# N8406-022 GbE インテリジェントスイッチ (L2)
# アプリケーションガイド

文書番号: 856-126757-101-00

2 版: 2007 年 10 月

- 著作権

- ご注意

  本書の内容は予告なく変更することがあります。NEC が製品やサービスについて行う保証は、添付の保証文書に記載の内容のみに限定します。本書のどの箇所であっても何ら新規の保証を行うものではありません。本書に技術的あるいは編集上の誤りや欠落があったとしても、NEC は一切の責任を負わないものとします。

- 商標

  Microsoft®、Windows®、および Windows NT®は、Microsoft Corporation の米国における登録商標です。

  SunOS™および Solaris™は、Sun Microsystems 社の米国およびその他の国における商標です。

  Cisco®は、Cisco Systems 社およびその系列会社の米国およびその他一部の国における登録商標です。

  文書番号: 856-126757-101-00

  2 版: 2007 年 10 月

# 目次

# スイッチへのアクセス

## はじめに

本書では、スイッチの設定、管理について説明します。個々の章は、概ね、機能の概要、使用例、構成方法の順に説明を行います。各章の概要は以下のとおりです。

- スイッチへのアクセス：IP ネットワーク経由でスイッチの設定や、情報、統計データを参照する方法について説明します。IP アドレスの設定方法や、RADIUS 認証、セキュアシェル (SSH) やセキュアコピー (SCP) を使用してスイッチに安全にアクセスする方法など、ネットワーク管理者がスイッチを管理する種々の方法も説明します。
- Ports and trunking：複数の物理ポートでトランクグループを構成し、帯域幅を広げる方法について説明します。
- VLAN：複数の仮想ローカルエリアネットワーク(VLAN) を構成し、ネットワークセグメントを分離する方法について説明します。
- Spanning Tree Protocol：複数の経路が存在するときにスイッチがもっとも効率的な経路を使用するようにネットワークを構成するスパニングツリーについて説明します。
- Rapid Spanning Tree Protocol／Multiple Spanning Tree Protocol：ネットワークトポロジが変化した際、早期に回復するために拡張されたスパニングツリープロトコルについて説明します。
- IGMP Snooping：マルチキャストにおいて IGMP を使用して帯域幅を確保する方法について説明します。
- Remote Monitoring：スイッチでネットワークのモニタリングデータを入手する、RMON エージェントを構成する方法について説明します。
- High Availability：ネットワークトポロジで高可用性を構成する方法について説明します。
- Troubleshooting tools：ポートミラーリングなどのトラブルシューティング方法について説明します。

## 関連マニュアル

本スイッチの実装方法、設定方法については、以下のマニュアルも参照してください。

- N8406-022 GbE インテリジェントスイッチ (L2)　ユーザーズガイド
- N8406-022 GbE インテリジェントスイッチ (L2)　コマンドリファレンスガイド (AOS)
- N8406-022 GbE インテリジェントスイッチ (L2)　コマンドリファレンスガイド (ISCLI)
- N8406-022 GbE インテリジェントスイッチ (L2)　ブラウザベースインタフェースリファレンスガイド

# 英字体および記号使用規約

次の表に、本ガイドの英字体および記号使用規約を示します。

表 1 英字体および記号使用規約

| 英字体または記号 | 意味 | 例 |
|---|---|---|
| AaBbCc123 | 画面上のコンピュータ出力かプロンプトを示します。 | Main# |
| AaBbCc123 | コマンド例または正確に入力しなければならない語句を示します。 | Main# sys |
| <AaBbCc123> | コマンドのパラメータを示します。実際のコマンドでは名前や値を指定します。< > は不要です。 | Telnet セッションを確立するのであれば、次のように入力します。<br>host# telnet <IP address> |
| | ガイドのタイトル、特殊用語、強調したい語句などに使用することもあります。 | ユーザーズガイドを参照してください。 |
| [ ] | コマンドで、鍵括弧で囲まれた項目はオプションです。必要に応じて入力します。[] は不要です。 | host# ls [-a] |

# マネジメントネットワーク

GbE インテリジェントスイッチ (L2) は、ブレード収納ユニットに実装されるスイッチモジュールです。ブレード収納ユニットには EM カードも実装され、ブレード収納ユニットの中に実装されるモジュールや CPU ブレードの管理を行います。

本スイッチはマネジメントポート (Port 19) を通じて EM カードと通信します。工場デフォルト設定では、マネジメントポートの 10/100Mbps イーサネットポート、もしくはシリアルポートを通じてスイッチの管理を行うことができます。本スイッチの管理に外部のイーサネットポートを使用することもできます。

本スイッチのマネジメントネットワークには以下の特徴があります。

- ポート 19 — 管理ポート 19 は次のように設定されています。
  - フロー制御：両方向
  - オートネゴシエーション
  - タグなし
  - ポート VLAN ID (PVID): 4095
- VLAN4095 — マネジメント用の VLAN で本スイッチ内の管理トラフィックを分離します。メンバポートはポート 19 のひとつだけです。他のポートを VLAN4095 のメンバにすることはできません。
- インタフェース 256 — マネジメント用のインタフェースです。インタフェース 256 は VLAN4095 と関連付けられています。他のインタフェースを VLAN4095 と関連付けることはできません。インタフェース 256 の IP アドレスは手動または DHCP により設定できます。
- ゲートウェイ 4 — マネジメントインタフェース（インタフェース 256）用のデフォルトゲートウェイです。
- STG32 — 複数のスパニングツリーを使用するように本スイッチを構成した場合、マネジメント VLAN4095 はスパニングツリーグループ 32 (STG32) にありますが、他の VLAN を追加することはできません。STG32 のデフォルトはオフです。RSTP を使用する場合、VLAN4095 は STG1 に移動します。

本スイッチのマネジメントインタフェースにアクセスするには、下記のどちらかで IP アドレスを割り当てます。

- EM カード内の DHCP サーバより IP アドレスを割り当てます。
- 手動で IP アドレスを本スイッチのマネジメントインタフェース（インタフェース 256）に割り当てます。

## シリアルポート経由の接続

シリアルケーブルを接続しシリアルポートを通じてスイッチに直接接続できます。Telnet などのリモートアクセスアプリケーションを使用するためには、コンソール接続が必要です。コンソールをスイッチに接続する方法については、「ユーザーズガイド」を参照してください。

## Telnet 経由の接続

デフォルトで、Telnet が有効になっています。IP パラメータを設定すれば、Telnet によりネットワーク経由で CLI にアクセスできます。Telnet アクセスには、シリアルポートを通じて利用できるコマンドと同じものが、ユーザとアドミニストレータに用意されています（一部のコマンドを除きます）。Telnet は同時に 4 つまで接続できます。

スイッチと Telnet 接続するには、ワークステーションで Telnet プログラムを実行し、次のように、スイッチの IP アドレスを付けた telnet コマンドを発行します。

```
telnet <switch IP address>
```

## セキュアシェル経由の接続

デフォルトで、セキュアシェル (SSH) プロトコルは無効です。SSH を利用すると、ネットワーク経由で別のコンピュータにログインして、コマンドをリモートで実行できます。SSH は、ネットワーク上で転送されるすべてのデータを暗号化して保護します。詳細については、本章で後述する「セキュアシェルとセキュアコピー」を参照してください。CLI の詳細については、「コマンドリファレンスガイド」を参照してください。

# コマンドラインインタフェースの使用法

コマンドラインインタフェース (CLI) は、シリアルコンソール接続か、Telnet または SSH を用いたリモートセッションによりアクセスできます。

本スイッチには CLI モードが 2 つあります。メニューベースの AOS CLI とツリーベースの ISCLI です。どちらか一方を選択して使用します。

アドミニストレータ権限でログインした時の AOS CLI のメインメニューを次に示します。

```
[Main Menu]
      info    - Information Menu
      stats   - Statistics Menu
      cfg     - Configuration Menu
      oper    - Operations Command Menu
      boot    - Boot Options Menu
      maint   - Maintenance Menu
      diff    - Show pending config changes  [global command]
      apply   - Apply pending config changes [global command]
      save    - Save updated config to FLASH [global command]
      revert  - Revert pending or applied changes [global command]
      exit    - Exit  [global command, always available]
```

AOS CLI の詳細については、「コマンドリファレンスガイド (AOS) 」を参照してください。

ISCLI はツリーベースのコマンド構造です。ISCLI コマンドの一例を次に示します。

```
Switch(config)# spanning-tree stp 1 enable
```

ISCLI の詳細については、「コマンドリファレンスガイド (ISCLI) 」を参照してください。

## IP インタフェースの設定

ネットワーク経由でスイッチにアクセスするためには、スイッチに IP アドレスを設定する必要があります。デフォルトでは、EM カード上の DHCP サーバに IP アドレスを要求するように設定されており、割り当てられた IP アドレスはマネジメントインタフェースに設定されます。

IP アドレスを手動で設定する場合、設定例を以下に示します。

1. 例として、インタフェース 256 に IP アドレス 205.21.17.3 を設定します。
2. サブネットマスクとブロードキャストアドレスは自動で計算されます。

```
>> # /cfg/l3/if 256                 (Select IP interface 256)
>> IP Interface 256# addr 205.21.17.3(Assign IP address for the interface)
Current IP address:     0.0.0.0
New pending IP address: 205.21.17.3
Pending new subnet mask: 255.255.255.0
. . . . . .
>> IP Interface 256# ena              (Enable IP interface 256)
```

3. 必要に応じて、デフォルトゲートウェイを設定します。
4. デフォルトゲートウェイを設定すると、スイッチからルータにトラフィックを送出できます。

```
>> IP Interface 256# ../gw 4            (Select default gateway 4)
>> Default gateway 4# addr 205.21.17.1  (Assign IP address for a router)
>> Default gateway 4# ena               (Enable default gateway 4)
```

5. 設定を適用、保存、確認します。

```
>> Default gateway 4# apply            (Apply the configuration)
>> Default gateway 4# save             (Save the configuration)
>> # /cfg/dump                         (Verify the configuration)
```

# ブラウザベースインタフェースの使用法

デフォルトでは、ブラウザベースインタフェース(BBI)は有効になっています。Web ブラウザでスイッチの設定、管理機能などにアクセスします。詳細については「ブラウザベースインタフェースリファレンスガイド」を参照してください。

BBI は、次のように、構成されています。

- Configuration — 以下のメニューで、スイッチ内の設定項目にアクセスします。
  - System — システム関連の項目を設定します。
  - Switch ports — スイッチポートと関連の機能を構成します。
  - Port-based port mirroring — ミラーリングするポートとモニタリングするポートを設定します。
  - Layer 2 — トランクグループ、VLAN、スパニングツリープロトコルなど、レイヤ 2 機能を設定します。
  - RMON — RMON 機能を設定します。
  - Layer 3 — IGMP スヌーピングなど、IP 関連情報のすべてを設定します。
  - Uplink Failure Detection — Link to Monitor (LtM) と Link to Disable（LtD）の Failure Detection Pair を設定します。
- Statistics — 配下のメニューで、スイッチの統計情報、ステータス情報にアクセスします。
- Dashboard — 配下のメニューで、各種スイッチ機能の設定状態、動作状態を表示します。

# SNMP の使用法

本スイッチは SNMP v1.0 と SNMP v3.0 をサポートしています。

## SNMP v1.0

SNMP エージェントにアクセスするためには、SNMP マネージャで Read と Write のコミュニティ名を設定して、スイッチ側の設定と一致させる必要があります。デフォルトの Read コミュニティ名は `public`、Write コミュニティ名は `private` です。

CLI で次のコマンドを使用すれば、スイッチの read/write コミュニティ名を変更できます。

```
>> /cfg/sys/ssnmp/rcomm
```

および

```
>> /cfg/sys/ssnmp/wcomm
```

SNMP マネージャは、スイッチのマネジメントインタフェースか IP インタフェースのどれか 1 つにアクセスできます。

スイッチの SNMP エージェントが送出するトラップを SNMP マネージャが受信する場合、トラップホストを次のコマンドで設定する必要があります。

```
/cfg/sys/ssnmp/snmpv3/taddr
```

詳細については、「SNMP トラップホストの設定」を参照してください。

## SNMP v3.0

SNMPv3 は SNMP の拡張バージョンで、2002 年 3 月に Internet Engineering Steering Group によって承認されたものです。認証、データ保全性チェック、適時性インジケータ、暗号化を行い、マスカレード、情報改変、メッセージストリーム改変、ディスクロージャなどの脅威から保護します。

SNMP v3 は、主にセキュリティのために使用します。

SNMP v3.0 メニューにアクセスするには、AOS CLI に次のコマンドを入力します。

```
>> #  /cfg/sys/ssnmp/snmpv3
```

SNMP MIB の詳細およびスイッチでの SNMP 設定用コマンドについては、「コマンドリファレンスガイド」を参照してください。

## デフォルト設定

スイッチソフトウェアにはデフォルトで 2 組のユーザが設定されています。'adminmd5' と 'adminsha' の 2 ユーザで、スイッチがサポートする MIB のすべてにアクセスできます。

1. ユーザ名 1: `adminmd5/password adminmd5`。使用する認証は MD5 です。
2. ユーザ名 2: `adminsha/password adminsha`。使用する認証は SHA です。
3. ユーザ名 3: `v1v2only/password none.`

SNMP ユーザ名を設定する場合、AOS CLI から次のコマンドを入力します。

```
>> #  /cfg/sys/ssnmp/snmpv3/usm 6
```

## ユーザ設定

ユーザを設定して、認証／プライバシオプションを使用できます。現在、MD5 と SHA の 2 つの認証アルゴリズムをサポートしています。コマンド`/cfg/sys/ssnmp/snmpv3/usm <x>/auth md5|sha` により指定できます。

1. 名前'test'、認証タイプ MD5、認証パスワード'test'のユーザ、プライバシパスワード'test'のプライバシオプション DES を設定する場合、次の AOS CLI コマンドを入力します。

```
>> # /cfg/sys/ssnmp/snmpv3/usm 5
>> SNMPv3 usmUser 5 # name "test"
>> SNMPv3 usmUser 5 # auth md5
>> SNMPv3 usmUser 5 # authpw test
>> SNMPv3 usmUser 5 # priv des
>> SNMPv3 usmUser 5 # privpw test
```

2. ユーザ設定時、そのユーザのアクセスレベルを、ユーザがアクセスできるビューとともに指定する必要があります。指定先はアクセステーブルです。

```
>> # /cfg/sys/ssnmp/snmpv3/access 5
>> SNMPv3 vacmAccess 5 # name "testgrp"
>> SNMPv3 vacmAccess 5 # level authPriv
>> SNMPv3 vacmAccess 5 # rview "iso"
>> SNMPv3 vacmAccess 5 # wview "iso"
>> SNMPv3 vacmAccess 5 # nview "iso"
```

3. グループテーブルでユーザを特定のアクセスグループにリンクします。

```
>> # /cfg/sys/ssnmp/snmpv3/group 5
>> SNMPv3 vacmSecurityToGroup 5 # uname test
>> SNMPv3 vacmSecurityToGroup 5 # gname testgrp
```

ユーザが特定の MIB にしかアクセスできないようにする場合、次の「ビューベース設定」を参照してください。

# ビューベース設定

## user と同等設定

SNMP ユーザを CLI の user (ユーザ) と同等の権限で設定する場合、以下の設定を行います。

```
/c/sys/ssnmp/snmpv3/usm 4
name "usr"
/c/sys/ssnmp/snmpv3/access 3
name "usrgrp"
rview "usr"
wview "usr"
nview "usr"
/c/sys/ssnmp/snmpv3/group 4
uname usr
gname usrgrp
/c/sys/ssnmp/snmpv3/view 6
name "usr"
tree " 1.3.6.1.4.1.11.2.3.7.11.33.1.2.1.2"
/c/sys/ssnmp/snmpv3/view 7
name "usr"
tree " 1.3.6.1.4.1.11.2.3.7.11.33.1.2.1.3"
/c/sys/ssnmp/snmpv3/view 8
name "usr"
tree " 1.3.6.1.4.1.11.2.3.7.11.33.1.2.2.2"
/c/sys/ssnmp/snmpv3/view 9
name "usr"
tree " 1.3.6.1.4.1.11.2.3.7.11.33.1.2.2.3"
/c/sys/ssnmp/snmpv3/view 10
name "usr"
tree " 1.3.6.1.4.1.11.2.3.7.11.33.1.2.3.2"
/c/sys/ssnmp/snmpv3/view 11
name "usr"
tree " 1.3.6.1.4.1.11.2.3.7.11.33.1.2.3.3"
```

## oper と同等設定

SNMP ユーザを CLI の oper (オペレータ) と同等の権限で設定する場合、以下の設定を行います。

```
/c/sys/ssnmp/snmpv3/usm 5
name "oper"
/c/sys/ssnmp/snmpv3/access 4
name "opergrp"
rview "oper"
wview "oper"
nview "oper"
/c/sys/ssnmp/snmpv3/group 4
uname oper
gname opergrp
/c/sys/ssnmp/snmpv3/view 20
name "oper"
tree " 1.3.6.1.4.1.11.2.3.7.11.33.1.2.1.2"
/c/sys/ssnmp/snmpv3/view 21
name "oper"
tree " 1.3.6.1.4.1.11.2.3.7.11.33.1.2.1.3"
/c/sys/ssnmp/snmpv3/view 22
name "oper"
tree " 1.3.6.1.4.1.11.2.3.7.11.33.1.2.2.2"
/c/sys/ssnmp/snmpv3/view 23
name "oper"
tree " 1.3.6.1.4.1.11.2.3.7.11.33.1.2.2.3"
/c/sys/ssnmp/snmpv3/view 24
name "oper"
tree " 1.3.6.1.4.1.11.2.3.7.11.33.1.2.3.2"
/c/sys/ssnmp/snmpv3/view 25
name "oper"
tree " 1.3.6.1.4.1.11.2.3.7.11.33.1.2.3.3"
```

# SNMP トラップホストの設定

## SNMPv1 トラップホスト

1. 認証、パスワードなしでユーザを設定します。

```
/c/sys/ssnmp/snmpv3/usm 10
name "v1trap"
```

2. ユーザのアクセスグループとグループテーブルを設定します。コマンド `/c/sys/ssnmp/snmpv3/access <x>/nview` により、ユーザが受信できるトラップを指定できます。次の例では、スイッチが送信したトラップを受信します。

```
/c/sys/ssnmp/snmpv3/access 10
name "v1trap"
model snmpv1
nview "iso"
/c/sys/ssnmp/snmpv3/group 10
model snmpv1
uname v1trap
gname v1trap
```

3. 通報テーブルにエントリを設定します。

```
/c/sys/ssnmp/snmpv3/notify 10
name v1trap
tag v1trap
```

4. ターゲットアドレステーブルとターゲットパラメータテーブルに IP アドレスとその他のトラップパラメータを指定します。コマンド `c/sys/ssnmp/snmpv3/tparam <x>/uname` により、ターゲットパラメータテーブルで使用するユーザ名を指定します。

```
/c/sys/ssnmp/snmpv3/taddr 10
name v1trap
addr 47.80.23.245
taglist v1trap
pname v1param
/c/sys/ssnmp/snmpv3/tparam 10
name v1param
mpmodel snmpv1
uname v1trap
model snmpv1
```

5. コミュニティテーブルを用いて、トラップに使用するコミュニティ名を指定します。

```
/c/sys/ssnmp/snmpv3/comm 10
index v1trap
name public
uname v1trap
```

## SNMPv2 トラップホストの設定

SNMPv2 トラップホスト設定は、SNMPv1 トラップホスト設定と同様です。ただ、モデルを指定するときに、snmpv1 ではなく、snmpv2 にする必要があります。

```
c/sys/ssnmp/snmpv3/usm 10
        name "v2trap"
/c/sys/ssnmp/snmpv3/access 10
        name "v2trap"
        model snmpv2
        nview "iso"
/c/sys/ssnmp/snmpv3/group 10
        model snmpv2
        uname v2trap
        gname v2trap
/c/sys/ssnmp/snmpv3/taddr 10
        name v2trap
        addr 47.81.25.66
        taglist v2trap
        pname v2param
/c/sys/ssnmp/snmpv3/tparam 10
        name v2param
        mpmodel snmpv2c
        uname v2trap
        model snmpv2
/c/sys/ssnmp/snmpv3/notify 10
        name v2trap
        tag v2trap
/c/sys/ssnmp/snmpv3/comm 10
        index v2trap
        name public
        uname v2trap
```

### SNMPv3 トラップホストの設定

SNMPv3 トラップ用にユーザを設定する場合、プライバシと認証の両方があるトラップ、認証だけのトラップ、プライバシか認証がないトラップのいずれかの送信を選択できます。

コマンド/c/sys/ssnmp/snmpv3/access <x>/level、/c/sys/ssnmp/snmpv3/tparam <x>によりアクセステーブルに設定します。ユーザの設定はユーザテーブルに設定します。

SNMPv3 トラップではコミュニティ名を使用しないためコミュニティテーブルは必要ありません。

次は、認証だけの SNMPv3 ユーザ v3trap を設定する例です。

```
/c/sys/ssnmp/snmpv3/usm 11
        name "v3trap"
        auth md5
        authpw v3trap
/c/sys/ssnmp/snmpv3/access 11
        name "v3trap"
        level authNoPriv
        nview "iso"
/c/sys/ssnmp/snmpv3/group 11
        uname v3trap
        gname v3trap
/c/sys/ssnmp/snmpv3/taddr 11
        name v3trap
        addr 47.81.25.66
        taglist v3trap
        pname v3param
/c/sys/ssnmp/snmpv3/tparam 11
        name v3param
        uname v3trap
        level authNoPriv
/c/sys/ssnmp/snmpv3/notify 11
        name v3trap
        tag v3trap
```

SNMP のコマンドの使用方法の詳細については「コマンドリファレンスガイド」を参照してください。

# セキュアなスイッチアクセス

インターネットを介した重要な管理機能の実行環境には、スイッチに安全にアクセスする必要があります。安全に管理するために必要な機能を次に示します。

- 管理ユーザからのアクセスを特定の IP アドレスレンジに限定。次項の「管理ネットワークの設定」を参照してください。
- リモート経由で管理ユーザの認証と権限付与。本章で後述の「RADIUS 認証」、「TACACS+認証」を参照してください。
- リモート経由で管理ユーザからスイッチに暗号化してアクセスします。本章で後述の「セキュアシェルとセキュアコピー」を参照してください。

## 管理ネットワークの設定

各ポートにフィルタを付けずに、スイッチへのアクセスを制限するには、Telnet、SSH、SNMP、 またはスイッチのブラウザベースインタフェース (BBI) を通じてスイッチのソース IP アドレス（またはレンジ）を設定します。

IP パケットがスイッチに達すると、管理ネットワークアドレスと管理ネットマスクで定義したアドレスレンジを元にソース IP アドレスをチェックします。ホストのソース IP アドレスがそのレンジ内にあると、ログインを行うことができます。パケットがスイッチの IP インタフェースに達しても、ソース IP アドレスがレンジ外ならば廃棄されます。

### 管理ネットワークの IP アドレスレンジの設定

管理ネットワークの IP アドレスとマスクは、次の例に示すように、AOS CLI の System メニューから設定します。

```
>> Main# /cfg/sys/access/mgmt/add
Enter Management Network Address: 192.192.192.0
Enter Management Network Mask:  255.255.255.128
```

この例では、管理ネットワークアドレスを 192.192.192.0、管理ネットマスクを 255.255.255.128 に設定しています。これから、IP アドレスの許容レンジは、192.192.192.1～192.192.192.127 になります。

スイッチへのアクセスが認められるソース IP アドレスと、認められないソース IP アドレスは次の通りです。

- ソース IP アドレスが 192.192.192.21 のホストは設定レンジ内のためアクセスできます。
- 192.192.192.192 のホストは設定レンジ外のためアクセスできません。このソース IP アドレスを有効にするには、管理ネットワークアドレス、管理ネットマスクで指定した有効レンジ内の IP アドレスをシフトするか、管理ネットワークアドレスを 192.192.192.128、管理ネットマスクを 255.255.255.128 に変更します。これで、192.192.192.192 のホストは、管理ネットワークアドレスと管理ネットマスクで決まる有効レンジ（192.192.192.128～255）内に入ります。

## RADIUS 認証と権限付与

リモート経由でユーザがスイッチにアクセスする際、ユーザを認証し、権限を付与する RADIUS 認証をサポートします。リモートアクセスサーバ (RAS) — スイッチ — は、バックエンドデータベースサーバ — RADIUS サーバ — の 1 クライアントです。管理ユーザは RAS にだけアクセスして、バックエンドサーバにはアクセスしません。

RADIUS 認証は以下のコンポーネントからなります。

- RFC 2138、2866 に基づいて、UDP を利用するフレームフォーマットを有するプロトコル
- すべてのユーザ認証情報を格納する中央サーバ
- クライアント（スイッチ）

スイッチが RADIUS クライアントとして機能する場合、RADIUS サーバと通信して、RFC 2138、2866 に定められたプロトコルにより、ユーザを認証、権限付与します。クライアントと RADIUS サーバの間のトランザクションの認証は、ネットワークに送出しない共有キーで行います。また、スイッチ（RADIUS クライアント）とバックエンド RADIUS サーバの間で、暗号化したユーザパスワードを転送します。

### RADIUS 認証の方法

RADIUS 認証は次のように行われます。

1. ユーザがスイッチに接続し、ユーザ名とパスワードを送信します。
2. 認証／権限付与プロトコルにより、スイッチから認証サーバにリクエストを出します。
3. 認証サーバがユーザ ID データベースに基づいてリクエストをチェックします。
4. RADIUS プロトコルにより、認証サーバが管理アクセスを許可または拒否するようスイッチに指示します。

## スイッチでの RADIUS の設定（AOS CLI の例）

スイッチで RADIUS を設定する手順は次のとおりです。

1. RADIUS 認証をオンにして、次の例に示すように、プライマリとセカンダリの RADIUS サーバを設定します。

```
>> Main# /cfg/sys/radius                (Select the RADIUS Server menu)
>> RADIUS Server# on                     (Turn RADIUS on)
Current status: OFF
New status:     ON
>> RADIUS Server# prisrv 10.10.1.1      (Enter primary server IP)
Current primary RADIUS server:     0.0.0.0
New pending primary RADIUS server: 10.10.1.1
>> RADIUS Server# secsrv 10.10.1.2      (Enter secondary server IP)
Current secondary RADIUS server:     0.0.0.0
New pending secondary RADIUS server: 10.10.1.2
```

2. RADIUS サーバのプライマリとセカンダリのシークレットを設定します。

```
>> RADIUS Server# secret
Enter new RADIUS secret: <1-32 character secret>
>> RADIUS Server# secret2
Enter new RADIUS second secret: <1-32 character secret>
```

**注意：シリアルコンソール以外の方法で接続して RADIUS シークレットを設定すると、平文でネットワーク上に転送される可能性があります。**

3. 必要ならば、RADIUS で使用するデフォルトの UDP ポート番号を変更します。
4. RADIUS 用にウェルノンポートは 1645 です。

```
>> RADIUS Server# port
Current RADIUS port: 1645
Enter new RADIUS port [1500-3000]: <port number>
```

5. RADIUS サーバにリトライする回数とタイムアウト時間を設定します。

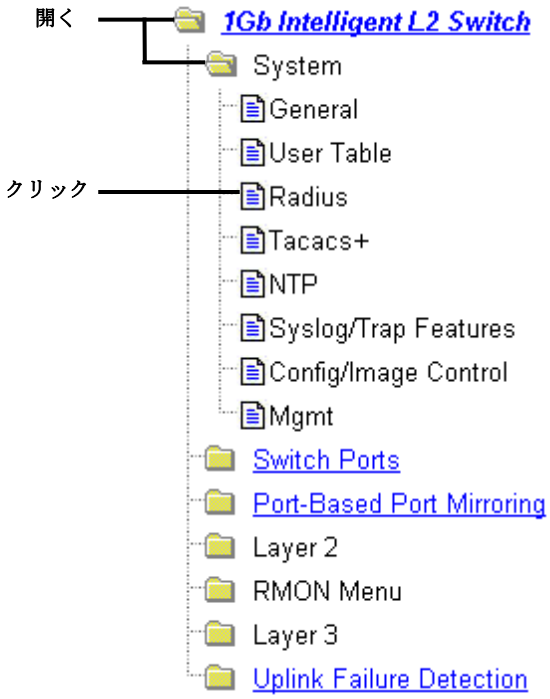
```
>> RADIUS Server# retries
Current RADIUS server retries: 3
Enter new RADIUS server retries [1-3]:<server retries>
>> RADIUS Server# time
Current RADIUS server timeout: 3
Enter new RADIUS server timeout [1-10]: 10  (Enter the timeout period
                                             in seconds)
```

6. 設定を適用、保存します。

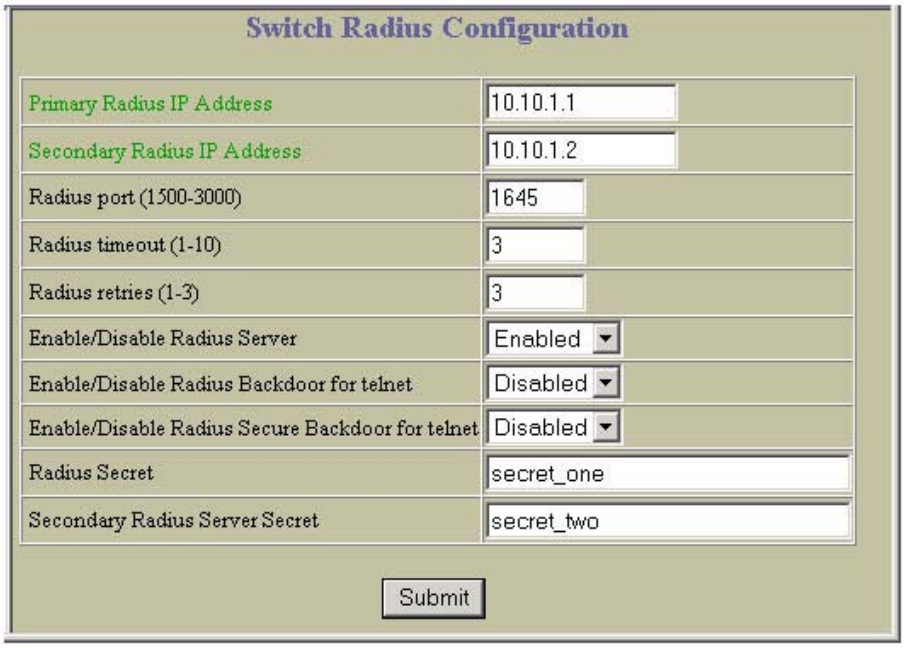
```
>> RADIUS Server# apply
>> RADIUS Server# save
```

## スイッチでの RADIUS の構成（BBI の例）

1. RADIUS パラメータを設定します。
   a. CONFIGURE ボタンをクリックします。
   b. System フォルダを開き、Radius を選択します。



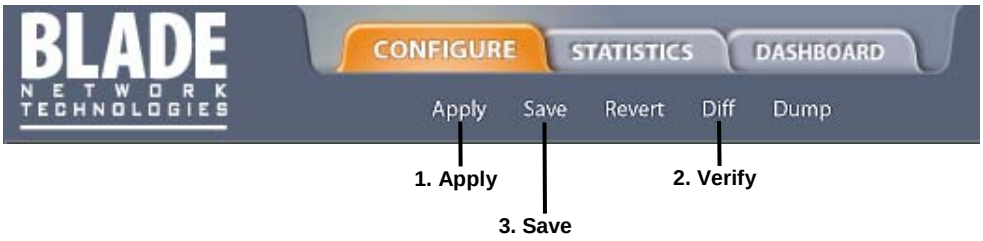

   c. プライマリ RADIUS サーバとセカンダリ RADIUS サーバの IP アドレス、各サーバの RADIUS シークレットを入力し、RADIUS サーバを有効にします。




注意：シリアルコンソール以外の方法で接続して RADIUS シークレットを設定すると、平文でネットワーク上に転送される可能性があります。

   d. Submit をクリックします。

2. 設定を適用、確認、保存します。




## RADIUS 認証機能

スイッチは以下の RADIUS 認証機能をサポートします。

- RFC 2138 と RFC 2866 のプロトコル定義に基づいて、RADIUS クライアントをサポートします。
- 32 バイトまでの RADIUS シークレットパスワードが可能です。
- セカンダリ認証サーバをサポートします。つまり、プライマリ認証サーバから応答がない場合、クライアント認証リクエストをセカンダリ認証サーバに送信できます。現在アクティブな RADIUS 認証サーバを調べる場合、`/cfg/sys/radius/cur` コマンドを使用します。
- RADIUS サーバのリトライ回数、タイムアウト値をユーザが設定できます。
  - タイムアウト値 = 1～10 秒
  - リトライ回数 = 1～3
- 1～3 回のリトライで RADIUS サーバから応答がないと、タイムアウトします。
- RADIUS アプリケーションポートをユーザが設定できます。デフォルトは、RFC2138 に基づいて、UDP/1645 ポート、ポート 1812 もサポートしています。

## RADIUS ユーザのユーザアカウント

次の表のユーザアカウントは RADIUS サーバに定義できます。

表2 ユーザアクセスレベル

| ユーザアカウント | 説明および実行する処理 |
|---|---|
| ユーザ | スイッチ統計データ、現在の状態を参照できますが、スイッチの設定を変更することはできません。 |
| オペレータ | スイッチの設定を変更することができますが、スイッチをリセットすると変更は解除されます。デフォルトでは、オペレータアカウントは無効で、パスワードはありません。 |
| アドミニストレータ | スイッチのすべての設定を行うことができます。 |

## ユーザ特権の RADIUS アトリビュート

ユーザがログインすると、スイッチは、RADIUS アクセスリクエストつまりクライアント認証リクエストを RADIUS 認証サーバに送り、アクセスのレベルを認証します。

認証サーバがリモートユーザの認証に成功すると、リモートユーザの特権を検証して、該当のアクセスを認めます。アドミニストレータであれば、コンソールポートだけ、またはコンソールと Telnet/SSH/HTTP/HTTPS アクセスを通じてバックドアアクセスを行うことができます。バックドアアクセスが有効であると、一次と二次の認証サーバに到達できればアクセスが可能です。一次と二次の両方の認証サーバに到達できない場合のみ、コンソールポートだけ、またはコンソールと Telnet/SSH/HTTP/HTTPS アクセスを通じてセキュアバックドア (secbd) アクセスを行うことができます。RADIUS がオンの場合、バックドアとセキュアバックドアのどちらかを有効にできます。両方同時にはできません。コンソールポートだけによるバックドアアクセスのデフォルト値は `enabled` です。バックドア／セキュアバックドアが有効か否かに関わらず、`noradius` とアドミニストレータパスワードにより、コンソールポートを介してスイッチに必ずアクセスできます。Telnet/SSH/HTTP/HTTPS を介したバックドアアクセス、セキュアバックドアアクセスのデフォルト値は `disabled` です。

ユーザ特権は、アドミニストレータに割り当てたものを除き、RADIUS サーバに定義しなければなりません。すべての RADIUS サーバに組み込まれる RADIUS アトリビュート 6 でアドミニストレータを規定します。定義ファイル名は RADIUS ベンダによります。次の表に示す RADIUS アトリビュートがユーザ特権レベル用に定義されています。

表3 RADIUS のアトリビュート

| ユーザ名／アクセス | ユーザサービスタイプ | 値 |
|---|---|---|
| ユーザ | ベンダ指定 | 255 |
| オペレータ | ベンダ指定 | 252 |

# TACACS+認証

スイッチは、Cisco Systems 社の TACACS+プロトコルを用いたネットワークで、認証、特権付与、アカウンティングをサポートします。リモートクライアントと連携し、TACACS+アクセスサーバによる認証セッション、特権付与セッションを開始することにより、ネットワークアクセスサーバ (NAS) として機能します。リモートユーザを、データポートか管理ポートを通じてスイッチに管理アクセスするユーザとして定義します。

TACACS+には RADIUS よりも以下のような利点があります。

- TCP ベースの接続指向トランスポートを使用します。RADIUS は UDP ベースです。TCP は接続指向型ですが、UDP はベストエフォート型です。RADIUS では、ベストエフォートトランスポートを補うため、再転送指向、タイムアウトなどのプログラマブル変数の追加が必要ですが、TCP トランスポートのような組込みサポートがありません。
- フルパケット暗号化を行います。RADIUS は認証リクエストでパスワードだけ暗号化します。
- 認証、権限付与、アカウンティングを分離します。

## TACACS+認証の方法

TACACS+の認証は RADIUS とほぼ同様です。

1. リモートアドミニストレータがスイッチに接続し、ユーザ名とパスワードを指定します。

   **注:ユーザ名、パスワードは最大 128 文字までです。パスワードを空白のままにすることはできません。**

2. 認証／権限付与プロトコルにより、スイッチから認証サーバにリクエストを送信します。
3. 認証サーバがユーザ ID データベースに基づいてリクエストをチェックします。
4. TACACS+プロトコルにより、管理アクセスを許可するか、拒否するかをスイッチに指示します。

セッション中に、新たに認証チェックが必要になると、スイッチが TACACS+サーバを調べて、特定のコマンドの使用をユーザに許可するかどうかを決めます。

## TACACS+認証機能

認証はユーザの身元を確認する処理で、通常、ユーザがはじめて装置にログインしようとしたときや、装置の機能にアクセスしようとしたときに行います。スイッチは、装置への ASCII インバウンドログインをサポートします。PAP、CHAP、ARAP ログイン、TACACS+変更パスワードリクエスト、ワンタイムパスワード認証はサポートしていません。

## 権限付与

権限付与は、ユーザが装置に対してもつ特権を決める処理で、通常、認証後に行います。

TACACS+認証特権レベルとスイッチ管理アクセスレベルの間のデフォルトマッピングを、次の表に示します。表にリストされている特権レベルを、TACACS+サーバで定義しなければなりません。

表4 デフォルト TACACS+特権レベル

| ユーザアクセスレベル | TACACS+レベル |
|---|---|
| user (ユーザ) | 0 |
| oper (オペレータ) | 3 |
| admin (アドミニストレータ) | 6 |

TACACS+特権レベルと本スイッチの管理アクセスレベルの間の指定マッピングを、次の表に示します。TACACS+特権レベルを指定するには、コマンド`/cfg/sys/tacacs/cmap ena` を用います。

表5 指定 TACACS+特権レベル

| ユーザアクセスレベル | TACACS+レベル |
|---|---|
| user (ユーザ) | 0～1 |
| oper (オペレータ) | 6～ 8 |
| admin (アドミニストレータ) | 14～15 |

TACACS+特権レベルと本スイッチの管理アクセスレベルの間のマッピングをカスタマイズできます。各 TACACS+特権レベル（0～15）を対応する本スイッチの管理アクセスレベル (user、oper、admin、none) に手動でマッピングするには、`/cfg/sys/tacacs/usermap` コマンドを使用します。

リモートユーザを認証サーバが認証すると、本スイッチがユーザの特権を確認して、該当のアクセス権を認めます。一次と二次の両方の認証サーバが到達できないと、アドミニストレータは、コンソールだけ、もしくはコンソールと Telnet アクセスを介してバックドアアクセスできます。デフォルトは Telnet アクセスは無効、コンソールアクセスは有効です。また、アドミニストレータはセキュアバックドア (/cfg/sys/tacacs/secbd) を有効にして、一次と二次の両方の TACACS+サーバが応答できない場合でもアクセスできます。

## アカウンティング

課金やセキュリティのために、装置でのユーザの活動を記録する処理です。認証、権限付与の処理に基づきます。認証や権限付与を TACACS+で実行しなければ、TACACS+アカウンティングメッセージは送出されません。

TACACS+では、ソフトウェアログイン、設定変更、対話型コマンドなどの記録、追跡を行うことができます。

スイッチは以下の TACACS+アカウンティングアトリビュートをサポートします。

- プロトコル (console/telnet/ssh/http)
- 開始時間
- 終了時間
- 経過時間

> **注:ブラウザベースインタフェースの場合、TACACS+アカウンティング停止記録が送信されるのは、ブラウザの Quit ボタンをクリックしたときだけです。**

## スイッチでの TACACS+認証の設定（AOS CLI の例）

1. TACACS+認証をオンにして、プライマリとセカンダリの TACACS+サーバを設定します。

```
>> Main# /cfg/sys/tacacs              (Select the TACACS+ Server menu)
>> TACACS+ Server# on                 (Turn TACACS+ on)
Current status: OFF
New status: ON
>> TACACS+ Server# prisrv 10.10.1.1  (Enter primary server IP)
Current primary TACACS+ server: 0.0.0.0
New pending primary TACACS+ server: 10.10.1.1
>> TACACS+ Server# secsrv 10.10.1.2  (Enter secondary server IP)
Current secondary TACACS+ server: 0.0.0.0
New pending secondary TACACS+ server: 10.10.1.2
```

2. TACACS+サーバのプライマリとセカンダリのシークレットを設定します。

```
>> TACACS+ Server# secret
Enter new TACACS+ secret: <1-32 character secret>
>> TACACS+ Server# secret2
Enter new TACACS+ second secret: <1-32 character secret>
```

**注意：シリアルコンソール以外の方法で接続して TACACS+シークレットを設定すると、平文でネットワークに転送される可能性があります。**

3. 必要ならば、TACACS+で使用するデフォルト TCP ポート番号を変更できます。
4. TACACS+用にウェルノーンポートは 49 です。

```
>> TACACS+ Server# port
Current TACACS+ port: 49
Enter new TACACS+ port [1-65000]: <port number>
```

5. TACACS+サーバへのリトライ回数とタイムアウトを設定します。

```
>> TACACS+ Server# retries
Current TACACS+ server retries: 3
Enter new TACACS+ server retries [1-3]: 2
>> TACACS+ Server# time
Current TACACS+ server timeout: 5
Enter new TACACS+ server timeout [4-15]: 10 (Enter the timeout period
                                             in minutes)
```

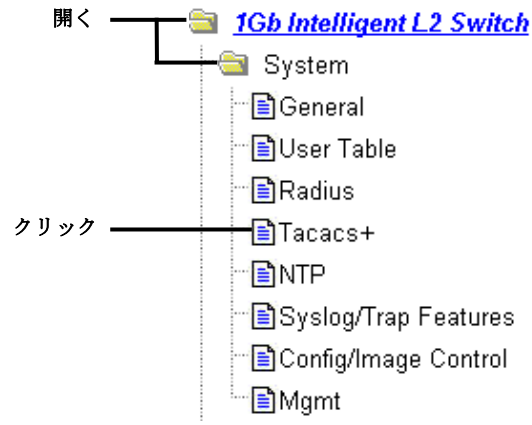
6. カスタム特権レベルマッピングを行います（オプション）。

```
>> TACACS+ Server# usermap 2
Current privilege mapping for remote privilege 2: not set
Enter new local privilege mapping: user
>> TACACS+ Server# usermap 3 user
>> TACACS+ Server# usermap 4 user
>> TACACS+ Server# usermap 5 oper
```

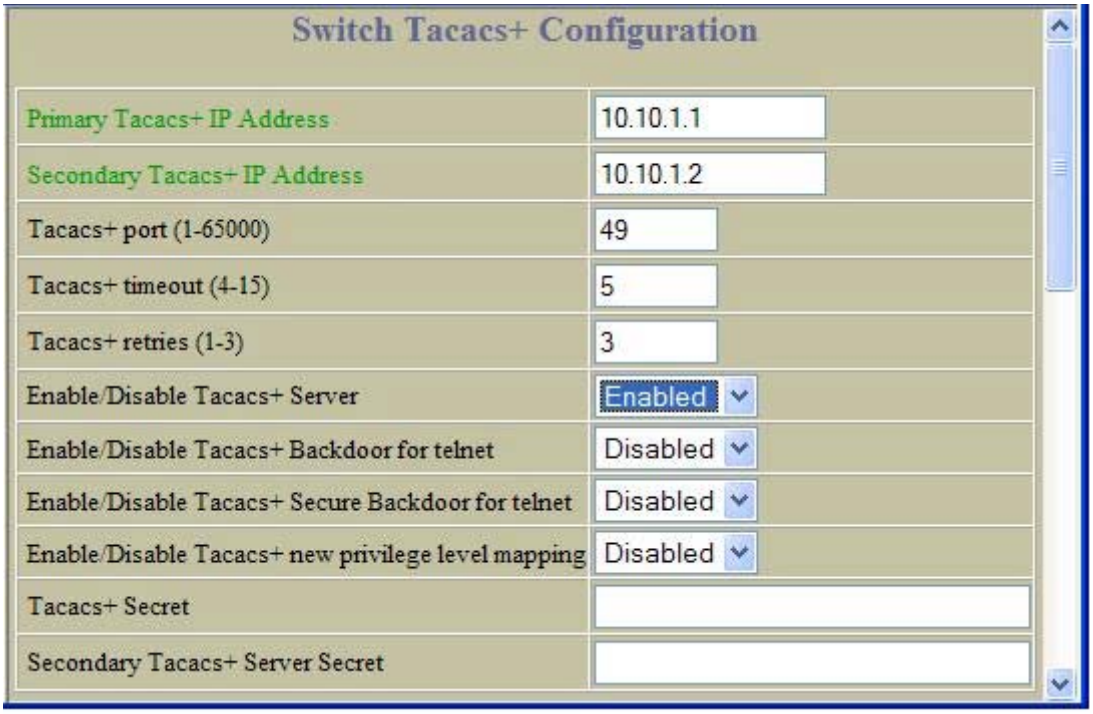
7. 設定を適用、保存します。

## スイッチでの TACACS+認証の設定（BBI の例）

1. スイッチ用に TACACS+認証を設定します。
   a. CONFIGURE ボタンをクリックします。
   b. System フォルダを開き、Tacacs+を選択します。

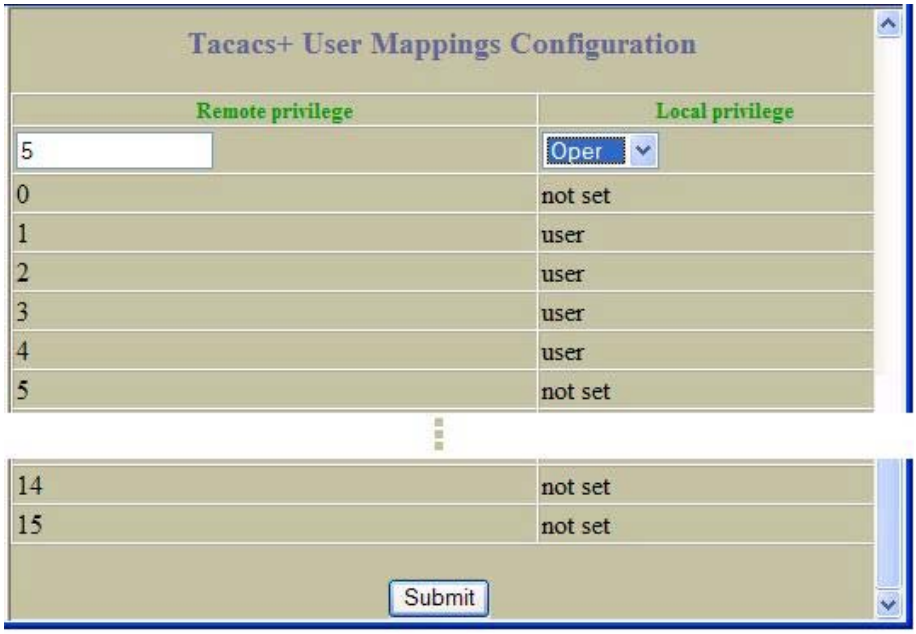



   c. プライマリとセカンダリの TACACS+サーバの IP アドレスを入力し、TACACS+シークレットを入力します。TACACS+を有効にします。

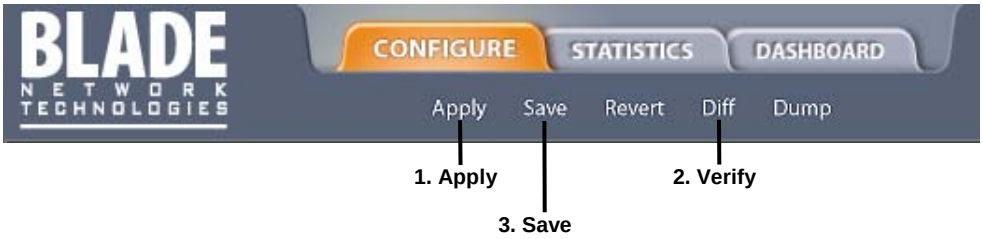



   d. Submit をクリックします。

e. カスタム特権レベルマッピングを行います（オプション）。Submit をクリックして各マッピング変更を設定します。




2. 設定を適用、確認、保存します。



# セキュアシェルとセキュアコピー

セキュアシェル (SSH) とセキュアコピー (SCP) でセキュアトンネルを使用して、ユーザとスイッチの間でメッセージを暗号化して保護します。Telnet はこのレベルのセキュリティを行いません。Telnet では、安全な接続を行うことができません。

SSH は、ネットワークを介してスイッチに安全にログインし、管理コマンドを実行するプロトコルです。デフォルトは無効（オフ）です。

SCP は、通常、マシンからマシンへファイルを安全にコピーするために使用します。ネットワーク上のデータの暗号化には SSH を使用します。スイッチで SCP を使用して、セキュアチャネル経由でスイッチの設定情報をダウンロード、アップロードします。デフォルトはスイッチで無効です。

SSH のスイッチへのインプリメントはバージョン 1.5、2.0 に基づき、バージョン 1.0～2.0 の SSH クライアントをサポートします。クライアントソフトウェアは SSH のバージョン 1 かバージョン 2 を使用できます。以下の SSH クライアントで動作実績があります。

- Linux 用 SSH 3.0.1（フリーウェア）
- SecureCRT® 4.1.8 (VanDyke Technologies, Inc.)
- Linux 用 OpenSSH_3.9 (FC 3)
- Linux 用 SCP コマンド (FC 3)
- Windows 用 PuTTY リリース 0.58 (Simon Tatham)

## SSH および SCP 機能の設定（AOS CLI の例）

SSH コマンドを使用する場合、まず以下のコマンドにより SSH と SCP を有効にしなければなりません。

### SSH の有効／無効

SSH 機能を有効にするためには、CLI に接続して以下のコマンドを入力します。

```
>> # /cfg/sys/sshd/on            (Turn SSH on)
Current status: OFF
New status: ON
SSHD# apply                       (Apply the changes to start generating
                                   RSA host and server keys)

RSA host key generation starts
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
RSA host key generation completes (lasts 212549 ms)
RSA host key is being saved to Flash ROM, please don’t reboot the box
immediately.
RSA server key generation starts
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
RSA server key generation completes (lasts 75503 ms)
RSA server key is being saved to Flash ROM, please don’t reboot the box
immediately.
------------------------------------------------------------------------
Apply complete; don’t forget to “save” updated configuration.
```

**注：セキュアシェルはコンソールポート経由のみで設定できます。Telnet やブラウザベースインタフェースでスイッチにアクセスしても、SSH メニューは表示されません。**

### SCP の適用と保存の有効／無効

SCP putcfg_apply、putcfg_apply_save コマンドを有効にする場合、AOS CLI の場合、次のコマンドを入力します。

```
>> # /cfg/sys/sshd/ena         (Enable SCP apply and save)
>> # /cfg/sys/sshd/dis         (Disable SCP apply and save)
SSHD# apply                    (Apply the changes)
```

### SCP アドミニストレータパスワードの設定

SCP アドミニストレータパスワードを設定する場合、まずシリアルコンソールからスイッチに接続します。セキュリティ上の理由から、SCP アドミニストレータパスワードを設定できるのは、シリアルコンソールに直接接続した場合のみです。

パスワードを設定するには、次の CLI コマンドを入力します。工場デフォルトは admin です。

```
>> # /cfg/sys/sshd/scpadm
Changing SCP-only Administrator password; validation required. . .
Enter current administrator password: <password>
Enter new SCP-only administrator password: <new password>
Re-enter new SCP-only administrator password: <new password>
New SCP-only administrator password accepted.
```

**重要：SCP 専用のアドミニストレータパスワードは通常のアドミニストレータパスワードと異なるパスワードにしなければなりません。**

## SSH および SCP クライアントコマンドの使用法

クライアントコマンドを使用した場合のフォーマットを以下に示します。以下の例ではスイッチの IP アドレスを 205.178.15.157 としています。

### スイッチへのログイン

スイッチにログインするには次のコマンドを入力します。

```
ssh <user>@<switch IP address>
```

次に例を示します。

```
>> # ssh admin@205.178.15.157
```

### SCP によるスイッチからの設定情報のダウンロード

SCP を用いてスイッチの設定情報をダウンロードする場合、次のコマンドを入力します。パスワードが要求されます。

```
scp <user>@<switch IP address>:getcfg <local filename>
```

次に例を示します。

```
>> # scp scpadmin@205.178.15.157:getcfg ad4.cfg
```

スイッチから SCP アドミニストレータパスワードが要求されます。

### SCP によるスイッチへの設定情報のアップロード

スイッチに設定情報をアップロードする場合、次のコマンドを入力します。パスワードが要求されます。

```
scp <local filename> <user>@<switch IP address>:putcfg
```

次に例を示します。

```
>> # scp ad4.cfg admin@205.178.15.157:putcfg
```

### 設定の適用と保存

上記のコマンド (`scp ad4.cfg admin@205.178.15.157:putcfg`) の後、以下の適用コマンドと保存コマンドを入力します。パスワードが要求されます。

```
>> # scp <local_filename> <user>@<switch IP addr>:putcfg_apply
>> # scp <local_filename> <user>@<switch IP addr>:putcfg_apply_save
```

次に例を示します。

```
>> # scp ad4.cfg admin@205.178.15.157:putcfg_apply
>> # scp ad4.cfg admin@205.178.15.157:putcfg_apply_save
```

以下の点に注意してください。

- putcfg の最後に diff コマンドが自動的に実行され、新設定と現設定の違いをリモートクライアントに知らせます。
- putcfg の後、putcfg_apply 適用コマンドを実行します。
- putcfg_apply の後、putcfg_apply_save により新しい設定をフラッシュメモリに保存します。
- putcfg_apply コマンドと putcfg_apply_save コマンドは、putcfg の後に適用コマンドと保存コマンドを実行するために用意されています。

## 管理メッセージの SSH および SCP 暗号化

SSH と SCP に以下の暗号化、認証方式がサポートされています。

- サーバホスト認証 — 各接続の最初にクライアント RSA がスイッチを認証します。
- キー交換 — RSA
- 暗号化 — AES256-CBC、AES192-CBC、3DES-CBC、3DES、ARCFOUR
- ユーザ認証 — ローカルパスワード認証、RADIUS、TACACS+

## SSH アクセスのための RSA ホストおよびサーバキーの生成

SSH サーバ機能をサポートするためには、2 つの RSA キー（ホストキーとサーバキー）が必要です。ホストキーは 1024 ビットで、スイッチの識別に使用します。サーバキーは 768 ビットで、取り込んだセッションをスイッチ侵入者が解読できないようにするためです。

SSH サーバをはじめて有効にして適用したとき、スイッチが自動的に RSA ホストキー、サーバキーを生成して、フラッシュメモリに格納します。

RSA ホストキー、サーバキーを設定する場合、まずシリアルコンソールに接続し（Telnet 接続ではコマンドを利用できません）、以下のコマンドを入力して手動で生成します。

```
>> # /cfg/sys/sshd/hkeygen                    (Generates the host key)
>> # /cfg/sys/sshd/skeygen                    (Generates the server key)
```

この 2 つのコマンドは直ちに有効になり、適用コマンドは必要ありません。

スイッチをリブートすると、ホストキーとサーバキーをフラッシュメモリから取り出します。フラッシュメモリになく、SSH サーバ機能が有効になっていると、リブート時に自動的に生成します。この処理に数分かかることがあります。

スイッチは、また、RSA サーバキーを自動的に再生します。RSA サーバキー自動生成の間隔を設定する場合、次のコマンドを使用します。

```
>> # /cfg/sys/sshd/intrval <number of hours (0-24)>
```

値を 0 にすると、RSA サーバキー自動生成は無効になります。0 以外であれば、指定した間隔毎に生成します。しかし、時間になったときに、スイッチが他のキーや暗号を作成していてビジーであると、RSA サーバキー生成は省略されます。

スイッチはキー／暗号生成を一度に 1 セッションしか行いません。したがって、キー生成を行っていたり、別のクライアントが先にログインしていると、SSH/SCP クライアントはログインできません。また、SSH/SCP クライアントがログインしていると、キー生成は失敗します。

## SSH/SCP と RADIUS、TACACS+認証の統合

SSH/SCP は RADIUS、TACACS+認証と統合されます。つまり、RADIUS サーバか TACACS+サーバをスイッチで有効にすると、後続の SSH 認証リクエストは認証のため RADIUS か TACACS+サーバに向けられます。その指示は SSH クライアントからは分かりません。

# ユーザアクセス制御

アドミニストレータのみユーザアカウントを設定することができます。ユーザアカウントを作成し有効にすると、ログイン時、ユーザ名が要求されます。

次の表に示すように、アドミニストレータが各スイッチユーザのアクセスレベルを定めます。

表6 ユーザアクセスレベル

| ユーザアカウント | 説明 | パスワード |
|---|---|---|
| admin | スイッチのすべてのメニュー、情報、設定コマンドにアクセスできます。ユーザパスワード、アドミニストレータパスワードを変更することもできます。 | admin |
| oper | スイッチのすべての機能を管理します。ポートやスイッチ全体のリセットも行えます。 | oper |
| user | ステータス情報と統計データを参照できますが、スイッチの構成を変更することはできません。 | user |

TACACS+、RADIUS、Telnet、SSH、コンソール、BBI アクセスの場合、パスワードの長さは 128 文字までです。

RADIUS 認証の場合、RADIUS サーバのユーザパスワードがスイッチのユーザパスワードより優先します。スイッチのパスワード変更コマンドはスイッチユーザのパスワードを変更するだけで、RADIUS サーバのユーザパスワードには影響しないことに注意してください。スイッチのアクセスに RADIUS 認証とスイッチに設定されているユーザパスワードを同時に使用することはできません。

## ユーザ ID の設定

アドミニストレータはユーザアカウントを 10 まで設定できます。

エンドユーザアカウントを設定する手順は、次のとおりです。

1. 指定するユーザ ID を選択します。

```
>> # /cfg/sys/access/user/uid 1
```

2. ユーザ名とパスワードを設定します。

```
>> User ID 1 # name jane            (Assign name "jane" to user ID 1)
Current user name:
New user name: jane
```

3. ユーザアクセスレベルを設定します。デフォルトでは、エンドユーザをユーザアクセスレベルに割り当てています。ユーザのアクセスレベルを変更するには、サービスクラスコマンド (cos) を入力して、オプションの 1 つを選択します。

```
>> User ID 1 # cos <user|oper|admin>
```

4. ユーザ ID を有効にします。

```
>> # /cfg/sys/access/user/uid <#>/ena
```

エンドユーザアカウントを設定して有効にすると、ユーザ名とパスワードを入力してスイッチにログインできます。スイッチアクセスのレベルはアカウントのユーザサービスクラスで決まります。サービスクラスは、ユーザアクセスレベルの表に示したレベルに対応します。

# Ports and trunking

## はじめに

本章では、まずスイッチで使用する各種ポートについて説明します。

ポートの速度、オートネゴシエーション、全二重／半二重モードを設定する方法については、「コマンドリファレンスガイド」のポートコマンドを参照してください。

本章の後半では、複数のポートをトランキングする例を示します。トランクグループは、スイッチなどのトランク可能な装置間で帯域幅を広げてトランク接続を行うことができます。トランクグループとは、相互に作用しあうリンクのグループのことで、帯域幅を結合して一つの大規模仮想リンクを生成します。スイッチは、5 つの外部ポート、2 つのインターリンクポート、16 のサーバポートに対してトランキングをサポートしています。

## スイッチのポート

次の表にスイッチのイーサネットポートを示します。ポート名と機能を示します。

**注：スイッチポートと NIC インタフェースとのマッピングは、オペレーティングシステム、CPU ブレードのタイプ、エンクロージャタイプなどによります。詳細については、「ユーザーズガイド」を参照してください。**

表7 スイッチのイーサネットポート

| ポート番号 | 名称 |
|---|---|
| 1 | Downlink1 |
| 2 | Downlink2 |
| 3 | Downlink3 |
| 4 | Downlink4 |
| 5 | Downlink5 |
| 6 | Downlink6 |
| 7 | Downlink7 |
| 8 | Downlink8 |
| 9 | Downlink9 |
| 10 | Downlink10 |
| 11 | Downlink11 |
| 12 | Downlink12 |
| 13 | Downlink13 |
| 14 | Downlink14 |
| 15 | Downlink15 |
| 16 | Downlink16 |
| 17 | XConnect1 |
| 18 | XConnect2 |
| 19 | Mgmt |
| 20 | Uplink1 |
| 21 | Uplink2 |
| 22 | Uplink3 |
| 23 | Uplink4 |
| 24 | Uplink5 |

# ポートトランクグループ

2 台のスイッチ間でポートトランクグループを使用する場合、組み合わせる物理ポート数によっては、最大 5 ギガビット／秒で動作する集約リンクを生成できます。各スイッチは最大で 12 のトランクグループをサポートし、1 トランクグループあたり 6 ポートまで構成できます。

スイッチ内で故障した（リンクダウンしたか無効になった）トランクリンクを検出し、同じトランクグループ内の他のトランクメンバにトラフィックを迂回します。なお、速度、フロー制御、オートネゴシエーションなどの設定が同じ各リンクでトランクグループを構成できます。

## 負荷分散

複数のポートで構成されたトランクグループは、データフレーム内の情報で負荷分布が決まります。IP トラフィックの場合、送信元 IP アドレスの最後の 3 ビットと宛先 IP アドレスの最後の 3 ビットの XOR の modulus に等しい値で負荷分布アルゴリズムを実行して、トラフィック転送に用いるトランクポートを計算します。IP トラフィック以外の場合、送信元 MAC アドレスの最後の 3 ビットと宛先 MAC アドレスの最後の 3 ビットの XOR の modulus に等しい値で、負荷分布アルゴリズムを実行して計算します。

## 耐障害性

各トランクグループは複数の物理リンクから構成されるため本質的に耐障害性があります。スイッチ間で物理リンクが 1 つでも利用できる限り、トランクはアクティブです。

# トランク構成前の作業

トランクを構成する場合、まず、次のように、その設定を構成ルールとともに考慮する必要があります。

1. 「トランクグループ構成ルール」の節で説明する構成ルールを確認します。
2. どのスイッチポート（6 つまで）をトランクメンバ（トランクを形成するポート）にするかを決めます。
3. `/cfg/port` コマンドにより、選択したスイッチポートが有効になっていることを確認します。
4. トランクメンバポートは同じ VLAN 構成にする必要があります。
5. 既存のスパニングツリーを新しいトランク構成にどのように作用させるかを考慮します。スパニングツリーグループ構成のガイドラインについては、「Spanning Tree Protocol」の章を参照してください。
6. トランクの追加で既存 VLAN にどのように影響するかを考慮します。

# トランクグループ構成ルール

トランクは構成ルールに応じて機能します。以下のルールに基づいて、ネットワークトポロジ内のトランクグループの構成を決めます。

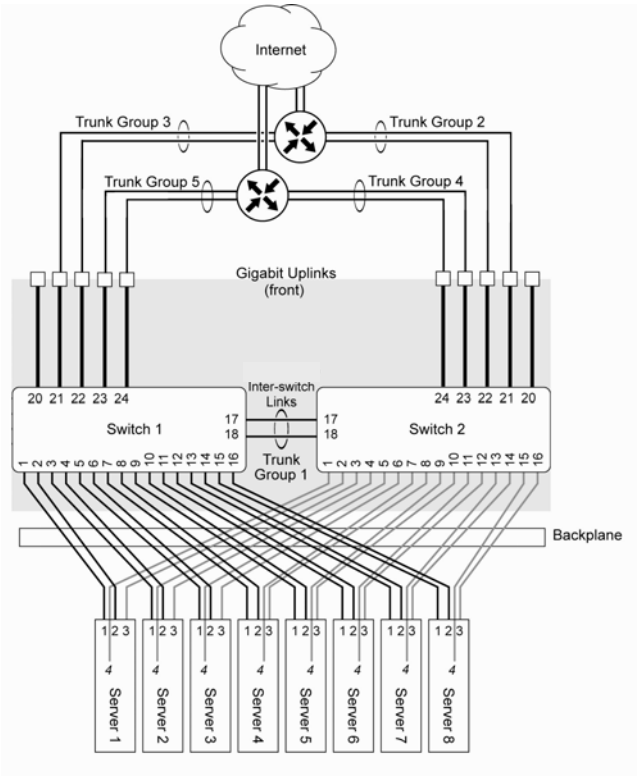
- どのトランクも 1 台の装置から出て 1 台の装置に向かわなければなりません。たとえば、サーバ 1 からのリンクとサーバ 2 からのリンクを 1 つのトランクグループにまとめることはできません。
- どの物理スイッチポートも 1 つのトランクグループだけに所属させます。
- Cisco® EtherChannel®テクノロジに準拠しなければなりません。
- トランクを有効にするためには、すべてのトランクメンバポートを同じ VLAN 構成に割り当てなければなりません。
- すべてのトランクメンバポートを全二重モードに設定しなければなりません。
- すべてのトランクメンバポートを同じ速度にしなければなりません。
- トランクメンバの VLAN 設定を変更しても、すべてのトランクメンバの VLAN 設定を変更しない限り、その変更を適用することはできません。
- トランクにアクティブポートを構成した場合、`/cfg/l2/trunk x/ena` コマンドによりトランクを有効にすると、ポートがトランクメンバになります。ポートのスパニングツリーパラメータが変化して、新しいトランク設定を反映します。
- すべてのトランクメンバが同じスパニングツリーグループに入る必要があります。また、所属できるのは 1 つのスパニングツリーグループだけです。ただし、すべてのポートにタグを付けると、複数のスパニングツリーグループに所属できます。
- トランクを有効にすると、そのトランクのスパニングツリー参加設定が、どのドランクメンバの参加設定よりも優先されます。
- トランクメンバをポートミラーリング構成のモニタポートとすることはできません。
- モニタポートはトランクをモニタできません。しかし、トランクメンバをモニタすることはできます。

# ポートトランキングの例

この例では、各スイッチのギガビットアップリンクポートと、インターリンクポートで、合計 5 つのトランクグループを構成します。各スイッチに 2 トランクグループ、2 台のスイッチ間のインターリンクに 1 トランクグループです。すべてのポートがギガビットイーサネット速度で動作します。

> **注：スイッチポートと NIC インタフェースとのマッピングは、オペレーティングシステム、サーバブレードのタイプ、エンクロージャタイプによります。詳細については「ユーザーズガイド」を参照してください。**

図1　ポートトランクグループの構成例




トランクグループは次のように構成します。

- トランクグループ 1 は、デフォルトで、スイッチ 1 と 2 を相互に接続するインターリンクポート 17、18 で構成されています。デフォルト設定のため、どちらのスイッチにもトランクグループ 1 を構成する必要はありません。デフォルトでは、ポート 17、18 は無効になっています。
- トランクグループ 2～5 は各々2 つのギガビットアップリンクポートからなり、アップストリームルータへの単一リンクとして機能するようになっています。各スイッチのトランクグループは、各ルータへのリンクが重複するように構成しています。

各スイッチの CLI にアドミニストレータでログインし、設定する必要があります。本例で説明するコマンドのアクセス、使用法の詳細については、「コマンドリファレンスガイド」を参照してください。

## トランクグループの設定（AOS CLI の例）

1. スイッチ 1 でトランクグループ 5、3 を設定します。

```
>> # /cfg/l2/trunk 5                  (Select trunk group 5)
>> Trunk group 5# add 23               (Add port 23 to trunk group 5)
>> Trunk group 5# add 24               (Add port 24 to trunk group 5)
>> Trunk group 5# ena                  (Enable trunk group 5)
>> Trunk group 5# apply                (Make your changes active)

>> # /cfg/l2/trunk 3                  (Select trunk group 3)
>> Trunk group 3# add 21               (Add port 21 to trunk group 3)
>> Trunk group 3# add 22               (Add port 22 to trunk group 3)
>> Trunk group 3# ena                  (Enable trunk group 3)
>> Trunk group 3# apply                (Make your changes active)
>> Trunk group 3# save                 (Save for restore after reboot)
```

2. スイッチ 2 でトランクグループ 4、2 を設定します。

```
>> # /cfg/l2/trunk 4                  (Select trunk group 4)
>> Trunk group 4# add 23               (Add port 23 to trunk group 4)
>> Trunk group 4# add 24               (Add port 24 to trunk group 4)
>> Trunk group 4# ena                  (Enable trunk group 4)
>> Trunk group 4# apply                (Make your changes active)

>> # /cfg/l2/trunk 2                  (Select trunk group 2)
>> Trunk group 2# add 21               (Add port 21 to trunk group 2)
>> Trunk group 2# add 22               (Add port 22 to trunk group 2)
>> Trunk group 2# ena                  (Enable trunk group 2)
>> Trunk group 2# apply                (Make your changes active)
>> Trunk group 2# save                 (Save for restore after reboot)
```

**注:この例では、スイッチを 2 台使用しています。リンクアグリゲーションをサポートする接続先のスイッチを手動で設定する必要があります。接続問題が発生する可能性があるのは、接続先の装置で自動トランクグループネゴシエーションを使用するときです。**

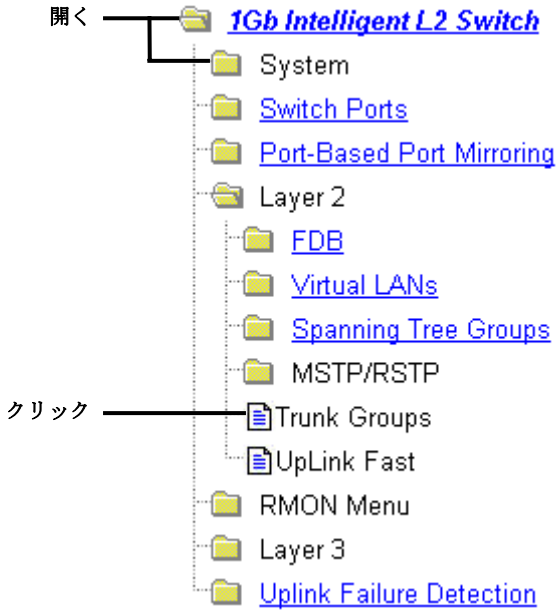
3. 次のコマンドにより、各スイッチのトランキング情報を確認します。

```
>> /info/l2/trunk                   (View trunking information)
```

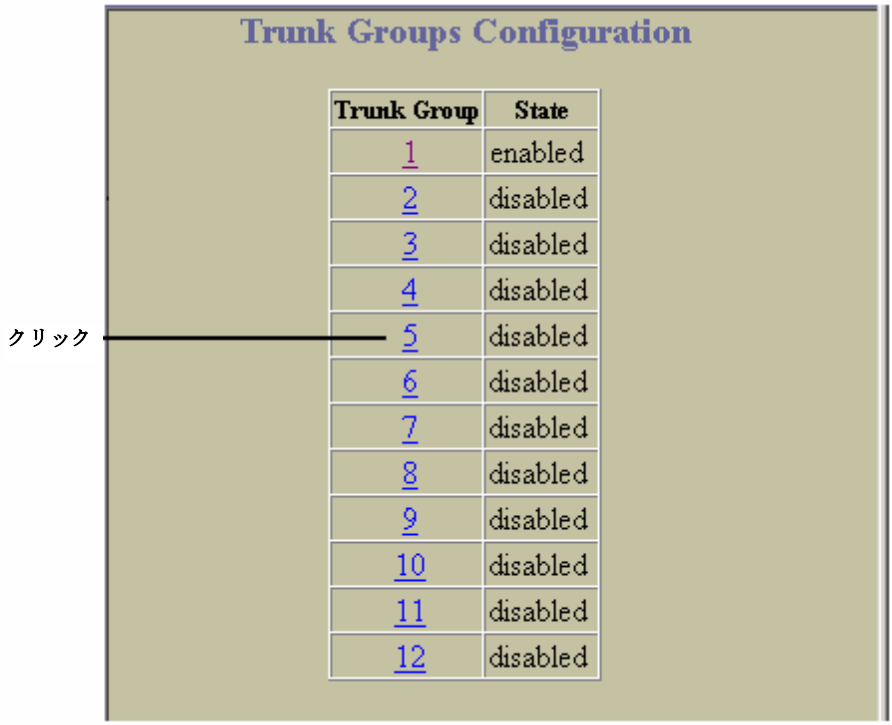
設定済みの各トランクグループの各ポートに関する情報が表示されます。トランクグループが予定したポートで構成されていること、各ポートが予定通りの状態にあることを確認します。

## トランクグループの設定（BBI の例）

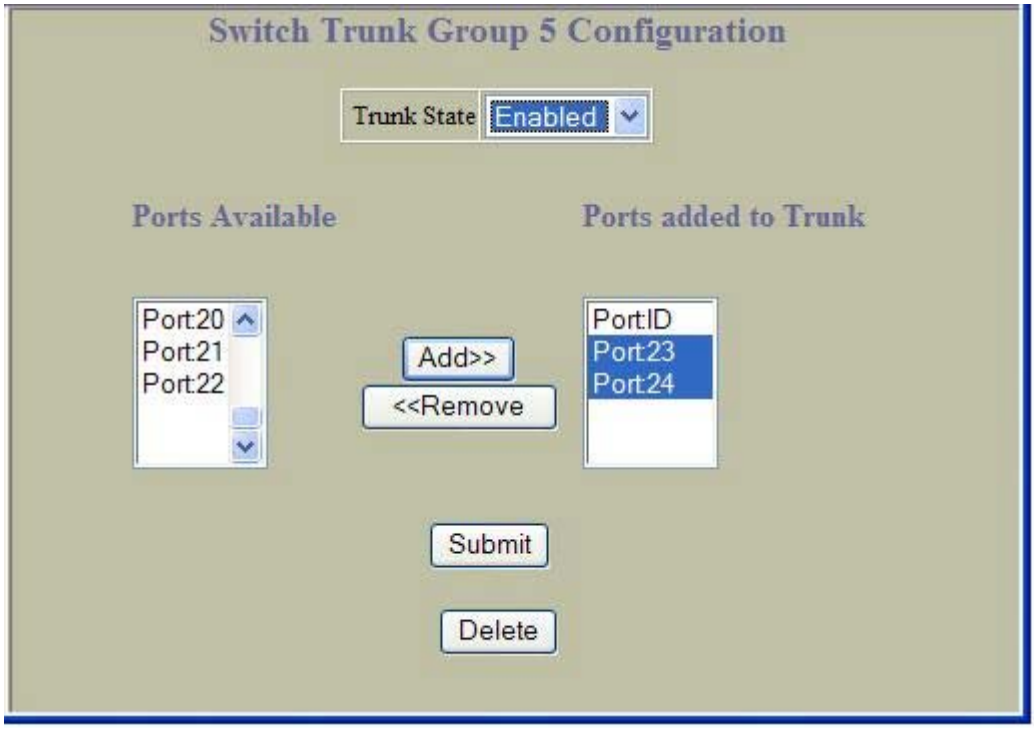
1. トランクグループを設定します。
   a. ツールバーの CONFIGURE ボタンをクリックします。
   b. Layer 2 フォルダを開き、Trunk Groups を選択します。




   c. Trunk Group 番号の 1 つをクリックして、選択します。

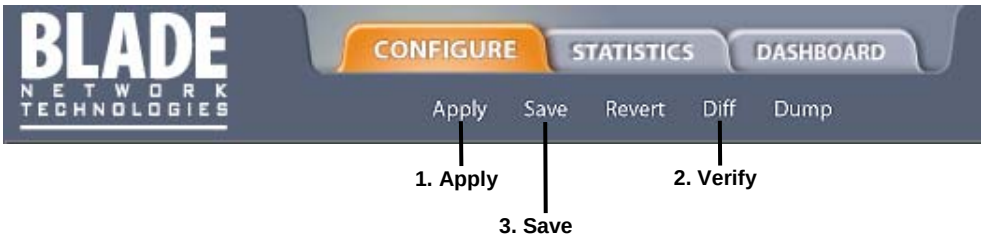


d. トランクグループを有効にします。ポートを追加するには、Ports Available リストの各ポートを選択し、Add をクリックします。




e. Submit をクリックします。

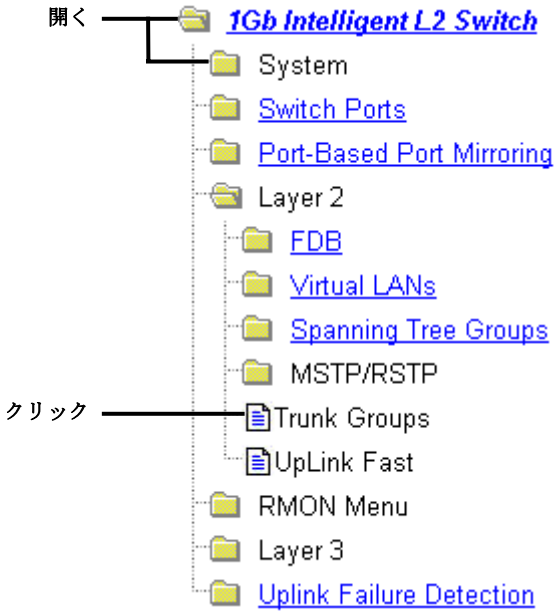
2. 設定を適用、確認、保存します。



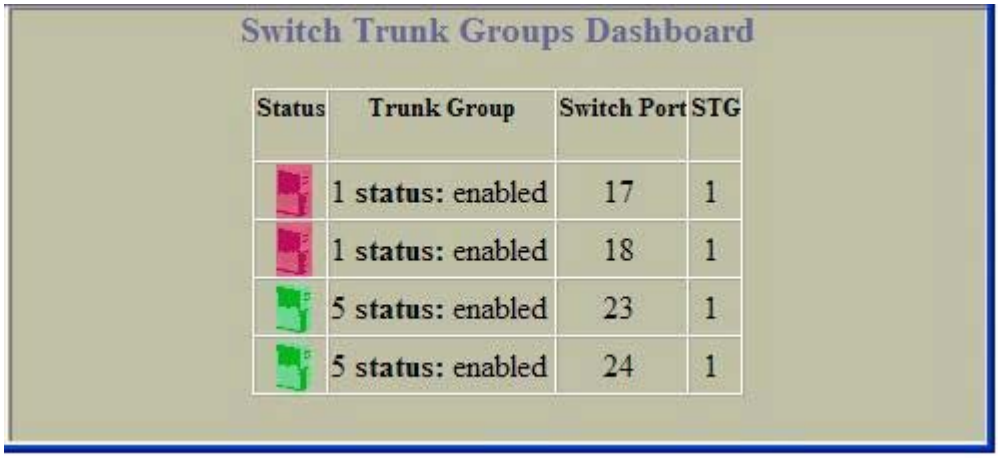

3. 各スイッチのトランキング情報を調べます。

a. ツールバーの DASHBOARD コンテキストボタンをクリックします。

b. Trunk Groups を選択します。




c. 構成済みの各トランクグループの情報が表示されます。トランクグループが予定したポートからなり、各ポートが予定通りの状態にあることを確認します。




# トランクハッシュアルゴリズム

**注:この機能はソフトウェアバージョン 1.0.0 では使用できません。**

本機能により、デフォルトをそのまま使用するのではなく、スイッチのトランクハッシュアルゴリズムの一部のパラメータを設定できます。CLI メニューcfg/l2/thash を使用して、レイヤ 2 トラフィック、レイヤ 3 トラフィック用に新しい動作を設定できます。以下の組み合わせの中から 1 つ選択できます。

- 送信元 IP (SIP)
- 宛先 IP (DIP)
- 送信元 MAC (SMAC)
- 宛先 MAC (DMAC)
- 送信元 IP (SIP) + 宛先 IP (DIP)
- 送信元 MAC (SMAC) + 宛先 MAC (DMAC)

# Link Aggregation Control Protocol

**注:この機能はソフトウェアバージョン 1.0.0 では使用できません。**

Link Aggregation Control Protocol (LACP)は IEEE 802.3ad で規定されているもので、複数の物理ポートを 1 つの論理ポートにグループ化するものです（グループ化したものをダイナミックトランクグループまたはリンクアグリゲーショングループといいます）。この規格の詳細については、IEEE 802.3ad-2002 を参照してください。

802.3ad では、LACP を使用して、複数のイーサネットリンクから単一のレイヤ 2 リンクを形成できます。リンクアグリゲーションは、同じメディアタイプと全二重の転送速度の複数の物理リンクセグメントをグループ化して、単一の論理リンクセグメントとして取り扱う手段です。LACP トランクグループ内の 1 つのリンクに障害が発生しても、トラフィックはダイナミックトランクグループの残りのリンクに動的に再割り当てされます。

**注: 本スイッチの LACP では Churn マシン（ポートがアクタとパートナの間で一定時間内に動作できるかどうかの確認に使用するオプション）をサポートしません。Marker Responder のみが実装され、Marker protocol generator はありません。**

ポートのリンクアグリゲーション識別子(LAG ID)で、そのポートの集約方法が決まります。LAG ID は、主にシステム ID とポートの管理キーから生成されます。

**重要: システム ID:スイッチの MAC アドレスと CLI で割り当てたシステムプライオリティに基づく整数値です。**

- admin key：ポートの admin key は CLI で設定できる整数値（1～65535）です。同じ LACP トランクグループに属するスイッチポートは、admin key の値を同じにする必要があります。admin key はローカルで使用される値です。つまり、パートナスイッチ側で同じ admin key を使用する必要はありません。

たとえば、次の表に示すように、2 台のスイッチ、アクタ（本スイッチ）とパートナ（別のスイッチ)を考えます。

表8 アクタとパートナの LACP 設定

| アクタスイッチ | パートナスイッチ 1 | パートナスイッチ 2 |
|---|---|---|
| ポート 20 (admin key = 100) | ポート 1 (admin key = 50) | |
| ポート 21 (admin key = 100) | ポート 2 (admin key = 50) | |
| ポート 22 (admin key = 200) | | ポート 3 (admin key = 60) |
| ポート 23 (admin key = 200) | | ポート 4 (admin key = 60) |

上記の表に示す構成では、アクタスイッチのポート 20、21 がまとまって、パートナスイッチのポート 1、2 と LACP トランクグループを形成します。同時に、アクタスイッチポート 22、23 は、他のパートナと別の LACP トランクグループを形成します。

LACP は、どのメンバリンクを集約できるかを自動的に確認して、集約します。物理リンクの追加、削除を制御して、リンク集約を行います。

本スイッチの各ポートの LACP モードは以下のいずれかになります。

- オフ（デフォルト）：ユーザがポートをスタティックトランクグループに設定できます。
- アクティブ：ポートで LACP トランクを形成できます。このポートから LACPDU パケットをパートナのポートに送信します。
- パッシブ：ポートで LACP トランクを形成できます。LACP のアクティブポートから送信された LACPDU ポートに応答するだけです。

アクティブの LACP 各ポートは LACP データユニット(LACPDU)を送信し、パッシブ LACP ポートは LACPDU をリスニングしています。LACP ネゴシエーションの際に admin key を交換します。リンクの両端で情報が一致する限り、LACP トランクグループは有効です。リンクの片側のポートで admin key の値が変わると、このポートは LACP トランクグループの関係が切れます。

システムを初期化すると、デフォルトですべてのポートが LACP オフモードになり、一意の admin key が割り当てられます。ポートを集約させるには、すべてに同じ admin key を割り当てます。LACP ネゴシエーションを動かすには、リンクの片側のポートの LACP モードをアクティブに設定する必要があります。リンクの反対側のポートの LACP モードはパッシブにでき、初期のトランク形成段階での LACPDU トラフィックの量を削減できます。

ポートがトランクされているかどうかの確認には、/info/l2/trunk コマンドもしくは/info/l2/lacp/dump コマンドを使用します。

## LACP の設定

ポート 20、ポート 21 でリンクアグリゲーションを構成する場合の、LACP を設定する手順は次のとおりです。

1. ポート 20 で LACP モードを設定します。

```
>> # /cfg/l2/lacp/port 20          (ポート20を選択)
>> LACP port 20# mode active      (LACP active modeに設定)
```

2. ポート 20 で admin key を設定します。LACP トランクグループを構成できるのは、admin key が同じポートだけです。

```
>> LACP port 20# adminkey 100     (ポート20のadminkeyを100に設定)
Current LACP port adminkey: 20
New pending LACP port adminkey: 100
```

3. ポート 21 で LACP モードを設定します。

```
>> # /cfg/l2/lacp/port 21          (ポート21を選択)
>> LACP port 21# mode active      (LACP active modeに設定)
```

4. ポート 21 で admin key を設定します。

```
>> LACP port 21# adminkey 100     (ポート21のadminkeyを100に設定)
Current LACP port adminkey: 21
New pending LACP port adminkey: 100
```

5. 設定を適用、確認します。

```
>> LACP port 21# apply            (適用)
>> LACP port 21# cur              (現在の設定を確認)
```

6. 新しい設定を保存します。

```
>> LACP port 21# save             (保存)
```

# VLANs

## はじめに

この章では、仮想ローカルエリアネットワーク(VLAN)を使用する際にネットワーク設計とトポロジに関して考慮すべき事項について説明します。VLAN は、通常、ワークグループの論理的セグメントの生成、論理セグメント内のセキュリティポリシの適用のために、ネットワークユーザのグループをブロードキャストドメインで分割するために使用します。

本章では以下の事項について説明します。

- VLAN とポート VLAN ID 番号
- VLAN タグ
- VLAN と IP インタフェース
- VLAN のトポロジと設計上の考慮事項

**注:基本的な VLAN は初期スイッチ構成時に構築できます。**

**詳細は「コマンドリファレンスガイド」を参照してください。**

## 概要

ネットワークをセグメント化して、物理ネットワークトポロジを変更せずにネットワークの柔軟性を高める方法の一つが、VLAN です。ネットワークをセグメント化した場合、各スイッチポートは 1 つのブロードキャストドメインであるセグメントに接続することになります。スイッチポートを VLAN のメンバにすると、1 ブロードキャストドメインに属するポートのグループ（ワークグループ）に追加されます。

ポートを同じ VLAN に割り当てると、ブロードキャストドメインにグループ分けされます。マルチキャストフレーム、ブロードキャストフレーム、未知ユニキャストフレームは、同じ VLAN のポートにだけ送られます。

## VLAN とポート VLAN ID 番号

### VLAN 番号

本スイッチはスイッチあたり 1,000 VLAN までサポートします。各時点でサポートする最大 VLAN 数は 1,000 ですが、ID 番号の範囲は 1～4095 です。VLAN 1 がデフォルト VLAN で、工場出荷時、Port19 以外のすべてのポートは VLAN1 に属しています。VLAN 4095 はマネジメントインタフェース用でメンバポートは Port19 のみです。

#### VLAN の確認

VLAN 情報メニュー (`/info/l2/vlan`) に、設定された VLAN とメンバポートが表示されます。次に例を示します。

```
>> Layer 2# vlan
VLAN                Name                Status Ports
----  --------------------------------- ------ ----------------------
1     Default VLAN                        ena   1 4-18 20-24
2     VLAN 2                              ena   2 3
4095  VLAN 4095                           ena   19
```

## PVID 番号

本スイッチの各ポートにはデフォルトの VLAN 番号があり、PVID（Port VLAN ID）といいます。これにより最初はすべてのポートを同じ VLAN に配置します。ただし、どのポートの PVID も、1～4094 の範囲であれば、別の VLAN 番号に設定できます。

スイッチのデフォルト設定では、Port19 以外のすべてのポートが VLAN 1 のタグなしメンバとして設定され、PVID = 1 になります。下図に示すデフォルト構成例の場合、デフォルトのポート VLAN ID (PVID =1) によって、受信したすべてのパケットが VLAN 1 に割り当てられます。

## PVID の確認と設定

AOS CLI の場合、次の CLI コマンドにより PVID を確認できます。

### ポート情報

```
>> /info/port
Port Tag RMON PVID      NAME                 VLAN(s)
---- --- ---- ---- -------------- --------------------------------
  1   n   d      1 Downlink1      1
  2   n   e      1 Downlink2      1
  3   n   d      1 Downlink3      1
  4   n   d      1 Downlink4      1
  5   n   d      1 Downlink5      1
  6   n   d      1 Downlink6      1
  7   n   d      1 Downlink7      1
  :
  :
```

### ポート構成

```
>>  /cfg/port 22/pvid 22
Current port VLAN ID:     1
New pending port VLAN ID: 22

>> Port 22#
```

各ポートは 1 つまたは複数の VLAN に属することができ、各 VLAN はメンバとして複数のスイッチポートを含めることができます。ただし、複数の VLAN に所属させるためには、ポートの VLAN タグを有効にする必要があります。本章の「VLAN タグ」の節を参照してください。

タグなしフレーム（VLAN が指定されていないフレーム）は送信するポートの PVID により分類します。

# VLAN タグ

本スイッチは IEEE 802.1Q VLAN タグをサポートし、イーサネットシステムに対して標準的な VLAN サポートを行います。

タグではフレームヘッダに VLAN ID を配置するので、各ポートが複数の VLAN に属することができます。1 ポートで複数の VLAN を構成する場合、タグを有効にする必要があります。

基本的に、タグによりタグ付きポートに転送されるフレームのフォーマットが変わるため、802.1Q VLAN タグをサポートしない装置や、タグが有効になっていない装置にタグ付きフレームが転送されることのないよう、ネットワーク設計には注意しなければなりません。

802.1Q タグで重要な用語を以下に説明します。

- VLAN ID (VID) — VLAN を特定する、フレームヘッダ内の 12 ビットの VLAN タグ
- ポート VLAN ID (PVID) — ポートを特定の VLAN と関連付けるクラス分けするための番号。たとえば、PVID が 3 のポートは、受信したタグなしフレームすべてを VLAN 3 に割り当てます。
- タグ付きフレーム — ヘッダに VLAN タグがあるフレーム。VLAN タグは、フレームヘッダ内の 32 ビットフィールド（VLAN タグ）で、フレームが特定の VLAN に属することを示すものです。タグ付きで設定されているポートからフレームを送信する場合、タグなしフレームにタグが付けられます。
- タグなしフレーム — ヘッダに VLAN タグがないフレーム
- タグなしメンバ — タグなしで設定されているポート。タグなしフレームがタグなしメンバポートを通じてスイッチから送信する場合、フレームヘッダは変化しません。タグ付きフレームを受け取り送信する場合、タグを削除し、タグなしフレームに変わります。
- タグ付きメンバ — タグ付きで設定されているポート。タグなしフレームがタグ付きメンバポートを通じてスイッチから送信する場合、フレームヘッダが変化して、PVID に応じた 32 ビットタグがヘッダの中に追加されます。タグ付きフレームを受け取り送信する場合、フレームヘッダは変化しません（元の VID はそのままです）。

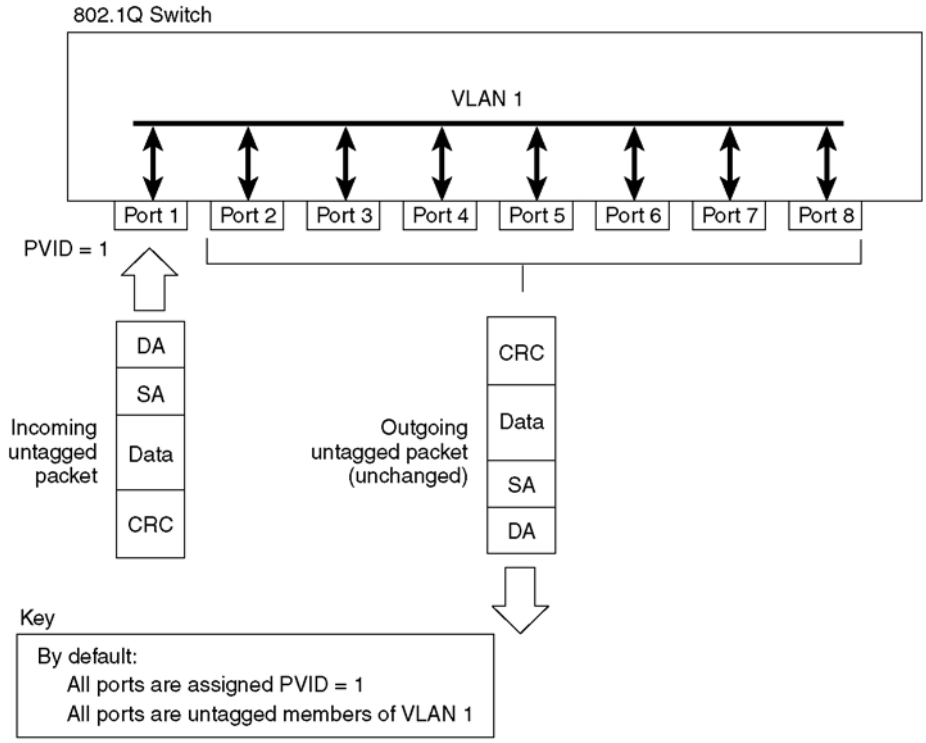
---

**注**: VLAN タグが無効になっているポートに 802.1Q タグ付きフレームを送信する場合、そのポートの VLAN ID (PVID)に基づいて送られます。

Port 毎に VLAN タグの有効／無効とは別に tagpvid の有効／無効の設定があります。tagpvid が有効の場合、PVID が一致するフレームを受信してもタグをそのままつけて送出されます。デフォルトで tagpvid は有効です。詳細はコマンドリファレンスを参照してください。

---

図2　デフォルト VLAN 設定

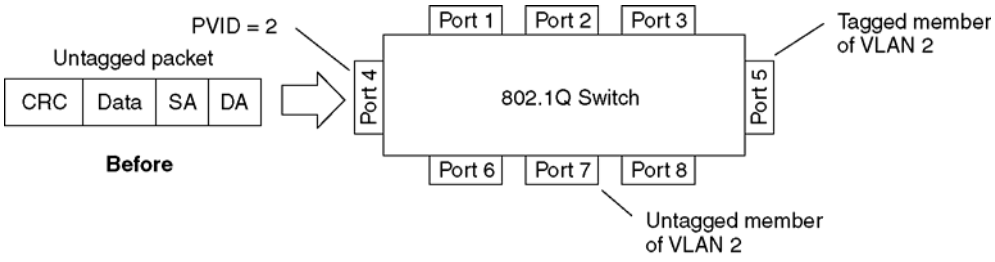



**注：図に示したポート番号は、スイッチの物理ポート構成に必ずしも対応しません。**

VLAN を構成する場合、特定の VLAN のタグ付きメンバかタグなしメンバとしてスイッチポートを構成します。後述の図を参照してください。

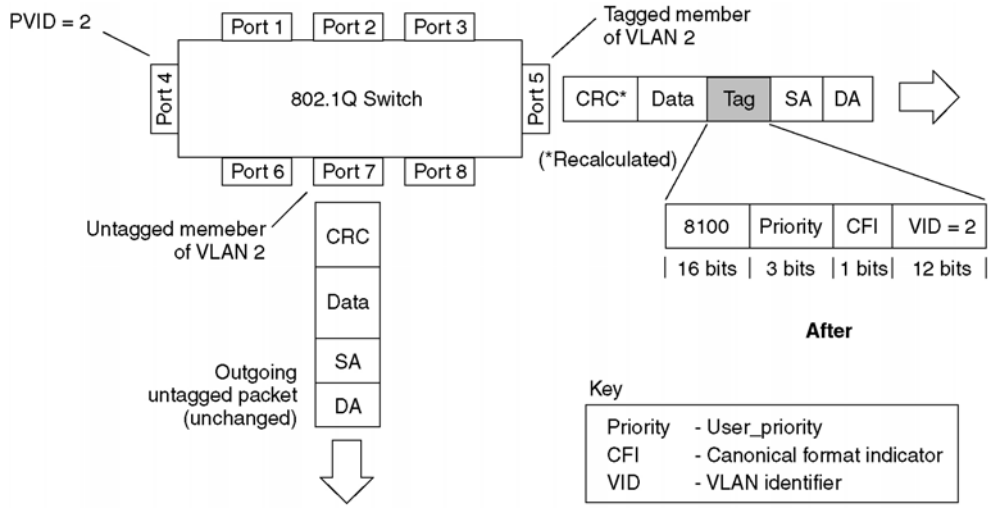
次の図は、タグなしパケットを VLAN 2 (PVID=2) の Port4 で受信する時の例です。ポート 5 を VLAN 2 のタグ付きメンバ、ポート 7 をタグなしメンバとしています。

図3 ポートベース VLAN 割当て



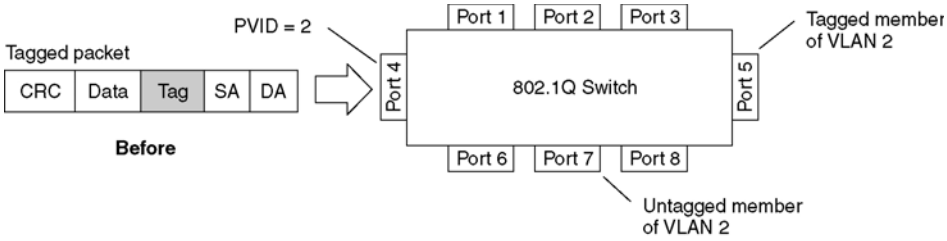

次の図に示すように、タグなしパケットは、VLAN 2 のタグ付きメンバに指定されているポート 5 を通じてスイッチから出る場合、マークされます（タグが付けられます）。
VLAN 2 のタグなしメンバに指定されているポート 7 を通じてスイッチから出るときには、元のまま変化しません。

図4 802.1Q タグ（ポートベース VLAN 割当て後）



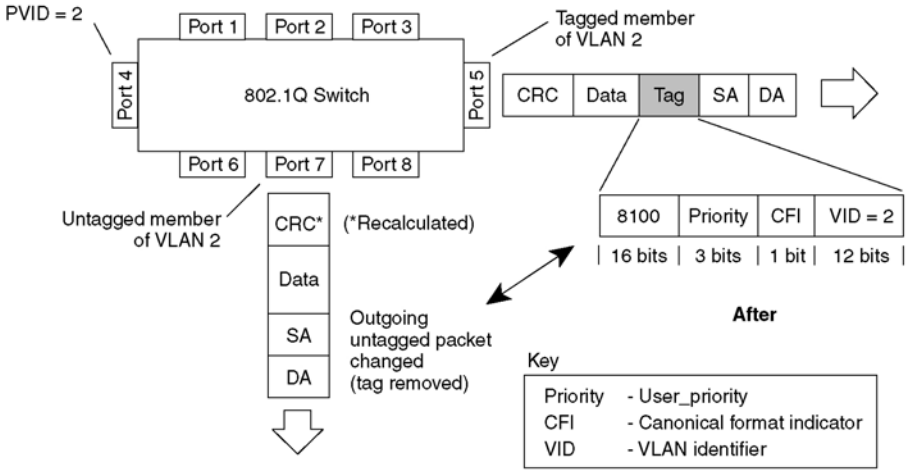

次の図は、タグ付きパケットを VLAN 2 (PVID=2) の Port4 で受信する時の例です。ポート 5 を VLAN 2 のタグ付きメンバ、 ポート 7 をタグなしメンバとしています。

図5 802.1Q タグ割当て




次の図に示すように、タグ付きパケットは、VLAN 2 のタグ付きメンバに指定されているポート 5 を通じてスイッチから出る場合、元のまま変化しません。しかし、VLAN 2 のタグなしメンバに指定されているポート 7 を通じてスイッチから出るときには、タグが剥ぎ取られます（タグなしになります）。

図6　802.1Q タグ（802.1Q タグ割当て後）




注：上図で Port7 から送出されるパケットでタグなしになるのは、Port7 の tagpvid の設定が無効のときです。tagpvid が有効のときはタグ付きのまま送出されます。

`/boot/conf factory` コマンドを使用すると、次のリブートで、すべてのポート（ポート 19 を除く）を VLAN 1 に、他のすべての設定を工場デフォルトにリセットします。

# VLAN と IP インタフェース

スイッチ内で VLAN を生成する方法については、スイッチとの通信が維持されるよう、十分な検討が必要です。リモート構成、トラップメッセージなどのスイッチの管理機能にアクセスするには、最低 1 つの IP インタフェースで VLAN が設定されていなければなりません。

ポートを VLAN メンバ構成から外すと、管理機能へのアクセスに気付かずに遮断してしまう可能性もあります。たとえば、すべての IP インタフェースが VLAN 1 のままで（デフォルト）、すべてのポートを VLAN 2 用に構成した場合、スイッチ管理機能が遮断されます。

これを回避するには、リモートスイッチ管理に使用するすべてのポートをデフォルト VLAN に残し、IP インタフェースをデフォルト VLAN に割り当てます。

IP インタフェースの設定については、「スイッチへのアクセス」の章の「IP インタフェースの設定」を参照してください。

# VLAN トポロジと設計上の考慮事項

デフォルトでは、Port19 を除いたすべてのポートがデフォルトの VLAN 1 に属しており、同じブロードキャストドメインにあります。デフォルトで、すべてのポートで VLAN タグはオフです。

スパニングツリープロトコル (`/cfg/l2/stp`) を構成する場合、スパニングツリーグループ 2～32 の各々に割り当てられる VLAN は 1 つだけであることに注意してください Multiple Spanning Tree Protocol (`/cfg/l2/mrst`) を構成する場合には、スパニングツリーグループ 1～31 の各々に複数の VLAN を割り当て可能です。

## VLAN 構成ルール

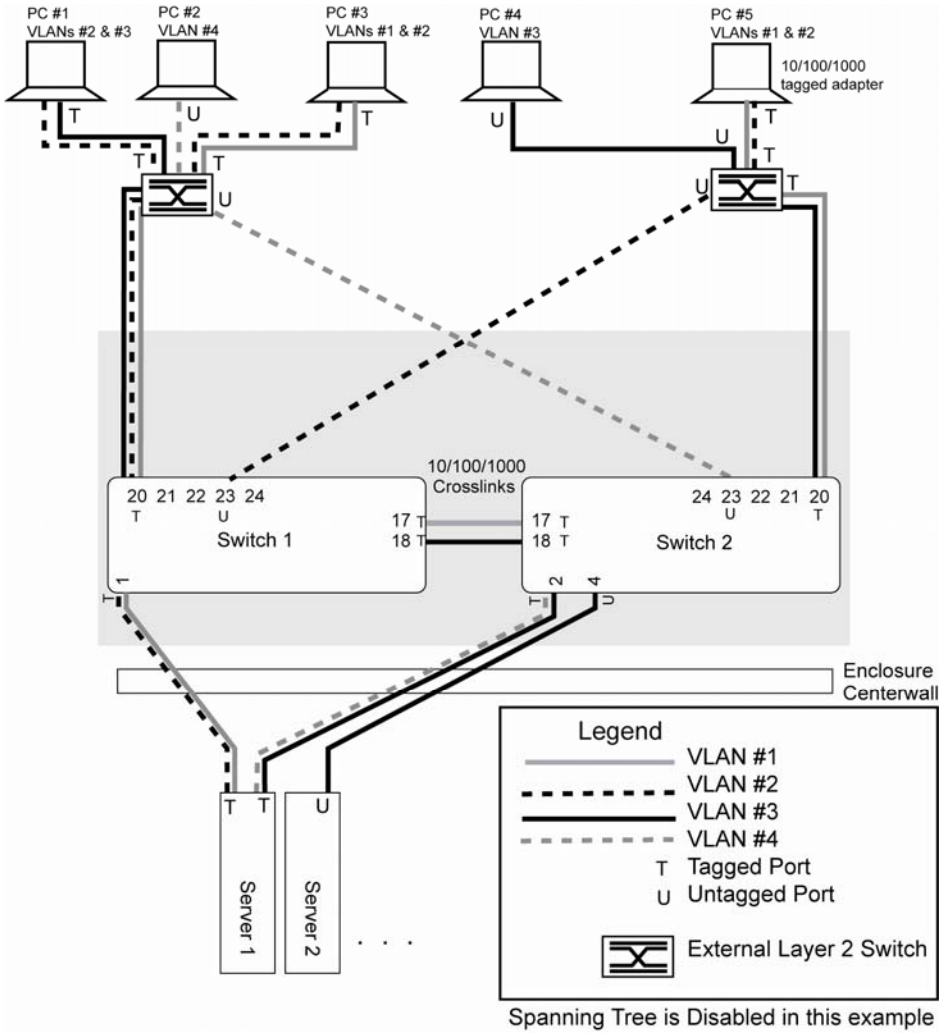
VLAN 構成時、以下の点を考慮してください。

- 推奨する方法は、トランキングとポートミラーリングに関連するすべてのポートを同じ VLAN 構成にすることです。ポートがミラーリングポートを有するトランクにある場合、VLAN 構成を変更することはできません。Ports and trunking の詳細については、「Ports and trunking」の章の「ポートトランキング例」を参照してください。
- ポートミラーリングに関わるポートはすべて、同じ VLAN メンバにしなければなりません。ポートをポートミラーリング用に構成した場合、VLAN メンバを変更することはできません。ポートミラーリングの構成については、「Troubleshooting tools」の「ポートミラーリング」を参照してください。
- VLAN を削除すると、タグなしポートはデフォルト VLAN（VLAN 1）に移動します。削除した VLAN にだけ属していたタグ付きポートは、PVID で識別される VLAN に移動します。複数の VLAN に属しているタグ付きポートは、削除した VLAN から外されるだけです。

# タグ付き多重 VLAN

次の図では、事例に合わせて構成しなければならない、スイッチポートからサーバへのリンクだけ示しています。図には示してない他のサーバリンクはデフォルト設定のままとします。

図7　VLAN タグ付き多重 VLAN




注：図に示したポート番号は、スイッチの物理ポート構成に必ずしも対応しません。

VLAN の機能を次の表に示します。

表9　タグ付き多重 VLAN

| コンポーネント | 説明 |
|---|---|
| スイッチ 1 | VLAN 1、2、3 を構成しています。ポート 1 にはトラフィックを VLAN 1、2 から受けるようにタグを付けています。ポート 17、18 はトラフィックを VLAN 1、3 からの受けるトランクのタグ付きメンバです。ポート 20 にはトラフィックを VLAN 1、2、3 から受けるようにタグを付けています。ポート 23 は VLAN 2 のタグなしメンバです。 |
| スイッチ 2 | VLAN 1、3、4 を構成しています。ポート 2 にはトラフィックを VLAN 3、4 から受けるようにタグを付けています。ポート 4 は VLAN 3 のみのため VLAN タグはオフです。ポート 20 にはトラフィックを VLAN 1、3 から受けるようにタグを付けています。ポート 23 は VLAN 4 のタグなしメンバです。 |
| CPU ブレードサーバ #1 | ブレードサーバで、VLAN と IP サブネットのすべてからアクセスする必要があります。また、VLAN タグを有効にしています。<br>1 つのアダプタをスイッチの 10/100/1000 Mbps ポートの 1 つに接続し、VLAN 1、2 用に構成しています。VLAN 3、4 用に 1 アダプタを構成しています。<br>アダプタとスイッチの両方に VLAN タグ機能があるので、サーバはこのネットワークの 4 つの VLAN すべてと通信でき、しかも、4 つの VLAN とサブネットのすべてでブロードキャスト分割を維持します。 |
| CPU ブレードサーバ #2 | VLAN 3 に属するブレードサーバです。VLAN を接続するポートは VLAN 3 のみで構成されているので、VLAN タグはオフです。 |
| PC #1 | VLAN 2、3 のメンバの PC です。VLAN 2 経由でサーバ 1、PC 3、PC 5 と、VLAN 3 経由でサーバ 1、サーバ 2、PC 4 と通信します。 |
| PC #2 | VLAN 4 のメンバの PC で、サーバ 1 とだけ通信します。 |
| PC #3 | VLAN 1、2 のメンバの PC です。VLAN 1 経由でサーバ 1、PC 5 と、VLAN 2 経由でサーバ 1、PC 1、PC 5 と通信します。 |
| PC #4 | VLAN 3 のメンバの PC で、サーバ 1、サーバ 2、PC 1 と通信できます。 |
| PC #5 | VLAN 1 と 2 の両方のメンバの PC です。VLAN 1 経由でサーバ 1、PC 3 と、VLAN 2 経由でサーバ 1、PC 1、PC 3 と通信します。接続するレイヤ 2 スイッチポートは VLAN 1 と VLAN 2 用に構成され、タグが有効になっています。 |

**注:タグ付きポートに接続したすべての PC に、VLAN タグ機能を使用できるイーサネットアダプタが必要です。**

# ネットワーク構成例

以下の例では、スイッチ 1 と 2 でポートと VLAN を構成する方法を説明します。

## スイッチ 1 でのポートと VLAN の設定（AOS CLI の例）

スイッチ 1 にポートと VLAN を設定する手順は次のとおりです。

1. スイッチ 1 で、タグが必要なポートに VLAN タグを有効にします。

```
Main# /cfg/port 1
>> Port 1# tag e                        (Select port 1: connection to server 1)

Current VLAN tag support: disabled
New VLAN tag support:     enabled      (Enable tagging)
Port 1 changed to tagged.

Main# /cfg/port 17                     (Select crosslink link port 17)
>> Port 17# tag e                      (Enable tagging)
Current VLAN tag support: disabled
New VLAN tag support:     enabled
Port 17 changed to tagged.

Main# /cfg/port 18                      (Select crosslink link port 18)
>> Port 18# tag e                       (Enable tagging)
Current VLAN tag support: disabled
New VLAN tag support:     enabled
Port 18 changed to tagged.

Main# /cfg/port 20                      (Select uplink port 20)
>> Port 20# tag e                       (Enable tagging)
Current VLAN tag support: disabled
New VLAN tag support:     enabled
Port 20 changed to tagged.
>> Port 20# apply                       (Apply the port configurations)
```

2. VLAN とそのメンバポートを構成します。デフォルトでは、すべてのポートが VLAN 1 に所属しているため、VLAN 2 に属するポートだけ構成します。インターリンクポート 17、18 は VLAN 1 と 3 の両方に所属させる必要があります。

```
>> /cfg/l2/vlan 2

>> VLAN 2# add 1                                (Add port 1 to VLAN 2)
Current ports for VLAN 2: empty
Pending new ports for VLAN 2: 1

>> VLAN 2# add 20                               (Add port 20 to VLAN 2)
Current ports for VLAN 2: 1
Pending new ports for VLAN 2: 20

>> VLAN 2# add 23                               (Add port 23 to VLAN 2)
Port 23 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 2 [y/n]: y
Current ports for VLAN 2: 1, 20
Pending new ports for VLAN 2: 23

>> /cfg/l2/vlan 3
>> VLAN 3# add 17                               (Add port 17 to VLAN 3)
Current ports for VLAN 3: empty
Pending new ports for VLAN 3: 17

>> VLAN 3# add 18
Current ports for VLAN 3: 17                    (Add port 18 to VLAN 3)
Pending new ports for VLAN 3: 18

>> VLAN 3# add 20                               (Add port 20 to VLAN 3)
Current ports for VLAN 3: 17, 18
Pending new ports for VLAN 3: 20

>> /cfg/port 23/tagpvid                         (Disable tagpvid)
Current tag pvid support: enabled
Enter new tag pvid support [d/e]: d
UNTAG on pvid

>> apply                                       (Apply the port configurations)
>> save                                        (Save the port configurations)
```

## スイッチ 2 でのポートと VLAN の設定（AOS CLI の例）

スイッチ 2 でポートと VLAN を構成する手順は次のとおりです。

1. スイッチ 2 で、タグが必要なポートに VLAN タグを有効にします。ポート 4（サーバ 2 に接続）はタグなしのため、設定はしません。

```
Main# /cfg/port 2                        (Select port 2: connection to server 1)
>> Port 2# tag e
Current VLAN tag support: disabled
New VLAN tag support:     enabled
Port 2 changed to tagged.

Main# /cfg/port 17                       (Select crosslink link port 17)
>> Port 17# tag e                                  (Enable tagging)
Current VLAN tag support: disabled
New VLAN tag support:     enabled
Port 17 changed to tagged.

Main# /cfg/port 18                           (Select crosslink link port 18)
>> Port 18# tag e                                    (Enable tagging)
Current VLAN tag support: disabled
New VLAN tag support:     enabled
Port 18 changed to tagged.

Main# /cfg/port 20                                    (Select uplink port 20)
>> Port 20# tag e                                           (Enable tagging)
Current VLAN tag support: disabled
New VLAN tag support:     enabled
Port 20 changed to tagged.

>> Port 20# apply                             (Apply the port configurations)
```

2. VLAN とそのメンバポートを構成します。デフォルトでは、すべてのポートが VLAN 1 に所属しているため、他の VLAN に属するポートだけ構成します。

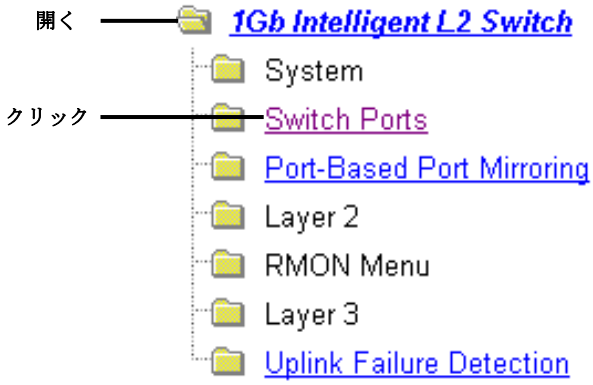
```
>> /cfg/l2/vlan 3
>> VLAN 3# add 2
Current ports for VLAN 3: empty
Pending new ports for VLAN 3: 2

>> VLAN 3# add 4
Current ports for VLAN 3: 2
Pending new ports for VLAN 3: 17

>> VLAN 3# add 17
Current ports for VLAN 3: 2, 4
Pending new ports for VLAN 3: 17

>> VLAN 3# add 18
Current ports for VLAN 3: 2, 17
Pending new ports for VLAN 3: 18

>> VLAN 3# add 20
Current ports for VLAN 3: 2, 17, 18
Pending new ports for VLAN 3: 20

>> /cfg/l2/vlan 4
>> VLAN 4# add 2
Current ports for VLAN 4: empty
Pending new ports for VLAN 4: 2

>> VLAN 4# add 23
Port 23 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 4 [y/n]: y
Current ports for VLAN 4: 2
Pending new ports for VLAN 4: 23

>> /cfg/port 4/tagpvid
Current tag pvid support: enabled
Enter new tag pvid support [d/e]: d
UNTAG on pvid

>> /cfg/port 23/tagpvid
Current tag pvid support: enabled
Enter new tag pvid support [d/e]: d
UNTAG on pvid


>> apply                                     (Apply the port configurations)
>> save                                      (Save the port configurations)
```

外部レイヤ 2 スイッチも VLAN とタグを設定する必要があります。

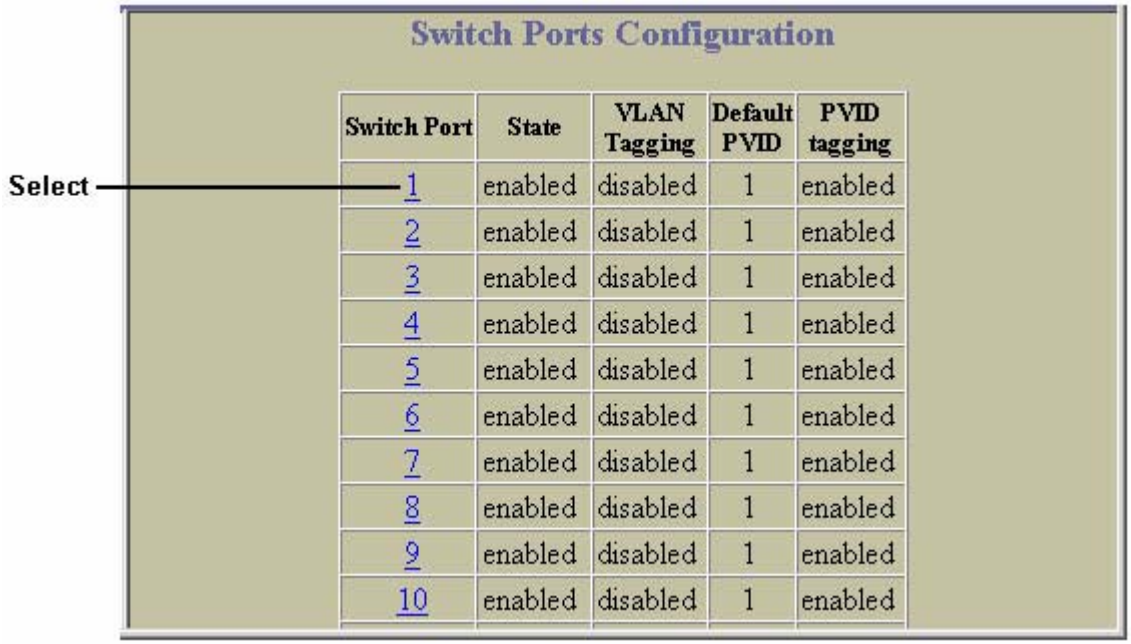
## スイッチ 1 でのポートと VLAN の構成（BBI の例）

スイッチ 1 でポートと VLAN を構成する手順は次のとおりです。

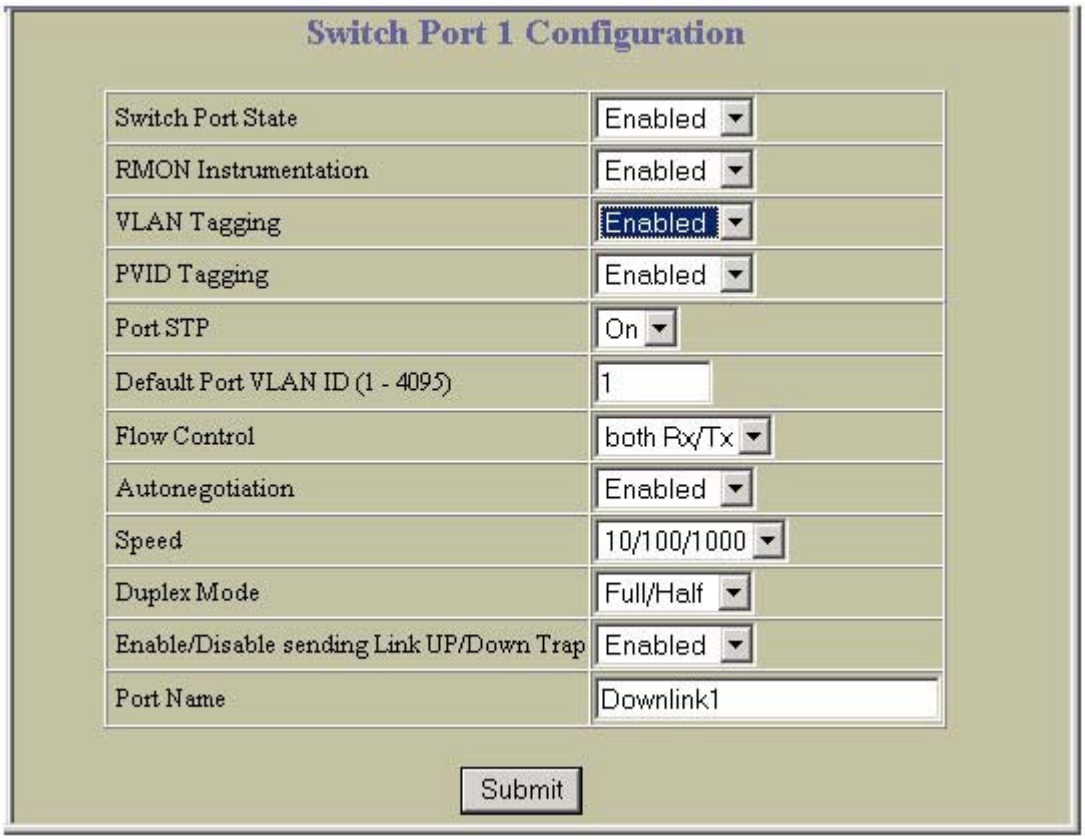
1. スイッチ 1 で、タグが必要なポートに VLAN タグを有効にします。
   a. ツールバーの CONFIGURE ボタンをクリックします。
   b. Switch フォルダを開き、Switch Ports を選択します（フォルダではなく、下線が引かれたフォルダ名をクリックしてください）。




   c. 該当のポート番号をクリックして選択します。



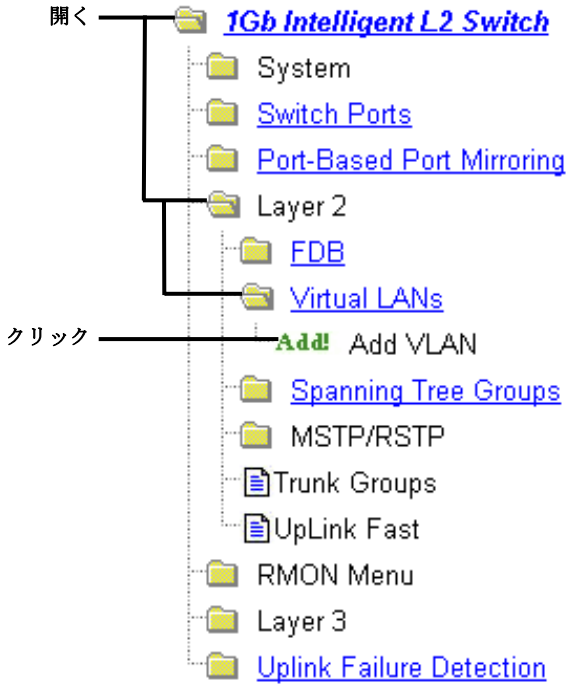
d. ポートと VLAN タグを有効にします。



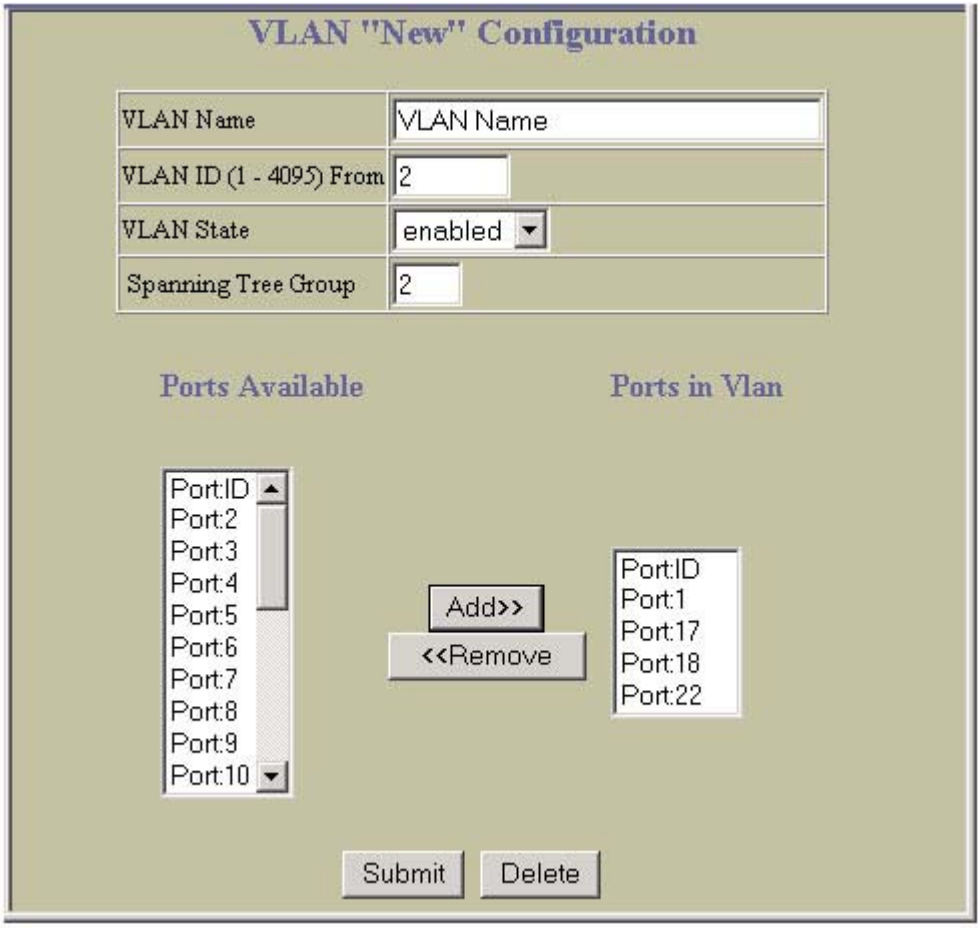

e. Submit をクリックします。

2. VLAN とそのメンバポートを設定します。

a. Virtual LANs フォルダを開き、Add VLAN を選択します。



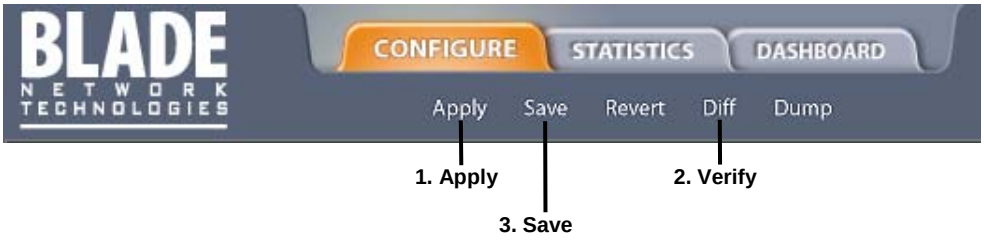
b. VLAN 名、VLAN ID を入力し、VLAN を有効 (enabled) にします。ポートを追加するには、Ports Available リストの各ポートを選択して、Add をクリックします。デフォルトでは、すべてのポートが VLAN 1 に所属しているため、VLAN 2 に属するポートだけ構成します。インターリンクポート 17、18 は VLAN 1 と 3 の両方に所属させる必要があります。




c. Submit をクリックします。

外部レイヤ 2 スイッチも VLAN とタグを設定する必要があります。

3. 設定を適用、確認、保存します。



# FDB スタティックエントリ

フォワーディングデータベース (FDB) のスタティックエントリにより、検索のためにポートをあふれさせることなく、スイッチからパケットを送り出すことができます。FDB スタティックエントリは、特定のポートと VLAN に関連付けた MAC アドレスです。本スイッチがサポートするスタティックエントリは 128 です。AOS CLI では`/cfg/l2/fdb/static` コマンドにより手動で設定できます。

FDB スタティックエントリは永続的なエントリのため、FDB エージング値は適用されません。FDB への追加、削除は手動で行います。

スタティックエントリで登録されている MAC の受信フレームは、そのスタティックエントリで設定されているポートでのみ使用できます。

## FDB スタティックエントリ用のトランクサポート

次のトランクグループのメンバであるポートに、FDB スタティックエントリを追加できます。

- スタティック（手動設定）トランクグループ
- ダイナミック(LACP)　トランクグループ

トランクグループは FDB スタティックエントリをサポートします。スタティックエントリがあるポートが故障すると、トランクの他のポートがトラフィックを処理します。ポートがトランクから削除されると、スタティックエントリも削除されますが、ポートには設定されたままです。

設定した場合、FDB 情報コマンド`/info/l2/fdb` でスタティック FDB エントリのトランク状態を表示できます。

```
>> Forwarding Database# dump
     MAC address     VLAN  Port  Trnk  State
  -----------------  ----  ----  ----  -----
  00:00:2e:9b:db:f8     1           1   TRK
  00:00:5e:00:01:f4     1  24           FWD
  00:01:81:2e:b5:60     1  24           FWD
  00:02:a5:e9:76:30     1           1   TRK
  00:03:4b:e2:15:f1     1  24           FWD
```

## スタティック FDB エントリの設定

スタティック FDB エントリを設定するには、次の処理を実行します。

```
Main# /cfg/l2/fdb/static                      (Select static FDB menu)
>> Static FDB# add 00:60:af:00:02:30
Enter VLAN number: 2
Enter port (1-24): 2
>> Static FDB# apply                          (Apply the configuration)
>> Static FDB# save                           (Save the configuration)
```

# Spanning Tree Protocol

## はじめに

スパニングツリープロトコル (STP) は、ネットワークに複数のパスが存在する場合、スイッチがもっとも効率的なパスだけを使用するようにネットワークを構成するプロトコルです。本章は以下の節からなります。

- 概要
- ブリッジプロトコルデータユニット (BPDU)
- スパニングツリーグループ (STG) の構成ガイドライン
- 複数のスパニングツリー

## 概要

スパニングツリープロトコル (STP) は、ブリッジネットワークやスイッチネットワーク内の論理ループを検出、削除します。冗長データパスを強制的に待機（ブロック）状態にします。複数のパスが存在すると、スイッチがもっとも効率的なパスだけを使用するようにネットワークを構成します。そのパスが故障すると、別のパスをアクティブにしてネットワーク動作を維持します。

スイッチは、デフォルトでは、STG 1 に IEEE 802.1D Spanning Tree Protocol、STG 2～32 に Per VLAN Spanning Tree Protocol (PVST+) を適用します。

> **注**：IEEE 802.1w Rapid Spanning Tree Protocol、IEEE 802.1s Multiple Spanning Tree Protocol もサポートしています。詳細については、「RSTP と MSTP」の章を参照してください。

## ブリッジプロトコルデータユニット

スパニングツリーを生成するには、スイッチが BPDU を作成しポートから送り出します。スパニングツリーに参加する、レイヤ 2 ネットワークのすべてのスイッチが、BPDU の交換によりネットワーク内の他のスイッチに関する情報を収集します。

BPDU は、一定間隔（通常 2 秒）で送出される 64 バイトパケットです。IP ルーティングにおける「ハローパケット」とほぼ同様で、パスの確立に使用します。BPDU には、ブリッジアドレス、MAC アドレス、ブリッジプライオリティ、ポートプライオリティ、ポートパスコストなど、転送ブリッジとそのポートに関する情報があります。ポートにタグを付けると、タグ付き情報が入っている特殊な BPDU を送出します。

スイッチが BPDU を受信したときに通常行う処理は、受信 BPDU をスイッチが独自に送信する BPDU と比較することです。受信 BPDU のプライオリティ値がスイッチ BPDU の値よりゼロに近い場合、スイッチ BPDU が受信 BPDU と置き換わります。次に、独自のブリッジ ID 番号を追加し、BPDU のパスコストをインクリメントします。この内容をもとに冗長パスをブロックします。

### BPDU フォワーディングパスの決定

フォワーディングに使用するポート、ブロックするポートを決める場合、各ブリッジのプライオリティ ID など、BPDU に関する情報を利用します。次に、「最小ルートコスト」に基づく手法で計算を行い、フォワーディングにもっとも効率的なパスを決定します。

## ブリッジプライオリティ

ブリッジプライオリティパラメータによって、ネットワーク上のどのブリッジを STP ルートブリッジにするかを決めます。スイッチをルートブリッジにする場合、ネットワーク上の他のスイッチやブリッジのどれよりもブリッジプライオリティ値を小さくします。値が小さい方が、プライオリティは高くなります。ブリッジプライオリティの設定は、AOS CLI の場合、`/cfg/l2/stp/brg/prior` コマンドで行います。

## ポートプライオリティ

どのブリッジポートを指定ポートにするかを決めるパラメータです。複数のブリッジポートが 1 セグメントに接続されているネットワークトポロジでは、ポートプライオリティ値が最小のポートが、そのセグメントの指定ポートになります。ポートプライオリティの設定は、AOS CLI の場合、`/cfg/l2/stp/port x/prior` コマンドで行います。

## ポートパスコスト

ギガビットイーサネットなどの高帯域幅ポートに小さい値を割り当てて、その利用を促進するのが、ポートパスコストです。その目的は、最高速リンクを使用して、コストが最小のルートが選択されるようにすることです。値を 0 にすると、リンク速度に基づいて、ポートコストが動的に計算されます。これはリンク速度を強制的に決めるときに機能するため、「オートネゴシエーションによるリンク速度」には適用されません。

デフォルトでは、リンク速度に関わらず、すべてのスイッチポートでパスコストは 4 に設定されています。リンク速度に基づいてパスコストを動的に使用するには、パスコストを 0 に設定します。たとえば、パスコストが 0 に設定されている場合、

- 100Mbps リンクのパスコストは 19 になります。
- 10Mbps リンクのパスコストは 100 になります。

# スパニングツリーグループの構成ガイドライン

この節では、スパニングツリーグループ (STG) の構成に重要な事項について説明します。

## デフォルトのスパニングツリー構成

デフォルト構成では、Port19 を除いた全ポートが、ID 1 の単一 STG に組み込まれています。これをデフォルト STG といいます。デフォルト STG と、STG32（マネジメントインタフェース用）を除くすべての STG が空で、使用する場合、VLAN を該当の STG に追加します。

ポートを STG に直接割り当てることはできません。ポートを VLAN に追加し、その VLAN を STG に追加します。デフォルトでは、STG 1〜31 が有効で、1〜31 の ID 番号を割り当てます。デフォルトでは STG 32 は無効で、管理 VLAN 4095 があります。

STG を削除することはできません。無効にできるだけです。VLAN メンバが入ったまま STG を無効にすると、その VLAN に属するすべてのポートでスパニングツリーがオフになります。

## スパニングツリーグループへの VLAN の追加

デフォルトの VLAN 1 以外に VLAN が存在しないという条件でポートを VLAN に追加する方法については、本章の「VLAN の生成」を参照してください。

VLAN を STG に追加するには、`/cfg/l2/stp <stg number>/add <vlan number>`コマンドを使用します。

## VLAN の生成

VLAN を生成すると、デフォルトの STG 1 に自動的に属することになります。別の STG に所属させる場合、該当の STG に割り当てて移動します。

新たに生成した VLAN を既存 STG に移動するには、

1. VLAN を生成します。
2. VLAN を既存 STG に追加します。

VLAN を生成するときには、以下についても考慮する必要があります。

- 複数の STG に属することはできません。
- 複数のスイッチにまたがる VLAN は、全スイッチにわたって同じスパニングツリーグループ（STG ID が同じ）内にマッピングする必要があります。

## VLAN タグ付きポートのルール

VLAN タグ付きポートのルールは次のとおりです。

- タグを付けると、複数の STG に属することができます。
- タグ付きポートが複数の STG に属する場合、送出する BPDU にタグを付けて、STG 毎に BPDU を区別します。
- タグなしポートは複数の STG に属することはできません。

## STG へのポートの追加、STG からの削除

STG へのポートの追加、STG からの削除については、次のルールがあります。

- デフォルトでは、Port19 を除くすべてのポートが VLAN 1 と STG 1 に属します。
- 各ポートは、常に、少なくとも 1 つの VLAN のメンバ、各 VLAN は少なくとも 1 つの STG のメンバです。VLAN 内のポートメンバ、STG 内の VLAN メンバを変更できます。ポートを STG から別の STG に移動するには、そのポートが属する VLAN を移動するか、STG に属する VLAN にポートを移動します。
- ポートを VLAN から削除すると、その VLAN が属する STG からも削除されます。しかし、同じ STG の別の VLAN にも属する場合、その STG に留まります。
- タグなしポートをデフォルト以外の VLAN、STG から削除すると、VLAN 1 と STG 1 に追加されます。

ポート、トランクグループ、VLAN、スパニングツリー間の関係を次の表に示します。

表10 ポート、トランクグループ、VLAN

| スイッチエレメント | 所属 |
|---|---|
| ポート | トランクグループまたは 1 つ以上の VLAN |
| トランクグループ | 1 つ以上の VLANs |
| VLAN（デフォルト以外） | 1 つのスパニングツリーグループ |

## ポートとトランクグループへのコストの割当て

トランクグループをスパニングツリーグループに参加させる場合、ポートコストとトランクコストを手動で割り当てて、各トランクグループの STP コストがトランクグループ内の各ポートのコストより低くなるようにします。これで、トランクグループはフォワーディング状態に留まります。

# 複数のスパニングツリー

各スイッチは最大で 32 のスパニングツリーグループ (STG) をサポートします。複数の STG で複数のデータパスが得られ、負荷バランシングや冗長化に利用できます。

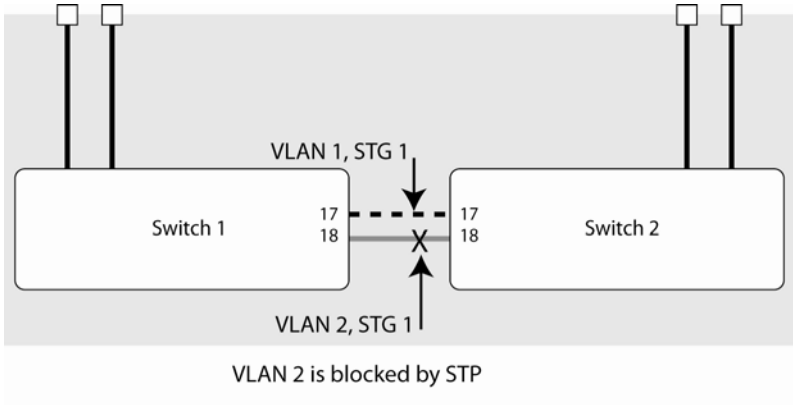
複数の STG を使用する 2 台のスイッチの各々に独立のリンクが可能です。それには、各パスを別々の VLAN で構成し、各 VLAN を別々の STG に割り当てます。各 STG は独立しています。独自の BPDU を送信し、また、個別に構成しなければなりません。

STG つまりブリッジグループは、VLAN が 1 つ以上で、ループのないトポロジを形成します。本スイッチは 32 の STG の同時動作をサポートします。デフォルトの STG 1 は IEEE 802.1D STP をサポートし、複数の VLAN が可能です。他の STG はどれも PVST+をサポートし、VLAN は各々1 つだけです。IEEE 802.1s MSTP モードを使用した場合、STG 2～32 で複数の VLAN をサポートできます。詳細については、「RSTP と MSTP」の章を参照してください。

## 複数のスパニングツリーが必要な理由

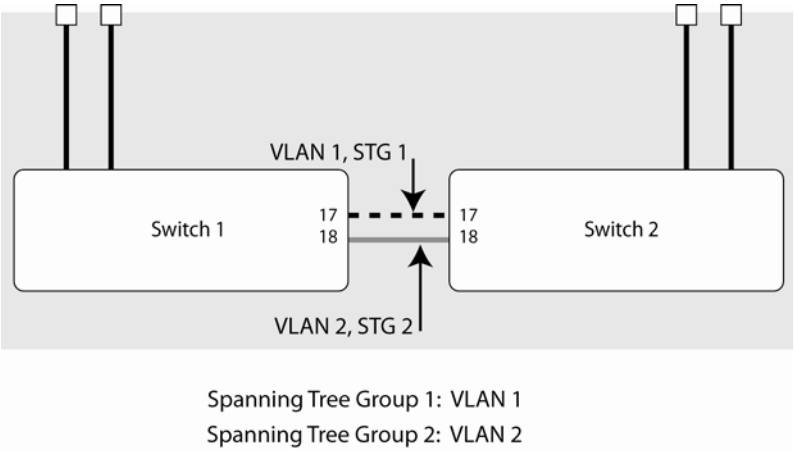
次の図に、複数のスパニングツリーが必要な理由を示す簡単な例を示します。この例では、ポート 17、18 がトランクグループ 1 には入っていないものとしています。2 つの VLAN（VLAN 1 と VLAN 2）がスイッチ 1 とスイッチ 2 の間に存在します。同じスパニングツリーグループが両方のスイッチで有効であると、見かけ上ループと判断し、スイッチ 2 のポート 18 をブロックし、VLAN 2 でのスイッチ間通信を遮断します。

図8　スパニングツリープロトコルの 1 インスタンスに 2 つの VLAN がある場合




次の図の場合、VLAN 1 と VLAN 2 は別々のスパニングツリーグループに属しています。スパニングツリーの 2 つのインスタンスで、ループを作らずにトポロジを分離するので、両 VLAN とも、接続性を失うことなく、スイッチ間でパケットを転送できます。

図9　スパニングツリープロトコルの別々のインスタンスに各 VLAN がある場合



## スパニングツリーグループ内の VLAN

次の表に、各スパニングツリーグループにどのスイッチポートが参加しているかを示します。デフォルトでは、サーバポート（ポート 1～16）は、該当の VLAN のメンバであっても、スパニングツリーには参加していません。

表11 スパニングツリーグループへの VLAN の参加

| | VLAN 1 | VLAN 2 |
|---|---|---|
| スイッチ 1 | スパニングツリーグループ 1<br>ポート 17 | スパニングツリーグループ 2<br>ポート 18 |
| スイッチ 2 | スパニングツリーグループ 1<br>ポート 17 | スパニングツリーグループ 2<br>ポート 18 |

## 複数のスパニングツリーグループの構成

この節では、各 VLAN をスイッチ 1、2 の個別のスパニングツリーグループに割り当てる方法について説明します。

デフォルトでは、スパニングツリーグループ 2～31 が空、設定済みのすべての VLAN（VLAN4095 は除く）はスパニングツリーグループ 1 に入ります。STP/PVST+動作時、デフォルトのスパニングツリーグループ 1 には複数の VLAN が入りますが、スパニングツリーグループ 2～32 では VLAN を 1 つだけ所属させることができます。

**注:スパニングツリーグループの各インスタンスは、デフォルトでは、有効になっています。**

### スイッチ 1 の設定（AOS CLI の例）

1. 「VLAN」の章の「スイッチ 1 でのポートと VLAN の設定（AOS CLI の例）」で説明したように、スイッチ 1 にポートと VLAN のメンバを構成します。
2. VLAN 2 をスパニングツリーグループ 2 に追加します。

```
>> /cfg/l2/stp 2                          (Select Spanning Tree Group 2)
>> Spanning Tree Group 2# add 2                 (Add VLAN 2)
```

   VLAN 2 がスパニングツリーグループ 1 から自動的に削除されます。
3. 適用、保存します。

```
>> apply                                 (Apply the port configurations)
>> save                                  (Save the port configurations)
```

### スイッチ 2 の設定（AOS CLI の例）

1. 「VLAN」の章の「スイッチ 2 でのポートと VLAN の設定（AOS CLI の例）」で説明したように、ポートと VLAN のメンバを構成します。
2. VLAN 2 をスパニングツリーグループ 2 に追加します。

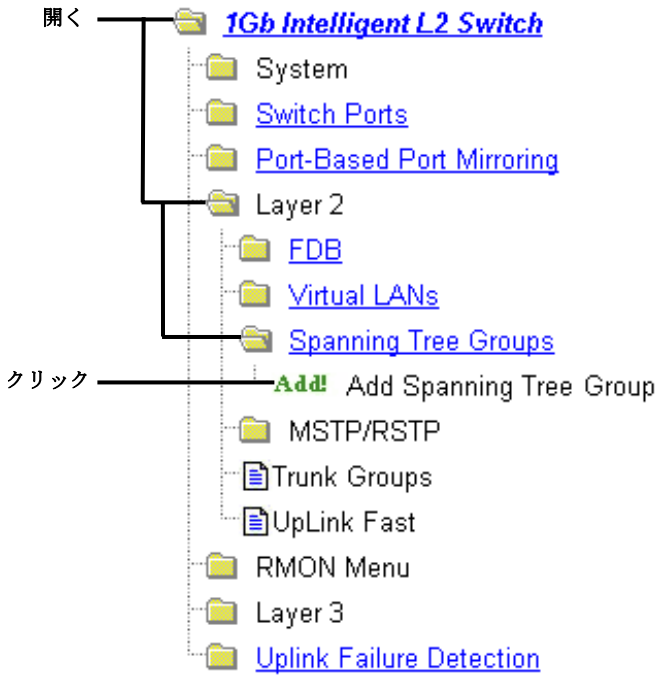
```
>> /cfg/l2/stp 2                          (Select Spanning Tree Group 2)
>> Spanning Tree Group 2# add 2           (Add VLAN 2)
```

3. VLAN 2 がスパニングツリーグループ 1 から自動的に削除されます。
4. 適用、保存します。

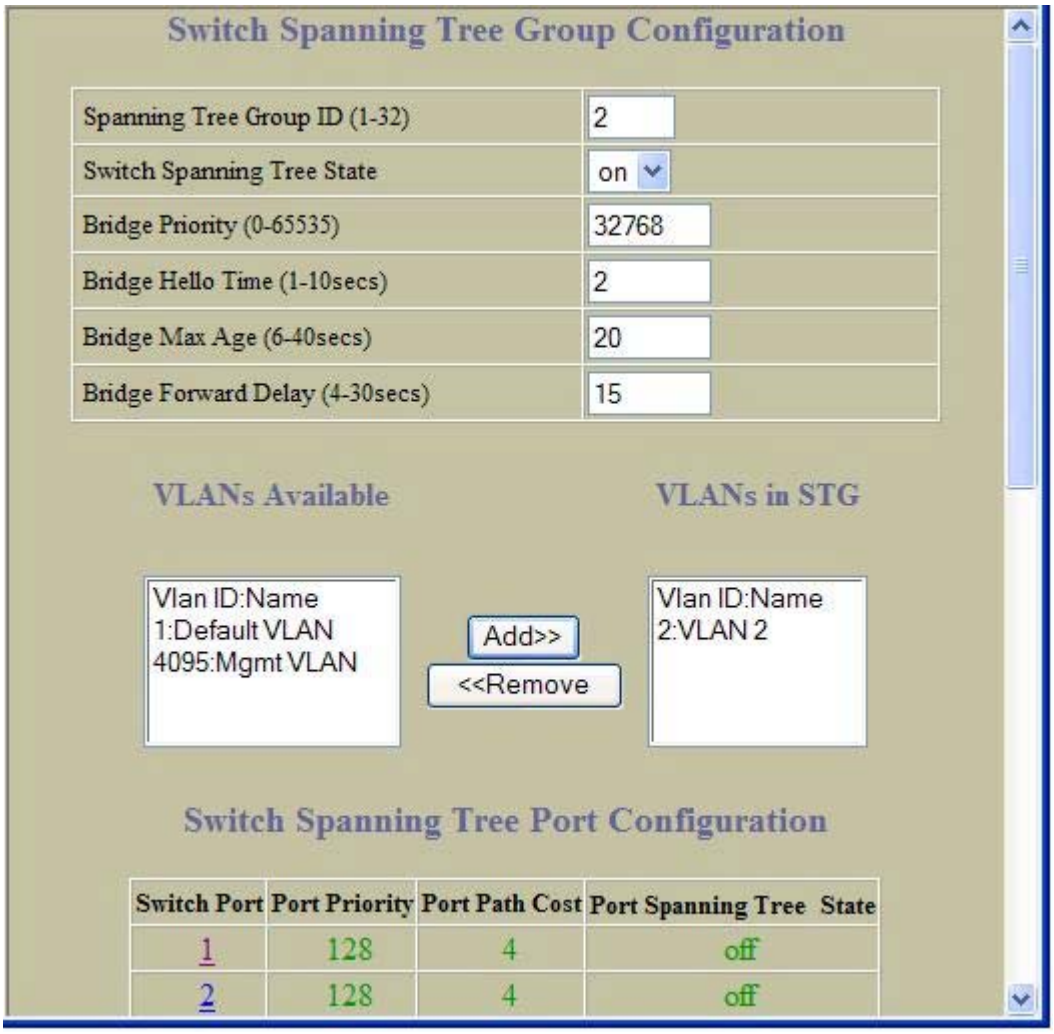
```
>> apply                                 (Apply the port configurations)
>> save                                  (Save the port configurations)
```

## スイッチ 1 の設定（BBI の例）

1. 「VLAN」の章の「スイッチ 1 でのポートと VLAN の設定（BBI の例）」で説明したように、スイッチ 1 にポートと VLAN のメンバを設定します。
2. VLAN 2 をスパニングツリーグループ 2 に追加します。
   a. ツールバーの CONFIGURE ボタンをクリックします。
   b. Spanning Tree Groups フォルダを開き、Add Spanning Tree Group を選択します。

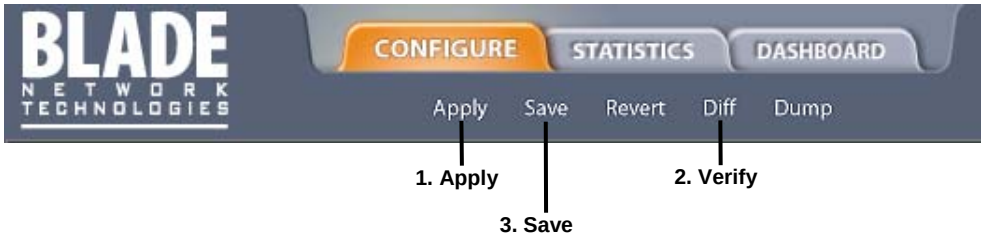


c. 次の図で、Spanning Tree Group ID を入力し、Switch Spanning Tree State を on にします。VLAN をスパニングツリーグループに追加するには、VLANs Available リストで選択して、Add をクリックします。VLAN 2 がスパニングツリーグループ 1 から自動的に削除されます。




d. 下にスクロールして、Submit をクリックします。

3. 設定を適用、確認、保存します。



# Port Fast Forwarding

Port Fast Forwarding を行うと、スパニングツリーに参加しているポートが、リスニング状態、ラーニング状態を省略して、直接フォワーディング状態に入ることができます。フォワーディング状態にある間、BPDU を見てループがあるか調べ、通常 STG 動作（プライオリティが低かった場合など）で指示された場合、ブロッキング状態に遷移します。

この機能があるため、スイッチと高速パス（NIC チーミング機能）が十分に連携できます。

## Port Fast Forwarding の設定

外部ポートでポート高速フォワーディングを有効にする CLI コマンドを、次に示します。

```
>> # /cfg/l2/stp 1/port 20            (Select port 20)
>> Spanning Tree Port 20# fastfwd ena (Enable Port Fast Forwarding)
>> Spanning Tree Port 20# apply       (Make your changes active)
>> Spanning Tree Port 20# save        (Save for restore after reboot)
```

# Fast Uplink Convergence

Fast Uplink Convergence を有効にすると、スパニングツリープロトコルを使用するレイヤ 2 ネットワーク内の一次リンクやトランクグループの故障からすぐに復旧できます。通常の復旧では 60 秒ほどかかりますが、その間に、バックアップリンクがブロッキングからリスニング、ラーニング、さらにフォワーディング状態に遷移します。Fast Uplink Convergence を有効になると、直ちに二次パスをフォワーディング状態にして、FDB と ARP テーブル内のアドレスのマルチキャストを二次リンクで送信します。したがって、アップストリームスイッチで新しいパスが分かります。

## 構成ガイドライン

Fast Uplink Convergence を有効にすると、スイッチが自動的に以下の構成変更を行います。

- ブリッジプライオリティを 65500 に上げて、ルートスイッチにならないようにします。
- すべての VLAN とスパニングツリーグループについて、全ての外部ポートのコストを 3000 上げます。したがって、他のパスがないということがない限り、トラフィックが本スイッチを通じて別のスイッチに至ることは決してありません。

Fast Uplink Convergence を無効にすると、すべての STP グループでブリッジプライオリティとパスコストがデフォルト値に設定されます。

## Fast Uplink Convergence の設定

外部ポートで Fast Uplink Convergence を有効にする CLI コマンドを、次に示します。

```
>> # /cfg/l2/upfast ena    (Enable Fast Uplink convergence)
>> Layer 2# apply         (Make your changes active)
>> Layer 2# save          (Save for restore after reboot)
```

# RSTP と MSTP

## はじめに

スパニングツリープロトコル (IEEE 802.1D) の拡張で、スパニングツリーグループ 1 において迅速にパス移行を行うプロトコルに Rapid Spanning Tree Protocol (IEEE 802.1w) があります。さらに、Rapid Spanning Tree Protocol の拡張で、VLAN 環境において迅速なパス移行と負荷バランシングの両方を行うものに Multiple Spanning Tree Protocol (IEEE 802.1s) があります。

本章では、これらのプロトコルについて説明します。

- Rapid Spanning Tree Protocol (RSTP)
- Multiple Spanning Tree Protocol (MSTP)

## Rapid Spanning Tree Protocol (RSTP)

音声やビデオなどディレイが問題になるトラフィックを搬送するネットワークに重要な、高速再構成を行うスパニングツリープロトコルです。物理トポロジやその構成パラメータが変化したときに、ネットワークのアクティブトポロジを再構成する時間を大幅に短縮します。ブリッジされた LAN トポロジを単一スパニングツリーにまで縮小します。

スパニングツリープロトコルの詳細については、「Spanning Tree Protocol」の章を参照してください。

RSTP パラメータはスパニングツリーグループ 1 に設定します。STP グループ 2～32 は RSTP に適用しないので、消去しなければなりません。RSTP をサポートする新しい STP パラメータがあり、一部の値が既存のスパニングツリーのパラメータとは異なるためです。

RSTP は、802.1D スパニングツリープロトコルを実行する装置に適応します。スイッチが 802.1D BPDU を検出した場合、802.1D 適合したデータユニットで応答します。Per VLAN Spanning Tree (PVST) とは互換ではありません。

### ポート状態の変化

スパニングツリーのフォワーディングプロセス、ラーニングプロセスをポート状態で制御します。RSTP では、ポート状態を、廃棄、ラーニング、フォワーディングに集約しています。

表12 RSTP と STP のポート状態

| ポート動作ステータス | STP ポート状態 | RSTP ポート状態 |
|---|---|---|
| 有効 | ブロッキング | 廃棄 |
| 有効 | リスニング | 廃棄 |
| 有効 | ラーニング | ラーニング |
| 有効 | フォワーディング | フォワーディング |
| 無効 | 無効 | 廃棄 |

### ポートタイプとリンクタイプ

スパニングツリー構成には、RSTP、MSTP をサポートする以下のパラメータがあります。

- エッジポート
- リンクタイプ

これらのパラメータはスパニングツリーグループ 1～32 用に設定しますが (`/cfg/l2/stp x/port x`)、RSTP/MSTP をオンにしたときしか有効になりません。

### エッジポート

サーバネットワークかスタブネットワークに接続するポートをエッジポートと言います。したがって、ポート 1～16 でエッジを有効にする必要があります（ポート 1～16 はデフォルトで有効です）。エッジポートは、リンクするとすぐにフォワーディングを開始できます。

エッジポートはスパニングツリーに加わらず、BPDU を受信しません。エッジポートとして設定されているポートで BPDU を受信すると、再びエッジを有効にするまで STP 処理を行います。

### リンクタイプ

RSTP に関連してポートがどのように動作するかはリンクタイプで決まります。リンクタイプは Duplex モードに対応します。全二重モードは二点間(p2p)リンク、半二重モードは共用リンクです。リンクタイプとして auto を選択すると、ポートが動的にリンクタイプを構成します。

## RSTP 構成ガイドライン

この節では、Rapid Spanning Tree グループの構成に重要な事項について説明します。

- RSTP がオンの場合、STP パラメータは STP グループ 1 にしか適用されません。
- RSTP をオンにすると、グループ 1 以外の STP グループの VLAN すべてがグループ 1 に移動します。他の STP グループ（2～32）はオフになります。

## RSTP 構成の例

以下では、AOS CLI またはブラウザベースインタフェース(BBI)で RSTP を設定する手順を示します。

### RSTP の設定（CLI の例）

1. 「VLAN」の章の「ポートと VLAN の設定（AOS CLI の例）」で説明したように、ポートと VLAN のメンバを設定します。
2. スパニングツリーモードを RSTP に設定します。

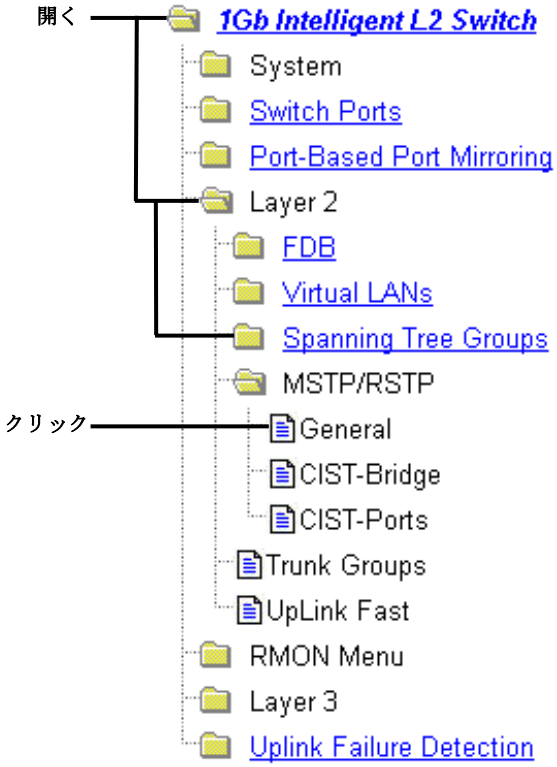
```
>> /cfg/l2/mrst                    (Select Multiple Spanning Tree menu)
>> Multiple Spanning Tree# mode rstp   (Set mode to Rapid Spanning Tree)
>> Multiple Spanning Tree# on             (Turn Rapid Spanning Tree on)
```

3. 設定を適用、保存します。

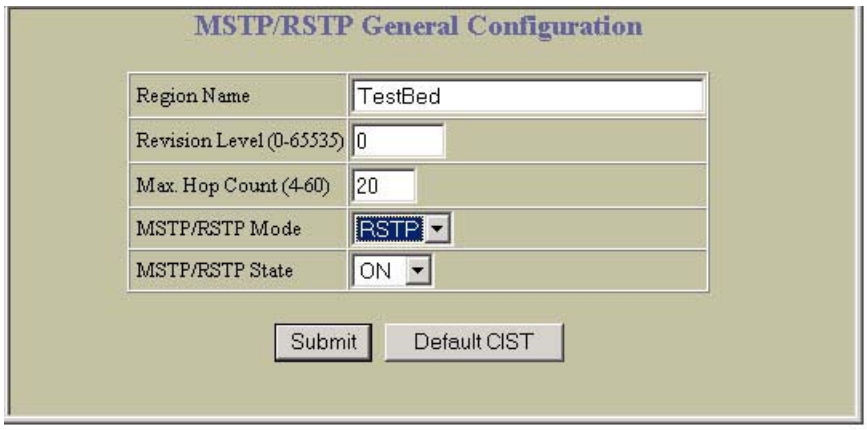
```
>> # apply               (Apply the configuration)
>> # save                (Save the configuration)
```

## RSTP プロトコルの設定（BBI の例）

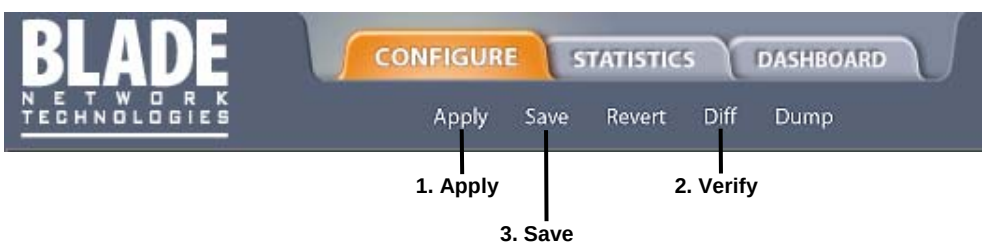
1. 「VLAN」章の「ポートと VLAN の設定（BBI の例）」で説明したように、ポートと VLAN のメンバを設定します。
2. RSTP パラメータを設定します。
   a. ツールバーの CONFIGURE ボタンをクリックします。
   b. MSTP/RSTP フォルダを開き、General を選択します。




   c. RSTP モードを選択し、MSTP/RSTP State を ON にします。




   d. Submit をクリックします。
3. 設定を適用、確認、保存します。



# Multiple Spanning Tree Protocol (MSTP)

複数のスパニングツリーグループにより、IEEE 802.1w Rapid Spanning Tree Protocol を拡張したものが IEEE 802.1s Multiple Spanning Tree Protocol です (MSTP)。STP グループ 1～32 に対応する最大 32 のスパニングツリーインスタンスを保持します。

MSTP では、複数の VLAN を各スパニングツリーインスタンスにマッピングできます。スパニングツリーインスタンス同士は互いに独立です。異なる VLAN に割り当てたフレームは別々のパスに追従し、各パスは独立のスパニングツリーインスタンスに基づきます。こうすることにより、データトラフィックに複数のフォワーディングパスが得られるため、負荷バランシングが可能になり、多数の VLAN のサポートに必要なスパニングツリーインスタンスの数を低減できます。

## MSTP リージョン

同じ属性を共有する相互接続ブリッジのグループを MSTP リージョンと言います。リージョン内の各ブリッジは以下の属性を共有しなければなりません。

- 英数字名
- リビジョンレベル
- VLAN-STG 間マッピング

MSTP は、リージョンのサポートにより、迅速な再構成、スケーラビリティ、コントロールを行い、各リージョン内で複数のスパニングツリーインスタンスをサポートします。

## Common Internal Spanning Tree (CIST)

スパニングツリープロトコルの一般的形式の一つで、1 つのスパニングツリーインスタンスを MSTP リージョン全体で使用できるプロトコルです。スイッチがレガシ装置（IEEE 802.1D (STP) を実行する装置を含む）と相互運用できます。

CIST では、MSTP リージョンがリージョン外の他のブリッジに対する仮想ブリッジとして機能でき、また、1 つのスパニングツリーインスタンスがブリッジと連携できます。

CIST はデフォルトのスパニングツリーグループです。VLAN を STG 1～32 から削除すると、自動的に CIST のメンバになります。

CIST ポート構成では、ハロー時間、エッジポートステータス（有効／無効）、リンクタイプなどの設定があります。これらのパラメータはスパニングツリーグループ 1～32 には影響しません。また、CIST を使用するときのみ適用されます。

## MSTP 構成ガイドライン

この節では、MSTP グループの構成に重要な事項について説明します。

- MSTP をオンにすると、VLAN 1 は Common Internal Spanning Tree (CIST) に自動的に移動します。
- リージョン名とリビジョンレベルを設定する必要があります。リージョン内のブリッジはリージョン名とリビジョンレベルが同じでなければなりません。
- VLAN および STP グループマッピングは、リージョン内のすべてのブリッジで同じでなければなりません。
- どの VLAN も CIST に移動できます。
- VLAN 1 はどのスパニングツリーグループにも移動できます。

# MSTP 構成の例

以下では、CLI または BBI で MSTP を設定する手順を示します。

## MSTP の設定（AOS CLI の例）

1. 「VLAN」章の「ポートと VLAN の設定（AOS CLI の例）」で説明したように、ポートと VLAN のメンバを構成します。
2. モードを MSTP に設定し、MSTP リージョンパラメータを設定します。

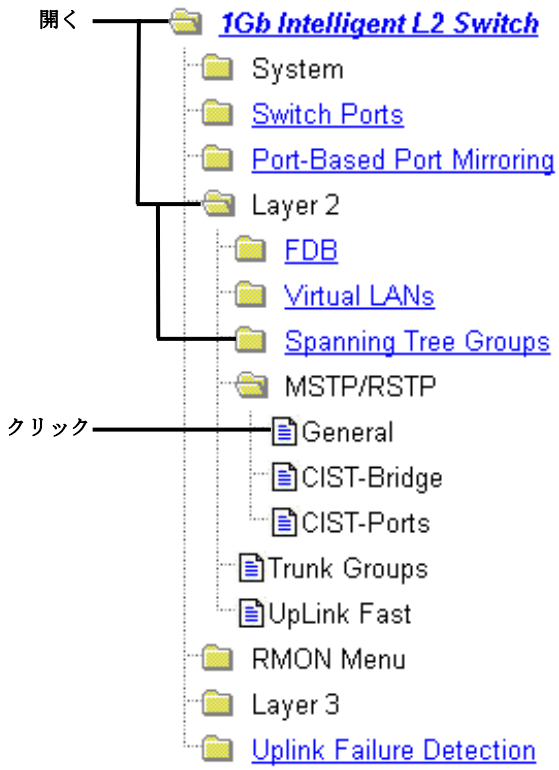
```
>> /cfg/l2/ mrst                          (Select Multiple Spanning Tree menu)
>> Multiple Spanning Tree# mode mstp      (Set mode to
                                           Multiple Spanning Trees)
>> Multiple Spanning Tree# on             (Turn Multiple Spanning Trees on)
>> Multiple Spanning Tree# name xxxxxx    (Define the Region name)
>> Multiple Spanning Tree: rev xx         (Define the Region revision level)
```

3. VLAN をスパニングツリーグループに割り当てます。

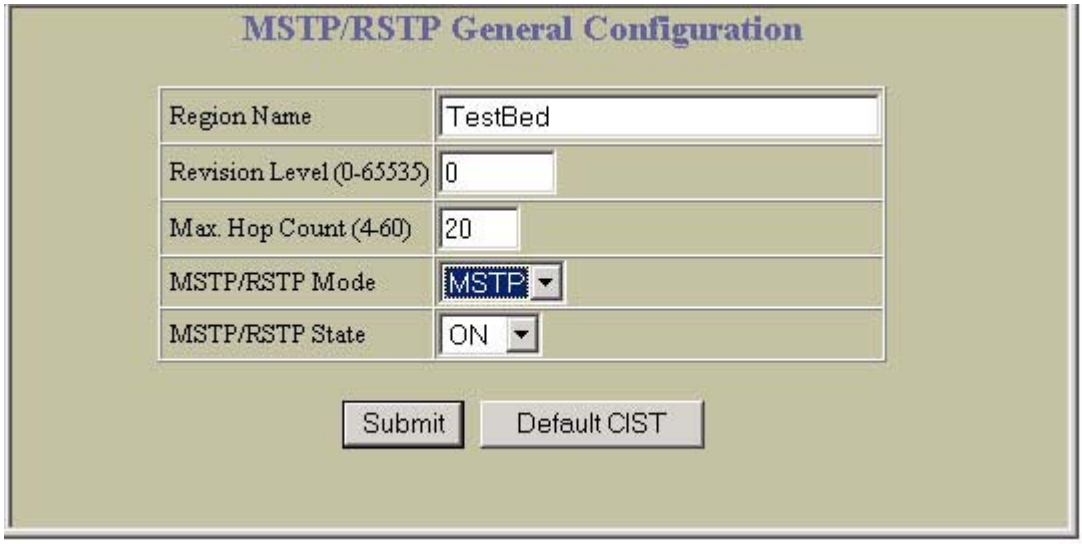
```
>> /cfg/l2/stp 2                          (Select Spanning Tree Group 2)
>> Spanning Tree Group 2# add 2           (Add VLAN 2)
>> Spanning Tree Group 2# apply           (Apply the configurations)
```

## MSTP の設定（BBI の例）

1. 「VLAN」章の「ポートと VLAN の設定（BBI の例）」で説明したように、ポートと VLAN のメンバを構成します。
2. MSTP の General パラメータを設定します。
   a. ツールバーの CONFIGURE ボタンをクリックします。
   b. MSTP/RSTP フォルダを開き、General を選択します。



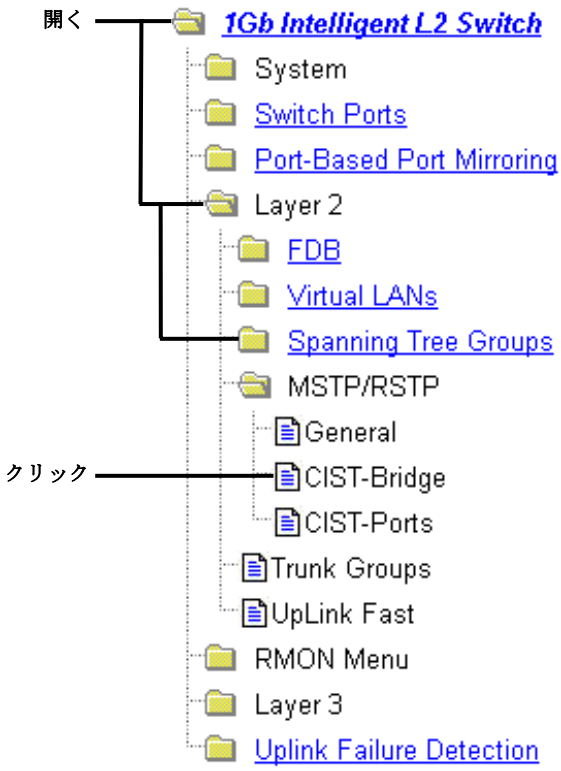
c. リージョン名とリビジョンレベルを入力します。MSTP モードを選択し、MSTP/RSTP State を ON にします。



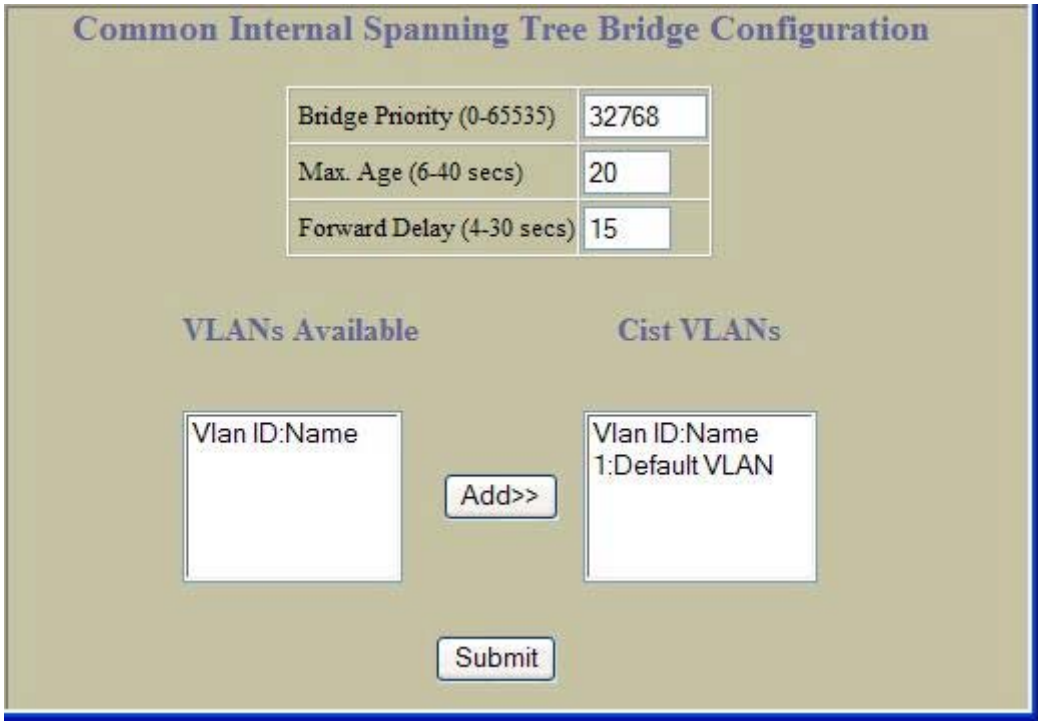

d. Submit をクリックします。

3. CIST-Bridge パラメータを設定します。

a. MSTP/RSTP フォルダを開き、CIST-Bridge を選択します。



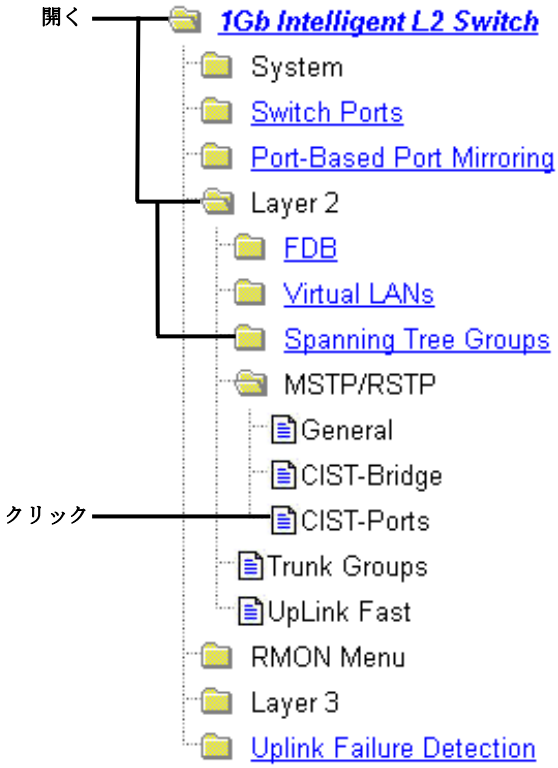
b. Bridge Priority、Max. Age、Forward Delay に値を入力します。



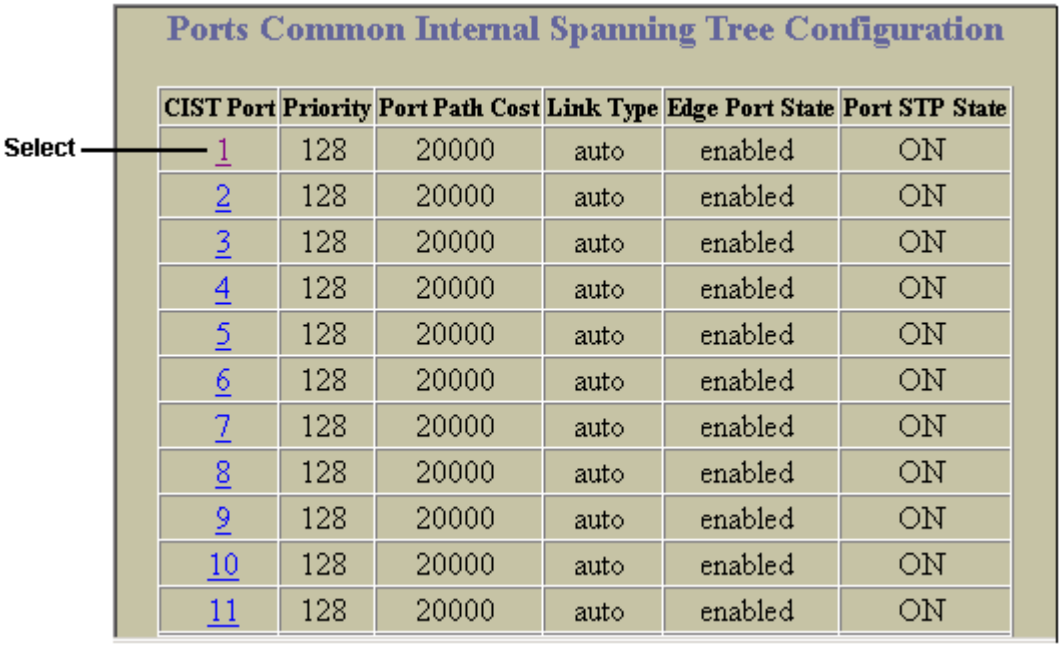

c. をクリックします。

4. CIST-Ports パラメータを設定します。

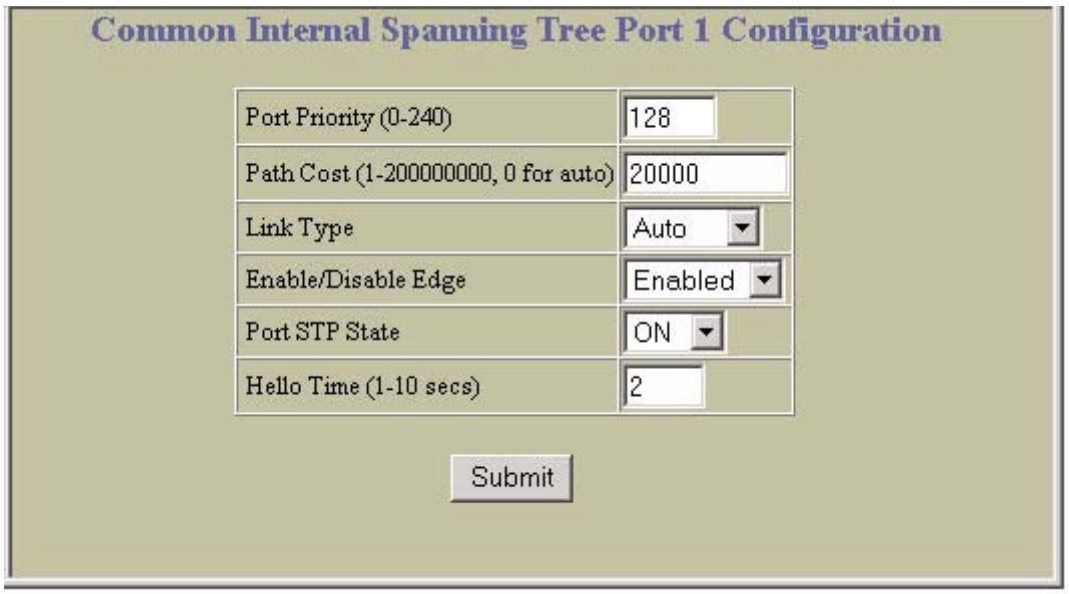
a. MSTP/RSTP フォルダを開き、CIST-Ports を選択します。



b. 該当のポート番号をクリックして、選択します。

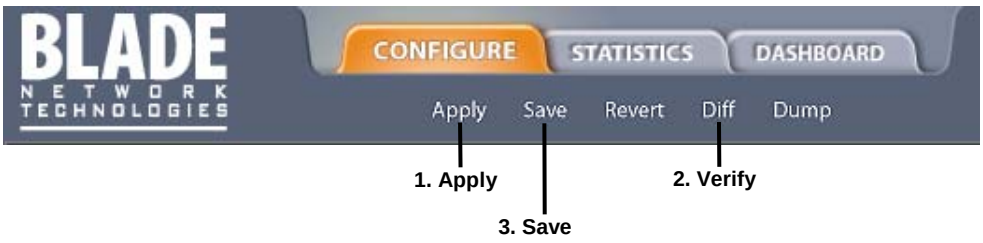



c. Port Priority、Path Cost に値を入力し、Link Type を選択します。CIST Port State を ON にします。




d. Submit をクリックします。

5. 設定を適用、検証、保存します。



# IGMP Snooping

## はじめに

IGMP スヌーピングとは、マルチキャストトラフィックを要求したポートにだけトラフィックを送る機能です。これによって、マルチキャストトラフィックがすべてのデータポートに送られるのを防止します。どのサーバホストがマルチキャストトラフィックを受信したいかをスイッチが調べて、そのサーバのポートにだけ送ります。

本章は以下の節からなります。

- 概要
- Fast Leave
- IGMP フィルタリング
- スタティックマルチキャストルータ
- IGMP スヌーピング構成の例

## 概要

Internet Group Management Protocol (IGMP) は、IP マルチキャストルータが、サブネットに接続されたホストグループメンバが存在するか調べるために使用されます（RFC 2236 参照)。IP マルチキャストルータは、その情報を得るため IGMP Query Report をブロードキャストし、IP ホストがホストグループメンバを報告するのを聞き取ります。このプロセスから、データストリームを送出する IP マルチキャストソースと、データを受信したいクライアントの間にクライアント／サーバ関係が構築されます。

IGMP スヌーピングは帯域幅を維持します。どのポートがマルチキャストデータを受信したいのかを調べ、そのポートにだけ転送します。したがって、他のポートには、不要なマルチキャストトラフィックの負荷がかかりません。

本スイッチが現在サポートしているのは、IGMP スヌーピング バージョン 1 とバージョン 2 です。

スイッチは、接続しているホストサーバから送られてくる IGMP Membership Report を感知し、要求元ホストとローカル IP マルチキャストルータ間の専用パスを形成するプロキシとして機能できます。パスが形成されると、ホストメンバに接続していないポートから出される IP マルチキャストストリームをすべてブロックするので、帯域幅を維持できます。

クライアント／サーバパスを形成する手順は次のとおりです。

- IP マルチキャストルータ (Mrouter) からスイッチに Membership Query を送り、スイッチから指定 VLAN のすべてのポートに転送します。
- マルチキャストデータストリームを受信したいホストからスイッチに Membership Report を送り、スイッチから Mrouter に Membership Report を転送します。
- スイッチが Mrouter とホスト間にパスを形成し、他のすべてのポートがマルチキャストを受信するのを防止します。
- Mrouter は、Membership Query を定期的に送信して、ホストがマルチキャストの受信の継続可否を確認します。ホストが Membership Report による応答に失敗すると、Mrouter はそのパスにマルチキャストの送信するのを止めます。
- ホストからスイッチに Leave report を送信し、スイッチから Mrouter に Leave report を送信すると、マルチキャストパスは直ちに終了します。

## Fast Leave

スイッチで IGMP スヌーピングが有効な場合、IGMPv2 leave メッセージを受信すると、Group-Specific Query を送信して、同じグループ（および同じポート）の他の装置が、指定したマルチキャストグループトラフィックをまだ求めているか確認します。以下の状態の場合、その特定のグループから該当のポートを削除します。

- クエリ応答時間内に IGMP Membership Report メッセージを受信しない。
- マルチキャストルータをポートでまったく学習していない。

VLAN で Fast Leave が有効になっていると、マルチキャストルータをポートで学習していなければ、IGMP Leave メッセージを受信したときに、グループエントリのポートリストから直ちに削除できます。

Fast Leave を有効にできるのは、各物理ポートに 1 ホストしか接続していない VLAN だけです。

## IGMP フィルタリング

IGMP フィルタリングを行うと、ポートが一定のマルチキャストグループとの間でマルチキャストトラフィックを送受信するのを許可／拒否できます。無許可のユーザがネットワークにマルチキャストトラフィックを転送するのを制限します。

マルチキャストグループへのアクセスを拒否すると、そのグループのポートから出される IGMP Membership Report を破棄し、グループから出される IP マルチキャストトラフィックを受信できません。許可すると、ポートから Membership Report を転送して、通常の処理が行われます。

IGMP フィルタリングを構成するには、フィルタリングを有効にし、IGMP フィルタを定義し、そのフィルタをポートに割り当て、そのポートで IGMP フィルタリングを有効にしなければなりません。IGMP フィルタを定義するには、IP マルチキャストグループのレンジを設定し、フィルタがそのレンジ内のグループのマルチキャストトラフィックを許可するか、拒否するかを選択し、フィルタを有効にしなければなりません。

**注：番号の小さいフィルタの方が大きいフィルタより優先されます。たとえば、IGMP フィルタ 1 に設定した処理が、IGMP フィルタ 2 に設定した処理に優先します。**

### 範囲の設定

各 IGMP フィルタで、フィルタが処理する IP アドレス範囲の先頭と最後を設定できます。レンジ内の IP アドレスは 224.0.0.0～239.255.255.255 の範囲になければなりません。

### 処理の設定

各 IGMP フィルタで、設定した IP アドレス範囲への IP マルチキャストを許可したり、拒否したりできます。IP マルチキャストを拒否するフィルタにすると、範囲内のマルチキャストグループからの IGMP Membership Report は破棄されます。

一次フィルタで拒否にした範囲内の狭いアドレス範囲への IP マルチキャストを許可する二次フィルタを設定できます。この 2 つのフィルタにより、アドレス範囲内の一部で IP マルチキャストを許可します。二次フィルタは一次フィルタより番号を小さくして、優先させる必要があります。

## スタティックマルチキャストルータ

特定の VLAN の特定のポートにスタティックマルチキャストルータ (Mrouter) を構成できます。スタティック Mrouter は IGMP スヌーピングで学習する必要はありません。

合計 8 つのスタティック Mrouter をスイッチに構成できます。トランクグループに属するポートはスタティック Mrouter を受けられません。受けられるのは IGMP スヌーピングで学習した Mrouter だけです。

VLAN でスタティック Mrouter を構成すると、IGMP スヌーピングで学習したダイナミック Mrouter と置き換わります。

## IGMP スヌーピング構成の例

以下では、AOS CLI または BBI で IGMP スヌーピングを設定する手順を示します。

## IGMP スヌーピングの設定（AOS CLI の例）

1. 「VLAN」章の「ポートと VLAN の設定（AOS CLI の例）」節で説明したように、ポートと VLAN のメンバを設定します。
2. VLAN を IGMP スヌーピングに追加し、機能を有効にします。

```
>> /cfg/l3/igmp/snoop                (Select IGMP Snooping menu)
>> IGMP Snoop# ena                   (Enable IGMP Snooping)
>> IGMP Snoop# apply                 (Make your changes active)
```

3. ダイナミック IGMP に関する情報を確認します。

```
>> /info/l3/igmp                   (Select IGMP Information menu)
>> IGMP Multicast# dump            (Show IGMP Group information)

>> Switch-A - IGMP Multicast# dump
      Group      VLAN      Version          Port
  -----------  ------    ---------     -------------
   238.1.0.0        1       V2              20
   238.1.0.1        1       V2              21
>> IGMP Multicast# mrouter         (Select MRouter Information menu)
>> IGMP Multicast Router# dump     (Show IGMP Group information)

      VLAN           Port              Version     L)earnt/(S)tatic
  ----------     -----------      ----------   -----------------
       1              23                V2             S
```

以上のコマンドでは、IGMP スヌーピングで学習した IGMP グループと Mrouter に関する情報を表示しています。

## IGMP フィルタリングの設定（AOS CLI の例）

1. スイッチで IGMP フィルタリングを有効にします。

```
>> /cfg/l3/igmp/igmpflt              (Select IGMP Filtering menu)
>> IGMP Filter# ena                   (Enable IGMP Filtering)
Current status: disabled
New status: enabled
```

2. IGMP フィルタを定義します。

```
>> //cfg/l3/igmp/igmpflt               (Select IGMP Filtering menu)
>>IGMP Filter# filter 1                (Select Filter 1 Definition
menu)
>>IGMP Filter 1 Definition# range 224.0.1.0  (Enter first IP
                                        address of the range)
Current multicast address2:
Enter new multicast address2: 226.0.0.0      (Enter second IP
                                        address of the range)
Current multicast address1:
New pending multicast address1: 224.0.1.0
Current multicast address2:
New pending multicast address2: 226.0.0.0
>>IGMP Filter 1 Definition# action deny  (Deny multicast traffic)
>>IGMP Filter 1 Definition# ena          (Enable the filter)
```

3. IGMP フィルタをポートに割り当てます。

```
>> //cfg/l3/igmp/igmpflt         (Select IGMP Filtering menu)
>>IGMP Filter# port 24           (Select port 24)
>>IGMP Port 24# filt ena     (Enable IGMP Filtering on the port)
Current port 24 filtering: disabled
New port 24 filtering: enabled
>>IGMP Port 24# add 1            (Add IGMP Filter 1 to the port)
>>IGMP Port 24# apply            (Make your changes active
```

## スタティック Mrouter の設定（AOS CLI の例）

1. スタティック Mrouter を接続するポートを設定し、該当の VLAN を入力します。

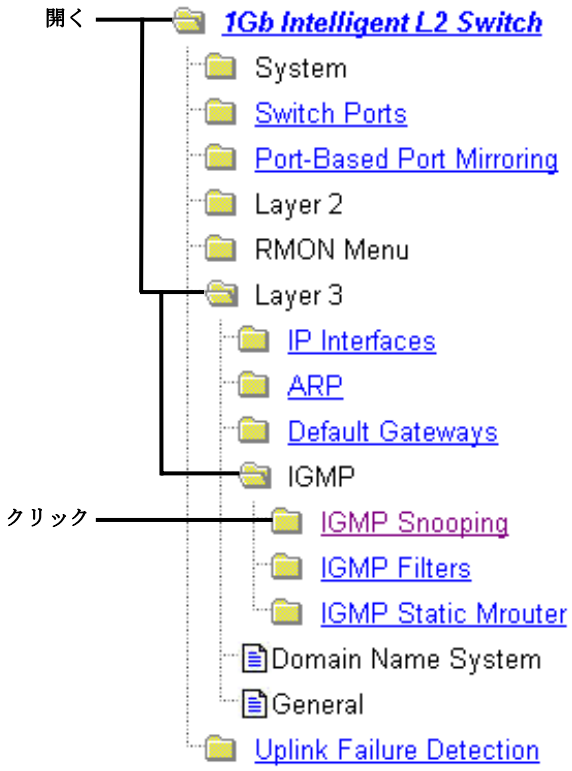
```
>> /cfg/l3/igmp/mrouter             (Select IGMP Mrouter menu)
>> Static Multicast Router# add 20  (Add port 20 as Static
                                     Mrouter port)
Enter VLAN number: (1-4094) 1       (Enter the VLAN number)
Enter the version number of mrouter [1|2]: 2 (Enter the IGMP
                                        version number)
```

2. 構成を適用、確認、保存します。

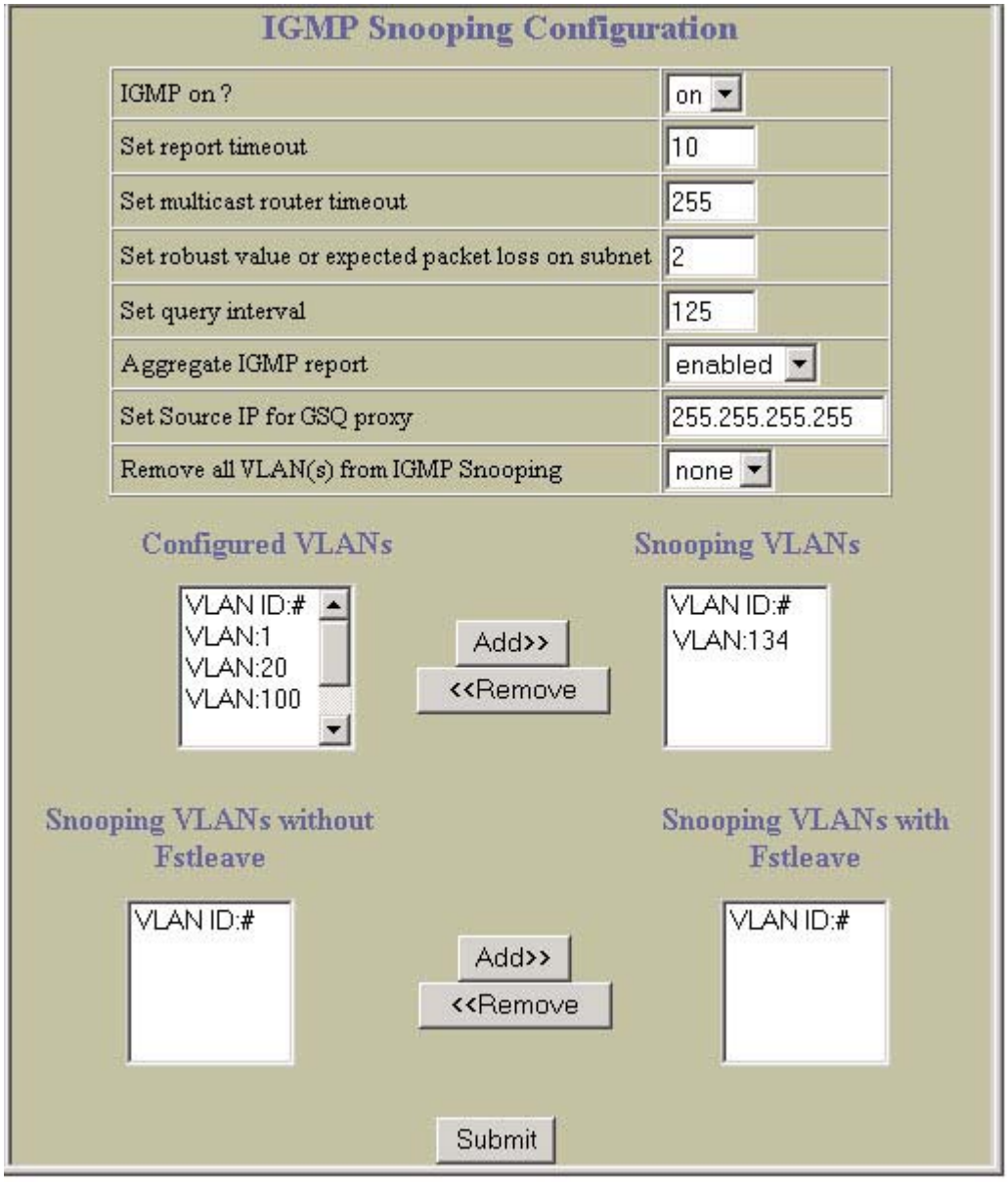
```
>> Static Multicast Router# apply    (Apply the configuration)
>> Static Multicast Router# cur      (View the configuration)
>> Static Multicast Router# save     (Save the configuration)
```

## IGMP スヌーピングの設定（BBI の例）

1. 「VLAN」の章の「ポートと VLAN の設定（BBI の例）」の節で説明したように、ポートと VLAN のメンバを設定します。
2. IGMP スヌーピングを設定します。
   a. CONFIGURE ボタンをクリックします。
   b. IGMP フォルダを開き、IGMP Snooping を選択します（フォルダではなく、下線が引かれたフォルダ名をクリックします）。

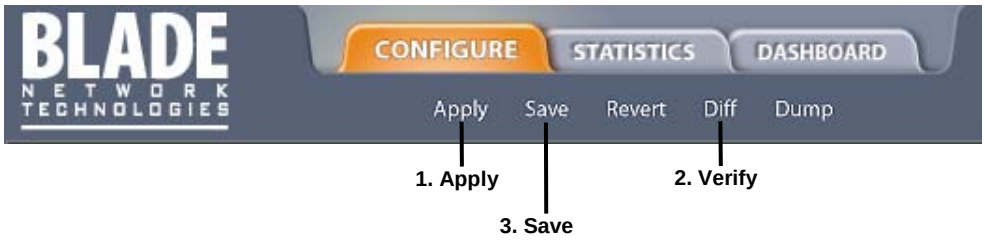


c. IGMP スヌーピングを有効にします。



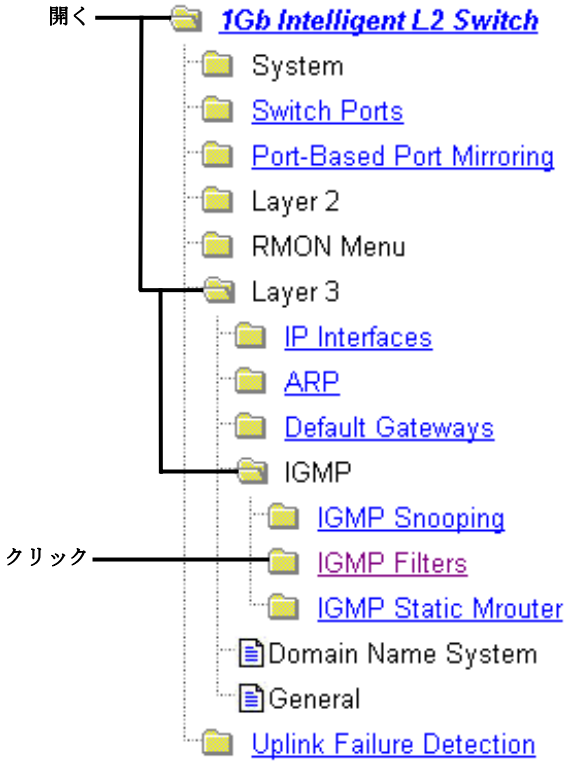

d. Submit をクリックします。

3. 設定を適用、確認、保存します。

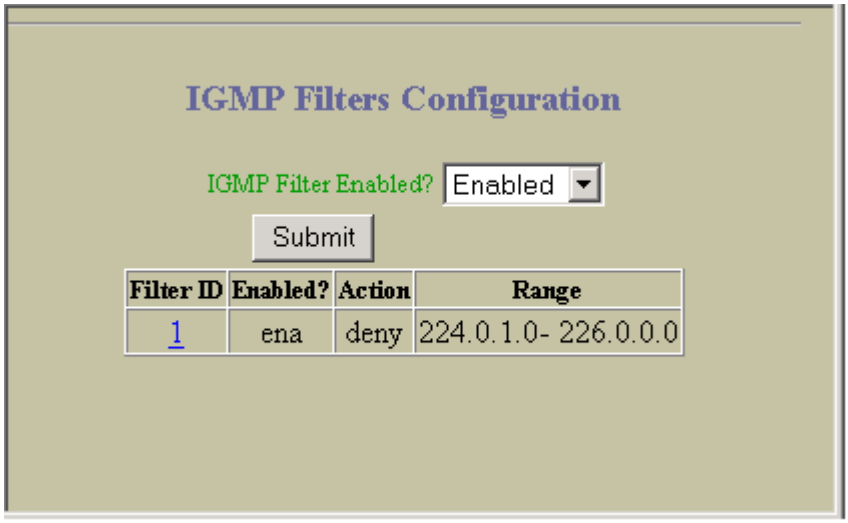


## IGMP フィルタリングの設定（BBI の例）

1. IGMP スヌーピングを設定します。
2. IGMP フィルタリングを有効にします。
   a. CONFIGURE ボタンをクリックします。
   b. IGMP フォルダを開き、IGMP Filters を選択します（フォルダではなく、下線が引かれたフォルダ名をクリックします）。



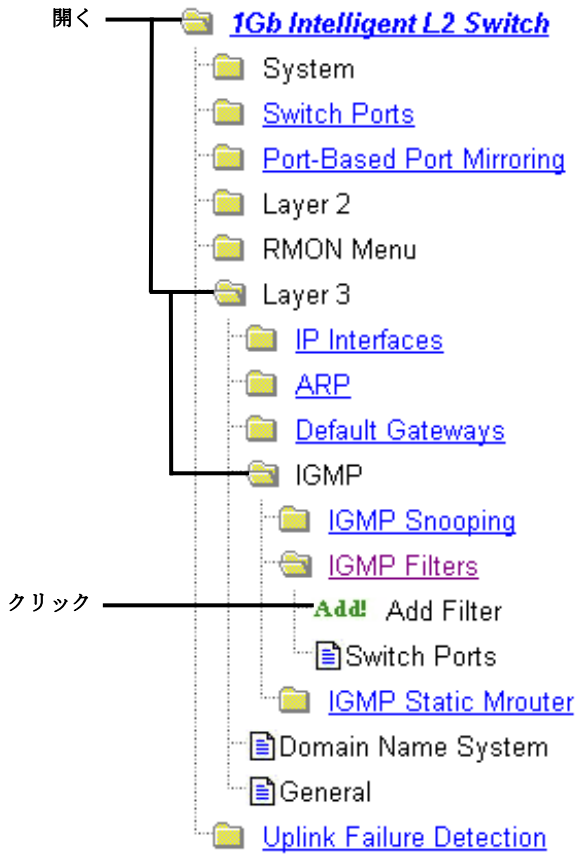

   c. IGMP フィルタリングをグローバルに有効にします。



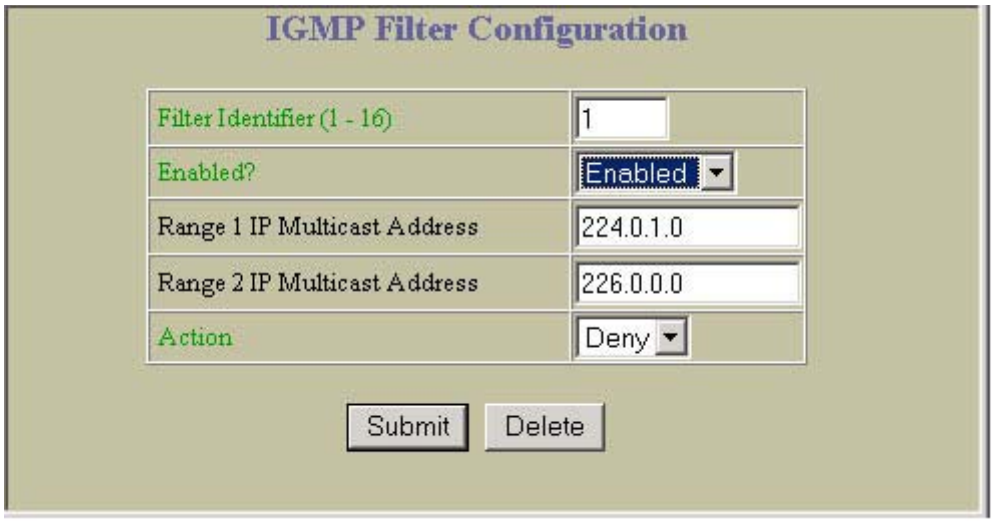

   d. Submit をクリックします。

3. IGMP フィルタを定義します。

a. Layer 3 > IGMP > IGMP Filters > Add Filter を選択します。



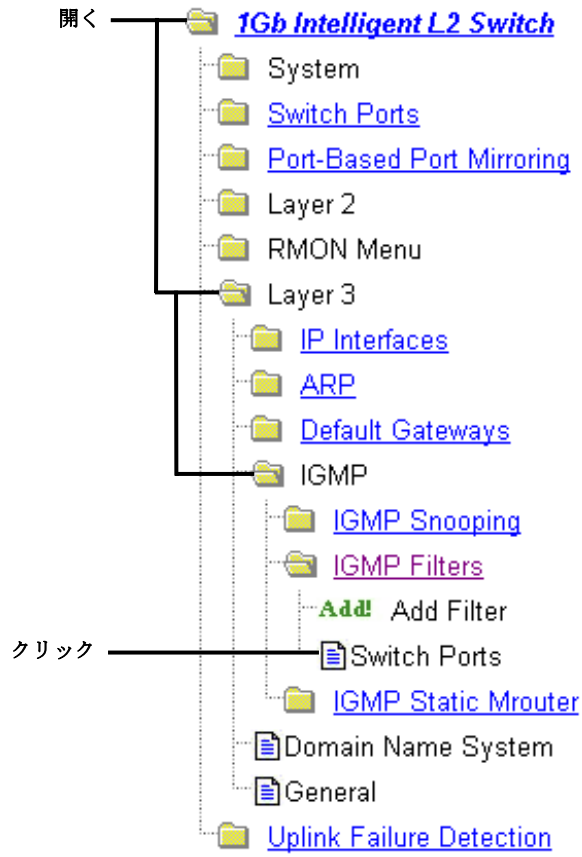

b. IGMP フィルタを有効にします。IP マルチキャストアドレスの範囲とファイタ処理（許可または拒否）を指定します。



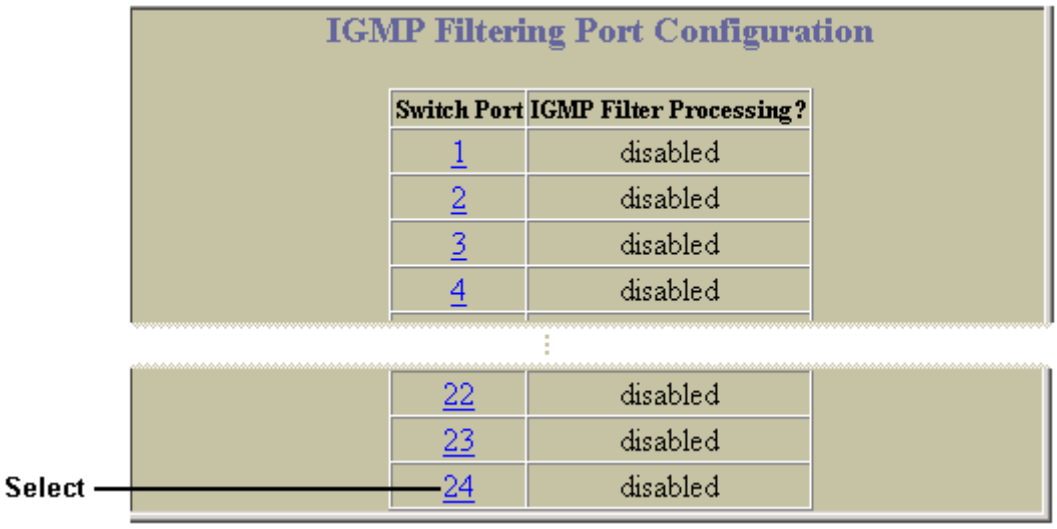

c. Submit をクリックします。

4. フィルタをポートに割り当て、そのポートで IGMP フィルタリングを有効にします。

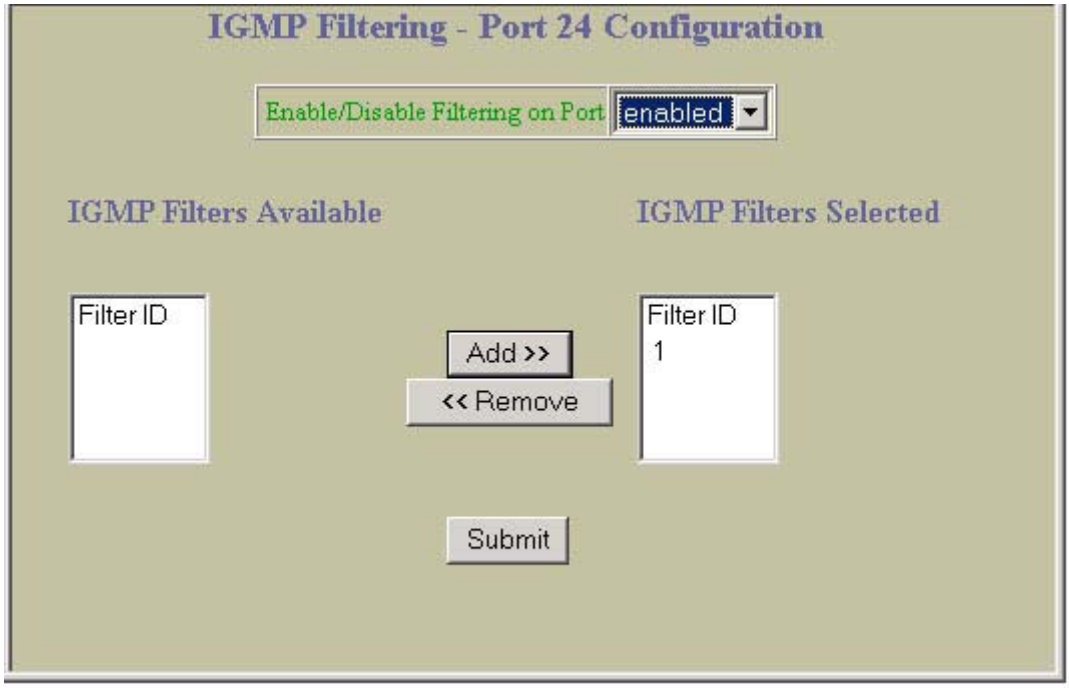
   a. Layer 3 > IGMP > IGMP Filters > Switch Ports を選択します。




   b. リストから該当のポートを選択します。

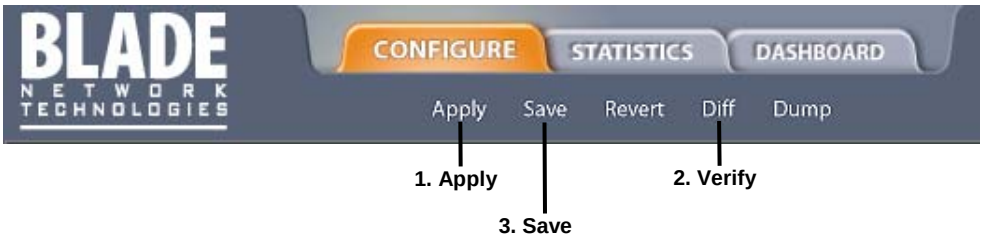


c. ポートで IGMP フィルタリングを有効にします。IGMP Filters Available リストから該当のフィルタを選択し、Add をクリックします。




d. Submit をクリックします。

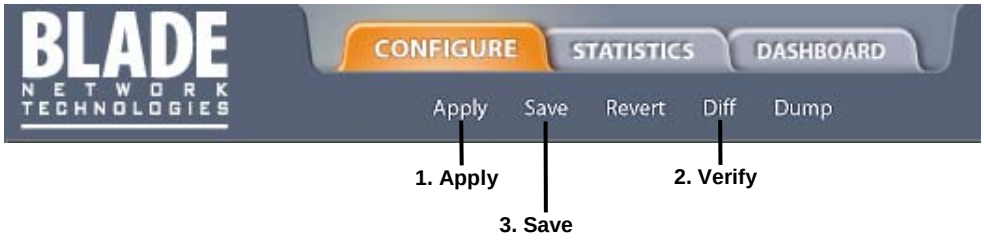
5. 設定を適用、確認、保存します。



## スタティックマルチキャストルータの設定（BBI の例）

1. スタティック Mrouter を設定します。
   a. CONFIGURE ボタンをクリックします。
   b. Switch フォルダを開き、IP Menu > IGMP > IGMP Static MRouter を選択します。
   c. ポート番号、VLAN ID、IGMP バージョン番号を入力します。


   d. Submit をクリックします。
2. 設定を適用、確認、保存します。



# Remote Monitoring

## はじめに

リモートモニタリング(RMON)は、ネットワーク装置とネットワークモニタリングデータを交換できるようにするものです。

RMON の主な機能は次のとおりです。

- イーサネットインタフェースの累積統計データを収集する。
- イーサネットインタフェースの統計データの履歴を収集する。
- ユーザ定義イベントのアラームを生成、トリガする。

## 概要

RMON MIB は、スイッチの RMON エージェントと RMON 管理アプリケーションの間のインタフェースをとるものです。RFC 1757 に規定されています。

RMON 標準で、イーサネットネットワークの管理に有効なオブジェクトを定義しています。RMON エージェントが継続的に統計データを収集し、スイッチの性能を監視します。スイッチのトラフィックフローを監視できます。

本スイッチは、RFC 1757 に規定されている、以下の RMON グループをサポートします。

- グループ 1：統計データ
- グループ 2：History（履歴）
- グループ 3：アラーム
- グループ 9：イベント

### RMON グループ 1 — 統計データ

RMON 統計データ MIB に定められたイーサネット統計データの収集を、etherStatsTable に従ってサポートします。
RMON 統計データはポート単位で有効にでき、`/stat/port x/rmon` コマンドで確認できます。毎秒サンプリングされ、指定のポートで新しいデータが古いデータに上書きされます。

> **注：ポートの RMON 統計データを確認するためには、RMON ポート統計データを有効にしなければなりません。**

#### RMON 統計データの設定（AOS CLI の例）

1. RMON 統計データを収集したい各ポートで RMON を有効にします。

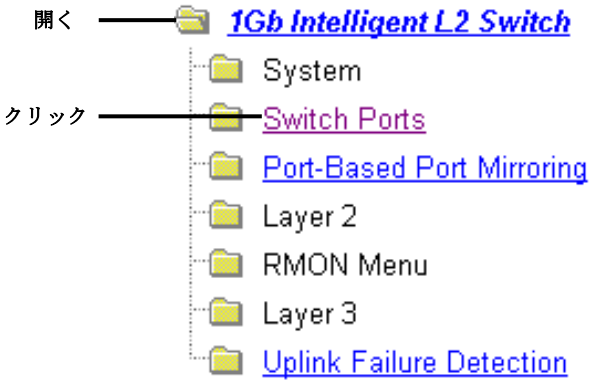
```
>> /cfg/port 23/rmon                    (Select Port 23 RMON)
>> Port 23 RMON# ena                    (Enable RMON)
>> Port 23 RMON# apply                  (Make your changes active)
>> Port 23 RMON# save                   (Save for restore after reboot)
```

2. ポートの RMON 統計データを確認します。

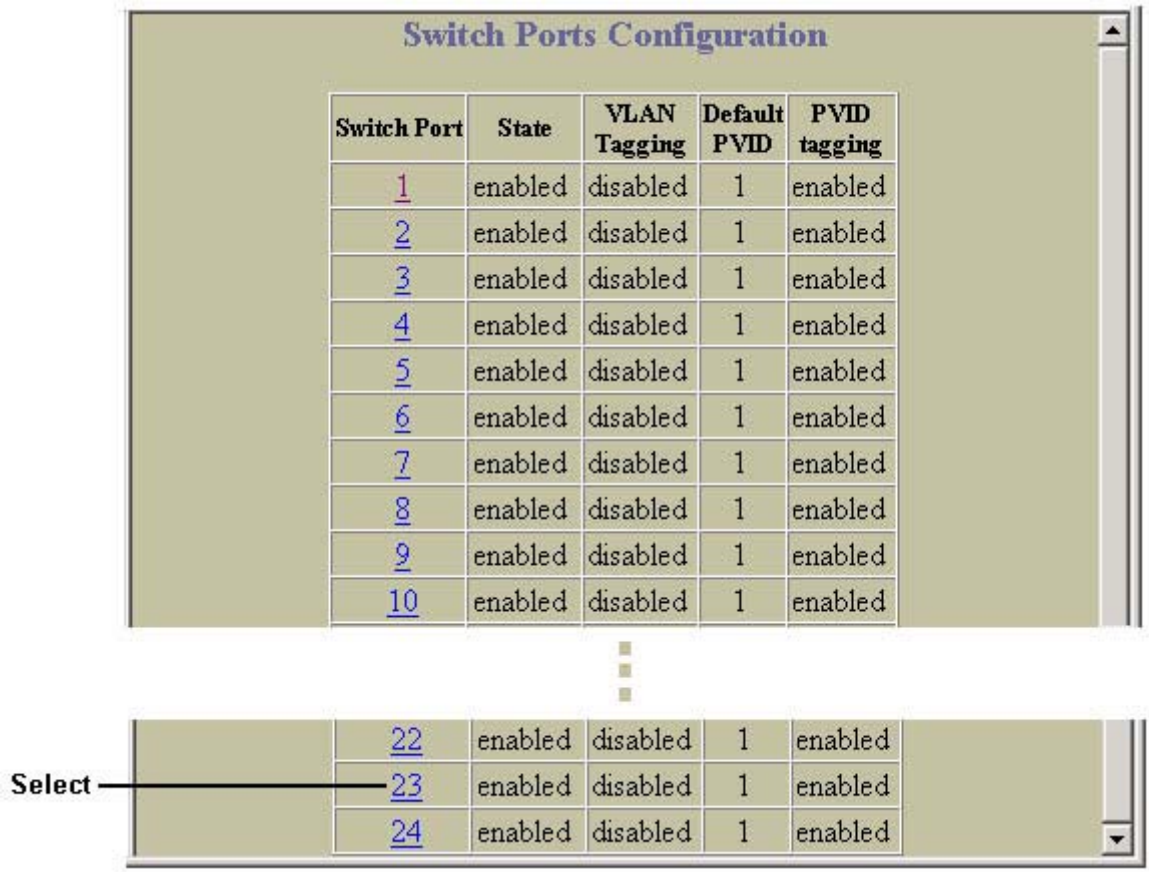
```
>> /stats/port 23                                (Select Port 23 Stats)
>> Port Statistics# rmon
------------------------------------------------------------------------
RMON statistics for port 23:
etherStatsDropEvents:                            NA
etherStatsOctets:                           7305626
etherStatsPkts:                               48686
etherStatsBroadcastPkts:                       4380
etherStatsMulticastPkts:                       6612
etherStatsCRCAlignErrors:                        22
etherStatsUndersizePkts:                          0
etherStatsOversizePkts:                           0
etherStatsFragments:                              2
etherStatsJabbers:                                0
etherStatsCollisions:                             0
etherStatsPkts64Octets:                       27445
etherStatsPkts65to127Octets:                  12253
etherStatsPkts128to255Octets:                  1046
etherStatsPkts256to511Octets:                   619
etherStatsPkts512to1023Octets:                 7283
etherStatsPkts1024to1518Octets:                  38
```

## RMON 統計データの設定（BBI の例）

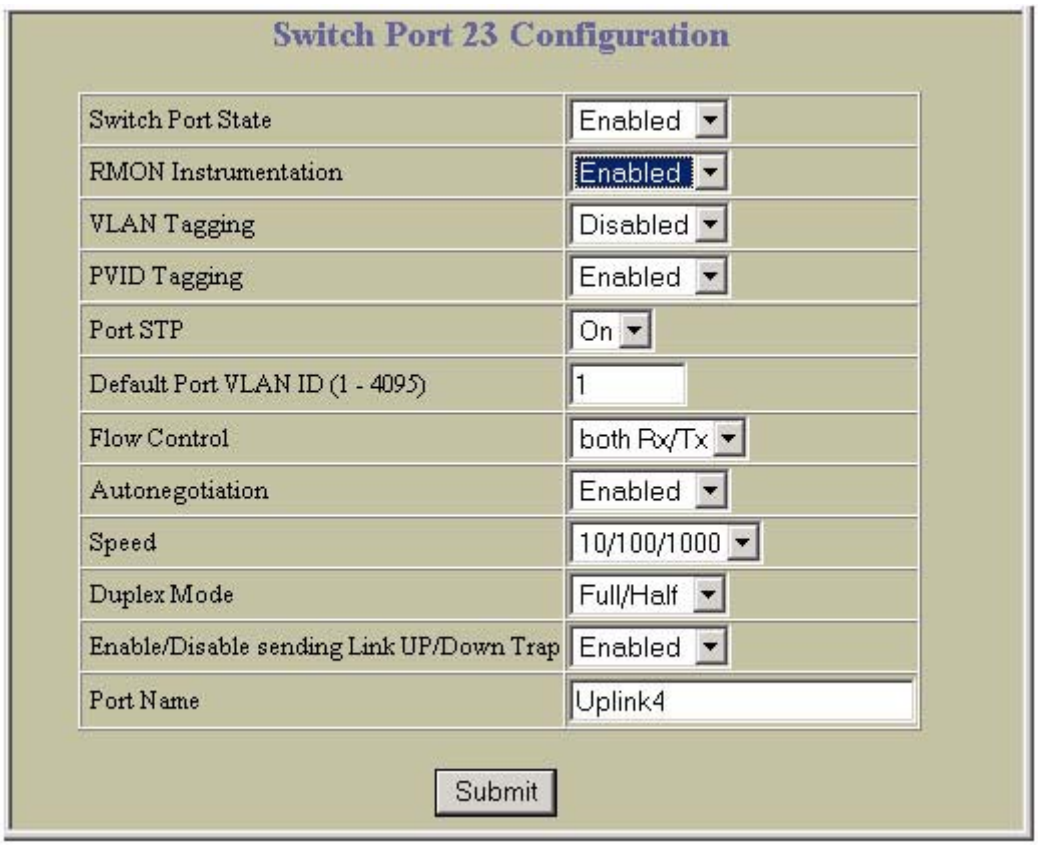
1. ポートを設定します。
   a. CONFIGURE ボタンをクリックします。
   b. Switch Ports を選択します（フォルダではなく、下線が引かれたフォルダ名をクリックします）。



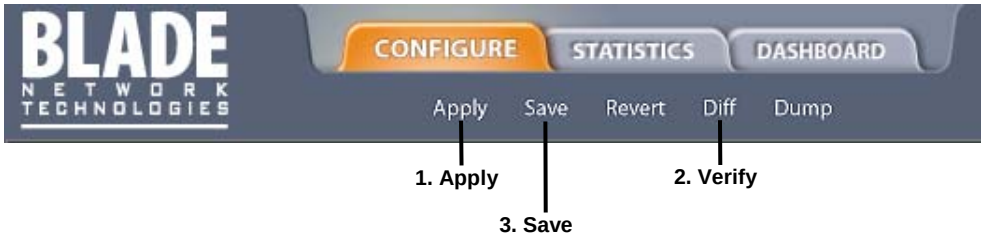

2. ポートを選択します。



3. ポートの RMON を有効にします。




4. Submit をクリックします。
5. 設定を適用、確認、保存します。



# RMON グループ 2 — History（履歴）

RMON History グループでは、一定時間中のインタフェースのイーサネット統計データをサンプリング、アーカイブできます。本スイッチは RMON History グループを 5 つまでサポートします。

> **注**：RMON History グループでポートをモニタするためには、そのポートの RMON ポート統計データを有効にしなければなりません。

データはバケットに格納されます。バケットとはあるサンプリング間隔で収集したデータを保存するものです。設定間隔毎に、History インスタンスが現イーサネット統計データのサンプルを取り出して、バケットに入れます。History データバケットはダイナミックメモリにあります。スイッチをリブートすると、バケットは空になります。

リクエストバケット(`/cfg/rmon/hist x/rbnum`)は各 History グループにユーザがリクエストしたバケット（つまりデータスロット）の数、グラントバケット(`/info/rmon/hist x/gbnum`)は、システムのメモリ容量に基づいて、システムが許可したバケット数です。システムが許可するパケット数は最大で 50 です。

SNMP ブラウザで History サンプルを確認できます。

## History MIB オブジェクト

RFC1213、RFC1573 に規定されているように、サンプリングできるデータのタイプは、ifIndex オブジェクトタイプです。History サンプルでもっとも一般的なデータタイプは次のようなものです。

`1.3.6.1.2.1.2.2.1.1.x -mgmt.interfaces.ifTable.ifIndex.interface`

最後の桁 (*x*) はモニタするインタフェースを示し、ポート番号（1～24）に対応します。History サンプリングはポート単位で行われ、インタフェース番号でポート番号を指定します。

### RMON History の設定（AOS CLI の例）

1. RMON History を収集したい各ポートで RMON を有効にします。

```
>> /cfg/port 23/rmon                    (Select Port 23 RMON)
>> Port 23# ena                         (Enable RMON)
>> Port 23 RMON# apply                  (Make your changes active)
>> Port 23 RMON# save                   (Save for restore after reboot)
```

2. RMON History パラメータを設定します。

```
>> /cfg/rmon/hist 1                              (Select RMON History 1)
>> RMON History 1# ifoid 1.3.6.1.2.1.2.2.1.1.23
>> RMON History 1# rbnum 30
>> RMON History 1# intrval 120
>> RMON History 1# owner "Owner_History_1"
```

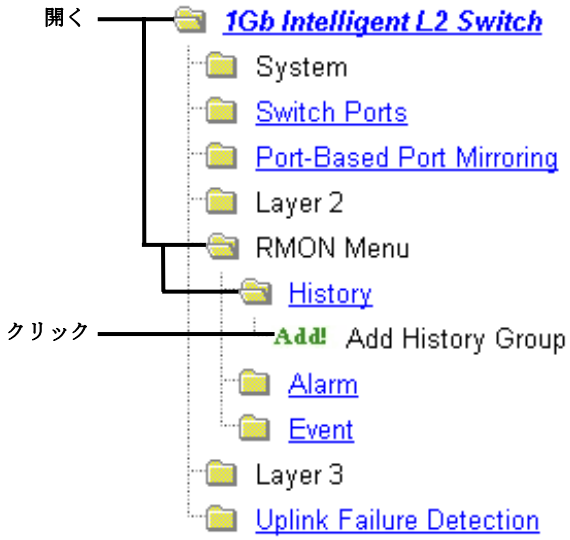
3. 設定を適用、保存します。

```
>> RMON History 1# apply                (Make your changes active)
>> RMON History 1# save                 (Save for restore after reboot)
```

この設定では、ポート 23 をモニタする RMON History グループを生成します。2 分毎にデータサンプルを取り出し、30 のリクエストバケットの 1 つに入れます。30 サンプルまで収集すると、最初のバケットから、新しいサンプルを古いサンプルに上書きします。データの確認には SNMP を用います。

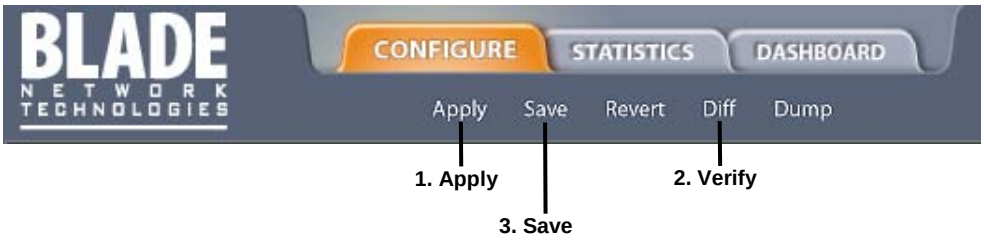
## RMON History の設定（BBI の例）

1. RMON History グループを設定します。
   a. CONFIGURE ボタンをクリックします。
   b. Switch フォルダを開き、RMON > History > Add History Group を選択します。




2. RMON History グループパラメータを設定します。


3. Submit をクリックします。
4. 設定を適用、確認、保存します。



# RMON グループ 3 — アラーム

RMON アラームグループでは、ネットワーク性能を決めるしきい値を設定できます。設定したしきい値を交差すると、アラームが上がります。たとえば、CRC エラーが 10 分間で 1,000 を超えるときにアラームが上がるようにできます。本スイッチは RMON アラームグループを 30 までサポートします。

各アラームインデックスは、モニタする変数、サンプリング間隔、立上り／立下りしきい値のパラメータからなります。アラームグループを使用して、MIB オブジェクトの立上り／立下りを探知できます。オブジェクトは、カウンタ、ゲージ、整数、または時間間隔のいずれかでなければなりません。

アラームインデックスをイベントインデックスに相関させるには、`/cfg/rmon/alarm x/revtidx` か `/cfg/rmon/alarm x/fevtidx` を使用します。アラームしきい値に達すると、対応するイベントがトリガされます。

## アラーム MIB オブジェクト

アラームモニタリングに使用するもっとも一般的なデータタイプは ifStats で、エラー、脱落、CRC 失敗などです。これらの MIB Object ID (OID) が、History グループで収集するものと関連します。ICMP 統計データの例を次に示します。

`1.3.6.1.2.1.5.1.0 – mgmt.icmp.icmpInMsgs`

最後の桁 (*x*) はモニタするインタフェースを示し、次のように、インタフェース番号つまりポート番号に対応します。

1-256 = IF 1-256
  257 = port 1
  258 = port 2
  …
  280 = port 24

アラームの MIB OID をストリングとして表しています。テーブルではない場合、.0 でエンドノードを指定しなければならないことに注意してください。

### RMON アラームの設定（AOS CLI の例 1）

1. ポートで受信するパケット数を収集する RMON アラームパラメータを設定します。

```
>> /cfg/rmon/alarm 6                                (Select RMON Alarm 6)
>> RMON Alarm 6# oid 1.3.6.1.2.1.2.2.1.10.276
>> RMON Alarm 6# intrval 3600
>> RMON Alarm 6# almtype rising
>> RMON Alarm 6# rlimit 2000000000
>> RMON Alarm 6# revtidx 6
>> RMON Alarm 6# sample abs
>> RMON Alarm 6# owner "Alarm_for_ifInOctets"
```

2. 設定を適用、保存します。

```
>> RMON Alarm 6# apply                (Make your changes active)
>> RMON Alarm 6# save                 (Save for restore after reboot)
```

ポート 20 で `ifInOctets` をチェックする RMON アラームを 1 時間毎に生成します。統計量が 20 億を超えると、イベントインデックス 6 をトリガするアラームが発生します。

### RMON アラームの設定（AOS CLI の例 2）

1. ICMP メッセージを収集する RMON アラームパラメータを設定します。

```
>> /cfg/rmon/alarm 5                                (Select RMON Alarm 5)
>> RMON Alarm 5# oid 1.3.6.1.2.1.5.8.0
>> RMON Alarm 5# intrval 60
>> RMON Alarm 5# almtype rising
>> RMON Alarm 5# rlimit 200
>> RMON Alarm 5# revtidx 5
>> RMON Alarm 5# sample delta
>> RMON Alarm 5# owner "Alarm_for_icmpInEchos"
```

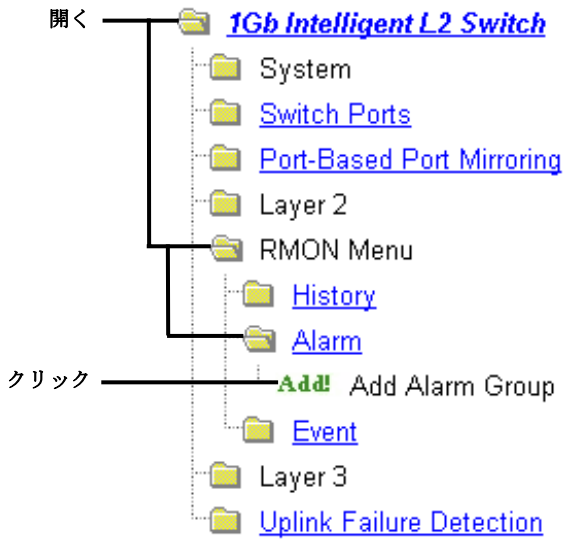
2. 設定を適用、保存します。

```
>> RMON Alarm 5# apply                (Make your changes active)
>> RMON Alarm 5# save                 (Save for restore after reboot)
```

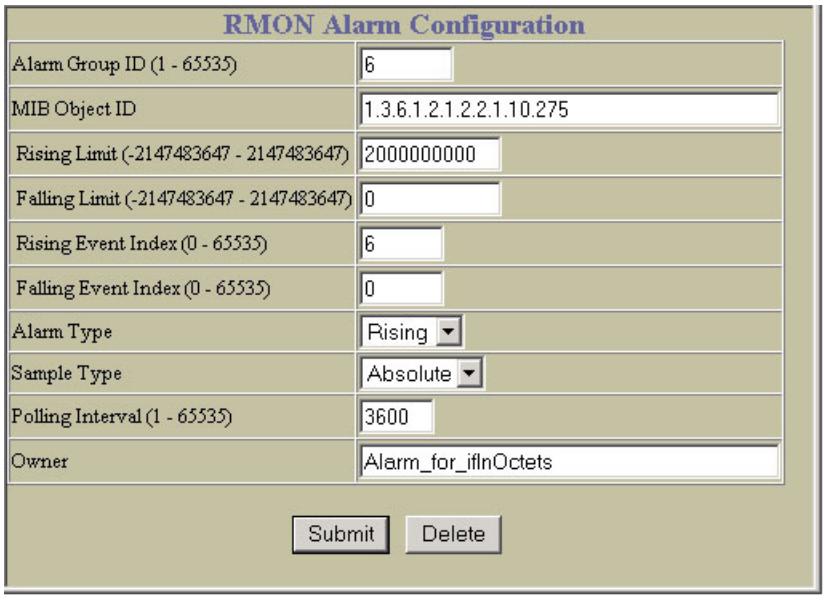
スイッチで `icmpInEchos` をチェックする RMON アラームを 1 分毎に生成します。60 秒間で統計量が 200 を超えると、イベントインデックス 5 をトリガするアラームが発生します。

## RMON アラームの設定（BBI の例 1）

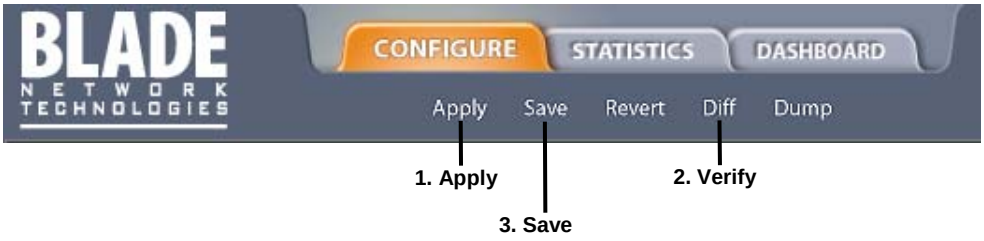
1. RMON アラームグループを設定します。
   a. CONFIGURE ボタンをクリックします。
   b. Switch フォルダを開き、RMON > Alarm > Add Alarm Group を選択します。




   c. ポート 19 で 1 時間毎に `ifInOctets` をチェックする RMON アラームグループパラメータを設定します。立上りしきい値 (Rising Limit) の 20 億と立上りイベントインデックス (Rising Event Index) の 6 を入力します。この設定では、ポート 19 で 1 時間毎に `ifInOctets` をチェックする RMON アラームを生成します。統計量が 20 億を超えると、イベントインデックス 6 をトリガするアラームが発生します。

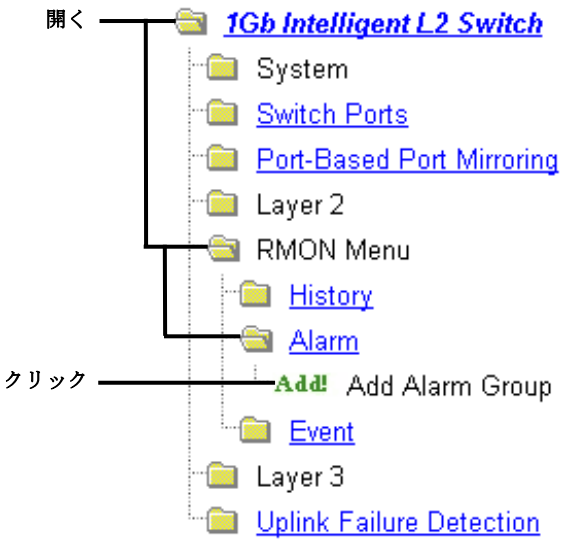



2. Submit をクリックします。
3. 設定を適用、確認、保存します。

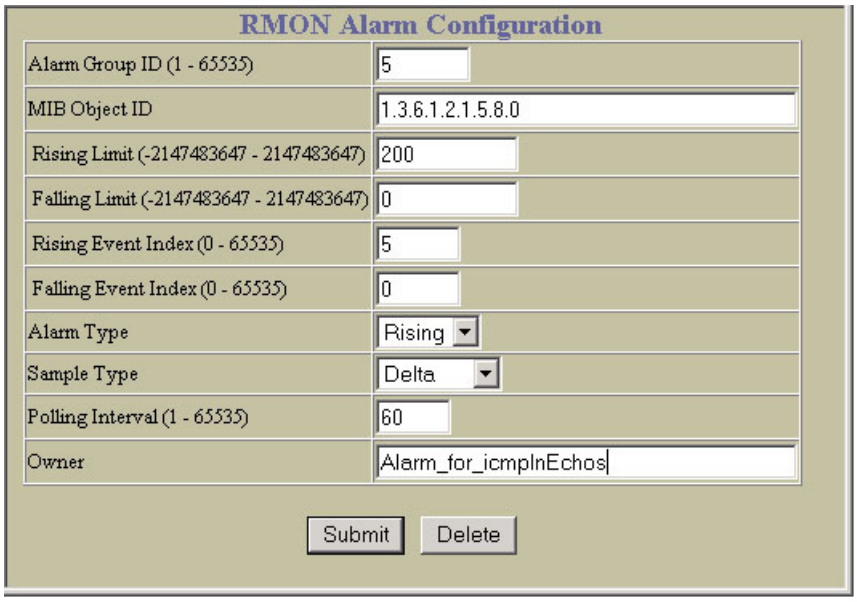


## RMON アラームの設定（BBI の例 2）

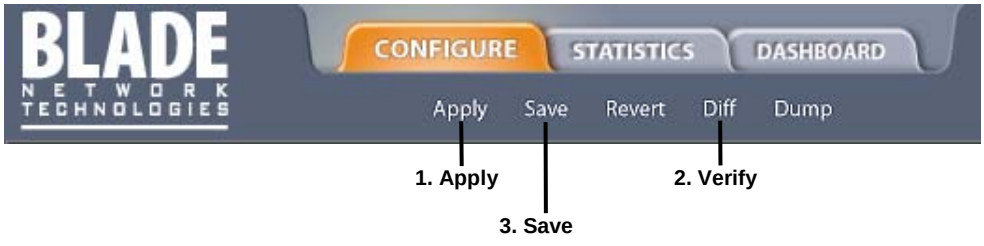
1. RMON アラームグループを設定します。
   a. CONFIGURE ボタンをクリックします。
   b. Switch フォルダを開き、RMON > Alarm > Add Alarm Group を選択します。




   c. ポーリング間隔 60、立上りしきい値 (Rising Limit) 200、立上りイベントインデックス (Rising Event Index) 5 で `icmpInEchos` をチェックする RMON アラームグループパラメータを設定します。この設定では、スイッチで 1 分毎に `icmpInEchos` をチェックする RMON アラームを生成します。60 秒以内に統計量が 200 を超えると、イベントインデックス 5 をトリガするアラームが発生します。




2. Submit をクリックします。
3. 設定を適用、確認、保存します。



# RMON グループ 9 — イベント

RMON イベントグループでは、アラームでトリガするイベントを指定できます。イベントには、ログメッセージ、SNMP トラップメッセージ、またはその両方が可能です。本スイッチは RMON イベントメッセージを 30 までサポートします。

アラームが発生すると、対応するイベント通報を発生させます。`/cfg/rmon/alarm x/revtidx` コマンドと`/fevtidx` コマンドによりイベントインデックスをアラームに関連付けます。

RMON イベントは SNMP とシスログにより通報を行います。したがって、トラップイベント通報を正常に機能させるためには、SNMP トラップホストを設定しなければなりません。

RMON は SYSLOG ホストを用いてシステムログメッセージを送信します。したがって、イベントログ通報が正常に機能するためには、稼動している SYSLOG ホスト (`/cfg/sys/syslog`) を設定しなければなりません。各ログイベントは、対応するシスログを RMON タイプで生成します。

## RMON イベントの設定（AOS CLI の例）

1. RMON イベントパラメータを設定します。

```
>> /cfg/rmon/event 5                              (Select RMON Event 5)
>> RMON Event 5# descn "SYSLOG_generation_event"
>> RMON Event 5# type log
>> RMON Event 5# owner "Owner_event_5"
```

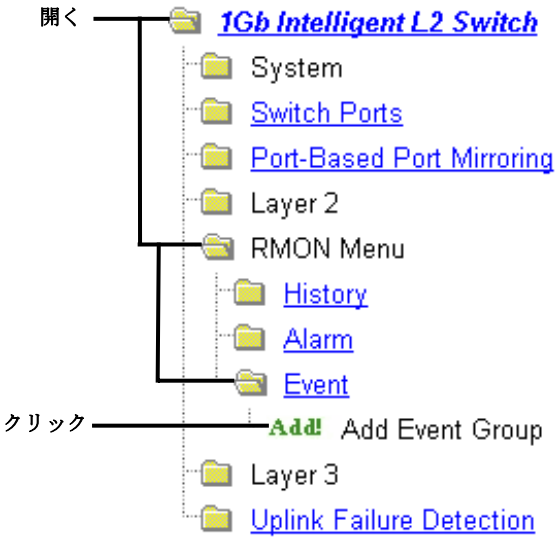
2. 設定を適用、保存します。

```
>> RMON Alarm 5# apply                  (Make your changes active)
>> RMON Alarm 5# save                   (Save for restore after reboot)
```

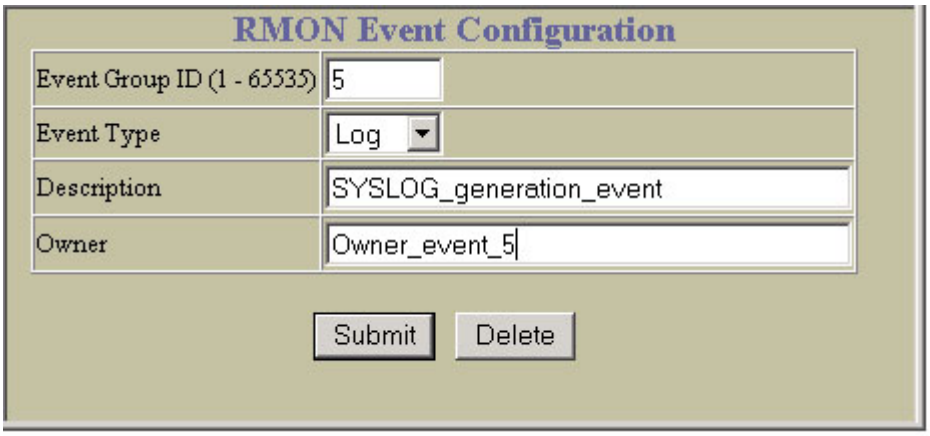
アラームが RMON イベントをトリガする毎にシスログメッセージを送信するイベントを生成します。

## RMON イベントの設定（BBI の例 1）

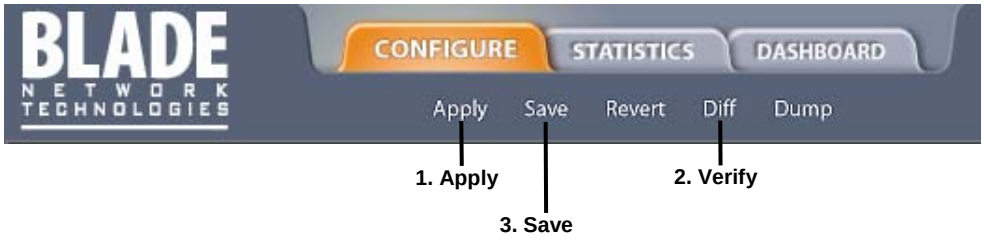
1. RMON イベントグループを設定します。
   a. CONFIGURE ボタンをクリックします。
   b. Switch フォルダを開き、RMON > Event > Add Event Group を選択します。




   c. RMON イベントグループパラメータを設定します。この設定では、アラームが RMON イベントをトリガする毎にシスログメッセージを送信するイベントを生成します。




2. Submit をクリックします。
3. 設定を適用、確認、保存します。



# High availability

## はじめに

本スイッチは高可用性のネットワークトポロジをサポートします。本章では、Uplink Failure Detection について説明します。

## Uplink Failure Detection

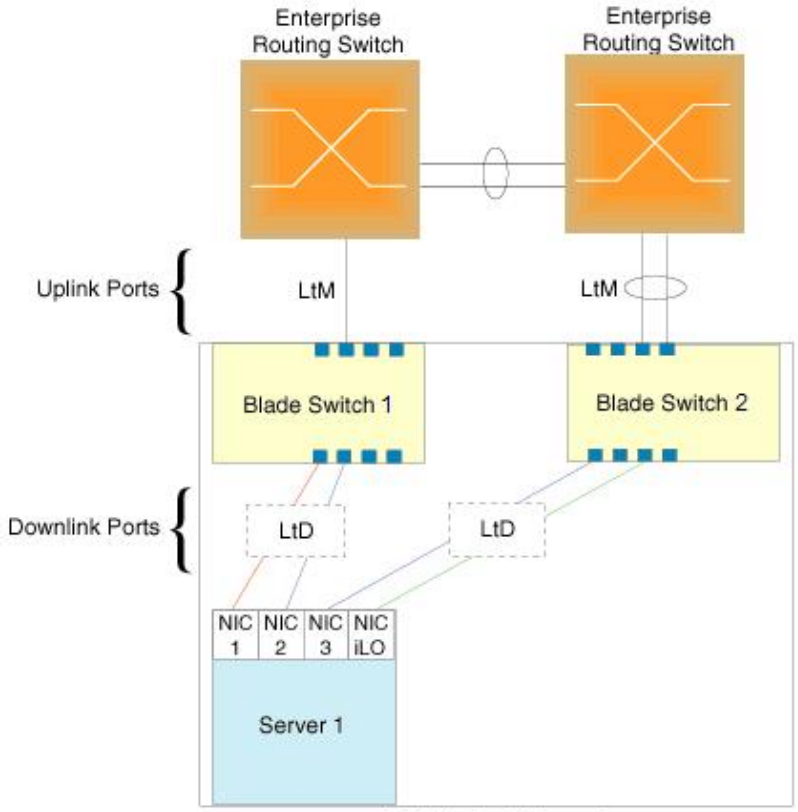
CPU ブレードのネットワークアダプタチーミングをサポートするため、Uplink Failure Detection (UFD) があります。

UFD を利用すると、アップリンクポートを監視してリンク故障を検出できます。リンク故障を検出すると、指定したダウンリンクポートが自動的に無効になります。サーバ側のネットワークアダプタで無効になったダウンリンクを検出し、スイッチの別のポートか、ブレード収納ユニットの別のスイッチにフェイルオーバを行うことができます。

アップリンクが復旧すると、スイッチが自動的にダウンリンクポートを有効に戻します。

次の図に基本的な UFD 構成を示します。1 つの LtM (Link to Monitor) 、1 つの LtD (Link to Disable) からなる Failure Detection Pair (FDP) で構成されています。スイッチは、LtM でリンク故障を検出すると、LtD の該当のポートを無効にします。CPU ブレードでは、無効になったダウンリンクポートを検出し、NIC のフェイルオーバを行います。

図10　スイッチの Uplink Failure Detection




注：図に示したポート番号は、システムの物理ポート構成に必ずしも対応しません。

## Failure Detection Pair

UFD を利用するには、Failure Detection Pair を構成し、UFD をオンにします。Failure Detection Pair は以下のポートグループからなります。

- Link to Monitor (LtM) グループ
  1 アップリンクポート（20～24）か、アップリンクポートのみで構成される、1 トランクグループもしくは 1LACP トランクグループのいずれかを割り当てることができます。スイッチが LtM をモニタして、リンク故障がないか調べます。
- Link to Disable (LtD) グループ
  1 つ以上のダウンリンクポート（1～16）と、ダウンリンクポートのみで構成されるトランクグループもしくは LACP トランクグループからなります。スイッチは、LtM でリンク故障を検出すると、LtD のすべてのポートを自動的に無効にします。

  LtM が復旧すると、LtD のすべてのポートを自動的に有効に戻します。

## UFD とスパニングツリープロトコルの同時動作

LtD のポートでスパニングツリープロトコル (STP) を有効にすると、STP 状態と、LtM ポートのリンク状態をモニタします。リンク故障や STP ブロック状態を検出した場合には、LtD ポートを自動的に無効にします。

LtM ポートが STP フォワーディング状態にあることを確認すると、LtD ポートを自動的に有効にして、通常の状態に戻します。

## 構成ガイドライン

この節では UFD の構成に重要な事項について説明します。

- UFD が必要なのは、スイッチのアップリンクパスが冗長になっていないときだけです。
- Failure Detection Pair（LtM の 1 グループと LtD の 1 グループ）は 4 つまで構成できます。
- LtM としては 1 アップリンクポートか、もしくはアップリンクポートのみで構成される、1 トランクグループもしくは 1LACP トランクグループを割り当てることができます。
  すでにトランクグループのメンバであるポートを LtM に割り当てることはできません。
- LtM として構成したトランクグループには複数のアップリンクポート（20～24）を入れることができますが、ダウンリンクポート（1～16）やインターリンクポート（17、18）はできません。
  すでに LtM に属しているアップリンクポートをトランクグループに追加することはできません。
- LtD にはポートやトランクを入れることができます。
- LtD として構成したトランクグループには複数のダウンリンクポート（1～16）を入れることができますが、アップリンクポート（20～24）やインターリンクポート（17、18）はできません。

---

- ソフトウェアバージョン 1.0.0 では使用できる FDP は1つだけです。

---

## UFD のモニタ

UFD 情報メニューに、LtM と LtD の現ステータス、そのメンバポート、メンバトランクが表示されます。次に例を示します。

```
>> Information# ufd
Uplink Failure Detection 1: Enabled
LtM status: Down
Member      STG    STG State       Link Status
---------   ---    ------------    -----------
  port 24                           down
             1       DISABLED
            10       DISABLED *
            15       DISABLED *
* = STP turned off for this port.

LtD status: Auto Disabled
Member       Link Status
---------    -----------
  port  1      disabled
  port  2      disabled
  port  3      disabled
  port  4      disabled

Uplink Failure Detection 2: Disabled

Uplink Failure Detection 3: Disabled

Uplink Failure Detection 4: Disabled
```

LtM でリンク故障を検出した回数、LtM でスパニングツリーブロック状態を検出した回数、LtD で UFD がポートを無効にした回数を調べるには、`/stats/ufd` コマンドを使用します。

## UFD の構成

以前の図で基本的な UFD 構成を示しました。スイッチ 1 のポート 21 は、シャーシ外のレイヤ 2/3 ルーティングスイッチに接続されています。スイッチ 2 のポート 20、22 で、別のレイヤ 2/3 ルーティングスイッチに接続したトランクを形成しています。インターリンクポート（17、18）は無効です。

この例では、NIC 1 が一次ネットワークアダプタ、NIC 2、NIC 3、NIC 4 はそれ以外です。NIC 1、NIC 2 はスイッチ 1 のポート 1、ポート 2 に、NIC 3、NIC 4 はスイッチ 2 のポート 1、ポート 2 に接続されています。

### スイッチ 1 での UFD の設定（AOS CLI の例）

1. 通信故障をモニタするアップリンクポート（20～24）を割り当てます。

```
>> Main# /cfg/ufd/fdp 1/ena          (Enable Failure Detection Pair 1)
>> FDP# ltm                          (Select Link to Monitor menu)
>> Failure Link to Monitor# addport 21 (Monitor uplink port 21)
```

2. アップリンク故障が発生したときに無効になるように、ダウンリンクポート（1～16）を割り当てます。

```
>> /cfg/ufd/fdp 1/ltd                (Select Link to Disable menu)
>> Failure Link to Disable# addport 1  (Add port 1 as a Link to Disable)
>> Failure Link to Disable# addport 2  (Add port 2 as a Link to Disable)
```

3. UFD をオンにします。

```
>> /cfg/ufd/on                     (Turn Uplink Failure Detection on)
>> Uplink Failure Detection# apply  (Make your changes active)
>> Uplink Failure Detection# save   (Save for restore after reboot)
```

ポート 21 でリンク故障かスパニングツリーブロックが発生すると、スイッチ 1 はポート 1、ポート 2 を無効にします。

## スイッチ 2 での UFD の設定（AOS CLI の例）

1. モニタするアップリンクポート（20～24）のトランクグループを生成します。最初、各ポートとも全二重モードにしなければなりません。

```
>> Main# /cfg/port 20/gig/mode full    (Set port 20 to full duplex)
>> Main# /cfg/port 22/gig/mode full    (Set port 22 to full duplex)
>> Main# /cfg/trunk 2                  (Create trunk group 2)
>> Trunk group 2# ena                  (Enable trunk group 2)
>> Trunk group 2# add 20               (Add port 20 to trunk group 2)
>> Trunk group 2# add 22               (Add port 22 to trunk group 2)
```

2. 通信故障をモニタするトランクグループを割り当てます。

```
>> Main# /cfg/ufd/fdp 1/ena         (Enable Failure Detection Pair 1)
>> FDP# ltm                            (Select Link to Monitor menu)
>> Failover Link to Monitor# addtrnk 2  (Monitor trunk group 2)
```

3. アップリンク故障が発生したときに無効になるように、ダウンリンクポート（1～16）を割り当てます。

```
>> Main# /cfg/ufd/fdp 1/ltd            (Select Link to Disable menu)
>> Failover Link to Disable# addport 1  (Add port 1 as a Link to Disable)
>> Failover Link to Disable# addport 2  (Add port 2 as a Link to Disable)
```

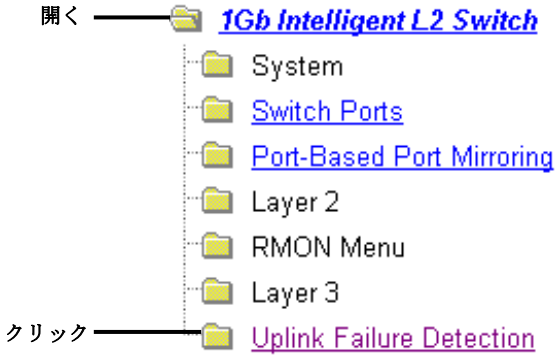
4. UFD をオンにします。

```
>> Main# /cfg/ufd/on               (Turn Uplink Failure Detection on)
>> Uplink Failure Detection# apply (Make your changes active)
>> Uplink Failure Detection# save  (Save for restore after reboot)
```

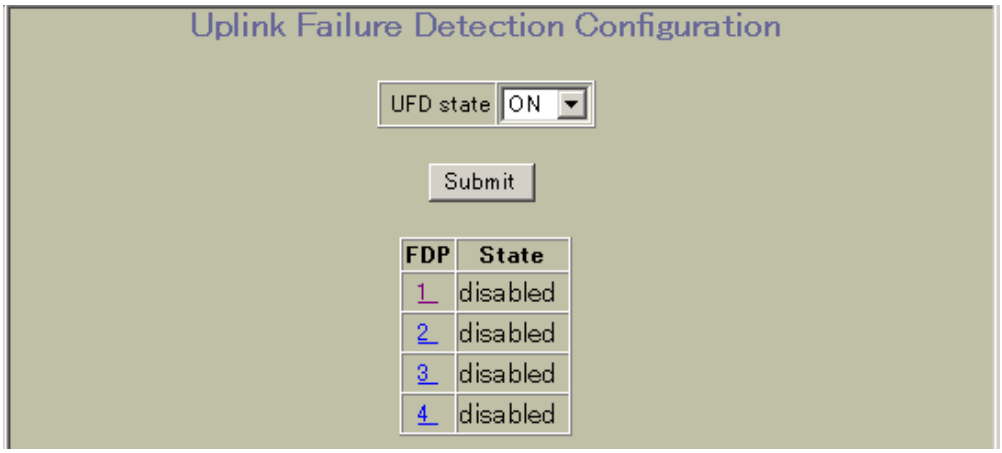
トランクグループ 2 でリンク故障かスパニングツリーブロックが発生すると、スイッチ 2 はポート 1、ポート 2 を無効にします。

## UFD の設定（BBI の例）

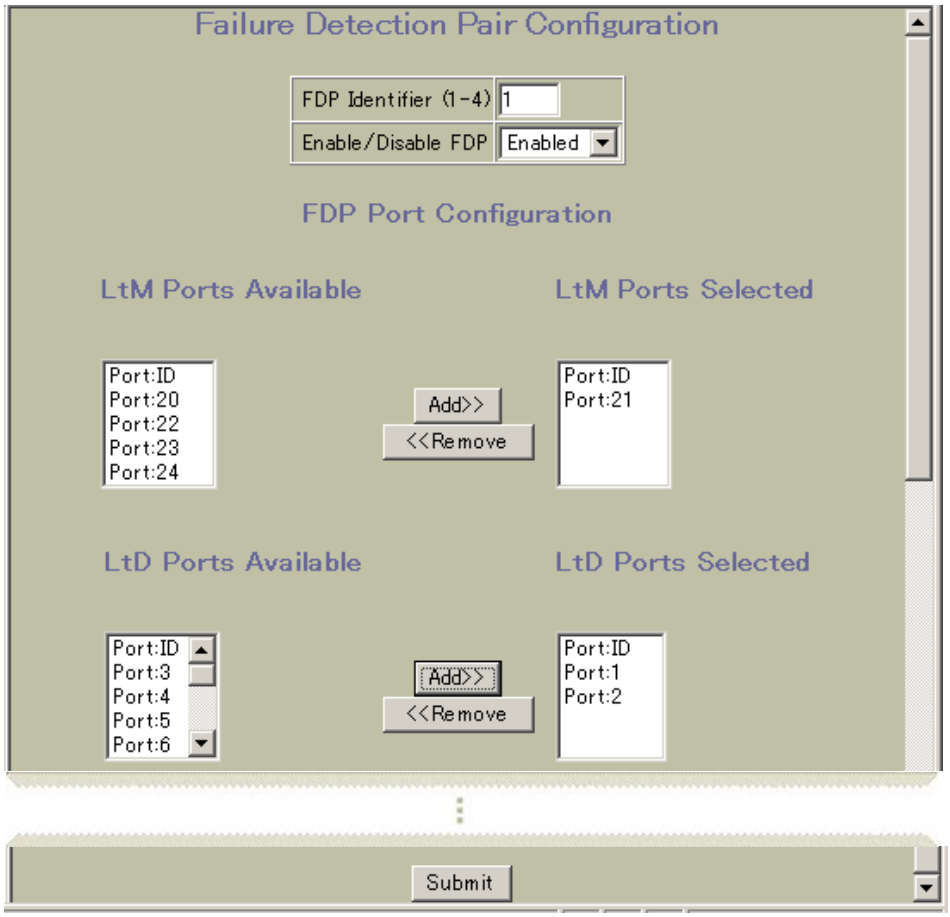
1. アップリンク故障検出を設定します。
   a. CONFIGURE ボタンをクリックします。
   b. Switch フォルダを開き、Uplink Failure Detection を選択します（フォルダではなく、下線が引かれたフォルダ名をクリックします）。




   c. UFD state を ON にして、FDP 1 を選択します。

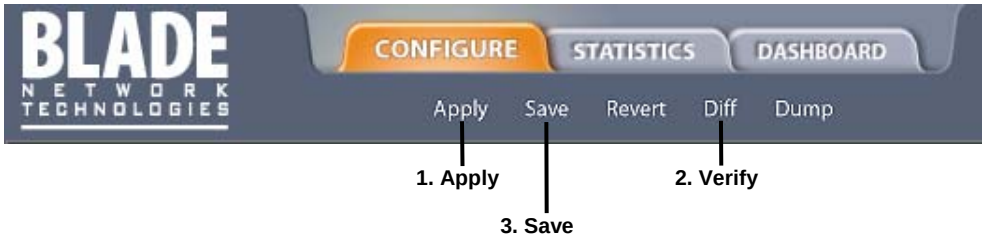


d. FDP を有効にします。LtM Ports Available リストからポートを選択し、Add をクリックしてポートを LtM に追加します。LtD Ports Available リストからポートを選択し、Add をクリックしてポートを LtD に追加します。




e. Submit をクリックします。

2. 設定を適用、確認、保存します。



# Troubleshooting tools

## はじめに

この付録では、ポートモニタリング機能によりスイッチの一般的ネットワーク問題をトラブルシューティングするときに役立つツールを紹介します。

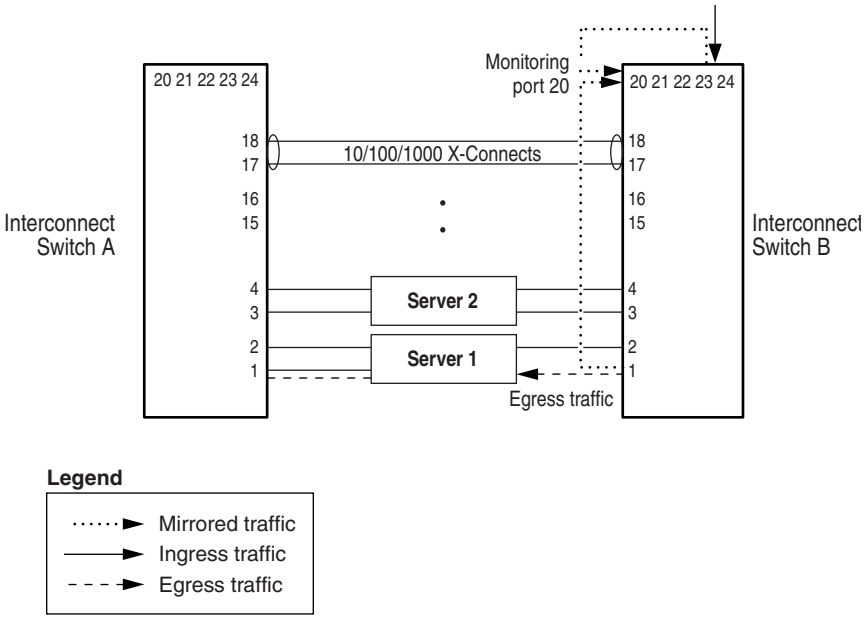
## ポートミラーリング

接続関連問題のトラブルシューティングに非常に有用な機能です。ポートを出入りするトラフィックを、ネットワークモニタを接続できるポートにミラーリングします。

トラブルシューティングツールとしても、また、ネットワークのセキュリティを高めるのにも利用できます。たとえば、侵入検出サービス (IDS) サーバをモニタポートに接続して、ネットワークを攻撃する侵入者を検出できます。

たとえば次の図では、ポート 20 でポート 23 の入りトラフィック（スイッチに入ってきたトラフィック）、ポート 1 の出トラフィック（スイッチから出ていくトラフィック）をモニタしています。装置をポート 20 に接続すれば、ポート 23 と 1 のトラフィックをモニタできます。

図11　ポートモニタリング




この図は、2 つの被ミラーリングポートを 1 つのポートでモニタしているケースです。同様に、1 つの被ミラーリングポートを 1 ポートで、多数の被ミラーリングポートを 1 ポートでモニタすることもできます。しかし、1 つのポートを複数のポートでモニタする機能はサポートしていません。一度にモニタするのは 1 ポートだけだからです。

入りトラフィックは、処理前に二重化して、ミラーリングポートに送られます。出力トラフィックは、処理後に二重化して、ミラーリングポートに送られます。

## ポートミラーリングの設定（AOS CLI の例）

上図の例でポートミラーリングを設定するには、

1. モニタリングポートを指定します。

```
>> # /cfg/pmirr/monport 20            (Select port 20 for monitoring)
```

2. ミラーリングしたいポートを選択します。

```
>> Port 20 # add 23                        (Select port 23 to mirror)
>> Enter port mirror direction [in, out, or both]: in
(Monitor ingress traffic on port 23)
>> Port 20 # add 11                        (Select port 11 to mirror)
>> Enter port mirror direction [in, out, or both]: out
(Monitor egress traffic on port 1)
```

3. ポートミラーリングを有効にします。

```
>> # /cfg/pmirr/mirr ena                     (Enable port mirroring)
```

4. 設定を適用、保存します。

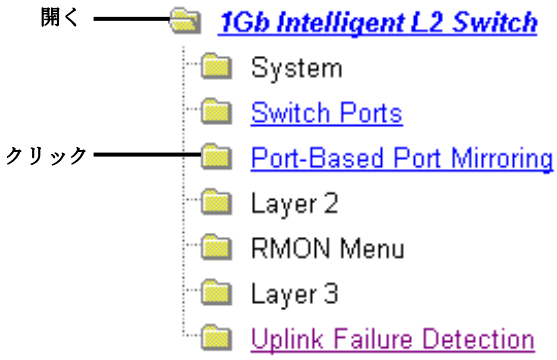
```
>> PortMirroring# apply                (Apply the configuration)
>> PortMirroring# save                  (Save the configuration)
```

5. 現在の設定を確認します。

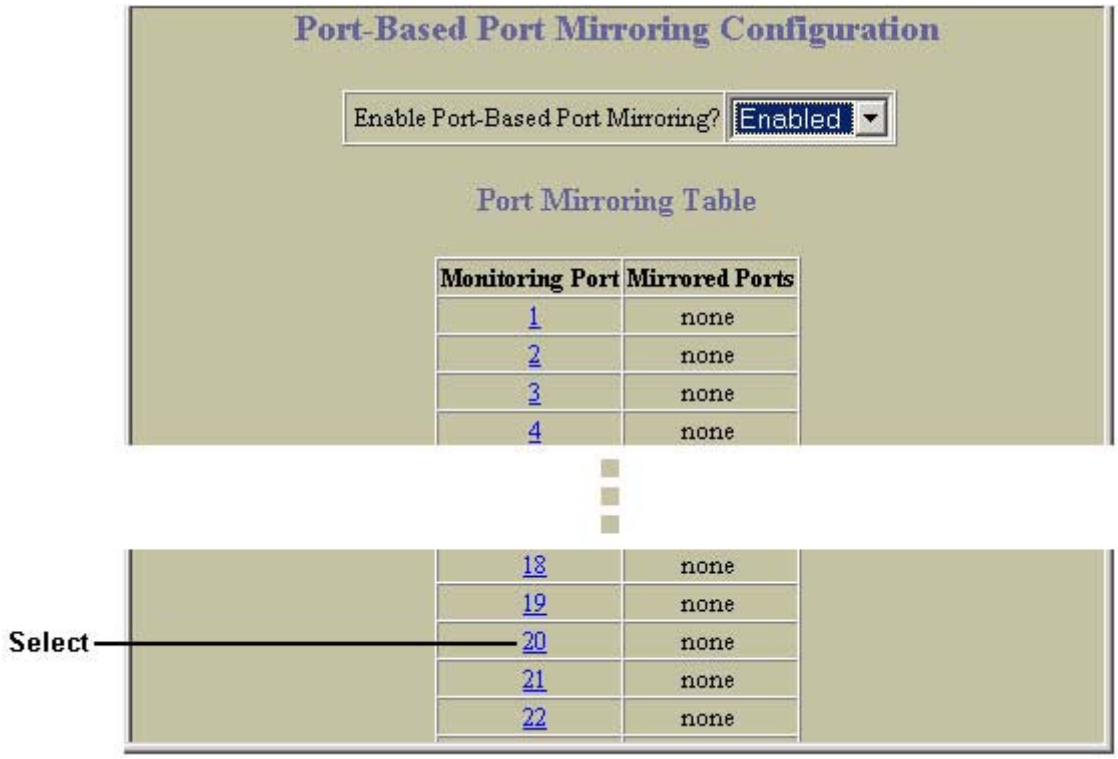
```
>> PortMirroring# cur              (Display the current settings)
Port mirroring is enabled
Monitoring Ports Mirrored Ports
1     none
2     none
3     none
4     none
5     none
   :
   :
17    none
18    none
20(23, in) (11, out)
21    none
   :
```

# ポートミラーリングの設定（BBI の例）

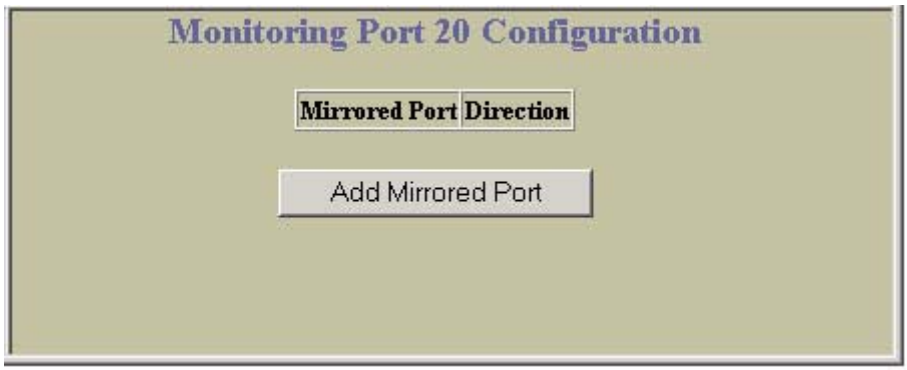
1. ポートミラーリングを設定します。
   a. CONFIGURE ボタンをクリックします。
   b. Switch フォルダを開き、Port-Based Port Mirroring を選択します（フォルダではなく、下線が引かれたフォルダ名をクリックします）。




   c. ポート番号をクリックしてミラーリングポートを選択します。



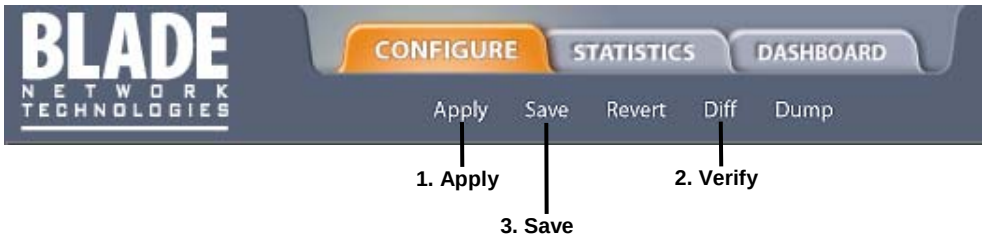

   d. Add Mirrored Port をクリックします。



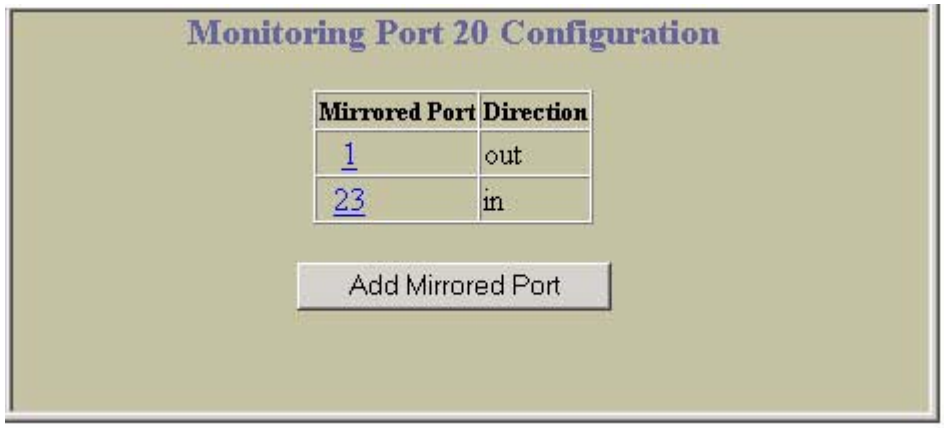
e. 被ミラーリングポートのポート番号を入力し、Port Mirror Direction を選択します。


f. Submit をクリックします。

2. 設定を適用、確認、保存します。




3. スイッチのポートミラーリング情報を確認します。



# その他のネットワークトラブルシューティング機能

その他、以下のネットワークトラブルシューティング機能があります。

## コンソールメッセージとシスログメッセージ

本スイッチに問題がある場合、コンソールメッセージとシスログメッセージを調べます。状態が変化して、システム問題が発生すると、メッセージがスイッチに表示されます。シスログメッセージは、`/info/sys/log` コマンドにより参照できます。シスログメッセージの詳細については、「コマンドリファレンスガイド」を参照してください。

## ping

ネットワーク経由のステーション間接続を調べるには、次のコマンドを実行します。

```
ping <host name> | <IP address> [ (number of tries) [ msec delay ]]
```

`IP address` は装置のホスト名か IP アドレス、`number of tries`（オプション）は試行回数（1〜32）です。`msec delay`（オプション）は試行間隔で、単位は msec です。

## traceroute

ネットワーク経由のステーション間接続に用いるルートを調べるには、次のコマンドを実行します。

```
traceroute <host name> | <IP address> [<max-hops> [ msec delay ]]
```

`IP address` はターゲットステーションのホスト名か IP アドレス、`max-hops`（オプション）はトレースする最大距離（1〜16 台）、`msec delay` はミリ秒単位の応答待ち時間です。

## 統計データとステータス情報

スイッチは大量の統計データを追跡しますが、その多くがエラー状態カウンタです。LAN 問題や実サーバ問題をトラブルシューティングするときには、統計データとステータス情報が非常に有効です。統計データの詳細については、以下を参照してください。

- 「ブラウザベースインタフェースリファレンスガイド」の「統計データの確認」の章
- 「コマンドリファレンスガイド (AOS) 」の「Statistics Menu」の章
- 「コマンドリファレンスガイド (ISCLI) 」の「Statistics Commands」の章

## カスタマサポートツール

以下の診断ツールはユーザが利用することはできません。

- オフライン診断 — スイッチのハードウェア問題をトラブルシューティングします。ハードウェアが仕様範囲内で動作しているかどうかを確認できます。
- ソフトウェアパニック — 実行中に致命的なソフトウェア問題が見つかると、その時点のハードウェアとソフトウェアのステータス情報をパニックダンプに送ります。そのダンプを事後分析して、問題の原因を突き止めることができます。
- スタックトレース — 致命的なソフトウェア問題が発生すると、スタックトレースデータをコンソールにダンプします。