *CIST* タブに切り替えます。
- ☐ エンドデバイスポートには、*Admin edge port*カラムのチェックボックスにチェックを入れます。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`interface <x/y>`	インターフェース `<x/y>` の Interface Configuration mode に変更します。
`spanning-tree edge-port`	ポートを端末デバイスポート（エッジポート）として指定します。
`show spanning-tree x/y`	確認用にパラメーターを表示します。
`exit`	Interface modeから退出します。

エッジポートがSTP-BPDUを受信すると、デバイスは以下のアクションを起こします。
- ➢ デバイスがこのポートをディアクティベートします。
  Basic Settings > Port ダイアログボックスの *Configuration* タブの、*Port on* カラムのチェックボックスが`unmarked`となります。
- ➢ デバイスがポートを指定します。

BPDUを受信するため、ユーザーはポートが無効化したか否かを判断することができます。以下の手順を実行します。

Switching > L2-Redundancy > Spanning Tree > Port ダイアログボックスの*Guards* タブの *BPDU guard effect* カラムのチェックボックスが`marked`となります。

`show spanning-tree port x/y`	確認用にポートのパラメーターを表示します。*BPDU guard effect* パラメーターの値は`enabled`となります。

デバイスポートのステータスを`forwarding`に設定します。以下の手順を実行します。
- ☐ ポートがまだBPDUを受信している場合：
  - – マニュアル定義したエッジポート（エンドデバイスポート）を削除します
  - – 又は、BPDUガードをディアクティベートします。
- ☐ デバイスポートを再度アクティベートします。

Root Guard / TCN Guard / Loop Guardのアクティベーション

以下の手順を実行します。

- ☐ *Switching > L2-Redundancy > Spanning Tree > Port* ダイアログボックスを開きます。
- ☐ *Guards* タブに切り替えます。
- ☐ 指定ポートには、*Root guard* カラムのチェックボックスにチェックを入れます。
- ☐ TCNフラグ付きのSTP-BPDUを受信するポートは、*TCN guard* カラムのチェックボックスにチェックを入れます。
- ☐ ルートポート、オルタネートポート、バックアップポートについては、*Loop guard* カラムのチェックボックスにチェックを入れます。

注記：*Root guard* 及び*Loop guard* 機能は相互排他的です。*Loop guard* 機能がアクティブな間に*Root guard* 機能のアクティベーションを試みると、デバイスは*Loop guard* 機能をディアクティベートします。

- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`interface <x/y>`	インターフェース `<x/y>` の Interface Configuration mode に変更します。
`spanning-tree guard-root`	指定ポートでRoot Guardをオンに切り替えます。
`spanning-tree guard-tcn`	TCNフラグ付きのSTP-BPDUを受信するポートのTCN Guardをオンに切り替えます。
`spanning-tree guard-loop`	ルートポート、オルタネートポート、バックアップポートのいずれかでLoop Guardをオンに切り替えます。
`exit`	Interface modeから退出します。
`show spanning-tree port x/y`	確認用にポートのパラメーターを表示します。

13.6 Link Aggregation（リンクアグリゲーション）

Single Switch法を使用した*Link Aggregation* 機能により、イーサネットリンク、即ち帯域幅及び冗長性という2つの制限を克服することができます。

Link Aggregation 機能は個別のポートの帯域幅の制限を超えることができます。*Link Aggregation* 機能では、2つ以上のリンクを並列で組合せることができ、デバイス間に論理リンクを1つ作ることができます。
並列リンクは2つのデバイス間のデータトラフィック用帯域幅を増加させます。

通常、*Link Aggregation* 機能は基幹回線網で使用します。この機能は、コストを押さえながらも帯域幅を徐々に増加させることができます。

更に、*Link Aggregation* 機能は冗長化並びにシームレスなフェイルオーバーを提供します。2つ以上で構成されたリンクのうちの1つがダウンすると、グループ内の他リンクがトラフィックを転送し続けます。

新規*Link Aggregation* のインスタンスのデフォルト設定は以下の通りです。
- *Active* カラムのチェックボックスにチェックが入っている。
- *Send trap (Link up/down)* カラムのチェックボックスにチェックが入っている。
- *Static link aggregation* カラムのチェックボックスにチェックが入っていない。
- *Active ports (min.)* カラムの値が 1。

13.6.1 オペレーションの方法

デバイスはSingle Switch法でオペレーションを行います。Single Switch法は、コストを押さえながらもネットワークを成長させることができます。Single Switch法は、リンクの両側それぞれにデバイス１つを、物理ポートに対して設けることとなっています。デバイスは、グループメンバーのポート全域でトラフィックの負荷を軽減します。

また、デバイスはグループメンバーポートが全二重、且つ同一伝送レートのポイント・ツー・ポイントリンクで、Same Link Speed法を使用します。グループに最初に加えたポートがマスターポートとなり、リンクアグリゲーショングループのメンバーである他ポートの帯域幅を決定します。

当デバイスでは、リンクアグリゲーショングループを2つまで設定することができます。リンクアグリゲーション毎に使用できるポート数は、デバイスによります。

13.6.2 Link Aggregation（リンクアグリゲーション）

⚠ 警告

機器の誤操作

コンフィグレーションの段階でループができるのを避けるには、*Link Aggregation* コンフィグレーションの各デバイスを個々に設定します。冗長化ラインを接続する前に、*Link Aggregation* の全デバイスのコンフィグレーションを完了させてください。

この指示に従わない場合、人的損害や装置の損傷を招くおそれがあります。

1つのアグリゲートリンク（Aggregated Link）グループを使用して、スイッチ１及びスイッチ2の間に複数のワークステーションを接続します。複数リンクを集約（アグリゲート）することで、ハードウェアをアップグレードすることなく高速化することができます。

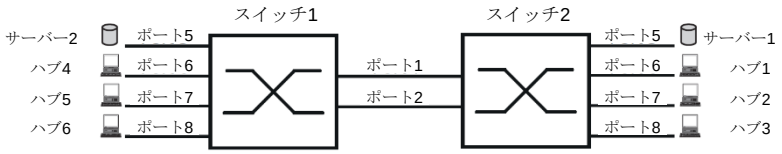


図48　リンクアグリゲーション　Switch to Switch ネットワーク

グラフィカルユーザーインターフェース内でスイッチ1及びスイッチ2のコンフィグレーションを実行します。以下の手順を実行します。

- ☐ *Switching > L2-Redundancy > Link Aggregation* ダイアログボックスを開きます。
- ☐  ボタンをクリックします。
  ダイアログが*Create* ウィンドウを表示します。
- ☐ *Trunk port* ドロップダウンリストから、リンクアグリゲーショングループのインスタンス番号を選択します。
- ☐ *Port* ドロップダウンリストから、ポート*1/1*を選択します。
- ☐ *Ok* ボタンをクリックします。
- ☐ 前述の手順を繰り返いし、ポート*1/2*を選択します。
- ☐ *Ok* ボタンをクリックします。
- ☐  ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`link-aggregation add lag/1`	Link Aggregation Group `lag/1`を作成します。
`link-aggregation modify lag/1 addport 1/1`	ポート*1/1* をリンクアグリゲーショングループに追加します。
`link-aggregation modify lag/1 addport 1/2`	ポート*1/2* をリンクアグリゲーショングループに追加します。

13.7 リンクバックアップ

リンクバックアップは、レイヤー2デバイスのトラフィックに冗長リンクを提供します。デバイスが一次リンクにエラーを検知すると、デバイスはバックアップリンクにトラフィックを転送します。通常、リンクバックアップはサービスプロバイダーやエンタープライズネットワークで使用されます。

バックアップリンクはペアで設定し、ペアの片方を一次、もう片方をバックアップとします。例えばエンタープライズネットワークを冗長化する場合、当デバイスでは1つ以上のペアを設定できます。リンクバックアップの最大ペア数は、物理ポートの総数÷2です。更に、リンクバックアップのペアに参加しているポートのステータスが変更されると、デバイスはSNMPトラップを送信します。

リンクバックアップのペアのコンフィグレーションをする際は、以下のルールにご留意ください。
- リンクのペアは、物理ポートのあらゆる組合せを含みます。例えば、あるポートが100Mbitで、もう片方が1000Mbit SFPポートの場合もあります。
- あらゆる所定の時間内におけるリンクバックアップペアには、特定のポートがメンバーとなっています。
- リンクバックアップペアのポートは、同一VLANの同一VLAN IDのメンバーであることを確認します。一次ポート又はバックアップポートがVLANのメンバーであれば、同一VLANにペアとなる2次ポートを指定します。

この機能のデフォルト設定は、リンクバックアップペアが無いとInactive（非アクティブ）となっています。

注記：リンクバックアップポートで、スパニングツリープロトコルが無効になっていることを確認してください。

13.7.1 フェイルバックの概要

リンクバックアップは、フェイルバックをオプションとして選択することもできます。フェイルバック機能をアクティベートして一次リンクが通常オペレーションに戻ると、デバイスは最初にバックアップポートのトラフィックをブロックし、一次ポートにトラフィックを転送します。このプロセスは、デバイスがネットワークのループの原因となることから保護します。

一次ポートがリンクに復帰しアクティブなステータスになると、デバイスは2つのオペレーションモードをサポートします。
- *Fail back*をインアクティベート（Inactivate）すると、ポートはバックアップリンクが障害を起こすまでブロック状態を維持します。
- *Fail back*をアクティベートし、*Fail back delay [s]* タイマーが経過した後、一次ポートはForwardingステータスに戻り、バックアップポートがDown状態へと切り替わります。

上記のケースでは、ポートがリンクに強制的にトラフィックを転送すると、最初に「flush FDB」パケットをリモートデバイスに送信します。フラッシュパケットは、リモートデバイスがMACアドレスを素早く再ラーニングするための助けになります。

13.7.2 コンフィグレーション例

⚠ 警告

機器の誤操作

コンフィグレーションの段階でループができるのを避けるには、*Link Backup* コンフィグレーションの各デバイスを個々に設定します。冗長化ラインを接続する前に、*Link Backup* の全デバイスのコンフィグレーションを完了させてください。

この指示に従わない場合、人的損害や装置の損傷を招くおそれがあります。

以下のネットワーク参考例では、スイッチAのポート*2/3* 及び*2/4* を、アップリンクスイッチB及びスイッチCに接続します。ポートをリンクバックアップペアとしてセットアップすると、1つのポートがトラフィックを転送し、もう片方のポートがBlockingモードになります。

一次側、即ちスイッチAのポート*2/3*は、アクティブポートとなりトラフィックをスイッチBのポート1へ転送します。スイッチAのポート*2/4*はバックアップポートとなり、トラフィックをブロックします。

エラーを検知したためにスイッチAがポート*2/3*を無効化した場合、スイッチAのポート*2/4* はトラフィックをスイッチCのポート2へと転送を開始します。

ポート*2/3* のステータスがアクティブに戻り、*Fail back* がアクティベートされた状態のno shutdownでは、*Fail back delay [s]*は30秒に設定されます。
[s] タイマーが経過すると、ポート*2/4* は最初にトラフィックをブロックし、次にポート*2/3* がトラフィックの転送を開始します。

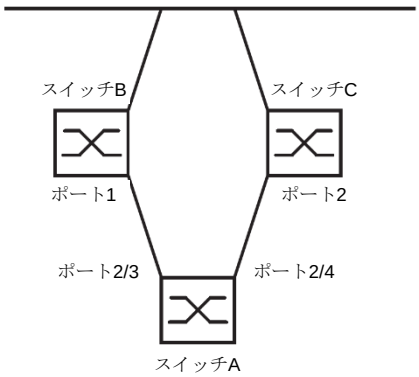


図49 Link Backupネットワーク参考例

以下のテーブルにはスイッチAのパラメーターのコンフィグレーション例を含みます。

以下の手順を実行します。

- ☐ *Switching > L2-Redundancy > Link Backup* ダイアログボックスを開きます。
- ☐ テーブルに新規のリンクバックアップペアを入力します。
  - ☐ ボタンをクリックします。
    ダイアログが*Create* ウィンドウを表示します。
  - ☐ *Primary port* ドロップダウンリストから、ポート*2/3*を選択します。*Backup port* ドロップダウンリストから、ポート*2/4*を選択します。
  - ☐ *Ok* ボタンをクリックします。
- ☐ *Description* で、バックアップペアの名前として`Link_Backup_1` を入力します。
- ☐ リンクバックアップペアの*Fail back* 機能をアクティベートするには、*Fail back* チェックボックスにチェックを入れます。

- リンクバックアップペア用にフェイルバックタイマーを設定するために、*Fail back delay [s]*に30 秒と入力します。
- リンクバックアップをアクティベートするには、*Active* チェックボックスにチェックを入れます。
- 機能を有効化するには*Operation* フレームの*On* のラジオボタンを選択します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`interface 2/3`	インターフェース2/3のInterface Configuration mode に変更します。
`link-backup add 2/4`	ポート*2/3* を一次ポート、ポート*2/4* をバックアップポートとするリンクバックアップインスタンスを作成します。
`link-backup modify 2/4 description Link_Backup_1`	ストリング`Link_Backup_1` をバックアップペア名として指定します。
`link-backup modify 2/4 failback-status enable`	フェイルバックタイマーを有効化します。
`link-backup modify 2/4 failback-time 30`	フェイルバック遅延タイムを30 秒に指定します。
`link-backup modify 2/4 status enable`	リンクバックアップインスタンスを有効化します。
`exit`	Configuration modeに切り替えます。
`link-backup operation`	*Link Backup* 機能をデバイス全域で有効化します。

13.8 FuseNet

FuseNet プロトコルでは、以下いずれかの冗長プロトコルでオペレーションを行うリングのカプリングを、ユーザーが行います。

- MRP
- HiPERリング
- RSTP

注記：*Ring/Network Coupling* プロトコルを使用してネットワークをメインリングとカプリングする条件は、接続されたネットワークが*Ring/Network Coupling* プロトコルをサポートするネットワークデバイスのみを含むことです。

以下のテーブルを参考に、ご使用のネットワークに適用する*FuseNet* カプリングプロトコルを選択します。

メインリング	接続されたネットワーク		
	のMRP	HiPERリング	RSTP
MRP	*Sub Ring*1)	*Ring/Network Coupling*	*Ring/Network Coupling*
HiPERリング	*Sub Ring*	*Ring/Network Coupling*	– *Ring/Network Coupling*
RSTP	–	–	–

– 適切なカプリングプロトコル無し

1) 異なるVLANに*MRP*がコンフィグレーションされていること

13.9 サブリング

Sub Ring 機能は、MRP（メディア冗長プロトコル）を拡張させたものです。この機能では、各種ネットワーク構造を使用してサブリングをメインリングとカプリングすることができます。

サブリングプロトコルは、フラットでないネットワークの両端をメインリングとカプリングするデバイスを冗長化します。

サブリングをセットアップすることで以下の利点を得ることができます。
- ➢ カプリングのプロセスにて、冗長コンセプトに新規のネットワークセグメントを含めます。
- ➢ サブリングは、新規エリアと既存ネットワークとの統合を簡略化します。
- ➢ サブリングがあれば、ネットワークトポロジーのエリアの組織的構造を簡単にマッピングすることができます。
- ➢ MRPリングにおける冗長化されたサブリングのフェイルオーバータイムは通常100ms未満です。

13.9.1 サブリングの概要

サブリングのコンセプトでは、新規ネットワークセグメントを既存リング（メインリング）の適切なデバイスとカプリングすることができます。サブリングとメインリングのカプリングにユーザーが使用するデバイスは、SRM（サブリングマネジャー）です。

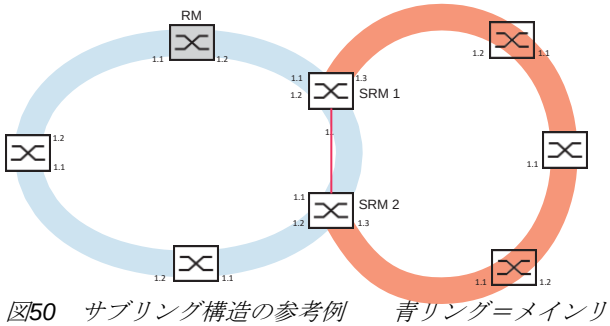


図50　サブリング構造の参考例　　青リング＝メインリング
橙リング＝サブリング
赤線＝サブリングSRMの冗長リンク＝サブリングマネジャー
RM＝Ring Manager（リングマネジャー）

サブリングマネジャーとして稼働できるデバイスは、8つのインスタンスまでサポートできる故、同時に8つのサブリングを管理することができます。

Sub Ring 機能では、MRPをサポートするデバイスを参加者として統合することができます。サブリングとメインリングのカプリングにユーザーが使用するデバイスは、*Sub Ring* マネジャー機能が必要です。

各サブリングは、サブリングマネジャー及びサブリングマネジャーとメインリング間のデバイスを除く、最大200参加者までで構成することができます。

構成可能なサブリングトポロジーの参考例を以下に示します。

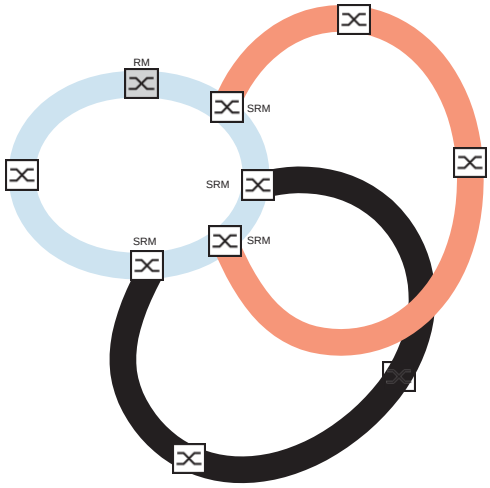


図51　重複するサブリング構造の参考例

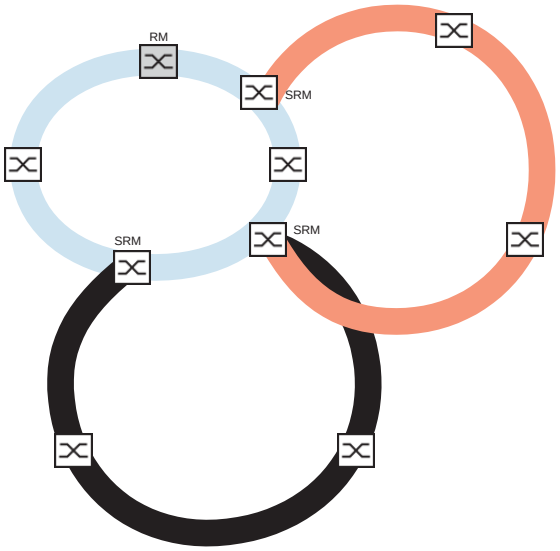


図52　特殊例：サブリングマネジャーが、サブリング2つを管理（インスタンス2つ）。
サブリングマネジャーは、インスタンス最大8つまで管理可能。

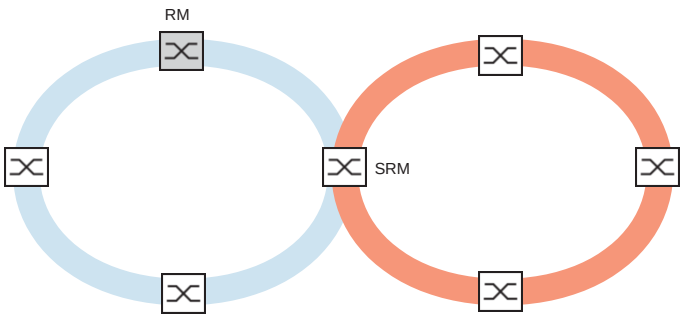


図53　特殊例：サブリングマネジャーが異なるポートでサブリングの両端を管理（Single Subring Manger）

注記：上記の例では、サブリングマネジャーはサブリングと既存メインリングとをカプリングするだけです。*Sub Ring* 機能はカスケード型サブリングを禁止します。例えば、新規サブリングと既存の別サブリングのカプリング。

メインリングとサブリングにMRPを使用する場合は、VLAN設定を以下のように指定します。
➢ メインリングのVLAN X
– メインリング参加者のリングポートに
– サブリングマネジャーのメインリングポートに
➢ サブリングのVLAN Y
– サブリング参加者のリングポートに
– サブリングマネジャーのサブリングポートに　　複数サブリングに、同じVLANを使用できます。

13.9.2 サブリング参考例

以下の例では、デバイス3つを構成する新規ネットワークセグメントを、MRPプロトコルを使用する既存メインリングにカプリングします。ネットワークを片端でなく両端でカプリングする場合、サブリングは対応するコンフィグレーションによって可用性を拡大します。

新規ネットワークセグメントをサブリングとしてカプリングします。サブリングを、以下コンフィグレーションを使用してメインリングの既存デバイスにカプリングをします。

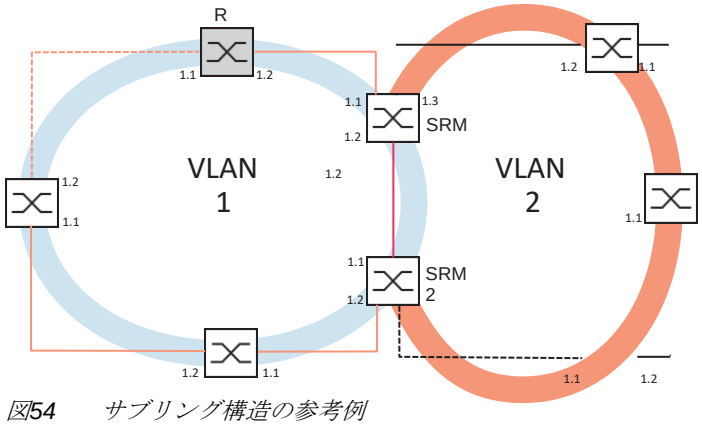


図54　サブリング構造の参考例
橙線＝VLAN1のメインリングメンバー
黒線＝VLAN2のサブリングメンバー
橙破線＝メインリングのループオープン
黒破線＝サブリングのループオープン
赤線＝VLAN1 SRMの冗長リンクメンバー＝サブリングマネジャー
RM＝Ring Manager（リングマネジャー）

サブリングのコンフィグレーションには、以下の手順を実行します。
☐ 新規ネットワークセグメントのデバイス3つをMRP参加者としてコンフィグレーションします。
– 以下テーブルを参考に、リングポートの伝送レート及びDuplex modeのコンフィグレーションを行います。

表37　サブリングポートのポート設定

ポート種別	ビットレート	ポートの状態	自動コンフィグレーション	手動コンフィグレーション
TX	100 Mbit/s	marked	unmarked	*100 Mbit/s FDX*
TX	1 Gbit/s	marked	marked	–
光	100 Mbit/s	marked	unmarked	*100 Mbit/s FDX*
光	1 Gbit/s	marked	marked	–
光	2.5 Gbit/s	marked	–	*2.5 Gbit/s FDX*

以下は、サブリングコンフィグレーションの追加設定の手順です。

- ☐ コンフィグレーションの際にループができることを防ぐため、メインリング及びサブリングのデバイスのサブリングマネジャー機能をディアクティベートします。メインリングに参加している全デバイスのコンフィグレーションを完全に実行したら、全域での*Sub Ring* 機能及びサブリングマネジャーをアクティベートします。
- ☐ サブリングで使用するMRPリングポートのラピッドスパニングツリープロトコル機能を無効化します。
- ☐ メインリング及びサブリングに参加しているポートの*Link Aggregation* 機能が非アクティブであることを確認します。
- ☐ メインリングがMRPプロトコルを使用していても、メインリングポート及びサブリングポートのVLANメンバーシップは異なるよう指定します。例えば、メインリング及び冗長リンクにはVLAN ID1を、サブリングにはVLAN ID2を使用します。
  - 参考例として、メインリングに参加しているデバイスの*Switching > VLAN > Configuration* ダイアログボックスを開きます。静的VLANテーブルにVLAN 1を作成します。VLAN1でメンバーシップ用にメインリングポートにタグを付ける場合、該当するポートのカラムから、ドロップダウンリストのT を選択します。
  - サブリングに参加しているデバイスについては、上記手順を行い、静的VLANテーブルのポートにVLAN2を追加します。

- ☐ メインリング及びサブリングのデバイス用の*MRP*機能をアクティベートします。
  - *Switching > L2-Redundancy > MRP* ダイアログボックスで、メインリングデバイスのリングポート2つのコンフィグレーションを実行します。
  - サブリングに参加しているデバイスについては、上記手順を行い、サブリングに参加しているサブリングデバイスの、リングポート2つのコンフィグレーションを実行します。
  - メインリング及びサブリングデバイスに、同じMRPドメインを割当てます。シュナイダーエレクトリック製デバイスのみを使用している場合、MRPドメインIDはデフォルト値で問題ありません。

注記：*MRP domain* は、0から255までの16個連続する数字です。デフォルト値は、次の通りです。255 .255 .255 .255 .255 .255 .255 .255 .255 .255 .255 .255 .255 .255 .255 .255.全てゼロの*MRP domain* は無効です。

Sub Ring ダイアログボックスでは、MRPドメインIDを変更することができます。別の方法としてコマンドラインインターフェースを使用します。以下の手順を実行します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`mrp domain delete`	現在のMRPドメインを削除します。
`mrp domain add domain-id 0.0.1.1.2.2.3.4.4.111.222.123.0.0.66.99`	指定したMRPドメインIDで新規MRPドメインを作成します。以降のMRPドメイン変更は、このドメインIDに適用されます。

13.9.3 サブリングコンフィグレーションの参考例

⚠ 警告

機器の誤操作

コンフィグレーションの段階でループができるのを避けるには、*Sub Ring* コンフィグレーションの各デバイスを個々に設定します。冗長化ラインを接続する前に、リングの全デバイスのコンフィグレーションを完了させてください。

この指示に従わない場合、人的損害や装置の損傷を招くおそれがあります。

注記：コンフィグレーションの段階でループができるのを避けてください。サブリングの全デバイスを個別に設定します。冗長リンクをアクティベートする前に、サブリングの全デバイスを完全に設定してください。

サブリングマネジャー2つのコンフィグレーション例を示します。以下の手順を実行します。

- ☐ *Switching > L2-Redundancy > Sub Ring* ダイアログボックスを開きます。
- ☐ テーブルエントリーを追加するには、  ボタンをクリックします。
- ☐ *Port* カラムで、デバイスをサブリングにカプリングするポートを選択します。この例では、ポート*1/3*を使用します。
  カプリングするには、メインリングに既に接続されているポート以外の有用なポートのうち1つを使用します。
- ☐ *Name* カラムで、サブリングの名前を指定します。この例では、`Test`と入力します。
- ☐ *SRM mode* カラムで、Subring Manager modeを選択します。
  これで、サブリングからメインリングをカプリングをどのポートが行い、Redundant Manager（冗長マネジャー）になるかを指定したこととなります。
  カプリングのオプションは以下の通りです。
  - ➢ `manager`
    いずれものサブリングマネジャーに同じ値を指定すると、MACアドレスの高い方のデバイスが冗長リンクを管理します。
  - ➢ `redundant manager`
    サブリングマネジャーを`manager`と指定すれば、デバイスは冗長リンクを管理します。
    指定がないと、MACアドレスの高い方のデバイスが冗長リンクを管理します。

  この例を表した図に従い、Subring Manager 1を`manager`と指定します。
- ☐ *VLAN* カラム及び*MRP domain* カラムの値は変更しません。このコンフィグレーション例では、デフォルト値が正しい値となっています。
- ☐  ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`sub-ring add 1`	サブリングID `1`で新規のサブリングを作成します。
`sub-ring modify 1 port 1/3`	ポート*1/3*をサブリングポートとして指定します。
`sub-ring modify 1 name Test`	サブリング`1`に名前`Test` を指定します。
`sub-ring modify 1 mode manager`	サブリング`1`に`manager` modeを指定します。
`show sub-ring ring`	当該デバイスのサブリングステートを表示します。
`show sub-ring global`	当該デバイスのサブリングのグローバルステートを表示します。

- ☐ 2つ目のサブリングも同様の手順でコンフィグレーションします。
  この例を表した図に従い、Subring Manager 2を`redundant manager`と指定します。

- ☐ サブリングマネジャー機能をアクティベートするには、該当する行の*Active* チェックボックスにチェックを入れます。
- ☐ サブリングに参加するサブリングマネージャー及びデバイスの両方のコンフィグレーションを実行したら、機能を有効化して冗長リンクを閉じます。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`sub-ring enable 1`	サブリング`1`をアクティベートします。
`sub-ring enable 2`	サブリング`2`をアクティベートします。
`enable`	Privileged Exec Modeに切り替えます。
`show sub-ring ring <Domain ID>`	選択したサブリングの設定を表示します。
`show sub-ring global`	サブリングのグローバル設定を表示します。
`copy config running-config nvm profile Test`	不揮発性メモリ（`nvm`）内の`Test` 名のコンフィグレーションプロファイルにある現在の設定を保存します。

13.10 LAGを含むサブリング

⚠ 警告

機器の誤操作

コンフィグレーションの段階でループができるのを避けるには、*Sub Ring* コンフィグレーションの各デバイスを個々に設定します。冗長化ラインを接続する前に、リングの全デバイスのコンフィグレーションを完了させてください。

この指示に従わない場合、人的損害や装置の損傷を招くおそれがあります。

デバイス間に少なくとも2本の並列冗長ライン（トランク）があり、これらのラインが一つの論理接続をしている場合をリンクアグリゲーション（LAG：Link Aggregation）接続と呼びます。

当デバイスではLAGポートを、*Sub Ring* プロトコルのリングポートとして使用できます。

13.10.1 例

以下にMRPリング及びサブリング間の簡単な設定の例を示します。

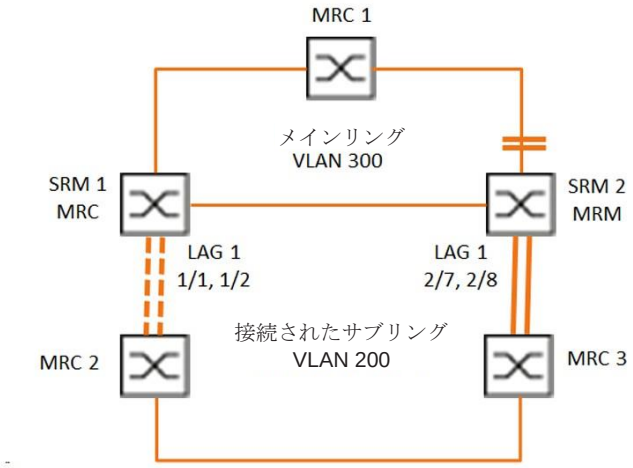


図55　リンクアグリゲーションを含むサブリング

以下のテーブルは、上記の図にあるデバイスのロールを示したものです。テーブルにはリングポート及びサブリングポートをLAGポートとして使用する際の情報を記載します。

表38　デバイス、ポート、ロール

デバイス名	リングポート	メインリングのロール	サブリングのロール	サブリングポート
MRC1	1/3, 1/4	MRPクライアント	-	-
SRM1	1/3, 1/4	MRPクライアント	冗長マネジャー	lag/1
SRM2	2/4, 2/5	MRPマネージャー	マネージャー	lag/1
MRC2	lag/1, 1/3	-	MRPクライアント	-
MRC3	lag/1, 1/3	-	MRPクライアント	-

MRPリングのコンフィグレーション

メインリングに参加しているデバイスは、VLAN 300のメンバーです。以下の手順を実行します。

SRM2

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`mrp domain add default-domain`	ID `default- domain`で新規MRPドメインを作成します。
`mrp domain modify portprimary 2/4`	ポート*2/4* をリングポート`1`として指定します。
`mrp domain modify portsecondary 1/2`	ポート*2/5* をリングポート`2`として指定します。
`mrp domain modify mode manager`	デバイスが*Ring manager*として作動することを指定します。 *Ring manager* 機能を他デバイスでアクティベートしないでください。
`mrp domain modify operation enable`	MRPリングをアクティベートします。
`mrp domain modify vlan 300`	VLAN IDを`300`で指定します。
`mrp operation`	デバイスの*MRP* 機能を有効化します。

MRC1, SRM1

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`mrp domain add default-domain`	ID `default- domain`で新規MRPドメインを作成します。
`mrp domain modify portprimary 1/3`	ポート*1/3* をリングポート`1`として指定します。
`mrp domain modify portsecondary 1/4`	ポート*1/4* をリングポート`2`として指定します。
`mrp domain modify mode client`	デバイスのロールをリングクライアントとして指定します。
`mrp domain modify operation enable`	MRPリングをアクティベートします。
`mrp domain modify vlan 300`	VLAN IDを`300`で指定します。
`mrp operation`	デバイスの*MRP* 機能を有効化します。

サブリングのコンフィグレーション

接するサブリングに参加しているデバイスは、VLAN 200のメンバーです。

以下の手順を実行します。

SRM1

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`link-aggregation add lag/1`	Link Aggregation Group `lag/1`を作成します。
`link-aggregation modify lag/1 addport 1/1`	ポート*1/1* をリンクアグリゲーショングループに追加します。
`link-aggregation modify lag/1 addport 1/2`	ポート*1/2* をリンクアグリゲーショングループに追加します。
`link-aggregation modify lag/1 adminmode`	Link Aggregation Groupをアクティベートします。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`sub-ring add 1`	サブリングID `1`で新規のサブリングを作成します。
`sub-ring modify 1 name SRM1`	サブリング`1`に名前`SRM1` を指定します。
`sub-ring modify 1 mode redundant-manager vlan 200 port lag/1`	サブリング`1`で、デバイスにロール`Sub-ring redundant manager`を割当てます。サブリングが閉じている場合、デバイスはリングポートをブロックします。VLAN `200` は、ドメインのVLAN IDに設定されています。`lag/1` ポートは、VLAN `200`のメンバーとして設定されています。
`sub-ring enable 1`	サブリング`1`をアクティベートします。
`sub-ring operation`	このデバイスのglobal Subring Manager機能を有効化します。

SRM2

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`link-aggregation add lag/1`	Link Aggregation Group `lag/1`を作成します。
`link-aggregation modify lag/1 addport 2/7`	ポート*2/7*をリンクアグリゲーショングループに追加します。
`link-aggregation modify lag/1 addport 2/8`	ポート*2/8*をリンクアグリゲーショングループに追加します。
`link-aggregation modify lag/1 adminmode`	Link Aggregation Groupをアクティベートします。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`sub-ring add 1`	サブリングID `1`で新規のサブリングを作成します。
`sub-ring modify 1 mode manager vlan 200 port lag/1`	サブリング`1`で、デバイスにロール`Subring manager` を割当てます。VLAN `200` は、ドメインのVLAN IDに設定されています。`lag/1` ポートは、VLAN `200`のメンバーとして設定されています。

`sub-ring modify 1 name SRM2`	サブリング`1`に名前`SRM2` を指定します。
`sub-ring enable 1`	サブリング`1`をアクティベートします。
`sub-ring operation`	このデバイスのglobal Subring Manager機能を有効化します。

`MRC 2, 3`

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`mrp domain add default-domain`	ID `default- domain`で新規MRPドメインを作成します。
`mrp domain modify portprimary lag/1`	ポート`lag/1` をリングポート`1`として指定します。
`mrp domain modify portsecondary 1/3`	ポート*1/3* をリングポート`2`として指定します。
`mrp domain modify mode client`	デバイスのロールをリングクライアントとして指定します。
`mrp domain modify operation enable`	MRPリングをアクティベートします。
`mrp domain modify vlan 200`	VLAN IDを`200`で指定します。
`mrp operation`	デバイスの*MRP* 機能を有効化します。

STPを無効にする

MRPポート又はサブリングポートと指定したポート全ての*Spanning Tree* 機能を無効化します。この例では、ポートを*1/3*使用します。

以下の手順を実行します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`interface 1/3`	インターフェース`1/3`のInterface Configuration mode に変更します。
`no spanning-tree operation`	ポートの*Spanning Tree* 機能を無効化します。

13.11 リング/ネットワークのカプリング

リング上では、*Ring/Network Coupling* 機能はリング又はネットワークセグメントを冗長的にカプリングします。
Ring/Network Coupling は、リング2つとネットワークセグメントを、2つの別パスから接続します。

カプリングされたネットワーク内のデバイスがシュナイダーエレクトリック製であれば、*Ring/Network Coupling*機能は、一次及び二次リング内のリングプロトコルに従いカプリングをサポートします。

- HiPERリング
- Fast HiPERリング
- MRP

Ring/Network Coupling 機能は、バス及びメッシュ構造のネットワークセグメントのカプリングをすることもできます。

13.11.1 リング/ネットワークのカプリングの方法

One-Switchカプリング

最初のリング/ネットワーク内のデバイス**1つ**のポート2つは、2つ目のリング/ネットワークのデバイス2つのポート各1つに接続します（図56参照）。One-Switchカプリング法では、基幹ラインがデータを転送し、デバイスが冗長化ラインをブロックします。

基幹ラインが機能しなくなると、デバイスは即時に冗長化ラインのブロックを解除します。基幹ラインが復旧すると、デバイスは冗長化ラインのデータをブロックします。基幹ラインは、再びデータを転送します。

リングのカプリングは、500ms（通常150ms）以内にエラーの検知・処理します。

Two-Switchカプリング

最初のリング/ネットワーク内のデバイス**2つ**のポート各1つは、2つ目のリング/ネットワークセグメントのデバイス2つのポート各1つに接続します（図58参照）。

冗長化ラインのデバイス及び基幹ラインのデバイスは、イーサネット又はコントロールラインを介したコントロールパケットを使用して自身のオペレーション状況を相互に通知します。

基幹ラインが機能しなくなると、冗長化デバイス（スタンバイ）は即時に冗長化ラインのブロックを解除します。基幹ラインが復旧すると、基幹ラインのデバイスは冗長化デバイスにこれを通知します。スタンバイデバイスは、冗長化ラインのデータをブロックします。基幹ラインは、再びデータを転送します。

リングのカプリングは、500ms（通常150ms）以内にエラーを検知・処理します。

カプリングのコンフィグレーションの種別は、主にネットワークトポロジー及び任意の可用性レベルにより決定します（表39参照）。

表39　冗長カプリングのコンフィグレーションの種別選択基準

	One-Switchカプリング	Two-Switchカプリング	Two-Switchカプリング、コントロールライン有り
用途	デバイス2つは、トポロジー不可の位置にあります。 従って、これらの間にリンクを配置することは、Two-Switchカプリングにおいては多くの労力を要します。	デバイス2つは、トポロジー実行可能な位置にあります。 コントロールラインをインストールすることは、多くの労力を要します。	デバイス2つは、トポロジー実行可能な位置にあります。 コントロールラインをインストールすることは、多くの労力を要します。
欠点	冗長カプリング用にコンフィグレーションしたスイッチが作動不能になると、ネットワーク間の接続が存在しなくなります。	（One-Switchカプリングと比較して）デバイス2つをネットワークに接続するのに更なる労力を要します。	（One-Switch及びTwo-Switchカプリングと比較して）デバイス2つをネットワークに接続するのに更なる労力を要します。
利点	（Two-Switchカプリングと比較して）2つのデバイスをネットワークに接続する労力は少なくなります。	冗長カプリングにコンフィグレーションしたデバイスの1つが作動不能になっても、カプリングしたネットワークは接続を維持します。	冗長カプリングにコンフィグレーションしたデバイスの1つが作動不能になっても、カプリングしたネットワークは接続を維持します。 カプリングするデバイス間のパートナー決定が、コントロールライン無しの場合よりも安全で速くなります。

13.11.2　リング/ネットワークのカプリングの準備

⚠ 警告

機器の誤操作

コンフィグレーションの段階でループができるのを避けるには、*Ring/Network Coupling* コンフィグレーションの各デバイスを個々に設定します。冗長化ラインを接続する前に、リングの全デバイスのコンフィグレーションを完了させてください。

ループになるのを防ぐために、RSTPが無効化されたポートのみで*Ring/Network Coupling* 機能を使用します。

この指示に従わない場合、人的損害や装置の損傷を招くおそれがあります。

ダイアログボックスの画像を使用し、*Ring/Network Coupling*内のデバイスのロールを定義してください。以下のスクリーンショットや図の凡例を示します。

- 青の囲い及び青線：デバイス又は説明されているアイテムの接続
- 実線：基幹の接続

- 破線：スタンバイ接続
- 点線：コントロールライン

以下の手順を実行します。

- ☐ *Switching > L2-Redundancy > Ring/Network Coupling* ダイアログボックスを開きます。
- ☐ *Mode* フレームの *Type* オプションリストで、任意のラジオボタンを選択します。
  - *one-switch coupling*
  - *two-switch coupling, master*
  - *two-switch coupling, slave*
  - *two-switch coupling with control line, master*
  - *two-switch coupling with control line, slave*

One-Switchカプリング

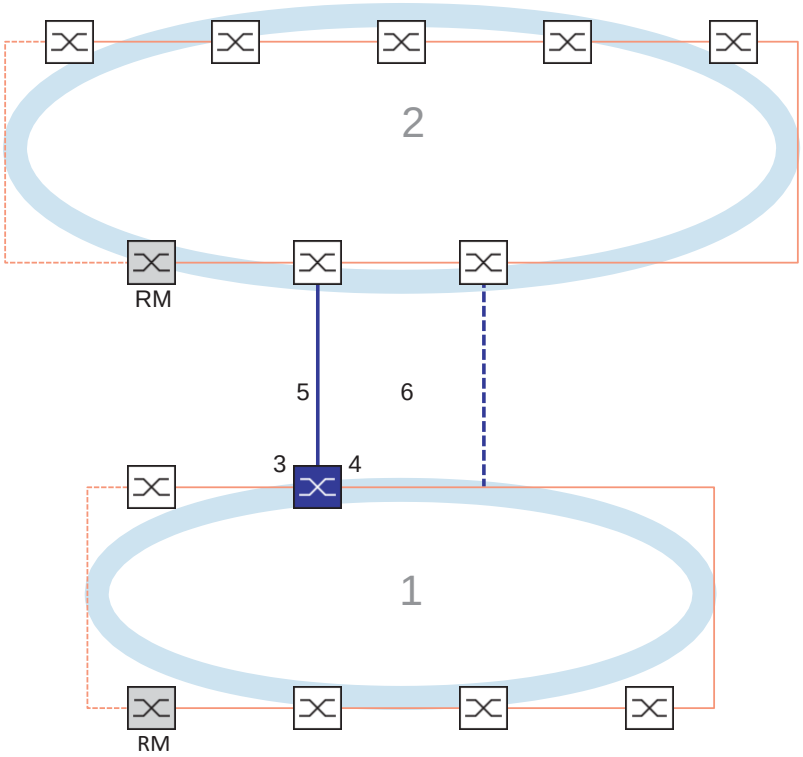


図56 One-Switch カプリング例
1:リング
2:基幹回線網
3:パートナーカプリングポート
4:カプリングポート
5:基幹ライン
6:冗長化ライン

パートナーカプリングポートに接続された青実線の基幹ラインは、通常のオペレーションでは、2つのネットワーク間のカプリングを行います。基幹ラインが作動不能の場合、カプリングポートに接続された青破線の冗長化ラインは、リング/ネットワークカプリングの役を引き継ぎます。スイッチ**1つ**がカプリングの切替えを行います。

以下は青で表示されたデバイスの設定です。

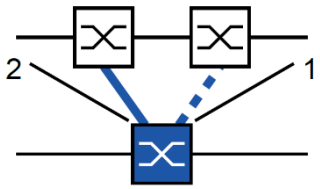


図57　One-switch カプリング
1: カプリングポート
2: パートナーカプリングポート

以下の手順を実行します。

- ☐ *Switching > L2-Redundancy > Ring/Network Coupling* ダイアログボックスを開きます。
- ☐ *Mode* フレームの *Type* オプションリストで、*one-switch coupling* のラジオボタンを選択します。

注記： *Partner coupling port* 及び別ポートのリングポートのコンフィグレーションを実行します。

- ☐ *Coupling port* フレームで、冗長化ラインに接続するポートを*Port* ドロップダウンリストから選択します。
- ☐ *Partner coupling port* フレームで、基幹ラインに接続するポートを*Port* ドロップダウンリストから選択します。
- ☐ 機能を有効化するには*Operation* フレームの*On* のラジオボタンを選択します。
- ☐ 変更を一時的に保存します。
- ☐ 冗長化ラインをパートナーカプリングポートに接続します。
  Partner coupling port フレームの*State* フィールドには、パートナーカプリングポートのステータスが表示されます。
- ☐ 基幹ラインをカプリングポートに接続します。
  Coupling port フレームの*State* フィールドには、カプリングポートのステータスが表示されます。

Information フレームの*Redundancy available* フィールドには、冗長化の可否が表示されます。*Configuration failure* フィールドには、設定が完全で正確になされたかが表示されます。

カプリングポートには、以下の手順を実行します。

注記： カプリングポートには、以下の設定が必須です。

- ☐ *Basic Settings > Port* ダイアログボックスの *Configuration* タブを開きます。
- ☐ カプリングポートとして選択したポートは、以下テーブルのパラメーターに従い設定します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

表40　リングポートのポート設定

ポート種別	ビットレート	ポートの状態	自動コンフィグレーション	手動コンフィグレーション
TX	100 Mbit/s	marked	unmarked	*100 Mbit/s FDX*
TX	1 Gbit/s	marked	marked	–
光	100 Mbit/s	marked	unmarked	*100 Mbit/s FDX*
光	1 Gbit/s	marked	marked	–
光	2.5 Gbit/s	marked	–	*2.5 Gbit/s FDX*

カプリングポートのVLANを構成したら、カプリングポート及びパートナーカプリングポートのVLAN設定を指定します。以下の手順を実行します。

- ☐ *Switching > VLAN > Port* ダイアログボックスを開きます。
- ☐ *Port-VLAN ID* 設定を、ポートに設定したVLAN IDに変更します。
- ☐ カプリングポート両方の*Ingress filtering* チェックボックスのチェックを外します。
- ☐ *Switching > VLAN > Configuration* ダイアログボックスを開きます。
- ☐ `VLAN 1` の冗長接続及びVLANメンバーシップにタグを付けるには、`VLAN 1`行の両カプリングポートに対応するセルに値`T`を入力します。
- ☐ ボタンをクリックし、変更を一時的に保存します。

カプリングをするデバイスは、`VLAN 1`に最優先の冗長パケットを送信します。

- ☐ *Configuration*フレームの*Redundancy mode* オプションリストで、冗長化の種別を選択します。
  - ➢ *redundant ring/network coupling* 設定では、基幹ライン又は冗長化ラインがアクティブです。この設定では、両ライン間での切替えをデバイスが行います。
  - ➢ *extended redundancy* 設定をアクティベートすると、基幹ライン及び冗長化ラインは同時にアクティブになります。この設定で、カプリングネットワークに冗長性を追加することができます。2つ目のネットワークのカプリングデバイス間接続に障害が起きても、カプリングデバイスはデータの送受信を継続します。

注記：コンフィグレーションの際に、パケットが複製される場合があります。このため、デバイスがパケットの複製を検知した場合、この設定を選択します。

Coupling mode は、リングネットワークを接続する基幹回線網の種別を示したものです（図56参照）。

- ☐ *Configuration*フレームの*Coupling mode* オプションリストで、2つ目のネットワークの種別を選択します。
  - ☐ リングネットワークに接続したら、*ring coupling* ラジオボタンを選択します。
  - ☐ バス又はメッシュ構造に接続したら、*network coupling* ラジオボタンを選択します。
- ☐ ボタンをクリックし、変更を一時的に保存します。

カプリングの設定をデフォルトに戻します。以下の手順を実行します。

- ☐ ボタンに続き、*Reset* の項目をクリックします。

Two-Switchカプリング

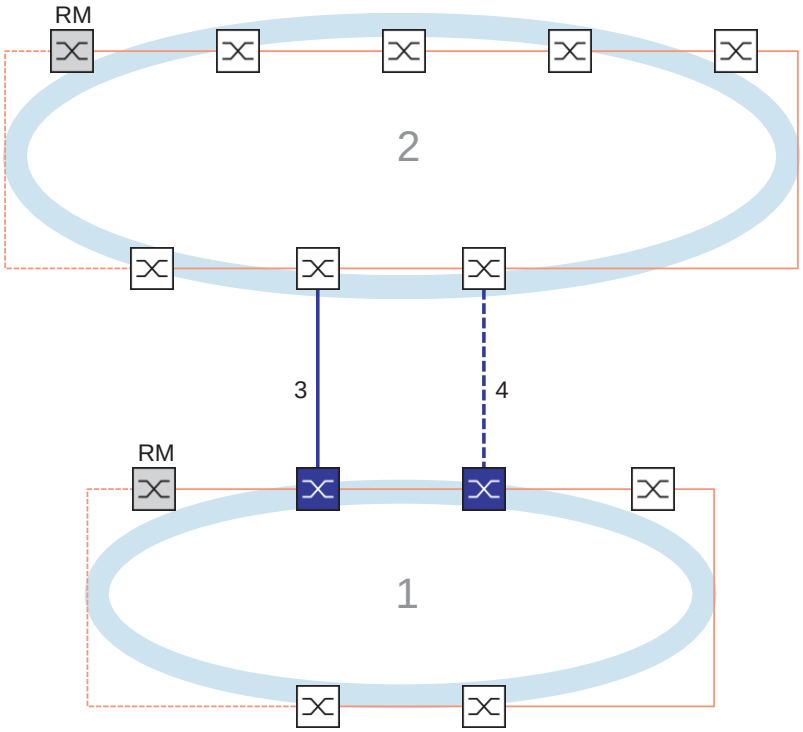


図58　Two-Switchカプリングの例
1:リング
2:基幹回線網
3:基幹ライン
4:冗長化ライン

2つのネットワークは、青実線で示した基幹ラインによりカプリングされています。基幹ライン又は隣接するデバイスのいずれかに障害が起きると、黒破線で示した冗長化ラインがネットワークカプリングの役割を引き継ぎます。カプリングはデバイス2つで実行します。

デバイスはイーサネットを通じて互いにコントロールパケットを送信します。

基幹ラインに接続された一次デバイス、並びに冗長化ラインに接続されたスタンバイデバイスは、カプリングする上でのパートナーです。
□ リングポートを使用してパートナー2つを接続します。

Two-Switchカプリング、一次デバイス

以下は青で表示されたデバイスの設定です。

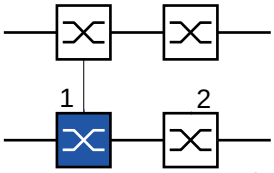


図59　Two-Switchカプリング、一次デバイス
1:カプリングポート
2:パートナーカプリングポート

以下の手順を実行します。

- ☐ *Switching > L2-Redundancy > Ring/Network Coupling* ダイアログボックスを開きます。
- ☐ *Mode* フレームの *Type* オプションリストで、*two-switch coupling, master* ラジオボタンを選択します。
- ☐ *Coupling port* フレームで、ネットワークセグメントに接続するポートを*Port* ドロップダウンリストから選択します。
  Coupling port 及び別ポートのリングポートのコンフィグレーションを実行します。
- ☐ 機能を有効化するには*Operation* フレームの*On* のラジオボタンを選択します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。
- ☐ 基幹ラインをカプリングポートに接続します。
  Coupling port フレームの*State* フィールドには、カプリングポートのステータスが表示されます。パートナーが既にネットワークでオペレーションをしている場合、*Partner coupling port* の*IP address* フィールドにはパートナーポートのIPアドレスが表示されます。

Information フレームの*Redundancy available* フィールドには、冗長化の可否が表示されます。*Configuration failure* フィールドには、設定が完全で正確になされたかが表示されます。

注記：同一デバイスで*Ring manager* 機能及びTwo-Switchカプリング機能を作動させると、ループができる可能性があります。

リングカプリングポートで接続が作動中に連続ループができるのを防ぐため、以下いずれかのアクションを実行します。デバイスはカプリングポートのポートステートをoffに設定します。

- オペレーションを無効化する
- コンフィグレーションを変更する

カプリングポートには、以下の手順を実行します。

- ☐ *Basic Settings > Port* ダイアログボックスの *Configuration* タブを開きます。
- ☐ カプリングポートとして選択したポートは、以下テーブルのパラメーターに従い設定します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

表41　リングポートのポート設定

ポート種別	ビットレート	ポートの状態	自動コンフィグレーション	手動コンフィグレーション
TX	100 Mbit/s	marked	unmarked	*100 Mbit/s FDX*
TX	1 Gbit/s	marked	marked	–
光	100 Mbit/s	marked	unmarked	*100 Mbit/s FDX*
光	1 Gbit/s	marked	marked	–
光	2.5 Gbit/s	marked	–	*2.5 Gbit/s FDX*

カプリングポートのVLANを構成したら、カプリングポート及びパートナーカプリングポートのVLAN設定を指定します。以下の手順を実行します。

- ☐ *Switching > VLAN > Port* ダイアログボックスを開きます。
- ☐ *Port-VLAN ID* 設定を、ポートに設定したVLAN IDに変更します。
- ☐ カプリングポート両方の*Ingress filtering* チェックボックスのチェックを外します。
- ☐ *Switching > VLAN > Configuration* ダイアログボックスを開きます。

- ☐ VLAN 1 の冗長接続及びVLANメンバーシップにタグを付けるには、`VLAN 1`行の両カプリングポートに対応するセルに値`T`を入力します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

カプリングをするデバイスは、`VLAN 1`に最優先の冗長パケットを送信します。

Two-Switchカプリング、スタンバイデバイス

以下は青で表示されたデバイスの設定です。

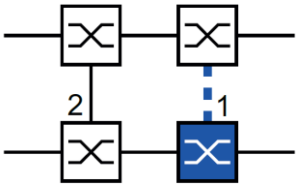


図60　Two-Switchカプリング、スタンバイデバイス
1:カプリングポート
2:パートナーカプリングポート

以下の手順を実行します。

- ☐ *Switching > L2-Redundancy > Ring/Network Coupling* ダイアログボックスを開きます。
- ☐ *Mode* フレームの *Type* オプションリストで、*`two-switch coupling, slave`* ラジオボタンを選択します。
- ☐ *Coupling port* フレームで、ネットワークセグメントに接続するポートを*Port* ドロップダウンリストから選択します。
  Coupling port 及び別ポートのリングポートのコンフィグレーションを実行します。
- ☐ 機能を有効化するには*Operation* フレームの*On* のラジオボタンを選択します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。
- ☐ 冗長化ラインを*Coupling port*に接続します。
  Coupling port フレームの*State* フィールドには、カプリングポートのステータスが表示されます。パートナーが既にネットワークでオペレーションをしている場合、*Partner coupling port* の*IP address* フィールドにはパートナーポートのIPアドレスが表示されます。

Information フレームの*Redundancy available* フィールドには、冗長化の可否が表示されます。*Configuration failure* フィールドには、設定が完全で正確になされたかが表示されます。

注記：同一デバイスで*Ring manager* 機能及びTwo-Switchカプリング機能を作動させると、ループができる可能性があります。

リングカプリングポートで接続が作動中に連続ループができるのを防ぐため、以下いずれかのアクションを実行します。デバイスはカプリングポートのポートステートをoffに設定します。

- オペレーションを無効化する
- コンフィグレーションを変更する

カプリングポートには、以下の手順を実行します。

- ☐ *Basic Settings > Port* ダイアログボックスの *Configuration* タブを開きます。
- ☐ カプリングポートとして選択したポートは、以下テーブルのパラメーターに従い設定します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

表42　リングポートのポート設定

ポート種別	ビットレート	ポートの状態	自動コンフィグレーション	手動コンフィグレーション
TX	100 Mbit/s	marked	unmarked	*100 Mbit/s FDX*
TX	1 Gbit/s	marked	marked	–
光	100 Mbit/s	marked	unmarked	*100 Mbit/s FDX*
光	1 Gbit/s	marked	marked	–
光	2.5 Gbit/s	marked	–	*2.5 Gbit/s FDX*

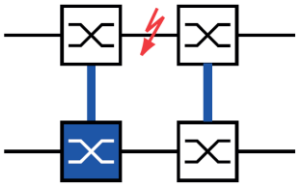
カプリングポートのVLANを構成したら、カプリングポート及びパートナーカプリングポートのVLAN設定を指定します。以下の手順を実行します。

- ☐ *Switching > VLAN > Port* ダイアログボックスを開きます。
- ☐ *Port-VLAN ID* 設定を、ポートに設定したVLAN IDに変更します。
- ☐ カプリングポート両方の*Ingress filtering* チェックボックスのチェックを外します。
- ☐ *Switching > VLAN > Configuration* ダイアログボックスを開きます。
- ☐ `VLAN 1` の冗長接続及びVLANメンバーシップにタグを付けるには、`VLAN 1`行の両カプリングポートに対応するセルに値`T`を入力します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

カプリングをするデバイスは、`VLAN 1`に最優先の冗長パケットを送信します。

Redundancy mode 及び*Coupling mode* を設定します。以下の手順を実行します。

- ☐ *Switching > L2-Redundancy > Ring/Network Coupling* ダイアログボックスを開きます。
- ☐ *Configuration*フレームの*Redundancy mode* オプションリストで、以下いずれかのラジオボタンを選択します。
  - ➢ *redundant ring/network coupling*
    この設定では、基幹ライン又は冗長化ラインがアクティブです。この設定では、両ライン間での切替えをデバイスが行います。
  - ➢ *extended redundancy*
    この設定では、基幹ライン及び冗長化ラインは同時にアクティブになります。この設定で、2つ目のネットワークに冗長性を追加することができます。2つ目のネットワークのカプリングデバイス間接続に障害が起きても、カプリングデバイスはデータの送受信を継続します。

    コンフィグレーションの際に、パケットが複製される場合があります。このため、デバイスがパケットの複製を検知した場合のみ、この設定を選択します。
- ☐ *Configuration*フレームの*Coupling mode* オプションリストで、以下いずれかのラジオボタンを選択します。
  - ☐ リングネットワークに接続したら、*ring coupling* ラジオボタンを選択します。
  - ☐ バス又はメッシュ構造に接続したら、*network coupling* ラジオボタンを選択します。

  Coupling mode は、リングネットワークを接続する基幹回線網の種別を示したものです（図58参照）。
- ☐ ボタンをクリックし、変更を一時的に保存します。

カプリングの設定をデフォルトに戻します。以下の手順を実行します。

- ☐ ボタンに続き、*Reset* の項目をクリックします。

Two-Switchカプリング、コントロールライン有り

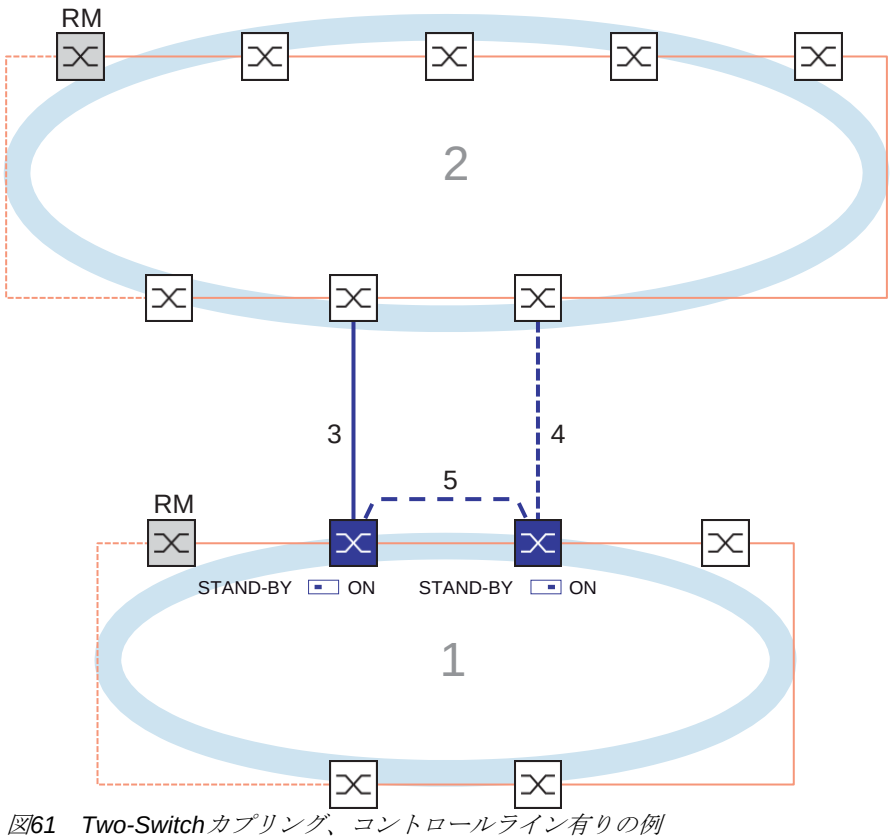


図61 Two-Switchカプリング、コントロールライン有りの例
1リング
2:基幹回線網
3:基幹ライン
4:冗長化ライン
5:コントロールライン

2つのネットワークは、青実線で示した基幹ラインによりカプリングされています。基幹ライン又は隣接するデバイスのいずれかに障害が起きると、青破線で示した冗長化ラインが2つのネットワークカプリングの役割を引き継ぎます。カプリングはデバイス2つで実行します。

デバイスは、下図（図62参照）に青点線で示されたコントロールライン上にコントロールパケットを送信します。

基幹ラインに接続された一次デバイス並びに冗長化ラインに接続されたスタンバイデバイスは、カプリングする上でのパートナーです。
☐ リングポートを使用してパートナー2つを接続します。

Two-Switchカプリング、コントロールライン有り、一次デバイス

以下は青で表示されたデバイスの設定です。

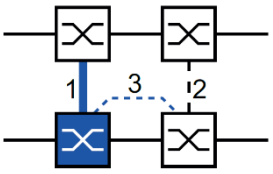


図62 Two-Switchカプリング、コントロールライン有り、一次デバイス
1:カプリングポート
2:パートナーカプリングポート
3コントロールライン

以下の手順を実行します。

☐ *Switching > L2-Redundancy > Ring/Network Coupling* ダイアログボックスを開きます。
☐ *Mode* フレームの *Type* オプションリストで、*two-switch coupling with control line, master* ラジオボタンを選択します。
☐ *Coupling port* フレームで、ネットワークセグメントに接続するポートを*Port* ドロップダウンリストから選択します。
Coupling port 及び別ポートのリングポートのコンフィグレーションを実行します。
☐ *Control port* フレームで、コントロールラインに接続するポートを*Port* ドロップダウンリストから選択します。
Coupling port 及び別ポートのリングポートのコンフィグレーションを実行します。
☐ 機能を有効化するには*Operation* フレームの*On* のラジオボタンを選択します。
☐ ☑ ボタンをクリックし、変更を一時的に保存します。
☐ 冗長化ラインをカプリングポートに接続します。
Coupling port フレームの*State* フィールドには、カプリングポートのステータスが表示されます。パートナーが既にネットワークでオペレーションをしている場合、*Partner coupling port* の*IP address* フィールドにはパートナーポートのIPアドレスが表示されます。
☐ コントロールラインをコントロールポートに接続します。
Control port フレームの*State* フィールドには、コントロールポートのステータスが表示されます。
パートナーが既にネットワークでオペレーションをしている場合、*Partner coupling port* の*IP address* フィールドにはパートナーポートのIPアドレスが表示されます。

Information フレームの*Redundancy available* フィールドには、冗長化の可否が表示されます。*Configuration failure* フィールドには、設定が完全で正確になされたかが表示されます。

注記：同一デバイスで*Ring manager* 機能及びTwo-Switchカプリング機能を作動させると、ループができる可能性があります。

リングカプリングポートで接続が作動中に連続ループができるのを防ぐため、以下いずれかのアクションを実行します。デバイスはカプリングポートのポートステートをoffに設定します。
- オペレーションを無効化する
- コンフィグレーションを変更する

カプリングポートには、以下の手順を実行します。

- ☐ *Basic Settings > Port* ダイアログボックスの *Configuration* タブを開きます。
- ☐ カプリングポートとして選択したポートは、以下テーブルのパラメーターに従い設定します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

表43　リングポートのポート設定

ポート種別	ビットレート	ポートの状態	自動コンフィグレーション	手動コンフィグレーション
TX	100 Mbit/s	marked	unmarked	*100 Mbit/s FDX*
TX	1 Gbit/s	marked	marked	–
光	100 Mbit/s	marked	unmarked	*100 Mbit/s FDX*
光	1 Gbit/s	marked	marked	–
光	2.5 Gbit/s	marked	–	*2.5 Gbit/s FDX*

カプリングポートのVLANを構成したら、カプリングポート及びパートナーカプリングポートのVLAN設定を指定します。以下の手順を実行します。

- ☐ *Switching > VLAN > Port* ダイアログボックスを開きます。
- ☐ *Port-VLAN ID* 設定を、ポートに設定したVLAN IDに変更します。
- ☐ カプリングポート両方の*Ingress filtering* チェックボックスのチェックを外します。
- ☐ *Switching > VLAN > Configuration* ダイアログボックスを開きます。
- ☐ `VLAN 1` の冗長接続及びVLANメンバーシップにタグを付けるには、`VLAN 1`行の両カプリングポートに対応するセルに値`T`を入力します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

カプリングをするデバイスは、`VLAN 1`に最優先の冗長パケットを送信します。

Two-Switchカプリング、コントロールライン有り、スタンバイデバイス

以下は青で表示されたデバイスの設定です。

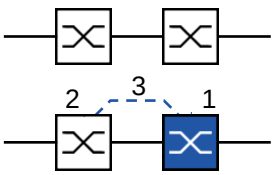


図63　Two-Switchカプリング、コントロールライン有り、スタンバイデバイス
1:カプリングポート
2:パートナーカプリングポート
3:コントロールライン

以下の手順を実行します。

- ☐ *Switching > L2-Redundancy > Ring/Network Coupling* ダイアログボックスを開きます。
- ☐ *Mode* フレームの *Type* オプションリストで、*two-switch coupling with control line, slave* ラジオボタンを選択します。
- ☐ *Coupling port* フレームで、ネットワークセグメントに接続するポートを*Port* ドロップダウンリストから選択します。
  Coupling port 及び別ポートのリングポートのコンフィグレーションを実行します。
- ☐ *Control port* フレームで、コントロールラインに接続するポートを*Port* ドロップダウンリストから選択します。
  Coupling port 及び別ポートのリングポートのコンフィグレーションを実行します。
- ☐ 機能を有効化するには*Operation* フレームの*On* のラジオボタンを選択します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。
- ☐ 冗長化ラインをカプリングポートに接続します。
  Coupling port フレームの*State* フィールドには、カプリングポートのステータスが表示されます。パートナーが既にネットワークでオペレーションをしている場合、*Partner coupling port* の*IP address* フィールドにはパートナーポートのIPアドレスが表示されます。
- ☐ コントロールラインをコントロールポートに接続します。
  Control port フレームの*State* フィールドには、コントロールポートのステータスが表示されます。
  パートナーが既にネットワークでオペレーションをしている場合、*Partner coupling port* の*IP address* フィールドにはパートナーポートのIPアドレスが表示されます。

Information フレームの*Redundancy available* フィールドには、冗長化の可否が表示されます。*Configuration failure* フィールドには、設定が完全で正確になされたかが表示されます。

注記：同一デバイスで*Ring manager* 機能及びTwo-Switchカプリング機能を作動させると、ループができる可能性があります。

リングカプリングポートで接続が作動中に連続ループができるのを防ぐため、以下いずれかのアクションを実行します。デバイスはカプリングポートのポートステートをoffに設定します。

- オペレーションを無効化する
- コンフィグレーションを変更する

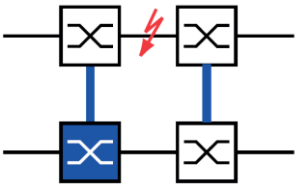
カプリングポートには、以下の手順を実行します。

- ☐ *Switching > VLAN > Port* ダイアログボックスを開きます。
- ☐ *Port-VLAN ID* 設定を、ポートに設定したVLAN IDに変更します。
- ☐ カプリングポート両方の*Ingress filtering* チェックボックスのチェックを外します。
- ☐ *Switching > VLAN > Configuration* ダイアログボックスを開きます。
- ☐ `VLAN 1` の冗長接続及びVLANメンバーシップにタグを付けるには、`VLAN 1`行の両カプリングポートに対応するセルに値`T`を入力します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

カプリングをするデバイスは、`VLAN 1`に最優先の冗長パケットを送信します。

Redundancy mode 及び*Coupling mode* を設定します。以下の手順を実行します。

- ☐ *Switching > L2-Redundancy > Ring/Network Coupling* ダイアログボックスを開きます。
- ☐ *Configuration*フレームの*Redundancy mode* オプションリストで、以下いずれかのラジオボタンを選択します。
  - ➢ *redundant ring/network coupling*
    この設定では、基幹ライン又は冗長化ラインがアクティブです。この設定では、両ライン間での切替えをデバイスが行います。
  - ➢ *extended redundancy*
    この設定では、基幹ライン及び冗長化ラインは同時にアクティブになります。この設定で、2つ目のネットワークに冗長性を追加することができます。2つ目のネットワークのカプリングデバイス間接続に障害が起きても、カプリングデバイスはデータの送受信を継続します。

    コンフィグレーションの際に、パケットが複製される場合があります。このため、デバイスがパケットの複製を検知した場合のみ、この設定を選択します。
- ☐ *Configuration*フレームの*Coupling mode* オプションリストで、以下いずれかのラジオボタンを選択します。
  - ☐ リングネットワークに接続したら、*ring coupling* ラジオボタンを選択します。
  - ☐ バス又はメッシュ構造に接続したら、*network coupling* ラジオボタンを選択します。

  Coupling mode は、リングネットワークを接続する基幹回線網の種別を示したものです（図61参照）。
- ☐ ボタンをクリックし、変更を一時的に保存します。

カプリングの設定をデフォルトに戻します。以下の手順を実行します。

- ☐ ボタンに続き、*Reset* の項目をクリックします。

14 オペレーション診断

当デバイスは、以下の診断ツールを提供します。
- SNMPトラップの送信
- デバイスのステータス監視
- 信号接点を使用したアウトオブバンド・シグナリング
- ポートステータス表示
- ポートレベルのイベントカウンター
- 不一致のDuplex Modeの検知
- 自動無効化
- SFPステータスの表示
- トポロジーディスカバリー
- 競合IPアドレスの検知
- ループ検知
- レイヤー2のネットワークループからの保護
- レポート
- ポートのデータトラフィック監視（ポートミラーリング）
- Syslog
- イベントログ
- セルフテスト中の原因及びアクション管理

14.1 SNMPトラップの送信

デバイスは通常オペレーション中に起こった異常イベントを、ネットワーク管理ステーションに即時にレポートします。これは、ポーリング（ポーリング：一定間隔でデータステーションにクエリーを送る）をバイパスするSNMPトラップと呼ばれるメッセージにより実行されます。SNMPトラップがあれば、ユーザーは異常イベントに対して素早く反応することができます。

これらイベントは以下の例の通りです。
- ハードウェアリセット
- コンフィグレーションの変更
- ポートのセグメンテーション

デバイスは様々なホストにSNMPトラップを送信してメッセージの伝送信頼性を向上させます。未認知のSNMPトラップメッセージは、異常イベント情報が含まれたパケットで構成されています。

デバイスはSNMPトラップをトラップ宛先テーブルに入力されているホストに送信します。トラップ宛先テーブルはSNMPを使用してネットワーク管理ステーションで設定することができます。

14.1.1 SNMPトラップリスト

以下の表にデバイスが送信する可能性のあるSNMPトラップを示します。

表44　可能性のあるSNMPトラップ

SNMPトラップ名	意味
authenticationFailure	ステーションが認証無しでエージェントにアクセスを試みると、このトラップが送信されます。
coldStart	再起動後に送信されます。
sa2DevMonSenseExtNvmRemoval	外部メモリが取り外されると、このトラップが送信されます。
linkDown	ポートへの接続が中断されると、このトラップが送信されます。
linkUp	ポート接続が確立されると、このトラップが送信されます。
sa2DevMonSensePSState	電源ユニットのステータスが変わると、このトラップが送信されます。
sa2SigConStateChange	オペレーション監視で信号接点のステータスが変わると、このトラップが送信されます。
newRoot	送信側エージェントがスパニングツリーの新規ルートになると、このトラップが送信されます。
topologyChange	ポートがblocking からforwarding へ、又はforwarding からblockingへと変わると、このトラップが送信されます。
alarmRisingThreshold	RMON入力がこの高位閾値を超過すると、このトラップが送信されます。
sa2AgentPortSecurityViolation	このポートで検知したMACアドレスがパラメーターsa2AgentPortSecurityEntryの現在設定と不一致だと、このトラップが送信されます。
sa2DiagSelftestActionTrap	セルフテストの4つのカテゴリー「task」「resource」「software」「hardware」が設定通りに実行されると、このトラップが送信されます。
sa2MrpReconfig	MRPリングのコンフィグレーションが変わると、このトラップが送信されます。
sa2DiagIfaceUtilizationTrap	インターフェースの閾値が指定された上限を上回る又は下限閾値を下回ると、このトラップが送信されます。
sa2LogAuditStartNextSector	1つの区画完了後に新しい監査証跡を開始すると、このトラップが送信されます。
sa2PtpSynchronizationChance	PTP同期のステータスが変わると、このトラップが送信されます。
sa2ConfigurationSavedTrap	デバイスがコンフィグレーションのローカル保存に成功すると、このトラップが送信されます。
sa2ConfigurationChangedTrap	デバイスのコンフィグレーションが初めてローカル保存された後に変更を施すと、このトラップが送信されます。
sa2PlatformStpInstanceLoopInconsistentStartTrap	STPインスタンスにあるポートのステータスが loop inconsistent に変わると、このトラップが送信されます。
sa2PlatformStpInstanceLoopInconsistentEndTrap	STPインスタンスにあるポートがステータス loop inconsistent のままBPDUパケットを受信すると、このトラップが送信されます。

14.1.2 コンフィグレーションに関わるアクティビティのSNMPトラップ

コンフィグレーションを保存した後、デバイスはsa2ConfigurationSavedTrapを送信します。SNMPトラップには、不揮発性メモリ（*NVM*）及び外部メモリ（*ENVM*）のいずれもの状態変数を含み、作動中のコンフィグレーションが不揮発性メモリ及び外部メモリと同期しているか否かを示します。また、コンフィグレーションファイルをデバイスにコピーし、既存のアクティブな保存済みコンフィグレーションと置換えることでSNMPトラップをトリガーすることもできます。

更に、ローカルコンフィグレーションを変更すると、デバイスは
sa2ConfigurationChangedTrapを送信し、稼働中コンフィグレーションと保存済みコンフィグレーションとの不一致を示します。

14.1.3 SNMPトラップの設定

ユーザーは特定イベントに対する対応としてSNMPトラップを送信することができます。少なくとも1つの、SNMPトラップを受信する宛先を作成します。

以下の手順を実行します。

- ☐ *Diagnostics > Status Configuration > Alarms (Traps)* ダイアログボックスを開きます。
- ☐  ボタンをクリックします。

  ダイアログが*Create* ウィンドウを表示します。
- ☐ *Name* フレームに、デバイスが自身をSNMPトラップのソースだと識別するための名前を指定します。
- ☐ *Address* に、デバイスがSNMPトラップを送信するトラップの宛先IPアドレスを指定します。
- ☐ *Active* カラムに、デバイスがSNMPトラップを送信する際に考慮すべきエントリーを選択します。
- ☐  ボタンをクリックし、変更を一時的に保存します。

参考例として、デバイスがSNMPトラップをトリガーした際に、ユーザーが指定するダイアログボックスを以下に示します。

- *Basic Settings > Port* ダイアログボックス
- *Basic Settings > Power over Ethernet > Global* ダイアログボックス
- *Network Security > Port Security* ダイアログボックス
- *Switching > L2-Redundancy > Link Aggregation* ダイアログボックス
- *Diagnostics > Status Configuration > Device Status* ダイアログボックス
- *Diagnostics > Status Configuration > Security Status* ダイアログボックス
- *Diagnostics > Status Configuration > Signal Contact* ダイアログボックス
- *Diagnostics > Status Configuration > MAC Notification* ダイアログボックス
- *Diagnostics > System > IP Address Conflict Detection* ダイアログボックス
- *Diagnostics > System > Selftest* ダイアログボックス
- *Diagnostics > Ports > Port Monitor* ダイアログボックス
- *Advanced > Digital IO Module* ダイアログボックス

14.1.4 ICMPメッセージング

ユーザーは、pingやトレースルート等のICMP（Internet Control Message Protocol）を診断に使用することができます。また、デバイスがパケットをソースのデバイスにICMPメッセージを返送するTTL（Time To Live）や、メッセージの破棄にもICMPを使用します。

IPネットワークの特定ホストへのパスをテストするためにpingネットワークツールを使用します。トレースルート診断ツールは、ネットワーク上のパス及びパケットのトランジット遅延を表示します。

14.2 デバイスのステータス監視

デバイスステータスは、デバイスの状態の概要を示します。多くのプロセス可視化システムは、デバイスのステータスを記録することでグラフィックスにその状況を反映します。

デバイスは現在のステータスを*Device status* フレーム内に*error* 又は*ok* と表示します。デバイスは個別の監視結果を基にこのステータスを判断します。

ユーザーは以下を実行することができます。
- 信号接点を使用したアウトオブバンド・シグナリング
- SNMPトラップを送信してデバイスステータス変更のシグナリング
- グラフィカルユーザーインターフェースの*Basic Settings > System* ダイアログボックスでデバイスステータスを検知
- コマンドラインインターフェース内でデバイスステータスをクエリー

Diagnostics > Status Configuration > Device Status ダイアログボックスの*Global* タブで、管理ステーションに以下のイベントに対するトラップをデバイスから送ることができます。
- 電圧供給の誤り
  - 2つのうち少なくとも1つの供給電圧が稼働していない
  - 内部供給電圧が稼働していない
- デバイスがユーザー定義された温度閾値を外れて稼働している時
- 冗長性の喪失（Ring Manager mode内）
- リンク接続の中断
  少なくともポート1つをこの機能のために構成します。リンクを失ったら、デバイスがどのポートにシングナリングをするのかを、*Diagnostics > Status Configuration > Device Status* ダイアログボックスの*Port* タブ内にある*Propagate connection error* 行で指定します。
- 外部メモリの取外し
  外部メモリ内のコンフィグレーションが、デバイスのコンフィグレーションと同期していません。

デバイスステータスに含めるイベントを決定するために、適切なエントリーを選択します。

注記：非冗長性の電圧供給の場合、デバイスは供給電圧が無いことをレポートします。このメッセージを無効にするには、両方のインプットから電圧を供給するか、モニタリングを無視します。

14.2.1 監視可能なイベント

表45 Device Status イベント

名称	意味
Temperature	温度が指定値を上回る（下回る）かを監視します。
Ring redundancy	リングが冗長化されている場合、この機能を有効化します。
Connection errors	*Propagate connection error* チェックボックスがアクティブになっているポート全てを監視するには、この機能を有効化します。
External memory removal	外部メモリデバイスの有無を監視するには、この機能を有効化します。
External memory not in sync	デバイスコンフィグレーションと、外部メモリ（*ENVM*）に保存されたコンフィグレーションとの同期を、デバイスが監視します。
Power supply	電源を監視するには、この機能を有効化します。

14.2.2 デバイスのステータス監視

以下の手順を実行します。

- ☐ *Diagnostics > Status Configuration > Device Status* ダイアログボックスを開きます。
- ☐ 監視するパラメーターについて、*Monitor* カラムのチェックボックスにチェックを入れます。
- ☐ 管理ステーションにSNMPトラップを送信するには、*Traps* フレーム内の*Send trap* 機能をアクティベートします。
- ☐ *Diagnostics > Status Configuration > Alarms (Traps)* ダイアログボックスで、少なくとも1つのSNMPトラップを受信する宛先を作成します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。
- ☐ *Basic Settings > System* ダイアログボックスを開きます。
- ☐ 温度を監視するには、*System data* フレームの最下段に温度閾値を指定します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`device-status trap`	デバイスのステータスが変わると、SNMPトラップを送信します。
`device-status monitor envm-not-in-sync`	デバイス内及び外部メモリ内のコンフィグレーションプロファイルを監視します。 以下の状況では、*Device status* が`error` に変わります。 • コンフィグレーションプロファイルがデバイス内のみに存在する。 • デバイス内のコンフィグレーションプロファイルと外部メモリ内のコンフィグレーションプロファイルが異なる。
`device-status monitor envm-removal`	アクティブな外部メモリを監視します。デバイスからアクティブな外部メモリを取り外すと、*Device status* フレーム内の値が`error`に変わります。
`device-status monitor power-supply 1`	電源ユニット`1`を監視します。デバイスが電源のフォルトを検知すると、*Device status* フレーム内の値が`error`に変わります。
`device-status monitor ring-redundancy`	リングの冗長性を監視します。 以下の状況では、*Device status* が`error` に変わります。 • 冗長化機能がアクティブになる（待機冗長の喪失） • デバイスはリングの一般参加者で、設定のエラーを検知した
`device-status monitor temperature`	デバイス内の温度を監視します。温度が指定したリミット値を上回る（下回る）と、*Device status* フレーム内の値が`error`に変わります。

デバイスが未接続のアクティブリンクを監視できるよう、最初にグローバル機能を有効化し、次に個別のポートを有効化します。

以下の手順を実行します。

- ☐ *Diagnostics > Status Configuration > Device Status* ダイアログボックスの*Global* タブを開きます。
- ☐ *Connection errors* パラメーターについて、*Monitor* カラムのチェックボックスにチェックを入れます。
- ☐ *Diagnostics > Status Configuration > Device Status* ダイアログボックスの*Port* タブを開きます。
- ☐ *Propagate connection error* パラメーターについて、監視するポートのカラムのチェックボックスにチェックを入れます。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`device-status monitor link-failure`	ポート/インターフェースリンクを監視します。リンクが監視されたポート/インターフェースを妨害すると、*Device status* フレームの値が*`error`*に変わります。
`interface 1/1`	インターフェース`1/1`のInterface Configuration mode に変更します。
`device-status link-alarm`	ポート/インターフェースリンクを監視します。リンクがポート/インターフェースを妨害すると、*Device status* フレームの値が*`error`*に変わります。

注記：サポートされるコンポーネントの監視及びトラップ送信は上記コマンドでアクティベートしされます。個別コンポーネントの監視をアクティベート・ディアクティベートしたい場合、これらに対応すシンタックスはコマンドラインインターフェースのマニュアル又はコマンドラインインターフェースコンソールのヘルプで検索することができます。コマンドラインインターフェースのヘルプを表示するには、クエスチョンマーク`?`を挿入し、＜Enter＞キーを押します。

14.2.3 デバイスステータスの表示

以下の手順を実行します。

- ☐ *Basic Settings > System* ダイアログボックスを開きます。

`show device-status all`	EXEC Privilege modeに、デバイスステータス及びデバイスステータス決定のための設定が表示されます。

14.3 セキュリティステータス

セキュリティステータスは、デバイス全体のセキュリティの概要を示します。記録したデバイスのセキュリティステータスをグラフィックスでその状態を示すため、多くのプロセスはシステムを可視化する手助けをするものです。デバイスは全体のセキュリティステータスを*Basic Settings* > System ダイアログボックスの *Security status* フレームに表示します。

Diagnostics > Status Configuration > Security Status ダイアログボックスの*Global* タブに、デバイスは現在のステータスを*Device status* フレーム内に`error` 又は`ok` と表示します。デバイスは個別の監視結果を基にこのステータスを判断します。

ユーザーは以下を実行することができます。
- 信号接点を使用したアウトオブバンド・シグナリング
- SNMPトラップを送信してセキュリティステータス変更のシグナリング
- グラフィカルユーザーインターフェースの*Basic Settings > System* ダイアログボックスでセキュリティステータスを検知
- コマンドラインインターフェース内でセキュリティステータスをクエリー

14.3.1 監視可能なイベント

以下の手順を実行します。
- ☐ デバイスに監視させるイベントを指定します。
- ☐ 該当するパラメーターについて、*Monitor* カラムのチェックボックスにチェックを入れます。

表46　セキュリティステータスイベント

名称	意味
Password default settings unchanged	インストール後はセキュリティ強化のためパスワードを変更してください。これがアクティブの時にパスワードがデフォルトのままだと、デバイスがアラームを表示します。
Min. password length < 8	高いセキュリティ意識のためにも8文字以上のパスワードを作成します。アクティブの時、デバイスは*Min. password length* 設定を監視します。
Password policy settings deactivated	デバイスは、*Device Security* > User Management ダイアログボックスにある設定のパスワード方針要件を監視します。
User account password policy check deactivated	デバイスは*Policy check* チェックボックスの設定を監視します。*Policy check* が非アクティブの時、デバイスはSNMPトラップを送信します。
Telnet server active	*Telnet* 機能が有効の時、デバイスが監視します。
HTTP server active	*HTTP* 機能が有効の時、デバイスが監視します。
SNMP unencrypted	*SNMPv1* 又は*SNMPv2*機能が有効の時、デバイスが監視します。
Access to system monitor with serial interface possible	デバイスはシステムモニターのステータスを監視します。
Saving the configuration profile on the external memory possible	デバイスは外部不揮発性メモリにコンフィグレーションを保存できる可能性を監視します。
Link interrupted on enabled device ports	デバイスはアクティブなポートのリンクステータスを監視します。
Access with Ethernet Switch Configurator possible	デバイスはEthernet Switch Configuratorの読出し・書込みアクセス機能を有効にすると監視します。
Load unencrypted config from external memory	デバイスは外部不揮発性メモリからコンフィグレーションを読み込むためのセキュリティ設定を監視します。

表46　セキュリティステータスイベント（続き）

名称	意味
IEC61850-MMS active	デバイスは IEC 61850-MMS プロトコルのアクティベーション設定を監視します。
Modbus TCP active	デバイスは Modbus TCP/IP プロトコルのアクティベーション設定を監視します。
Self-signed HTTPS certificate present	デバイスはHTTPSサーバーが自身で作成したデジタル証明書を監視します。

14.3.2 セキュリティステータスのコンフィグレーション

以下の手順を実行します。

- ☐ *Diagnostics* > *Status Configuration* > *Security Status* ダイアログボックスの*Global* タブを開きます。
- ☐ 監視するパラメーターについて、*Monitor* カラムのチェックボックスにチェックを入れます。
- ☐ 管理ステーションにSNMPトラップを送信するには、*Traps* フレーム内の*Send trap* 機能をアクティベートします。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。
- ☐ *Diagnostics > Status Configuration > Alarms (Traps)* ダイアログボックスで、少なくとも1つのSNMPトラップを受信する宛先を作成します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`security-status monitor pwd-change`	ローカルにセットアップしたユーザーアカウント `user` 及び `admin`のパスワードを監視します。`user` 又は`admin` のユーザーアカウントがデフォルト設定の場合、*Security status* フレームの値が *`error`*に変わります。
`security-status monitor pwd-min-length`	*Min. password length* 方針に指定した値を監視します。*Min. password length* 方針が `8`未満の場合、*Security status* フレームの値が *`error`*に変わります。
`security-status monitor pwd-policy- config`	パスワード方針の設定を監視します。以下方針のうち少なくとも1つが`0`と指定されている場合、*Security status* フレームの値が *`error`*に変わります。 • *Upper-case characters (min.)* • *Lower-case characters (min.)* • *Digits (min.)* • *Special characters (min.)*
`security-status monitor pwd-policy- inactive`	パスワード方針の設定を監視します。以下方針のうち少なくとも1つが`0`と指定されている場合、*Security status* フレームの値が *`error`*に変わります。
`security-status monitor telnet-enabled`	Telnetサーバーを監視します。Telnetサーバーを有効化すると、*Security status* フレームの値が *`error`*に変わります。

`security-status monitor http-enabled`	HTTPサーバーを監視します。HTTPサーバーを有効化すると、*Security status* フレームの値が `error`に変わります。
`security-status monitor snmp-unsecure`	SNMPサーバーを監視します。 以下方針のうち少なくとも1つの条件を満たした場合、*Security status* フレームの値が `error`に変わります。 • *SNMPv1* 機能が有効 • *SNMPv2* 機能が有効 • SNMPv3 の暗号化が無効 *Device Security > User Management* ダイアログボックスの*SNMP encryption type* フィールドで、暗号化を有効にします。
`security-status monitor sysmon-enabled`	デバイスのシステムモニター機能のアクティベーションを監視します。
`security-status monitor extnvm-upd- enabled`	外部不揮発性メモリのアップデートのアクティベーションを監視します。
`security-status monitor iec61850-mms- enabled`	*IEC61850-MMS* 機能を監視します。*IEC61850-MMS* 機能を有効化すると、*Security status* フレームの値が`error`に変わります。
`security-status trap`	デバイスのステータスが変わると、SNMPトラップを送信します。

デバイスが未接続のアクティブリンクを監視できるよう、最初にグローバル機能を有効化し、次に個別のポートを有効化します。

以下の手順を実行します。

- ☐ *Diagnostics > Status Configuration > Security Status* ダイアログボックスの*Global* タブを開きます。
- ☐ *Link interrupted on enabled device ports* パラメーターについて、*Monitor* カラムのチェックボックスにチェックを入れます。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。
- ☐ *Diagnostics > Status Configuration > Device Status* ダイアログボックスの*Port* タブを開きます。
- ☐ *Link interrupted on enabled device ports* パラメーターについて、監視するポートのカラムのチェックボックスにチェックを入れます。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`security-status monitor no-link-enabled`	アクティブポートのリンクを監視します。リンクがアクティブポートを妨害すると、*Security status* フレームの値が`error`に変わります。
`interface 1/1`	インターフェース`1/1`のInterface Configuration mode に変更します。
`security-status monitor no-link`	インターフェース/ポート`1`のリンクを監視します。

14.3.3 セキュリティステータスを表示する

以下の手順を実行します。

☐ *Basic Settings > System* ダイアログボックスを開きます。

```
show security-status all
```

EXEC Privilege modeに、セキュリティステータス及びセキュリティステータス決定のための設定が表示されます。

14.4 アウトオブバンド・シグナリング

当デバイスは、外部デバイスの制御及びデバイス機能の監視に信号接点を使用します。機能監視により、遠隔で診断を実行することができます。

デバイスは、選択したモードのポテンシャルフリー信号接点（リレー接点、閉回路）を中断することでオペレーションステータスをレポートします。デバイスは以下の機能を監視します。

- 電圧供給の誤り
  - 2つのうち少なくとも1つの供給電圧が稼働していない
  - 内部供給電圧が稼働していない
- デバイスがユーザー定義された温度閾値を外れて稼働している時
- リングの冗長イベント
  冗長性の喪失（Ring Manager mode内）
  デフォルトでは、リング冗長性の監視は非アクティブです。デバイスはリングの一般参加者で、ローカルコンフィグレーションのエラーを検知します。
- リンク接続の中断
  少なくともポート1つをこの機能のために構成します。*Propagate connection error* フレームで、デバイスがリンクを中断させる信号をどのポートに送るかを指定します。デフォルトでは、リンク監視は非アクティブです。
- 外部メモリの取外し
  外部メモリ内のコンフィグレーションが、デバイスのコンフィグレーションと一致しません。

デバイスステータスに含めるイベントを決定するために、適切なエントリーを選択します。

注記：非冗長性の電圧供給の場合、デバイスは供給電圧が無いことをレポートします。このメッセージを無効にするには、両方のインプットから電圧を供給するか、モニタリングを無視します。

14.4.1 信号接点の制御

Manual setting modeで、遠隔で信号接点を制御します。用途のオプション

- SPSエラー監視中に検知したエラーのシミュレーション
- SNMPを使用したデバイスの遠隔制御、例えばカメラのスイッチをオンにする等。

以下の手順を実行します。

- ☐ *Diagnostics > Status Configuration > Signal Contact* ダイアログボックスの*Global* タブを開きます。
- ☐ 信号接点をマニュアルで制御するには、*Configuration* フレームの*Mode* ドロップダウンリストから*Manual setting* を選択します。
- ☐ 信号接点を開くには、*Configuration* フレームの*open* ラジオボタンを選択します。
- ☐ 信号接点を閉じるには、*Configuration* フレームの*close* ラジオボタンを選択します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。

`signal-contact 1 mode manual`	信号接点1のマニュアル設定モードを選択します。
`signal-contact 1 state open`	信号接点1が開きます。
`signal-contact 1 state closed`	信号接点1が閉じます。

14.4.2 デバイス及びセキュリティステータスの監視

Configuration フィールドで、信号接点が示すイベントを指定します。

- *`Device status`*
  この設定を使用すると、信号接点は*Diagnostics > Status Configuration > Device Status* ダイアログボックスで監視するパラメーターのステータスを示します。
- *`Security status`*
  この設定を使用すると、信号接点は*Diagnostics > Status Configuration > Security Status* ダイアログボックスで監視するパラメーターのステータスを示します。
- *`Device/Security status`*
  この設定を使用すると、信号接点は*Diagnostics > Status Configuration > Device Status* 及び *Diagnostics > Status Configuration >* Security Status ダイアログボックスで監視するパラメーターのステータスを示します。

オペレーション監視のコンフィグレーション

以下の手順を実行します。

- ☐ *Diagnostics > Status Configuration > Signal Contact* ダイアログボックスの*Global* タブを開きます。
- ☐ 信号接点を使用してデバイス機能を監視するには、*Configuration* フレームの*Mode* フィールドに、値*`Monitoring correct operation`* を指定します。
- ☐ 監視するパラメーターについて、*Monitor* カラムのチェックボックスにチェックを入れます。
- ☐ 管理ステーションにSNMPトラップを送信するには、*Traps* フレーム内の*Send trap* 機能をアクティベートします。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。
- ☐ *Diagnostics > Status Configuration > Alarms (Traps)* ダイアログボックスで、少なくとも1つのSNMPトラップを受信する宛先を作成します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。
- ☐ *Basic Settings > System* ダイアログボックスで、温度監視用の温度閾値を指定します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`signal-contact 1 monitor temperature`	デバイス内の温度を監視します。温度が閾値を上回る（下回る）と、信号接点が開きます。

`signal-contact 1 monitor ring-redundancy`	リングの冗長性を監視します。 信号接点は以下の状況で開きます。 • 冗長化機能がアクティブになる（待機冗長の喪失）。 • デバイスはリングの一般参加者で、設定のエラーを検知した。
`signal-contact 1 monitor link-failure`	ポート/インターフェースリンクを監視します。リンクが監視されたポート/インターフェースを妨害すると、信号接点が開きます。
`signal-contact 1 monitor envm-removal`	アクティブな外部メモリを監視します。デバイスからアクティブな外部メモリを取り外すと、信号接点が開きます。
`signal-contact 1 monitor envm-not-in- sync`	デバイス内及び外部メモリ内のコンフィグレーションプロファイルを監視します。 信号接点は以下の状況で開きます。 • コンフィグレーションプロファイルがデバイス内のみに存在する。 • デバイス内のコンフィグレーションプロファイルと外部メモリ内のコンフィグレーションプロファイルが異なる。
`signal-contact 1 monitor power-supply 1`	電源ユニット1を監視します。デバイスが電源のフォルトを検知すると、信号接点が開きます。
`signal-contact 1 monitor module-removal 1`	モジュール1を監視します。デバイスからモジュール1を取り外すと、信号接点が開きます。
`signal-contact 1 trap`	オペレーション監視のステータスが変わると、デバイスがSNMPトラップを送信できるようになります。
`no signal-contact 1 trap`	SNMPトラップを無効化します。

デバイスが未接続のアクティブリンクを監視できるよう、最初にグローバル機能を有効化し、次に個別のポートを有効化します。

以下の手順を実行します。

- ☐ *Monitor* カラムで、*Link interrupted on enabled device ports* 機能をアクティベートします。
- ☐ *Diagnostics > Status Configuration > Device Status* ダイアログボックスの*Port* タブを開きます。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`signal-contact 1 monitor link-failure`	ポート/インターフェースリンクを監視します。リンクが監視されたポート/インターフェースを妨害すると、信号接点が開きます。
`interface 1/1`	インターフェース1/1のInterface Configuration mode に変更します。
`signal-contact 1 link-alarm`	ポート/インターフェースリンクを監視します。リンクがポート/インターフェースを妨害すると、信号接点が開きます。

監視可能なイベント

表47　Device Status イベント

名称	意味
Temperature	温度が指定値を上回った（下回った）時。
Ring redundancy	リングが冗長化されている場合、この機能の監視を有効化します。
Connection errors	*Propagate connection error* チェックボックスがアクティブになっているポート全てを監視するには、この機能を有効化します。
External memory not in sync with NVM	デバイスコンフィグレーションと、外部メモリ（*ENVM*）に保存されたコンフィグレーションとの同期を、デバイスが監視します。
External memory removed	外部メモリデバイスの有無を監視するには、この機能を有効化します。
Power supply	電源を監視するには、この機能を有効化します。

信号接点のステータスを表示する

追加オプションとして、信号接点のステータスを表示することができます。
- グラフィカルユーザーインターフェース内で表示します。
- コマンドラインインターフェース内でクエリーを実行します。

以下の手順を実行します。

☐ *Basic Settings > System* ダイアログボックスを開きます。
Signal contact status フレームは、信号接点のステータスを表示し、発生したアラームについて通知します。アラームが現在ある場合、フレームがハイライトされます。

```
show signal-contact 1 all
```
指定した信号接点の設定を表示します。

14.5 ポートステータス表示

ポートのステータスを視認するには、以下の手順を実行します。

- *Basic Settings > System* ダイアログボックスを開きます。

ダイアログボックスにデバイスの現在のコンフィグレーションが表示されます。また、ダイアログボックスには記号付きで個別ポートのステータスが表示されます。

以下の記号は個別ポートのステータスを示します。状況によっては、これら記号は互いに干渉し合うことがあります。ポートアイコンにマウスオーバーすると、吹き出しヘルプにポートステータスの詳細が表示されます。

表48　ポートのステータスを示す記号

基準	記号
ポートの帯域幅	10 Mbit/s ポートアクティブ状態、接続OK、全二重モード 100 Mbit/s ポートアクティブ状態、接続OK、全二重モード 1000 Mbit/s ポートアクティブ状態、接続OK、全二重モード
オペレーションステータス	半二重モード有効 *Basic Settings > Port* ダイアログボックスの *Configuration* タブの、*Automatic configuration* チェックボックス、*Manual configuration* フィールド、*Manual cable crossing (Auto. conf. off)* フィールドを確認してください。 オートネゴシエーション有効 *Basic Settings > Port* ダイアログボックスの *Configuration* タブの *Automatic configuration*チェックボックスを確認してください。 冗長機能がこのポートをブロックしています。
AdminLink	このポートはディアクティベートされています。接続OK。 このポートはディアクティベートされています。接続は確立されていません。 *Basic Settings > Port* ダイアログボックスの *Configuration* タブの*Port on* チェックボックス、*Link/Current settings* フィールドを確認してください。

14.6 ポートイベントカウンター

経験豊かなネットワークアドミニストレーターであれば、ポート統計情報テーブルを使用してネットワーク内で検知した問題を識別することができます。

このテーブルには、各種イベントカウンターがコンテンツとして表示されます。パケットカウンターは送信されたイベント及び受信したイベントを積算します。このイベントカウンターは、*Basic Settings > Restart* ダイアログボックスでリセットすることができます。

表49　既知の脆弱性の参考例

カウンター	発生可能性のある既知の脆弱性
受信フラグメント	• 接続デバイスの機能していないコントローラー • 伝送媒体内の電磁妨害
CRCエラー	• 接続デバイスの機能していないコントローラー • 伝送媒体内の電磁妨害 • ネットワーク内に作動不能のコンポーネント
コリジョン	• 接続デバイスの機能していないコントローラー • ネットワークの拡張過多、またはラインが長すぎる • コリジョン又はデータパケットと一緒にフォルトを検知

以下の手順を実行します。

- ☐ イベントカウンターを表示するには、*Basic Settings > Port* ダイアログボックスの *Statistics* タブを開きます。
- ☐ カウンターをリセットするには、*Basic Settings > Restart* ダイアログボックスの*Clear port statistics*ボタンをクリックします。

14.6.1 不一致のDuplex Modeの検知

相互に接続されたポート2つが不一致のDuplex Modeの場合、問題が発生します。これら問題の原因を追うことは容易ではありません。このような状況の自動検知及びレポートは、問題が発生する前に不一致のDuplex Modeを認知する上で役立ちます。

問題の原因は不正確なコンフィグレーション、例えばリモートポートの自動コンフィグレーションをディアクティベートした場合などがあります。

この不一致による典型的な影響としては、データ伝送レートが低い時は接続が機能しているように見えますが、双方向の高トラフィックではローカルデバイスが多くのCRCエラーを記録し、通信も通常のキャパシティより大きく落ちることになります。

デバイスはこの状況をユーザーに検知させ、ネットワーク管理ステーションにレポートします。この処理において、デバイスはポート設定という視点から、ポートのエラーカウンターを評価します。

ポートのエラーイベントの原因となり得るもの

以下の表に、TXポートのDuplexオペレーションモードのリストと、フォルトの原因となり得るものを示します。表で使用する用語の意味は以下の通りです。

- ➢ Collisions
  Half-duplexモードでは、Collisionsは通常オペレーションを意味します。
- ➢ Duplex problem
  Duplexモードの不一致

- EMI
  電磁妨害。
- Network extension
  ネットワークの拡張が過大、もしくはハブのカスケード接続が多すぎます。
- Collisions, Late Collisions
  Full-duplex modeでは、Collisions又はLate Collisionsのポートカウンターは増加しません。
- CRC Error
  マニュアルFull-duplex mode内では、デバイスはこれらエラーを不一致Duplex modeとして評価します。

表50　Duplex modeの不一致の評価

No.	自動コンフィグレーション	現在のDuplex Mode	検知したエラーイベント（リンクアップ後≧10）	Duplex Mode	原因可能性
1	marked	Half duplex	None	OK	
2	marked	Half duplex	Collisions	OK	
3	marked	Half duplex	Late Collisions	Duplex問題を検知	Duplex問題、EMI、ネットワーク拡張
4	marked	Half duplex	CRC Error	OK	EMI
5	marked	Full duplex	None	OK	
6	marked	Full duplex	Collisions	OK	EMI
7	marked	Full duplex	Late Collisions	OK	EMI
8	marked	Full duplex	CRC Error	OK	EMI
9	unmarked	Half duplex	None	OK	
10	unmarked	Half duplex	Collisions	OK	
11	unmarked	Half duplex	Late Collisions	Duplex問題を検知	Duplex問題、EMI、ネットワーク拡張
12	unmarked	Half duplex	CRC Error	OK	EMI
13	unmarked	Full duplex	None	OK	
14	unmarked	Full duplex	Collisions	OK	EMI
15	unmarked	Full duplex	Late Collisions	OK	EMI
16	unmarked	Full duplex	CRC Error	Duplex問題を検知	Duplex問題、EMI

14.7 自動ディスエーブル

当デバイスは、設定可能な複数の理由により、ポートを無効化（ディスエーブル）することができます。これら理由はどれもポートのシャットダウンの原因となります。ポートをシャットダウン状態から復旧させるには、ポートのシャットダウン原因をマニュアルでクリアするか、又はポートを再度、自動で有効化するようタイマー指定をします。

コンフィグレーションでポートが有効と表示されていれるのにデバイスがエラー又は条件の変更を検知したら、ソフトウェアがそのポートをシャットダウンします。即ち、デバイスソフトウェアは検知したエラーや条件変更によってポートを無効化します。

ポートが自動で無効化された場合、デバイスはポートを効果的にシャットダウンし、ポートはトラフィックをブロックします。ポートのLEDが一定時間内に緑色に3回点滅し、シャットダウンの原因を識別します。また、デバイスは無効化の原因をリスト化したログファイルのエントリーを作成します。*Auto-Disable* 機能を使ってタイムアウト後にポートが再度有効化されたら、デバイスはログエントリーを作成します。

Auto-Disable とは、自動で無効化されたポートをユーザー定義された時間経過後に自動で有効化し、ポートを復旧させる機能です。この機能によってポートが有効化されると、デバイスはポート番号付きでSNMPトラップを送信しますが、*Reason* パラメーターに値はありません。

Auto-Disable 機能は以下の目的を果たします。
- ネットワークアドミニストレーターのポート解析をアシストします。
- 当該ポートがネットワークを不安定にする原因となる可能性を軽減します。

Auto-Disable 機能は以下の機能に有効です。
- *Link flap* (*Port Monitor* 機能)
- *CRC/Fragments* (*Port Monitor* 機能)
- 全二重・半二重の不一致検知 (*Port Monitor* 機能)
- *DHCP Snooping*
- *Dynamic ARP Inspection*
- *Spanning Tree*
- *Port Security*
- *Overload detection* (*Port Monitor* 機能)
- *Link speed/Duplex mode detection* (*Port Monitor* 機能)

以下の例では、*Diagnostics > Ports > Port Monitor* の*CRC/Fragments* タブで指定した閾値を超えた・下回ったためにポートを無効化するようユーザーがデバイスを設定し、無効になったポートを再び自動で有効化させます。

以下の手順を実行します。

- ☐ *Diagnostics > Ports > Port Monitor* ダイアログボックスの*CRC/Fragments* タブを開きます。
- ☐ テーブルに指定された閾値が、ユーザーが求めるポート`1/1`の要件と同じであることを確認します。
- ☐ *Diagnostics > Ports > Port Monitor* ダイアログボックスの*Global* タブを開きます。
- ☐ 機能を有効化するには*Operation* フレームの`On` のラジオボタンを選択します。
- ☐ エラー検知の際、デバイスにポートを無効化させるには、ポート`1/1`の*CRC/Fragments on* カラム内のチェックボックスにチェックを入れます。

- *Action* カラムで、検知したエラーに対してどのようにデバイスに反応させるかを選択します。ここの例では、閾値を上回った（下回った）ためにデバイスがポート`1/1` を無効化し、その後ポートを再び有効化します。
  - ポートの無効化及び自動で再有効化をデバイスにさせるには、値`auto-disable` を選択し、*Auto-Disable* 機能を設定します。値`auto-disable` は、*Auto-Disable* 機能と連動している時のみ作動します。

  デバイスは、自動の再有効化がなくてもポートを無効化することができます。
  - ポートの無効化及び自動で再有効化をデバイスにさせるには、値`disable port`を選択します。
    無効化されたポートをマニュアルで再有効化するには、ポートにハイライトを入れます。
    ボタンに続き、*Reset* の項目をクリックします。
  - *Auto-Disable* 機能を設定すると、値`disable port` もポートを自動的に再有効化するようになります。
- *Diagnostics > Ports > Port Monitor* ダイアログボックスの*Auto-disable* タブを開きます。
- 閾値を上回った（下回った）ために無効化されたポートをデバイスに自動再有効化させるには、*CRC error* カラム内のチェックボックスにチェックを入れます。
- *Diagnostics > Ports > Port Monitor* ダイアログボックスの*Port* タブを開きます。
- 有効化したポートについて、*Reset timer [s]* カラムの遅延タイムを120秒に指定します。

注記：*Reset* 項目により、*Reset timer [s]*カラムに指定したタイムのカウントダウン前にポートを有効化することができます。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`interface 1/1`	インターフェース`1/1`のInterface Configuration mode に変更します。
`port-monitor condition crc-fragments count 2000`	CRC-Fragmentカウンターを2000ppmに指定します。
`port-monitor condition crc-fragments interval 15`	CRC-Fragment検知の測定間隔を15秒に設定します。
`auto-disable timer 120`	*Auto-disable* 機能がポートを再有効化した後の待機時間を`120` 秒に設定します。
`exit`	Configuration modeに切り替えます。
`auto-disable reason crc-error`	auto-disable CRC機能をアクティベートします。
`port-monitor condition crc-fragments mode`	アクションをトリガーする為に、CRC-Fragments条件をアクティベートします。
`port-monitor operation`	*Port Monitor* 機能をアクティベートします。

閾値を上回った（下回った）ためにデバイスがポートを無効化したら、ユーザーは以下のコマンドを使用してマニュアルで無効ポートをリセットすることができます。

以下の手順を実行します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`interface 1/1`	インターフェース`1/1`のInterface Configuration mode に変更します。
`auto-disable reset`	タイマーのカウントダウン前にユーザーがポートを有効化することができます。

14.8 SFPステータスの表示

SFPステータスを表示することで、現在のSFPモジュール接続及びそのプロパティを視認することができます。プロパティには以下を含みます。

- モジュール種別
- 媒体モジュールのシリアル番号
- 温度（℃）
- 送信電力（mW）
- 電力をmWで受信

以下の手順を実行します。

1. *Diagnostics > Ports > SFP* ダイアログボックスを開きます。

14.9 トポロジーディスカバリー

IEEE 802.1ABでは、LLDP（Link Layer Discovery Protocol）について定義されています。LLDPにより、自動的にLANネットワークトポロジーを検知することができます。

デバイスのLLDPがアクティブな場合、以下が発生します。
- 接続情報や管理情報を、共有LANの近隣デバイスに送信します。受信側デバイスのLLDPがアクティブな場合、デバイスの検証がなされます。
- 共有LANの近隣デバイスのLLDPがアクティブな場合、接続情報や管理情報を共有LANの近隣デバイスに送信します。
- LLDPがアクティブな近隣デバイスの情報を保存するために、管理情報データベース及びオブジェクト定義を作成します。

主要素として、接続情報には接続終端の厳格な固有識別子が含まれています：MAC（サービスアクセスポイント：SAP）これはネットワーク全域で固有のデバイスの識別子と、当デバイスの固有ポート識別子で構成されています。
- 筐体識別子（そのMACアドレス）
- ポート識別子（そのポートMACアドレス）
- ポートのディスクリプション
- システム名
- システムのディスクリプション
- サポートするシステムの性能
- 現在アクティブなシステムの性能
- 管理アドレスのインターフェースID
- ポートのVLAN ID
- ポートのオートネゴシエーションステータス
- 媒体、全二重・半二重設定及びポート速度設定
- デバイスにインストールしたVLANの情報（ポートがVLAN参加者であるか否かに関わらず、VLAN ID及びVLAN名）。

ネットワーク管理ステーションは、LLDPがアクティブなデバイスからこの情報を取り寄せることができます。この情報はネットワーク管理ステーションにネットワークトポロジーをマッピングさせます。

通常、非LLDPデバイスは情報交換に使用される特殊マルチキャストIEEE MACアドレスをブロックします。したがって、非LLDPデバイスはLLDPパケットを破棄します。LLDP可のデバイス2つの間にLLDP不可のデバイスを配置すると、LLDP不可デバイスはLLDP可のデバイス2つの間で情報交換をさせません。

LLDP可のデバイスのMIB（Management Information Base）は、lldp MIB、並びにプライベートSA2-LLDP-EXT-HM-MIB及びSA2-LLDP-MIB内にLLDP情報を保留します。

14.9.1 トポロジーディスカバリー結果の表示

ネットワークトポロジーを表示します。以下の手順を実行します。

□ *Diagnostics > LLDP > Topology Discovery* ダイアログボックスの*LLDP* タブを開きます。

複数デバイスを接続するのにハブ経由などのポートを使用した場合、テーブルには接続された個々のデバイスのラインが含まれます。

テーブル下段のDisplay FDB Entriesをアクティベートすると、テーブルにアクティブLLDPサポートの無いデバイスが表示されます。この場合、デバイスは自身のFDB（forwarding database）からの情報も含みます。

トポロジーディスカバリー機能が有効なデバイスとポートを接続すると、デバイスはLLDPデータユニット（LLDPDU）を交換し、トポロジーテーブルにはこれら近隣デバイスが表示されます。

トポロジーディスカバリーがアクティブでないデバイスのみとポートを接続する場合、このポートが接続されたデバイスを代表し、テーブルに当該ポートのラインが含まれます。このラインには接続されたデバイス数も含まれます。

トポロジーテーブルに非表示となったデバイスのMACアドレスは、明確化を目的としてFDBテーブルアドレスに含まれます。

14.9.2 LLDP-Med

メディアエンドポイントデバイス用LLDP（LLDP-MED）は、エンドポイントデバイス間で作動するLLPDへの拡張子です。エンドポイントはIP電話やその他VoIP（Voice over IP）等デバイス、サーバー、スイッチなどのネットワークデバイスを含みます。VoIPアプリケーションに特化してサポートを提供します。LLDP-MEDは、共有のTLV（type-length-value）広告メッセージ、性能（Capabilities）ディスカバリー、ネットワークポリシー、在庫管理、位置情報等を追加セットとしてサポートします

デバイスは以下のTLVメッセージをサポートします。

- capabilities TLV
  接続されたデバイスのサポート性能及びデバイスがどの性能を有効化するのかを、LLDP-MEDエンドポイントに決定させます。
- Network policy TLV
  VLANコンフィグレーションの広告や、当該ポートの特定アプリケーション関連アトリビュートを、ネットワーク接続デバイス及びエンドポイントの両方に送信させます。例えば、デバイスはVLAN番号の電話を通知したとします。この電話はスイッチに接続し、VLAN番号を取得し、コールコントロールと通信を開始します。

LLDP-MEDは以下の機能を提供します。

- VLAN ID、802.1p優先度、Diffserv code point（DSCP）を含むネットワークポリシー・ディスカバリー
- デバイス位置及びLANレベルでのMAC/ポート情報をもとにしたトポロジーディスカバリー
- ネットワーク接続デバイスから関連VoIP管理アプリケーションにエンドポイントの移動検知を通知
- 在庫管理のためのデバイス識別機能の拡張
- 例えばスイッチ又はブリッジ内蔵のマルチポートIP電話等の、エンドポイントネットワークの接続性能の識別
- LLDPプロトコルエレメントとアプリケーションレベルでの相互作用による、緊急電話サービスに迅速に有用となるよう適時なスタートアップ
- LLDP-MEDからワイヤレスLAN環境への適用性、VoWLAN（Voice over Wireless LAN：ボイスオーバーワイヤレスLAN）のサポート

14.10 ループ検知

ネットワーク内のループは接続障害又はデータ損失の原因となります。一時的なループも同様です。この状況の自動検知及びレポートにより、ユーザーがより速くこれを検知・診断することが容易となります。

⚠ 警告

機器の誤操作

コンフィグレーションの段階でループができるのを避けるには、リングの各デバイスを個々に設定します。冗長化ラインを接続する前に、リングの全デバイスのコンフィグレーションを完了させてください。

この指示に従わない場合、人的損害や装置の損傷を招くおそれがあります。

不正確なコンフィグレーションは、例えばスパニングツリーを無効化する等のループの原因となります。

デバイスは主にループが原因となる影響をユーザーに検知させ、ネットワーク管理ステーションにレポートします。ここで、デバイスにレポートを送信させるトリガーとなるループの影響の度合いを、ユーザーが指定することができます。

指定ポートから送信され、同一デバイスの別ポート又は同一ポートで短時間内に受信したBPDUフレームは、ループによる典型的な影響です。

デバイスループを検知したかを確認するには、以下の手順を実行します:

- ☐ *Switching > L2-Redundancy > Spanning Tree > Port* ダイアログボックスを開きます。
- ☐ *Port state* 及び*Port role* フィールドの値を確認します。*Port state* フィールドが値`discarding` を表示し、*Port role* フィールドが値`backup`を示していると、ポートはループ状態になっています。

  或いは...
- ☐ *Switching > L2-Redundancy > Spanning Tree > Port* ダイアログボックスを開きます。
- ☐ *Loop state* カラムの値を確認します。フィールドに値`true`が表示されていると、ポートはループ状態になっています。

14.11 レイヤー2のネットワークループからの保護

当デバイスは、レイヤー2のネットワークループからの保護をアシストします。

ネットワークのループは、過負荷によりネットワークの停止の原因となることがあります。考えられる原因は、誤ったコンフィグレーションによるデータパケットの複製です。その他原因の例として、ケーブルの不正確な挿入やデバイスのフォルト誤設定などがあります。

例として、レイヤー2のネットワークループは、冗長プロトコルがアクティブでないと以下の場合に発生する可能性があります。
- 同一デバイスのポート2つが互いに直接接続されている
- 1つ以上のアクティブな接続が2つのデバイス間で構築されている

⚠ 警告

機器の誤操作

コンフィグレーションの段階でループができるのを避けるには、レイヤー2のネットワークの各デバイスを個々に設定します。冗長化ラインを接続する前に、レイヤー2ネットワークの他デバイスのコンフィグレーションを完了させてください。

この指示に従わない場合、人的損害や装置の損傷を招くおそれがあります。

14.11.1 適用例

以下の図は、ネットワークにレイヤー2のループが疑われる例を示します。*Loop Protection* 機能は全デバイスで有効になっています。

➢ **A**:*Active mode*
エンドデバイスに接続することを意図されたポートは*active* modeで作動します。デバイスはこれらポートを評価し、*ループ検知*パケットをポートに送信します。

- **P**:*Passive mode*
  冗長リングに属するポートは、*passive* modeで作動します。デバイスはこれらポートの*ループ検知*パケットを評価するのみです。
- ***ループ1..ループ4***
  意図せず構成したレイヤー2のネットワークループ。

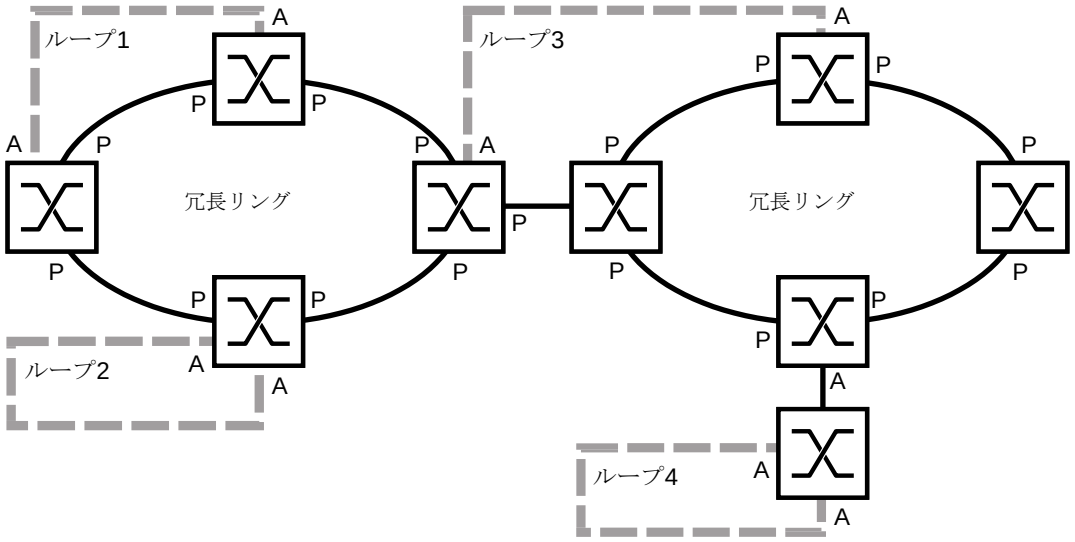


図64　意図せず構成したレイヤー2のネットワークループの例

ループ保護設定をポートに指定する

各アクティブ及びパッシブなポートに、*Loop Protection* 機能の設定を指定します。

以下の手順を実行します。

- ☐ *Diagnostics > Loop Protection* ダイアログボックスを開きます。
- ☐ *Global* フレームの*Transmit interval* フィールドで、必要があれば値を調整します。
- ☐ *Global* フレームの*Receive threshold* フィールドで、必要があれば値を調整します。
- ☐ *Mode* カラムで、ポートの*Loop Protection* 機能のアクションを指定します。
  - `active` ：エンドデバイスに接続することを意図されたポート
  - `passive` ：冗長リングに属するポート
- ☐ *Action* カラムに、値*all*を指定します。
  デバイスがこのポートにレイヤー2のループを検知すると、トラップを送信して*Auto-Disable* 機能を使用してポートを無効化します。必要に応じ数値を調整します。
- ☐ *Active* カラムのチェックボックスにチェックを入れます。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`loop-protection tx-interval 5`	必要があれば、transmit interval（伝送間隔）を指定します。
`loop-protection rx-threshold 1`	必要があれば、receive threshold（受信閾値）を指定します。
`interface 1/1`	Interface modeに切り替えます。 例：ポート*1/1*

`loop-protection mode active`	エンドデバイスに接続することを意図されたポートにモード`active` を指定します。
`loop-protection mode passive`	冗長リングに属するポートにモード`passive` を指定します。
`loop-protection action all`	デバイスがレイヤー2のネットワークループを当該ポートで検知した際にとるアクションを指定します。
`loop-protection operation`	ポートの*Loop Protection* 機能をアクティベートします。
`exit`	Configuration modeに切り替えます。

Auto-Disable機能をアクティベートする

ポートに*Loop Protection* 設定を指定したら、*Auto-Disable* 機能をアクティベートします。

以下の手順を実行します。

- ☐ *Configuration* フレームで、*Auto-disable* チェックボックスにチェックを入れます。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`loop-protection auto-disable`	*Auto-Disable* 機能をアクティベートします。

デバイス内のループ機能を有効化する 終了したら、デバイス内の*Loop Protection* 機能を有効化します。

以下の手順を実行します。

- ☐ *Operation* フレームで、*On* ラジオボタンを選択します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`loop-protection operation`	デバイスの*Loop Protection* 機能を有効化します。

14.11.2 冗長ポートの推奨設定

Loop Protection の設定によっては、デバイスはレイヤー2のループを検知すると*Auto-Disable* 機能を使用してポートを無効化します。

ポートで如何なる冗長化機能でもアクティブであれば、当該ポートの*active* modeをアクティベートしないでください。さもなければ、冗長ネットワークのパスでポートがシャットダウンすることがあります。上記の例は、冗長リングに属するポートになります。

冗長ネットワークパスが、バックアップメディアとして有用であることを確認します。デバイスは一次パスの障害に備え、冗長パスに変わります。

以下の設定は、冗長ネットワークパスでのポートのシャットダウンを防止する役に立ちます。

- ☐ 冗長ポートで*Loop Protection* 機能をディアクティベートします。或いは...
- ☐ 冗長ポートで*passive* modeを有効化します。

Loop Protection 機能及び*Spanning Tree* 機能は、相互に影響し合います。以下の手順は、デバイスの不意な挙動を防ぐ役に立ちます。

- ☐ *Loop Protection*機能を有効化したいポートの*Spanning Tree* 機能を無効化します。*Switching > L2-Redundancy > Spanning Tree > Global* ダイアログボックスの*STP active* カラムを確認します。
- ☐ 接続された各デバイスのポートの*Spanning Tree* 機能を無効化します。*Switching > L2-Redundancy > Spanning Tree* ダイアログボックスを確認します。

14.12 Eメール通知機能を使用する

当デバイスは、発生したイベントについてユーザーにEメールで通知することができます。メールサーバーが、デバイスがEメールを伝送するネットワークで使用可能であることが条件となります。

デバイスにEメールを送信させるためのセットアップは、以下の章の手順通りに進めます。

- ☐ 送信元アドレスの指定
- ☐ トリガーとなるイベントの指定
- ☐ 受取人の指定
- ☐ メールサーバーの指定
- ☐ Eメール通知機能の有効化・無効化
- ☐ テストメールを送信する

14.12.1 送信元アドレスの指定

送信元アドレスは、Eメールを送信したデバイスのメールアドレスです。デバイス内のデフォルト設定は`switch@se.com`となっています。

初期値を変更します。以下の手順を実行します。

- ☐ *Diagnostics > Email Notification > Global* ダイアログボックスを開きます。
- ☐ *Sender* フレームで、*Address* フィールドの値を変更します。有効なEメールアドレスを追加します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`logging email from-addr <user@doma.in>`	送信元アドレスを変更します。

14.12.2 トリガーとなるイベントの指定

デバイスは、以下の重要度をそれぞれに区別しています。

表51 イベントの重要度の意味

重要度	意味
`emergency`	デバイスのオペレーション準備ができていません
`alert`	直ちにユーザーの介入を必要としています
`critical`	重大ステータス
`error`	エラーステータス
`warning`	警告
`notice`	重要、通常ステータス
`informational`	情報メッセージ
`debug`	デバッグメッセージ

デバイスがユーザーに通知するイベントを指定することができます。これをするには、デバイスの通知レベルの最小重要度を指定します。

デバイスは以下のように、受信者に通知します。

- *Notification immediate*
  指定した重要度と同等以上に重大なイベントが発生すると、デバイスは即時にEメールを送信します。
- *Notification periodic*
  - 指定した重要度と同等以上に重大なイベントが発生すると、デバイスはイベントログをバッファします。
  - デバイスは、定期的に或いはバッファが一杯になると、ログファイルをEメールで送信します。
  - 重要度の低いイベントが発生しても、デバイスはこのイベントログを記録しません。

以下の手順を実行します。

☐ *Diagnostics > Email Notification > Global* ダイアログボックスを開きます。

Notification immediate フレームで、デバイスが即時にEメールを送信する設定を指定します。

☐ *Severity* フィールドで、最小重要度を指定します。

☐ *Subject* フィールドでEメールの件名を指定します。

Notification periodic フレームで、デバイスが定期的にEメールを送信する設定を指定します。

☐ *Severity* フィールドで、最小重要度を指定します。

☐ *Subject* フィールドでEメールの件名を指定します。

☐ ✓ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`logging email severity immediate <level>`	デバイスが即時にEメールを送信するイベントの最小重要度を指定します。
`logging email severity periodic <level>`	デバイスが定期的にEメールを送信するイベントの最小重要度を指定します。
`logging email subject add <immediate | periodic> TEXT`	コンテンツ`TEXT`を含む件名にラインを作成します。

14.12.3 送信間隔を変更する

ログファイル付きのEメールをどの間隔で送信するかを指定することができます。デフォルトは、`30` 分となっています。

以下の手順を実行します。

☐ *Diagnostics > Email Notification > Global* ダイアログボックスを開きます。

Notification periodic フレームで、デバイスが定期的にEメールを送信する設定を指定します。

☐ 送信間隔を変更するには、*Sending interval [min]* の値を変更します。

☐ ✓ ボタンをクリックし、変更を一時的に保存します。

```
enable
configure

logging email duration <30..1440>
```

Privileged Exec Modeに切り替えます。
Configuration modeに切り替えます。
ログファイル付きEメールをデバイスがどの間隔で送信するかを指定します。

14.12.4 受信者の指定

当デバイスでは、受信者10個まで指定することができます。

以下の手順を実行します。

- ☐ *Diagnostics > Email Notification > Recipients* ダイアログボックスを開きます。
- ☐ テーブルエントリーを追加するには、  ボタンをクリックします。
- ☐ *Notification type* カラムで、当該受信者にデバイスがEメールを即時に、又は定期的に送信するかを指定します。
- ☐ *Address* カラムで、受信者のメールアドレスを指定します。
- ☐ *Active* カラムのチェックボックスにチェックを入れます。
- ☐  ボタンをクリックし、変更を一時的に保存します。

```
enable

configure

logging email to-addr add <1..10>
addr <user@doma.in> msgtype
<immediately | periodically>
```

Privileged Exec Modeに切り替えます。

Configuration modeに切り替えます。

受信者をメールアドレス`user@doma.in`付きで指定します。デバイスはメモリ内に`1..10`の範囲で設定を管理します。

14.12.5 メールサーバーの指定

当デバイスは、暗号化、非暗号化のメールサーバーへの接続をサポートします。

以下の手順を実行します。

- ☐ *Diagnostics > Email Notification > Mail Server* ダイアログボックスを開きます。
- ☐ テーブルエントリーを追加するには、  ボタンをクリックします。
- ☐ *IP address* カラムで、サーバーのIPアドレス又はDNS名を指定します。
- ☐ *Encryption* カラムで、デバイスとメールサーバー間の接続を暗号化するプロトコルを指定します。
- ☐ メールサーバーが熟知しているポートでないポートを使用する場合、*Destination TCP port* カラムのTCPポートを指定します。

メールサーバーが認証リクエストする場合：

- ☐ *User name* 及び*Password* カラムで、デバイスがメールサーバーを認証するアカウントの認証情報を指定します。

- ☐ *Description* カラムで、分かりやすい名前を入力します。
- ☐ *Active* カラムのチェックボックスにチェックを入れます。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

```
enable
```
Privileged Exec Modeに切り替えます。

```
configure
```
Configuration modeに切り替えます。

```
logging email mail-server add <1..5> addr <IP ADDRESS> [security
<none|tlsv1>] [username <USER NAME>] [password <PASSWORD>]
[port <1..65535>]
```
IPアドレスと共にメールサーバーを指定します。`IP ADDRESS`.デバイスはメモリ内に`1..5`の範囲で設定を管理します。

14.12.6 Eメール通知機能の有効化・無効化

以下の手順を実行します。

- ☐ *Diagnostics > Email Notification > Global* ダイアログボックスを開きます。
- ☐ 機能を有効化するには*Operation* フレームの*On* のラジオボタンを選択します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

```
enable
```
Privileged Exec Modeに切り替えます。

```
configure
```
Configuration modeに切り替えます。

```
logging email operation
```
Eメールの送信を有効化します。

```
no logging email operation
```
Eメールの送信を無効化します。

14.12.7 テストメールを送信する

当デバイスでは、テストメールを送信して設定を確認することができます。

条件：
- ➢ Eメール設定は完全に指定されていなければなりません。
- ➢ *Email Notification* 機能が有効でなければなりません。

以下の手順を実行します。

- ☐ *Diagnostics > Email Notification > Mail Server* ダイアログボックスを開きます。
- ☐ ☰ ボタンに続き、*Connection test* の項目をクリックします。ダイアログボックスに *Connection test* ウィンドウが表示されます。
- ☐ *Recipient* ドロップダウンリストで、デバイスがテストメールを送信する受信者を選択します。
- ☐ *Message text* フィールドで、テストメールのテキストを指定します。
- ☐ テストメールを送信するには、*Ok* ボタンをクリックします。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`logging email test msgtype <urgent|non- urgent> TEXT`	受信者に、コンテンツ`TEXT` 付きのEメールを送信します。

エラーメッセージが現れずに受信者がメールを受信すると、デバイスは正しく設定されています。

14.13 レポート

以下に診断に有用なレポートやボタンを示します。

- System Log file（システムログファイル）
  ログファイルは、デバイスがデバイス内部イベントを書き込むHTMLファイルです。
- Audit Trail（監査証跡）
  成功したコマンド及びユーザーコメントをログします。ファイルにはSNMPロギングも含まれます。
- Persistent Logging（パーシステントロギング）
  外部メモリがある場合、デバイスはログのエントリーファイルを外部メモリに保存します。これらファイルは、電源を失った後も有用です。保存可能ファイルの最大・最小サイズ及びイベントログの重要度は、設定可能です。保存可能なファイルの、ユーザー定義された最大・最小数を取得した後、デバイスはエントリーをアーカイブし、新規ファイルを開始します。デバイスは古いファイルを削除し、他ファイルの名前を変更することで設定されたファイル数を維持します。これらファイルを閲覧するには、コマンドラインインターフェースを使用するか、将来の閲覧用に外部サーバーにコピーします。
- *Download support information*
  このボタンでは、システム情報をzipアーカイブとしてダウンロードすることができます。

保守の場合、これらレポートは技師に必要な情報を提供します。

14.13.1 グローバル設定

このダイアログでは、例えばコンソール、Syslogサーバー、コマンドラインインターフェースへの接続等、デバイスが何処へレポートを送信するかを有効化・無効化することができます。また、どの重要度でデバイスがレポートにイベントの書込みをするかを、設定することもできます。

以下の手順を実行します。

- ☐ *Diagnostics > Report > Global* ダイアログボックスを開きます。
- ☐ コンソールにレポートを送信するには、*Console logging* フレームの*Severity* フィールドで、任意のレベルを指定します。
- ☐ 機能を有効化するには*Console logging*フレームの`On` のラジオボタンを選択します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

デバイスはイベントログを個別の保存エリア2つに分けてバッファすることで、緊急のイベントの時のためにログエントリーが保持されます。高優先の保存エリアにデバイスにバッファさせるデバイスログの、イベントの最小重要度を指定します。

以下の手順を実行します。

- ☐ イベントをバッファに送信するには、*Buffered logging* フレームの*Severity*フィールドに任意のレベルを指定します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

SNMPリクエストのログをアクティベートすると、デバイスは当リクエストをイベントとしてSyslogにログします。*Log SNMP get request* 機能は、デバイスコンフィグレーション情報のユーザーリクエストをログします。*Log SNMP get request* 機能は、デバイスコンフィグレーションのイベントをログします。デバイスにSyslogへとログさせるイベントの最小レベルを指定します。

以下の手順を実行します。

- ☐ SNMP読出しリクエストをイベントとしてデバイスにSyslogサーバーに送信させるには、*Log SNMP get request* 機能を有効化します。
  機能を有効化するには*SNMP logging* フレームの*On* のラジオボタンを選択します。
- ☐ SNMP書込みリクエストをイベントとしてデバイスにSyslogサーバーに送信させるには、*Log SNMP set request* 機能を有効化します。
  機能を有効化するには*SNMP logging* フレームの*On* のラジオボタンを選択します。
- ☐ 読出し・書込み（get / set）リクエストの重要度を選択します。
- ☐ ボタンをクリックし、変更を一時的に保存します。

アクティブな時、デバイスはコマンドラインインターフェース及び監査証跡を使用して施したコンフィグレーションの変更をログします。この機能はIEEE 1686規定の、Substation Intelligent Electronic Devices（変電所のインテリジェント電子装置）を基にしたものです。

以下の手順を実行します。

- ☐ *Diagnostics > Report > Global* ダイアログボックスを開きます。
- ☐ 機能を有効化するには*CLI logging* フレームの*On* のラジオボタンを選択します。
- ☐ ボタンをクリックし、変更を一時的に保存します。

当デバイスでは、以下のシステム情報を1つのzipファイルとしてPCに保存することができます。

- `audittrail.html`
- `defaultconfig.xml`
- `script`
- `runningconfig.xml`
- `supportinfo.html`
- `systeminfo.html`
- `systemlog.html`

デバイスは自動的にzip形式のファイル名を作成します。
`<IP_address>_<system_name>.zip`.

以下の手順を実行します。

- ☐ ボタンに続き、*Download support information* の項目をクリックします。
- ☐ サポート情報を保存するディレクトリを選択します。
- ☐ ボタンをクリックし、変更を一時的に保存します。

14.13.2 Syslog

当デバイスでは、デバイス内部のイベントを1つ以上（最大8つ）のSyslogサーバーにメッセージを送ることができます。また、SNMPリクエストをSyslog内のイベントとしてデバイスにリクエストすることもできます。

注記：全てのイベントログを表示するには、*Diagnostics > Report > Audit Trail* ダイアログボックス又は*Diagnostics > Report > System Log* ダイアログボックスを開きます。

以下の手順を実行します。

- ☐ *Diagnostics > Syslog* ダイアログボックスを開きます。
- ☐ テーブルエントリーを追加するには、  ボタンをクリックします。
- ☐ *IP address* カラムで、Syslogサーバーの*IP*アドレス又は*ホスト名*を入力します。Syslogサーバーには有効なIPv4又はIPv6アドレスを指定することができます。
- ☐ *Destination UDP port* カラムで、Syslogサーバーがログエントリーを待機するTCP又はUDPポートを指定します。
- ☐ *Min. severity* カラムで、デバイスがSyslogサーバーにログエントリーを送信するイベントに必要な最小重要度を指定します。
- ☐ *Active* カラムのチェックボックスにチェックを入れます。
- ☐ 機能を有効化するには*Operation* フレームの*On* のラジオボタンを選択します。
- ☐  ボタンをクリックし、変更を一時的に保存します。

SNMP logging フレームで、以下のようにSNMPの読出し・書込みリクエストを設定します。

以下の手順を実行します。

- ☐ *Diagnostics > Report > Global* ダイアログボックスを開きます。
- ☐ SNMP読出しリクエストをイベントとしてデバイスにSyslogサーバーに送信させるには、*Log SNMP get request* 機能を有効化します。
  機能を有効化するには*SNMP logging* フレームの*On* のラジオボタンを選択します。
- ☐ SNMP書込みリクエストをイベントとしてデバイスにSyslogサーバーに送信させるには、*Log SNMP set request* 機能を有効化します。
  機能を有効化するには*SNMP logging* フレームの*On* のラジオボタンを選択します。
- ☐ 読出し・書込み（get / set）リクエストの重要度を選択します。
- ☐  ボタンをクリックし、変更を一時的に保存します。

```
enable
```
Privileged Exec Modeに切り替えます。

```
configure
```
Configuration modeに切り替えます。

```
logging host add 1 addr 10.0.1.159
severity 3
```
Syslogサーバーリストに新規受信者を追加します。数値`3` はデバイスがログするイベントの重要度を指定したものです。数値`3` は`error`を意味します。

```
logging host add 2 addr 2001::1
severity 4
```
Syslogサーバーリストに新規IPv6受信者を追加します。数値`4` は`warning`を意味します。

```
logging syslog operation
```
Syslog 機能を有効化します。

```
enable
```
Privileged Exec Modeに切り替えます。

```
show logging host
```
Syslogホスト設定を表示します。

```
No.   Server IP      Port  Max.Severity   Type        Status
----  -------------- ----  -------------  ----------  ------
1     10.0.1.159     514   error          systemlog   active
2     2001::1        514   warning        systemlog   active
```

```
configure
```
Configuration modeに切り替えます。

```
logging snmp-requests get operation
```
SNMP GETリクエストをログします。

```
logging snmp-requests get severity 5
```
数値`5` は、SNMP GETリクエストがあった場合にデバイスがログするイベントの重要度を指定したものです。数値`5` は`notice`を意味します。

`logging snmp-requests set operation`	SNMP SET リクエストをログします。
`logging snmp-requests set severity 5`	数値`5` は、SNMP SET リクエストがあった場合にデバイスがログするイベントの重要度を指定したものです。数値`5` は`notice`を意味します。
`exit`	Privileged Exec Modeに切り替えます。
`show logging snmp`	SNMPロギングの設定を表示します。

```
Log SNMP GET requests            : enabled
Log SNMP GET severity            : notice
Log SNMP SET requests            : enabled
Log SNMP SET severity            : notice
```

14.13.3 システムログ

当デバイスではシステムイベントのログファイルを呼び出すことができます。*Diagnostics > Report* >System Log ダイアログボックスのテーブルには、イベントログのリストが表示されています。
以下の手順を実行します。

- ☐ ログのカウンターを更新するには、  ボタンをクリックします。
- ☐ ログコンテンツをhtmlファイルとして保存するには、  ボタンに続き、*Reset* の項目をクリックします。
- ☐ ログコンテンツを削除するには、  ボタンに続き、*Reset* の項目をクリックします。
- ☐ ログコンテンツをキーワードで検索するには、ウェブブラウザの検索機能を使用します。

注記：イベントログを1つ以上のSyslogサーバーに送信するオプションもあります。

14.13.4 Syslog over TLS

TLS（トランスポート層セキュリティ）とは、コンピューターネットワーク上に通信セキュリティを付するための暗号化プロトコルです。TLSプロトコルの主な目的は、コンピューターアプリケーション間2つの通信に、プライバシー及びデータ完全性を付することです。

Syslogサーバーとの接続を開始した後、デバイスはTLSハンドシェイクを使用し、サーバーから受信した証明書を検証します。このため、ユーザーはリモートサーバー又は外部メモリから、デバイスにPEM証明書を転送します。構成したサーバーのIPアドレス又はDNS名が、証明書にある情報と一致することを確認します。この情報は証明書のCommon Nameフィールド又はSubject Alternative Nameフィールドにあります。

デバイスは暗号化されたTLS Syslogメッセージを、*Destination UDP port* カラムに指定したTCPポートを通して送信します。

注記：サーバーのIPアドレス又はDNS名を、サーバー証明書にあるIPアドレス又はDNS名と一致するように指定します。証明書に入力した値は、Common Nameフィールド又はSubject Alternative Nameフィールドにあります。

参考例

ここの例では、*Syslog* 機能のコンフィグレーションについて示します。この手順通りに進めることで、暗号化されたTLS Syslogメッセージを、*Destination UDP port* カラムに指定したTCPポートを通して送信することができます。

デバイスからSyslogサーバーへ送信されるSyslogメッセージは、セキュリティ保護のないネットワーク上を通過することができます。SyslogサーバーをTLS上でコンフィグレーションするには、CA（認証局）証明書をデバイスに転送します。

注記：新規にロードした証明書を直ぐに発効させるには、*Syslog*機能を再起動します。

以下の手順を実行します。

- ☐ *Diagnostics > Syslog*ダイアログボックスを開きます。
- ☐ *SSH* サーバーをとの接続を開始するには*Operation* フレームの`On` のラジオボタンを選択します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

デバイスは受信した証明書を検証します。また、デバイスはサーバーも認証し、Syslogメッセージの送信を開始します。

- ☐ リモートサーバー又は或いは外部メモリから、デバイスにPEM証明書を転送してください。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`logging host add 1 addr 192.168.3.215`	インデックス`1` を、右記のIPv4アドレスのSyslogサーバーに追加します。`192.168.3.215`
`logging host add 2 addr 2001::1`	インデックス`2` を、右記のIPv6アドレスのSyslogサーバーに追加します。`2001::1.`
`logging host modify 1 port 6512 type systemlog`	ポート番号`6512` を指定し、イベントをシステムログにログします。
`logging host modify 1 transport tls`	伝送を`tls`と指定します。
`logging host modify 1 severity informational`	イベントの種別をシステムログで`informational`と指定します。
`enable`	Privileged Exec Modeに切り替えます。
`copy syslogcacert evmm`	CA証明書を外部メモリからこのデバイスにコピーします。
`show logging host`	Syslogホスト設定を表示します。

14.13.5 監査証跡

Diagnostics > Report > Audit Trail ダイアログボックスにはシステム情報が含まれ、コマンドラインインターフェース及びSNMPを通したデバイスコンフィグレーションが変わります。デバイスコンフィグレーションが変わった場合、ダイアログボックスに「誰」が「何」を「いつ」変えたかが表示されます。

Diagnostics > Syslog ダイアログボックスでは、デバイスが監査証跡を送信する最大8つのSyslogサーバーを指定できます。

以下のリストにイベントログを示します。
- コンフィグレーションパラメーターの変更
- コマンドラインインターフェースを使用したコマンド（show コマンド除く）
- コメントをログするコマンドラインインターフェースを使用した、コマンドlogging audit-trail <string>
- システム時計の自動変更
- ウォッチドッグイベント
- ログイン試行の失敗数回後にユーザーをロック
- コマンドラインインターフェースを使用した、ローカル又は遠隔でのユーザーログイン
- ユーザーがマニュアルで開始したログアウト
- コマンドラインインターフェースのアクティビティが無く、ユーザー定義された時間経過後の自動ログアウト
- ファームウェアアップデートを含むファイル転送操作
- Ethernet Switch Configuratorを使用したコンフィグレーションの変更
- 外部メモリを使用した自動コンフィグレーション又はファームウェアアップデート
- 無効なログインを原因とするデバイス管理へのアクセスブロック
- リブート
- HTTPSトンネル上でのSNMPの開閉
- 検知された電源喪失

14.14 TCPdumpでのネットワーク分析

TCPdumpとは、ネットワークアドミニストレーターが使用するパケットスニッフィングのUNIXユーティリティで、ネットワークトラフィックのスニッフィングと分析を行うものです。ネットワークトラフィックのスニッフィングをする幾つかの理由として、ホスト間の接続性の確認、又はネットワークを往来するトラフィックを分析することが挙げられます。

デバイス内のTCPdumpは、管理CPUが送受信するパケットのデコードやキャプチャーの可能性を与えるます。この機能はコマンド`debug` で使用可能です。TCPdump機能の更なる詳細については、コマンドラインインターフェースマニュアルを参照。

14.15 データトラフィックの監視

当デバイスでは、デバイスを通過するデータパケットを宛先ポートに転送することができます。その際にユーザーはデータパケットを監視し、評価することができます。

当デバイスは、以下のオプションを提供します。
➢ ポートミラーリング

14.15.1 ポートミラーリング

ポートミラーリング機能では、ユーザーが物理ソースポートから物理宛先ポートにデータパケットをコピーすることができます。

ソースポートの送受信方向のデータトラフィックを、RMONプローブ等に接続された管理ツールで宛先ポートを監視することができます。この機能は、ソースポートで稼働するデータトラフィックに影響することはありません。

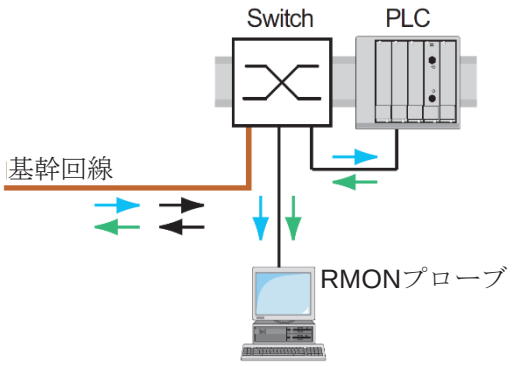


図65 参考例

デバイスは、他のソースポートからコピーしたデータパケットのみを宛先ポートに転送します。

宛先ポートを介してデバイス管理にアクセスするためには、*Port Mirroring* 機能のスイッチをオンにする前に*Allow management* チェックボックスにチェックを入れます。当デバイスでは、ユーザーがアクティブな*Port Mirroring* セッションを中断することなく、宛先ポートを介してデバイス管理にアクセスすることができます。

注記：デバイスはマルチキャスト、ブロードキャスト、不明なユニキャストを宛先ポートに複製します。

宛先ポートのVLAN設定が変わることはありません。宛先ポートからデバイス管理にアクセスするための条件として、宛先ポートがデバイス管理のVLANメンバーでなければなりません。

ポートミラーリング機能の有効化

以下の手順を実行します。

- ☐ *Diagnostics > Ports > Port Mirroring* ダイアログボックスを開きます。
- ☐ ソースポートを指定します。
  関連ポートの*Enabled* カラムのチェックボックスにチェックを入れます。
- ☐ 宛先ポートを指定します。
  Destination port フレームの*Primary port* ドロップダウンリストから任意のポートを選択します。
  このドロップダウンリストには有用なポートのみがリストされています。既にソースポートと指定されたポートは対象になりません。
- ☐ 必要があれば、2つ目の宛先ポートを指定します。
  Destination port フレームの*Secondary port* ドロップダウンリストから任意のポートを選択します。一次（primary）宛先ポートを既に指定していることが条件となります。
- ☐ 宛先ポートを介してデバイス管理にアクセスするためには、
  Destination port フレームで、*Allow management* チェックボックスにチェックを入れます。
- ☐ ボタンをクリックし、変更を一時的に保存します。

Port Mirroring 機能を無効化してデフォルト設定に戻すには、ボタンに続き、*Reset config* の項目をクリックします。

14.16 セルフテスト

デバイスは自身のアセットを、ブート中及びそれ以降も定期的に確認します。デバイスはシステムタスクが有用か或いは終了か、また、メモリの残量を確認します。加えて、デバイスはアプリケーションの機能及びハードウェアのチップセットに劣化がないかを確認します。

デバイスがインテグリティの劣化を検知すると、ユーザー定義したアクションで当劣化に対して反応します。以下カテゴリーのコンフィグレーションが実行できます。

- `task`
  タスクが失敗した場合に取るべきアクション。
- `resource`
  リソース不足の場合に取るべきアクション。
- `software`
  ソフトウェアのインテグリティ低下の場合に取るべきアクション、例えば、コードセグメントのチェックサム又は違反アクセス。
- `hardware`
  ハードウェア劣化の際に取るべきアクション。

インテグリティの低下をデバイスが検知した場合に、各カテゴリーでアクションが取られるように設定します。以下アクションのコンフィグレーションが実行できます。

- `log only`
  このアクションは、ロギングファイルにメッセージを書き込みます。
- `send trap`
  トラップ宛先にSNMPトラップを送信します。
- `reboot`
  アクティベートすると、カテゴリーに発生したエラーが以下手順でデバイスにリブートを実行させます。

- ☐ *Diagnostics > System > Selftest* ダイアログボックスを開きます。
- ☐ *Action* カラムに、原因に対して取るべきアクションを指定します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`selftest action task log-only`	タスクに失敗した場合にイベントログにメッセージを送信します。
`selftest action resource send-trap`	リソース不足の場合、SNMPトラップを送信します。
`selftest action software send-trap`	ソフトウェアのインテグリティが低下すると、SNMPトラップを送信します。
`selftest action hardware reboot`	ハードウェアが劣化すると、デバイスをリブートします。

これらの機能を無効化することで、コールドスタート後のデバイスの再起動に要する時間が短くなります。これらオプションは、*Diagnostics > System > Selftest* ダイアログボックスにあります。

- *RAM test*
  コールドスタート中の*RAM test* 機能をアクティベート・ディアクティベートします。

- *SysMon1 is available*
  コールドスタート中のシステムモニター機能をアクティベート・ディアクティベートします。
- *Load default config on error*
  再起動中に読出し可能なコンフィグレーションがない場合での、デフォルトのデバイスコンフィグレーションをロードする機能をアクティベート・ディアクティベートします。

以下の設定では、デバイスが再起動中に読出し可能なコンフィグレーションプロファイルを検知できない場合、デバイスへのアクセスが恒久的にブロックされます。
- *SysMon1 is available* チェックボックスにチェックが入っていない。
- *Load default config on error* チェックボックスにチェックが入っていない。

上記のケースとは、例えばロード中のコンフィグレーションプロファイルのパスワードがデバイスに設定されたパスワードと異なる場合が挙げられます。デバイスのロックを再度解除するには、現地販売代理店にご連絡ください。

以下の手順を実行します。

`selftest ramtest`	コールドスタートの際、RAMのセルフテストを有効化します。
`no selftest ramtest`	ramtest機能を無効化します。
`selftest system-monitor`	SysMon1機能を有効化します。
`no selftest system-monitor`	SysMon1機能を無効化します。
`show selftest action`	デバイスが劣化した場合に取るべきアクションのステータスを表示します。
`show selftest settings`	コールドスタートの際のramtest及びSysMon設定を表示します。

14.17 銅線ケーブルテスト

この機能は、短絡又は開放回路用のインターフェースに接続されている銅線ケーブルのテストに使用します。このテストを行うと、当該ポートにトラフィックがある場合は妨害されてしまいます。

テーブルには、各ペアのステータス及び長さが表示されます。デバイスは以下の意味を成す結果を返信します。

- normal：ケーブルは異常なく作動している
- open：ケーブルが妨害されている
- short circuit：ケーブルに短絡がある
- untested：未テストのケーブル
- Unknown：ケーブル未挿入・抜け

15 デバイスの拡張機能

15.1 デバイスをDHCPサーバーとして使用する

DHCPサーバー（Dynamic Host Configuration Protocol：ダイナミックホスト コンフィグレーションプロトコル）は、IPアドレス、ゲートウェイ、クライアントへのDNSやNTPパラメーター等のその他ネットワーク定義を割当てるものです。

DHCPのオペレーションは、4つの基本フェーズ：サーバー探索、IPリース提示、IPリース要求、IPリース確認に分けることができます。略語DORA（Discovery：探索、Offer：提示、Request：要求、Acknowlegment：確認）として各段階を覚えておくと便利です。サーバーはクライアントデータをUDPポート67で受信し、このデータをUDPポート68のクライアントに転送します。

DHCPサーバーは、IPアドレスをクライアントに割当てるIPアドレスプール（pool）を提供します。プールにはエントリーのリストが含まれます。エントリーは特定IPアドレス又はIPアドレスの範囲を定義しています。

当デバイスでは、DHCPサーバーを全域又はインターフェース毎にアクティベートすることができます。

15.1.1 ポート毎又はVLAN毎に割当てるIPアドレス

DHCPサーバーは静的IPアドレス又は一定範囲の動的IPアドレスを、ポート又はVLANに接続されたクライアントに割当てます。当デバイスではポート又はVLANにこれらのエントリーを作成することができます。VLANにIPアドレスを割当てるためのエントリーを作成すると、ポートのエントリーはグレーアウトします。ポートにIPアドレスを割当てるためのエントリーを作成すると、VLANのエントリーはグレーアウトします。

静的なIPアドレスの割当てとは、DHCPサーバーが特定クライアントに同一のIPアドレスを割当てることを意味します。DHCPサーバーは、固有のハードウェアIDを使用してクライアントを識別します。静的アドレスエントリーはIPアドレス1つを含み、サーバーが特定クライアントからリクエストを受信するポート又はVLANに適用されます。静的アドレスの割当てには、特定のポート又は複数ポートにプールエントリーを作成しIPアドレスを入力しますが、*Last IP address* カラムは空のままとします。DHCPサーバーがクライアントを固有に識別するハードウェアIDを指定します。このIDは、MACアドレス、クライアントID、リモートID、回路IDのいずれかとなります。クライアントがコンフィグレーション済みのハードウェアIDにコンタクトをする際、DHCPサーバーは動的IPアドレスを割当てます。

また、当デバイスでは動的IPアドレスの範囲を、DHCPサーバーがプールからフリーのIPアドレスを割当てるポート又はVLANをユーザーが割当てることができます。ポート又はVLANに動的プールエントリーを追加するには、IPアドレス範囲の最初と最後のIPアドレスを指定しますが、*MAC address*、*Client ID*、*Remote ID*、*Circuit ID* カラムは空のままとします。複数のプールエントリーを作成することで、ギャップを含むＩＰアドレスの範囲を得ることができます。

15.1.2 DHCPサーバーの静的IPアドレス参考例

ここの例では、デバイスがポートに静的IPアドレスを割当てるようコンフィグレーションします。デバイスは、固有ハードウェアIDを持つクライアントを認識します。ここではハードウェアIDはクライアントのMACアドレス`00:24:E8:D6:50:51`となります。以下の手順を実行します。

- ☐ *Advanced > DHCP Server > Pool* ダイアログボックスを開きます。
- ☐ テーブルエントリーを追加するには、  ボタンをクリックします。
- ☐ *IP address* カラムに、値`192.168.23.42`を指定します。
- ☐ *Port* カラムに、値`1/1`を指定します。
- ☐ *MAC address* カラムに、値`00:24:E8:D6:50:51`を指定します。
- ☐ クライアントに時間制限無くIPアドレスを割当てるには、*Lease time [s]* カラムに値`4294967295`を指定します。
- ☐ *Active* カラムのチェックボックスにチェックを入れます。
- ☐ *Advanced > DHCP Server > Global* ダイアログボックスを開きます。
- ☐ ポート`1/1`には、*DHCP server active* カラムのチェックボックスにチェックを入れます。
- ☐ 機能を有効化するには*Operation* フレームの*On* のラジオボタンを選択します。
- ☐  ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`dhcp-server pool add 1 static 192.168.23.42`	インデックス`1`のエントリーを作成し、IPアドレス`192.168.23.42`を静的プールに追加します。
`dhcp-server pool modify 1 mode interface 1/1`	インデックス静的アドレス`1`で、インターフェース`1/1`に静的アドレスを割当てます。
`dhcp-server pool modify 1 mode mac 00:24:E8:D6:50:51`	MACアドレス`00:24:E8:D6:50:51`のデバイスには、インデックス`1`にIPアドレスを割当てます。
`dhcp-server pool mode 1`	インデックス`1` のプールエントリーを有効化します。
`dhcp-server pool modify 1 leasetime infinite`	クライアントに時間制限無くIPアドレスを割当てるには、エントリーをインデックス`1`に変更します。
`dhcp-server operation`	DHCPサーバーを全域で有効化します。
`interface 1/1`	インターフェース`1/1`のInterface Configuration modeに変更します。
`dhcp-server operation`	このポートの*DHCP Server* サーバー機能をアクティベートします。

15.1.3 DHCPサーバーの動的IPアドレス範囲の参考例

当デバイスでは動的IPアドレスの範囲を作成することができます。*MAC address*、*Client ID*、*Remote ID* 、*Circuit ID* のフィールドは空のままとします。動的IPアドレスの範囲を、範囲内にギャップを保って作成するには、テーブルに複数エントリーを作成します。以下の手順を実行します。

- ☐ *Advanced > DHCP Server > Pool* ダイアログボックスを開きます。
- ☐ テーブルエントリーを追加するには、  ボタンをクリックします。
- ☐ *IP address* カラムに、値192.168.23.92を指定します。これが範囲内で1番目のIPアドレスとなります。
- ☐ *Last IP address* カラムに、値192.168.23.142を指定します。これが範囲内で最後のIPアドレスとなります。

Lease time [s] カラムのデフォルトは60日です。

- ☐ *Port* カラムに、値1/2を指定します。
- ☐ *Active* カラムのチェックボックスにチェックを入れます。
- ☐ *Advanced > DHCP Server > Global* ダイアログボックスを開きます。
- ☐ ポート1/2には、*DHCP server active* カラムのチェックボックスにチェックを入れます。
- ☐ 機能を有効化するには*Operation* フレームの*On* のラジオボタンを選択します。
- ☐  ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`dhcp-server pool add 2 dynamic 192.198.23.92 192.168.23.142`	IP範囲が192.168.23.92 から192.168.23.142までの動的プールを追加します。
`dhcp-server pool modify 2 leasetime {seconds | infinite}`	Lease Timeを秒単位又は無限で入力します。
`dhcp-server pool add 3 dynamic 192.198.23.172 192.168.23.180`	IP範囲が192.168.23.172 から192.168.23.180までの動的プールを追加します。
`dhcp-server pool modify 3 leasetime {seconds | infinite}`	Lease Timeを秒単位又は無限で入力します。
`dhcp-server pool mode 2`	インデックス2 のプールエントリーを有効化します。
`dhcp-server pool mode 3`	インデックス3 のプールエントリーを有効化します。
`dhcp-server operation`	DHCPサーバーを全域で有効化します。
`interface 2/1`	インターフェース2/1のInterface Configuration mode に変更します。
`dhcp-server operation`	このポートの*DHCP Server* サーバー機能をアクティベートします。

15.2 DHCP L2 リレー

デバイスの前面パネルには、以下の警告メッセージがあります。

⚠ 警告
誤操作 DHCPオプション82が有効な場合、ケーブル配置を変えないでください。保守に先立ってユーザーマニュアルをご確認ください。 **この指示に従わない場合、人的損害や装置の損傷を招くおそれがあります。**

ネットワークアドミニストレーターは、DHCPクライアント情報を追加するのにDHCPレイヤー2*リレーエージェント*を使用します。この情報は、クライアントにアドレス割当て及びコンフィグレーションを実行するため、レイヤー3*リレーエージェント*及びDHCPサーバーで要求されるものです。

DHCPクライアントとサーバーが同じIPサブネットにある場合、互いにIPアドレスリクエストを交換し、直接返信します。但し、サブネット毎にDHCPサーバーを置くことはコストが高く、あまり実用的ではありません。サブネット毎にDHCPサーバーを置く代わりの方法として、異なるサブネットのDHCPクライアントとDHCPサーバーの間でネットワークデバイスにパケットをリレーさせることができます。

レイヤー3の*リレーエージェント*は、基本的にはクライアントおよびサーバーサブネット両方にIPインターフェースのあるルーターで、これらの間にトラフィックを導きます。但しレイヤー2に切り替えたネットワークでは、クライアント及びレイヤー3の*リレーエージェント*又はDHCPサーバーの間に、例えばスイッチ等1つ以上のネットワークデバイスがあります。このような場合、デバイスはレイヤー2の*リレーエージェント*に、レイヤー3の*リレーエージェント*及びDHCPサーバーがアドレス及びコンフィグレーションのアサイメントロールを実行しなければならないという情報を追加させます。

この機能のデフォルト設定の一部は以下リストの通りです。

- Global setting:
  - アクティブ設定：disable
- Interface settings:
  - アクティブ設定：disable
  - Trustedポート：disable
- VLAN settings:
  - アクティブ設定：disable
  - *回路ID*：enable
  - *リモートID*種別：mac
  - *リモートID*：空白

DHCPv6プロトコルについて、*リレーエージェント*はクライアント及びDHCPv6サーバー間で交換されるDHCPv6パケットに*リレーエージェント*オプションを追加するのに使用します。軽量化DHCPv6リレーエージェント（LDRA）は、RFC 6221に記載されています。

LDRAは2種類のメッセージを処理します。
- 1種類目のメッセージは、クライアントの固有情報を含む*リレー転送*（Relay-Forward）メッセージです。
- 2種類目のメッセージは、DHCPv6 が*リレーエージェント*に送信する*リレー返信*（Relay-Reply）メッセージです。次に、*リレーエージェント*は当初の*Relay-Forward*メッセージにカプセル化された情報を含めるようメッセージを検証し、有効となれば、パケットをクライアントに送信します。

*Relay-Forward*メッセージは*インターフェースID*情報を含み、*Option 18*と呼ばれます。このオプションでは、クライアントリクエインターフェースインターフェースを識別するための情報が得られます。デバイスは*Option 18*情報を含まないDHCPv6パケットは破棄します。

15.2.1 回路及びリモートID

IPv4環境では、クライアントのリクエストをDHCPサーバーに送信する前に、デバイスは*回路ID*及び*リモートID*をDHCPリクエストパケットの*Option 82*フィールドに追加します。
- *回路ID*にはデバイスがどのポートでクライアントのリクエストを受信したかが保存されます。
- *リモートID*にはMACアドレス、IPアドレス、システム名又はユーザー定義された文字ストリングが含まれます。これを使用することで、参加デバイスはクライアントリクエストを受信した*リレーエージェント*を識別します。

デバイス及び他の*リレーエージェント*は、DHCP *リレーエージェント*から元のクライアントに対する返信をリダイレクトするのにこの情報を使用します。DHCPサーバーは、例えば特定のアドレスプールからクライアントにIPアドレスを割当てるなど、このデータを分析します。

また、DHCPサーバーのリレーパケットには*回路ID*及び*リモートID*が含まれます。クライアントに返信を転送する前に、デバイスは*Option 82*フィールドからこの情報を削除します。

15.2.2 DHCP L2 リレーのコンフィグレーション

Advanced > DHCP L2 Relay > Configuration ダイアログボックスでは、アクティブなポート及びVLANの情報をアクティベートすることができます。*Operation* フレームで、*On* ラジオボタンを選択します。 ボタンをクリックします。

デバイスは、*Option 82*情報を含むDHCPv4パケット及び*Option 18*情報を含むDHCPv6パケットを、*DHCP L2 Relay* カラム及び*Trusted port* カラムのチェックボックスにチェックが入ったポートに転送します。通常、これらはDHCPサーバーのネットワークにあるポートとなります。

DHCPクライアントが接続されているポートは、*DHCP L2 Relay* 機能をアクティベートしますが、*Trusted port* チェックボックスにはチェック無しのままとします。これらポートでは、デバイスは*Option 82*情報を含むDHCPv4パケット及び*Option 18*情報を含むDHCPv6パケットを破棄します。

以下にDHCPv4 L2リレー機能のコンフィグレーション例を示します。DHCPv6 L2リレー機能のコンフィグレーション手順はこれに類似しますが、*Option 82*に指定する*回路ID*及び*リモートID*エントリーは異なります。

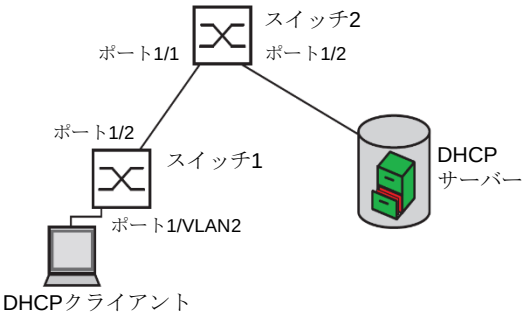


図66　DHCP レイヤー2 ネットワーク参考例

スイッチ1には以下の手順を実行します。

- ☐ *Advanced > DHCP L2 Relay > Configuration* ダイアログボックスの、*Interface* タブを開きます。
- ☐ ポート`1/1`には以下を設定します。
  - *Active* カラムのチェックボックスにチェックを入れます。
- ☐ ポート`1/2`には以下を設定します。
  - *Active* カラムのチェックボックスにチェックを入れます。
  - *Trusted port* カラムのチェックボックスにチェックを入れます。
- ☐ *Advanced > DHCP L2 Relay > Configuration* ダイアログボックスの*VLAN ID* タブを開きます。
- ☐ VLAN2には以下を設定します。
  - *Active* カラムのチェックボックスにチェックを入れます。
  - *Circuit ID* カラムのチェックボックスにチェックを入れます。
  - デバイスのIPアドレスを*Remote ID*として使用するには、*Remote ID type* カラムで値`ip`を指定します。
- ☐ 機能を有効化するには*Operation* フレームの`On` のラジオボタンを選択します。
- ☐ ボタンをクリックし、変更を一時的に保存します。

スイッチ2には以下の手順を実行します。

- ☐ *Advanced > DHCP L2 Relay > Configuration* ダイアログボックスの*Interface* タブを開きます。
- ☐ ポート`1/1`及び`1/2`には以下を設定します。
  - *Active* カラムのチェックボックスにチェックを入れます。
  - *Trusted port* カラムのチェックボックスにチェックを入れます。
- ☐ 機能を有効化するには*Operation* フレームの`On` のラジオボタンを選択します。
- ☐ ボタンをクリックし、変更を一時的に保存します。

VLAN2の存在を確認します。スイッチ1には以下の手順を実行します。

☐ VLAN2のコンフィグレーションを実行し、ポート`1/1` をVLAN2のメンバーとして指定します。

`enable`	Privileged Exec Modeに切り替えます。
`vlan database`	VLAN Configuration modeに切り替えます。
`dhcp-l2relay circuit-id 2`	VLAN`2`の回路ID及びDHCP Option 82をアクティベートします。
`dhcp-l2relay remote-id ip 2`	デバイスのIPアドレスをVLAN `2`のリモートIDとして指定します。

`dhcp-l2relay mode 2`	VLAN2の*DHCP L2 Relay* 機能をアクティベートします。
`exit`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`interface 1/1`	インターフェース1/1のInterface Configuration mode に変更します。
`dhcp-l2relay mode 2`	ポートの*DHCP L2 Relay* 機能をアクティベートします。
`exit`	Configuration modeに切り替えます。
`interface 1/2`	インターフェース1/2のInterface Configuration mode に変更します。
`dhcp-l2relay trust`	ポートを*Trusted port*と指定します。
`dhcp-l2relay mode 2`	ポートの*DHCP L2 Relay* 機能をアクティベートします。
`exit`	Configuration modeに切り替えます。
`dhcp-l2relay mode`	デバイス内の*DHCP L2 Relay* 機能を有効化します。

スイッチ2には以下の手順を実行します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`interface 1/1`	インターフェース1/1のInterface Configuration mode に変更します。
`dhcp-l2relay trust`	ポートを*Trusted port*と指定します。
`dhcp-l2relay mode 2`	ポートの*DHCP L2 Relay* 機能をアクティベートします。
`exit`	Configuration modeに切り替えます。
`interface 1/2`	インターフェース1/2のInterface Configuration mode に変更します。
`dhcp-l2relay trust`	ポートを*Trusted port*と指定します。
`dhcp-l2relay mode 2`	ポートの*DHCP L2 Relay* 機能をアクティベートします。
`exit`	Configuration modeに切り替えます。
`dhcp-l2relay mode`	デバイス内の*DHCP L2 Relay* 機能を有効化します。

15.3 デバイスをDNSクライアントとして使用する

DNS（Domain Name System）クライアントはDNSサーバーにクエリーを送り、ネットワークデバイスのホスト名やIPアドレスをリゾルブします。DNSクライアントは、まるで電話帳のようにデバイス名をIPアドレスに変換します。DNSクライアントが新規の名前をリゾルブする目的でリクエストを受信すると、DNSクライアントは最初に内部静的データベースにクエリーを送り、次に割当てたDNSサーバーに情報を送信します。DNSクライアントはクエリーされた情報を、将来のリクエストに備えてキャッシュに保存します。

当デバイスではDHCPサーバーからのDNSクライアントを、デバイス管理VLANを使用して設定することができます。また、ホスト名をIPアドレスに静的に割当てることもできます。

DNSクライアントは以下のユーザー機能を提供します。
- ドメイン名サーバーIPアドレス4つ分の空きのあるDNSサーバーリスト
- 静的ホスト名からのIPアドレスマッピング、静的ホスト64個分の空きスペース含む
- ホストキャッシュ、128エントリー分の空きスペース含む

15.3.1 DNSサーバーのコンフィグレーション例

DNSクライアントに名前を付け、ホスト名のリゾルブのためにDNSサーバーにクエリーを送信するよう設定します。以下の手順を実行します。

- ☐ *Advanced > DNS > Client > Static* ダイアログボックスを開きます。
- ☐ *Configuration* フレームの*Configuration source* フィールドで、値`user`を指定します。
- ☐ *Configuration* フレームの*Domain name* フィールドで、値`device1`を指定します。
- ☐ テーブルエントリーを追加するには、  ボタンをクリックします。
- ☐ *Address* カラムで、DNSサーバーのIPv4アドレスとして値`192.168.3.5` を指定します。また、有効なIPv6アドレスをDNSサーバーのIPアドレスとして指定することも可能です。
- ☐ *Active* カラムのチェックボックスにチェックを入れます。
- ☐ *Advanced > DNS > Client > Global* ダイアログボックスを開きます。
- ☐ 機能を有効化するには*Operation* フレームの*On* のラジオボタンを選択します。
- ☐  ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`dns client source user`	DNSクライアント設定をユーザーがマニュアルでコンフィグレーションを行うことを指定します。
`dns client domain-name devicel`	ストリング`device1` をデバイスの固有ドメイン名として指定します。
`dns client servers add 1 ip 192.168.3.5`	IPv4アドレスのDNSサーバーにインデックス`1`としてアドレス`192.168.3.5` を追加します。
`dns client servers add 2 ip 2001::1`	IPv6アドレスのDNSサーバーにインデックス`2`としてアドレス`2001::1` を追加します。
`dns client adminstate`	*DNS Client* 機能を全域で有効化します。

DNSクライアントがIPアドレスのある静的ホストをマッピングするよう設定します。以下の手順を実行します。

- ☐ *Advanced > DNS > Client > Static Hosts* ダイアログボックスを開きます。
- ☐ テーブルエントリーを追加するには、  ボタンをクリックします。
- ☐ *Name* カラムに値`example.com`を入力します。これはネットワーク内のデバイス名です。
- ☐ *IP address* カラムに、値`192.168.3.9`を指定します。
- ☐ *Active* カラムのチェックボックスにチェックを入れます。
- ☐  ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`dns client host add 1 name example.com ip 192.168.3.9`	`example.com` をIPアドレス`192.168.3.9`の静的ホストとして追加します。
`dns client adminstate`	*DNS Client* 機能を全域で有効化します。

15.4 GARP

GARP（Generic Attribute Registration Protocol）は、IEEEの規定する、スイッチがアトリビュートの値を登録・登録解除するための汎用フレームワークで、VLAN識別子やマルチキャストグループメンバーシップなどがその例として挙げられます。

参加者のアトリビュートが*GARP* 機能に従い登録・登録解除された場合、その参加者は特定のルールに沿って改修されます。参加者とは、到達可能なエンドステーションやネットワークデバイスを組合せたセットのことです。セットとして定義された参加者はそのアトリビュートと共に、ネットワークトポロジーのサブセット用の、一定時間内に到達可能なツリーです。デバイスは、データフレームを登録済みエンドステーションのみに転送します。ステーションの登録は、到達不能なエンドステーションにデータ送信を試行することを防ぐのに役立ちます。

15.4.1 GMRPのコンフィグレーション

GMRP（GARP Multicast Registration Protocol）とは、ネットワークデバイス及びエンドステーションにグループメンバーシップを動的に登録させる*GARP*（Generic Attribute Registration Protocol）のことです。デバイスは、同一LANセグメントに繋がっているデバイス類と共にグループメンバーシップ情報を登録します。*GARP*機能は、拡張フィルタリングサービスをサポートするネットワーク中のデバイスに情報を拡散することもできます。

注記：*GMRP*機能を有効化する前に、*MMRP*機能が無効であることを確認してください。

以下の例は、*GMRP*機能のコンフィグレーションを示したものです。当デバイスでは選択したポートに制限付きマルチキャストフラッディングを提供します。以下の手順を実行します。

- ☐ *Switching > GARP > GMRP* ダイアログボックスを開きます。
- ☐ ポートに制限付きマルチキャストフラッディングを実行するには、*GMRP active*カラムのチェックボックスにチェックを入れます。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`interface 1/1`	インターフェース`1/1`のInterface Configuration mode に変更します。
`garp gmrp operation`	ポートの*GMRP* 機能を有効にします。
`exit`	Configuration modeに切り替えます。
`garp gmrp operation`	全域で*GMRP* 機能を有効にします。

15.4.2 GVRPのコンフィグレーション

*GVRP*機能を使用して、デバイスが他の*GVRP*デバイスとVLANコンフィグレーション情報を交換できるようにします。これによって不要なブロードキャスト及び不明のユニキャストトラフィックを軽減します。*GVRP*機能はこの他にも、802.1Qトランクポートに接続されたデバイスのVLANを動的に作成し、管理します。

以下の例は、*GVRP* 機能のコンフィグレーションを示したものです。当デバイスでは他の*GVRP*デバイスとVLANコンフィグレーション情報を交換することができます。以下の手順を実行します。

- ☐ *Switching > GARP > GVRP* ダイアログボックスを開きます。
- ☐ *GVRP* デバイスを使用して、他の*GVRP*デバイスとVLANコンフィグレーション情報を交換するには、ポートの*GVRP active* カラムのチェックボックスにチェックを入れます。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`interface 3/1`	インターフェース`3/1`のInterface Configuration mode に変更します。
`garp gvrp operation`	ポートの*GVRP*機能を有効にします。
`exit`	Configuration modeに切り替えます。
`garp gvrp operation`	*GVRP* 機能を全域で有効化します。

15.5 MRP-IEEE

IEEE 802.1Qの修正版であるIEEE 802.1akでは、MRP（Multiple Registration Protocol）を*GARP*（Generic Attribute Registration Protocol）の代替としています。IEEEは更に、*GARP*アプリケーション、*GMRP*（Multicast Registration Protocol）及び*GVRP*（*GARP* VLAN Registration Protocol）、並びに*MMRP*（Multiple MAC Registration Protocol）及び*MVRP*（Multiple VLAN Registration Protocol）を修正し、置換えています。

要求されるネットワークエリア内にトラフィックを制限するため、MRPアプリケーションはLAN全体のMRPが有効なデバイスにアトリビュートの値を拡散します。MRPアプリケーションはマルチキャストグループメンバーシップ及びVLAN識別子の登録・登録解除を行います。

注記：MRP（Multiple Registration Protocol）にはループフリーネットワークが必要です。ネットワークにループが出来ないようにするには、メディア冗長プロトコル、スパニングツリープロトコル、MRPの有効なラピッドスパニングツリープロトコル等のネットワークプロトコルを使用します。

15.5.1 MRPオペレーション

各参加者にはアプリカントコンポーネント及びMAD（MRP Attribute Declaration）コンポーネントが含まれます。アプリカントコンポーネントは、アトリビュートの値の形成及びそれらの登録・登録解除の責任を負います。MADコンポーネントは、他の参加者から受信したメッセージの伝送及び処理のためのMRPメッセージを作成します。MADコンポーネントはMRPDU（MRPデータユニット）内の他の参加者へ向けてエンコードしたアトリビュートを伝送します。スイッチ内では、MAP（MRP Attribute Propagation）コンポーネントが参加ポートにアトリビュートを分配します。

各MRPアプリケーション及び各LANポートには参加者がいます。例えば、エンドデバイスに参加者アプリケーションが存在し、スイッチポートには別のアプリケーションが存在します。アプリカント・ステートマシン（Applicant state machine）は、各MRP参加者のアトリビュート及びエンドデバイス又はスイッチでの宣言（Declaration）のポートを記録します。アプリカント・ステートマシンの変数の変更は、MRPDUが宣言（Declaration）又は解除（Withdrawal）の通信をするトリガーとなります。

*MMRP*インスタンスを確立するには、エンドデバイスは最初にJoin empty（JoinMt）メッセージを適切なアトリビュートで送信します。次に、スイッチが参加ポート及び近隣スイッチにJoinMtのフラッディングを行います。近隣スイッチはメッセージを自身の参加ポートに、更にその先へとフラッディングすることで、グループトラフィックにパスが確立されます。

15.5.2 MRPタイマー

デフォルトのタイマー設定により、アトリビュートの不要な宣言や解除を防止することができます。タイマー設定により、参加者はLeave又はLeaveAllタイマーが経過する前にMRPメッセージを受信し、処理することができます。

タイマーを設定する時、以下の相関関係を守ります。

- Leave又はLeaveAllイベント後の再登録をするには、メッセージが多くとも、LeaveTimeの値を次の通りに設定します。≧(2x JoinTime) + 60 （1/100秒内で）
- LeaveAll後に生成されたトラフィックに合流する量を最小化するには、LeaveAllタイマーの値をLeaveTimeの値より大きく指定します。

以下リストに、デバイスが伝送する各種MRPイベントを示します。
- Join：次のJoinメッセージ伝送までの間隔を制御します。
- Leave：スイッチがLeave状態がWithdraw状態に変更されるまでの間、スイッチがLeave状態で待機する時間を制御します。
- LeaveAll：スイッチがLeaveAllメッセージを生成する頻度を制御します。

タイマーが経過すると、周期タイマーはスイッチがLAN上の参加者に送信するJoinリクエストMRPメッセージを開始します。スイッチはこのメッセージを使用して不要な解除を防止します。

15.5.3 MMRP

デバイスはブロードキャスト、マルチキャスト又は不明なトラフィックをポートで受信すると、デバイスは他のポートにトラフィックのフラッディングを実行します。このプロセスは、LAN上の帯域幅を無駄に使用する原因となります。

MMRP（Multiple MAC Registration Protocol）では、トラフィックのフラッディングをLAN上の参加者にアトリビュートの宣言を分配することで制御できます。MADコンポーネントがMRPメッセージとしてエンコードし、LANに伝送するアトリビュートの値は、48ビットMACアドレスのグループサービスの要件情報です。

スイッチはアトリビュートをMACアドレス登録エントリーとしてフィルタリングデータベースに保存します。転送プロセスでは、フィルタリングデータベースエントリーを、グループメンバーLANに到達する必要のあるポートを通して伝送するためだけに使用します。

スイッチはパケットをアクティブなポートで受信し、グループメンバーのポートにのみ転送するという、Open Host Groupコンセプトを基にしてグループ配分のメカニズムを促します。この方法によって、特定のグループ又は複数グループにパケットの伝送を要求するあらゆる*MMRP*参加者は、グループメンバー加入をリクエストします。MACサービスユーザーはLAN上のどこからでも特定グループにパケットを送信することができます。グループは、登録された*MMRP*参加者と繋がったLANでこれらパケットを受信します。*MMRP*及びMACアドレス登録エントリーは、このように要求されるループフリーLANのセグメントへのパケットを制限しています。

登録・登録解除の状態及びトラフィックの受信を維持するため、ポートは定期的に関心があることを示します。LAN上の*MMRP*機能が有効な全デバイスは、フィルタリングデータベースを維持し、これをグループのMACアドレスのトラフィックがリストされた参加者に転送します。

MMRP参考例

ここの例では、ホストAはグループG1宛てのトラフィックをリッスンする意図があります。スイッチAは、ホストAから受信した*MMRP* Joinリクエストを処理し、両近隣スイッチにこのリクエストを送信します。LAN上のデバイスはこれで、グループG1宛てのトラフィックの受信に関心のあるホストがいることを認識することができます。ホストBがグループG1宛てのデータ伝送を開始すると、登録用のパスにデータが流れ、ホストAがそれを受信します。

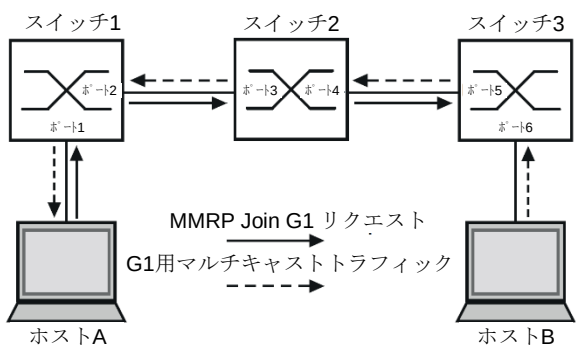


図67　MACアドレス登録用MMRPネットワーク

スイッチに*MMRP*機能を有効化します。以下の手順を実行します。

- ☐ *Switching > MRP-IEEE > MMRP* ダイアログの*Configuration* タブを開きます。
- ☐ ポート1 及びポート2 を*MMRP*参加者としてアクティベートするには、スイッチ1のポート1 及びポート2 の*MMRP*カラムのチェックボックスにチェックを入れます。
- ☐ ポート3及びポート4を*MMRP*参加者としてアクティベートするには、スイッチ2のポート3 及びポート4の*MMRP*カラムのチェックボックスにチェックを入れます。
- ☐ ポート5及びポート6を*MMRP*参加者としてアクティベートするには、スイッチ3のポート5 及びポート6の*MMRP*カラムのチェックボックスにチェックを入れます。
- ☐ 定期イベントを送信してデバイスにMACアドレスグループの登録を維持させるには、*Periodic state machine*を有効化します。*Configuration* フレームで、*On* ラジオボタンを選択します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

スイッチ1の*MMRP*ポートを有効にするには、以下のコマンドを使用します。コマンドのインターフェース部は該当するものと入れ替え、スイッチ2及び3のポートの*MMRP*機能を有効化します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`interface 1/1`	インターフェース1/1のInterface Configuration mode に変更します。
`mrp-ieee mmrp operation`	ポートの*MMRP* 機能を有効にします。
`interface 1/2`	インターフェース1/2のInterface Configuration mode に変更します。
`mrp-ieee mmrp operation`	ポートの*MMRP* 機能を有効にします。
`exit`	Configuration modeに切り替えます。
`mrp-ieee mrp periodic-state-machine`	全域で*Periodic state machine* 機能を有効にします。
`mrp-ieee mmrp operation`	全域で*MMRP* 機能を有効にします。

15.5.4 MVRP

MVRP（Multiple VLAN Registration Protocol：マルチVLAN登録プロトコル）とは、LAN上の動的VLAN登録及び解除を提供するMRPアプリケーションです。

*MVRP*機能は動的VLAN登録エントリーの保守メカニズムを提供するもので、他デバイスに情報を伝送します。この情報は、*MVRP*を認識したデバイスに、VLANの確立及びメンバーシップ情報のアップデートをさせるものです。VLANにメンバーが存在している場合、この情報には、スイッチがこれらメンバーに到達するのにどのポートにトラフィックを転送するかが含まれます。

*MVRP*機能の主な目的は、ユーザーがマニュアルでセットアップした以外のVLAN情報をスイッチに探索させるためです。この情報を発見することで、スイッチは、帯域幅の消費やVLANネットワークでの多くのコンバージェンス時間といった制限を克服することができます。

MVRP参考例

MVRPを認識するスイッチ（1~4）を、エンドデバイスグループA1、A2、B1、B2及び別途2つのVLANにスイッチA、Bのあるリングトポロジーに接続し、ネットワークを構築します。スイッチはSTPが有効で、スイッチ1から4に接続したポートはディスカード状態にあり、ループが出来ることを防ぎます。

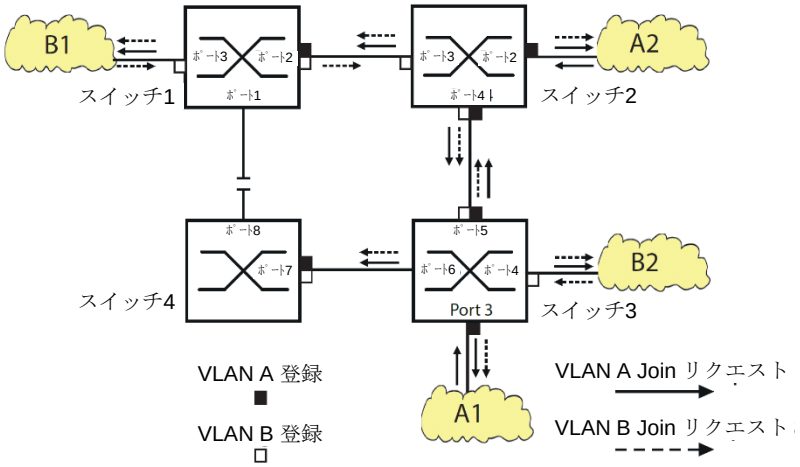


図68　VLAN登録用MVRP ネットワーク参考例

このMVRPネットワーク参考例では、最初にLANはスイッチにJoinリクエストを送信します。スイッチは、フレームを受信するポート用の転送データベースにVLAN登録を入力します。

すると、スイッチはリクエストを他ポートに拡散し、近隣LANや数一致にリクエストを送信します。このプロセスは、スイッチが受信ポートの転送データベースにVLANを登録するまで継続します。

スイッチのMVRPを有効にします。以下の手順を実行します。

- ☐ *Switching > MRP-IEEE > MVRP* ダイアログの*Configuration* タブを開きます。
- ☐ ポート1から3までを*MVRP*参加者としてアクティベートするには、スイッチ1のポート1から3までの*MVRP*カラムのチェックボックスにチェックを入れます。
- ☐ ポート2から4までを*MVRP*参加者としてアクティベートするには、スイッチ2のポート2から4 までの*MVRP*カラムのチェックボックスにチェックを入れます。
- ☐ ポート3から6までを*MVRP*参加者としてアクティベートするには、スイッチ3のポート3から6までの*MVRP*カラムのチェックボックスにチェックを入れます。
- ☐ ポート7及びポート8を*MVRP* 参加者としてアクティベートするには、スイッチ4のポート7及びポート8の*MMRP*カラムのチェックボックスにチェックを入れます。
- ☐ VLANの登録を維持するには、*Periodic state machine*を有効にします。*Configuration* フレームで、*On* ラジオボタンを選択します。
- ☐ 機能を有効化するには*Operation* フレームの*On* のラジオボタンを選択します。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

スイッチ１の*MVRP* ポートを有効にするには、以下のコマンドを使用します。コマンドのインターフェース部は該当するものと入れ替え、スイッチ2、3、4のポートの*MVRP* 機能を有効化します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`interface 1/1`	インターフェース`1/1`のInterface Configuration mode に変更します。

`mrp-ieee mvrp operation`	ポートの*MVRP* 機能を有効にします。
`interface 1/2`	インターフェース`1/2`のInterface Configuration mode に変更します。
`mrp-ieee mvrp operation`	ポートの*MVRP* 機能を有効にします。
`exit`	Configuration modeに切り替えます。
`mrp-ieee mvrp periodic-state-machine`	全域で*Periodic state machine* 機能を有効にします。
`mrp-ieee mvrp operation`	全域で*MVRP* 機能を有効にします。

16 産業用プロトコル

16.1 IEC 61850/MMS

IEC 61850/MMSは産業通信用プロトコルで、IEC（International Electrotechnical Commission：国際電気標準会議）によって標準化されています。このプロトコルは変電所のオートメーション、例えば電力サプライヤーの制御技術などで利用されています。

パケットを重視したこのプロトコルは、TCP/IPトランスポートプロトコルをベースとし、MMS（Manufacturing Messaging Specification）をクライアント/サーバー通信に使用します。このプロトコルはオブジェクト重視であり、標準化された設定言語を定義し、その一部としてネットワーク制御技術にSCADA、IED（Intelligent Electronic Devices）等が含まれます。

IEC 61850の第6部には、SCL（Substation Configuration Language：変電所構成言語）が定義されています。SCLはデバイスのプロパティ及びシステム構造を、自動処理可能な形で表現したものです。SCLで書かれたデバイスプロパティは、デバイスのICDファイル内に保存されています。

16.1.1 IEC 61850のスイッチモデル

IEC 61850 90-4の技術レポートでは、ブリッジモデルについて指定されています。ブリッジモデルはスイッチの機能を、IED（Intelligent Electronic Device：インテリジェント電子装置）のオブジェクトとして表しています。MMSクライアント（例えば制御室のソフトウェアとして）は、これらオブジェクトをデバイスの監視及びコンフィグレーションに使用します。

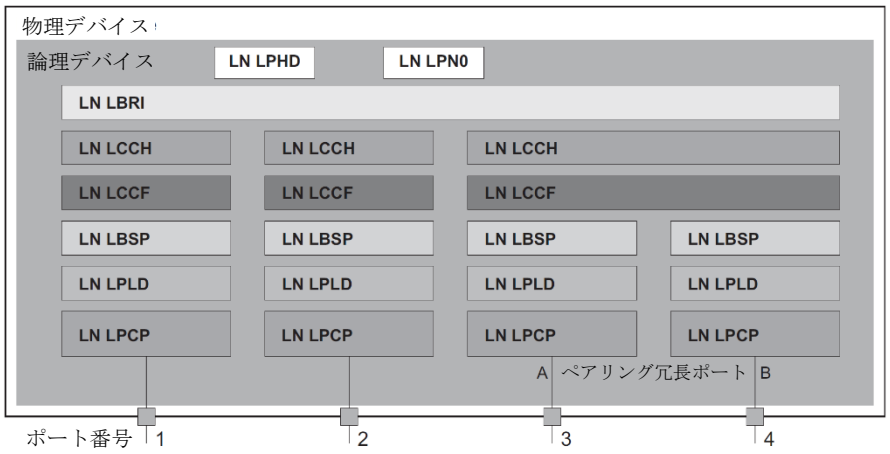


図69　IEC 61850 90-4技術レポートをベースとしたブリッジモデル

表52　TR IEC61850 90-4をベースとしたブリッジモデルのクラス

クラス	概要
LN LLN0	Bridge IEDのZero 論理ノード： デバイスの論理プロパティを定義。
LN LPHD	Bridge IEDのPhysical Device 論理ノード：デバイスの物理プロパティを定義。
LN LBRI	Bridge 論理ノード： デバイスのブリッジ機能の一般設定を示したもの。
LN LCCH	Communication Channel 論理ノード： 1つ以上の物理デバイスポートで構成する論理Communication Channel を定義。
LN LCCF	Channel Communication Filtering 論理ノード： 高位レベルのCommunication Channel用のVLAN及びマルチキャスト設定を定義。
LN LBSP	Port Spanning Tree Protocol 論理ノード： 個別の物理デバイスポート用の、スパニングツリーのステータス及び設定を定義。
LN LPLD	Port Layer Discovery 論理ノード： 個別の物理デバイスポート用の、LLDP のステータス及び設定を定義。
LN LPCP	Physical Communication Port 論理ノード：個別の物理デバイスポートを示す。

16.1.2　制御システムへの統合

デバイスの準備

以下の手順を実行します。

- ☐ デバイスにIPアドレスが割当てられていることを確認します。
- ☐ *Advanced > Industrial Protocols > IEC61850-MMS* ダイアログボックスを開きます。
- ☐ MMSサーバーを開始するには、*Operation* フレームで、*On* ラジオボタンを選択し、☑ボタンをクリックします。後に、MMSクライアントはデバイスに接続し、ブリッジモデルで定義したオブジェクトの読出し・監視が可能となります。

IEC 61850/MMSには、認証メカニズムはありません。IEC 61850/MMSの書込みアクセスがアクティベートされると、TCP/IPを使用してデバイスにアクセス可能なクライアントは、デバイス設定を変更することができます。その反面、デバイスに誤った設定をするとネットワークに障害が起きることとなります。

注記
デバイスへの未認証アクセスの危険性 追加の対策（ファイヤーウォール、VPN等）を取った場合、書込みアクセスのみをアクティベートし、未認証アクセスの可能性を低減させてください。 **この指示に従わない場合、装置の損傷を招くおそれがあります。**

☐ MMSクライアントに設定変更を許可するには、*Write access* チェックボックスにチェックを入れ、☑ ボタンをクリックします。

オフラインでのコンフィグレーション

当デバイスでは、グラフィカルユーザーインターフェースを使用してICDファイルをダウンロードすることができます。このファイルには、SCLで書かれたデバイスプロパティが含まれ、デバイスに直接接続することなく変電所のコンフィグレーションを実行することができます。

☐ *Advanced > Industrial Protocols > IEC61850-MMS* ダイアログボックスを開きます。

☐ ICDファイルをPCにロードするには、☰ に続き、*Download* 項目をクリックします。

デバイスの監視

デバイスにIEC61850/MMSサーバーが統合されていれば、RCB（Report Control Block）を利用してデバイスの複数ステータスを監視することができます。最大5つのMMSクライアントが同時にReport Control Blockに登録することができます。

当デバイスでは以下の機能を監視することができます。

表53　IEC 61850/MMS で監視可能なデバイスステータス

クラス	RCBオブジェ	概要
LN LPHD	TmpAlm	デバイスで測定した温度が設定温度の閾値を上回る（下回る）と、ステータスが変わります。
	PhyHealth	LPHD.TmpAlm RCBオブジェクトのステータスが変わると、ステータスが変わります。
LN LPHD	TmpAlm	デバイスで測定した温度が設定温度の閾値を上回る（下回る）と、ステータスが変わります。
	PwrSupAlm	冗長電源の1つが落ちる又は再始動した場合、ステータスが変わります。
	PhyHealth	LPHD.PwrSupAlm 又はLPHD.TmpAlm RCBオブジェクトのステータスが変わると、ステータスが変わります。

表53　IEC 61850/MMS で監視可能なデバイスステータス（続き）

クラス	RCBオブジェクト	概要
LN LBRI	RstpRoot	デバイスがルートブリッジのロールを引き継ぐ又は放棄した時に、ステータスが変わります。
	RstpTopoCnt	ルートブリッジの変更によりトポロジーが変わると、ステータスが変わります。
LN LCCH	ChLiv	物理ポートのリンクステータスが変わると、ステータスが変わります。
LN LPCP	PhyHealth	物理ポートのリンクステータスが変わると、ステータスが変わります。

16.2 Modbus TCP

Modbus TCP とは、クライアント及びイーサネットTCP/IPネットワーク間のクライアント/サーバー通信のためのアプリケーション層メッセージングプロトコルです。

Modbus TCP 機能により、既に*Modbus TCP* を使用しているネットワークにデバイスをインストールすることができ、デバイスに保存されたレジスターを読み出すことができます。

16.2.1 クライアント/サーバーModbus TCP/IP モード

当デバイスは、Modbus TCP/IPのクライアント/サーバーモデルをサポートします。当デバイスはこの配置でサーバーとして作動し、レジスターに保存した情報に関するクライアントのリクエストに返答します。

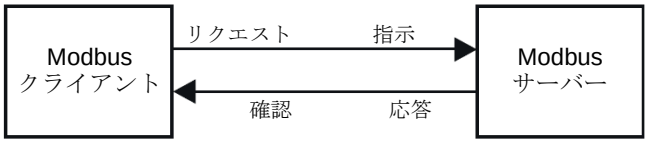


図70 クライアント/サーバー Modbus TCP/IP モード

クライアント/サーバーモデルは4種類のメッセージをクライアントとサーバー間で交換します。

- Modbus TCP/IP Request（リクエスト）：クライアントが情報のリクエストを作成し、サーバーに送信します。
- Modbus TCP/IP Indication（指示）：サーバーは、クライアントが情報を要求する指示としてリクエストを受信します。
- Modbus TCP/IP Response（応答）：要求された情報が有用であれば、サーバーは要求された情報を含む返答を送信します。要求された情報が無い場合、サーバーはException Response（例外応答）を送信し、処理中のエラーについてクライアントに通知します。例外応答は検知したエラーの原因を示す例外コードが含まれます。
- Modbus TCP/IP Confirmation（確認）：クライアントはサーバーからの、リクエスト情報を含んだ応答を受信します。

16.2.2 機能サポート及びメモリーマッピング

当デバイスは、パブリックコード0x03 （Read Holding Registers：保持レジスターの読出し）及び0x05 （Write Single Coil：シングルコイル書込み）の機能をサポートします。これらコードにより、システム名を含むシステム情報、システム位置、ソフトウェアバージョン、IPアドレス、MACアドレス等のレジスターに保存された情報を読み出すことができます。また、ポート情報及びポート統計情報を読み出す事もできます。0x05 コードでは、ポートカウンターを個別又は全域でリセットすることができます。

以下のリストには、Format カラムに入力した値の定義が含まれます。

- Bitmap: 2つのレジスターに保存されたビッグエンディアンのバイトオーダーでエンコードされた32ビットのグループです。ビッグエンディアンシステムは、最小のアドレス内ワードの最も重要なバイト部を保存し、最大のアドレスの最も重要でないバイトも保存します。
- F1:16ビットの未署名整数
- F2:エニュメレーション、電源アラーム
  - 0 = 電源良好
  - 1 = 電源喪失検知
- F3:エニュメレーション、OFF/ON
  - 0 = Off
  - 1 = On

- F4:エニュメレーション、ポート種別
  - 0 = Giga：Gigabit Interface Converter (GBIC)
  - 1 = 銅線：ツイストペアケーブル（TP）
  - 2 = 光ファイバー、10 Mb/s
  - 3 = 光ファイバー、100 Mb/s
  - 4 = Giga：10/100/1000 Mb/s （3倍速）
  - 5 = Giga：銅線、 1000 Mb/s TP
  - 6 = Giga：SFP（Small Form-factor Pluggable）
- F9:32ビット未署名、ロング
- String：オクテット、順に保存、レジスター当たり2オクテット

Modbus TCP/IP コード

クライアントにポートカウンターをリセットさせ、デバイスレジスターから特定の情報を読み出させることのできるアドレスを下表に示します。

ポート情報

表54　ポート情報

アドレス	数量	ディスクリプション	Min	Max	Step	単位	フォーマット
0400	1	Port 1 Type	0	6	1	-	F4
0401	1	Port 2 Type	0	6	1	-	F4
		...					
043F	1	Port 64 Type	0	6	1	-	F4
0440	1	Port 1 Link Status	0	1	1	-	F1
0441	1	Port 2 Link Status	0	1	1	-	F1
		...					
047F	1	Port 64 Link Status	0	1	1	-	F1
0480	1	Port 1 STP State	0	1	1	-	F1
0481	1	Port 2 STP State	0	1	1	-	F1
		...					
04BF	1	Port 64 STP State	0	1	1	-	F1
04C0	1	Port 1 Activity	0	1	1	-	F1
04C1	1	Port 2 Activity	0	1	1	-	F1
		...					
04FF	1	Port 64 Activity	0	1	1	-	F1
0500	1	Port 1 Counter Reset	0	1	1	-	F1
0501	1	Port 2 Counter Reset	0	1	1	-	F1
		...					
053F	1	Port 64 Counter Reset	0	1	1	-	F1

ポート統計情報

表55　ポート統計情報

アドレス	数量	ディスクリプション	Min	Max	Step	単位	フォーマット
0800	1	Port1 - Number of bytes received	0	4294967295	1	-	F9
0802	1	Port1 - Number of bytes sent	0	4294967295	1	-	F9
0804	1	Port1 - Number of frames received	0	4294967295	1	-	F9
0806	1	Port1 - Number of frames sent	0	4294967295	1	-	F9
0808	1	Port1 - Total bytes received	0	4294967295	1	-	F9
080A	1	Port1 - Total frames received	0	4294967295	1	-	F9
080C	1	Port1 - Number of broadcast frames received	0	4294967295	1	-	F9
080E	1	Port1 - Number of multicast frames received	0	4294967295	1	-	F9
0810	1	Port1 - Number of frames with CRC error	0	4294967295	1	-	F9
0812	1	Port1 - Number of oversized frames received	0	4294967295	1	-	F9
0814	1	Port1 - Number of bad fragments rcvd(<64 bytes)	0	4294967295	1	-	F9
0816	1	Port1 - Number of jabber frames received	0	4294967295	1	-	F9
0818	1	Port1 - Number of collisions occurred	0	4294967295	1	-	F9
081A	1	Port1 - Number of late collisions occurred	0	4294967295	1	-	F9
081C	1	Port1 - Number of 64-byte frames rcvd/sent	0	4294967295	1	-	F9
081E	1	Port1 - Number of 65-127 byte frames rcvd/sent	0	4294967295	1	-	F9
0820	1	Port1 - Number of 128-255 byte frames rcvd/sent	0	4294967295	1	-	F9
0822	1	Port1 - Number of 256-511 byte frames rcvd/sent	0	4294967295	1	-	F9
0824	1	Port1 - Number of 512-1023 byte frames rcvd/sent	0	4294967295	1	-	F9
0826	1	Port1 - Number of 1023-MAX byte frames rcvd/sent	0	4294967295	1	-	F9
0828	1	Port1 - Number of Mac Error Packets	0	4294967295	1	-	F9
082A	1	Port1 - Number of dropped received packets	0	4294967295	1	-	F9
082C	1	Port1 - Number of multicast frames sent	0	4294967295	1	-	F9
082E	1	Port1 - Number of broadcast frames sent	0	4294967295	1	-	F9
0830	1	Port1 - Number of <64 byte fragments w/ good CRC	0	4294967295	1	-	F9
		...					
147E	1	Port64 - Number of <64 byte fragments w/ good CRC	0	4294967295	1	-	F9

16.2.3 コンフィグレーション例

ここの例では、デバイスがクライアントリクエストに応答するよう設定します。このコンフィグレーションの条件として、クライアントデバイスに、特定範囲内でIPアドレスが設定されていなければなりません。*Write access* 機能はここの例では非アクティブのままとします。*Write access* 機能をアクティベートすると、ポートカウンターのみをリセットすることができます。デフォルトのコンフィグレーションでは、*Modbus TCP* 及び*Write access* 機能は非アクティブになっています。

Modbus TCP プロトコルには、認証メカニズムはありません。*Modbus TCP* の書込みアクセスがアクティベートされると、TCP/IPを使用してデバイスにアクセス可能なクライアントは、デバイス設定を変更することができます。その反面、デバイスに誤った設定をするとネットワークに障害が起きることとなります。

注記
デバイスへの未認証アクセスの危険性 追加の対策（ファイヤーウォール、VPN等）を取った場合、書込みアクセスのみをアクティベートし、未認証アクセスの可能性を低減させてください。 **この指示に従わない場合、装置の損傷を招くおそれがあります。**

以下の手順を実行します。

- ☐ *Device Security > Management Access > IP Access Restriction* ダイアログボックスを開きます。
- ☐ テーブルエントリーを追加するには、  ボタンをクリックします。
- ☐ *Index* カラムの値が2の行で、IPアドレスの範囲を指定します。以下の値を入力します。
  - *Address* カラム：`10.17.1.0`
  - *Netmask* カラム：`255.255.255.248`
- ☐ *Modbus TCP* カラムのチェックボックスにチェックが入っていることを確認します。
- ☐ IPアドレス範囲をアクティベートします。*Active* カラムのチェックボックスにチェックを入れます。
- ☐  ボタンをクリックし、変更を一時的に保存します。
- ☐ *Diagnostics > Status Configuration > Security Status* ダイアログボックスの*Global* タブを開きます。
- ☐ *Modbus TCP active* に関連するパラメーターのチェックボックスにチェックが入っていることを確認します。
- ☐ *Advanced > Industrial Protocols > Modbus TCP* ダイアログボックスを開きます。
- ☐ 標準の*Modbus TCP* リスニングポートでは、ポート`502`がデフォルトです。但し、他のTCPポートをリッスンした場合は、*TCP port* フィールドにリスニングポートの値を入力します。
- ☐ 機能を有効化するには*Operation* フレームの`On` のラジオボタンを選択します。
- ☐  ボタンをクリックし、変更を一時的に保存します。

Modbus TCP 機能を有効にすると、*Security Status* 機能がアクティベーションを検知して*Basic Settings > System* ダイアログボックスの*Security status* フレームにアラームを表示します。

`enable`	Privileged Exec Modeに切り替えます。
`network management access add 2`	ネットワークのアドレス範囲のエントリーを作成します。 ここの例では、次に有用なインデックスは `2` となります。
`network management access modify 2 ip 10.17.1.0`	IPアドレスを指定します。

```
network management access modify 2 mask 29
```
ネットマスクを指定します。

```
network management access modify 2 modbus-tcp enable
```
デバイスが*Modbus TCP* にデバイス管理へのアクセスを許可することを指定します。

```
network management access operation
```
IPアクセス制限を有効化します。

```
configure
```
Configuration modeに切り替えます。

```
security-status monitor modbus-tcp- enabled
```
デバイスが*Modbus TCP* サーバーのアクティベーションを監視することを指定します。

```
modbus-tcp operation
```
Modbus TCP サーバーをアクティベートします。

```
modbus-tcp port <1..65535>
```
*Modbus TCP*通信のTCPポートを指定します（任意）。デフォルト値のポートは、502です。

```
show modbus-tcp
```
Modbus TCP サーバー設定を表示します。

```
Modbus TCP/IP server settings
-------------------------
Modbus TCP/IP server operation.....enabled Write-access.....disabled
Listening port. ..... 502
Max number of sessions. ..... 5
Active sessions. ..... 0
```

```
show security-status monitor
```
セキュリティステータスを表示します。

```
Device Security Settings Monitor
--------------------------------
Password default settings unchanged...........monitored
...
Write access using Ethernet Switch Configurator is possible....monitored Loading unencrypted configuration from ENVM...monitored
IEC 61850 MMS is enabled.....monitored
Modbus TCP/IP server active.....monitored
```

```
show security-status event
```
発生したセキュリティステータスイベントを表示します。

```
Time stamp           Event                    Info
-------------------  -----------------------  ------
2014-01-01 01:00:39  password-change(10)        -
.................................................
2014-01-01 01:00:39  ext-nvm-load-unsecure(21)   -
2014-01-01 23:47:40  modbus-tcp-enabled(23)     -
```

```
show network management access rules 1
```
インデックス1の管理アクセスルールの制限を表示します。

```
Restricted management access settings
-------------------------------------
Index. ..... 1
IP Address. .....10.17.1.0
Prefix Length. ..... 29
HTTP.....yes
SNMP.....yes
Telnet.....yes
SSH.....yes
HTTPS.....yes
IEC61850-MMS.....yes
Modbus TCP/IP.....yes
Active.....[x]
```

16.3 EtherNet/IP

EtherNet/IP は全世界で認められた標準化された産業通信プロトコルで、ODVA（Open DeviceNet Vendor Association）によって維持されています。プロトコルは広く使用されている標準イーサネットトランスポートプロトコルであるTCP/IP及びUDP/IPをベースとしています。*EtherNet/IP* は大手メーカーによって支えられていて、産業セクターでの効果的なデータ通信の大きな基盤となっています。

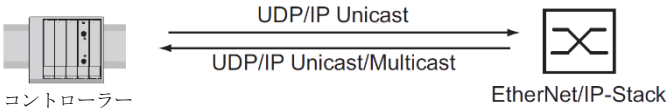


図71 EtherNet/IP ネットワーク

EtherNet/IP は、産業用プロトコルCIP（Common Industrial Protocol）を、標準イーサネットプロトコルに追加します。*EtherNet/IP* はセッション層以上の層にCIPを実装し、トランスポート層以下の層には特定の*EtherNet/IP* 技術にCIPを適応させます。オートメーション用アプリケーションでは、*EtherNet/IP* はCIPをアプリケーションレベルに実装します。したがって、*EtherNet/IP* は産業制御技術セクターに理想的といえます。

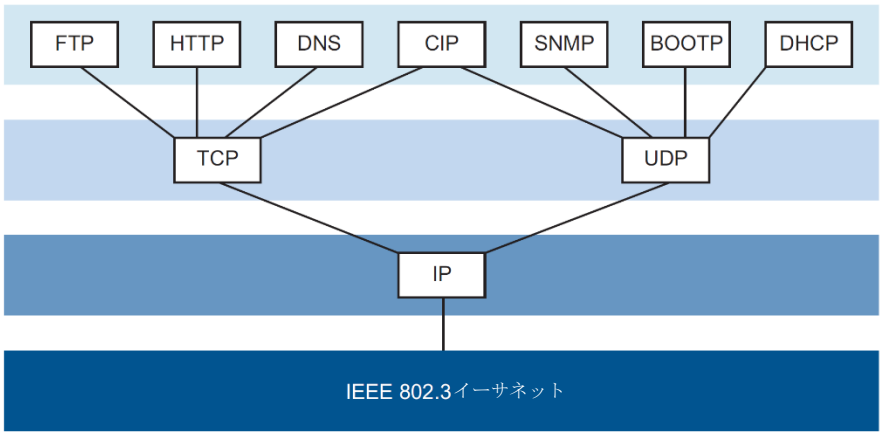


図72 IEEE802.3 EtherNet/IP

*EtherNet/IP*の詳細については、右記ODVAウェブサイトを参照。www.odva.org

16.3.1 制御システムへの統合

以下の手順を実行します。

- ☐ *Switching > IGMP Snooping > Global* ダイアログボックスを開きます。*IGMP Snooping* 機能が有効であることを確認します。
- ☐ *Advanced > Industrial Protocols > EtherNet/IP* ダイアログボックスを開きます。*EtherNet/IP* 機能が有効であることを確認します。
- ☐ *Advanced > Industrial Protocols > EtherNet/IP* ダイアログボックスを開きます。
- ☐ EDSをzipアーカイブとしてPCに保存するには、*Download*をクリックします。
  zipアーカイブには*EtherNet/IP* のコンフィグレーションファイル及びデバイスへ接続するコントローラーのコンフィグレーションに使用するアイコンが含まれます。

16.3.2 EtherNet/IP エンティティパラメーター

以下の章では、デバイスがサポートするオブジェクト及びオペレーションについて記載します。

サポート対象のオペレーション

表56　サポートされるオブジェクトインスタンスのEtherNet/IPリクエスト概要

サービスコード	アイデンティティオブジェクト	TCP/IPインターフェースオブジェクト	イーサネットリンクオブジェクト	スイッチエージェントオブジェクト	ベーススイッチオブジェクト
0x01 Get Attribute All	全アトリビュート	全アトリビュート	全アトリビュート	全アトリビュート	全アトリビュート
0x02 Set Attribute All	–	設定可アトリビュート (0x3, 0x5, 0x6, 0x8, 0x9, 0xA)	設定可アトリビュート (0x6, 0x9)	–	–
0x0e Get Attribute Single	全アトリビュート	全アトリビュート	全アトリビュート	全アトリビュート	全アトリビュート
0x10 Set Attribute Single	–	設定可アトリビュート (0x3, 0x5, 0x6, 0x8, 0x9, 0xA, 0x64)	設定可アトリビュート (0x6, 0x9, 0x65, 0x67, 0x68, 0x69, 0x6C)	設定可アトリビュート (0x5, 0x7)	–
0x05 Reset	パラメーター (0x0, 0x1)	–	–	–	–
0x35 Save Configuration Vendor specific	–	–	–	Saveスイッチコンフィグレーション	–
0x36 Mac Filter Vendor specific	–	–	–	MACフィルター追加 STRUCT of: USINT VlanId ARRAY of 6 USINT Mac DWORD PortMask	–

アイデンティティオブジェクト

当デバイスは、*EtherNet/IP*のアイデンティティオブジェクト（Class Code 0x01）をサポートします。シュナイダーエレクトリック製造IDは634です。シュナイダーエレクトリックでは、製品「マネージドサービスイーサネットスイッチ（Managed Ethernet Switch）」を、ID「44（0x2C）」としています。

表57　インスタンスアトリビュート（インスタンス1のみ可能）

Id	アトリビュート	アクセスルール	データ種別	備考
0x1	Vendor ID	Get	UINT	Schneider Electric634
0x2	Device Type	Get	UINT	Managed Ethernet Switch 44 (0x2C) (0x2C)
0x3	Product Code	Get	UINT	製品コード：各種デバイス毎にマッピングを定義
0x4	Revision	Get	STRUCT of: USINT Major USINT Minor	EtherNet/IP implementation 2.1の修正版
0x5	Status	Get	WORD	以下Bitステータスのみサポート： 0: Owned （常時1） 2: Configured （常時1） 4: Extend Device Status 5: 0x3:I/O未接続 6: 0x7:少なくとも1つのI/O接続済み 全てidleモード 7:
0x6	Serial number	Get	UDINT	デバイスのシリアル番号（MACアドレスの最後の3バイトを含む）
0x7	Product name	Get	SHORT-STRING	表示が、Schneider Electric + 製品グループ（product family） + 製品ID（product ID） + ソフトウェアバリアント（software variant）

TCP/IPインターフェースオブジェクト

当デバイスは*EtherNet/ IP*の、TCP/IPインターフェースオブジェクト（クラスコード0xF5）のインスタンス1のみサポートします。

書込みアクセスステータスによっては、デバイスは自身のフラッシュメモリにコンフィグレーション全てを保存します。コンフィグレーションファイルの保存には最大10秒ほどかかります。電源の喪失等の原因で保存プロセスが中断されると、以降デバイスのオペレーションができなくなる可能性があります。

注記：当デバイスはコンフィグレーション変更の`Get Request` に対し、コンフィグレーションの保存が不完全であっても`Response` で応答します。

表58　クラスのアトリビュート

Id	アトリビュート	アクセスルール	データ種別	備考
0x1	Vendor ID	Get	UINT	当オブジェクトの修正：3
0x2	Device Type	Get	UINT	インスタンス番号最大：1
0x3	Product Code	Get	UINT	現在まで作成したオブジェクトインスタンス数：1

表59　インスタンス1のアトリビュート

Id	アトリビュート	アクセスルール	データ種別	備考
0x1	Status	Get	DWORD	0: インターフェースステータス（0=インターフェースコンフィグレーションされていない、1=インターフェースに有効なコンフィグ含む） 6: ACDステータス（デフォルト0） 7: ACDフォルト（デフォルト0）
0x2	Interface Capability flags	Get	DWORD	0: BOOTPクライアント 1: DNSクライアント 2: DHCPクライアント 3: DHCP-DNSアップデート 4: コンフィグレーション可（CIP内） 予備の他ビット（0） 7: ACD可（0=不可、1=可）
0x3	Config Control	Set/Get	DWORD	0: 0x0=保存済みコンフィグ使用 1: 0x1=BOOTP使用 2: 0x2=DHCP使用 3: 4: デバイス1つはDNSをNameLookupを使用（サポートされないため常時0） 他ビットは予備（0）
0x4	Physical Link Object Get	Get	STRUCT of: UINT PathSize EPATH Path	物理リンクオブジェクトへのパスは常時{0x20, 0xF6, 0x24, 0x01} で、イーサネットリンクオブジェクトのインスタンス1を示す
0x5	Interface Configuration	Set/Get	STRUCT of: UDINT IpAddress UDINT Netmask UDINT GatewayAddress UDINT NameServer1 UDINT NameServer2 STRING DomainName	IPスタックコンフィグレーション（IPアドレス、ネットマスク、ゲートウェイ、ネームサーバー（サポートされていればDNS）及びドメイン名）
0x6	Host Name	Set/Get	STRING	ホスト名（DHCP DNSアップデート用）
0x7	Safety Network Number			サポート無し
0x8	TTL Value	Get/Set	USINT	IPマルチキャストパケットのＴＴＬ値　範囲 1..255 （デフォルト=1）

表59　インスタンス1のアトリビュート（続き）

Id	アトリビュート	アクセスルール	データ種別	備考
0x9	Mcast Config	Get/Set	STRUCT of: USINT AllocControl USINT reserved UINT NumMcast UDINT McastStartAddr	Alloc Control = 0 IPマルチキャストアドレス数 = 32 マルチキャストスタートアドレス = 239.192.1.0
0xA	Selected Acd	Get/Set	BOOL	0=ACD disable 1=ACD enable （デフォルト）
0xB	Last Conflict Detected	Get	STRUCT of: USINT AcdActivity ARRAY of: 6 USINT RemoteMac ARRAY of: 28 USINT ArpPdu	ACD診断パラメーター

表60　TCP/IPインターフェースオブジェクトの、シュナイダーエレクトリック版拡張機能

Id	アトリビュート	アクセスルール	データ種別	備考
0x64	Cable Test	Set/Get	STRUCT of: USINT Interface USINT Status	インターフェース ステータス（1=アクティブ、2=成功、3=失敗、4=未初期化）
0x65	Cable Pair Size	Get	USINT	ケーブルテスト結果のサイズ STRUCT of: 100BASEはペア2つ 1000BASEはペア4つ

表60　TCP/IPインターフェースオブジェクトの、シュナイダーエレクトリック版拡張機能（続き）

Id	アトリビュート	アクセスルール	データ種別	備考

0x66	Cable Test Result	Get	STRUCT of:
			USINT Interface
			USINT CablePair
			USINT CableStatus
			USINT CableMinLength
			USINT CableMaxLength
			USINTCableFailureLocation
				100BASE:{
				{Interface, CablePair1, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair2, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				} 1000BASE:{
				{Interface, CablePair1, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair2, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair3, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair4, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				}

イーサネットリンクオブジェクト

以下2つのテーブルの情報は、イーサネットリンクオブジェクトの一部です。情報へのアクセスには、以下の値を使用します。

- Class(####)
- Instance(###)
- Attribute(#)

例えば、explicitメッセージを使用してUtilization Alarmへアクセスするための*class* （クラス）、*instance* （インスタンス）、*attribute* （アトリビュート）の値は、次の通りです。

- Class = 0xF6
- Instance = 1
- Attribute = 6

表61　イーサネットリンクオブジェクトの、インスタンスアトリビュート及びシュナイダーエレクトリック版拡張機能

Id	アトリビュート	アクセスルール	データ種別	備考
インスタンスアトリビュート				
0x1	Interface Speed	Get	UDINT	MBit/s (10,100, 1000, …)でインターフェース速度を使用。
0x2	Interface Flags	Get	DWORD	インターフェースステータスフラグ： 0: Link State (0=リンク無し、1=リンク) 1: Duplex mode (0=半二重、1=全二重) 2: 0x0=Auto-Negotiation中 3: 0x1=Auto-Negotiation失敗 4: 0x2=失敗したが、速度検知 0x3=Auto-Negotiation成功 0x4=Auto-Negotiation無し 5: マニュアルコンフィグレーションは要リセット（不要なため、常時0） 6: ハードウェアエラー
0x2	Interface Flags	Get	DWORD USINT Interface USINT CablePair USINT CableStatus USINT CableMinLength USINT CableMaxLength USINTCableFailure L ocation	インターフェースステータスフラグ：
0x3	Physical Address	Get	ARRAY of: 6 USINT	物理インターフェースのMACアドレス
0x4	Interface Counters	Get	STRUCT of: UDINT MibIICounter1 UDINT MibIICounter2 …	InOctets, InUcastPackets, InNUcastPackets, InDiscards, InErrors, InUnknownProtos, OutOctets, OutUcastPackets, OutNUcastPackets, OutDiscards, OutErrors
0x5	Media Counters	Get	STRUCT of: UDINT EthernetMib Counter1 UDINT EthernetMib Counter2 …	Alignment Errors, FCS Errors, Single コリジョン、複数コリジョン、SQEテストエラー、送信保留、コリジョン遅延、コリジョン超過、MAX TX Error、Carrier Sense Error、フレーム超過、MAC RX Error

表61　イーサネットリンクオブジェクトの、インスタンスアトリビュート及びシュナイダーエレクトリック版拡張機能（続き）

Id	アトリビュート	アクセスルール	データ種別	備考
0x6	Interface Control	Get/Set	STRUCT of:	Control Bits:
			WORD ControlBits	0: Auto-negotiation有効／無効 (0=無効, 1=有効)
				1: Auto-negotiation無効の場合、Duplex mode (0=半二重、1=全二重) 2:
			UINT ForcedInterface Speed	Auto-negotiation無効の場合、MBits/s: 10,100,…, でインターフェース速度
0x7	Interface type	Get	USINT	インターフェース種別 0: インターフェース種別不明 1: インターフェースは内部 2: ツイストペアケーブル 3: 光ファイバーケーブル
0x8	Interface state	Get	USINT	インターフェースの現在のステータス: 0: インターフェースのステータス不明 1: インターフェース有効 2: インターフェース無効 3: インターフェーステスト中
0x9	Admin State	Set/Get	USINT	Administrative state: 1: インターフェースを有効にする 2: インターフェースを無効にする
0xA	Interface label	Get	SHORT-STRING	人間に判読可能なID
イーサネットリンクオブジェクトのシュナイダーエレクトリック版拡張機能				
0x64	Ethernet Interface Index	Get	USINT	インターフェース/ポートインデックス (ifIndex out of MIBII)
0x65	Port Control	Get/Set	DWORD	0: リンクステータス (0=リンクダウン, 1=リンクアップ) 1: リンクアドミステータス (0=無効, 1=有効) 8: 不正アクセスアラーム（リードオンリー） 9: Utilization アラーム（リードオンリー）
0x66	Interface Utilization	Get	USINT	プライベートMIB hm2IDiagfaceUtilizationの既存カウンターを使用中。 利用率（単位1%=100、%/100）RX インターフェース利用率
0x67	Interface Utilization Alarm Upper Threshold	Get/Set	USINT	このパラメーター内の hm2DiagIfaceUtilizationAlarmUpperThreshold（可変）にアクセス可能。利用率（単位1%=100） RX インターフェース利用率上限
0x68	Interface Utilization Alarm Lower Threshold	Get/Set	USINT	このパラメーター内の hm2DiagIfaceUtilizationAlarmLowerThreshold（可変）にアクセス可能。利用率（単位1%=100）RX インターフェース利用率下限
0x69	Broadcast limit	Get/Set	USINT	Get/Set USINT Broadcast limiterサービス （Egress BC-Frame制限、0=無効）、フレーム/秒

表61　イーサネットリンクオブジェクトの、インスタンスアトリビュート及びシュナイダーエレクトリック版拡張機能（続き）

Id	アトリビュート	アクセスルール	データ種別	備考
0x6A	Ethernet Interface Description	Get/Set	STRING	インターフェース/ポート ディスクリプション（MIB II ifDescrより）、例えば Unit: 1 Slot: 2 Port: 1 - 10/100 Mbit TX" 又は unavailable、最大64バイト
0x6B	Port Monitor	Get/Set	DWORD	0: リンクフラップ (0=Off, 1=On) 1: CRC/Fragment (0=Off, 1=On) 2: Duplex不一致 (0=Off, 1=On) 3: 過負荷検知 (0=Off, 1=On) 4: リンク速度/ Duplexモード (0=Off, 1=On) 5: ポートを再度無効化する (0=Off, 1=On) 6: トラップ送信アクション (0=Off, 1=On) 7: アクティブ状態（どの状態がこのアクションを発生させたかを表示） 8: 9: 00001B:リンクフラップ 00010B:CRC/フラグメント 10: 00100B:Duplex不一致 01000B:過負荷検知 11: 10000B:リンク速度/ Duplexモード 12: 予備（常時0） 13: 予備（常時0） 14: 予備（常時0） 15: 予備（常時0）
0x6C	Quick Connect	Get/Set	USINT	インターフェースにQuick Connect (0=Off, 1=On) Quick Connectを有効にすると、デバイスはポート速度を100FDに設定し、インターフェースのAuto-Negotiation及びスパニングツリーを無効化する
0x6D	SFP Diagnostics	Get	STRUCT of:	
			STRING ModuleType	
			SHORT-STRING SerialNumber	
			USINT Connector	
			USINT Supported	
			DINT Temperature	in °C
			DINT TxPower	in mW
			DINT RxPower	in mW
			DINT RxPower	in dBm
			DINT TxPower	in dBm

表62　ポートからイーサネットリンクオブジェクトインスタンスのアサイメント

イーサネットポート	イーサネットリンクオブジェクトインスタンス
CPU	1
1	2
2	3
3	4
4	5
…	…

注記：ポート数はハードウェアの種別によります。ポートが接続されている場合のみ、イーサネットリンクオブジェクトが存在します。

スイッチエージェントオブジェクト

当デバイスは、シュナイダーエレクトリック特有の、デバイスコンフィグレーション及びインスタンス1を含む情報パラメーター用のイーサネットスイッチエージェントオブジェクト（クラスコード 0x95）をサポートします。

表63　クラスのアトリビュート

Id	アトリビュート	アクセスルール	データ種別	備考
0x1	Switch Status	Get	DWORD	0: 信号接点と同様、値はデバイス全体の状態を示す (0=ok, 1=失敗)
				1: デバイスセキュリティステータス (0=ok, 1=失敗)
				2: 電源1 (0=ok, 1=失敗)
				3: 電源2 (0=ok, 1=失敗または存在せず)
				4: 予備
				5: 予備
				6: 信号接点1 (0=閉、1=開)
				7: 信号接点2 (0=閉、 1=開又は存在せず)
				8: 予備
				9: 温度 (0=ok, 1=失敗)
				10: モジュール取外し (1=取外し済み)
				11: EAM取外し (1=取外し済み)
				12: EAM-SD取外し (1=取外し)
				13: 予備
				14: 予備
				15: 予備
				16: 予備
				17: 予備
				18: 予備
				19: 予備
				20: 予備
				21: 予備
				22: 予備
				23: MRP (0=無効, 1=有効)
				24: 予備
				25: 予備
				26: RSTP (0=無効, 1=有効)
				27: LAG (0=無効, 1=有効)
				28: 予備
				29: 予備
				30: 予備
				31: 接続エラー (1=失敗)

表63　クラスのアトリビュート（続き）

Id	アトリビュート	アクセスルール	データ種別	備考
0x2	Switch Temperature	Get	STRUCT of:	
			INT TemperatureF	in °F
			INT TemperatureC	in °C
0x3	Reserved	Get	UDINT	将来用の予備（常時0）
0x4	Switch Max Ports	Get	UINT	イーサネットスイッチポート数の最大
0x5	Multicast Settings (IGMP Snooping)	Get/Set	WORD	0: IGMPスヌーピング (0=無効, 1=有効) 1: IGMPクエリア (0=無効, 1=有効) 2: IGMP Querier モード (リードオンリー) (0=非クエリア, 1=クエリア) 3: IGMP クエリアパケットバージョン 4: Off=0 IGMP クエリア 無効 5: V1=1 6: V2=2 7: V3=3 8: 不明マルチキャストの処理： 9: 0=全ポートへ送信 10: 2=破棄
0x6	Switch Existing Ports	Get	ARRAY of:	既存スイッチポートのビットマスク
			DWORD	ビット当たり、ビット0 (=ポート1) (0=ポート使用不可, 1=ポートあり)から開始 配列（ビットマスク）サイズは、スイッチポートの最大数のサイズによって調整（最大ポート28個、DWORD1個を使用）
0x7	Switch Port Control	Get/Set	ARRAY of:	Bitmask Link Admin Status スイッチポート
			DWORD	ビット当たり、ビット0 (=ポート1) (0=ポート使用不可, 1=ポートあり)から開始　配列（ビットマスク）サイズは、スイッチポートの最大数のサイズによって調整（最大ポート28個、DWORD1個を使用）
0x7	Switch Ports Mapping	Get	ARRAY of:	イーサネットリンクオブジェクトのインスタンス数
			USINT	インデックス0（=ポート1）から開始イーサネットリンクオブジェクトインスタンスは全て既存のイーサネットスイッチポート用（1..N、最大ポート数）。 エントリーが0の場合、当ポートのイーサネットリンクオブジェクトは存在せず

表63　クラスのアトリビュート（続き）

Id	アトリビュート	アクセスルール	データ種別	備考
0x9	Switch Action Status	Get	DWORD	最後に実行したアクションのステータス（例：コンフィグ保存、ソフトウェアアップデート等） 0: Flash保存コンフィグレーション中/Flash書込み中 1: Flash保存コンフィグレーション失敗/Flash書込み失敗 4: コンフィグレーション変更（稼働中コンフィグレーションと当コンフィグレーションが同期せず）

シュナイダーエレクトリック特有のイーサネットスイッチエージェントオブジェクトは、追加の固有ベンダーサービスを提供し、サービスコード0x35によってスイッチコンフィグレーションを保存することができます。PCからデバイスコンフィグレーションを保存するリクエストを送信すると、デバイスはフラッシュメモリにコンフィグレーションを保存後に返答を送信います。

ベーススイッチオブジェクト

ベーススイッチオブジェクトは、マネージドイーサネットスイッチ（改訂1）用に、CIPアプリケーションレベルのインターフェースを基礎ステータス情報に提供します。

ベーススイッチ（クラスコード0x51）のインスタンス1のみが有用可能です。

表64　インスタンスアトリビュート

Id	アトリビュート	アクセスルール	データ種別	備考
0x1	Device Up Time	Get	UDINT	デバイスに電源が入ってからの時間
0x2	Total port count	Get	UDINT	物理ポート数
0x3	System Firmware Version	Get	SHORT-STRING	人間に判読可能な、システムファームウェアバージョンの表記
0x4	Power source	Get	WORD	スイッチ電源のステータス
0x5	Port Mask Size	Get	UINT	ポート配列アトリビュート内のDWORD数
0x6	Existing ports	Get	ARRAY of: DWORD	ポートマスク
0x7	Global Port Admin State	Get	ARRAY of: DWORD	ポートAdminステータス
0x8	Global Port link	Get	ARRAY of: DWORD	ポートリンクステータス
0x9	System Boot Loader Version	Get	SHORT-STRING	判読可能なシステムファームウェアバージョン
0xA	Contact Status	Get	UDINT	スイッチの接点閉じる

表64　インスタンスアトリビュート（続き）

Id	アトリビュート	アクセスルー	データ種別	備考
0xB	Aging Time	Get	UDINT	範囲 10..1000000 · 1/10秒 （デフォルト=300） 0=ラーニングはoff
0xC	Temperature C	Get	UINT	スイッチ温度（℃）
0xD	Temperature F	Get	UINT	スイッチ温度（℉）

サービス、接続、I/O Data

デバイスは以下の接続及びパラメーターをサポートします。

表65　新規モジュールを統合するための設定

設定	I/O接続	入力のみ	リッスンのみ
Comm Format:	Data - DINT	Data - DINT	Input Data - DINT - Run/Program
IP Address	デバイスのIPアドレス	デバイスのIPアドレス	デバイスのIPアドレス
Input Assembly Instance	100	100	100
Input Size	32	32	32
Output Assembly Instance	150	152	153
Output Size	32	0	0
Configuration Assembly Instance	151	151	151
Data Size	10	10	10

表66　デバイス I/O データ構造

I/O データ	値（定義するデータ種別やサイズ等）	方向	サイズ[1]
Device Status	Bitmask (Switch Agent Attribute 0x1 参照)	入力	DWORD
Link Status	Bitmask, ポート毎1ビット (0=リンク無し, 1=リンクアップ)	入力	DWORD
Output Links Admin State applied	Bitmask, （出力の肯定応答に）ポート毎1ビット リンクステート変更は拒否される場合も。例えば、コントローラーアクセスポート。 (0=ポート有効、1=ポート無効)	入力	DWORD
Utilization Alarm[2]	Bitmask, ポート毎1ビット (アラーム無し、1=ポートにアラーム)	入力	DWORD
Access Violation Alarm[3]	Bitmask, ポート毎1ビット (アラーム無し、1=ポートにアラーム)	入力	DWORD
Multicast Connections	接続数、整数	入力	DINT

表66　デバイス I/O データ構造（続き）

I/O データ	値（定義するデータ種別やサイズ等）	方向	サイズ[1]
TCP/IP Connections	接続数、整数	入力	DINT
Quick Connect Mask	Bitmask（ポート毎1ビット） (0=Quick Connect 無効、1=Quick Connect 有効)	入力	DINT
Link Admin State	Bitmask, ポート毎1ビット (0=ポート有効、1=ポート無効)	出力	DWORD

1. ポートビットマスクのデフォルトサイズは32ビットです（DWORD）。ポートビットマスクが28ポートを超えるデバイスは、n*DWORD に拡張されます。
2. Utilization Alarm設定は、*Basic Settings > Port* ダイアログボックスの*Utilization* タブで指定します。上限閾値に達すると、アラーム条件がアクティブになります。下限閾値に達すると、アクティブなアラーム条件が非アクティブになります。
3. Access Violation（アクセス違反）アラーム設定は、*Network Security > Port Security* ダイアログボックスで指定します。上限閾値に達すると、アラーム条件がアクティブになります。下限閾値に達すると、アクティブなアラーム条件が非アクティブになります。

表67　データ種別によるビットサイズのマッピング

オブジェクト種別	ビットサイズ
BOOL	1 bit
DINT	32 bit
DWORD	32 bit
SHORT-STRING	max.32 bytes
STRING	max.64 bytes
UDINT	32 bit
UINT	16 bit
USINT	8 bit
WORD	16 bit

A コンフィグレーション環境のセットアップ

A.1 DHCP/BOOTP サーバーのセットアップ

以下の例では、haneWIN DHCP Serverソフトウェアを使用してDHCPサーバーのコンフィグレーションを実行します。なお、このシェアウェアはIT-Consulting Dr. Herbert Hanewinkel の製品となります。このソフトウェアは右記リンクからダウンロードします。www.hanewin.net試用版のソフトウェアは初期インストールから30日までですので、以降はライセンスを購入するかご判断ください。

以下の手順を実行します。

- ☐ PCにDHCPサーバーをインストールします。
  インストールアシスタントに従い、インストールを行います。
- ☐ *haneWIN DHCP Server* プログラムを開始します。

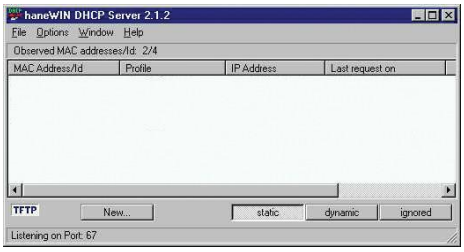


図73 haneWIN DHCP Server のスタートウィンドウ

注記：このウィンドウをアクティベートすると、インストール手順に含まれるサービスが基本設定内で自動的に開始されます。このサービスは、プログラムそのものが開始していなくてもアクティブな状態です。開始すると、サービスはDHCPのクエリーに応答します。

- ☐ メニューバーの、*Options > Preferences* をクリックし、Program Settingsウィンドウを開きます。
- ☐ *DHCP*タブを選択します。
- ☐ 図に示した通りの設定を指定します。

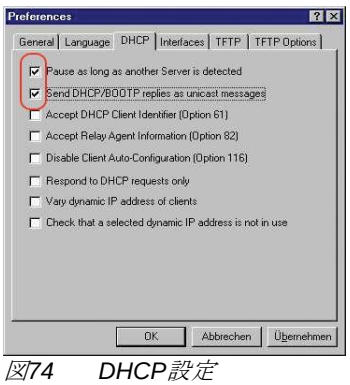


図74 DHCP設定

- ☐ *Ok* ボタンをクリックします。
- ☐ コンフィグレーションプロファイルを入力するには、メニューバーの*Options > Configuration Profiles*項目をクリックします。

☐ 新規コンフィグレーションプロファイルの名前を指定します。

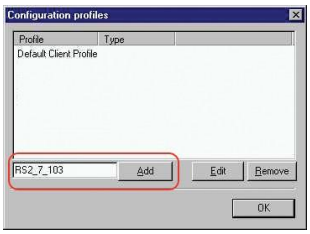


図75　コンフィグレーションプロファイルの追加

☐ *Add* ボタンをクリックします。
☐ ネットマスクを指定します。

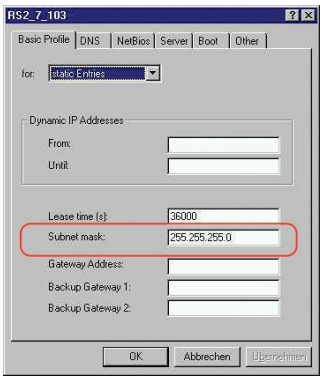


図76　コンフィグレーションプロファイル内のネットマスク

☐ *Apply* ボタンをクリックします。
☐ *Boot* タブを選択します。
☐ tftpサーバーのIPアドレスを入力します。
☐ パス及びコンフィグレーションファイルのファイル名を入力します。

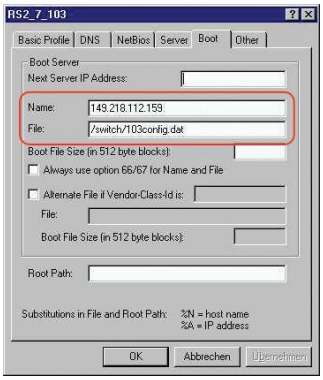


図77　tftp サーバーのコンフィグレーションファイル

☐ *Apply* ボタンに続き、*OK* ボタンをクリックします。

☐ 各デバイス種別にプロファイルを追加します。
同種のデバイスで異なるコンフィグレーションがある場合、各コンフィグレーションそれぞれにプロファイルを追加します。

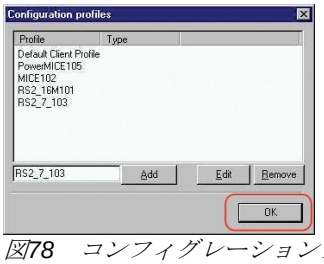


図78　コンフィグレーションプロファイルの管理

☐ コンフィグレーションプロファイルの追加作業を完了するには、*Ok* ボタンをクリックします。
☐ 静的アドレスを入力するには、メインウィンドウで*Static* ボタンをクリックします。

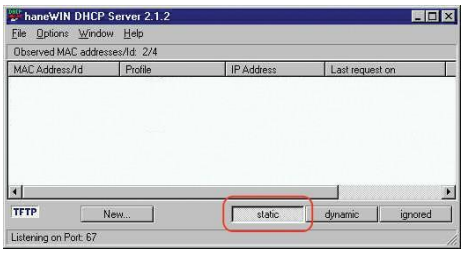


図79　静的アドレスの入力

☐ *Add* ボタンをクリックします。

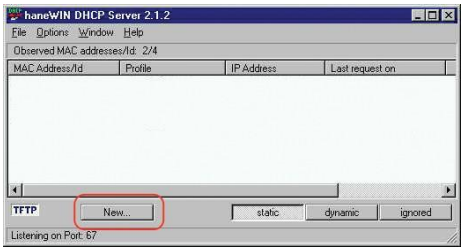


図80　静的アドレスの追加

☐ デバイスのMACアドレスを入力します。
☐ デバイスのIPアドレスを入力します。

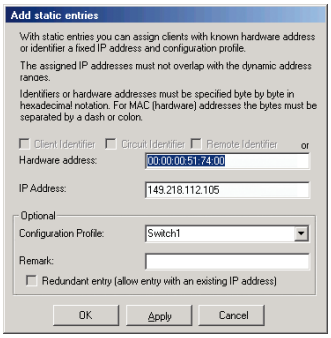


図81　静的アドレスのエントリー

☐ デバイスのコンフィグレーションプロファイルを選択します。

- ☐ *Apply* ボタンに続き、*OK* ボタンをクリックします。
- ☐ DHCPサーバーからパラメーターを取得するデバイス毎のエントリーを追加します。

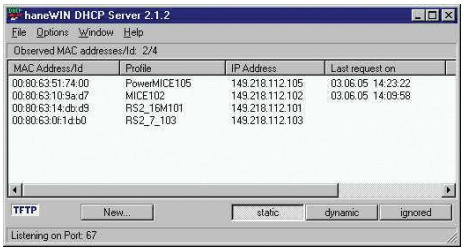


図82　DHCPサーバー、エントリー有り

A.2 オプション82でDHCPサーバーのセットアップ

以下の例では、haneWIN DHCP Serverソフトウェアを使用してDHCPサーバーのコンフィグレーションを実行します。なお、このシェアウェアはIT-Consulting Dr. Herbert Hanewinkel の製品となります。このソフトウェアは右記リンクからダウンロードします。www.hanewin.net試用版のソフトウェアは初期インストールから30日までですので、以降はライセンスを購入するかご判断ください。

以下の手順を実行します。

- ☐ PCにDHCPサーバーをインストールします。
  インストールアシスタントに従い、インストールを行います。
- ☐ *haneWIN DHCP Server* プログラムを開始します。

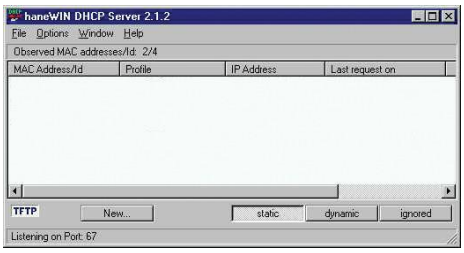


図83 haneWIN DHCP Server のスタートウィンドウ

注記：このウィンドウをアクティベートすると、インストール手順に含まれるサービスが基本設定内で自動的に開始されます。このサービスは、プログラムそのものが開始していなくてもアクティブな状態です。開始すると、サービスはDHCPのクエリーに応答します。

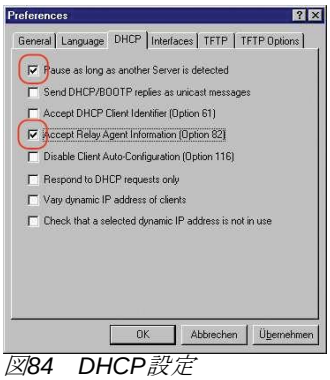


図84　DHCP設定

☐ 静的アドレスを入力するには、*Add* ボタンをクリックします。

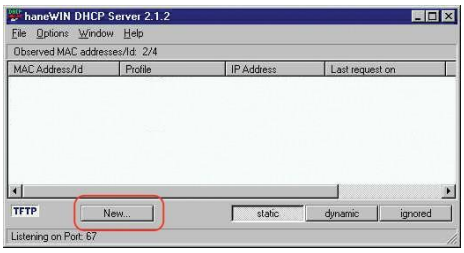


図85　静的アドレスの追加

☐ *Circuit Identifier* チェックボックスにチェックを入れます。
☐ *Remote Identifier* チェックボックスにチェックを入れます。

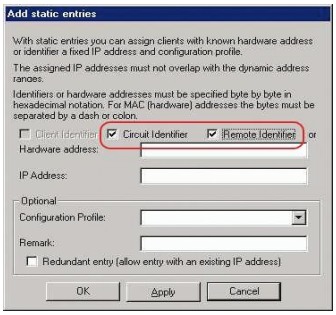


図86　固定アドレス割当てのデフォルト設定

☐ *Hardware address* フィールドで、スイッチとポートの値に*Circuit Identifier* 及び*Remote Identifier* を指定します。
DHCPサーバーは、*Hardware address* フィールドに指定されたポートに接続させるデバイスに対し、*IP address* フィールドに指定されているIPアドレスを割当てます。
ハードウェアアドレスは次の形式となあります。

`ciclvvvvssmmpprirlxxxxxxxxxxxx`

- `ci`
  Circuit ID（回路ID）種のサブ識別子
- `cl`
  Circuit ID（回路ID）の長さ
- Schneider Electric 識別子
  シュナイダーエレクトリック製デバイスがポートに接続されている時は`01` 、それ以外は`00`。
- `vvvv`
  DHCPリクエストのVLAN IDデフォルト設定：`0001` = VLAN 1
- `ss`
  デバイスと接続されたポートとモジュールの位置にあるデバイスのソケット

値00を指定します。

- mm
  デバイスと接続されたポートとモジュールの位置にあるデバイスのソケット
- pp
  デバイスと接続されたポート
- ri
  Remote ID（リモートID）種のサブ識別子
- rl
  Remote ID（リモートID）の長さ
- xxxxxxxxxxxx
  デバイスが接続されているデバイスの、Remote ID（例：MACアドレス）

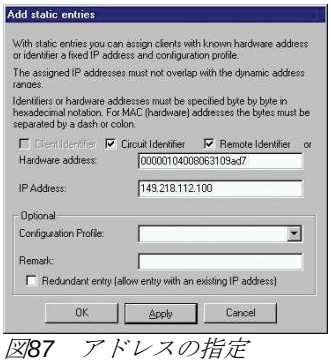


図87　アドレスの指定

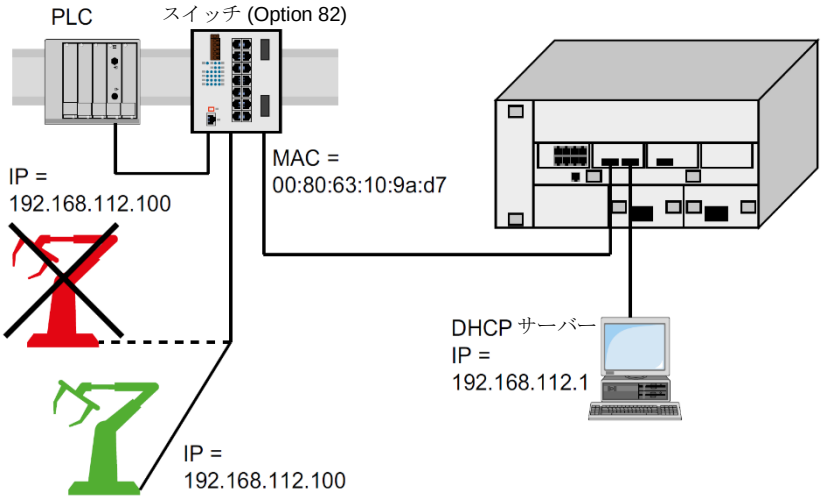


図88　Option 82使用例

A.3 SSHを介したアクセスの準備

SSHを介してデバイスに接続することができます。以下の手順を実行します。
➢ デバイス内にキーを作成します。又は…
➢ 既にあるご自身のキーをデバイスに転送します。
➢ SSHクライアントプログラムでデバイスにアクセスする準備を行います。

注記：キーはデフォルトから既にあり、SSHへのアクセスは有効となっています。

A.3.1 デバイス内にキーを作成する

当デバイス内に直接キーを作成することができます。以下の手順を実行します。

- ☐ *Device Security > Management Access > Server* ダイアログボックスの*SSH* タブを開きます。
- ☐ SSHサーバーを無効化するには*Operation* フレームの*Off* のラジオボタンを選択します。
- ☐ ボタンをクリックし、変更を一時的に保存します。
- ☐ RSAキーを作成するには、*Signature* フレームで*Create* ボタンをクリックします。
- ☐ *SSH* サーバーを有効化するには*Operation* フレームの*On* のラジオボタンを選択します。
- ☐ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`ssh key rsa generate`	新規RSAキーを作成します。

A.3.2 既にあるご自身のキーをデバイスにロードする

OpenSSHは、経験豊かなネットワークアドミニストレーターであれば自身のキーを作成することができます。キーを作成するには、PCで以下コマンドを入力します。

```
ssh-keygen(.exe) -q -t rsa -f rsa.key -C '' -N '' rsaparam -out rsaparam.pem 2048
```

当デバイスでは既にあるご自身のキーをデバイスに転送することができます。以下の手順を実行します。

- ☐ *Device Security > Management Access > Server* ダイアログボックスの*SSH* タブを開きます。
- ☐ SSHサーバーを無効化するには*Operation* フレームの*Off* のラジオボタンを選択します。
- ☐ ボタンをクリックし、変更を一時的に保存します。
- ☐ ホストキーがPC又はネットワークドライブにある場合は、エリア内にキーを含むファイルをドラッグ&ドロップします。もしくは、エリア内をクリックしてファイルを選択します。

- ☐ *Key import* フレームの*Start* ボタンをクリックし、キーをデバイスにロードします。
- ☐ *SSH* サーバーを有効化するには*Operation* フレームの*On* のラジオボタンを選択します。
- ☐ ✔ ボタンをクリックし、変更を一時的に保存します。

以下の手順を実行します。
- ☐ ご自身で作成したキーを、PCから外部メモリにコピーします。
- ☐ 外部メモリからデバイスにキーをコピーします。

`enable`	Privileged Exec Modeに切り替えます。
`copy sshkey envm <file name>`	外部メモリにあるご自身のキーをデバイスにロードします。

A.3.3 SSHクライアントプログラムの準備

PuTTY プログラムを使用すると、SSHを介してデバイスにアクセスすることができます。このソフトウェアは右記リンクからダウンロードします。www.putty.org

以下の手順を実行します。
- ☐ プログラムをダブルクイックして開始します。

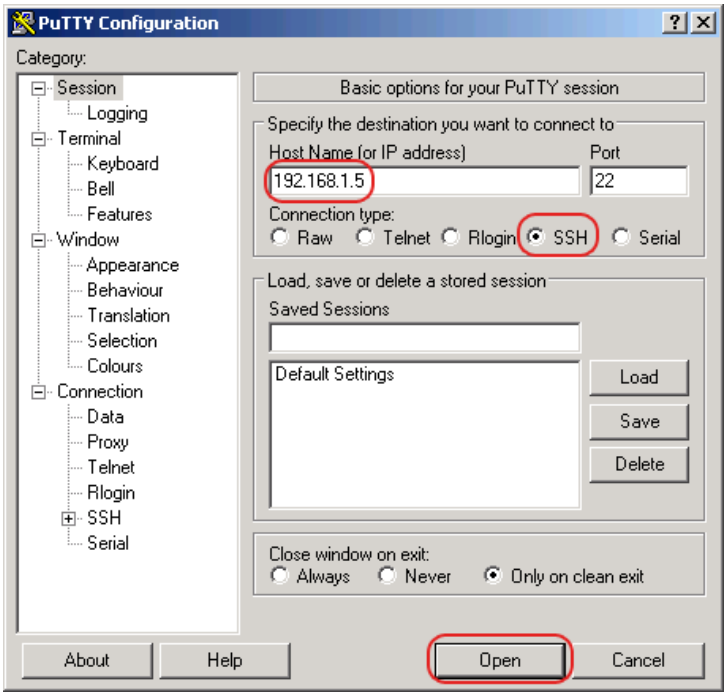


図89 PuTTY 入力画面

- ☐ *Host Name (or IP address)* フィールドに、使用デバイスのIPアドレスを入力します。IPアドレス（a.b.c.d）は0から255までの10進数4つで構成されています。これら4つの10進数はドットで分けられています。
- ☐ 接続の種別（connection type）を選択するには、*Connection type* のオプションリストから、*SSH*のラジオボタンを選択します。
- ☐ *Open* ボタンをクリックし、デバイスのデータ接続をセットアップします。

接続が確立される前に、*PuTTY* がセキュリティ警報メッセージを表示しますので、この時にキーのフィンガープリントを確認します。

図90　フィンガープリントのセキュリティ警報プロンプト

接続が確立される前に、*PuTTY* がセキュリティ警報メッセージを表示しますので、この時にキーのフィンガープリントを確認します。

- キーのフィンガープリントを確認することで、目的のデバイスに確実に接続されたことを確認します。
- このフィンガープリントがキーと一致した場合、*Yes* ボタンをクリックします。

経験豊かなネットワークアドミニストレーターであれば、SSHを介したデバイスアクセスの別の方法として、OpenSSH Suiteの使用が挙げられます。データ接続を確立するには、以下コマンドを入力します。

```
ssh admin@10.0.112.53
```

ユーザー名：`admin`

デバイスのIPアドレス：`10.0.112.53`

A.4 HTTPS証明書

ウェブブラウザから、HTTPSプロトコルを使用したデバイスへの接続を確立します。条件として、*Device Security > Management Access > Server* ダイアログボックスの*HTTP* タブにある、*HTTPS server* 機能を有効にします。

注記：ウェブブラウザ等のサードパーティー製ソフトウェアは、有効期限やクリプトグラフィーによるパラメーター推奨値等を基準として証明書を認証しています。従って、有効期限が切れた場合やクリプトグラフィーによる推奨値が変更された場合などは、古い証明書ではエラーとなることがあります。このように、サードパーティー製ソフトウェアによる認証エラーを解決するには、ユーザーの最新証明書をデバイスに移行させるか、或いは最新のファームウェアで証明書を再度作成してください。

A.4.1 HTTPS証明書管理

X.509/PEM（Public Key Infrastructure：PKI：キー基盤）では、証明書は暗号化することとされています。デフォルトでは、デバイス内に自動生成された証明書が既に存在します。以下の手順を実行します。

- ☐ *Device Security > Management Access > Server* ダイアログボックスの*HTTPS* タブを開きます。
- ☐ X509/PEMに基づく証明書を作成するには、*Certificate* フレームで*Create* ボタンをクリックします。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。
- ☐ HTTPSサーバーを再起動してキーをアクティベートします。サーバーはコマンドラインインターフェースを使用して再起動します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`https certificate generate`	X.509/PEM証明書を作成します。
`no https server`	*HTTPS* 機能を無効化します。
`https server`	*HTTPS* 機能を有効化します。

☐ また、当デバイスでは外部で生成したX.509/PEM証明書をデバイスに転送することもできます。

- ☐ *Device Security > Management Access > Server* ダイアログボックスの*HTTPS* タブを開きます。
- ☐ 証明書がPC内又はネットワークドライブにある場合は、証明書を エリア内にドラッグ&ドロップします。もしくは、エリア内をクリックして証明書を選択します。
- ☐ 証明書をデバイスにコピーするには、*Start* ボタンをクリックします。
- ☐ ☑ ボタンをクリックし、変更を一時的に保存します。

`enable`	Privileged Exec Modeに切り替えます。
`copy httpscert envm <file name>`	HTTPS証明書を外部不揮発性メモリにコピーします。

`configure`	Configuration modeに切り替えます。
`no https server`	*HTTPS* 機能を無効化します。
`https server`	*HTTPS* 機能を有効化します。

注記：証明書を作成又は転送した後にアクティベートするには、デバイスをリブート又はHTTPSサーバーを再起動します。HTTPSサーバーはコマンドラインインターフェースを使用して再起動します。

A.4.2 HTTPSを介したアクセス

HTTPSデータ接続のデフォルト設定は、TCPポート`443`となっています。HTTPSポート番号を変更した場合、デバイス又はHTTPSサーバーをリブートします。これで変更が有効になります。以下の手順を実行します。

- ☐ *Device Security > Management Access > Server* ダイアログボックスの*HTTPS* タブを開きます。
- ☐ 機能を有効化するには*Operation* フレームの`On` のラジオボタンを選択します。
- ☐ HTTPSでデバイスにアクセスする場合、ブラウザーでHTTPの代わりにHTTPSと入力し、続いてデバイスのIPアドレスを入力します。

`enable`	Privileged Exec Modeに切り替えます。
`configure`	Configuration modeに切り替えます。
`https port 443`	ウェブブラウザがクライアントからHTTPSリクエストを受信するTCPポートの番号を指定します。
`https server`	*HTTPS* 機能を有効化します。
`show https`	*HTTPS* サーバーのステータス及びポート番号を表示します。

HTTPSポート番号を変更した場合、HTTPSサーバーを無効化した後に再度有効化することで、変更が有効になります。

デバイスはHTTPSプロトコルを使用して新規のデータ接続を確立します。セッション後にログアウトすると、デバイスはデータ接続を遮断します。

B 付録

B.1 MIB（Management Information Base：管理情報ベース）

MIB（Management Information Base：管理情報ベース）は、ツリー構造の一部を抜粋した設計になっています。

分岐点は、オブジェクトのクラスを示しています。MIBの「葉」の部分は、「generic object class（ジェネリックオブジェクトクラス）」と呼ばれます。

このgeneric object classが固有性の識別に利用される時はインスタンス化されますが、言い換えると、ポートやソースアドレスを指定することで抜粋された構造が現実的にマッピングされます。

数値（整数、timeTick、カウンター、オクテットストリング）はこれらインスタンスに割当てられます。これらの数値は読み出すことが出来る他、場合によっては変更することもできます。オブジェクトのディスクリプション又はID（OID）は、オブジェクトクラスを表します。サブ識別子（SID）はこれらをインスタンス化するのに使用されます。

例：

generic object class `sa2PSState` （`OID` = `1.3.6.1.4.1.3833.1.1.11.11.1.1.2.1`）は、`power supply status`の抜粋情報を示したものです。但し、これがどの電源（power supply）であるかをシステムが理解しているわけではないので、これから如何なる値を読み取ることもできません。

サブ識別子`2`を指定することでこの抜粋情報が現実化（インスタンス化）され、これにより電源`2`のステータスをオペレーション中と判断することができます。このインスタンスに値を割当てることで、読み取ることが可能となります。インスタンス `get 1.3.6.1.4.1.3833.1.1.11.11.1.1.2.1` は応答`1`を返すことで、即ち電源がオペレーションの準備が出来ていることを示します。

使用されるSyntaxの定義	
Integer	範囲が -2^{31} - 2^{31}-1 の整数（integer）
IP address	`xxx.xxx.xxx.xxx` (`xxx` = 整数、範囲は`0..255`)
MAC address	ISO/IEC 8802-3に基づき、12桁の16進数
Object Identifi	er x.x.x.x… (例： 1.3.6.1.1.4.1.3833...)
Octet String	ASCII文字ストリング
PSID	電源識別子（電源ユニット番号）
TimeTicks	ストップウォッチ、経過時間=数値/100（秒） 数値=範囲 0-2^{32}-1 の整数
Timeout	100分の1秒単位のタイムバリュー タイムバリュー=範囲 0-2^{32}-1 の整数
Type field	ISO/IEC 8802-3に基づき、4桁の16進数
Counter	整数（0-2^{32}-1）、特定のイベント発生時に、数値が`1`単位で増加。

B.2 RFC一覧

RFC 768	UDP
RFC 783	TFTP
RFC 791	IP
RFC 792	ICMP
RFC 793	TCP
RFC 826	ARP
RFC 854	Telnet
RFC 855	Telnet Option（Telnetオプション）
RFC 951	BOOTP
RFC 1112	IGMPv1
RFC 1157	SNMPv1
RFC 1155	SMIv1
RFC 1212	Concise MIB Definitions（簡潔なMIB定義） RFC 1213
RFC 1493	Dot1d
RFC 1542	BOOTP-Extensions（BOOTP拡張機能）
RFC 1643	Ethernet-like -MIB（イーサネットのようなMIB）
RFC 1757	RMON
RFC 1867	Form-Based File Upload in HTML（HTML におけるフォームを基にしたファイルのアップロード）
RFC 1901	Community based SNMP v2（コミュニティベースのSNMP v2）
RFC 1905	Protocol Operations for SNMP v2（SNMPv2のプロトコル動作）
RFC 1906	Transport Mappings for SNMP v2（SNMPv2のトランスポートマッピング） RFC 1945
RFC 2068	HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03（ハイパテキスト転送プロトコル HTTP/1.1）
RFC 2131	DHCP
RFC 2132	DHCP-Options（DHCPオプション）
RFC 2233	The Interfaces Group MIB using SMI v2（SMIv2を使用したインターフェースグループMIB）
RFC 2236	IGMPv2
RFC 2246	The TLS Protocol, Version 1.0（TLSプロトコルVer.1.0）
RFC 2346	AES Ciphersuites for Transport Layer Security（トランスポートレイヤーセキュリティのAES暗号化スイート）
RFC 2365	Administratively Scoped IP Multicast（管理用スコープのIPマルチキャスト）
RFC 2578	SMIv2
RFC 2579	Textual Conventions for SMI v2（SMIv2のためのテキストの表記法）
RFC 2580	Conformance statements for SMI v2（SMIv2の適合宣言）
RFC 2613	SMON
RFC 2618	RADIUS Authentication Client MIB（RADIUS認証クライアントMIB）
RFC 2620	RADIUS Accounting MIB（RADIUSアカウンティングクライアントMIB）
RFC 2674	Dot1p/Q
RFC 2818	HTTP over TLS
RFC 2851	Internet Addresses MIB（インターネットアドレスMIB）
RFC 2863	The Interfaces Group MIB（インターフェイスグループMIB）
RFC 2865	RADIUS Client（RADIUSクライアント）
RFC 2866	RADIUS Accounting（RADIUSアカウンティング）

RFC 2868	RADIUS Attributes for Tunnel Protocol Support（トンネリングプロトコルサポートのRADIUSアトリビュート）
RFC 2869	RADIUS Extensions（RADIUS拡張機能）
RFC 2869bis	RADIUS support for EAP（EAP認証用RADIUSサポート）
RFC 2933	IGMP MIB
RFC 3164	The BSD Syslog Protocol（BSD Syslogプロトコル）
RFC 3376	IGMPv3
RFC 3410	Introduction and Applicability Statements for Internet Standard Management Framework（インターネット標準管理フレームワークの概要と適応方針）
RFC 3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks（簡易ネットワーク管理プロトコル（SNMP）管理フレームワークの表記アーキテクチャー）
RFC 3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)（SNMPのメッセージ処理とディスパッチ）
RFC 3413	Simple Network Management Protocol (SNMP) Applications（SNMPアプリケーション）
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)（SNMPv3のユーザーベースセキュリティモデル（USM））
RFC 3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)（SNMP用VACM）
RFC 3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)（SNMPのためのMIB）
RFC 3580	802.1X RADIUS Usage Guidelines（802.1X RADIUS使用ガイドライン）
RFC 3584	Coexistence between Version 1, Version 2, and Version 3 of the Internet- standard Network Management Framework（インターネット標準NMPフレームワークのVer.1 Ver.2 Ver.3の共存）
RFC 3621	Power Ethernet MIB（PoE MIB）
RFC 4022	Management Information Base for the Transmission Control Protocol (TCP)（TCPのためのMIB） RFC 4113
RFC 4113	Management Information Base for the User Datagram Protocol (UDP)（ユーザーデータグラムプロトコル（UDP）のためのMIB）
RFC 4188	Definitions of Managed Objects for Bridges（ブリッジのマネージドオブジェクトの定義）
RFC 4251	SSH protocol architecture（SSHプロトコルアーキテクチャー）
RFC 4291	IPv6 Addressing Architecture（IPv6アドレッシングアーキテクチャー））
RFC 4252	SSH authentication protocol（SSH認証プロトコル）
RFC 4253	SSH transport layer protocol（SSHトランスポート層プロトコル）
RFC 4254	SSH connection protocol（SSHコネクションプロトコル）
RFC 4293	Management Information Base for the Internet Protocol (IP)（インターネットプロトコルのためのMIB）
RFC 4318	Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol（ラピッドスパニングツリープロトコルとブリッジのための管理オブジェクトの定義）
RFC 4330	Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI（OSI用のSNTP Ipv4、IPv6のVer.4）
RFC 4363	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions（トラフィッククラス、マルチキャストフィルタリング、および仮想LAN拡張機能を持つブリッジのための管理オブジェクトの定義）
RFC 4541	Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches（IGMP及びMLDスヌーピングスイッチの検討）
RFC 4836	Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)（IEEE 802.3中型アタッチメントユニット（MAU）の管理対象オブジェクトの定義）
RFC 4861	Neighbor Discovery for IPv6（IPバージョン6の近隣探索（IPv6））
RFC 5321	Simple Mail Transfer Protocol（シンプルメール転送プロトコル）
RFC 6221	Leightweight DHCPv6 Relay Agent（軽量のDHCPv6リレーエージェント）
RFC 8200	IPv6 Specification（IPv6仕様）
RFC 8415	DHCPv6

B.3 基礎となるIEEE規格

IEEE 802.1AB	Station and Media Access Control Connectivity Discovery（ステーション及びメディアアクセスコントロールのコネクティビティディスカバリー）
IEEE 802.1D	MAC Bridges (switching function)（MACブリッジ（スイッチング機能））
IEEE 802.1Q	Virtual LANs (VLANs, MRP, Spanning Tree)（仮想LAN（VLAN、MRP、スパニングツリー） IEEE 802.1X
IEEE 802.1X	Port Authentication （ポート認証）
IEEE 802.3	Ethernet（イーサネット）
IEEE 802.3ac	VLAN Tagging（VLANタギング） IEEE 802.3x
IEEE 802.3X	Flow Control （フローコントロール）
IEEE 802.3af	Power over Ethernet（PoE）

B.4 基礎となるIEC規格

IEC 62439	High availability automation networks （高可用性オートメーションネットワーク）

B.5 基礎となるANSI規格

ANSI/TIA-1057	Link Layer Discovery Protocol for Media Endpoint Devices, April 2006 （メディアエンドポイントデバイスのLLDP、2006年4月）

B.6 技術資料

16.3.3 スイッチ

MACアドレステーブルサイズ（静的フィルター含む）	16384
静的に設定したMACアドレスフィルター最大数	100
IGMPスヌーピングを通してラーニング可能なMACアドレスフィルター最大数	1024
MAC アドレスエントリー（MMRP）最大数	64
優先キュー数	8キュー
設定可能なポート優先順位	0..7
MTU（ポートで送受信可能なパケットの最大許容長）	9720バイト

16.3.4 VLAN

VLAN ID範囲	1..4042
VLAN数	デバイス当たり、同時に最大128個 ポート当たり、同時に最大128個

16.3.5 ACL（アクセスコントロールリスト）

ACL最大数	50
ACL当たりの最大ルール数	256
ポート当たりの最大ルール数	256
設定可能なルール合計	2048 (8 × 256)
VLANアサイメント最大数	12
イベントログルールの最大数	128
イングレスルール最大数	514

B.7 統合ソフトウェアの著作権について

当製品には、第三者によって開発され、オープンソースソフトウェアとしてライセンスされたオープンソースソフトウェアファイルが含まれます。

ライセンスの規約はグラフィカルユーザーインターフェース内の*Help > Licenses* ダイアログボックスにあります。

B.8 略語一覧

ACL	Access Control List （アクセス コントロール　リスト）
BOOTP	Bootstrap Protocol（ブートストラップ プロトコル）
CLI	Command Line Interface（コマンド ライン　インターフェース）
DHCP	Dynamic Host Configuration Protocol（ダイナミック ホスト コンフィギュレーション プロトコル） DHCPv6
DUID	DHCP Unique Identifier（DHCPユニーク アイデンティファイア）
EUI	Extended Unique Identifier（エクステンデッド ユニーク アイデンティファイア）
FDB	Forwarding Database（フォワーディング データベース）
GUI	Graphical User Interface（グラフィカル ユーザー インターフェース）
HTTP	Hypertext Transfer Protocol（ハイパーテキスト トランスファー プロトコル）
HTTPS	Hypertext Transfer Protocol Secure（ハイパーテキスト トランスファー プロトコル セキュア）
ICMP	Internet Control Message Protocol（インターネット コントロール メッセージ プロトコル）
IEEE	Institute of Electrical and Electronics Engineers（米国電気電子学会）
IGMP	Internet Group Management Protocol（インターネット グループ マネジメント プロトコル）
IP	Internet Protocol（インターネット プロトコル）
IPv6	Internet Protocol version 6（インターネット プロトコル バージョン6）
LDRA	Lightweight DHCPv6 Relay Agent（ライトウェイト DHCPv6 リレー エージェント）
LED	Light Emitting Diode（発光ダイオード）
LLDP	Link Layer Discovery Protocol（リンク レイヤー ディスカバリー プロトコル）
MAC	Media Access Control（メディア アクセス コントロール）
MIB	Management Information Base（管理情報ベース）
MRP	Media Redundancy Protocol（メディア冗長プロトコル）
NDP	Neighbor Discovery Protocol（近隣探索プロトコル）
NMS	Network Management System（ネットワーク管理システム）
PC	Personal Computer（パーソナル コンピューター）
PTP	Precision Time Protocol（プリシジョン タイム プロトコル）
QoS	Quality of Service（クオリティ オブ サービス）
RFC	Request For Comment（リクエスト フォー コメンツ）
RM	Redundancy Manager（冗長マネジャー）
RSTP	Rapid Spanning Tree Protocol（ラピッド スパニングツリー プロトコル）
SCP	Secure Copy（セキュア コピー）
SFP	Small Form-factor Pluggable（スモール フォームファクター プラガブル）
SFTP	SSH File Transfer Protocol（SSH ファイル転送プロトコル）
SNMP	Simple Network Management Protocol（シンプル ネットワーク マネジメント プロトコル）
SNTP	Simple Network Time Protocol（シンプル ネットワーク タイム プロトコル）
TCP	Transmission Control Protocol（トランスミッション コントロール プロトコル）
TFTP	Trivial File Transfer Protocol（トリビアル ファイル トランスファー プロトコル）
TP	Twisted Pair（ツイストペア）
UDP	User Datagram Protocol（ユーザー データグラム プロトコル）

URL	Uniform Resource Locator（ユニフォーム リソース ロケーター）
UTC	Coordinated Universal Time（協定世界時）
VLAN	Virtual Local Area Network（仮想ローカル エリア ネットワーク）

C 索引

P

Q

R

S

T

U

V

W