N8406-026　10GbE **インテリジェントスイッチ** (L3)

アプリケーションガイド

文書番号: 856-127813-026-A

初版: 2008 **年** 7 **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 の米国およびその他の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: 856-127813-026-A

  初版: 2008 年 7 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。
- Port-based Network Access and Traffic Control：スイッチの LAN ポートにポイントツーポイントで接続したデバイスの認証方法を説明します。また、ポートベースのトラフィック制御はブロードキャストストームを防御します。
- 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。
- Quality of Service：ACL を利用した IP フィルタリング、IEEE802.1p を利用した QoS 機能について説明します。
- 基本 IP ルーティング：IP ルーティングの設定方法について説明します。
- Routing Information Protocol (RIP)：他のルータとルート情報を交換する RIP 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。
- Open Shortest Path First (OSPF)：本スイッチでの OSPF の実装、設定例について説明します。
- Remote Monitoring (RMON)：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。本スイッチでは Uplink Failure Detection と Virtual Router Redundancy Protocol (VRRP)を実装しています。
- 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。

- N8406-026 10GbE インテリジェントスイッチ (L3) ユーザーズガイド
- N8406-026 10GbE インテリジェントスイッチ (L3) コマンドリファレンスガイド (AOS)
- N8406-026 10GbE インテリジェントスイッチ (L3) コマンドリファレンスガイド (ISCLI)
- N8406-026 10GbE インテリジェントスイッチ (L3) 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。 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

10GbE インテリジェントスイッチ (L3) 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 17) 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 17 — 管理ポート 17 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 17 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 250— マネジメント用のインタフェースです。インタフェース 250 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 250 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 254 — マネジメントインタフェース（インタフェース 250）用のデフォルトゲートウェイです。
- STG128 — 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 128 (STG128) にありますが、他の VLAN を追加することはできません。STG128 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 250）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 250 に IP アドレス 205.21.17.3 を設定します。
2. dhcp クライアントを無効にします。

```
>> # /cfg/sys/dhcp disable                (Disable dhcp)
```

3. 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 250                  (Select IP interface 250)
>> IP Interface 250# 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 250# ena             (Enable IP interface 250)
```

4. 必要に応じて、デフォルトゲートウェイを設定します。
5. 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 250# ../gw 254            (Select default gateway 254)
>> Default gateway 254# addr 205.21.17.1   (Assign IP address for a router)
>> Default gateway 254# ena                (Enable default gateway 254)
```

6. 設定を適用、保存、確認します。

```
>> Default gateway 254# apply           (Apply the configuration)
>> Default gateway 254# save            (Save the configuration)
>> # /cfg/dump                          (Verify the configuration)
```

注：インタフェース 250 **に** IP **アドレスを手動で設定する場合、**dhcp **を無効にしてください。**dhcp **が有効で** DHCP **サーバから** IP **アドレスを取得した場合、手動で設定した** IP **アドレスより優先されます。**

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 Menu — 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。
  - QoS — QoS 機能を設定します。
  - Access Control — Access Control List/Group 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 マネージャで設定する Read と Write のコミュニティ名と、スイッチ側の設定を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. アクセスグループを、グループがアクセスできるビューとともに設定します。アクセステーブルを使用してグループのアクセスレベルを設定します。

```
>> # /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"
```

read view (rview)、write view (wview)、notify view (nview)をすべて iso に設定すると、ユーザは public と privateMIB のすべてにアクセスできます。

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"                                  (ユーザを設定)
/c/sys/ssnmp/snmpv3/access 3                (アクセスグループ3を設定)
name "usrgrp"
rview "usr"
wview "usr"
nview "usr"
/c/sys/ssnmp/snmpv3/group 4                 (アクセスグループにuserを割当)
uname usr
gname usrgrp
/c/sys/ssnmp/snmpv3/view 6                  (ユーザ用のviewを作成)
name "usr"
tree "1.3.6.1.4.1.26543.2.6.1.2"            (Agent statistics)
/c/sys/ssnmp/snmpv3/view 7
name "usr"
tree "1.3.6.1.4.1.26543.2.6.1.3"            (Agent information)
/c/sys/ssnmp/snmpv3/view 8
name "usr"
tree "1.3.6.1.4.1.26543.2.6.2.2"            (L2 statistics)
/c/sys/ssnmp/snmpv3/view 9
name "usr"
tree "1.3.6.1.4.1.26543.2.6.2.3"            (L2 information)
/c/sys/ssnmp/snmpv3/view 10
name "usr"
tree "1.3.6.1.4.1.26543.2.6.3.2"            (L3 statistics)
/c/sys/ssnmp/snmpv3/view 11
name "usr"
tree "1.3.6.1.4.1.26543.2.6.3.3"            (L3 information)
```

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"                                  (ユーザを設定)
/c/sys/ssnmp/snmpv3/access 4                 (アクセスグループ4を設定)
name "opergrp"
rview "oper"
wview "oper"
nview "oper"
/c/sys/ssnmp/snmpv3/group 5                  (アクセスグループにoperを割当)
uname oper
gname opergrp
/c/sys/ssnmp/snmpv3/view 20                  (ユーザ用のviewを作成)
name "oper"
tree "1.3.6.1.4.1.26543.2.6.1.2"              (Agent statistics)
/c/sys/ssnmp/snmpv3/view 21
name "oper"
tree "1.3.6.1.4.1.26543.2.6.1.3"              (Agent information)
/c/sys/ssnmp/snmpv3/view 22
name "oper"
tree "1.3.6.1.4.1.26543.2.6.2.2"              (L2 statistics)
/c/sys/ssnmp/snmpv3/view 23
name "oper"
tree "1.3.6.1.4.1.26543.2.6.2.3"              (L2 information)
/c/sys/ssnmp/snmpv3/view 24
name "oper"
tree "1.3.6.1.4.1.26543.2.6.3.2"              (L3 statistics)
/c/sys/ssnmp/snmpv3/view 25
name "oper"
tree "1.3.6.1.4.1.26543.2.6.3.3"              (L3 information)
```

SNMP トラップホストの設定

SNMPv1 トラップホストの設定

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"                          (v1trapという名前のユーザを設定)
```

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      (SNMPv1トラップを受信するアクセスグループを設定)
name "v1trap"
model snmpv1
nview "iso"
/c/sys/ssnmp/snmpv3/group 10         (アクセスグループにユーザを割当)
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        (通報テーブルにユーザを割当)
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         (トラップを送信するIPアドレスを設定)
name v1trap
addr 47.80.23.245
taglist v1trap
pname v1param
/c/sys/ssnmp/snmpv3/tparam 10        (ターゲットパラメータテーブルを設定)
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          (コミュニティ名を設定)
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"                              (v2trapという名前のユーザを設定)
/c/sys/ssnmp/snmpv3/access 10      (SNMPv2トラップを受信するアクセスグループを設定)
        name "v2trap"
        model snmpv2
        nview "iso"
/c/sys/ssnmp/snmpv3/group 10               (アクセスグループにユーザを割当)
        model snmpv2
        uname v2trap
        gname v2trap
/c/sys/ssnmp/snmpv3/taddr 10               (トラップを送信するIPアドレスを設定)
        name v2trap
        addr 47.81.25.66
        taglist v2trap
        pname v2param
/c/sys/ssnmp/snmpv3/tparam 10              (ターゲットパラメータテーブルを設定)
        name v2param
        mpmodel snmpv2c
        uname v2trap
        model snmpv2
/c/sys/ssnmp/snmpv3/notify 10              (通報テーブルにユーザを割当)
        name v2trap
        tag v2trap
/c/sys/ssnmp/snmpv3/comm 10                (コミュニティ名を設定)
        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"                    (v3trapという名前のユーザを設定)
        auth md5
        authpw v3trap
/c/sys/ssnmp/snmpv3/access 11     (SNMPv3トラップを受信するアクセスグループを設定)
        name "v3trap"
        level authNoPriv
        nview "iso"
/c/sys/ssnmp/snmpv3/group 11             (アクセスグループにユーザを割当)
        uname v3trap
        gname v3trap
/c/sys/ssnmp/snmpv3/taddr 11             (トラップを送信するIPアドレスを設定)
        name v3trap
        addr 47.81.25.66
        taglist v3trap
        pname v3param
/c/sys/ssnmp/snmpv3/tparam 11            (ターゲットパラメータテーブルを設定)
        name v3param
        uname v3trap
        level authNoPriv                 (認証レベルを設定)
/c/sys/ssnmp/snmpv3/notify 11            (通報テーブルにユーザを割当)
        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します。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されます。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]: <UDP 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。

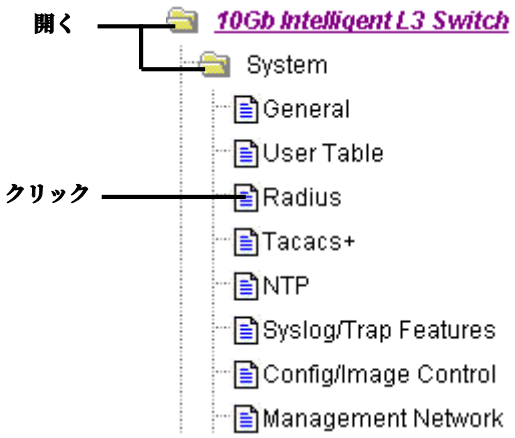
```
>> RADIUS Server# retries
Current RADIUS server retries: 3
Enter new RADIUS server retries [1-3]:<server retries>
>> RADIUS Server# time
Current RADIUS server timeout: 3
Enter new RADIUS server timeout [1-10]: 10  (Enter the timeout period
                                             in seconds)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

6. 設定を適用、保存します。

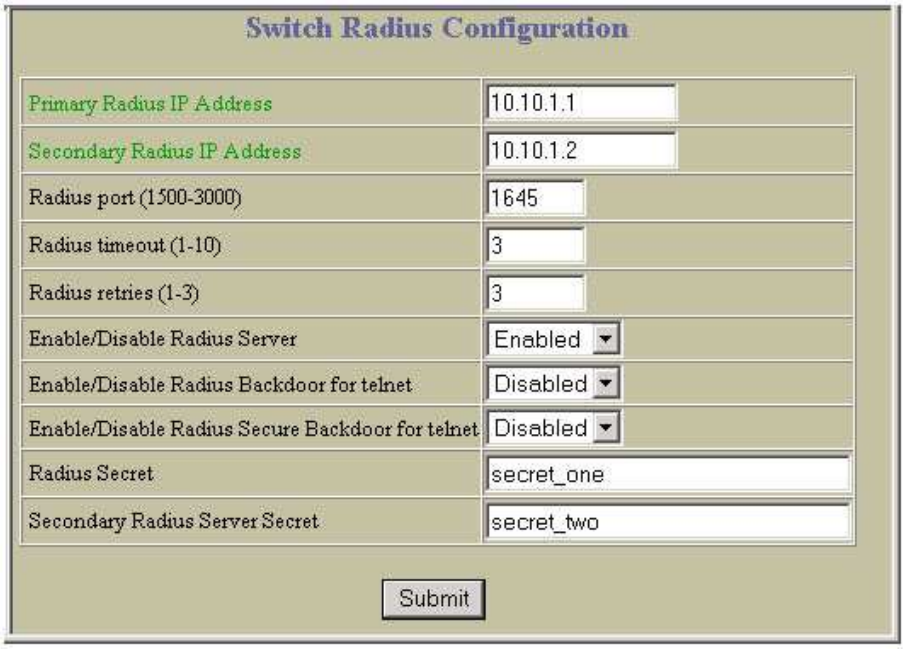
```
>> RADIUS Server# apply
>> RADIUS Server# save
```

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。



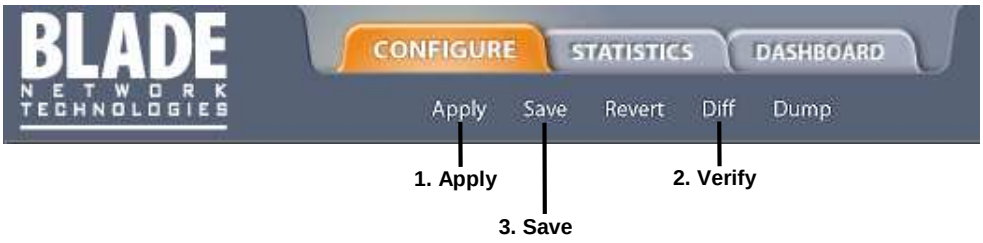
   c. プライマリ RADIUS サーバとセカンダリ RADIUS サーバの IP アドレス、各サーバの RADIUS シークレットを入力し、RADIUS サーバを有効にします。



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。TACACS+用にウェルノンポートは 49 です。

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

4. 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)
```

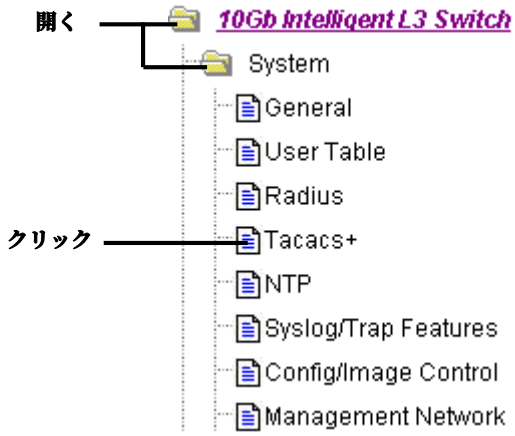
5. カスタム特権レベルマッピングを行います（オプション）。

```
>> 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
```

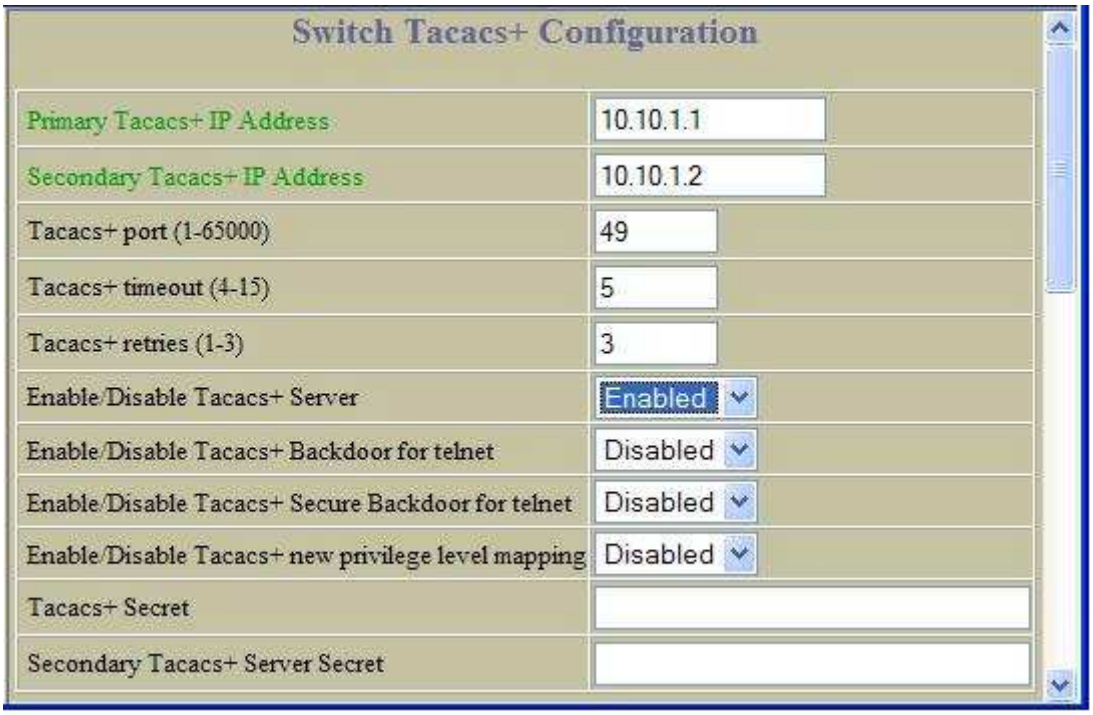
6. 設定を適用、保存します。

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。

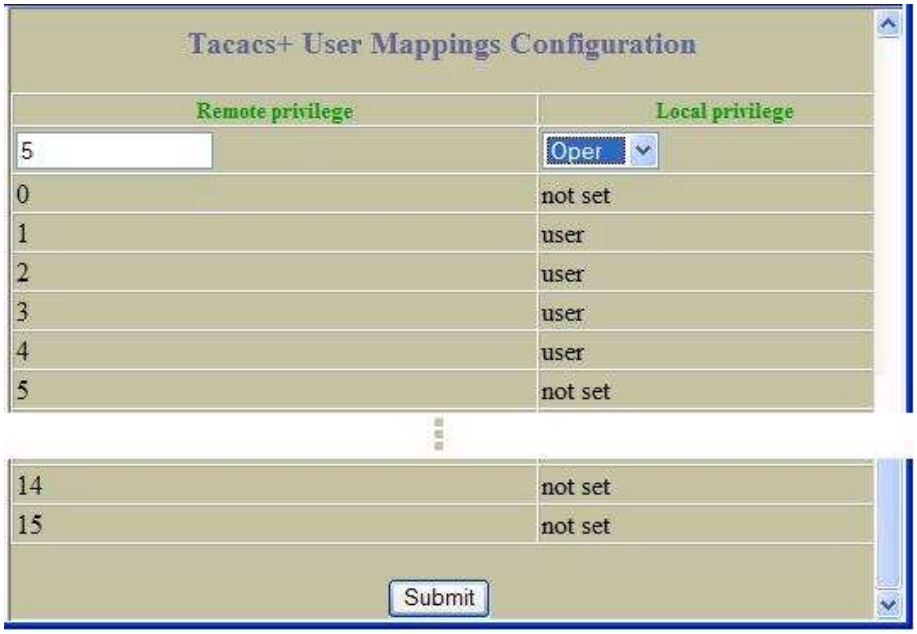


   c. プライマリとセカンダリの TACACS+サーバの IP アドレスを入力し、TACACS+シークレットを入力します。TACACS+を有効にします。

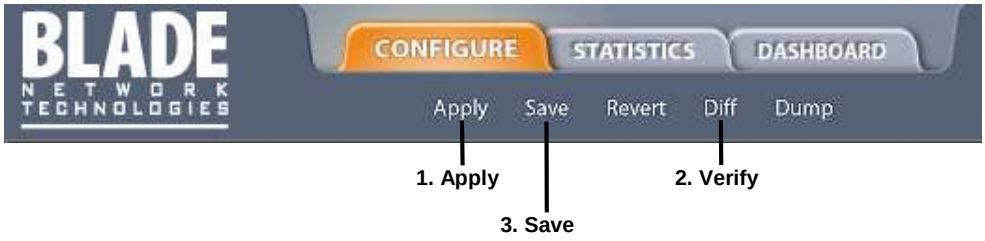


   d. Submit をクリックします。

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 を有効にする必要があります。

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.
```

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、AES128-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、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+、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 認証は、パスワードの長さは 16 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、4 つの外部ポート、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	Mgmt
18	Uplink1
19	Uplink2
20	Uplink3
21	Uplink4

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 40 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。

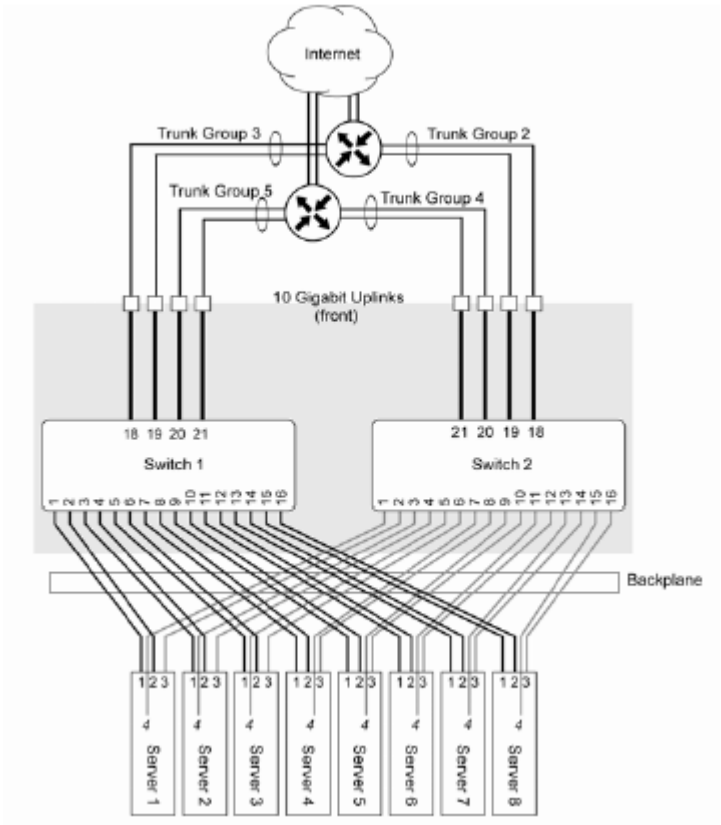
- どのトランクも 1 台の装置から出て 1 台の装置に向かわなければなりません。たとえば、サーバ 1 からのリンクとサーバ 2 からのリンクを 1 つのトランクグループにまとめることはできません。
- どの物理スイッチポートも 1 つのトランクグループだけに所属させます。
- Cisco® EtherChannel®テクノロジに準拠しなければなりません。
- トランクを有効にする前に、すべてのトランクメンバポートを同じ VLAN 構成に割り当てなければなりません。
- トランクメンバの VLAN 設定を変更しても、すべてのトランクメンバの VLAN 設定を変更しない限り、その変更を適用することはできません。
- 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、どのト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で、合計 4 つのトランクグループを構成します。各スイッチに 2 トランクグループです。

> **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 2～5 は各々2 つの 10 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 20               (Add port 20 to trunk group 5)
>> Trunk group 5# add 21               (Add port 21 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 18               (Add port 18 to trunk group 3)
>> Trunk group 3# add 19               (Add port 19 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 20               (Add port 20 to trunk group 4)
>> Trunk group 4# add 21               (Add port 21 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 18               (Add port 18 to trunk group 2)
>> Trunk group 2# add 19               (Add port 19 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。

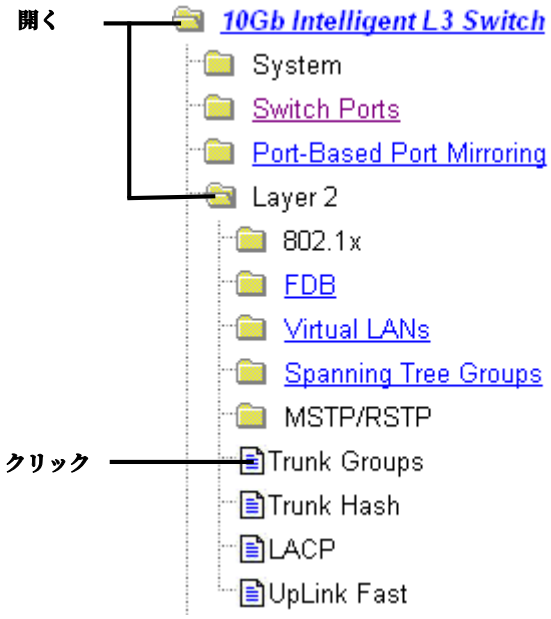
3. 次のコマンドにより、各スイッチのトランキング情報を確認します。

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

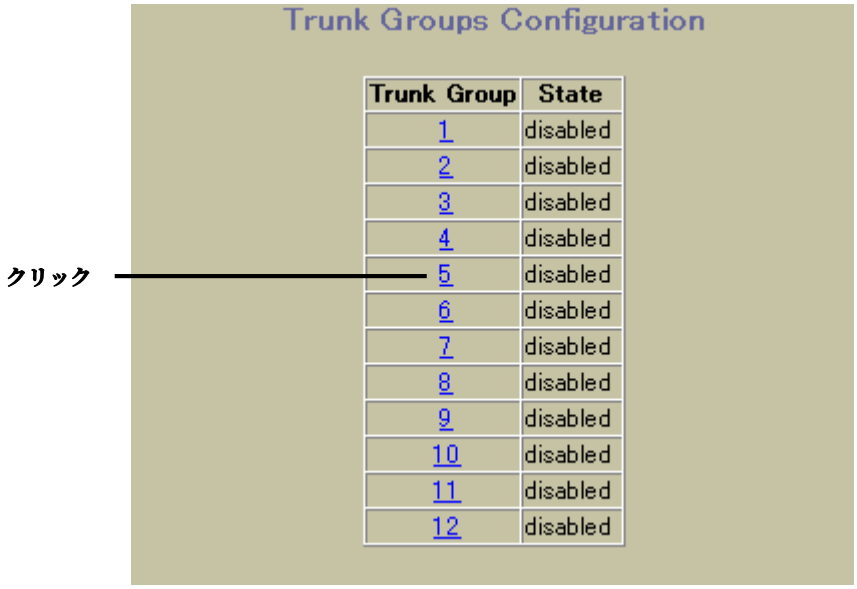
設定済みの各トランクグループの各ポートに関する情報が表示されます。トランクグループが予定したポートで構成されていること、各ポートが予定通りの状態にあることを確認します。

トランクグループの設定（BBI の例）

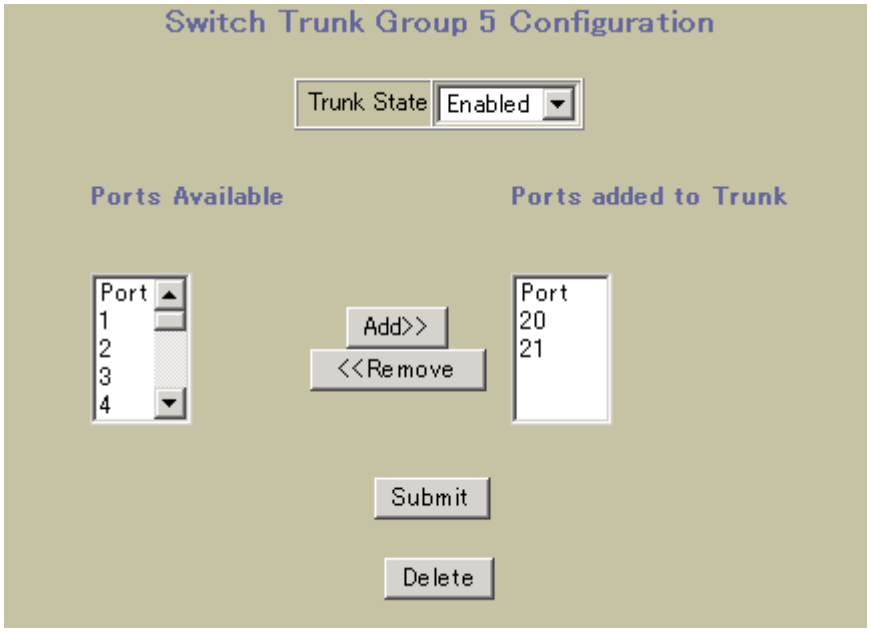
1. トランクグループを設定します。
   a. ツールバーの CONFIGURE ボタンをクリックします。
   b. Layer 2 フォルダを開き、Trunk Groups を選択します。



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

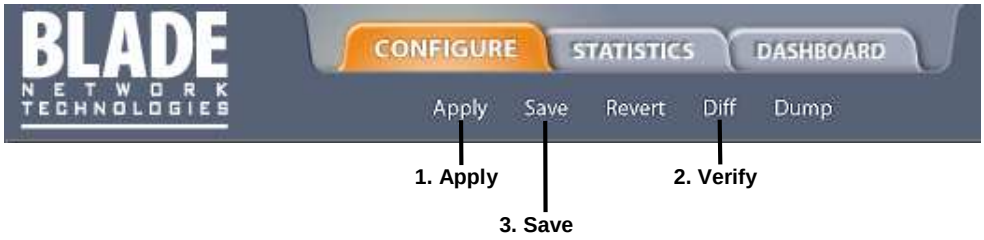


d. トランクグループを有効にします。ポートを追加するには、Ports Available リストの各ポートを選択し、Add をクリックします。



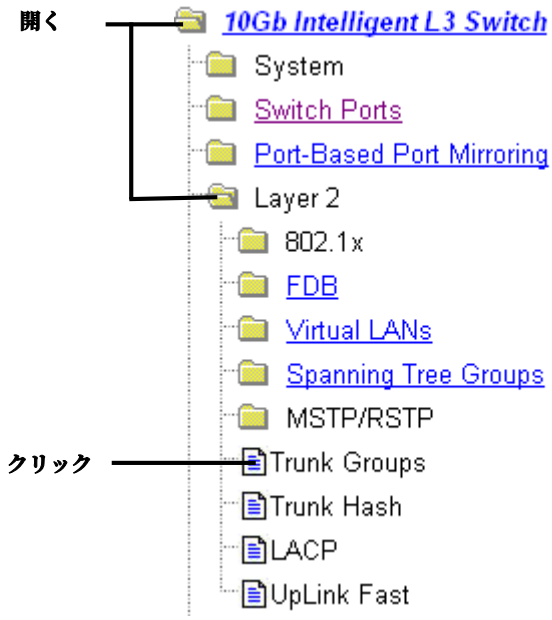
e. Submit をクリックします。

2. 設定を適用、確認、保存します。

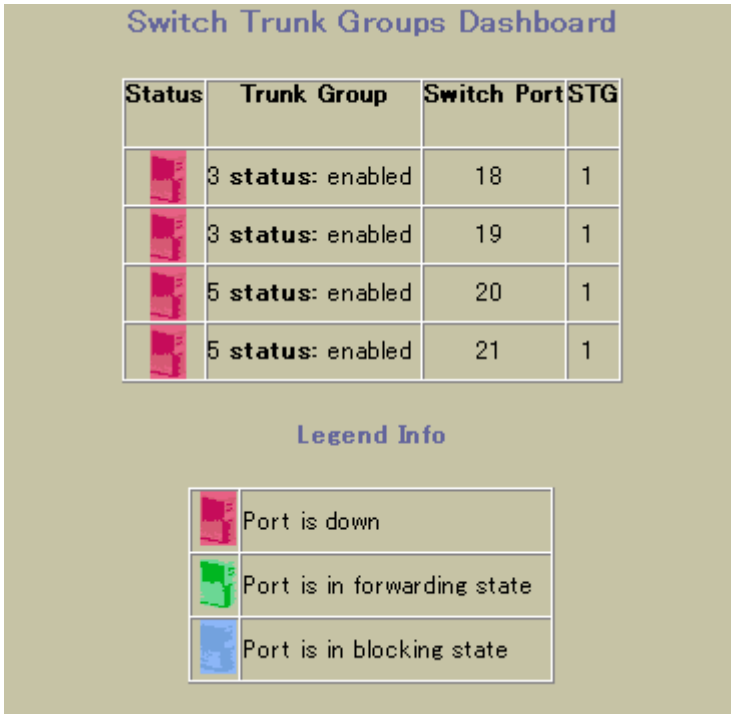


3. 各スイッチのトランキング情報を調べます。
   a. ツールバーの DASHBOARD コンテキストボタンをクリックします。

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

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

Link Aggregation Control Protocl (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 18 (admin key = 100)	ポート 1 (admin key = 50)	
ポート 19 (admin key = 100)	ポート 2 (admin key = 50)	
ポート 20 (admin key = 200)		ポート 3 (admin key = 60)
ポート 21 (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 18、19 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 20、21 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。

注:ポートに LACP **と** 802.1x **ネットワークアクセス制御を設定する場合、接続される両側のポートの** LACP **および** 802.1x **の設定が適切に設定されていることを確認してください。**

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)
```

Port-based Network Access and traffic control

Port-based Network Access Control

ポートベースのネットワークアクセス制御は、LAN ポートにポイントツーポイントで接続された装置を認証、許可する機能です。認証、許可に失敗したポートへのアクセスを防止します。この機能により、10GbE インテリジェントスイッチのすべてのポートにセキュリティを実現します。

本節で説明する項目は次のとおりです。

- Extensible Authentication Protocol over LAN
- 802.1x 認証プロセス
- 802.1x ポート状態
- サポートされる RADIUS アトリビュート
- 設定のガイドライン

Extensible authentication protocol over LAN (EAPoL)

IEEE 802.1x プロトコルを使用して、ポートのユーザレベルセキュリティを確保できます。他のポートベースのネットワークアクセス制御方法より安全です。 認証に失敗した 802.1x 有効ポートに接続した装置は、ネットワークにアクセスできなくなり、そのポートを通じて提供されるサービスが拒否されます。

802.1x 規格において、EAPoL を用いたポートベースのネットワークアクセス制御が説明されています。EAPoL には、LAN ポートにポイントツーポイントで接続された装置を認証、許可する機能、認証/許可に失敗したポートのアクセスを防止する機能があります。

EAPoL は、以下のコンポーネントからなるクライアントサーバプロトコルです。

- サプリカントまたはクライアント：サプリカントはネットワークアクセスを要求し、必要な証明書（ユーザ名とパスワード）をオーセンティケータと認証サーバに提示するデバイスです。
- オーセンティケータ：オーセンティケータは認証を実施して、ネットワークへのアクセスを制御します。サプリカントから提示された情報、認証サーバからの応答に基づいて、ネットワークアクセスを許可／拒否します。サプリカントと認証サーバの仲介役で、クライアントに識別情報を要求し、その情報を（RADIUS パケットに封入して）認証サーバに送り、サーバの応答をクライアントに中継し、認証交換の結果に基づいてネットワークアクセスを認定します。本スイッチはオーセンティケータとして動作します。
- 認証サーバ：サプリカントから出された証明書をチェックし、オーセンティケータによるネットワークアクセスを許可してよいかどうかを判定します。オーセンティケータと同じ場所に配置してもかまいません。本スイッチは、外部の RADIUS サーバによって認証を行います。

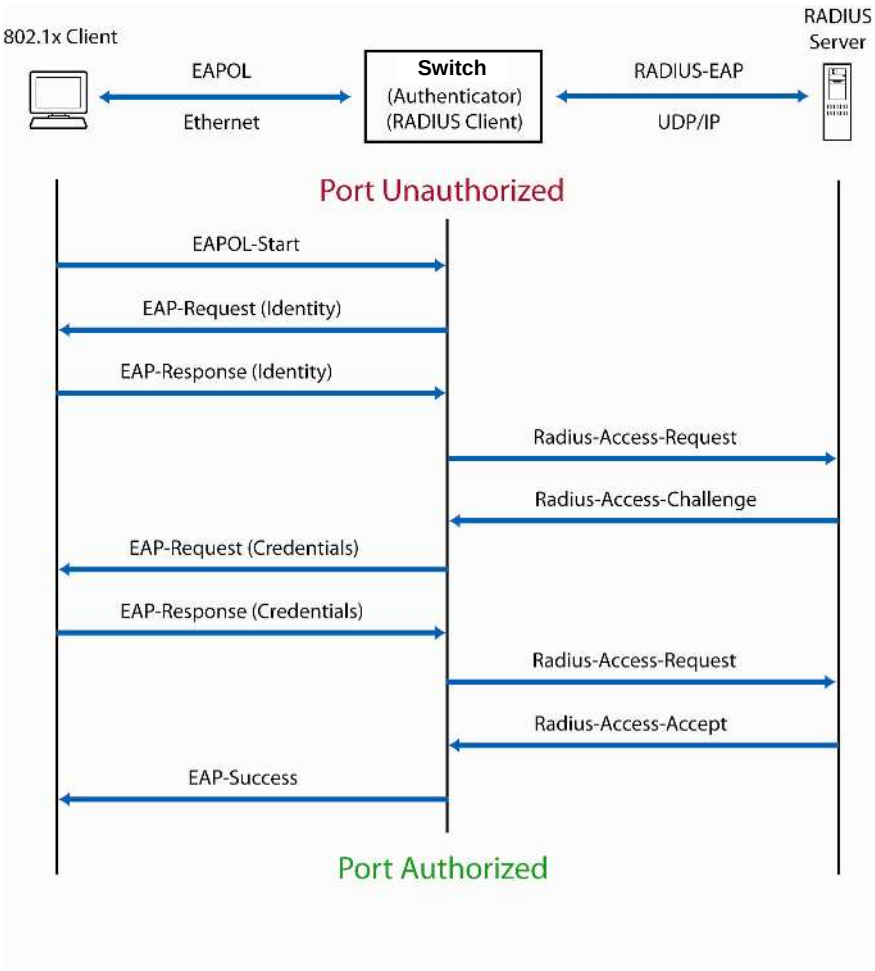
認証サーバによるクライアントの認証に成功すると、802.1x 制御ポートが Unauthorized から Authorized 状態に遷移し、クライアントはそのポートを通じてサービスにフルアクセスできます。クライアントが EAPOL-Logoff メッセージをオーセンティケータに送ると、ポートが Authorized から Unauthorized 状態に戻ります。

802.1x 認証プロセス

クライアントとオーセンティケータの通信には Extensible Authentication Protocol(EAP)を使用しますが、このプロトコルは当初 PPP 上で実行するように設計されたものです。また、IEEE 802.1x では、EAP over LAN (EAPoL)と呼ばれるイーサネットフレームでのカプセル化を規定しました。

次の図に、クライアントによって開始される一般的なメッセージ交換を示します。

図2　EAP によるポート認証



EAPoL メッセージ交換

認証時、クライアントとスイッチのオーセンティケータ間で EAPOL メッセージを交換し、スイッチのオーセンティケータと Radius 認証サーバ間で RADIUS-EAP メッセージを交換します。

認証の開始には以下の方法があります。

- スイッチのオーセンティケータがクライアントに EAP-Request/Identity フレームを送信する。
- クライアントがスイッチのオーセンティケータに EAPOL-Start フレームを送信する。オーセンティケータは EAP-Request/Identity フレームで応答します。

クライアントが EAP-Response/Identity フレームをスイッチのオーセンティケータに送って、自分の識別を確認する。オーセンティケータはその情報を RADIUS パケットにカプセル化したフレームをサーバに転送します。

RADIUS サーバが EAP サポート認証アルゴリズムを選択して、クライアントの識別を確認し、EAP-Request パケットをスイッチオーセンティケータ経由でクライアントに送信します。クライアントは、証明書が入っている EAP-Response で RADIUS サーバに返答します。

サーバがクライアントを認証すると、802.1x 制御ポートが Unauthorized から Authorized 状態に遷移し、クライアントはそのポートを通じてサービスにフルアクセスできます。クライアントが後で EAPOL-Logoff メッセージをスイッチのオーセンティケータに送ると、ポートが Authorized から Unauthorized 状態に戻ります。

802.1x をサポートしないクライアントが 802.1x 制御ポートに接続すると、スイッチのオーセンティケータは、ポートの動作状態の変化を検出したときに、クライアントに対して識別情報を要求します。この要求にクライアントは応答せず、ポートは Unauthorized 状態のままです。

注：802.1x **が有効なクライアントが** 802.1x **制御されていないポートに接続されると、**EAPOL-Start **フレームを送信して、認証プロセスを開始します。応答がない場合、クライアントは既定回数の要求を再送信します。応答がないと、ポートが** Authorized **状態であると見なし、**Unauthorized **状態であってもフレームの送信を開始します。**

802.1x **ポート状態**

ポートの状態は、次のように、ネットワークのアクセスがクライアントに認められているかどうかで決まります。

- Unauthorized：**この状態の間、ポートは、**EAP **パケットを除き、すべての** Ingress **トラフィック、**Egress **トラフィックを廃棄します。**
- Authorized：**クライアントが認証されると、ポートは** Authorized **状態に遷移し、クライアントとやり取りするすべてのトラフィックを正常に転送できます。**
- Force Unauthorized：**ポートの全アクセスを拒否する状態です。**
- Force Authorized：**ポートをフルアクセスできる状態です。**

スイッチのすべてのポートに 802.1x **認証を行うには、**802.1x Global Configuration Menu (/cfg/l2/8021x/global)**を使用します。ポート毎に設定する場合は** 802.1x Port Menu (/cfg/l2/8021x/port x) **を使用します。**

サポートされる RADIUS **アトリビュート**

スイッチの 802.1x **オーセンティケータは、外部** RADIUS **サーバによって** EAP **による認証を行います。**802.1x **規格の付録** D **と** RFC 3580 **に示されたガイドラインに基づいて、**RADIUS-EAP **認証の一部としてサポートされている** RADIUS **アトリビュートを、次の表に示します。**

表9 RADIUS **アトリビュートのサポート**

#	アトリビュート	アトリビュート値	A-R	A-A	A-C	A-R
1	User-Name	**サプリカントの** EAP-Response/Identity **メッセージの** Type-Data **フィールドの値。**Identity **が不明の場合（**Type-Data **フィールドの長さが** 0 **バイト）、この値は** Calling-Station-ID **と同じです。**	1	0-1	0	0
4	NAS-IP-Address	RADIUS **通信に使用されるオーセンティケータの** IP **アドレス**	1	0	0	0
5	NAS-Port	**サプリカントが接続されているオーセンティケータのポート番号**	1	0	0	0
24	State	**サーバ固有値。**Access-Challenge **の応答である** Access-Request **で、変更されずにサーバに戻されます。**	0-1	0-1	0-1	0
30	Called-Statioin-ID	ASCII **文字列としてコード化されたオーセンティケータの** MAC **アドレス。** **例：**000D5622E39F	1	0	0	0
31	Calling-Station-ID	ASCII **文字列としてコード化されたサプリカントの** MAC **アドレス。** **例：**00034B436206	1	0	0	0
79	EAP-Message	**サプリカントと認証サーバ(**RADIUS**)の間で転送する、カプセル化された** EAP **パケット。デコードされたパケットをオーセンティケータが両方のデバイスに中継します。**	1+	1+	1+	1+
80	Message-Authenticator	EAP-Message **アトリビュートも含めるときには必ず必要です。パケットの整合性を保持するために使用します。**	1	1	1	1
87	NAS-Port-ID	**オーセンティケータのポートに割り当てられた名前。例：**Server1_Port3	1	0	0	0

凡例：

RADIUS **パケットタイプ：**A-R (Access-Request), A-A (Access-Accept), A-C (Access-Challenge), A-R(Access-Reject)

RADIUS **アトリビュートサポート**

0 **パケットの内に存在してはいけないアトリビュート**

0+ **このアトリビュートのインスタンスは、パケットにないか、**1 **つ以上存在します。**

0-1 **このアトリビュートのインスタンスは、パケットにないか、**1 **つだけ存在します。**

1 **このアトリビュートのインスタンスは、パケットに** 1 **つ存在しなければなりません。**

1+ **このアトリビュートは** 1 **つ以上含める必要があります。**

EAPoL 設定ガイドライン

EAPoL を設定する場合、以下のガイドラインを考慮してください。

- 802.1x ポートベース認証は、ポイントツーポイント接続つまり 802.1x が有効なスイッチポートに接続した単一のサプリカントだけサポートしています。
- 802.1x を有効にした場合、別のレイヤ 2 機能の動作を有効にする前に、ポートを Authorized 状態にしなければなりません。たとえば、ポートが Unauthorized 状態にあるとき、STG 状態の動作は無効です。
- 802.1x サプリカント機能はサポートしていません。したがって、オーセンティケータとして機能する別装置で 802.1x が有効なポートに正常に接続するためには、リモートポートのアクセス制御を無効にするか、Force Authorized モードに設定する必要があります。たとえば、本スイッチが同じスイッチに接続していて、両スイッチで 802.1x が有効な場合、接続される 2 つのポートは Force Authorized モードに設定する必要があります。
- 802.1x 規格には、Tunnel-Type(=VLAN)、Tunnel-Medium-Type(=802)、Tunnel-Private-Group-ID(=VLAN id)などの、RADIUS トンネリングアトリビュートを介して動的に VLAN の割当てをサポートするオプションがあります。本スイッチではこれらのアトリビュートはサポートされていないため、802.1x 動作に影響する可能性があります。その他未サポートのアトリビュートには、Service-Type、Sesson-Timeout、Termination-Action があります。

802.1x 認証デバイスやユーザ向けの RADIUS アカウンティングサービスはサポートしていません。

SNMP、標準 802.1x MIB を用いて行った設定変更は、直ちに有効になります。

Port-based traffic control

ポートベースのトラフィック制御により、スイッチのポートがストームのために混乱するのを防止できます。ブロードキャストフレームや宛先未学習フレームが LAN で満たされるとストーム状態となり、ネットワークが混雑して、遅くなります。プロトコルスタックインプリメントやネットワーク設定の不具合により LAN ストームを引き起こします。

以下のトラフィックタイプの各々に対して、ポートベースのトラフィック制御を有効にできます。

- ブロードキャスト：宛先 MAC アドレスが ff:ff:ff:ff:ff:ff のパケット
- マルチキャスト：MAC アドレスの先頭オクテットの最下位ビットが 1 のパケット
- Destination Lookup Failed (DLF)：宛先 MAC アドレスが未知のパケット。ブロードキャストパケットと同様に処理します。

ポートベースのトラフィック制御を有効にすると、ポートに入ってくる、上記の各タイプのトラフィックを監視します。トラフィックが、設定したしきい値より多くなると、しきい値以内に戻るまで、越えた分をポートでブロックします。

本スイッチでは、ブロードキャスト、マルチキャスト、DLF トラフィックに別々のしきい値を設定できます。しきい値の単位はフレーム数／秒です。

注：1 トランク内のすべてのポートは、同じトラフィック制御設定にする必要があります。

ポートベーストラフィック制御の設定

ポートにトラフィック制御を設定する手順は次のとおりです。

1. トラフィック制御しきい値を設定し、トラフィック制御を有効にします。

```
Main# /cfg/port 2
>> Port 2# brate 150000          (ブロードキャストのしきい値を設定)
>> Port 2# mrate 150000          (マルチキャストのしきい値を設定)
>> Port 2# drate 150000          (DLFのしきい値を設定)
```

2. トラフィック制御しきい値を無効にするには、次のコマンドを使用します。

```
>> Port 2# mrate dis             (マルチキャストを無効)
```

3. 設定を適用、保存します。

```
>> Port 2# apply                 (適用)
>> Port 2# 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、Port17 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 Port17 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 4-16 18-21
2     VLAN 2                              ena   2 3
4095  VLAN 4095                           ena   17
```

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、Port17 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 21/pvid 21
Current port VLAN ID:     1
New pending port VLAN ID: 21

>> 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。

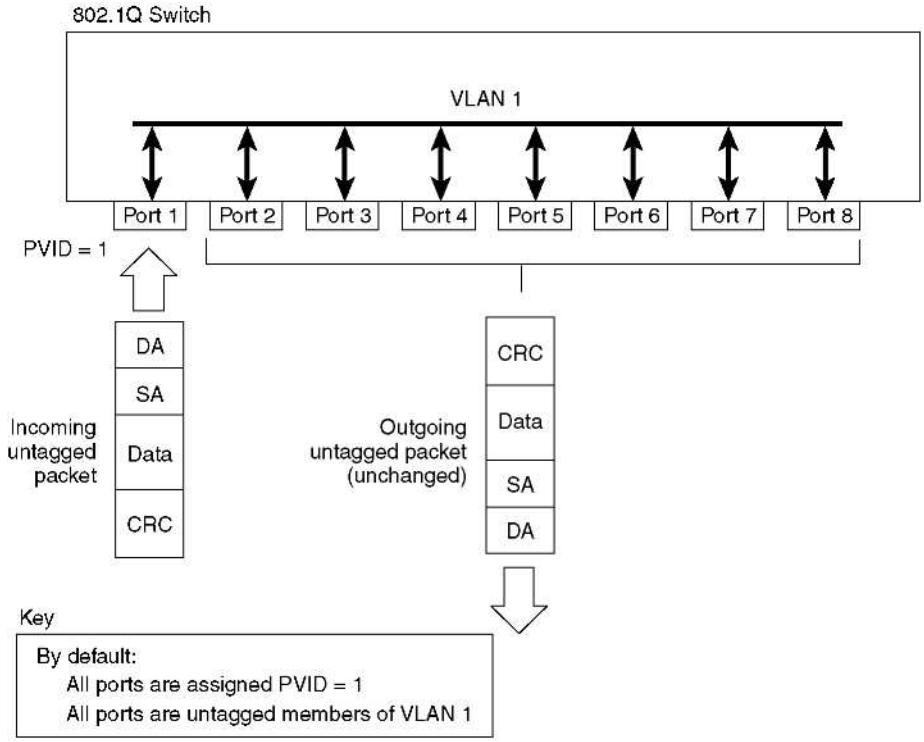
802.1Q タグで重要な用語を以下に説明します。

- 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3　デフォルト VLAN 設定

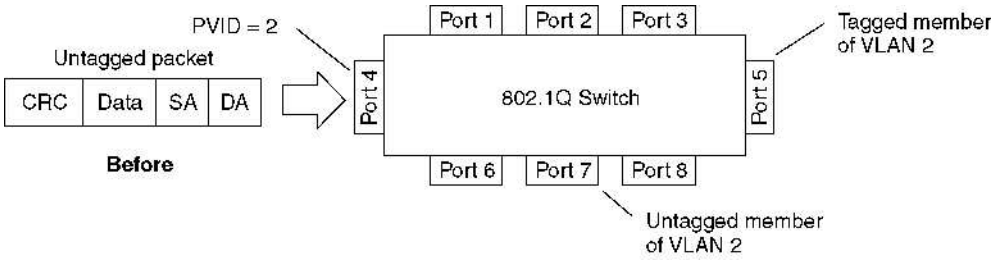


注：図に示したポート番号は、スイッチの物理ポート構成に必ずしも対応しません。

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。

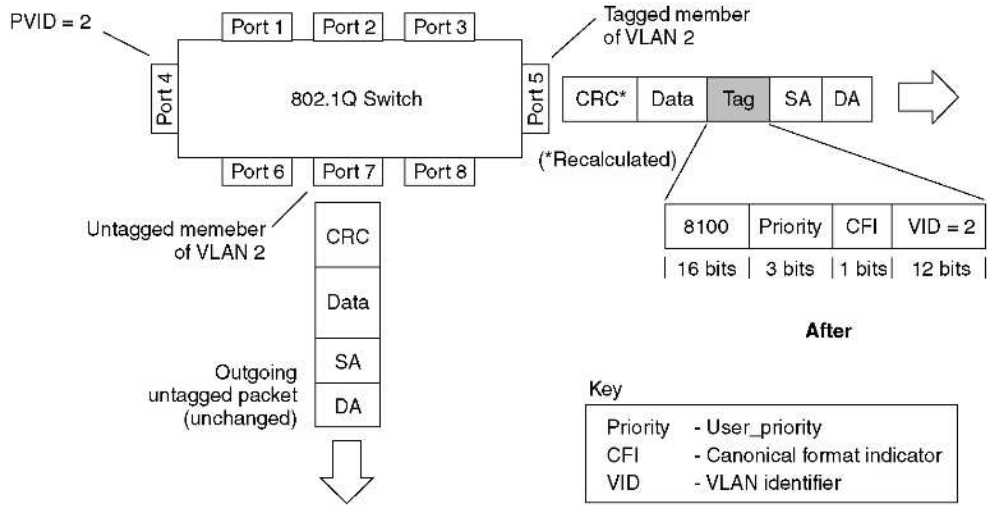
次の図は、タグなしパケットを VLAN 2 (PVID=2) の Port4 で受信する時の例です。ポート 5 を VLAN 2 のタグ付きメンバ、ポート 7 をタグなしメンバとしています。

図4　ポートベース VLAN 割当て



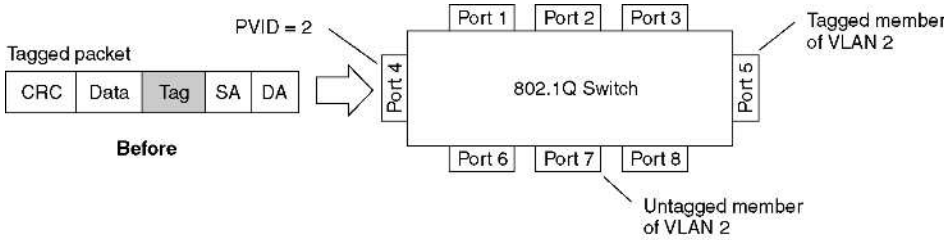
次の図に示すように、タグなしパケットは、VLAN 2 のタグ付きメンバに指定されているポート 5 を通じてスイッチから出る場合、マークされます（タグが付けられます）。
VLAN 2 のタグなしメンバに指定されているポート 7 を通じてスイッチから出るときには、元のまま変化しません。

図5 802.1Q タグ（ポートベース VLAN 割当て後）



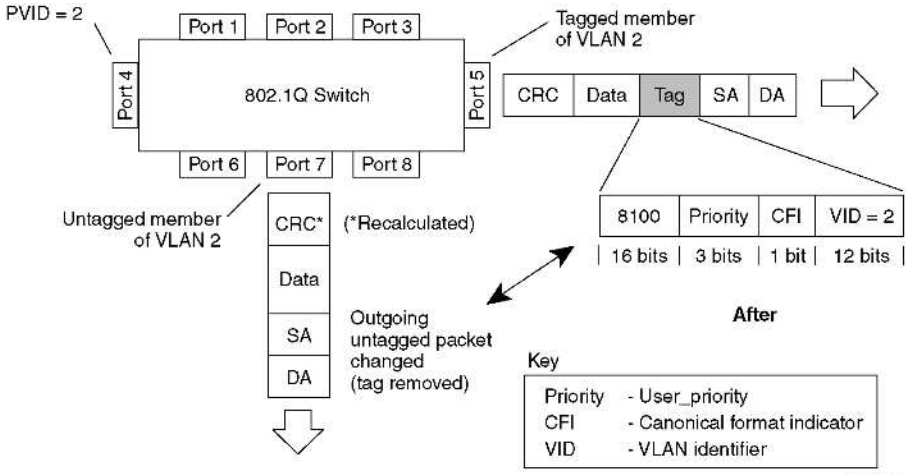
次の図は、タグ付きパケットを VLAN 2 (PVID=2) の Port4 で受信する時の例です。ポート 5 を VLAN 2 のタグ付きメンバ、 ポート 7 をタグなしメンバとしています。

図6 802.1Q 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7　802.1Q 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** 17 **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、Port17 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 2～128 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 1～32 の各々に複数の VLAN を割り当て可能です。

VLAN 構成ルール

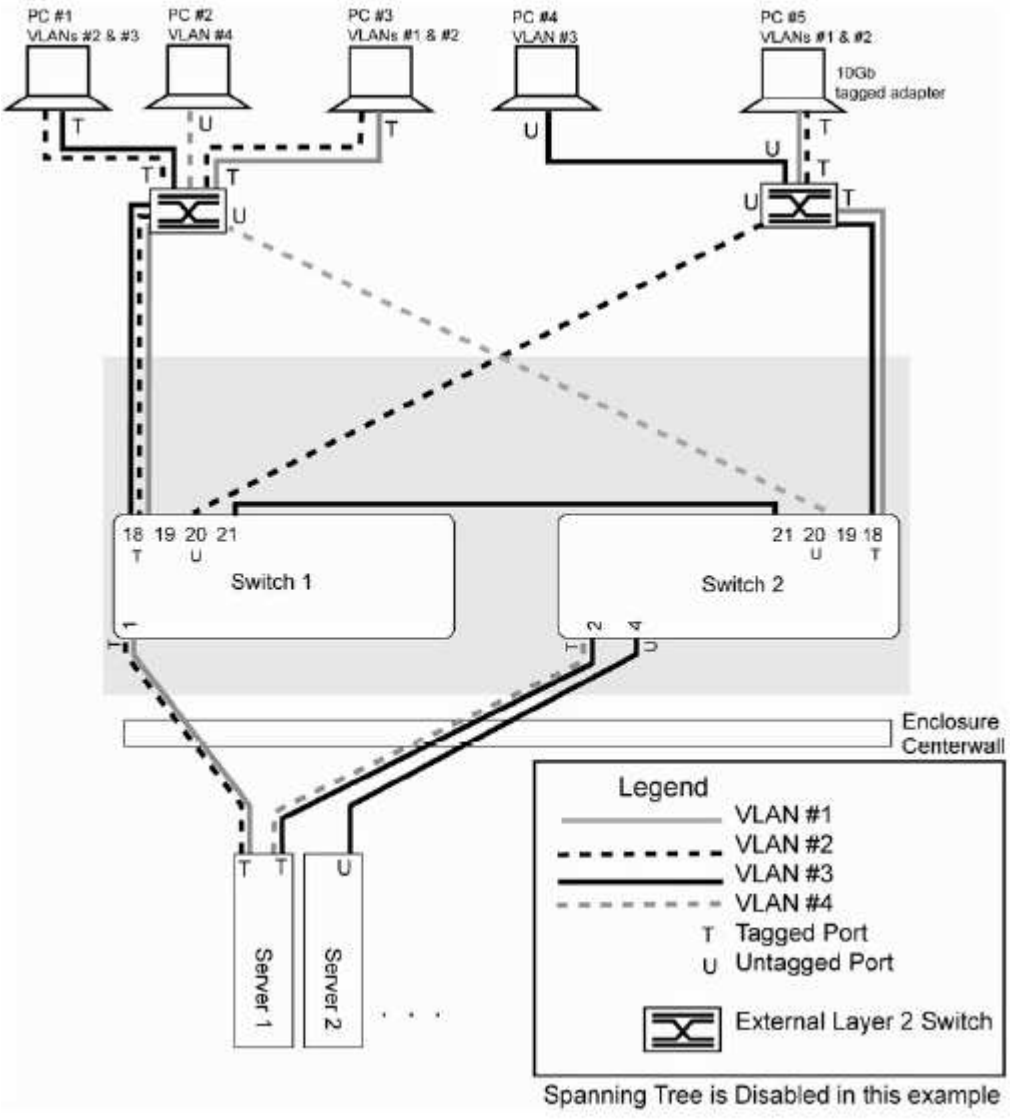
VLAN 構成時、以下の点を考慮してください。

- 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を示しています。図には示してい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8　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10　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 18 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 20 は VLAN 2 のタグなしメンバです。ポート 21 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。
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 18 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 20 は VLAN 4 のタグなしメンバです。ポート 21 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。
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。 1 つのアダプタをスイッチの 10Gbps 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。 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 18                      (Select uplink port 18)
>> Port 18# tag e                       (Enable tagging)
Current VLAN tag support: disabled
New VLAN tag support:     enabled
Port 18 changed to tagged.
>> Port 18# 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 と VLAN 3 に属するポートだけ構成します。

```
>> /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 18                                 (Add port 18 to VLAN 2)
Current ports for VLAN 2: 1
Pending new ports for VLAN 2: 18

>> VLAN 2# add 20                                 (Add port 20 to VLAN 2)
Port 20 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, 18
Pending new ports for VLAN 2: 20

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

>> VLAN 3# add 21                                 (Add port 21 to VLAN 3)
Current ports for VLAN 3: 18
Pending new ports for VLAN 3: 21

>> /cfg/port 20/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 18                                (Select uplink port 18)
>> Port 18# tag e                                        (Enable tagging)
Current VLAN tag support: disabled
New VLAN tag support:     enabled
Port 18 changed to tagged.

>> Port 18# 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。

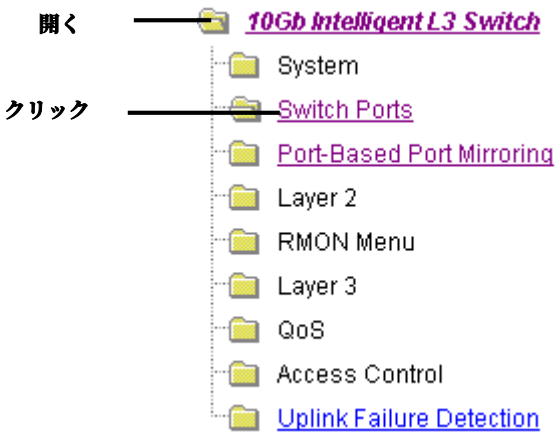
```
>> /cfg/l2/vlan 3
>> VLAN 3# add 2
Current ports for VLAN 3: empty
Pending new ports for VLAN 3: 2

>> VLAN 3# add 4
Port 4 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 2 [y/n]: y
Current ports for VLAN 3: 2
Pending new ports for VLAN 3:

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

>> VLAN 3# add 21                                (Add port 21 to VLAN 3)
Current ports for VLAN 3: 2, 18
Pending new ports for VLAN 3: 21

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

>> VLAN 4# add 20
Port 20 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: 20

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

>> /cfg/port 20/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）。



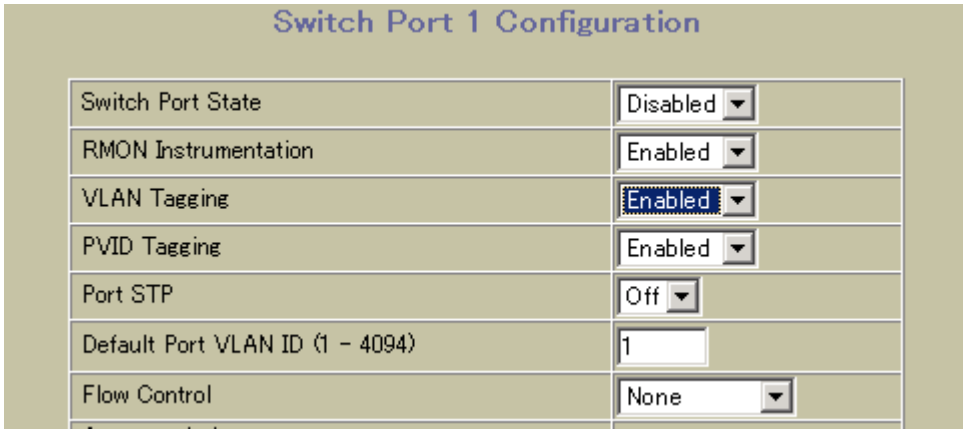
   c. 該当のポート番号をクリックして選択します。

クリック

Switch Ports Configuration

Switch Port	State	VLAN Tagging	Default PVID	PVID tagging	Multicast Threshold	Broadcast Threshold	Destination Lookup Fail Threshold	802.1p Priority
1	disabled	disabled	1	enabled	disabled	disabled	disabled	0
2	disabled	disabled	1	enabled	disabled	disabled	disabled	0
3	disabled	disabled	1	enabled	disabled	disabled	disabled	0
4	disabled	disabled	1	enabled	disabled	disabled	disabled	0
5	disabled	disabled	1	enabled	disabled	disabled	disabled	0
6	disabled	disabled	1	enabled	disabled	disabled	disabled	0
7	disabled	disabled	1	enabled	disabled	disabled	disabled	0
8	disabled	disabled	1	enabled	disabled	disabled	disabled	0
9	enabled	disabled	1	enabled	disabled	disabled	disabled	0
10	disabled	disabled	1	enabled	disabled	disabled	disabled	0
11	disabled	disabled	1	enabled	disabled	disabled	disabled	0
12	disabled	disabled	1	enabled	disabled	disabled	disabled	0
13	disabled	disabled	1	enabled	disabled	disabled	disabled	0
14	disabled	disabled	1	enabled	disabled	disabled	disabled	0
15	disabled	disabled	1	enabled	disabled	disabled	disabled	0
16	disabled	disabled	1	enabled	disabled	disabled	disabled	0
17	enabled	disabled	4095	disabled	disabled	disabled	disabled	0
18	enabled	disabled	1	enabled	disabled	disabled	disabled	0
19	enabled	disabled	1	enabled	disabled	disabled	disabled	0
20	enabled	disabled	1	enabled	disabled	disabled	disabled	0
21	enabled	disabled	1	enabled	disabled	disabled	disabled	0

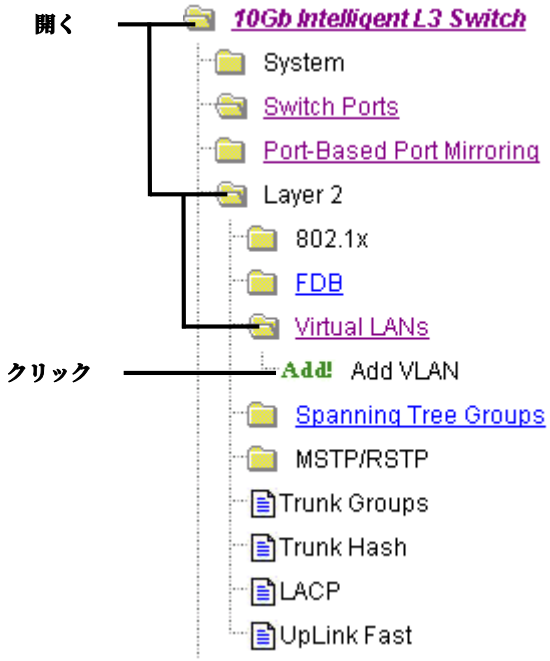
d. ポートと VLAN タグを有効にします。



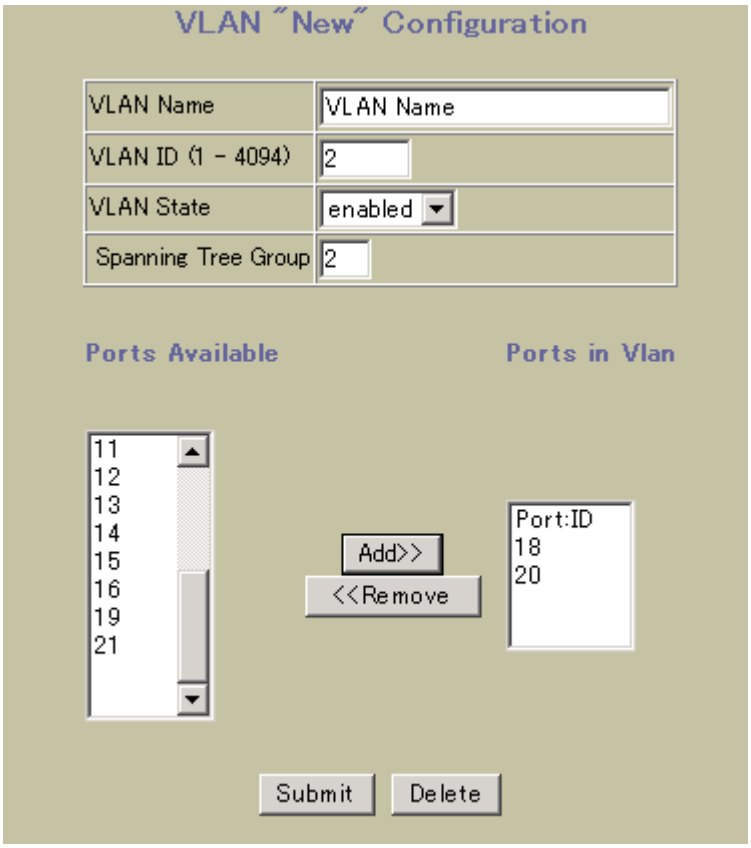
e. Submit をクリックします。

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。



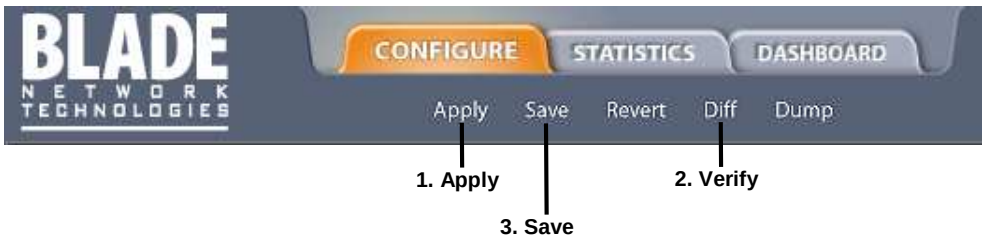
b. VLAN 名、VLAN ID を入力し、VLAN を有効 (enabled) にします。ポートを追加するには、Ports Available リストの各ポートを選択して、Add をクリックします。デフォルトでは、すべてのポートが VLAN 1 に所属しているため、VLAN 2 に属するポートだけ構成します。



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  21           FWD
  00:01:81:2e:b5:60     1  21           FWD
  00:02:a5:e9:76:30     1           1   TRK
  00:03:4b:e2:15:f1     1  21           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 (1-21): 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 2〜128 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 x/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 x/port y/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、すべてのスイッチポートでパスコストは 2 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、

- 10Gbps リンクのパスコストは 2 になります。
- 100Mbps リンクのパスコストは 19 になります。

ポートパスコストの設定は/cfg/l2/stp x/port y/cost コマンドで行います。

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) の構成の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、Port17 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、STG128（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 1～127 が有効で、1～127 の ID 番号を割り当てます。デフォルトでは STG 128 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、Port17 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11 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、次のスパニングツリーの設定をすべてのポートで同じ設定にする必要があります。

- ポートプライオリティ
- パスコスト
- リンクタイプ
- Edge port status
- Port Fast Forward status

トランクグループの各メンバのパスコストを低く設定し、トランクグループがフォワーディング状態になるようにしてください。

複数のスパニングツリー

各スイッチは最大で 128 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。

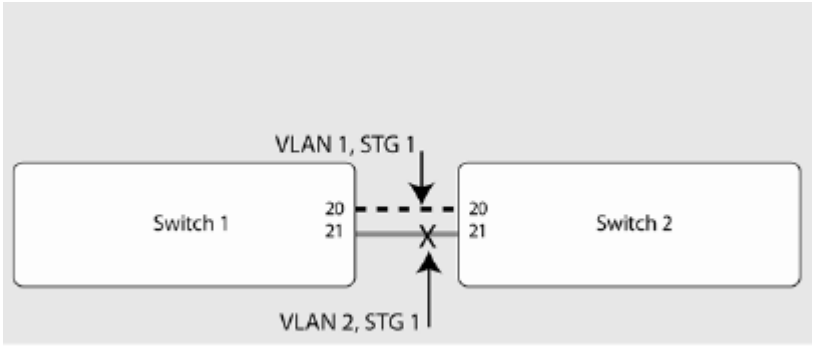
複数の STG を使用する 2 台のスイッチの各々に独立のリンクが可能です。それには、各パスを別々の VLAN で構成し、各 VLAN を別々の STG に割り当てます。各 STG は独立しています。独自の BPDU を送信し、また、個別に構成しなければなりません。

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 128 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、STG2～32 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 20、21 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 21 をブロックし、VLAN 2 でのスイッチ間通信を遮断します。

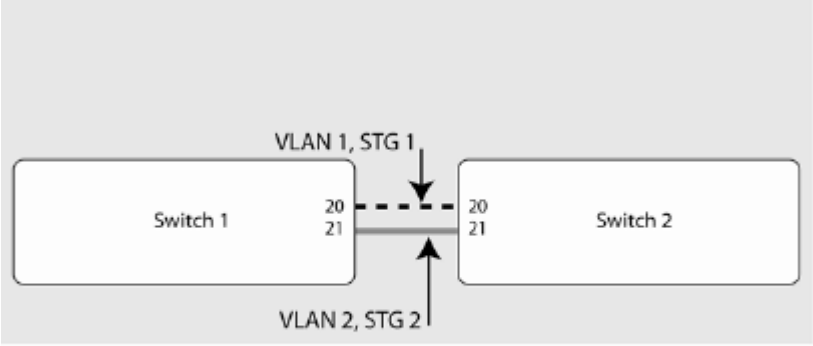
図9　スパニングツリープロトコルの 1 インスタンスに 2 つの VLAN がある場合



VLAN 2 is blocked by STP

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10　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



Spanning Tree Group 1: VLAN 1
Spanning Tree Group 2: VLAN 2

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12 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 ポート 20	スパニングツリーグループ 2 ポート 21
スイッチ 2	スパニングツリーグループ 1 ポート 20	スパニングツリーグループ 2 ポート 21

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 2～127 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 2～128 には 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。

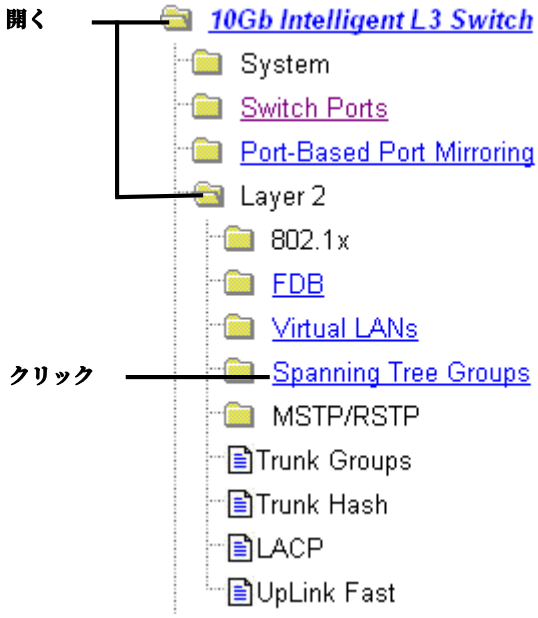
```
>> /cfg/l2/stp 2                          (Select Spanning Tree Group 2)
>> Spanning Tree Group 2# add 2           (Add VLAN 2)
```

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）

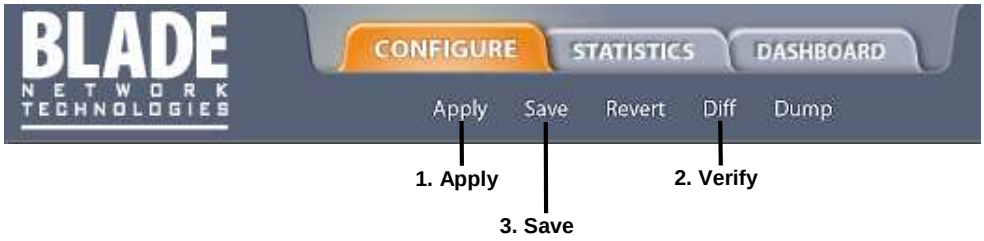
1. 「VLAN」の章の「スイッチ 1 でのポートと VLAN の設定（BBI の例）」で説明したように、スイッチ 1 にポートと VLAN のメンバを設定します。
2. VLAN 2 をスパニングツリーグループ 2 に追加します。
   a. ツールバーの CONFIGURE ボタンをクリックします。
   b. Spanning Tree Groups を選択します。



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 を有効にすると、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 2～128 は RSTP に適用されませんので、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13 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 1～128 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（2～128）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。

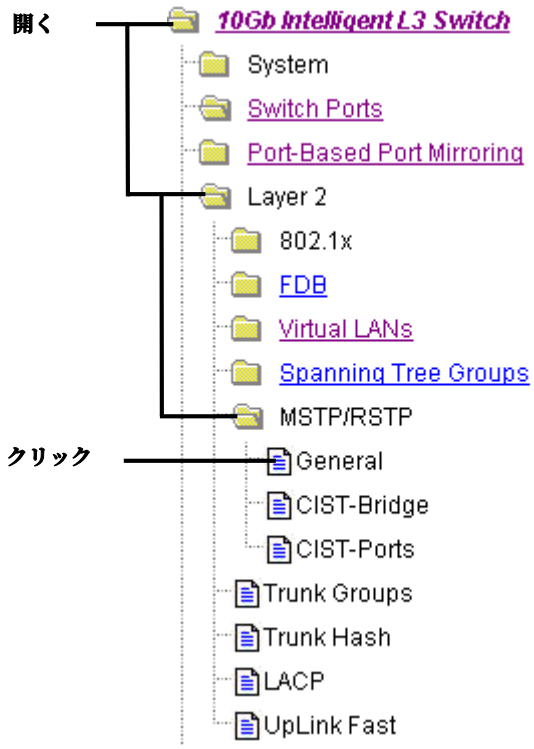
```
>> /cfg/l2/mrst                     (Select Multiple Spanning Tree menu)
>> Multiple Spanning Tree# mode rstp   (Set mode to Rapid Spanning Tree)
>> Multiple Spanning Tree# on              (Turn Rapid Spanning Tree on)
```

3. 設定を適用、保存します。

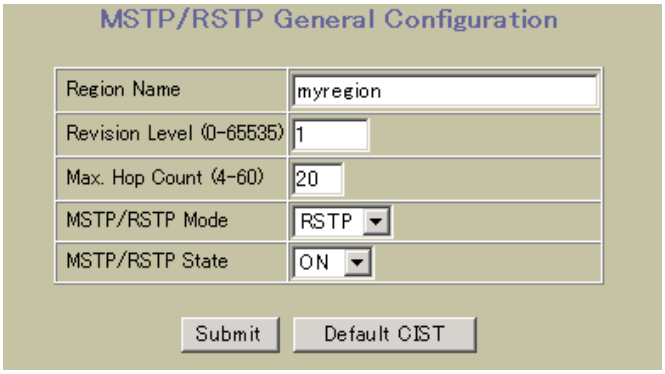
```
>> # apply                (Apply the configuration)
>> # save                 (Save the configuration)
```

RSTP プロトコルの設定（BBI の例）

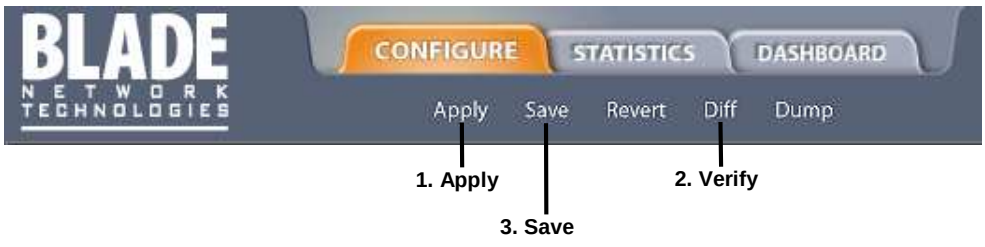
1. 「VLAN」章の「ポートと VLAN の設定（BBI の例）」で説明したように、ポートと VLAN のメンバを設定します。
2. RSTP パラメータを設定します。
   a. ツールバーの CONFIGURE ボタンをクリックします。
   b. MSTP/RSTP フォルダを開き、General を選択します。



   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。

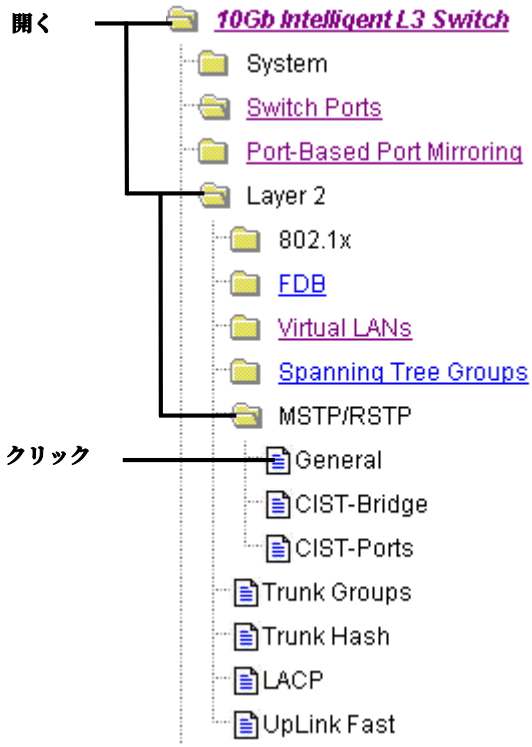
```
>> /cfg/l2/ mrst                        (Select Multiple Spanning Tree menu)
>> Multiple Spanning Tree# mode mstp    (Set mode to
                                         Multiple Spanning Trees)
>> Multiple Spanning Tree# on           (Turn Multiple Spanning Trees on)
>> Multiple Spanning Tree# 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。

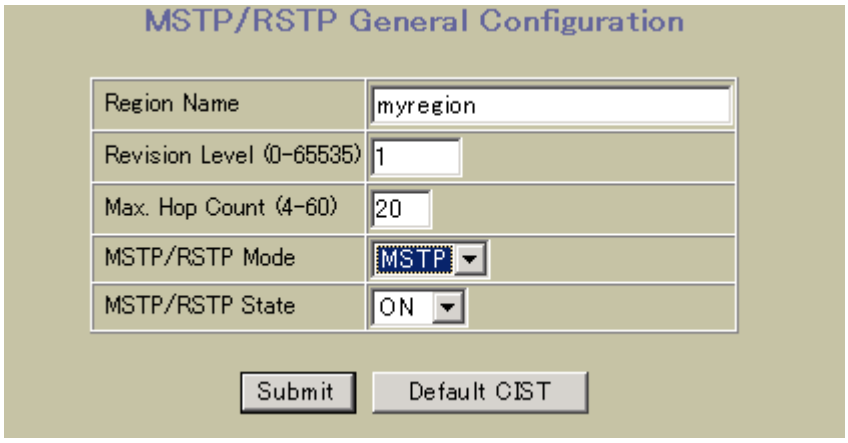
```
>> /cfg/l2/stp 2                        (Select Spanning Tree Group 2)
>> Spanning Tree Group 2# add 2         (Add VLAN 2)
>> Spanning Tree Group 2# apply         (Apply the configurations)
```

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 のメンバを設定します。
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。



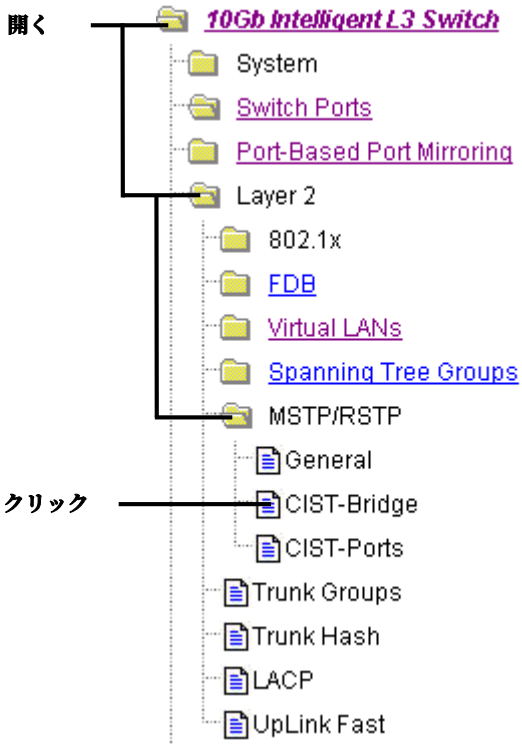
c. リージョン名とリビジョンレベルを入力します。MSTP モードを選択し、MSTP/RSTP State を ON にします。



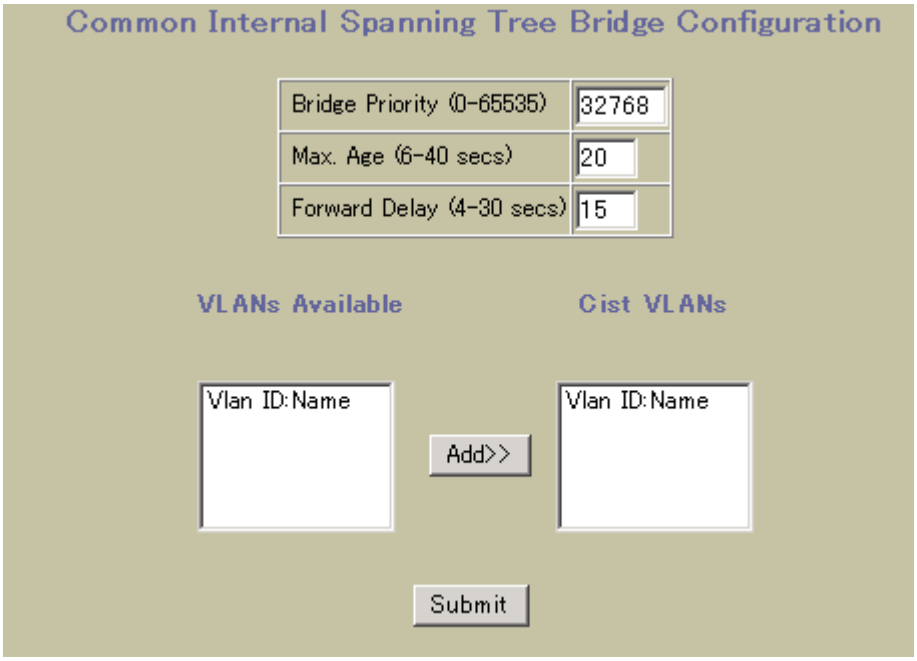
d. Submit をクリックします。

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。



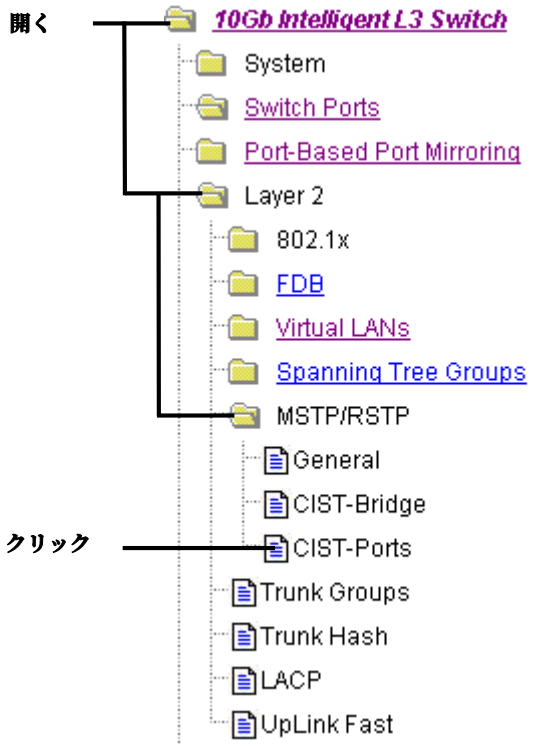
b. Bridge Priority、Max. Age、Forward Delay に値を入力します。



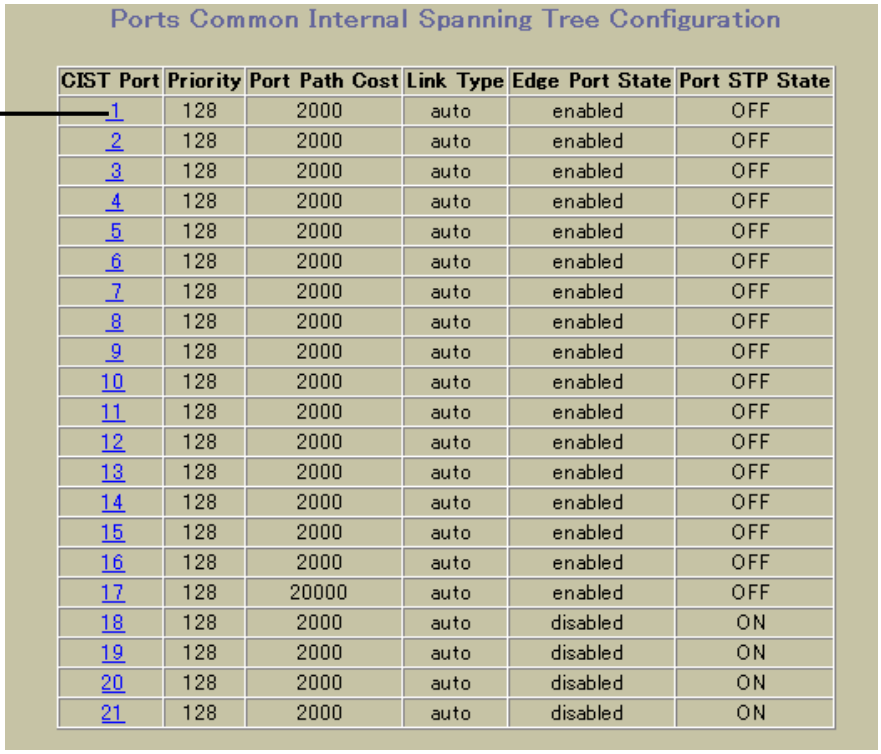
c. をクリックします。

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。

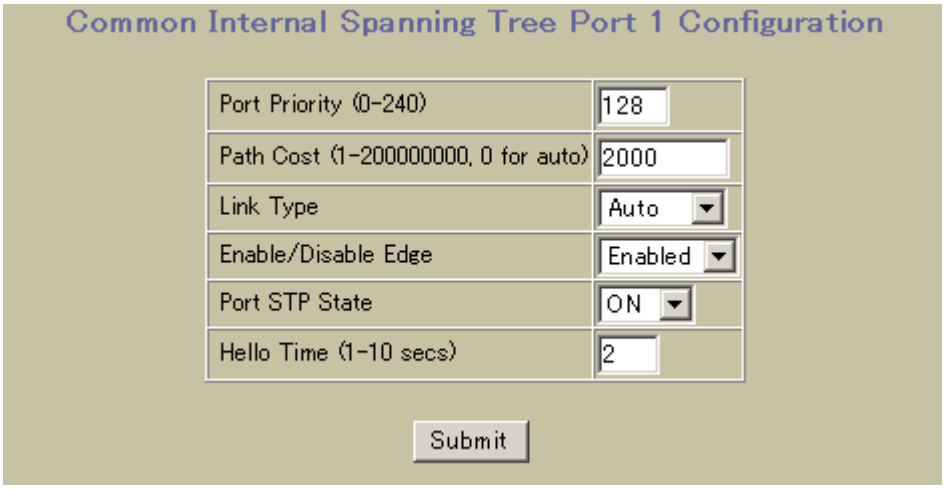


b. 該当のポート番号をクリックして、選択します。



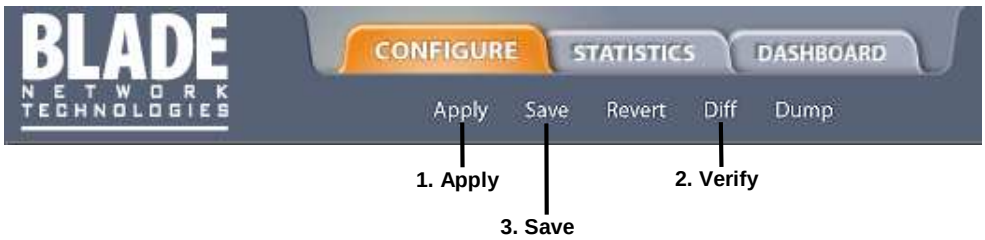
クリック

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、確認、保存します。



Quality of Service

はじめに

QoS 機能を利用すると、遅延やネットワークの輻輳などにあまり影響を受けないアプリケーションを後回しにして、ミッションクリティカルなアプリケーションにネットワークリソースを割り当てることができます。特定のタイプのトラフィックを優先するようにネットワークを設定し、各タイプのトラフィックで適切な Quality of Service (QoS)レベルを受けられます。

本章で説明する項目は以下のとおりです。

- QoS の概要
- ACL フィルタの使用
- DSCP 値を使用
- 802.1p プライオリティの使用
- キューイングとスケジューリング

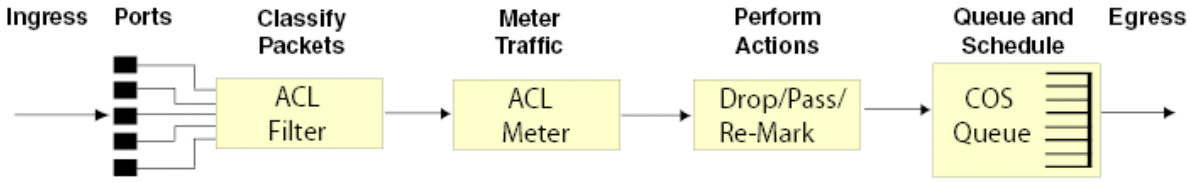
概要

QoS は、重要なアプリケーションに保証された帯域幅を割り当て、重要度の低いアプリケーションには帯域幅を制限することができます。ビデオや音声などのアプリケーションを正常に動作させるには一定量の帯域幅が必要ですが、QoS を利用すると、必要に応じてその帯域幅を確保できます。タイムアウトに影響を受けるアプリケーションや、遅延を許容できないアプリケーションのトラフィックを、プライオリティの高いキューに割り当てることができます。

ネットワークのトラフィックフローに QoS レベルを割り当てることによって、ネットワーク資源を最も必要なところに確実に割り当てることができます。ネットワークトラフィックに優先順位をつけることができるので、選択したアプリケーションの各々に応じたサービスを提供できます。

次の図に本スイッチで使用される基本的な QoS モデルを示します。

図11　QoS モデル



本スイッチは Differentiated Services (DiffServ)アーキテクチャにより QoS 機能を提供します。DiffServ は IETF RFC2474、2475 に説明されています。

DiffServ によりトラフィックを制御するポリシーを確立できます。ポリシーにより、トラフィックの特徴（送信元、宛先、プロトコルなど）を監視し、ある特徴が一致したときにトラフィックに対して制御するアクションを実行します。

本スイッチは、IEEE 802.1p プライオリティ値を読み取るか、特有の条件に一致するフィルタを使用して、トラフィックを分類できます。ネットワークトラフィックの属性がトラフィックパターンに指定した属性と一致すると、通過する各パケットに特定の処理を実行するようにポリシーからスイッチに指示されます。パケットは異なる Class of Service (COS) キューに割り当てられ、送出のスケジュールが立てられます。

基本的なスイッチ QoS モデルは次のように動作します。

- トラフィックの分類
  - 802.1p プライオリティの読み取り
  - ACL フィルタパラメータとの照合
- トラフィックの測定
  - 帯域幅パラメータ、バーストパラメータの指定
  - in-profile、out-of-profile のトラフィックに対して実行するアクションの選択
- アクションの実行
  - パケットの廃棄

- パケットの通過
- DSCP または 802.1p プライオリティのマーキング
- COS キューの設定（リマーキングの有無）

- トラフィックのキューイングとスケジューリング
  - 2 つの COS キューへのパケットの配置
  - COS キューのウェイトに基づく送信のスケジューリング

ACL フィルタの使用

アクセスコントロールリストはトラフィックを分類、セグメント化できるフィルタです。トラフィックタイプに応じて異なるレベルのサービスを提供できます。各フィルタでは、一致させる条件と、条件に一致したときに実行するアクションも定義します。

パケット分類子の概要

本スイッチでは、以下のパラメータに基づいて、パケットを分類できます。

- イーサネット
  - 送信元 MAC アドレス／マスク
  - 宛先 MAC アドレス／マスク
  - VLAN 番号／マスク
  - イーサネットタイプ
  - イーサネットプライオリティ（IEEE 802.1p プライオリティ）
- IPv4
  - 送信元 IP アドレス／マスク
  - 宛先 IP アドレス／マスク
  - ToS 値
  - IP プロトコル番号。次の表に示すプロトコル番号または名前

表14 ウェルノンプロトコルタイプ

番号	プロトコル名
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF
112	VRRP

- TCP/UDP
  - 表 15 で記載されている TCP/UDP アプリケーション送信元ポート
  - 表 15 で記載されている TCP/UDP アプリケーション宛先ポート
  - 表 16 で記載されている TCP/UDP フラグ値

表15 ウェルノンアプリケーションポート

番号	TCP/UDP アプリケーション	番号	TCP/UDP アプリケーション	番号	TCP/UDP アプリケーション
20	ftp-data	79	finger	179	bgp
21	ftp	80	http	194	irc
22	ssh	109	pop2	220	imap3
23	telnet	110	pop3	389	ldap
25	smtp	111	sunrpc	443	https
37	time	119	nntp	520	rip
42	name	123	ntp	554	rtsp
43	whois	143	imap	1645;1812	radius
53	domain	144	news	1813	radius accounting
69	tftp	161	snmp	1985	hsrp
70	gopher	162	snmptrap		

表16 TCP フラグ値

フラグ	値
URG	0x0020
ACK	0x0010
PSH	0x0008
RST	0x0004
SYN	0x0002
FIN	0x0001

- パケットフォーマット
  - イーサネットフォーマット(EthernetⅡ, SNAP, LLC)
  - イーサネットタギングフォーマット
- Egress ポートパケット
  Egress ポート ACL は、ブロードキャスト、マルチキャスト、未知ユニキャスト、レイヤ 3 パケットとは一致しないことに注意してください。また、宛先ポートがトランクメンバの場合も一致しません。

ACL アクションの概要

ACL のアクションでトラフィックの処理方法が決まります。本スイッチの QoS のアクションには次のようなものがあります。

- 通過または廃棄
- 新しい DiffServ Code Point (DSCP)のリマーキング
- 802.1p フィールドのリマーキング
- COS キューの設定

ACL の優先順位について

各 ACL には、番号で決まる特定の優先レベルがあります。受信したパケットが優先順位の最も高い ACL に一致した場合、その ACL に設定されているアクションが実行されます。優先順位を考慮して ACL の割り当てを考慮します。

ACL は、次の表に示すように優先グループで分類されます。

優先グループ	ACL	優先レベル
優先グループ 1	ACL 1 ～ ACL 128	低
優先グループ 2	ACL 129 ～ ACL 256	
優先グループ 3	ACL 257 ～ ACL 384	高

注:優先グループと ACL グループとは何の関連もありません。

各優先グループには独自の優先レベルがあります。たとえば、優先グループ 2 はグループ 1 より優先レベルが上です。各優先グループ内では、番号が大きい ACL の方が優先度が高く、番号が最小の ACL が優先レベル最低、最大の ACL が最高になります。

ACL グループの使用

アクセスコントロールリスト(ACL)に基づき、送信元アドレス、宛先アドレス、送信元ポート番号、宛先ポート番号など、パケットヘッダの内容にしたがってパケットを分類できます。

多数の ACL を ACL グループにまとめ、その ACL グループをポートに割り当てることができます。

ACL グループはポート単位で割り当てて有効にします。各 ACL は単独か、他の ACL や ACL グループと組み合わせて使用できます。

ACL のグループ化には以下の方法があります。

- アクセスコントロールリスト

本スイッチは ACL を 384 までサポートします。各 ACL で 1 つのフィルタルールを指定します。各フィルタルールは 1 つの処理（パケットの許可または拒否）を含めることができます。

```
ACL 200:
VLAN = 1
SIP = 10.10.10.1 (255.255.255.0)
Action = permit
```

- **アクセスコントロールグループ**

  アクセスコントロールグループ（ACL グループ）は ACL の集合です。次に例を示します。

```
                              ACL Group 1
ACL 382:
VLAN = 1
SIP = 10.10.10.1 (255.255.255.0)
Action = permit

ACL 383:
VLAN = 2
SIP = 10.10.10.2 (255.255.255.0)
Action = deny

ACL 384:
PRI = 7
DIP = 10.10.10.3 (255.255.0.0)
Action = permit
```

上記の例では、各 ACL でフィルタルールを決めています。番号から、ACL 383 の方が ACL 382 より優先度が高くなります。

ACL グループを使用してトラフィックプロファイルを生成します。つまり、ACL を 1 つの ACL グループにまとめ、その ACL グループを 1 ポートに割り当てます。本スイッチは ACL グループを 384 までサポートします。

ACL のメータリングとリマーキング

（必要に応じて）QoS メータを設定し、ACL グループをポートに割り当てて、本スイッチを通過するトラフィックのプロファイルを設定します。ACL グループをポートに追加する場合、優先度を考慮して正しい順番になるように確認してください。

ACL によって実行されるアクションを In-Profile アクションといいます。1 つのポートに In-Profile アクションと Out-of-Profile アクションを設定できます。データトラフィックを計測し、各種のネットワークトラフィックの帯域幅に対して一定のサービルレベルを提供するようにリマーキングできます。

メータリング

QoS メータリングでは、ユーザが設定できるパラメータによって、データストリームに対して種々のレベルのサービスを提供します。作成したトラフィックプロファイルに対してトラフィックストリームを測定するために、メータを使用します。したがって、メータを生成すると、次のように、各 ACL に In-Profile トラフィックと Out-of-Profile トラフィックができます。

In-Profile：メータが設定されていない場合、またはパケットがメータの範囲内にある場合、そのパケットは In-Profile として分類されます。

Out-of-Profile：メータが設定されており、パケットがメータの範囲内に入らない（メータのコミットレートもしくは最大バーストレートを越えている）場合、Out-of-Profile として分類されます。

メータを使用する場合、コミットレートを Kb/s 単位で設定します（1Kb/s は 1024 ビット／秒）。このコミットレート内のトラフィックはすべて In-Profile です。また、短時間であれば許容される、コミットレートより大きい値の最大バーストサイズを設定できます。以上のパラメータで In-Profile を設定します。

メータは、特定のパラメータ内にソートしたパケットを保持します。ACL でメータを設定し、メータで計測したトラフィックに対し、リマーキングなどのアクションを実行できます。

リマーキング

リマーキングは、新しいネットワーク仕様や必要なサービスレベルに基づいて、パケットの処理をリセットできます。
ACL の設定により、パケットを次のようにリマークできます。

- パケットの DSCP 値を変更する。トラフィックが受けられるサービスレベルの指定に使用します。
- パケットの 802.1p プライオリティを変更する。

ACL 統計情報の表示

ACL 統計情報で、各 ACL にヒット（一致）したパケット数を表示します。各 ACL 優先グループに対して最大 64 の統計カウンタを表示できます。ACL 統計情報を使用して、フィルタのパフォーマンスを確認したり、ACL フィルタをデバッグします。

監視する各 ACL の統計情報(cfg/acl/acl x/stats ena)を有効にする必要があります。

ACL 設定例

アクセスコントロールリストの設定（AOS CLI の例）

以下の設定例で、アクセスコントロールリスト(ACL)を使用してトラフィックをブロックする方法を示します。これらの基本的な設定で、ACL フィルタリングの基本を示します。

> **注**：各 ACL は、その ACL が設定されたポートに入ってくるトラフィックをフィルタリングします。egrport で指定した ACL は、その ACL が設定されたポートで受信し、egrport で指定したポートから送信されるトラフィックをフィルタリングします。ほとんどの設定では egrport は使用しません。

例 1：特定のホストへのトラフィックをブロックする例です。

```
>> Main# /cfg/acl/acl 255                       (Define ACL 255)
>> ACL 255# ipv4/dip 100.10.1.116 255.255.255.255
>> Filtering IPv4# ..
>> ACL 255# action deny
>> ACL 255# /cfg/port 20/aclqos                 (Add ACL to port 20)
>> Port 20 ACL# add acl 255
>> Port 20 ACL# apply
>> Port 20 ACL# save
```

この例では、ポート 20 から入る、宛先 IP アドレスが 100.10.1.116 のトラフィックはすべて拒否します。

例 2：あるネットワークから特定のホストへのトラフィックをブロックする例です。

```
>> Main# /cfg/acl/acl 256                       (Define ACL 256)
>> ACL 256# ipv4/sip 100.10.1.0 255.255.255.0
>> ACL 256# ipv4/dip 200.20.1.116 255.255.255.255
>> Filtering IPv4# ..
>> ACL 256# action deny
>> ACL 256# /cfg/port 20/aclqos                 (Add ACL to port 20)
>> Port 20 ACL# add acl 256
>> Port 20 ACL# apply
>> Port 20 ACL# save
```

この例では、ポート 20 に入る、送信元 IP アドレスが 100.10.1.0/24 で、宛先 IP アドレスが 200.20.1.116 のトラフィックをすべて拒否します。

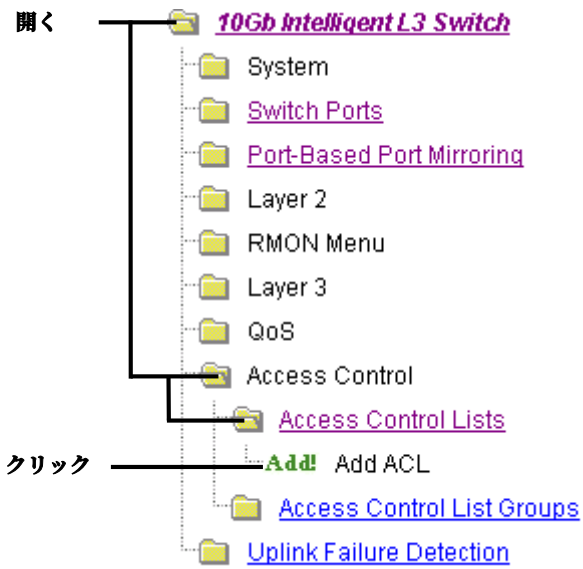
例 3：ある送信元からのトラフィックと、特定のポートへ転送されるトラフィックをブロックする例です。

```
>> Main# /cfg/acl/acl 1                          (Define ACL 1)
>> ACL 1# ethernet/smac 00:21:00:00:00:00 ff:ff:ff:ff:ff:ff
>> Filtering Ethernet# ..
>> ACL 1# action deny
>> ACL 1# stats e
>> ACL 1# /cfg/acl/acl 257                       (Define ACL 257)
>> ACL 257# egrport 21
>> ACL 257# action deny
>> ACL 257# stats e
>> ACL 257# /cfg/port 20/aclqos
>> Port 20 ACL# add acl 1                        (Add ACL 1 to port 20)
>> Port 20 ACL# add acl 257                      (Add ACL 257 to port 20)
>> Port 20 ACL# apply
>> Port 20 ACL# save
```

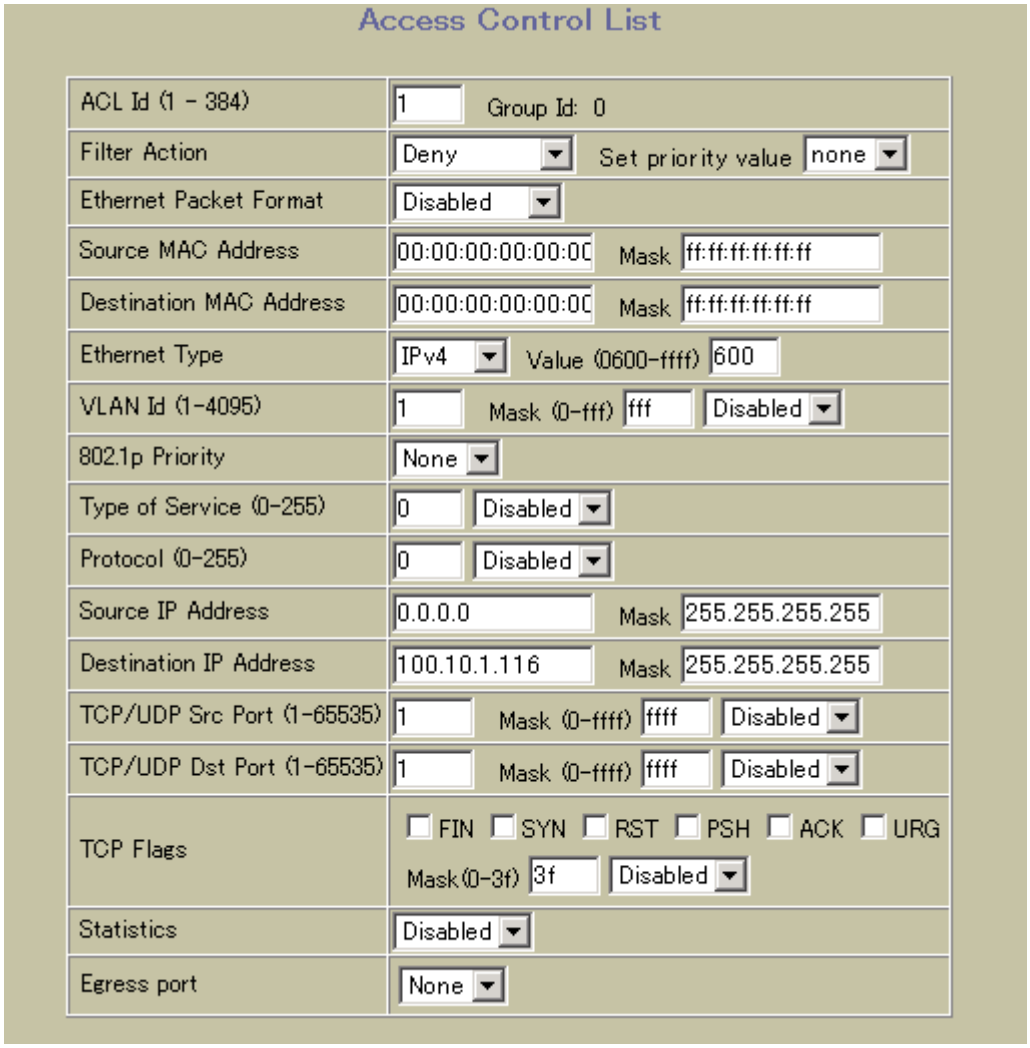
この例では、送信元 MAC アドレスが 00:21:00:00:00:00 で Port23 に入るトラフィックと、Port23 から Port24 に向けられたトラフィックはすべて拒否します。

アクセスコントロールリストの例（BBI の例）

1. アクセスコントロールリストを設定します。
   a. ツールバーの CONFIGURE ボタンをクリックします。
   b. Access Control Lists フォルダを開き、Add ACL を選択します。

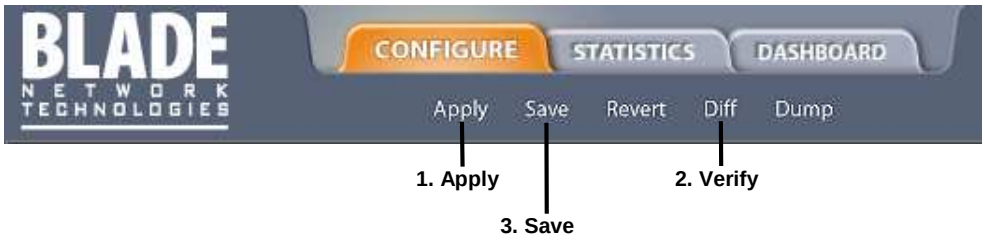


c. ACL パラメータを設定します。Filter Action に Deny を、Ethernet Type に IPv4 を、Destination IP Address に 100.10.1.116 を設定します。

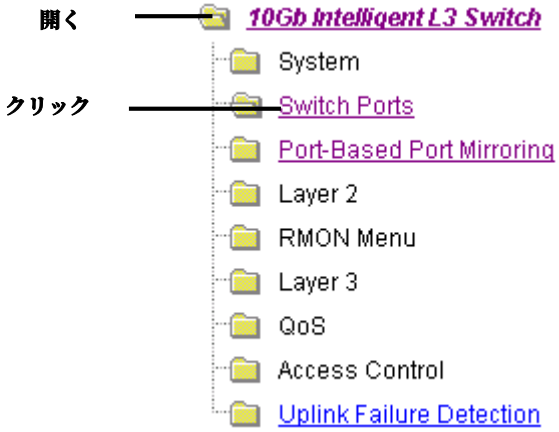


d. Submit をクリックします。

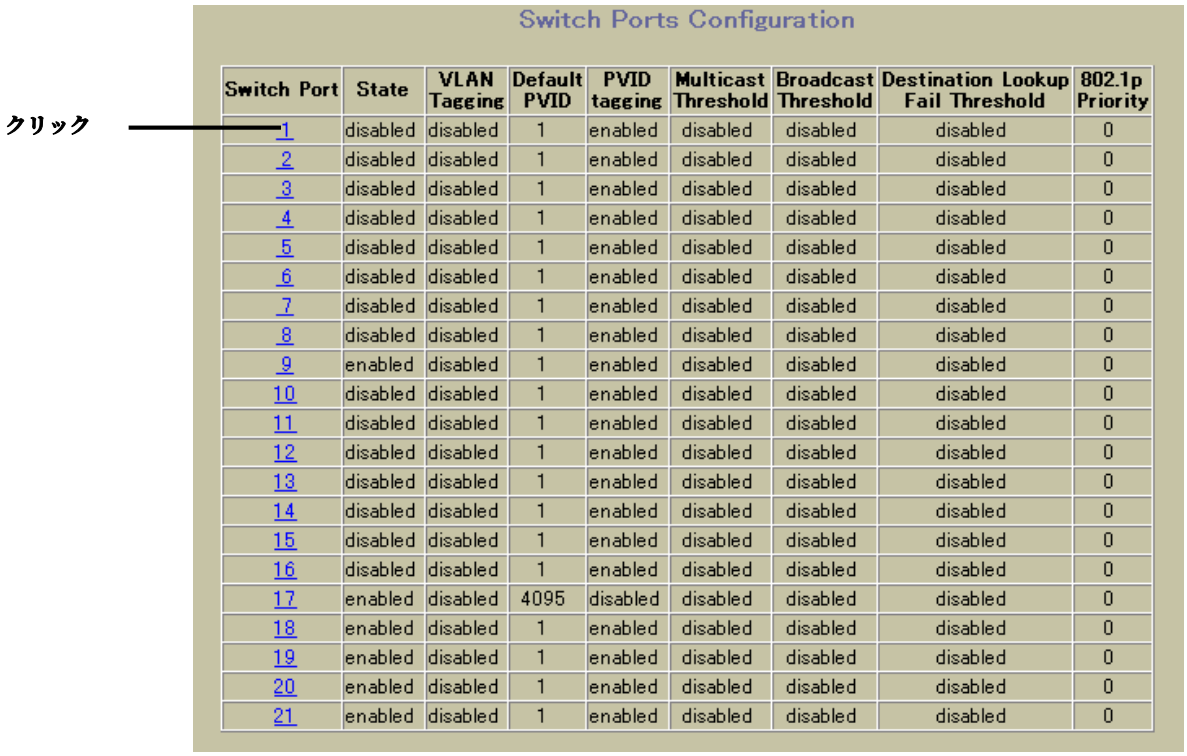
2. 設定を適用、確認、保存します。



3. ポート 1 に ACL 1 を追加します。
   a. ツールバーの CONFIGURE ボタンをクリックします。
   b. 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）。



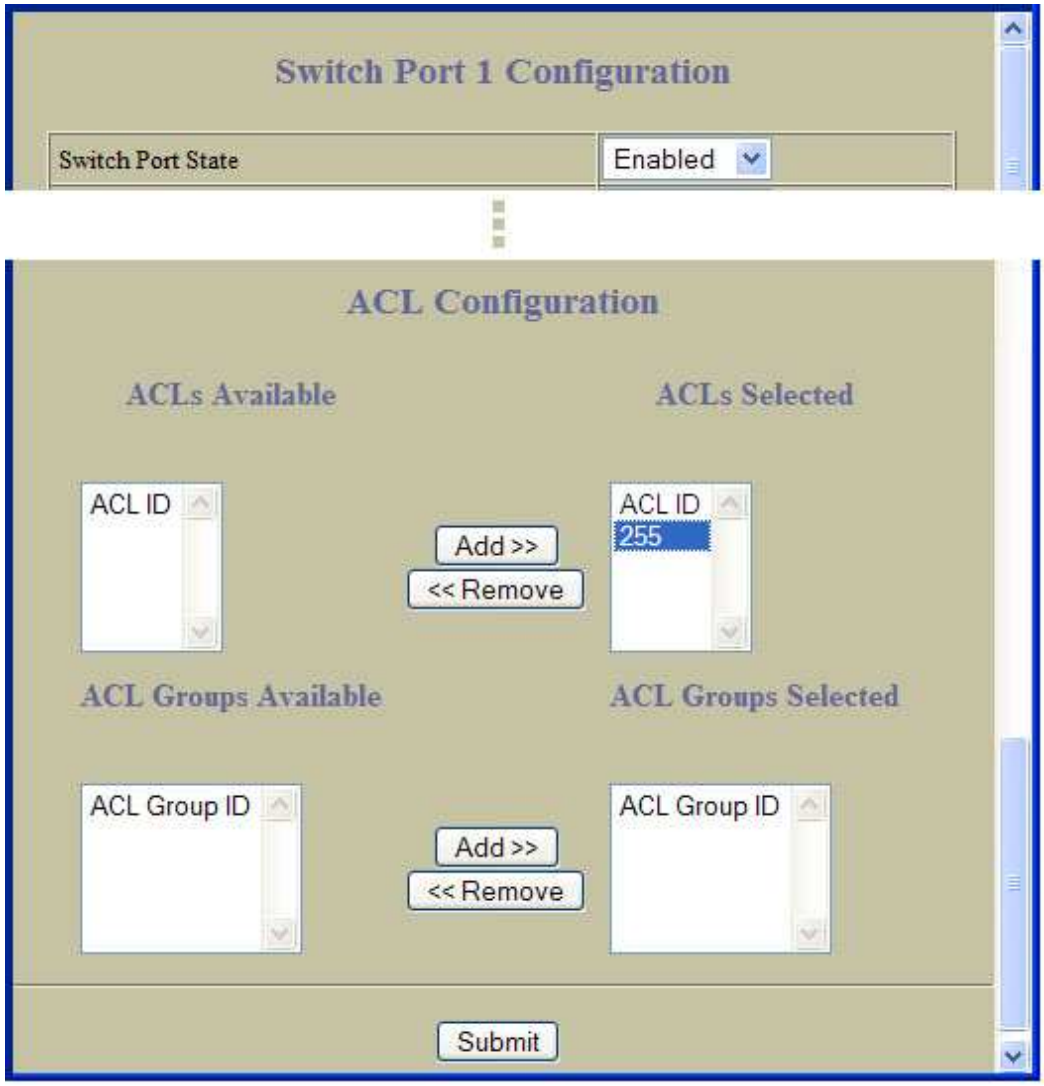
   c. ポートを選択します。



Switch Ports Configuration

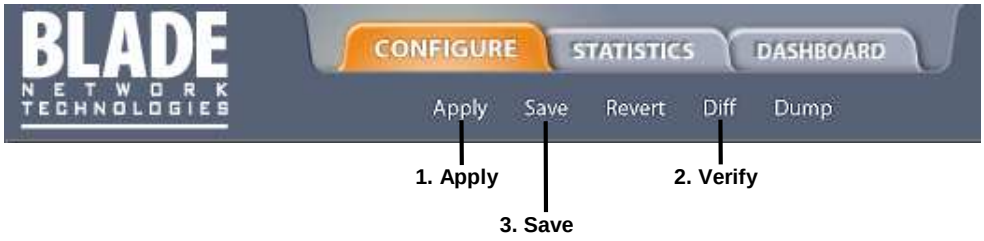
Switch Port	State	VLAN Tagging	Default PVID	PVID tagging	Multicast Threshold	Broadcast Threshold	Destination Lookup Fail Threshold	802.1p Priority
1	disabled	disabled	1	enabled	disabled	disabled	disabled	0
2	disabled	disabled	1	enabled	disabled	disabled	disabled	0
3	disabled	disabled	1	enabled	disabled	disabled	disabled	0
4	disabled	disabled	1	enabled	disabled	disabled	disabled	0
5	disabled	disabled	1	enabled	disabled	disabled	disabled	0
6	disabled	disabled	1	enabled	disabled	disabled	disabled	0
7	disabled	disabled	1	enabled	disabled	disabled	disabled	0
8	disabled	disabled	1	enabled	disabled	disabled	disabled	0
9	enabled	disabled	1	enabled	disabled	disabled	disabled	0
10	disabled	disabled	1	enabled	disabled	disabled	disabled	0
11	disabled	disabled	1	enabled	disabled	disabled	disabled	0
12	disabled	disabled	1	enabled	disabled	disabled	disabled	0
13	disabled	disabled	1	enabled	disabled	disabled	disabled	0
14	disabled	disabled	1	enabled	disabled	disabled	disabled	0
15	disabled	disabled	1	enabled	disabled	disabled	disabled	0
16	disabled	disabled	1	enabled	disabled	disabled	disabled	0
17	enabled	disabled	4095	disabled	disabled	disabled	disabled	0
18	enabled	disabled	1	enabled	disabled	disabled	disabled	0
19	enabled	disabled	1	enabled	disabled	disabled	disabled	0
20	enabled	disabled	1	enabled	disabled	disabled	disabled	0
21	enabled	disabled	1	enabled	disabled	disabled	disabled	0

d. ポートに ACL を追加します。



e. Submit をクリックします。

4. 設定を適用、確認、保存します。



DSCP 値の使用

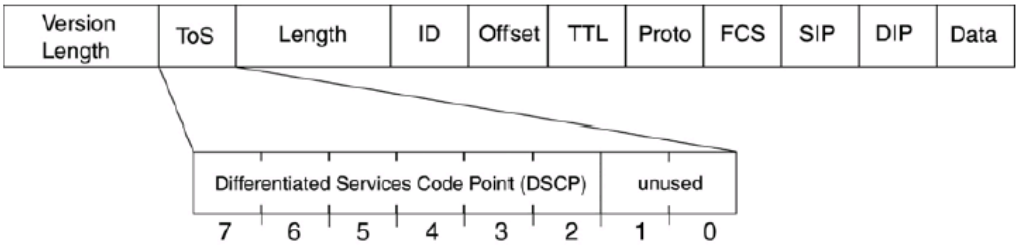
IP ヘッダの TOS バイトの上位 6 ビットを DiffServ Code Point (DSCP)として定義されます。ネットワークデバイスで受ける必要のある処理のタイプに応じて、パケットにマークを付けます。DSCP は、パケットの QoS レベルを示します。

Differentiated Services の概念

トラフィックフローを差別化するために、パケットを DSCP 値によって分類できます。IP ヘッダの Differentiated Services(DS) フィールドは 1 オクテットで、DS Code Point(DSCP)と呼ぶ上位の 6 ビットにより QoS 機能を提供できます。

各パケットは DSCP 内に QoS 状態を示します。可能な DSCP 値は 64 あります(0～63)。

図12　レイヤ 3 IPv4 パケット



本スイッチは DSCP に対して以下の処理を実行できます。

- DSCP 値の新しい値へのリマーキング
- DSCP 値の 802.1p プライオリティへのマッピング

Per Hop Behavior

DSCP 値で各パケットの Per Hop Behavior(PHB)が決まります。PHB は、各ホップのパケットに対する転送処理です。パケットがネットワークを移動するときに、DSCP 値に基づいて一連のルールを適用することによって、QoS のポリシーが構築されます。本スイッチのデフォルト設定は、IEEE 標準規格に定義されている通り、以下の標準 PHB に基づいています。

- Expedited Forwarding(EF)：Egress の優先度が最高で、廃棄の優先度は最低です。EF トラフィックは他のトラフィックよりも先に転送されます。EF PHB については RFC 2598 に説明されています。
- Assured Forwarding(AF)：以下に示すように廃棄の優先度が異なる 4 つのサービスレベルがあります。ルータは、ネットワークが輻輳したときに、優先度を使用してどのパケットを廃棄するかを決めます。AF PHB については RFC 2597 に説明されています。

表17　優先度

優先度	クラス 1	クラス 2	クラス 3	クラス 4
低	AF11 (DSCP 10)	AF21 (DSCP 18)	AF31 (DSCP 26)	AF41 (DSCP 34)
中	AF12 (DSCP 12)	AF22 (DSCP 20)	AF32 (DSCP 28)	AF42 (DSCP 36)
高	AF13 (DSCP 14)	AF23 (DSCP 22)	AF33 (DSCP 30)	AF43 (DSCP 38)

- Class Selector(CS)：以下に示すように、この PHB には 8 つのプライオリティクラスがあります（CS7 が最高のプライオリティ、CS0 が最低のプライオリティです）。CS PHB については RFC 2474 に規定されています。

表18　Class Selector のプライオリティクラス

プライオリティ	クラスセレクタ	DSCP
最高	CS7	56
	CS6	48
	CS5	40
	CS4	32
	CS3	24
	CS2	16

	CS1	8
最低	CS0	0

QoS レベル

次の表に、本スイッチのデフォルトサービスレベルを重要度の高い順に示します。

表19 デフォルト QoS サービルレベル

サービスレベル	デフォルト PHB	802.1P プライオリティ
Critical	CS7	7
Network Control	CS6	6
Premium	EF, CS5	5
Platinum	AF41, AF42, AF43, CS4	4
Gold	AF31, AF32, AF33, CS3	3
Silver	AF21, AF22, AF23, CS2	2
Bronze	AF11, AF12, AF13, CS1	1

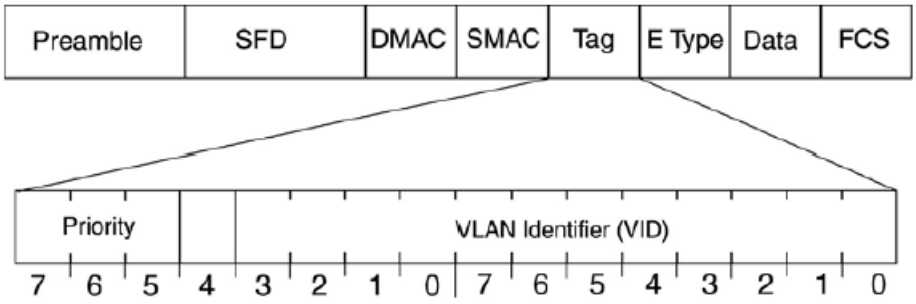
802.1p プライオリティの使用

本スイッチは、パケットの VLAN ヘッダの中にあるプライオリティビットに基づいて QoS 機能を提供します（プライオリティビットは、802.1p 標準規格により、IEEE 802.1q VLAN ヘッダ内に定義されています）。802.1p ビットがパケットの中にある場合、転送時にパケットに与えられるプライオリティを指定します。プライオリティ値（ゼロ以外）が大きいパケットの方が、小さいパケットより優先して送信されます。

Class of Service (COS)、COS キュー(COSq)のウェイトが高くマッピングされたパケットは、COS、COSq のウェイトが低いパケットより、高い転送優先度が与えられます。スケジューリング方式は重み付けラウンドロビン(WRR)で、1 つの COSq に対して 1～15 の重みを設定できます。本スイッチは、出力 COS キュー(COSq)を 2 つもしくは 8 つに設定できます。

IEEE 802.1p では 8 レベルのプライオリティ(0～7)を使用します。プライオリティ 7 は、OSPF や RIP のルーティングテーブルのアップデートなどのプライオリティが最高のネットワークトラフィックに、プライオリティ 5、6 は、音声、ビデオなど、遅延に影響を受けるアプリケーションに、その他の低いプライオリティは標準的なアプリケーションに割り当てます。値 0 は、ベストエフォート型を示し、ネットワークでプライオリティが設定されていない場合のデフォルト値です。本スイッチは 802.1p 値に基づいてパケットをフィルタリングし、802.1p 値をパケットに割り当てたり、上書きができます。

図13 レイヤ 2 802.1q / 802.1p VLAN タグ付きパケット



Ingress パケットはプライオリティ値を次のように受け取ります。

- タグ付きパケット：VLAN タグ内の 802.1p プライオリティを読み取ります。
- タグなしパケット：受信したポートのデフォルトプライオリティ(/cfg/port x/8021ppri)に基づいて、パケットにタグを付け、802.1p プライオリティを割り当てます。

Egress パケットの場合、プライオリティ値に基づいて COS キューに入れられ、COS キューのスケジューリングのウェイトに基づいて、送信のスケジュールがされます。

/cfg/qos/8021p/cur コマンドを使用して、802.1p 値、COSq、COSq スケジューリングウェイトのマッピングを表示できます。

```
>> 802.1p# cur
Current priority to COS queue configuration:
Number of COSq: 2
Priority COSq Weight
-------- ---- ------
   0    0    1
   1    0    1
   2    0    1
   3    0    1
   4    1    2
   5    1    2
   6    1    2
   7    1    2
```

802.1p の設定（AOS CLI の例）

1. ポートのデフォルト 802.1 プライオリティを設定します。

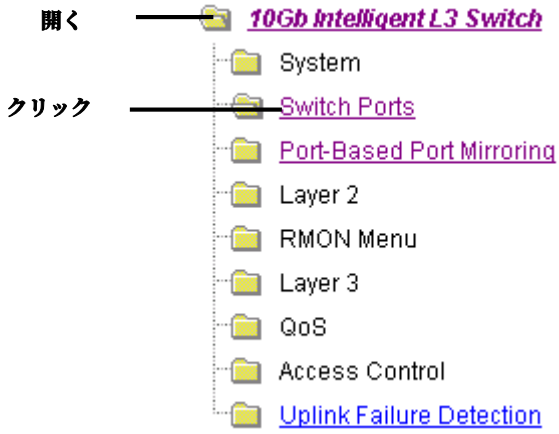
```
>> Main# cfg/port 20              (Select port)
>> Port 20# 8021ppri              (Set port's default 802.1p priority)
Current 802.1p priority: 0
Enter new 802.1p priority [0-7]: 1
>> Port 20# apply
```

2. 802.1p プライオリティ値を COS キューにマップし、COS キュースケジューリングのウェイトを設定します。

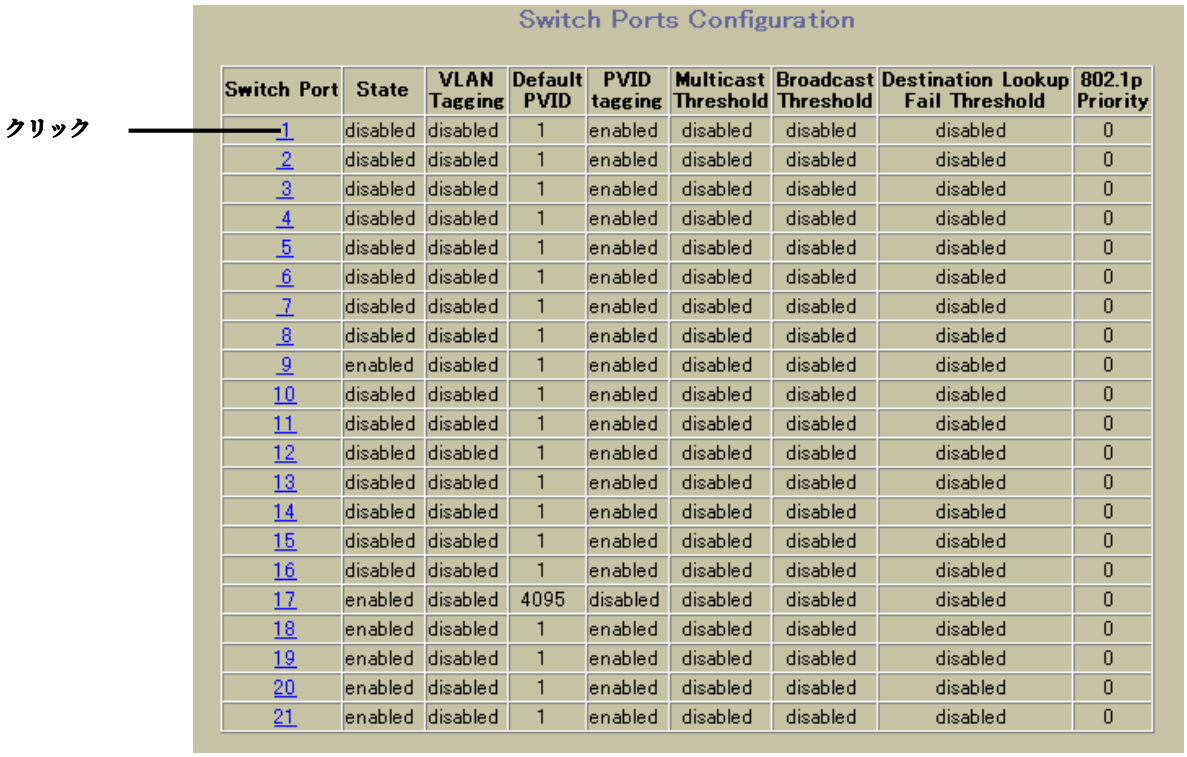
```
>> Main# cfg/qos/8021p                    (Select 802.1p menu)
>> 802.1p# priq                           (Set COS queue assignments)
Enter priority [0-7]: 1
Current COS queue (for priority 1): 0
Enter new COS queue (for priority 1) [0-1]: 1
>> 802.1p# qweight                        (Set COS queue weights)
Enter COS queue [0-1]: 1
Current weight (for COS queue 1): 0
Enter new weight (for COS queue 1) [0-15]: 1
>> 802.1p# apply
```

802.1p の設定（BBI の例）

1. ポート 1 に ACL 1 を追加します。
   a. ツールバーの CONFIGURE ボタンをクリックします。
   b. 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. ポートを選択します。



Switch Port	State	VLAN Tagging	Default PVID	PVID tagging	Multicast Threshold	Broadcast Threshold	Destination Lookup Fail Threshold	802.1p Priority
1	disabled	disabled	1	enabled	disabled	disabled	disabled	0
2	disabled	disabled	1	enabled	disabled	disabled	disabled	0
3	disabled	disabled	1	enabled	disabled	disabled	disabled	0
4	disabled	disabled	1	enabled	disabled	disabled	disabled	0
5	disabled	disabled	1	enabled	disabled	disabled	disabled	0
6	disabled	disabled	1	enabled	disabled	disabled	disabled	0
7	disabled	disabled	1	enabled	disabled	disabled	disabled	0
8	disabled	disabled	1	enabled	disabled	disabled	disabled	0
9	enabled	disabled	1	enabled	disabled	disabled	disabled	0
10	disabled	disabled	1	enabled	disabled	disabled	disabled	0
11	disabled	disabled	1	enabled	disabled	disabled	disabled	0
12	disabled	disabled	1	enabled	disabled	disabled	disabled	0
13	disabled	disabled	1	enabled	disabled	disabled	disabled	0
14	disabled	disabled	1	enabled	disabled	disabled	disabled	0
15	disabled	disabled	1	enabled	disabled	disabled	disabled	0
16	disabled	disabled	1	enabled	disabled	disabled	disabled	0
17	enabled	disabled	4095	disabled	disabled	disabled	disabled	0
18	enabled	disabled	1	enabled	disabled	disabled	disabled	0
19	enabled	disabled	1	enabled	disabled	disabled	disabled	0
20	enabled	disabled	1	enabled	disabled	disabled	disabled	0
21	enabled	disabled	1	enabled	disabled	disabled	disabled	0

d. 802.1p プライオリティ値を設定します。

Switch Port 1 Configuration

Switch Port State	Disabled
RMON Instrumentation	Enabled
VLAN Tagging	Disabled
PVID Tagging	Enabled
Port STP	Off
Default Port VLAN ID (1 - 4094)	1
Flow Control	None
Autonegotiation	Off
Speed	10000
Duplex Mode	Full
Enable/Disable sending Link UP/Down Trap	Enabled
Port Name	Downlink1
Multicast Threshold	Disabled
Multicast Threshold Rate (0-262143)	0
Broadcast Threshold	Disabled
Broadcast Threshold Rate (0-262143)	0
Destination Lookup Fail Threshold	Disabled
Destination Lookup Fail Threshold Rate (0-262143)	0
802.1p Port Priority (0-7)	1

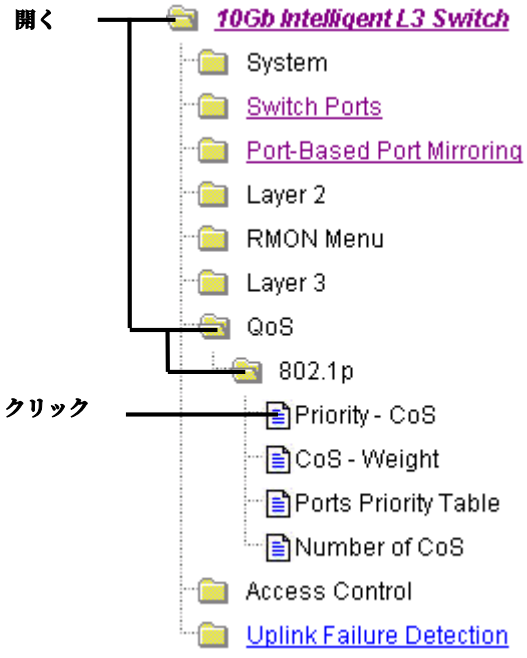
e. Submit をクリックします。

2. 802.1p プライオリティを COS キューにマッピングします。

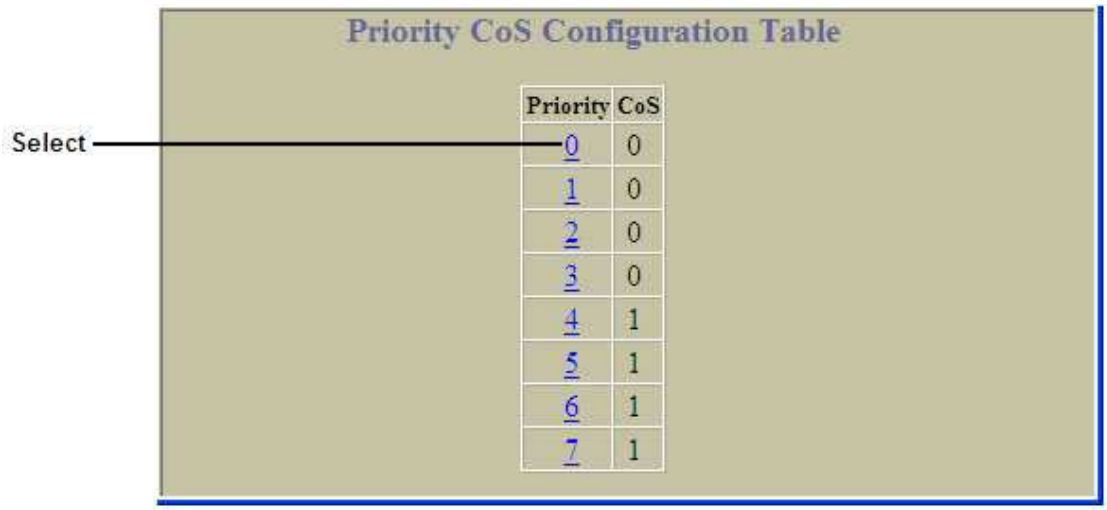
a. ツールバーの CONFIGURE ボタンをクリックします。

b. 802.1p フォルダを開き、Priority-CoS を選択します。

c.



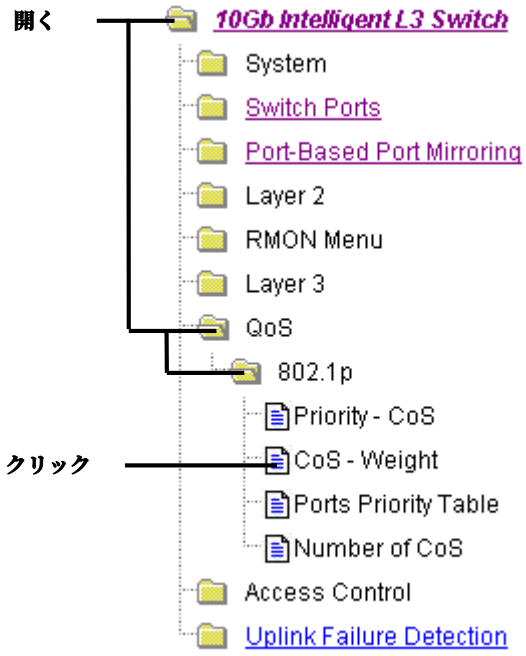
802.1p プライオリティ値を選択します。



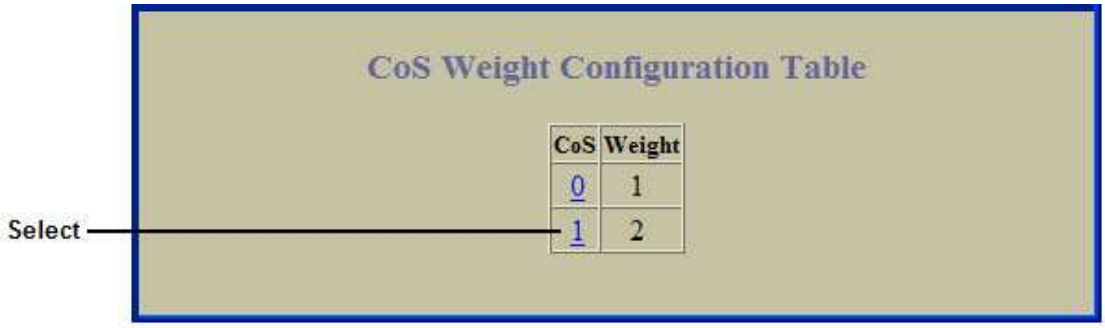
d. 802.1p プライオリティ値に対応づける COS キューを選択します。

e. Submit をクリックします。

3. COS キューのスケジューリングのウェイトを設定します。
   a. ツールバーの CONFIGURE ボタンをクリックします。
   b. 802.1p フォルダを開き、CoS-Weight を選択します。



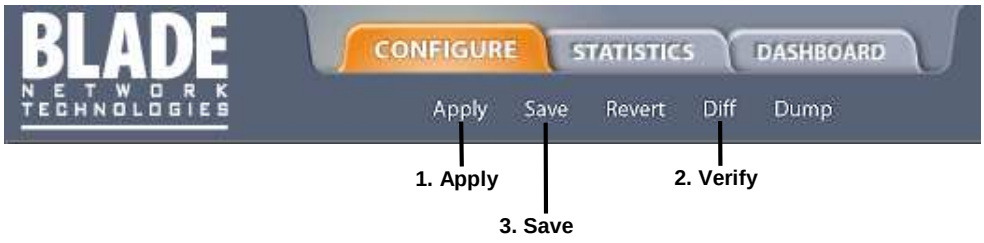
c. COS キューを選択します。



d. COS キューのウェイトの値を入力します。

e. Submit をクリックします。

4. 設定を適用、確認、保存します。



キューイングとスケジューリング

本スイッチは、出力 COS キュー(COSq) を 2 つもしくは 8 つに設定でき、そこに各パケットを配置します。ACL のアクションでパケットの COSq を設定する場合を除き、各パケットの 802.1p プライオリティで COSq が決まります。

COS キューには以下のアトリビュートを設定できます。

- COS キューへの 802.1p プライオリティ値のマッピング
- 各 COS キューにスケジューリングするウェイトの設定

802.1p メニュー(/cfg/qos/8021p)を使用して COS キューを設定します。

基本 IP ルーティング

本章では、本スイッチを使用して IP ルーティング機能を実行する例を示します。本章では以下の節からなります。

- IP ルーティングの特長
- IP サブネット間のルーティング
- サブネットルーティングの例

IP ルーティングの特長

本スイッチは、設定可能な IP スイッチインタフェースと IP ルーティングオプションを組み合わせて使用します。スイッチの IP ルーティング機能には以下の特長があります。

- ジャンボフレームをサポートしていない VLAN またはサブネットにルーティングする場合、UDP ジャンボフレームを自動でフラグメント化することにより、ジャンボフレームテクノロジを意識せずに導入する手段を提供します。
- スイッチに設定した複数の VLAN 間で IP トラフィックをルーティングできます。

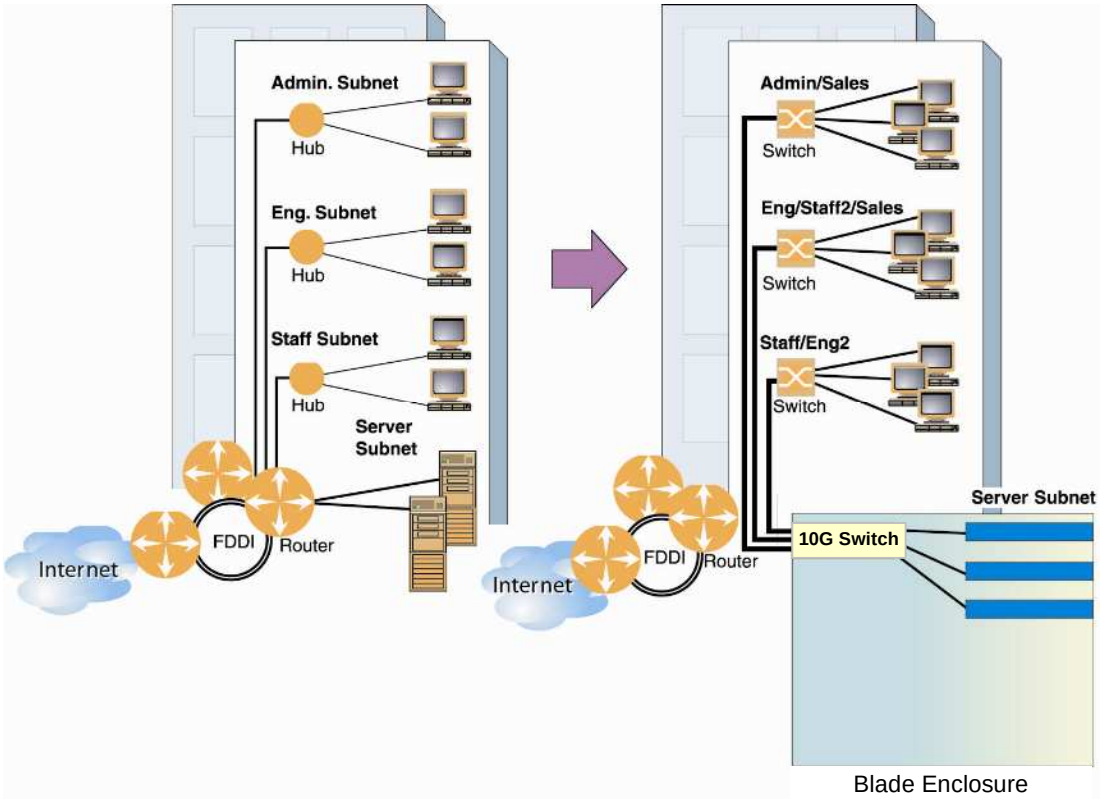
IP サブネット間のルーティング

大半の企業ネットワークの物理的なレイアウトは日々進化しています。スイッチがますますインテリジェントになっている現在、従来のハブ／ルータトポロジは、より高速なスイッチトポロジに取って代えられています。本スイッチはインテリジェントかつ高速で、ワイヤスピードのレイヤ 2 スイッチングと同等のルーティング機能を実現できます。

1 つのデバイスにより高速なルーティングとスイッチングを組み合わせることにより、従来の構成を含めて多様なトポロジを構築できるという別の利点も得られます。

たとえば、次のようなトポロジ移行が考えられます。

図14　ルータの従来のネットワーク



この例では、企業キャンパスをルータ中心のトポロジから、より高速かつ強力なスイッチベーストポロジに移行しています。よく見られるケースですが、従来の構成のネットワークを拡大したり、変更を加えると、システムの中でサブネットが非合理的に分散することになってしまいます。

このような状況はスイッチングだけでは対処できません。むしろ、サブネット間通信のためにルータに情報があふれてしまいます。

この場合、次のように効率に影響します。

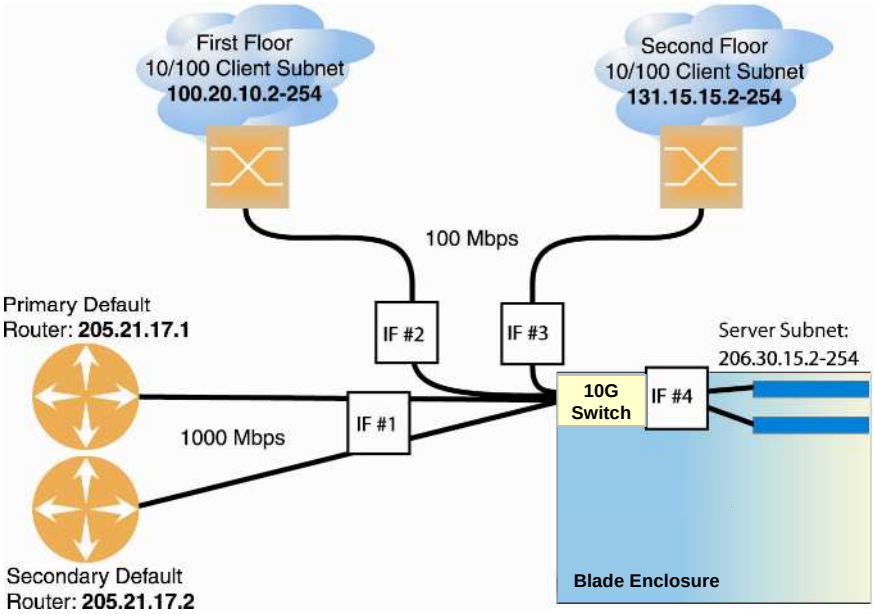
- ルータがスイッチより遅くなる可能性があります。スイッチからルータへの通信と逆向きの通信でサブネット間の通信がおき、データに 2 ホップの追加があるため、スループットが大幅に低下します。
- ルータへのトラフィックが増加し、輻輳が激しくなります。

すべてのエンドステーションをよりよい論理サブネットに移行させたとしても（困難な作業ですが）、異なるサブネットから共用のサーバプールへのアクセスが競合するため、依然としてルータに負荷がかかります。

この問題は、IP ルーティング機能を持つ本スイッチを使用することにより解決します。サブネット間 LAN トラフィックを、ワイヤスピードのレイヤ 2 スイッチング性能を有するスイッチ内でルーティングできます。ルータの負荷を軽減するだけでなく、ネットワーク管理者が、ネットワークの再構成やすべてのエンドステーションの IP アドレスを再設定する必要がなくなります。

次のような構成例で本スイッチの特長を詳しく見てみます。

図15　スイッチベースのルーティングトポロジ



本スイッチは、1 棟のビル全体の各サブネットからギガビットイーサネットトランク、ファーストイーサネットトランクに接続されています。また、共用のサーバは別のサブネットからスイッチに接続されます。さらに別のサブネットのスイッチにプライマリルータ、バックアップルータを接続します。

スイッチにレイヤ 3 IP ルーティングがない場合、サブネット間通信はデフォルトゲートウェイ（本例の場合ルータ）に中継されます。ルータには必要なアドレス情報が入り、そのデータをスイッチに返送します。スイッチは、レイヤ 2 スイッチングにより、適切な宛先サブネットにパケットを中継します。

本装置に実装されているレイヤ 3 IP ルーティングがあれば、IP サブネット間のルーティングをスイッチ内で完全に処理できます。したがって、このサブネットグループの受信トラフィック、送信トラフィックの処理からルータは解放されます。

実装をさらに簡単にするためには、ジャンボフレームをサポートしていない VLAN またはサブネットにルーティングするとき、UDP ジャンボフレームトラフィックを通常のイーサネットフレームサイズに自動的にフラグメント化します。この自動でフレーム変換を行うと、ジャンボフレームを使用して、サーバからユーザに対してすべて透過的に通信を行うことができます。

サブネットルーティングの例

設定を行う前に、スイッチのコマンドラインインタフェース(CLI)にアドミニストレータとして接続する必要があります。

> **注：本例で説明するメニューコマンドをアクセス、使用する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。**

1. 各ルータ、クライアントワークステーションに IP アドレスを割り当てます（または、既存のアドレスを記録します）。

   このトポロジ例では、以下の IP アドレスを使用します。

表20 サブネットルーティング例：IP アドレスの割り当て

サブネット	デバイス	IP アドレス
1	プライマリおよびセカンダリデフォルトルータ	205.21.17.1 および 205.21.17.2
2	1 階のクライアントワークステーション	100.20.10.2-254
3	2 階のクライアントワークステーション	131.15.15.2-254
4	共用サーバ	206.30.15.2-254

2. スイッチに接続した各サブネットに IP インタフェースを割り当てます。
   4 つの IP サブネットがスイッチに接続されているので、4 つの IP インタフェースが必要です。

表21 サブネットルーティング例：IP インタフェースの割り当て

インタフェース	デバイス	IP インタフェースのアドレス
IF 1	プライマリおよびセカンダリデフォルトルータ	205.21.17.3
IF 2	1 階のクライアントワークステーション	100.20.10.1
IF 3	2 階のクライアントワークステーション	131.15.15.1
IF 4	共用サーバ	206.30.15.1

CLI で以下のコマンドを使用して、IP インタフェースを設定します。

```
>> # /cfg/l3/if 1                  (Select IP interface 1)
>> IP Interface 1# addr 205.21.17.3(Assign IP address)
>> IP Interface 1# ena             (Enable IP interface 1)
>> IP Interface 1# ../if 2         (Select IP interface 2)
>> IP Interface 2# addr 100.20.10.1(Assign IP address)
>> IP Interface 2# ena             (Enable IP interface 2)
>> IP Interface 2# ../if 3         (Select IP interface 3)
>> IP Interface 3# addr 131.15.15.1(Assign IP address)
>> IP Interface 3# ena             (Enable IP interface 3)
>> IP Interface 3# ../if 4         (Select IP interface 4)
>> IP Interface 4# addr 206.30.15.1(Assign IP address)
>> IP Interface 4# ena             (Enable IP interface 4)
```

3. 各サーバおよびワークステーションのデフォルトゲートウェイを該当のスイッチの IP インタフェース（サーバやワークステーションと同じサブネット内の IP インタフェース）に設定します。
4. デフォルトゲートウェイをルータのアドレスに設定します。
   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 5# ../gw 1          (Select primary default gateway)
>> Default gateway 1# addr 205.21.17.1(Assign IP address)
>> Default gateway 1# ena           (Enable primary default gateway)
>> Default gateway 1# ../gw 2       (Select secondary default gateway)
>> Default gateway 2# addr 205.21.17.2(Assign address)
>> Default gateway 2# ena           (Enable secondary default gateway)
```

5. 設定を有効にして、適用、確認します。

```
>> Default gateway 2# ../fwrd       (Select the IP Forwarding Menu)
>> IP Forwarding# on                (Turn IP forwarding on)
>> IP Forwarding# apply             (Make your changes active)
>> IP Forwarding# /cfg/l3/cur       (View current IP settings)
```

   結果を確認します。設定に誤りがある場合は修正します。

6. 新しい設定を保存します。

```
>> IP# save                         (Save for restore after reboot)
```

VLAN を使用したブロードキャストドメインの分離

前例では、共通の IP ネットワークを共有するデバイスは、すべて同じブロードキャストドメインにありました。ネットワークでブロードキャストを制限する場合、VLAN を使用して異なるブロードキャストドメインを作成することができます。たとえば、以下の手順に示すように、クライアントトランク用に 1 つ、ルータ用に 1 つ、サーバ用に 1 つ、VLAN を作成できます。

本例では、前例から設定の追加を行います。

1. スイッチポートおよび IP インタフェースをどの VLAN に属するかを決定します。
   次の表にポートおよび VLAN 情報を追加します。

表22 サブネットルーティング例：オプションの VLAN ポート

VLAN	装置	IP インタフェース	スイッチポート	VLAN 番号
1	1 階のクライアントワークステーション	2	20	1
	2 階のクライアントワークステーション	3	21	1
2	プライマリデフォルトルータ	1	18	2
	セカンダリデフォルトルータ	1	19	2
3	共用サーバ 1	4	1	3
	共用サーバ 2	4	2	3

2. スイッチポートを該当の VLAN に追加します。
   上表に示す VLAN の場合、次のように設定します。

```
>> # /cfg/l2/vlan 1                (Select VLAN 1)
>> VLAN 1# add port 20            (Add port for 1st floor to VLAN 1)
>> VLAN 1# add port 21            (Add port for 2nd floor to VLAN 1)
>> VLAN 1# ena                    (Enable VLAN 1)
>> VLAN 1# ../VLAN 2              (Select VLAN 2)
>> VLAN 2# add port 18            (Add port for default router 1)
>> VLAN 2# add port 19            (Add port for default router 2)
>> VLAN 2# ena                    (Enable VLAN 2)
>> VLAN 2# ../VLAN 3              (Add port for default router 3)
>> VLAN 3# add port 1             (Select VLAN 3)
>> VLAN 3# add port 2             (Select port for common server 1)
>> VLAN 3# ena                    (Enable VLAN 3)
```

   ポートを VLAN に追加するごとに、以下のプロンプトが表示されます。

```
Port 4 is an untagged port and its current PVID is 1.
Confirm changing PVID from 1 to 2 [y/n]?
```

   [y]を入力して、ポートにデフォルトのポート VLAN ID (PVID)を設定します。

3. 各 IP インタフェースを該当の VLAN に追加します。
   ポートは 3 つの VLAN に分散しているので、各サブネットの IP インタフェースを該当の VLAN に配置する必要があります。以下のように設定します。

```
>> VLAN 3# /cfg/l3/if 1        (Select IP interface 1 for def. routers)
>> IP Interface 1# vlan 2      (Set to VLAN 2)
>> IP Interface 1# ../if 2     (Select IP interface 2 for first floor)
>> IP Interface 2# vlan 1      (Set to VLAN 1)
>> IP Interface 2# ../if 3     (Select IP interface 3 for second floor)
>> IP Interface 3# vlan 1      (Set to VLAN 1)
>> IP Interface 3# ../if 4     (Select IP interface 4 for servers)
>> IP Interface 4# vlan 3      (Set to VLAN 3)
```

4. 設定を適用、確認します。

```
>> IP Interface 4# apply        (Make your changes active)
>> IP Interface 4# /info/vlan   (View current VLAN information)
>> Information# port            (View current port information)
```

   結果を確認します。設定に誤りがある場合は修正します。

5. 新しい設定を保存します。

```
>> Information# save             (Save for restore after reboot)
```

Routing Information Protocol(RIP)

ルーティング環境では、ルータ間で通信して利用可能なルートを保持します。

Routing Information Protocol(RIP)を使用して、利用可能なルートを動的に学習することができます。本スイッチでは、TCP/IP ルート情報を他のルータと交換する、RIP バージョン 1 (RIPv1)、RIP バージョン 2 (RIPv2)をサポートしています。

ディスタンスベクタプロトコル

RIP はディスタンスベクタプロトコルです。ベクタはネットワーク番号とネクストホップ、ディスタンスはネットワーク番号に関連付けられたコストです。コストはホップ数として定義されており、RIP はコストに基づいてネットワークの到達可能性を判断します。通常、スイッチから次のスイッチまでのディスタンスを 1 ホップとします。このコストつまりホップ数をメトリックといいます。

スイッチは、新しいか変更された宛先ネットワークエントリが入っているルーティングアップデートを受信すると、アップデートに示されたメトリック値に 1 を加算し、そのネットワークをルーティングテーブルに登録します。送信側の IP アドレスはネクストホップとして使用します。

安定性

RIP には、多くのルーティングプロトコルに共通の安定化機能が多数あります。たとえば、スプリットホライズン、ホールドダウンメカニズムが実装されており、誤ったルーティング情報の伝播を防止します。

RIP は、送信元から宛先までの 1 つの経路のホップ数を制限することにより、無限に続くルーティングループを防止します。1 つの経路の最大ホップ数は 15 です。メトリック値が 1 つ増えて 16（無限を示します）になると、宛先に到達不可能と判断します。このため、RIP ネットワークの最大距離は 16 ホップ未満に限定されます。

RIP は、冗長経路が少ないスタブネットワークや小規模な自律システムでよく使用されます。

ルーティングアップデート

RIP は、定期的に、もしくはネットワークトポロジが変更されたときに、ルーティングアップデートメッセージを送信します。各ルータから 30 秒毎にルーティングアップデートを送信することにより、ルーティング情報を通知します。あるルータが別のルータからアップデート情報を 180 秒間受信しない場合、そのルートは無効になります。さらに 120 秒間そのルートに関するアップデートを受信しない場合、そのルートはルーティングテーブルと該当する定期的なアップデートから削除されます。

ルータは、エントリに変更があるルーティングアップデートを受信した場合、ルーティングテーブルを更新して新しいルートとして反映させます。経路のメトリック値が 1 つ増え、送信側をネクストホップとして指定されます。RIP ルータは、宛先までの最適ルート（メトリック値が最小のルート）しか保持しません。

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。

RIPv1

RIP バージョン 1 では、定期的なルーティングアップデートにブロードキャストの UDP データパケットを使用します。ただし、ルーティングアップデートにサブネットマスク情報がないという大きな欠点があります。そのため、サブネットルートとホストルートのどちらであるかを、ルータは判断できません。RIPv2 の導入後は限定的にしか使用されていません。RIPv1、RIPv2 の詳細については、RFC 1058、RFC 2453 を参照してください。

RIPv2

RIPv2 は、大半のネットワークで最も一般的で望ましいプロトコルです。RIP メッセージで搬送できる有効な情報が増え、またセキュリティ機能があります。RIPv2 の詳細については、RFC 1723、RFC 2453 を参照してください。

RIPv2 では、ルーティングアップデートにマルチキャスト UDP（アドレス 224.0.0.9）データパケットを使用して、効率が改善しています。サブネットマスク情報はルーティングアップデートで提供されます。また、共用パスワードを使用してルーティングアップデートの認証を行う、セキュリティオプションが追加されています。本スイッチでは、RIPv2 の平文パスワードをサポートしています。

RIPv1 互換モードの RIPv2

本スイッチのソフトウェアでは、RIPv2 を RIPv1 互換モードにして、1 ネットワーク内で RIPv2 ルータと RIPv1 ルータの両方を使用できます。このモードでは、定期的なルーティングアップデートでブロードキャスト UDP データパケットが使用されるため、RIPv1 ルータはこれらのパケットを受信できます。RIPv1 ルータが受信側の場合、ルーティングアップデートがナチュラルマスクかホストマスクを搬送しなければなりません。そのため、ほとんどのネットワークトポロジには推奨できません。

注：1 ネットワーク内で RIPv1 と RIPv2 の両方を利用する場合、ネットワーク全体でサブネットマスクを 1 つにしてください。

RIP の機能

本スイッチのソフトウェアには、RIPv1、RIPv2 をサポートする以下の機能があります。

ポイズン

RIP での単純なスプリットホライズンでは、あるネイバから学習したルートを、そのネイバに送信するアップデートには含めません。RIP では一般的にポイズンの設定を無効にしています。ポイズンリバース付きのスプリットホライズンは、そのようなアップデートに含めますが、メトリックを 16 に設定します。この機能の欠点はルーティングアップデートでサイズが大きくなることです。

Triggered update

Triggered update は収束を高速化するために使用されます。有効にした場合(/cfg/l3/rip/if x/trigg ena)、ルータがルートのメトリックを変更すると、通常のアップデート間隔を待たずに、アップデートメッセージを直ちに送信します。Triggered update は有効にすることを推奨します。

マルチキャスト

RIPv2 メッセージでは定期的なブロードキャストに IP マルチキャストアドレス(224.0.0.9)を使用します。RIPv1 ルータではマルチキャスト RIPv2 通知を処理しません。外部に転送されない、ルータ間のメッセージのため、IGMP は必要ありません。

RIPv2 を RIPv1 互換モードにするには、マルチキャストを無効に設定してください。

デフォルト

RIP ルータは、ルーティングテーブルで通常 0.0.0.0 と表されるデフォルトルートを提供します。ルーティングテーブルに宛先ネットワークまでの明示的なルートがない場合、デフォルトルートにパケットを転送します。

メトリック

メトリックフィールドの値は 1～15 で、インタフェースの現在のメトリックを示します。メトリック値は、通常宛先までの総ホップ数を示します。メトリック値が 16 は、到達不可能な宛先を示します。

認証

RIPv2 認証では平文パスワードを使用します。認証パスワードを使用する場合、認証キー値を入力する必要があります。

RIP メッセージの認証には次の方法が使用されます。

- ルータが RIPv2 メッセージを認証するように設定されていない場合、RIPv1 メッセージと未認証の RIPv2 メッセージを受信します。認証済み RIPv2 メッセージは廃棄されます。
- RIPv2 メッセージを認証するように設定されている場合、RIPv1 メッセージと認証テストをパスした RIPv2 メッセージを受信します。未認証と認証に失敗した RIPv2 メッセージは廃棄されます。

セキュリティを最大限にするために認証を有効にすると（cfg/l3/rip/if x/auth パスワード）、RIPv1 メッセージは無視されます。それ以外の場合、認証メッセージのルーティング情報は、未認証の状態で RIPv1 ルータによって伝播されます。

RIP 設定例

注：RIP を無効にしたインタフェースでは、RIP パラメータがどのように設定されているかに関わらず、RIP のすべてのデフォルト値が使用されます。RIP は稼働中のインタフェースを含めたアップデートを定期的に送信しますが、停止中のインタフェースは含めません。

1. ルーティングインタフェース用の VLAN を追加します。

```
>> Main# cfg/l2/vlan 2/ena                          (Enable VLAN 2)
>> VLAN 2# add 20                                   (Add port 20 to VLAN 2)
Port 20 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 2 [y/n]: y
>> VLAN 2# /cfg/l2/vlan 3/ena                       (Enable VLAN 3)
>> VLAN 3# add 21 (Add port 21 to VLAN 3)
Port 21 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 3 [y/n]: y
```

2. IP インタフェースを VLAN に追加します。

```
>> Main# cfg/l3/if 2/ena              (Enable interface 2)
>> IP Interface 2# addr 102.1.1.1     (Define IP address for interface 2)
>> IP Interface 2# vlan 2             (Add interface 2 to VLAN 2)
>> IP Interface 2# /cfg/l3/if 3/ena   (Enable interface 3)
>> IP Interface 3# addr 103.1.1.1     (Define IP address for interface 3)
>> IP Interface 3# vlan 3             (Add interface 3 to VLAN 3)
```

3. RIP をグローバルにオンにして、各インタフェースの RIP を有効にします。RIP を有効にする前に、IP Forwarding を有効にする必要があります(/cfg/l3/frwd/on)。

```
>> Main# cfg/l3/rip on                          (Turn on RIP globally)
>> Routing Information Protocol# if 2/ena       (Enable RIP on IP interface 2)
>> RIP Interface 2# ..
>> Routing Information Protocol# if 3/ena       (Enable RIP on IP interface 3)
>> RIP Interface 3# apply                       (Apply your changes)
>> RIP Interface 3# save                        (Save the configuration)
```

スイッチのルーティングテーブルで現在有効なルートは、/maint/route/dump コマンドを使用して確認します。

ガーベジコレクション期間内に RIP で学習されたルート、つまりメトリック値が 16 でルーティングテーブルから削除されるルートについては、/info/l3/rip/routes コマンドを使用します。ローカルで設定したスタティックルートは RIP ルーティングテーブルには表示されません。

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
- IGMPv3
- 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、バージョン 2 とバージョン 3 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。

IGMPv3

IGMPv3 には、IGMP 機能を拡張する新しい Membership Report メッセージがあります。本スイッチは、RFC3376 に記載される全てのタイプの IGMPv3 Membership Report についてスヌーピングをサポートします。

IGMPv3 は、Source-Specific Multicast(SSM)をサポートします。SSM は、ソースとグループ双方のアドレスによりセッショントラフィックを識別します。本スイッチは、定義したソースアドレスからのみのマルチキャストパケットをホストが受信できるソースフィルタリングを用います。

本スイッチは、以下の IGMPv3 フィルタモードをサポートします。

- INCLUDE モード: ホストは、マルチキャストグループにメンバシップリクエストを発行し、トラフィックを受信したい IP アドレスのリストを提供します。
- EXCLUDE モード: ホストは、マルチキャストグループにメンバシップリクエストを発行し、トラフィックを受信したくない IP アドレスのリストを提供します。すなわち、ホストは Exclude リストに入っていないソースからのトラフィックのみ受信します。

EXCLUDE モードのスヌーピングを無効にするには、以下のコマンドを用います。

/cfg/l3/igmp/snoop/igmpv3/exclude dis

デフォルトでは、IGMPv3 Group Record に登録された最初の 8 つのソースをスヌープします。スヌープするソース数を変更する場合は、以下のコマンドを用います。

/cfg/l3/igmp/snoop/igmpv3/source <1-64>

IGMPv3 スヌーピングは、IGMPv1、IGMPv2 スヌーピングと互換性があります。以下のコマンドにより、バージョン 1 とバージョン 2 のスヌーピングを無効にすることができます。

/cfg/l3/igmp/snoop/igmpv3/v1v2 dis

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。

マネジメントポート 17 を除いたポートでスタティック Mrouter を構成できます。本スイッチは、合計 16 までスタティック Mrouter をサポートします。

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/on                    (Globally turn IGMP on)
>> IGMP# snoop                        (Select IGMP Snooping menu)
>> IGMP Snoop# add 1                  (Add VLAN 1 to IGMP Snooping)
>> IGMP Snoop# apply                  (Make your changes active)
```

3. IGMPv3 スヌーピングを有効にします。

```
>> IGMP Snoop# igmpv3                 (Select IGMPv3 menu)
>> IGMP V3 Snoop# ena                 (Enable IGMPv3 Snooping)
>> IGMP V3 Snoop# apply               (Apply the configuration)
>> IGMP V3 Snoop# save                (Save your changes)
```

4. 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)
Note: Local groups (224.0.0.x) are not snooped and will not appear.
      Source           Group       VLAN   Port   Version    Mode  Expires   Fwd
 ---------------- --------------- ------ ------- --------   ---- ---------- ---
 224.10.2.0       232.1.0.0       2      18      V3         INC  4:17       Yes

>> /info/l3/igmp/mrouter          (Select Mrouter Information menu)
>> IGMP Multicast Router# dump                 (Show IGMP Group information)
VLAN       Port       Version    Expires    Max Query Resp. Time     QRV   QQIC
-------    -------    ---------  --------   ---------------------- ----   ----
1          21         V2         atatic     unknown                -      -
2          20         V3         4:09       128                    2      125
```

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 21          (Select port 21)
>>IGMP Port 21# filt ena     (Enable IGMP Filtering on the port)
Current port 21 filtering: disabled
New port 21 filtering: enabled
>>IGMP Port 21# add 1            (Add IGMP Filter 1 to the port)
>>IGMP Port 21# 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。

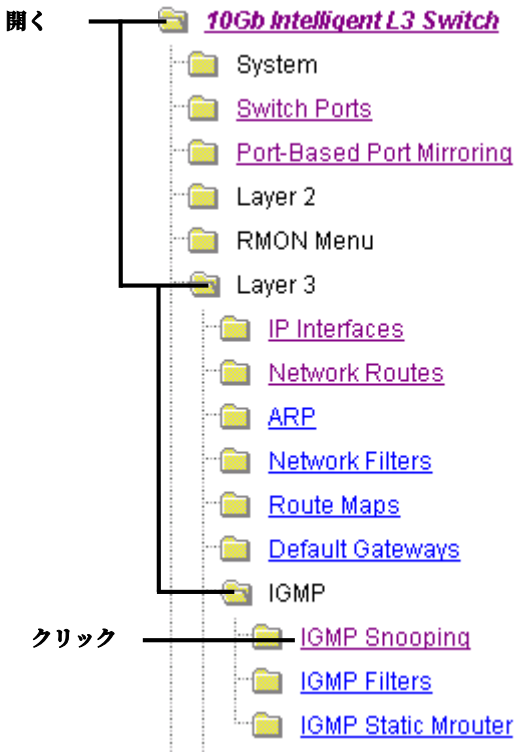
```
>> /cfg/l3/igmp/mrouter             (Select IGMP Mrouter menu)
>> Static Multicast Router# add 20  (Add port 20 as Static
                                     Mrouter port)
Enter VLAN number: (1-4094) 1       (Enter the VLAN number)
Enter the version number of mrouter [1|2|3]: 2 (Enter the IGMP
                                               version number)
```

2. 構成を適用、確認、保存します。

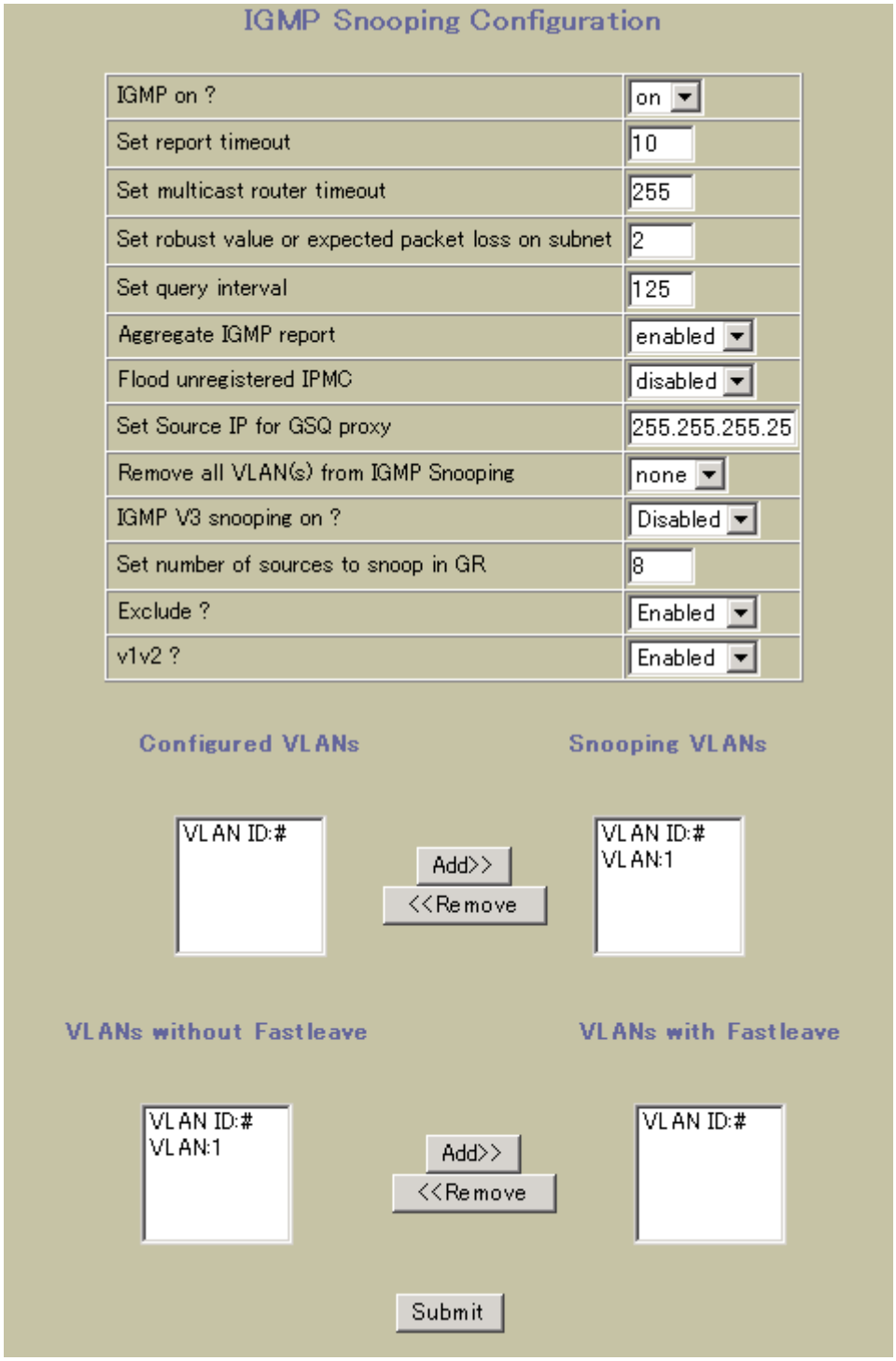
```
>> Static Multicast Router# apply    (Apply the configuration)
>> Static Multicast Router# cur      (View the configuration)
>> Static Multicast Router# save     (Save the configuration)
```

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）。

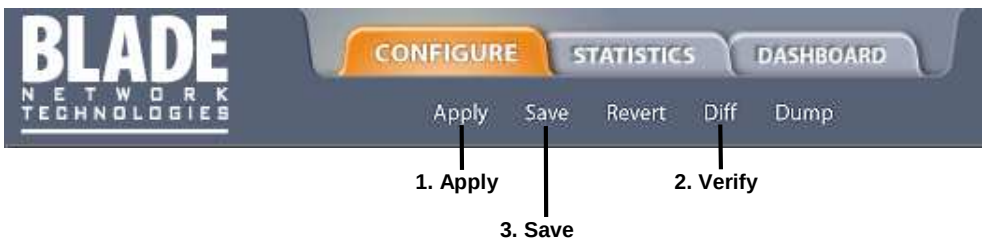


c. IGMP スヌーピングを有効にします。



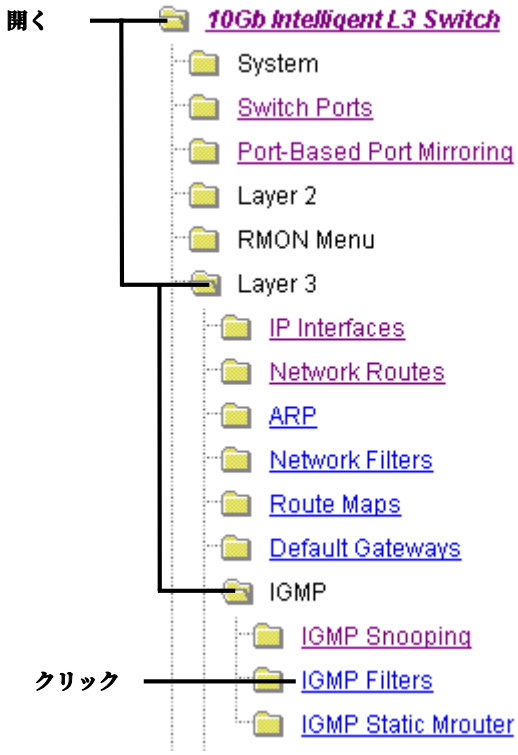
d. Submit をクリックします。

3. 設定を適用、確認、保存します。

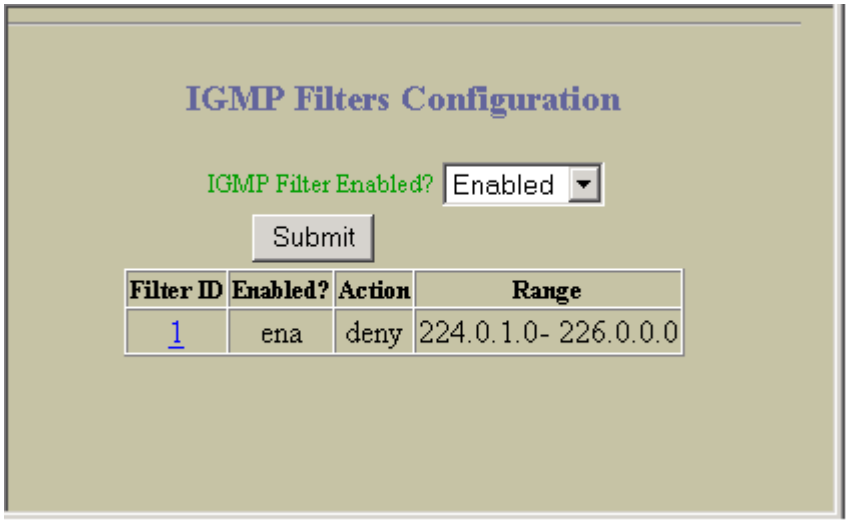


IGMP フィルタリングの設定（BBI の例）

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）。



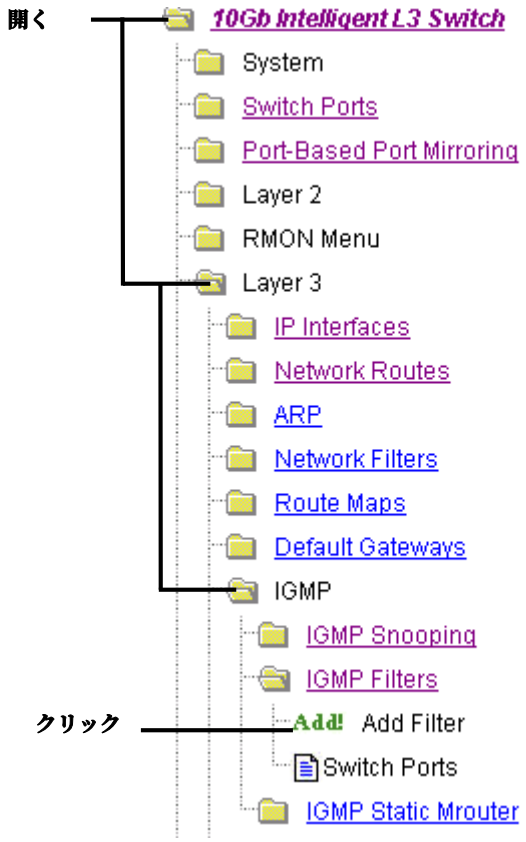
   c. IGMP フィルタリングをグローバルに有効にします。



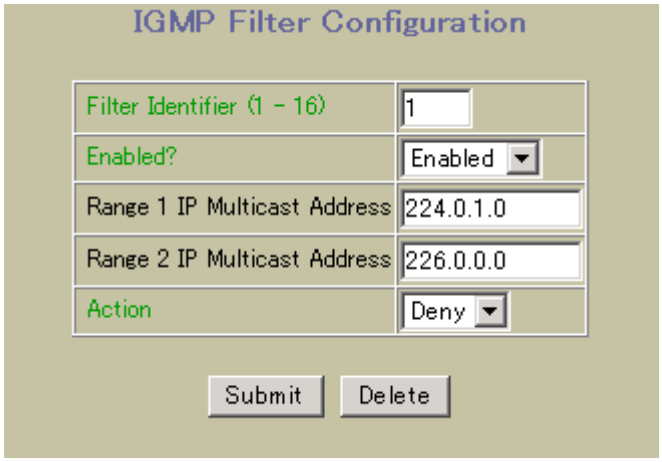
   d. Submit をクリックします。

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。

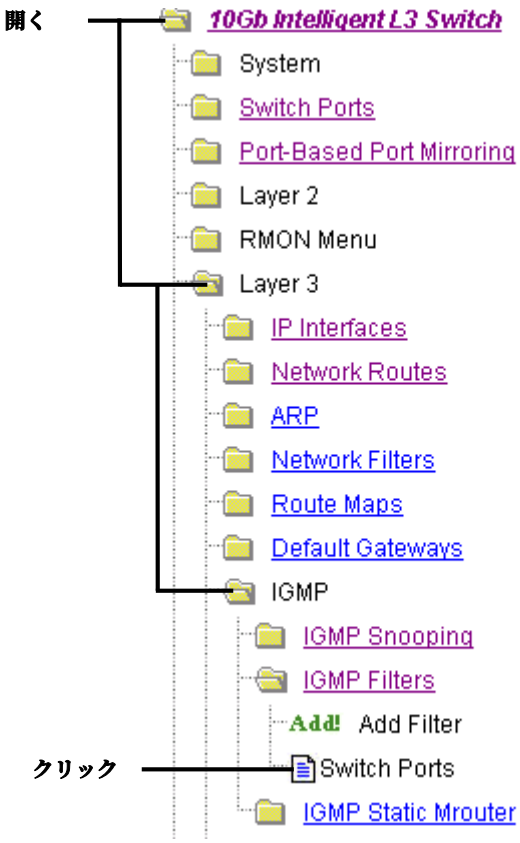


b. IGMP フィルタを有効にします。IP マルチキャストアドレスの範囲とファイタ処理（許可または拒否）を指定します。

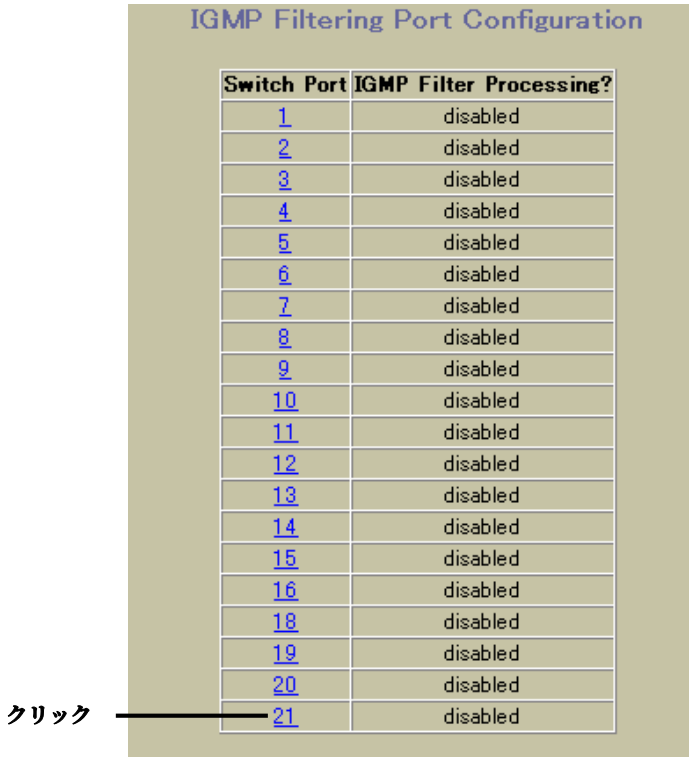


c. Submit をクリックします。

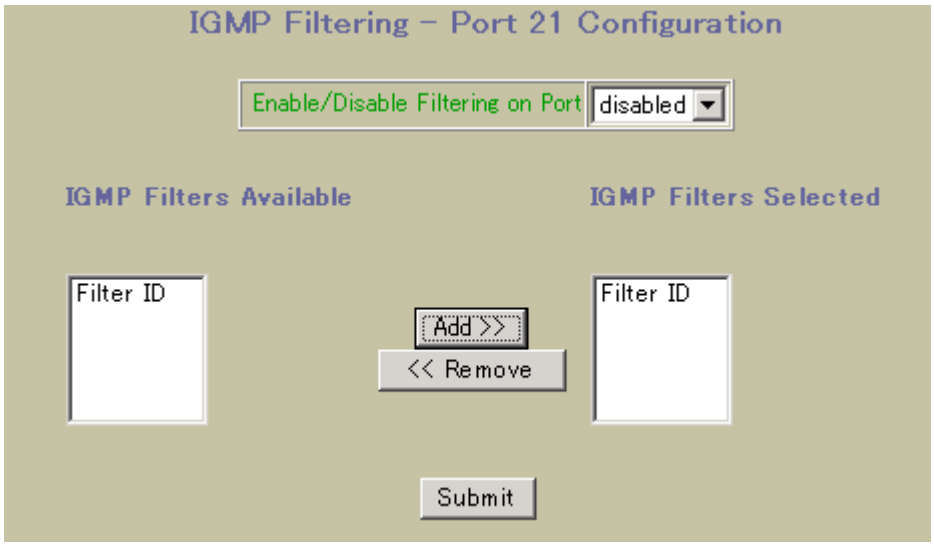
4. フィルタをポートに割り当て、そのポートで IGMP フィルタリングを有効にします。
   a. Layer 3 > IGMP > IGMP Filters > Switch Ports を選択します。



   b. リストから該当のポートを選択します。

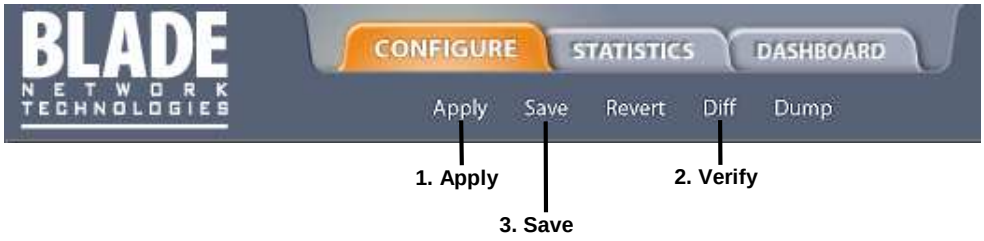


c. ポートで IGMP フィルタリングを有効にします。IGMP Filters Available リストから該当のフィルタを選択し、Add をクリックします。



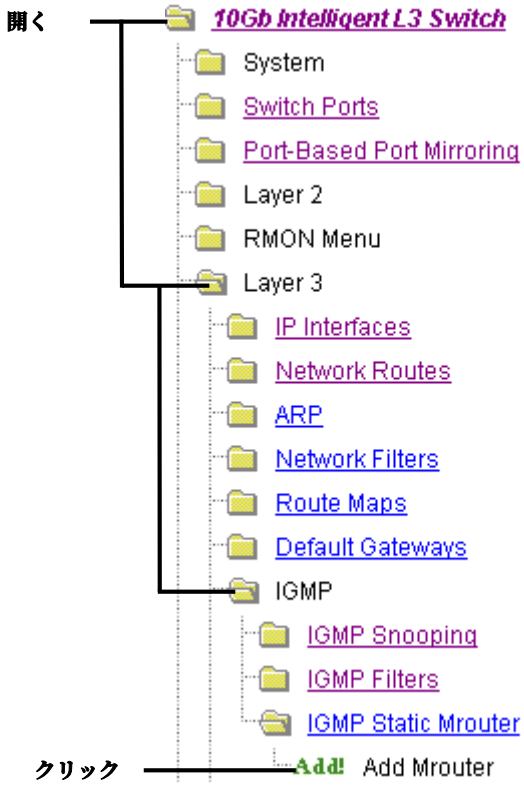
d. Submit をクリックします。

5. 設定を適用、確認、保存します。

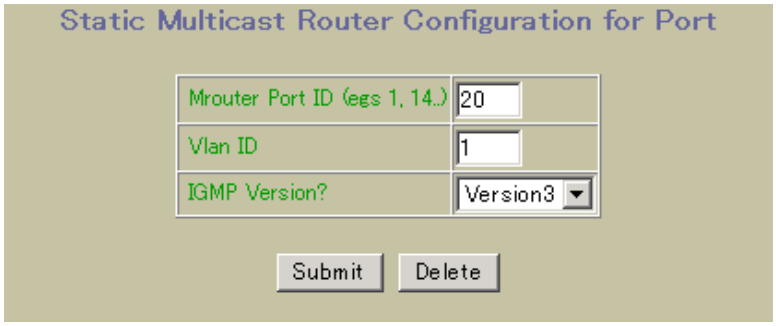


スタティックマルチキャストルータの設定（BBI の例）

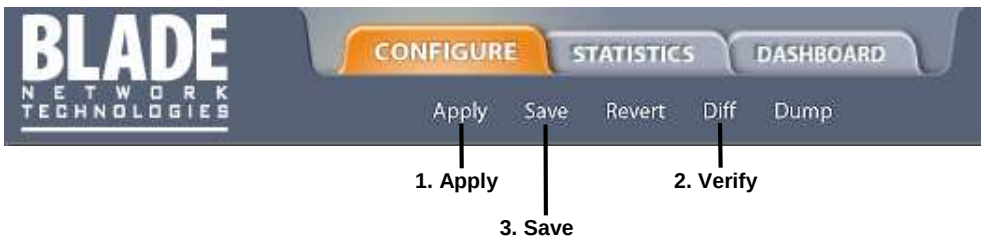
1. スタティック Mrouter を設定します。
   a. CONFIGURE ボタンをクリックします。
   b. Switch フォルダを開き、IP Menu > IGMP > IGMP Static MRouter > Add Mrouter を選択します。



   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。



OSPF

本スイッチは Open Shortest Path First(OSPF)ルーティングプロトコルをサポートします。RFC1583 で説明されている OSPF バージョン 2 仕様に準拠しています。以下の節では、本スイッチでの OSPF のサポートについて説明します。

- OSPF の概要：OSPF エリアのタイプ、ルーティングデバイスのタイプ、ネイバ(neighbor)、アジャセンシ(adjacency)、リンクステートデータベース(link state database)、認証、内部ルーティングと外部ルーティングなど、OSPF の概念について説明します。
- 本スイッチでの OSPF の実装：パラメータの設定、Designated Router の選出、ルート集約、ルートマップの作成など、本スイッチでの OSPF の実装について説明します。
- OSPF 設定例：各種の設定例について、その手順を詳細に説明します。
  - 単純な OSPF ドメインの作成
  - 仮想リンクの作成
  - ルート集約

OSPF の概要

OSPF は、自律システム(AS)という単一の IP ドメイン内のトラフィックをルーティングするために設計されています。AS はエリアと呼ばれるより小さい論理ユニットに分割できます。

ルーティングデバイスは、独自のリンクステートデータベース(LSDB)でリンク情報を保持します。同じエリア内のすべてのルーティングデバイスの LSDB は同一ですが、異なるエリア間では交換されません。エリア間では、ルーティングアップデートのみ交換されるため、大規模で動的なネットワークでルーティング情報を維持するためのオーバヘッドが大幅に低減されます。

以下の節で OSPF の主要な概念について説明します。

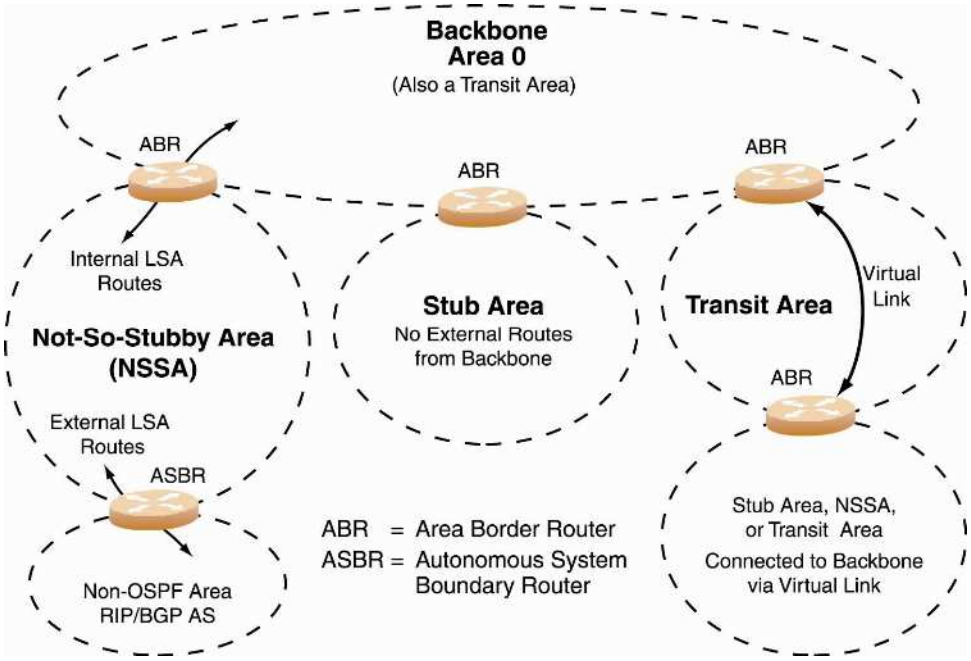
OSPF エリアのタイプ

AS はエリアという論理ユニットに分割できます。エリアが複数ある AS では、エリアの 1 つをバックボーンと呼ばれるエリア 0 にする必要があります。バックボーンは OSPF エリアの中心で機能します。AS 内の他のエリアはすべてバックボーンに接続する必要があります。各エリアからバックボーンにルーティング情報を送り、必要に応じてバックボーンから他のエリアに配信します。

OSPF が以下のエリアのタイプが定義されています。

- スタブエリア：他の 1 つのエリアのみに接続されているエリア。スタブエリアには外部のルート情報を配信しません。
- Not-So-Stubby-Area(NSSA)：スタブエリアに似ていますが、機能が追加されています。AS 外からの外部ルートは NSSA 内に通知できますが、他のエリアには配信されません。
- トランジットエリア：ルーティングデバイス間でエリアサマリ情報を交換できるエリア。バックボーン（エリア 0）、2 つのエリアを接続する仮想リンクを有するエリアで、スタブエリア、NSSA ではないエリアは、トランジットエリアと見なされます。

図16　OSPF エリアのタイプ

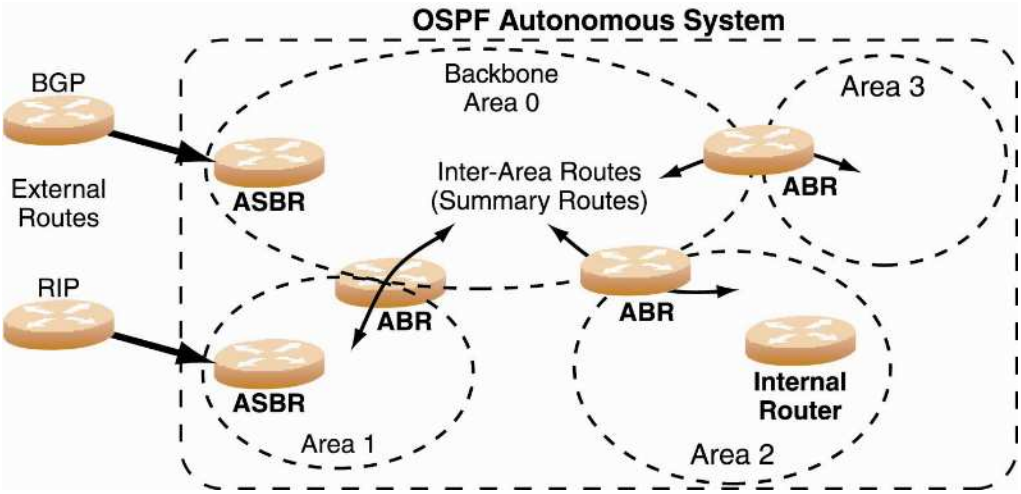


OSPF ルーティング装置のタイプ

図に示すように、OSPF は以下のタイプのルーティング装置を使用します。

- 内部ルータ(Internal Router: IR)：全インタフェースが同一エリア内にあるルータ。ローカルエリア内の他のルーティングデバイスと同じ LSDB を保持します。
- エリア境界ルータ(Area Border Router: ABR)：複数のエリアにインタフェースを有するルータ。接続されているエリア毎に 1 つの LSDB を保持し、エリア間でルーティング情報を配布します。
- 自律システム境界ルータ(Autonomous System Boundary Router: ASBR)：RIP、BGP、スタティックルートなどの非 OSPF ドメインと、OSPF ドメイン間のゲートウェイとして機能するルータ。

図17　OSPF ドメインと自律システム



ネイバ(neighbor)とアジャセンシ(adjacency)

ルーティングデバイスが 2 台以上あるエリアでは、ネイバとアジャセンシを構成します。

ネイバは、相互にヘルス状態に関する情報を保持するルーティングデバイスです。ネイバ関係を確立するため、ルーティングデバイスは各インタフェースに hello パケットを定期的に送信します。ネットワークセグメントを共有し、同じエリアにあり、同じヘルスパラメータ（hello interval, dead interval）、同じ認証パラメータを有するルーティングデバイスが、互いの hello パケットに応答して、ネイバになります。ネイバは hello パケットを定期的に送信しつづけ、ヘルス状態をネイバに知らせます。一方、

ルーティングデバイスは hello パケットを見て、ネイバのヘルス状態を確認したり、新しいネイバとの接続を確立します。

hello プロセスを使用して、ネイバの中から 1 つのデバイスをエリアの Designated Router(DR)に、別の 1 つのデバイスをエリアの Backup Designated Router(BDR)に選出します。DR は他の全ネイバに隣接し、データベースの交換の中心として機能します。各ネイバは DR にデータベース情報を送り、DR はその情報を他のネイバに渡します。

BDR は他の全ネイバ（DR を含む）に隣接します。BDR には、DR と同じように、各ネイバからデータベース情報が送られますが、保持するだけで配信を行いません。ただし、DR に障害が発生した場合、他のネイバにデータベース情報を配信するタスクを受け継ぎます。

リンクステートデータベース(LSDB)

OSPF はリンクステート型のルーティングプロトコルです。リンクとはルーティングデバイスからのインタフェース（つまりルーティング可能な経路）を表します。DR とアジャセンシを確立することにより、OSPF エリア内の各ルーティングデバイスが、そのエリアのネットワークトポロジを示す同一のリンクステートデータベース(LSDB)を保持します。

各ルーティングデバイスは各インタフェースに Link-State Advertisement(LSA)を送信します。LSA は各ルーティングデバイスの LSDB に入ります。OSPF では、フラッディングを使用して、ルーティングデバイス間に LSA を配信します。

LSA によってルーティングデバイスの LSDB が変更された場合、ルーティングデバイスから隣接のネイバ（DR、BDR）にその変更を転送し、続いて他のネイバにも配信されます。

OSPF ルーティングのアップデートは、定期的ではなく、変更が発生した時のみ行われます。あるアジャセンシで新しいルートがある場合、その新ルートを知らせるアップデートメッセージが送信されます。また、ルートテーブルからルートが削除された場合、削除を知らせるアップデートメッセージが送信されます。

Shortest Path First Tree

ルーティングデバイスは、リンクステートアルゴリズム（ダイクストラアルゴリズム）を使用して、宛先に到達するために必要な累積コストに基づいて最短経路を計算します。

OSPF の各インタフェースのコストは、そのインタフェースを通じてパケットを送信する際に必要なオーバヘッドを示します。コストはインタフェースの帯域幅と反比例します。コストが低いほど、帯域幅は広いことを示します。

内部ルーティングと外部ルーティング

ネットワークトラフィックの処理を有効かつ確実に行うためには、ネットワーク上のすべてのルーティングデバイスが、ネットワーク内の他の場所や宛先にパケットを（直接または間接的に）送信する方法を知っている必要があります。これを内部ルーティングといい、スタティックルートによるか、OSPF、RIP、RIPv2 などのアクティブな内部ルーティングプロトコルを使用して実現できます。

ネットワーク内でアクセスするルートについて、ネットワーク外のルータ（アップストリームプロバイダ等）に知らせることも有効です。AS 間のルーティング情報の共有を外部ルーティングといいます。

通常、AS には、1 台以上の境界ルータ（他の OSPF ネットワークとルートを交換するピアルータ）と、AS 内の各ルータが AS 内の他のルータや宛先に到達できるようにする内部ルーティングシステムがあります。

ルーティングデバイスは、他の AS の境界ルータにルートを通知する場合、通知されているルートに示された IP 空間に効率的にデータを送信するようにします。たとえば、192.204.4.0/24 を通知する場合、別のルータが 192.204.4.0/24 の範囲内のアドレスにデータを送信すると、同じ範囲にデータを送ることを宣言します。

本スイッチでの OSPF の実装

本スイッチは、OSPF を 1 インスタンス、ルートを 4K までサポートしています。以下の節では、本スイッチでの OSPF の実装について説明します。

- 設定可能なパラメータ

- エリアの定義
- インタフェースコスト
- DR と BDR の選出
- ルート集約
- デフォルトルート
- 仮想リンク
- ルータ ID
- 認証

設定可能なパラメータ

本スイッチでは、コマンドラインインタフェース(CLI)、ブラウザベースインタフェース(BBI)、または SNMP により OSPF パラメータを設定できます。詳細については、「スイッチへのアクセス」を参照してください。

CLI でサポートするパラメータ：interface output cost、interface priority、dead interval、hello interval、retransmission interval、interface transit delay

OSPF トラップ：トラップは、hello メッセージの失敗、ネイバの障害、SPF の再計算など、イベントやエラーの発生時にメッセージを送信します。

以上のほか、以下のパラメータも指定することができます。

- リンクステートデータベースサイズ：外部 LSA データベースのサイズを指定すると、スイッチのメモリ資源の管理に役立ちます。
- Shortest Path First (SPF) interval：ダイクストラアルゴリズムを使用して、最短経路ツリーを計算する間隔。
- スタブエリアメトリック：スタブエリアにメトリック値を送信するように設定できます。ルート決定に影響を及ぼすメトリック値を、スタブエリア経由で受信したすべてのルートに持たせることができます。
- デフォルトルート：メトリックがあるデフォルトルートを手動でトランジットエリアに入れることができます。2 つのエリア間に複数のルーティングデバイスがあるとき、優先ルートの設定に役立ちます。外部ネットワークへのトラフィックの送出にも役立ちます。

エリアの定義

OSPF ドメインに複数のエリアを設定する場合、エリアの 1 つをバックボーンと呼ばれるエリア 0 として指定する必要があります。バックボーンは OSPF エリアの中心で、通常、他のすべてのエリアと物理的に接続されます。各エリアからバックボーンにルーティング情報を送信し、バックボーンから他のエリアに配信します。

バックボーンはネットワーク内の各エリアに接続するため、各エリアの隣接エリアである必要があります。バックボーンが分割されている場合（離れた OSPF ネットワークを結合した場合など）、AS の一部に到達できないため、仮想リンクを形成して、分割されたエリアを再接続する必要があります（「仮想リンク」参照）。

本スイッチには、最大 3 つの OSPF エリアを接続できます。エリアを設定するためには、OSPF 番号を決め、スイッチのネットワークインタフェースに関連付ける必要があります。手順については後の節で説明します。

OSPF エリアは area index と area ID の 2 つの情報を割り当てることで定義します。OSPF エリアを定義するコマンドは次のとおりです。

```
>> # /cfg/l3/ospf/aindex <area index>/areaid <n.n.n.n>
```

注：上記の aindex **オプションは本スイッチだけで使用する任意インデックスで、実際の** OSPF **エリア番号を示すものではありません。実際の** OSPF **エリア番号は、後の節で説明するように、**areaid **で設定します。**

エリアインデックスの割当て

aindex <area index>オプションは、実際には本スイッチでしか使用しない任意インデックス(0～2)です。このインデックスは OSPF エリア番号にする必要はありませんが、設定を簡単にするため、可能であれば同じ番号にします。

たとえば、以下のコマンドセットは両方とも OSPF エリア 0（バックボーン）とエリア 1 を定義しています。コマンドのエリア ID 部にその情報が入っています。しかし、最初のコマンドセットの方が、エリアインデックスがエリア ID と同じであるため、管理が容易です。

- エリアインデックスとエリア ID が同じ値にした設定

  /cfg/l3/ospf/aindex 0/areaid 0.0.0.0
  （インデックス 0 を使用して ID オクテットフォーマットでエリア 0 を設定）

  /cfg/l3/ospf/aindex 1/areaid 0.0.0.1
  （インデックス 1 を使用して ID オクテットフォーマットでエリア 1 を設定）

- エリアインデックスに任意の値を設定

  /cfg/l3/ospf/aindex 1/areaid 0.0.0.0
  （インデックス 1 を使用して ID オクテットフォーマットでエリア 0 を設定）

  /cfg/l3/ospf/aindex 2/areaid 0.0.0.1
  （インデックス 2 を使用して ID オクテットフォーマットでエリア 1 を設定）

OSPF エリア番号の割り当て

OSPF エリア番号は areaid < IP address >オプションで設定します。他の OSPF ネットワークベンダが使用する 2 通りの表記と互換にするため、オクテットフォーマットにしています。エリア ID の指定には 2 通りの方法があります。

- 最終オクテット(0.0.0.n)をエリア番号に指定

  多くの OSPF ベンダはエリア ID を 1 つの番号で表わします。たとえば、Cisco IOS ベースのルータコマンド“network 1.1.1.0 0.0.0.255 area 1”では、エリア番号を単に“area 1”として定義します。本スイッチでエリア ID に最終オクテットを使用すると、“area 1”は“areaid 0.0.0.1”と同等です。

- マルチオクテット（IP アドレス）

  一部の OSPF ベンダはエリア ID 番号をマルチオクテットフォーマットで表示しています。たとえば、“area 2.2.2.2”は OSPF エリア 2 を表し、本スイッチではそのまま“areaid 2.2.2.2”と指定できます。

注：エリア ID の両方のフォーマットがサポートされていますが、エリア内では同じフォーマットのエリア ID を使用してください。

ネットワークへのエリアの接続

OSPF エリアを定義した場合、そのエリアをネットワークにと関連付ける必要があります。エリアをネットワークに関連付けるには、エリアに接続している IP インタフェースに OSPF エリアインデックスを割り当てる必要があります。コマンドは次のとおりです。

```
>> # /cfg/l3/ospf/if <interface number>/aindex <area index>
```

たとえば、次のコマンドでは、IP インタフェース 14 を 10.10.10.1/24 に設定し、OSPF エリア 1 を定義した後、そのエリアをネットワークに関連付けています。

```
>> # /cfg/l3/if 14                          (Select menu for IP interface 14)
>> IP Interface 14# addr 10.10.10.1     (Define IP address on backbone network)
>> IP Interface 14# mask 255.255.255.0          (Define IP mask on backbone)
>> IP Interface 14# ena                             (Enable IP interface 14)
>> IP Interface 14# ../ospf/aindex 1          (Select menu for area index 1)
>> OSPF Area (index) 1 # areaid 0.0.0.1      (Define area ID as OSPF area 1)
>> OSPF Area (index) 1 # ena                          (Enable area index 1)
>> OSPF Area (index) 1 # ../if 14         (Select OSPF menu for interface 14)
>> OSPF Interface 14# aindex 1       (Attach area to network on interface 14)
>> OSPF Interface 14# enable           (Enable interface 14 for area index 1)
```

インタフェースコスト

OSPF リンクステートアルゴリズム（ダイクストラアルゴリズム）は、各ルーティングデバイスをツリーのルートに配置し、各宛先に到達するために必要な累積コストを決定します。通常、コストはインタフェースの帯域幅と反比例します。つまり、コストが低ければ、帯域幅は広いことを示します。次のコマンドにより、出力ルートのコストを手動で入力できます。

```
>> # /cfg/l3/ospf/if <OSPF interface number>/cost <cost value (1-65535)>
```

DR と BDR の選出

ルーティングデバイスが 2 台以上あるエリアでは、ネイバ間のデータベースを交換する中央窓口として Designated Router(DR)を選出し、DR で障害が発生した時のバックアップとして Backup Designated Router(BDR)を選出します。

DR と BDR の選出は hello プロセスを通じて行われます。スイッチの OSPF インタフェースへのプライオリティの割当てが選定に影響します。コマンドは次のとおりです。

```
>> #/cfg/l3/ospf/if <OSPF interface number>/prio <priority value (0-255)>
```

プライオリティの最大値は 255、最小値は 1 です。プライオリティ値を 0 に設定した場合、そのインタフェースは DR または BDR として使用されません。プライオリティ値が同じ場合、ルータ ID が小さいルーティングデバイスが優先されます。

ルート集約

ルート集約はルーティング情報をまとめます。集約を行わないと、OSPF ネットワーク内の各ルーティングデバイスが、そのネットワークのすべてのサブネットへのルートを保持することになります。集約を行うと、複数のルートを 1 つの通知に集約でき、ルーティングデバイスにかかる負荷を低減し、また、ネットワークが複雑になるのを抑制できます。ルート集約の重要性は、ネットワークの規模に応じて増大します。

次のコマンドを使用すると、最大 16 の IP アドレスレンジに対してサマリルートを指定できます。

```
>> # /cfg/l3/ospf/range <range number>/addr <IP address>/mask <mask>
```

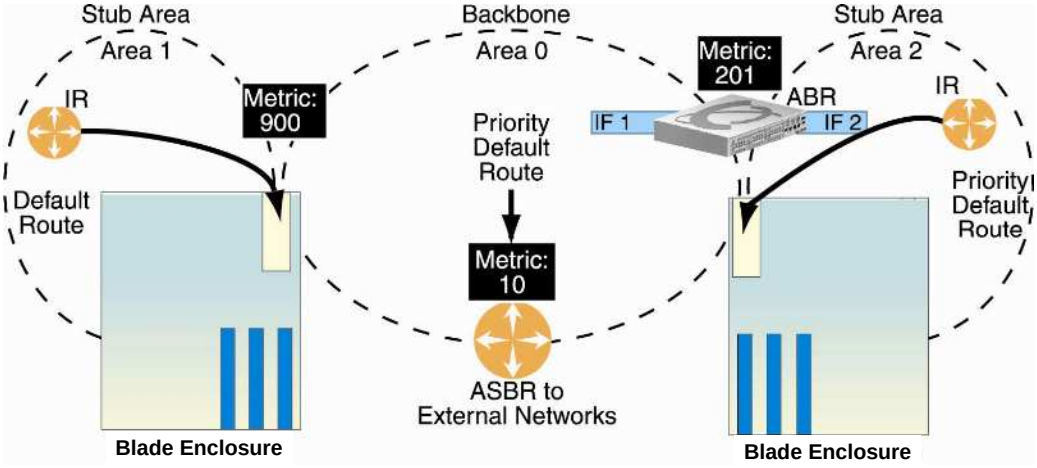
ここで、<range number>は 1～16 の番号、<IP address>はアドレスレンジのベース IP アドレス、<mask>はレンジの IP アドレスマスクです。

デフォルトルート

OSPF ルーティングデバイスは宛先アドレスが未知のトラフィックがあると、デフォルトルートに転送します。通常、デフォルトルートは、目的のエリアか外部ルータに達するまで、バックボーンに向かってアップストリームをたどります。

ABR として機能する各スイッチは、デフォルトルートを各接続エリアに自動的に挿入します。単純な OSPF スタブエリアまたはアップストリーム側に 1 つの ABR だけがある NSSA では（下図の Area 1 参照）、宛先 IP アドレスがエリア外のトラフィックを、スイッチの IP インタフェースに転送し、さらに接続されたトランジットエリア（通常はバックボーン）に転送されます。これは自動的に行われるため、このエリアにはそれ以上の設定は必要ありません。

図18　デフォルトルートの注入



複数の ABR や ASBR がある複雑な OSPF エリアの場合（図の Area 0、Area 2 など）、エリアから複数のルートがあります。このようなエリアでは、さらに設定しないと、未知の宛先のトラフィックの転送先がわかりません。

この状況を打開し、エリア内の複数の選択肢から 1 つのデフォルトルートを選択するためには、各 ABR にメトリック値を手動で設定します。エリア内の優先のデフォルトルートを選択するためにメトリックでプライオリティを割り当てます。メトリック値の設定には次のコマンドを使用します。

```
>> # /cfg/l3/ospf/default <metric value> <metric type (1 or 2)>
```

ここで、<metric value>はこのスイッチをデフォルトルートとして選択するためのプライオリティです。値 none はデフォルトなし、1 はデフォルトルートとして最高のプライオリティが設定されます。メトリックタイプで、外部へのルーティング方法を決定します。

デフォルトルートメトリックをスイッチから削除するには、次のコマンドを使用します。

```
>> # /cfg/l3/ospf/default none
```

仮想リンク

通常、OSPF 内のすべてのエリアがバックボーンに物理的に接続されています。 それが不可能な場合、仮想リンクを使用します。つまり、仮想リンクを形成して、バックボーンではない別のエリアを経由してバックボーンに接続します。

仮想リンクがあるエリアは、すべてのルート情報を持つトランジットエリアである必要があります。仮想リンクをスタブエリアや NSSA の内部に設定することはできません。また、次のコマンドにより、エリアタイプをトランジットとして定義する必要があります。

```
>> # /cfg/l3/ospf/aindex <area index>/type transit
```

仮想リンクの各エンドポイントにあるルーティングデバイスで、仮想リンクを形成する必要がありますが、複数のルーティングデバイスにまたがってもかまいません。スイッチを仮想リンクのエンドポイントに設定するには、次のコマンドを使用します。

```
>> # /cfg/l3/ospf/virt <link number>/aindex <area index>/nbr <router ID>
```

ここで、<link number>は 1～3、<area index>はトランジットエリアの OSPF エリアインデックス、<router ID>は仮想ネイバ(nbr)、つまり対象のエンドポイントにあるルーティングデバイスの IP アドレスです。別の方向に仮想リンクを形成するときには、別のルータ ID が必要です。スイッチにルータ ID を設定する方法については、「ルータ ID」を参照してください。

仮想リンクの詳細な設定例については、「例２：仮想リンク」を参照してください。

ルータ ID

OSPF エリア内のルーティングデバイスは、ルータ ID で識別されます。ルータ ID は IP アドレスのフォーマットで表されます。IP インタフェース範囲や OSPF エリアに、ルータ ID の IP アドレスを含める必要はありません。

ルータ ID は次の 2 とおりの方法で設定できます。

- 動的：OSPF プロトコルでは IP インタフェースの最小の IP アドレスをルータ ID として設定します。これがデフォルトです。
- 静的：次のコマンドにより手動でルータ ID を設定します。

```
>> # /cfg/l3/rtrid <IP address>
```

ルータ ID を静的から動的に変更するには、ルータ ID に 0.0.0.0 を設定して保存しスイッチを再起動します。ルータ ID の表示は次のコマンドを使用します。

```
>> # /info/l3/ospf/gen
```

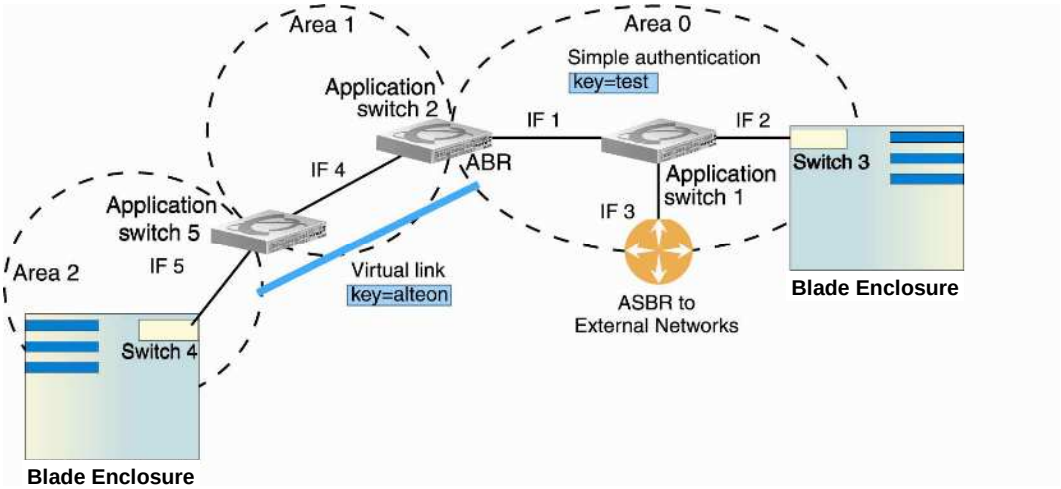
認証

OSPF プロトコルの交換で認証を使い、信認したルーティングデバイスのみ参加させることができます。これにより OSPF パケットを見ていないルーティングデバイスの処理が軽減されます。

OSPF ではパケット認証が可能で、パケットを送受信するときに IP マルチキャストを使用します。ルータは、事前に設定されたパスワードに基づいて、ルーティングドメインに加わります。本スイッチでは、単純パスワード（タイプ 1 平文パスワード）と MD5 暗号化認証です。この認証により、エリア毎にパスワードを設定できます。

次の図は、エリア 0 に test というパスワードを設定した認証を示します。エリア 2 とエリア 0 の間の仮想リンクにも認証を設定しています。エリア 1 には OSPF 認証を設定していません。

図19　OSPF 認証



図に示すスイッチに単純な平文 OSPF パスワードを設定するには、次のコマンドを使用します。

1. スイッチ 1、2、3 のエリア 0 に OSPF 認証を有効にします。

```
>> # /cfg/l3/ospf/aindex 0/auth password
```

2. スイッチ 1、2、3 のエリア 0 の各 OSPF IP インタフェースに 8 文字までの平文パスワードを指定します。

```
>> # /cfg/l3/ospf/if 1
>> OSPF Interface 1 # key test
>> OSPF Interface 1 # ../if 2
>> OSPF Interface 2 # key test
>> OSPF Interface 1 # ../if 3
>> OSPF Interface 3 # key test
```

3. スイッチ 4 のエリア 2 に対する OSPF 認証を有効にします。

```
>> # /cfg/l3/ospf/aindex 2/auth password
```

4. スイッチ 2 と 4 のエリア 2 とエリア 0 間の仮想リンクに最大 8 文字の平文パスワードを設定します。

```
>> # /cfg/l3/ospf/virt 1/key alteon
```

次のコマンドでは、図に示すスイッチで MD5 認証を行います。

5. スイッチ 1、2、3 のエリア 0 に対して OSPF MD5 認証を有効にします。

```
>> # /cfg/l3/ospf/aindex 0/auth md5
```

6. スイッチ 1、2、3 のエリア 0 に MD5 キーID を設定します。

```
>> # /cfg/l3/ospf/md5key 1/key test
```

7. スイッチ 1、2、3 の OSPF インタフェースに MD5 キーID を割り当てます。

```
>> # /cfg/l3/ospf/if 1
>> OSPF Interface 1 # mdkey 1
>> OSPF Interface 1 # ../if 2
>> OSPF Interface 2 # mdkey 1
>> OSPF Interface 1 # ../if 3
>> OSPF Interface 3 # mdkey 1
```

8. スイッチ 4 のエリア 2 に対して OSPF MD5 認証を有効にします。

```
>> # /cfg/l3/ospf/aindex 2/auth md5
```

9. スイッチ 2 と 4 のエリア 2 とエリア 0 間の仮想リンクに対して MD5 キーを設定します。

```
>> # /cfg/l3/ospf/md5key 2/key alteon
```

10. スイッチ 2 と 4 の OSPF 仮想リンクに MD5 キーID を割り当てます。

```
>> # /cfg/l3/ospf/virt 1/mdkey 2
```

負荷分散のためのホストルート

本スイッチでの OSPF の実装にはホストルートが含まれます。ホストルートは、ネットワークデバイスの IP アドレスを外部ネットワークに知らせるために使用され、以下の目的で実現されます。

- ABR 負荷共有

  負荷分散の 1 つとして、ホストルートを使用して複数の ABR 間で OSPF トラフィックを分担できます。これを実現するため、各スイッチで同一のサービスを提供しますが、異なる IP アドレスのホストルートを外部ネットワークに通知します。各 IP アドレスが、外部から異なる、同等のトラフィックを扱う場合、アップストリームルータから入ってくるトラフィックを ABR 間で均等に分担する必要があります。

- ABR フェイルオーバ

  ABR 負荷共有を補完するために、各 ABR に同じホストルートを設定できます。これらのホストルートには異なるコストを指定することにより、サーバ毎に異なる ABR が優先ルートとして選択され、他の ABR はフェイルオーバしたときのバックアップとして利用できます。

- Equal Cost Multipath(ECMP)

  ECMP では、ルータから宛先に向かって複数のホップ可能なルートを持ちます。ECMP は、サービスの IP タイプから計算してルートを分離します。全てのパスの宛先へのコストが等しくなるように計算され、全ての等コストパスに関する次ホップはルーティングテーブルに格納されます。

複数のルーティングプロセスを経由する冗長経路（OSPF、RIP、スタティックルートなど）がネットワーク上に存在する場合、スイッチは OSPF で得た経路をデフォルトにします。

未サポートの OSPF 機能

OSPF の以下の機能は未サポートです。

- 外部ルートの集約
- OSPF ルートのフィルタリング
- OSPF を使用したマルチキャストルートの転送
- 非ブロードキャストマルチアクセスネットワーク（フレームリレー、X.25、ATM など）での OSPF の設定

OSPF 設定例

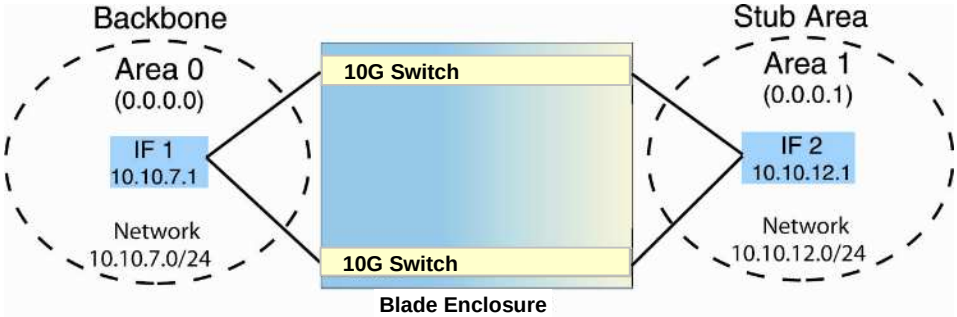
本スイッチで OSPF を設定する基本的手順を以下にまとめます。各ステップの詳細については、後の節で説明します。

- IP インタフェースの設定
  スイッチの OSPF エリアに割り当てる各ネットワーク（IP アドレスレンジ）に 1 つの IP アドレスが必要です。
- ルータ ID の設定（オプション）
  ルータ ID は、スイッチで仮想リンクを設定する場合のみ必要です。
- スイッチでの OSPF の有効化
- OSPF エリアの定義
- OSPF インタフェースパラメータの設定
  IP インタフェースを使用して、各エリアにネットワークを接続します。
- OSPF エリア間のルート集約の設定（オプション）
- 仮想リンクの設定（オプション）
- ホストルートの設定（オプション）

例１：単純な OSPF ドメイン（AOS CLI の例）

この例では、バックボーンとスタブエリアの 2 つの OSPF エリアを定義します。スタブエリアは外部ルートに通知できないので、データベースのサイズが減少します。代わりに、IP アドレス 0.0.0.0 のデフォルトサマリルートが自動的にスタブエリアに挿入されます。宛先 IP アドレスがスタブエリア外のトラフィックは、スタブエリアの IP インタフェースに転送され、次にバックボーンに転送されます。

図20　単純な OSPF ドメイン



図に示すような OSPF を設定する手順は次のとおりです。

1. OSPF エリアに接続する各ネットワークで IP インタフェースを設定します。
   この例では、IP インタフェースが 2 つ必要です。10.10.7.0/24 のバックボーンネットワーク用に 1 つ、10.10.12.0/24 のスタブエリアネットワーク用に 1 つです。

```
>> # /cfg/l3/if 1                              (Select menu for IP interface 1)
>> IP Interface 1 # addr 10.10.7.1          (Set IP address on backbone network)
```

```
>> IP Interface 1 # mask 255.255.255.0        (Set IP mask on backbone network)
>> IP Interface 1 # enable                              (Enable IP interface 1)
>> IP Interface 1 # ../if 2                    (Select menu for IP interface 2)
>> IP Interface 2 # addr 10.10.12.1       (Set IP address on stub area network)
>> IP Interface 2 # mask 255.255.255.0       (Set IP mask on stub area network)
>> IP Interface 2 # enable                              (Enable IP interface 2)
```

2. OSPF を有効にします。

```
>> IP Interface 2 # /cfg/l3/ospf/on                 (Enable OSPF on the switch)
```

3. **バックボーンを定義します。**
   バックボーンは、areaid 0.0.0.0 **を使用してトランジットエリアとして設定します。**

```
>> Open Shortest Path First # aindex 0          (Select menu for area index 0)
>> OSPF Area (index) 0 # areaid 0.0.0.0       (Set the ID for backbone area 0)
>> OSPF Area (index) 0 # type transit        (Define backbone as transit type)
>> OSPF Area (index) 0 # enable                                (Enable the area)
```

4. **スタブエリアを定義します。**

```
>> OSPF Area (index) 0 # ../aindex 1            (Select menu for area index 1)
>> OSPF Area (index) 1 # areaid 0.0.0.1       (Set the area ID for OSPF area 1)
>> OSPF Area (index) 1 # type stub                   (Define area as stub type)
>> OSPF Area (index) 1 # enable                                (Enable the area)
```

5. **ネットワークインタフェースをバックボーンに接続します。**

```
>> OSPF Area 1 # ../if 1                 (Select OSPF menu for IP interface 1)
>> OSPF Interface 1 # aindex 0              (Attach network to backbone index)
>> OSPF Interface 1 # enable                   (Enable the backbone interface)
```

6. **ネットワークインタフェースをスタブエリアに接続します。**

```
>> OSPF Interface 1 # ../if 2            (Select OSPF menu for IP interface 2)
>> OSPF Interface 2 # aindex 1             (Attach network to stub area index)
>> OSPF Interface 2 # enable                  (Enable the stub area interface)
```

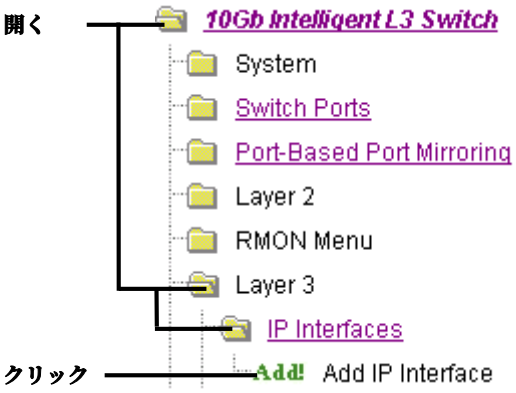
7. **設定変更を適用、保存します。**

```
>> OSPF Interface 2 # apply              (Global command to apply all changes)
>> OSPF Interface 2 # save                (Global command to save all changes)
```

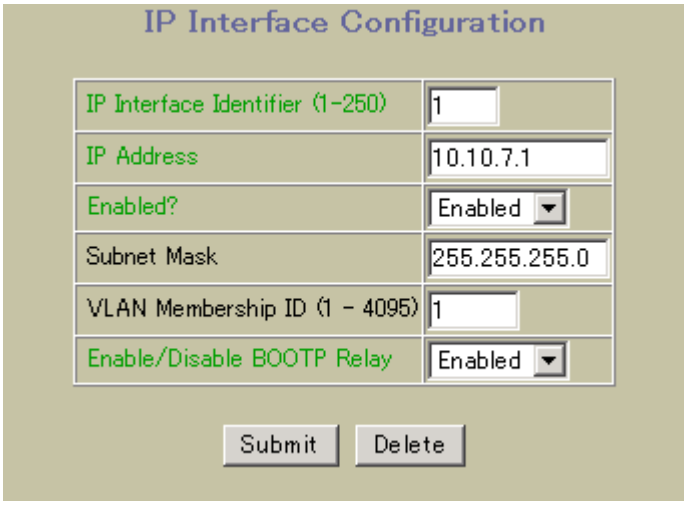
例１：単純な OSPF ドメイン（BBI の例）

1. OSPF エリアに接続する各ネットワークに IP インタフェースを設定します。
   - IF 1
     IP アドレス = 10.10.7.1
     サブネットマスク = 255.255.255.0
   - IF 2
     IP アドレス = 10.10.12.1
     サブネットマスク= 255.255.255.0

   a. CONFIGURE ボタンをクリックします。
   b. IP Interfaces フォルダを開き、Add IP Interface を選択します。

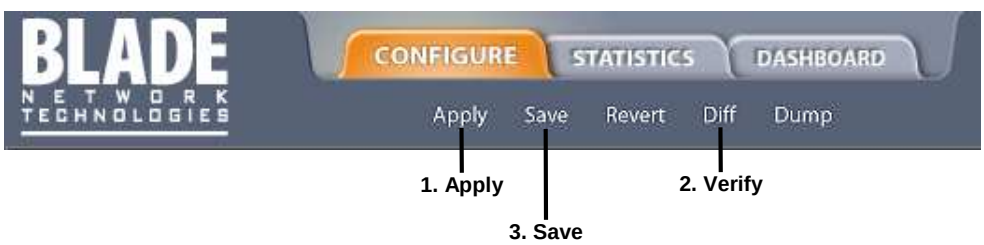


   c. IP インタフェースを設定します。IP アドレス、サブネットマスクを入力し、インタフェースを有効にします。

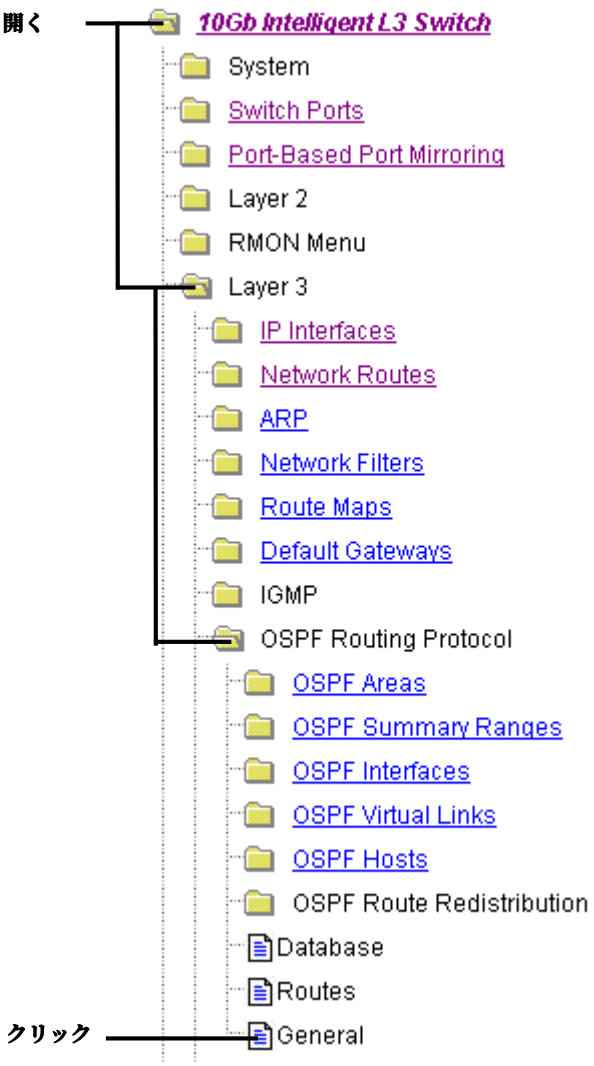


   d. Submit をクリックします。

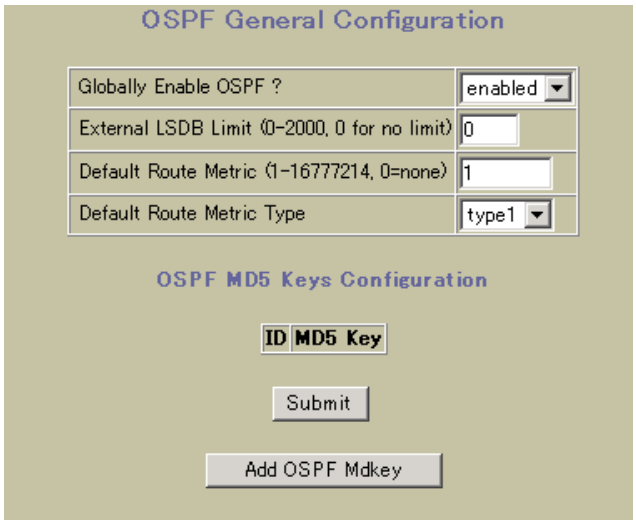
2. 設定を適用、確認、保存します。



3. OSPF を有効にします。
   a. OSPF Routing Protocol フォルダを開き、General を選択します。

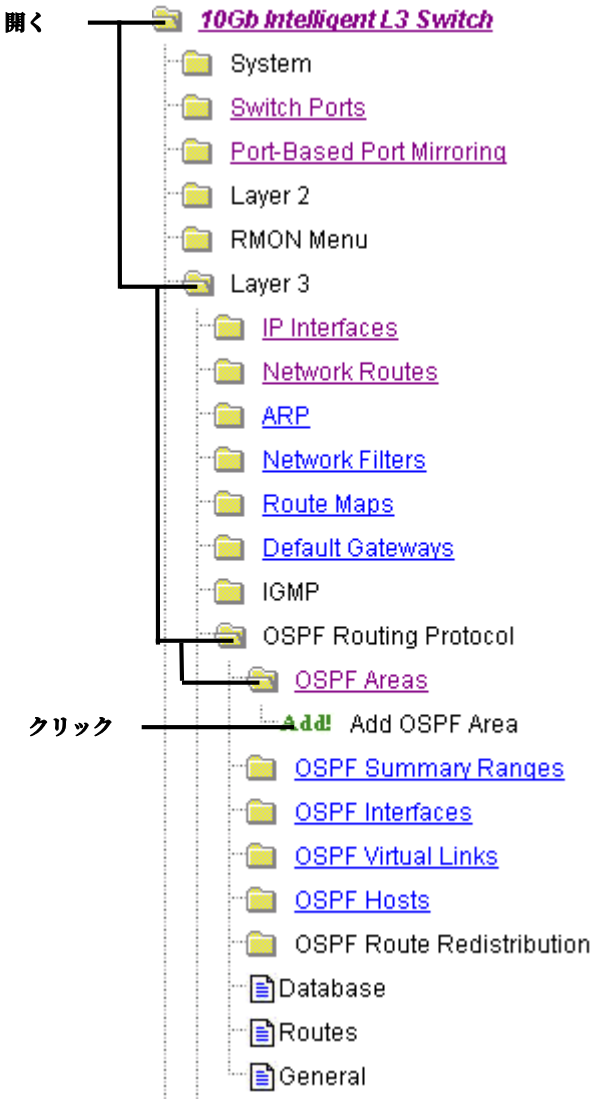


   b. OSPF を有効にします。

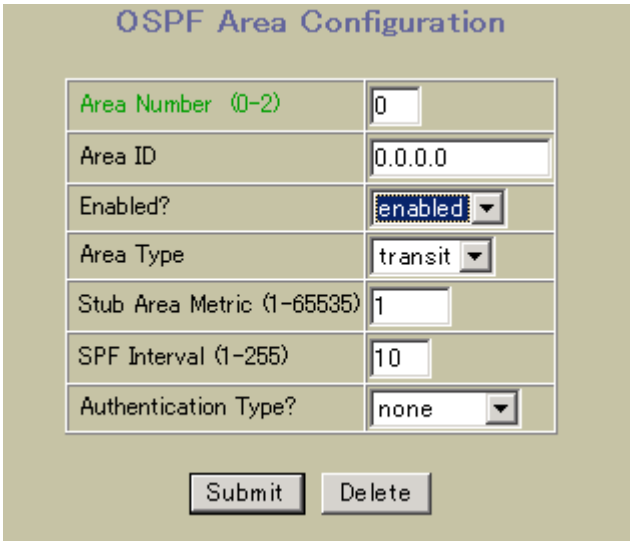


   c. Submit をクリックします。

4. OSPF エリアを設定します。
   a. OSPF Areas フォルダを開き、Add OSPF Area を選択します。

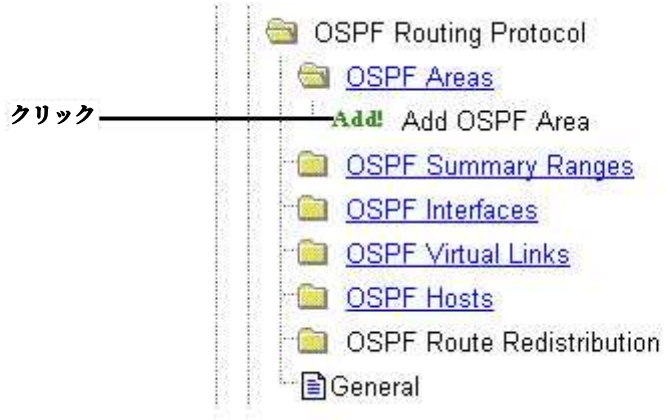


   b. OSPF のバックボーンエリア 0 を設定します。

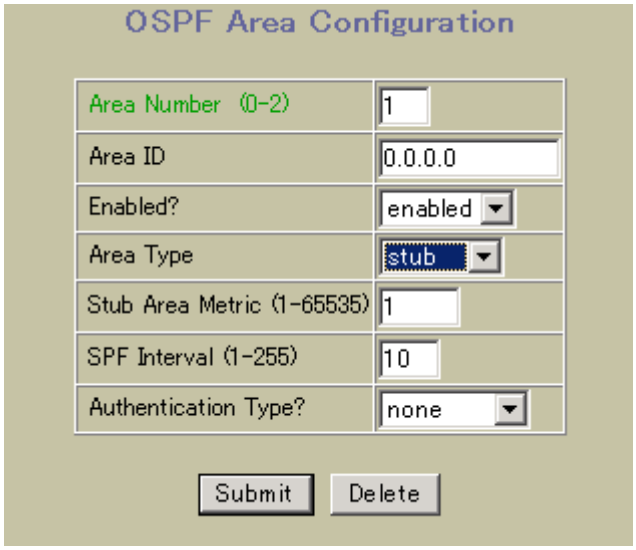


   c. Submit をクリックします。

d. Add OSPF Area を選択します。

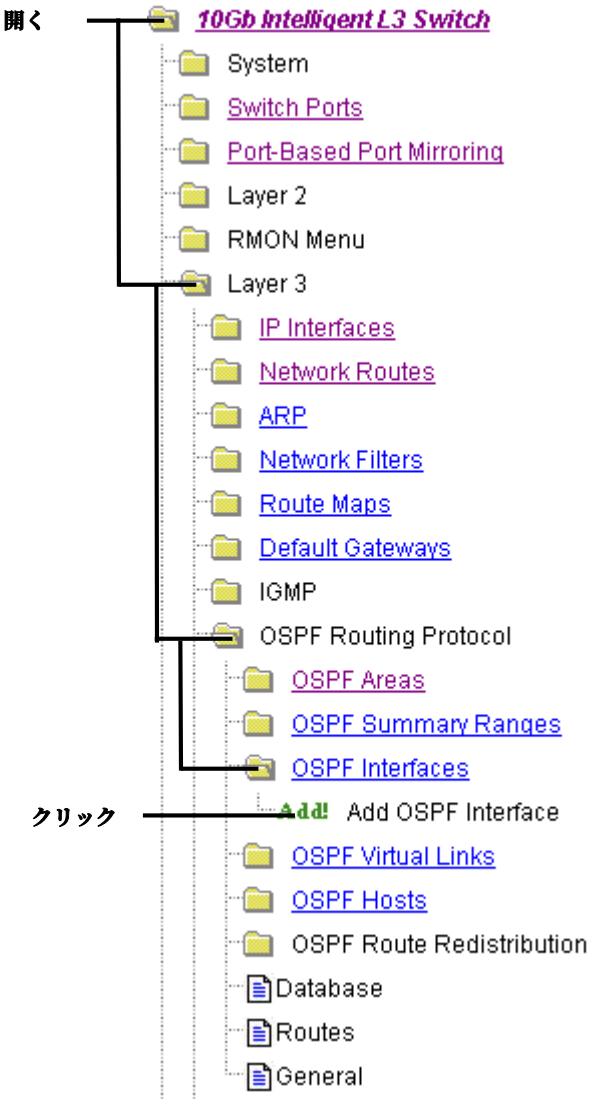


e. OSPF エリア 1 を設定します。

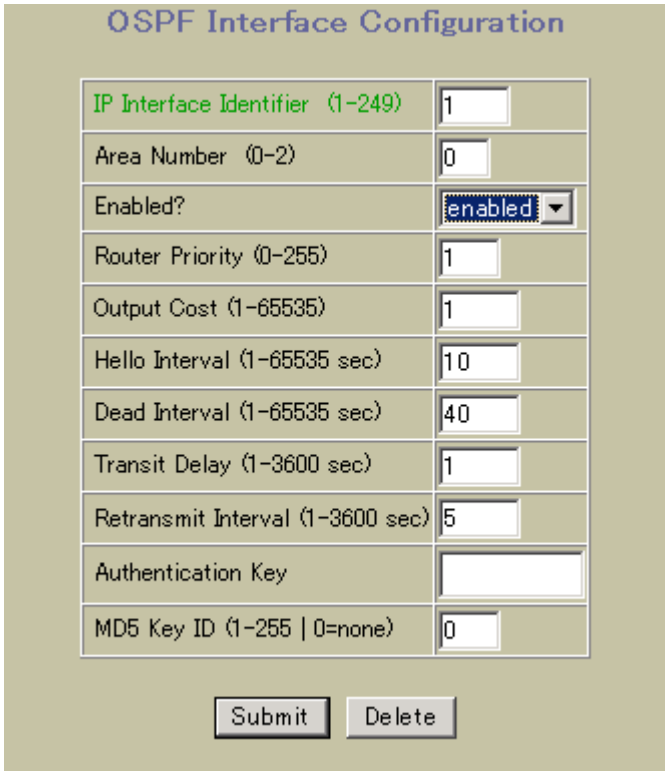


f. Submit をクリックします。

5. OSPF のインタフェースを設定します。
   a. OSPF Interfaces フォルダを開き、Add OSPF Interface を選択します。

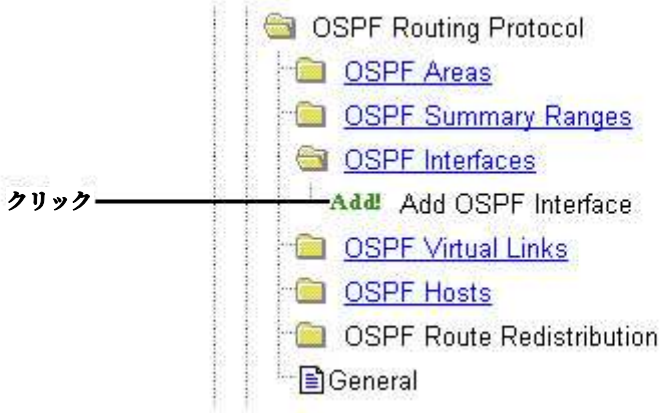


b. OSPF インタフェース 1 を設定し、バックボーンエリア 0 に接続します。

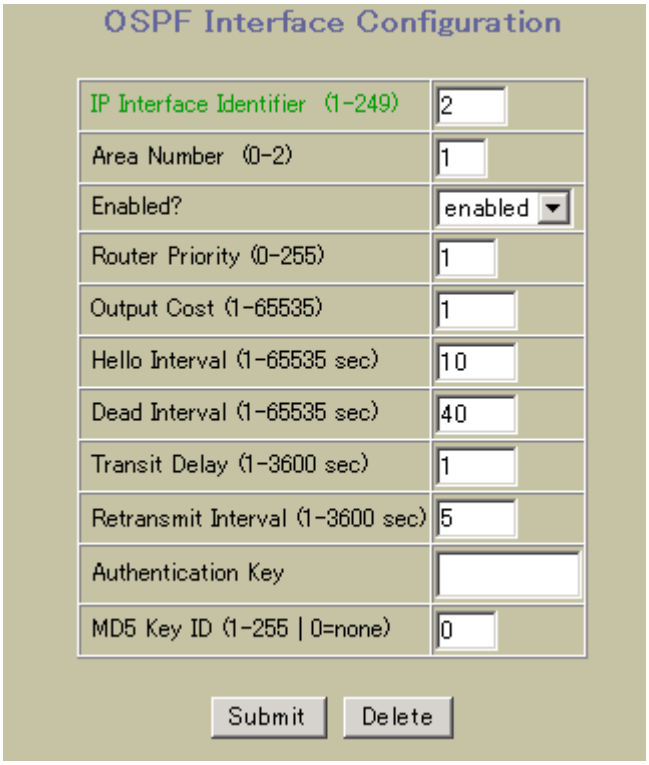


c. Submit をクリックします。

d. Add OSPF Interface を選択します。

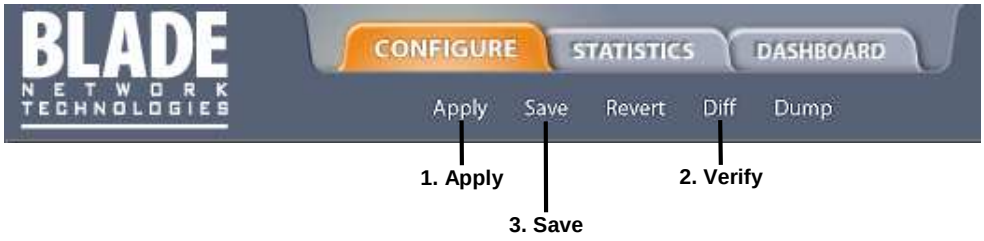


e. OSPF Interface 2 を設定し、スタブエリア 1 に接続します。



f. Submit をクリックします。

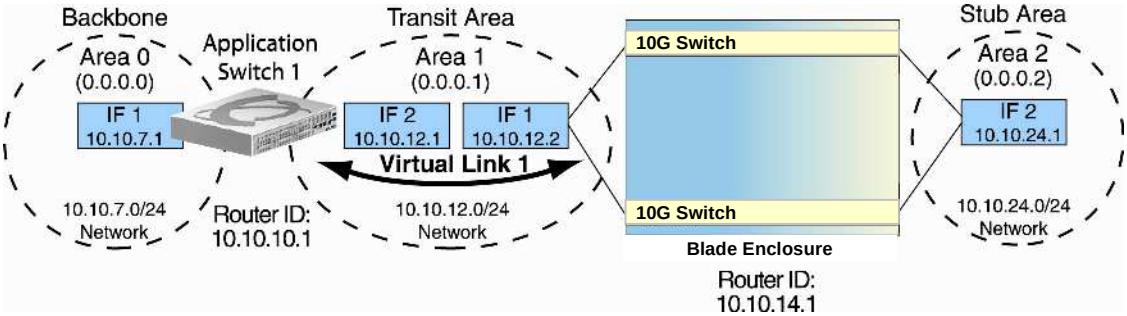
6. 設定を適用、確認、保存します。



例 2：仮想リンク

次の図に示す例では、エリア 2 が通常接続が必要なバックボーンに物理的に接続されていません。代わりに、エリア 1 を通過する仮想リンクを介して、エリア 2 をバックボーンに接続しています。仮想リンクは各エンドポイントで設定する必要があります。

図21　仮想リンクの設定



スイッチ A の仮想リンクに対する OSPF の設定

1. スイッチに接続する各ネットワークで IP インタフェースを設定します。

   この例では、スイッチ A に IP インタフェースが 2 つ必要です。10.10.7.0/24 のバックボーンネットワークに 1 つ、10.10.12.0/24 のトランジットエリアネットワークに 1 つです。

```
>> # /cfg/l3/if 1                              (Select menu for IP interface 1)
>> IP Interface 1 # addr 10.10.7.1          (Set IP address on backbone network)
>> IP Interface 1 # mask 255.255.255.0         (Set IP mask on backbone network)
>> IP Interface 1 # enable                                (Enable IP interface 1)
>> IP Interface 1 # ../if 2                    (Select menu for IP interface 2)
>> IP Interface 2 # addr 10.10.12.1     (Set IP address on transit area network)
>> IP Interface 2 # mask 255.255.255.0     (Set IP mask on transit area network)
>> IP Interface 2 # enable                                 (Enable interface 2)
```

2. ルータ ID を設定します。

   仮想リンクを形成する場合、ルータ ID が必要です。後で、スイッチ B の仮想リンクのエンドポイントを設定するときには、ここで指定したルータ ID を仮想ネイバ(nbr)アドレスとして使用します。

```
>> IP Interface 2 # /cfg/l3/rtrid 10.10.10.1              (Set static router ID)
```

3. OSPF を有効にします。

```
>> IP # /cfg/l3/ospf/on
```

4. バックボーンを定義します。

```
>> Open Shortest Path First # aindex 0           (Select menu for area index 0)
>> OSPF Area (index) 0 # areaid 0.0.0.0                      (Set the area ID)
>> OSPF Area (index) 0 # type transit         (Define backbone as transit type)
>> OSPF Area (index) 0 # enable                             (Enable the area)
```

5. トランジットエリアを定義します。

   仮想リンクを含むエリアはトランジットエリアとして設定する必要があります。

```
>> OSPF Area (index) 0 # ../aindex 1             (Select menu for area index 1)
>> OSPF Area (index) 1 # areaid 0.0.0.1       (Set the area ID for OSPF area 1)
>> OSPF Area (index) 1 # type transit            (Define area as transit type)
>> OSPF Area (index) 1 # enable                             (Enable the area)
```

6. ネットワークインタフェースをバックボーンに接続します。

```
>> OSPF Area (index) 1 # ../if 1          (Select OSPF menu for IP interface 1)
>> OSPF Interface 1 # aindex 0              (Attach network to backbone index)
```

```
>> OSPF Interface 1 # enable                        (Enable the backbone interface)
```

7. ネットワークインタフェースをトランジットエリアに接続します。

```
>> OSPF Interface 1 # ../if 2              (Select OSPF menu for IP interface 2)
>> OSPF Interface 2 # aindex 1           (Attach network to transit area index)
>> OSPF Interface 2 # enable                (Enable the transit area interface)
```

8. 仮想リンクを設定します。

   本ステップで設定する nbr ルータ ID は、ステップ 2 でスイッチ B に設定したルータ ID と同じである必要があります。

```
>> OSPF Interface 2 # ../virt 1                  (Specify a virtual link number)
>> OSPF Virtual Link 1 # aindex 1     (Specify the transit area for the virtual link)
>> OSPF Virtual Link 1 # nbr 10.10.14.1     (Specify the router ID of the recipient)
>> OSPF Virtual Link 1 # enable                        (Enable the virtual link)
```

9. 設定変更を適用、保存します。

```
>> OSPF Interface 2 # apply                                    (Apply all changes)
>> OSPF Interface 2 # save                                     (Save all changes)
```

スイッチ B の仮想リンクに対する OSPF の設定

1. OSPF エリアに接続する各ネットワークに IP インタフェースを設定します。

   スイッチ B には IP インタフェースが 2 つ必要です。10.10.12.0/24 のトランジットエリアネットワークに 1 つ、10.10.24.0/24 のスタブエリアネットワークに 1 つです。

```
>> # /cfg/l3/if 1                               (Select menu for IP interface 1)
>> IP Interface 1 # addr 10.10.12.2    (Set IP address on transit area network)
>> IP Interface 1 # mask 255.255.255.0    (Set IP mask on transit area network)
>> IP Interface 1 # enable                              (Enable IP interface 1)
>> IP Interface 1 # ../if 2                    (Select menu for IP interface 2)
>> IP Interface 2 # addr 10.10.24.1       (Set IP address on stub area network)
>> IP Interface 2 # mask 255.255.255.0       (Set IP mask on stub area network)
>> IP Interface 2 # enable                              (Enable IP interface 2)
```

2. ルータ ID を設定します。

   仮想リンクを形成するときにはルータ ID が必要です。このルータ ID は、スイッチ A の仮想ネイバ(nbr)に指定した ID と同じである必要があります。

```
>> IP Interface 2 # /cfg/l3/rtrid 10.10.14.1             (Set static router ID)
```

3. OSPF を有効にします。

```
>> IP# /cfg/l3/ospf/on
```

4. バックボーンを定義します。

   次に示すように、仮想リンクの非バックボーン側にバックボーンインデックスを設定する必要があります。

```
>> Open Shortest Path First # aindex 0       (Select the menu for area index 0)
>> OSPF Area (index) 0 # areaid 0.0.0.0       (Set the area ID for OSPF area 0)
>> OSPF Area (index) 0 # enable                                (Enable the area)
```

5. トランジットエリアを定義します。

```
>> OSPF Area (index) 0 # ../aindex 1             (Select menu for area index 1)
>> OSPF Area (index) 1 # areaid 0.0.0.1       (Set the area ID for OSPF area 1)
>> OSPF Area (index) 1 # type transit            (Define area as transit type)
>> OSPF Area (index) 1 # enable                                (Enable the area)
```

6. スタブエリアを定義します。

```
>> OSPF Area (index) 1 # ../aindex 2         (Select the menu for area index 2)
```

```
>> OSPF Area (index) 2 # areaid 0.0.0.2       (Set the area ID for OSPF area 2)
>> OSPF Area (index) 2 # type stub                  (Define area as stub type)
>> OSPF Area (index) 2 # enable                                (Enable the area)
```

7. **ネットワークインタフェースをバックボーンに接続します。**

```
>> OSPF Area (index) 2 # ../if 1          (Select OSPF menu for IP interface 1)
>> OSPF Interface 1 # aindex 1          (Attach network to transit area index)
>> OSPF Interface 1 # enable              (Enable the transit area interface)
```

8. **ネットワークインタフェースをトランジットエリアに接続します。**

```
>> OSPF Interface 1 # ../if 2            (Select OSPF menu for IP interface 2)
>> OSPF Interface 2 # aindex 2            (Attach network to stub area index)
>> OSPF Interface 2 # enable                (Enable the stub area interface)
```

9. **仮想リンクを設定します。**

   ここで設定する nbr **ルータ** ID **は、スイッチ** A **のステップ** 2 **で設定したルータ** ID **と同じある必要があります。**

```
>> OSPF Interface 2 # ../virt 1                (Specify a virtual link number)
>> OSPF Virtual Link 1 # aindex 1     (Specify the transit area for the virtual link)
>> OSPF Virtual Link 1 # nbr 10.10.10.1     (Specify the router ID of the recipient)
>> OSPF Virtual Link 1 # enable                       (Enable the virtual link)
```

10. **設定変更を適用、保存します。**

```
>> OSPF Interface 2 # apply                                  (Apply all changes)
>> OSPF Interface 2 # save                                    (Save all changes)
```

その他の仮想リンクオプション

- **仮想リンクを複数設定することにより、冗長経路を使用できます。**
- **仮想リンクのエンドポイントのみ設定されます。エンドポイント間にルーティング可能な経路がある限り、仮想リンクの経路はエリア内で複数のルータを横断できます。**

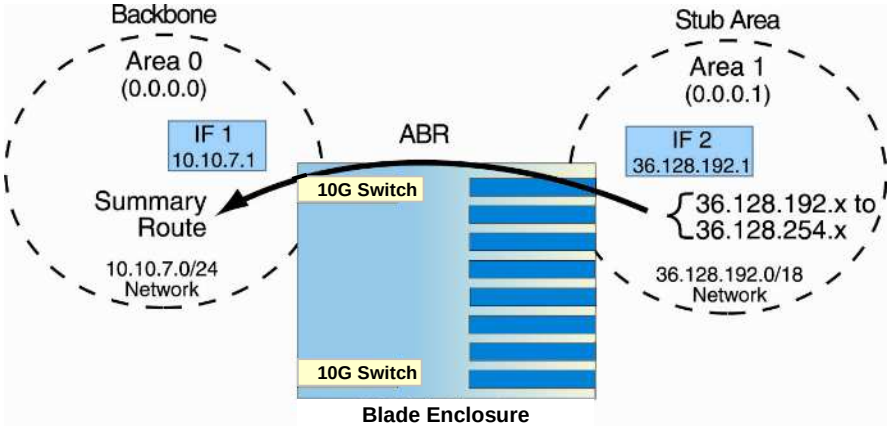
例 3：ルート集約

デフォルトでは、ABR **は一方のエリアからもう一方のエリアにすべてのネットワークアドレスを通知します。ルート集約は、通知するアドレスを集約したり、ネットワークの複雑性を低減するために、ルート集約を利用できます。**

あるエリア内のネットワーク IP **アドレスを連続したサブネットレンジに割り当てると、**ABR **を設定して、そのエリア内の個別** IP **アドレスすべてを含む** 1 **つのサマリルートを通知できます。**

次の例に、エリア 1**（スタブエリア）からエリア** 0**（バックボーン）に至るサマリルートを示します。サマリルートは、**36.128.200.0～36.128.200.255 **の範囲のルートを除いた、**36.128.192.0～36.128.254.255 **の全** IP **アドレスが含まれます。**

図22　ルート集約



注：hide **オプションを使用することにより、通知しないアドレスレンジを指定することができます。この例では、**36.128.200.0～36.128.200.255 **の範囲のルートは非公開となっています。**

図に従って、スイッチ A**、スイッチ** B **の** OSPF **を設定する手順は次のとおりです。**

1. OSPF **エリアに接続する各ネットワークの** IP **インタフェースを設定します。**

```
>> # /cfg/l3/if 1                              (Select menu for IP interface 1)
>> IP Interface 1 # addr 10.10.7.1          (Set IP address on backbone network)
>> IP Interface 1 # mask 255.255.255.0        (Set IP mask on backbone network)
>> IP Interface 1 # ena                                 (Enable IP interface 1)
>> IP Interface 1 # ../if 2                   (Select menu for IP interface 2)
>> IP Interface 2 # addr 36.128.192.1      (Set IP address on stub area network)
>> IP Interface 2 # mask 255.255.192.0        (Set IP mask on stub area network)
>> IP Interface 2 # ena                                 (Enable IP interface 2)
```

2. OSPF **を有効にします。**

```
>> IP Interface 2 # /cfg/l3/ospf/on
```

3. **バックボーンを定義します。**

```
>> Open Shortest Path First # aindex 0           (Select menu for area index 0)
>> OSPF Area (index) 0 # areaid 0.0.0.0        (Set the ID for backbone area 0)
>> OSPF Area (index) 0 # type transit         (Define backbone as transit type)
>> OSPF Area (index) 0 # enable                              (Enable the area)
```

4. **スタブエリアを定義します。**

```
>> OSPF Area (index) 0 # ../aindex 1             (Select menu for area index 1)
>> OSPF Area (index) 1 # areaid 0.0.0.1       (Set the area ID for OSPF area 1)
>> OSPF Area (index) 1 # type stub                   (Define area as stub type)
>> OSPF Area (index) 1 # enable                              (Enable the area)
```

5. **ネットワークインタフェースをバックボーンに接続します。**

```
>> OSPF Area (index) 1 # ../if 1          (Select OSPF menu for IP interface 1)
>> OSPF Interface 1 # aindex 0               (Attach network to backbone index)
>> OSPF Interface 1 # enable                   (Enable the backbone interface)
```

6. **ネットワークインタフェースをスタブエリアに接続します。**

```
>> OSPF Interface 1 # ../if 2             (Select OSPF menu for IP interface 2)
>> OSPF Interface 2 # aindex 1              (Attach network to stub area index)
>> OSPF Interface 2 # enable                   (Enable the stub area interface)
```

7. **集約するアドレスの開始アドレスとアドレスレンジのマスクを指定して、ルート集約を設定します。**

```
>> OSPF Interface 2 # ../range 1                (Select menu for summary range)
>> OSPF Summary Range 1 # addr 36.128.192.0   (Set base IP address of summary range)
>> OSPF Summary Range 1 # mask 255.255.192.0    (Set mask address for summary range)
>> OSPF Summary Range 1 # aindex 0         (Inject summary route into backbone)
>> OSPF Summary Range 1 # enable                          (Enable summary range)
```

8. hide **コマンドを使用して、バックボーンに通知しないアドレスレンジを設定します。**

```
>> OSPF Interface 2 # ../range 2                (Select menu for summary range)
>> OSPF Summary Range 2 # addr 36.128.200.0               (Set base IP address)
>> OSPF Summary Range 2 # mask 255.255.255.0                 (Set mask address)
>> OSPF Summary Range 2 # hide enable            (Hide the range of addresses)
```

9. **設定変更を適用、保存します。**

```
>> OSPF Summary Range 2 # apply                              (Apply all changes)
>> OSPF Summary Range 2 # save                               (Save all changes)
```

OSPF **設定の確認**

以下のコマンドを使用して、スイッチの OSPF **設定を確認します。**

- /info/l3/ospf/general
- /info/l3/ospf/nbr
- /info/l3/ospf/dbase/dbsum
- /info/l3/ospf/routes
- /stats/l3/route

コマンドの詳細については、コマンドリファレンスガイドを参照してください。

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。

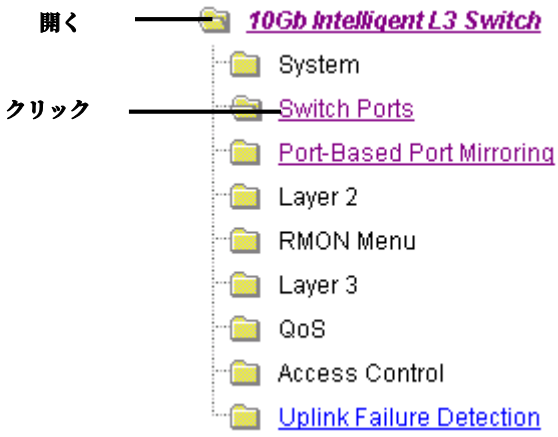
```
>> /cfg/port 20/rmon                    (Select Port 20 RMON)
>> Port 20 RMON# ena                    (Enable RMON)
>> Port 20 RMON# apply                  (Make your changes active)
>> Port 20 RMON# save                   (Save for restore after reboot)
```

2. **ポートの** RMON **統計データを確認します。**

```
>> /stats/port 20                                (Select Port 20 Stats)
>> Port Statistics# rmon
------------------------------------------------------------------------
RMON statistics for port 20:
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）。



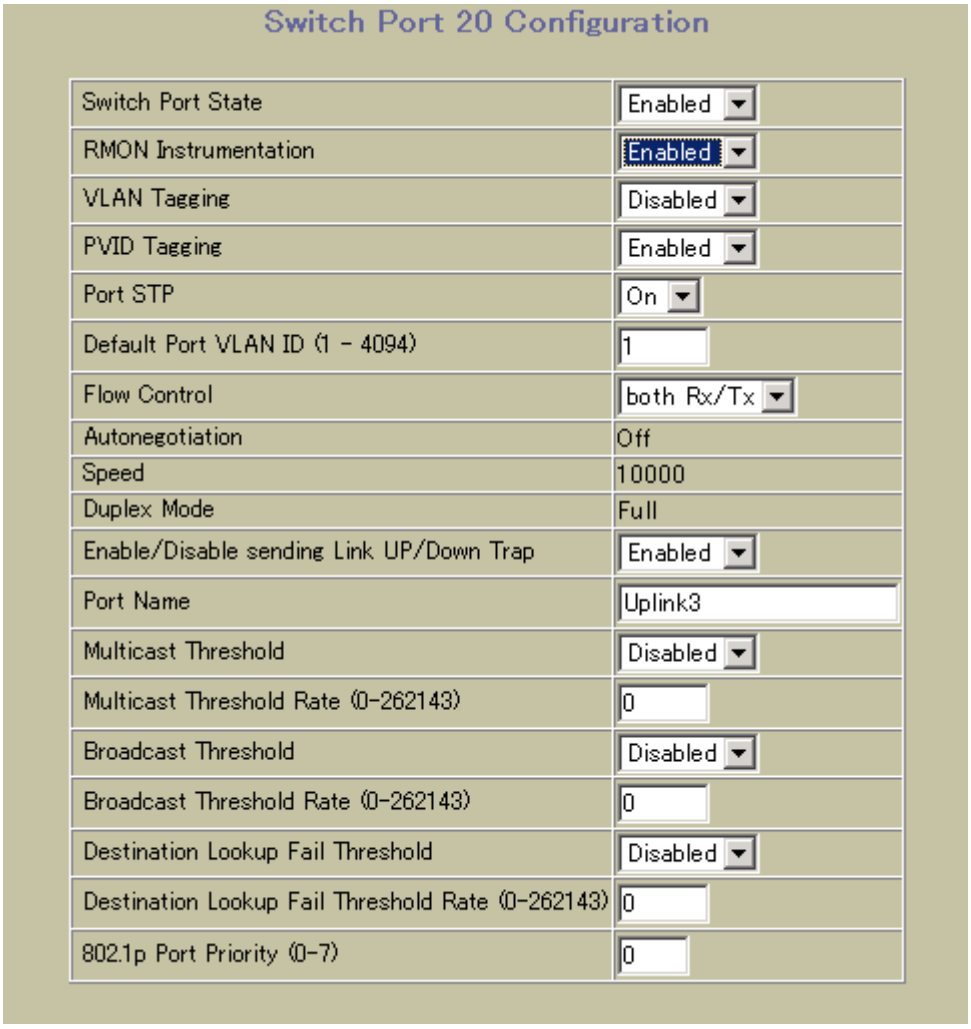
   c. ポートを選択します。

Switch Ports Configuration

Switch Port	State	VLAN Tagging	Default PVID	PVID tagging	Multicast Threshold	Broadcast Threshold	Destination Lookup Fail Threshold	802.1p Priority
1	disabled	disabled	1	enabled	disabled	disabled	disabled	0
2	disabled	disabled	1	enabled	disabled	disabled	disabled	0
3	disabled	disabled	1	enabled	disabled	disabled	disabled	0
4	disabled	disabled	1	enabled	disabled	disabled	disabled	0
5	disabled	disabled	1	enabled	disabled	disabled	disabled	0
6	disabled	disabled	1	enabled	disabled	disabled	disabled	0
7	disabled	disabled	1	enabled	disabled	disabled	disabled	0
8	disabled	disabled	1	enabled	disabled	disabled	disabled	0
9	enabled	disabled	1	enabled	disabled	disabled	disabled	0
10	disabled	disabled	1	enabled	disabled	disabled	disabled	0
11	disabled	disabled	1	enabled	disabled	disabled	disabled	0
12	disabled	disabled	1	enabled	disabled	disabled	disabled	0
13	disabled	disabled	1	enabled	disabled	disabled	disabled	0
14	disabled	disabled	1	enabled	disabled	disabled	disabled	0
15	disabled	disabled	1	enabled	disabled	disabled	disabled	0
16	disabled	disabled	1	enabled	disabled	disabled	disabled	0
17	enabled	disabled	4095	disabled	disabled	disabled	disabled	0
18	enabled	disabled	1	enabled	disabled	disabled	disabled	0
19	enabled	disabled	1	enabled	disabled	disabled	disabled	0
20	enabled	disabled	1	enabled	disabled	disabled	disabled	0
21	enabled	disabled	1	enabled	disabled	disabled	disabled	0

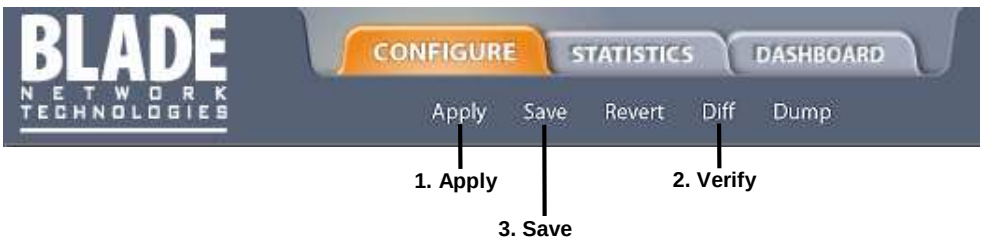
クリック

d. **ポートの RMON を有効にします。**



e. Submit **をクリックします。**

2. **設定を適用、確認、保存します。**



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（1〜16, 18〜21）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 21/rmon                    (Select Port 21 RMON)
>> Port 21# ena                         (Enable RMON)
>> Port 21 RMON# apply                  (Make your changes active)
>> Port 21 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 1.3.6.1.2.1.2.2.1.1.21
>> RMON History 1# rbnum 30
>> RMON History 1# intrval 120
>> RMON History 1# owner "Owner_History_1"
```

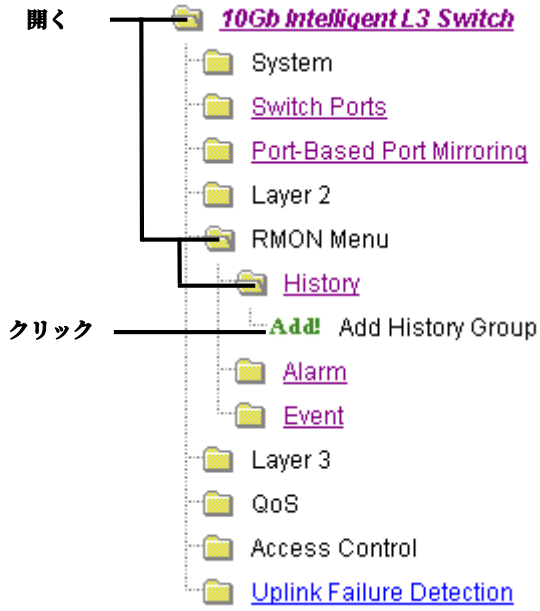
3. 設定を適用、保存します。

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

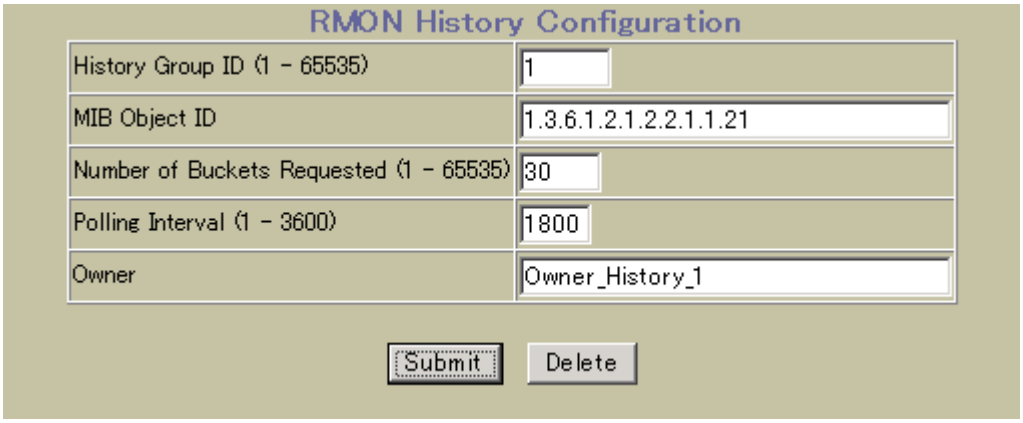
この設定では、ポート 21 をモニタする RMON History グループを生成します。2 分毎にデータサンプルを取り出し、30 のリクエストバケットの 1 つに入れます。30 サンプルまで収集すると、最初のバケットから、新しいサンプルを古いサンプルに上書きします。データの確認には SNMP を用います。

RMON History の設定（BBI の例）

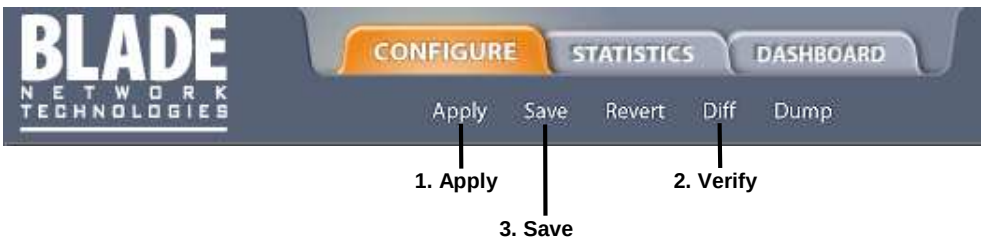
1. RMON History グループを設定します。
   a. CONFIGURE ボタンをクリックします。
   b. Switch フォルダを開き、RMON > History > Add History Group を選択します。



   c. RMON History グループパラメータを設定します。



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



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。

1-250 = IF 1-250
  251 = port 1
  252 = port 2
  …
  271 = port 21

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 1.3.6.1.2.1.2.2.1.10.270
>> 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"
```

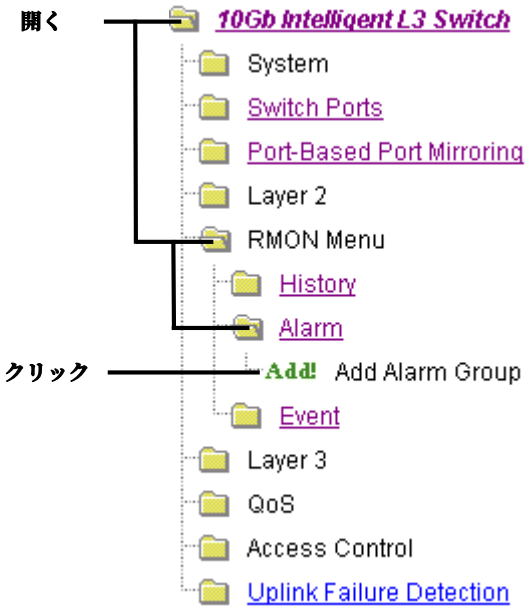
2. 設定を適用、保存します。

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

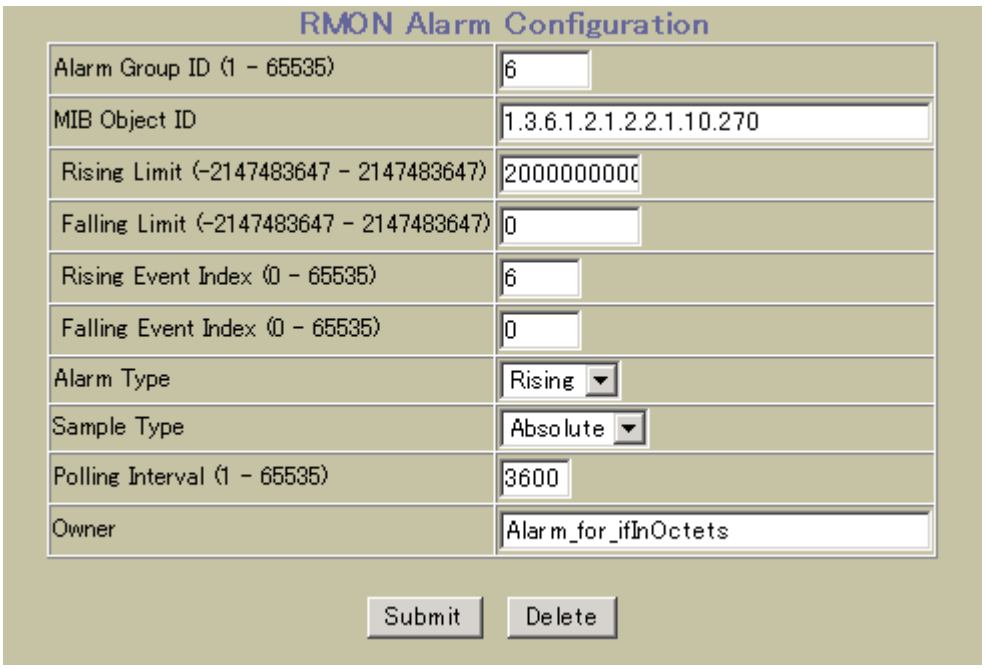
スイッチで icmpInEchos をチェックする RMON アラームを 1 分毎に生成します。60 秒間で統計量が 200 を超えると、イベントインデックス 5 をトリガするアラームが発生します。

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。

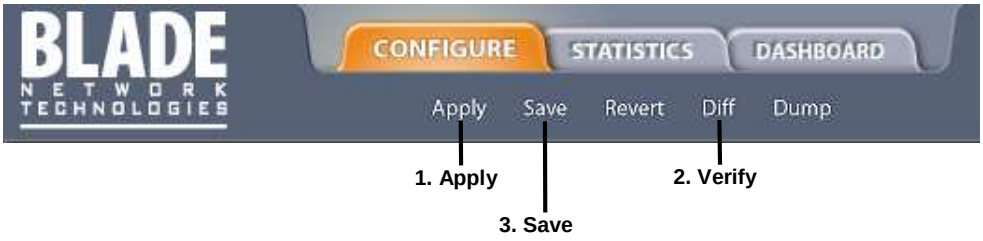


c. ポート 20 で 1 時間毎に `ifInOctets` をチェックする RMON アラームグループパラメータを設定します。立上りしきい値 (Rising Limit) の 20 億と立上りイベントインデックス (Rising Event Index) の 6 を入力します。この設定では、ポート 20 で 1 時間毎に `ifInOctets` をチェックする RMON アラームを生成します。統計量が 20 億を超えると、イベントインデックス 6 をトリガするアラームが発生します。



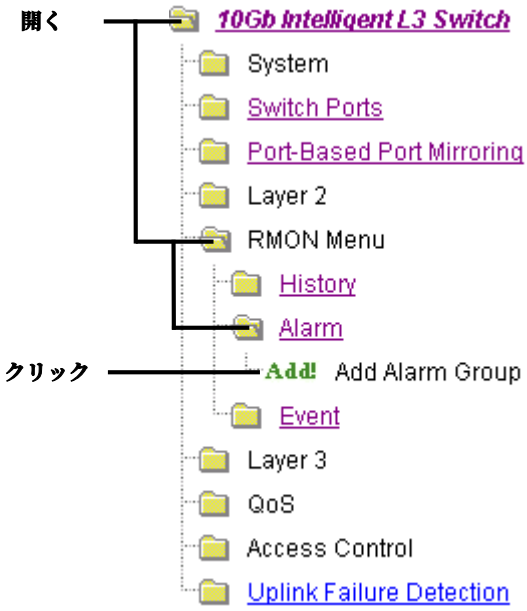
d. Submit をクリックします。

2. 設定を適用、確認、保存します。

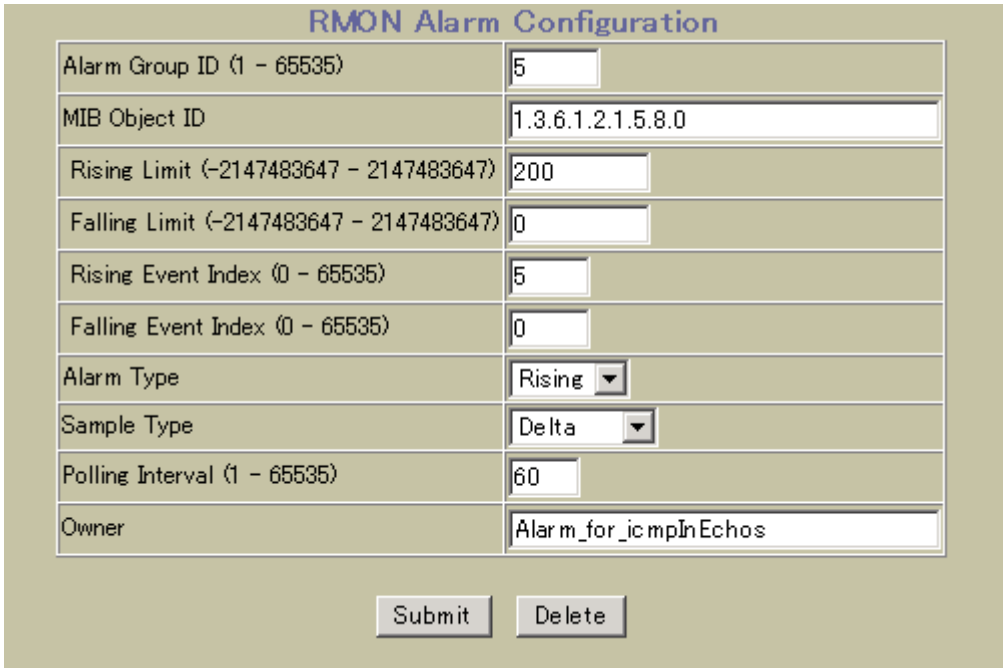


RMON アラームの設定（BBI の例 2）

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。

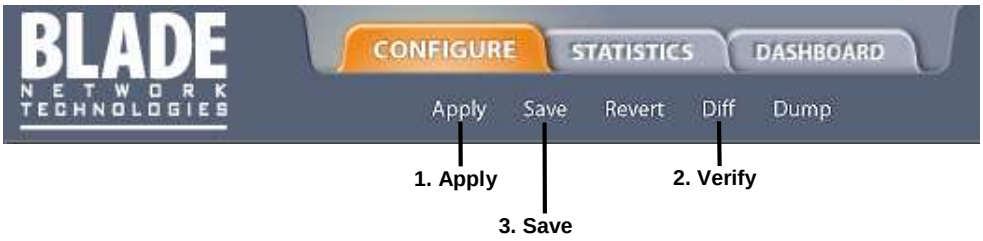


   c. ポーリング間隔 60、立上りしきい値 (Rising Limit) 200、立上りイベントインデックス (Rising Event Index) 5 で `icmpInEchos` をチェックする RMON アラームグループパラメータを設定します。この設定では、スイッチで 1 分毎に `icmpInEchos` をチェックする RMON アラームを生成します。60 秒以内に統計量が 200 を超えると、イベントインデックス 5 をトリガするアラームが発生します。



   d. Submit をクリックします。

2. 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"
```

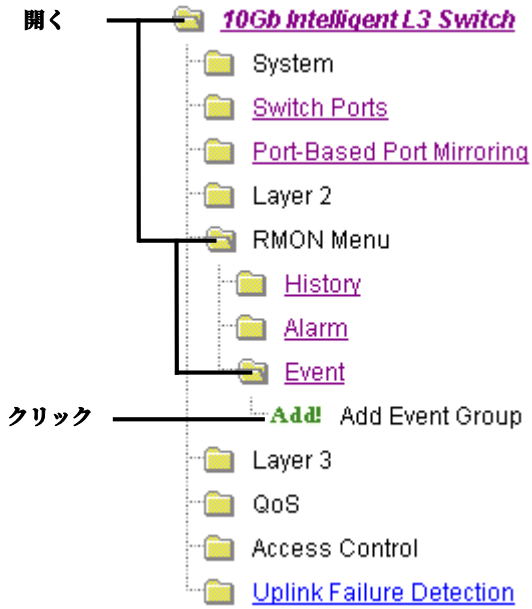
2. 設定を適用、保存します。

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

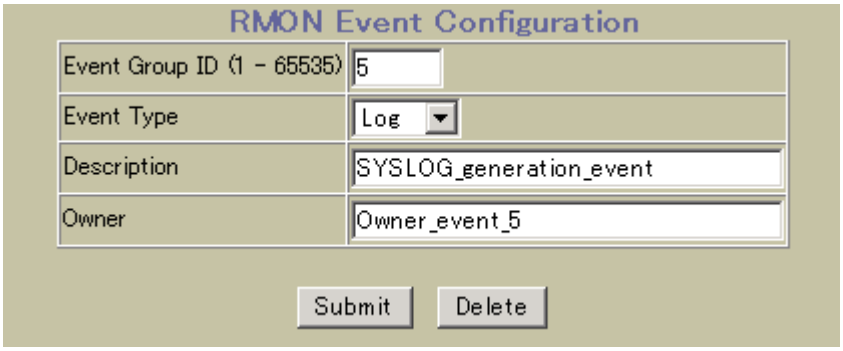
アラームが RMON イベントをトリガする毎にシスログメッセージを送信するイベントを生成します。

RMON イベントの設定（BBI の例 1）

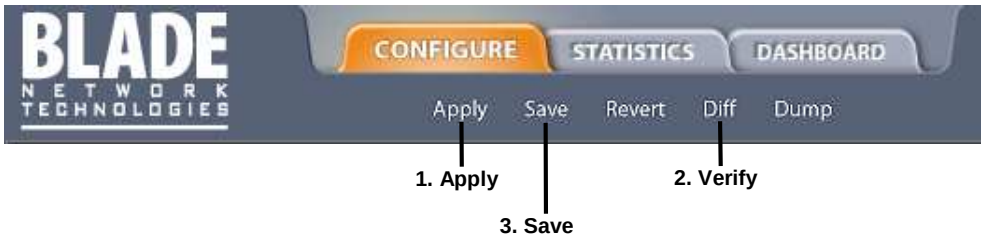
1. RMON イベントグループを設定します。
   a. CONFIGURE ボタンをクリックします。
   b. Switch フォルダを開き、RMON > Event > Add Event Group を選択します。



   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。



   d. Submit をクリックします。
2. 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 と Virtual Router Redundancy Protocol (VRRP) について説明します。

Uplink Failure Detection

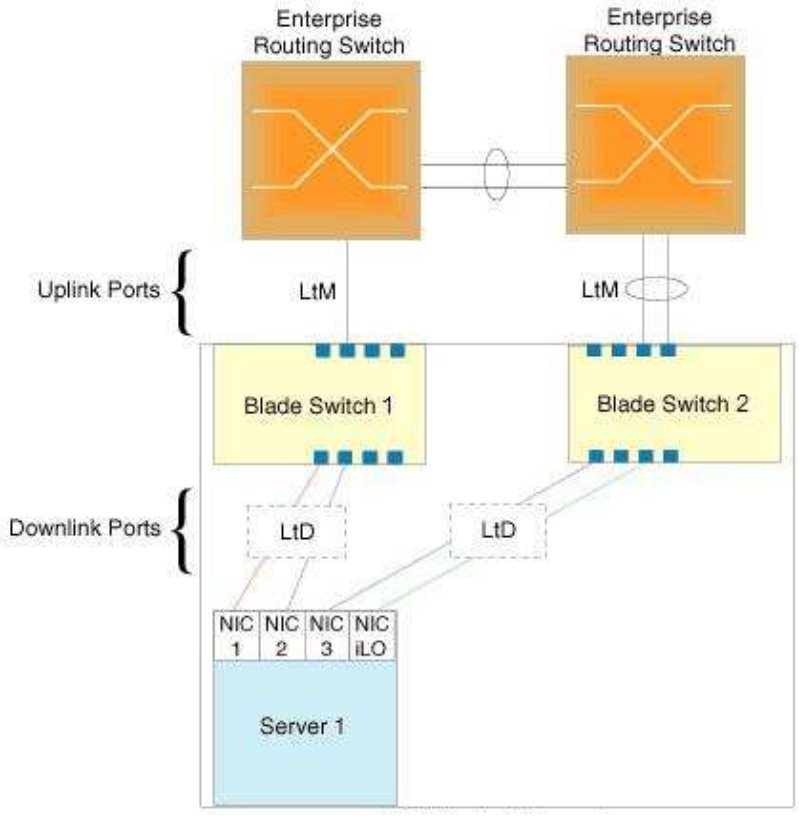
CPU ブレードのネットワークアダプタチーミングをサポートするため、Uplink Failure Detection (UFD) があります。

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23　スイッチの Uplink Failure Detection



Blade Enclosure

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（18～21）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（18～21）を入れることができますが、ダウンリンクポート（1～16）を入れることはできません。
  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（18～21）を入れることはできません。

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 19                          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 19 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 18、19 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。

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（18～21）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 19   (Monitor uplink port 19)
```

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 18 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（18～21）のトランクグループを生成します。

```
>> Main# /cfg/trunk 2                    (Create trunk group 2)
>> Trunk group 2# ena                    (Enable trunk group 2)
>> Trunk group 2# add 18                 (Add port 18 to trunk group 2)
>> Trunk group 2# add 19                 (Add port 19 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)
```

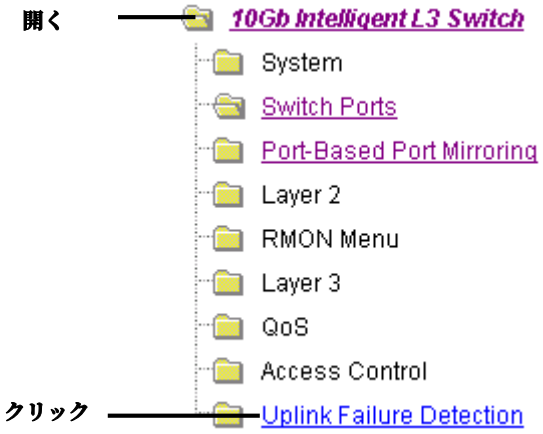
4. UFD をオンにします。

```
>> 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)
```

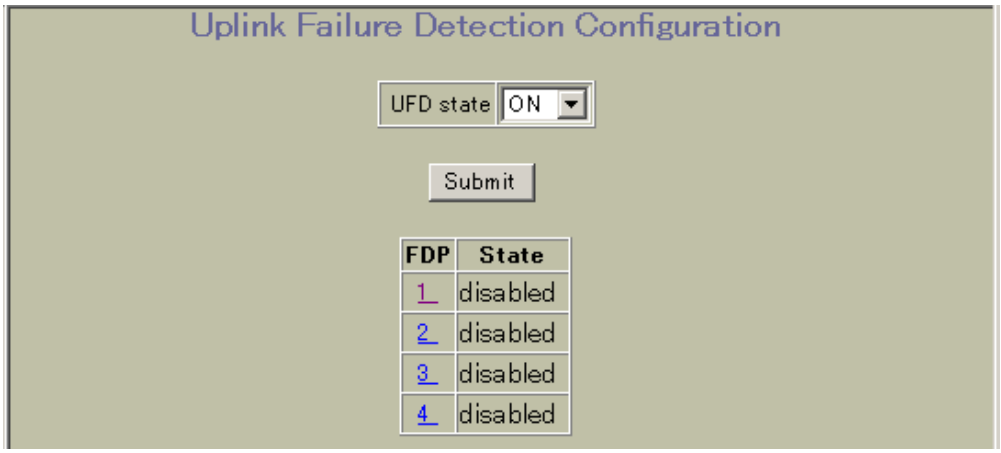
トランクグループ 2 でリンク故障かスパニングツリーブロックが発生すると、スイッチ 2 はポート 1、ポート 2 を無効にします。

UFD の設定（BBI の例）

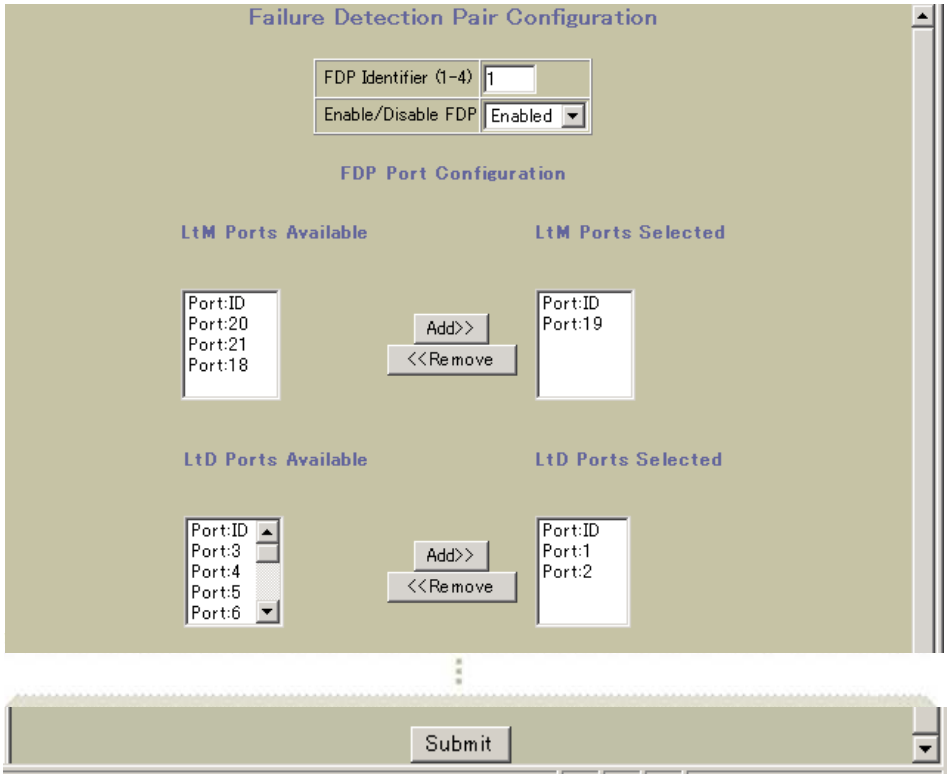
1. アップリンク故障検出を設定します。
   a. CONFIGURE ボタンをクリックします。
   b. Switch フォルダを開き、Uplink Failure Detection を選択します（フォルダではなく、下線が引かれたフォルダ名をクリックします）。



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

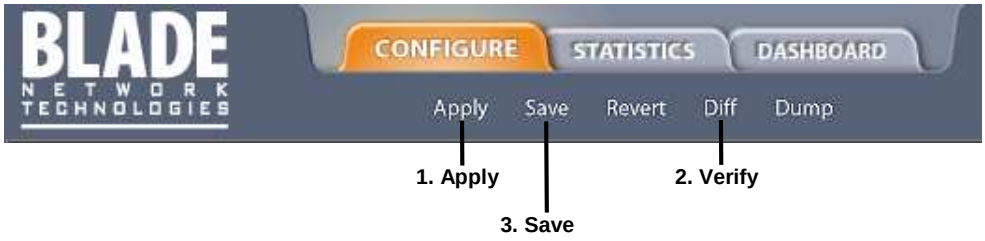


d. FDP を有効にします。LtM Ports Available リストからポートを選択し、Add をクリックしてポートを LtM に追加します。LtD Ports Available リストからポートを選択し、Add をクリックしてポートを LtD に追加します。



e. Submit をクリックします。

2. 設定を適用、確認、保存します。



VRRP の概要

高可用性のネットワークトポロジでは、ネットワークに single point-of-failure(SPOF)が生じたり、SPOF がネットワークの他の部分に影響を与えることはありません。つまり、1 つのデバイスで障害が発生しても、ネットワークの動作は継続することを意味します。これを実現するためには、すべての重要なネットワークコンポーネントを冗長化する必要があります。

VRRP では LAN 内に冗長ルータ構成が可能で、ホストに対して代替の経路を提供し、ネットワーク内の SPOF が解消されます。VRRP が稼動している各ルーティングデバイスは、同じ仮想ルータ IP アドレスと ID 番号を持ちます。プライオリティに基づいて、仮想ルータの内 1 台がマスタとしてに選出され、共有する仮想ルータ IP アドレスの制御を行います。マスタに障害が発生した場合、バックアップの 1 台が仮想ルータ IP アドレスの制御を受け継ぎ、トラフィックを処理します。

VRRP では、仮想インタフェースルータ(VIR)によって、2 台の VRRP ルータがルータ間の 1 つの IP インタフェースを共用することができます。VIR は、アップストリームルータに各サーバにアクセスする 1 つの宛先 IP(DIP)を提供し、サーバブレードには仮想デフォルトゲートウェイを提供します。

VRRP コンポーネント

VRRP を実行する各ルータを VRRP ルータといいます。

仮想ルータ

2 台以上の VRRP ルータで仮想ルータを構成できます(RFC 2338)。各 VRRP ルータは 1 つ以上の仮想ルータを実行できます。各仮想ルータには、ユーザが設定した仮想ルータ ID(VRID)と IP アドレスで構成されます。

仮想ルータの MAC アドレス

VRID は仮想ルータの MAC アドレスを作成するために使用されます。仮想ルータの MAC アドレスの上位 5 オクテットには、RFC 2338 に定義された値(00-00-5E-00-01)が入ります。VRID は下位オクテットに入ります。

owner と renter

仮想ルータ内で 1 台の VRRP ルータだけが、IP アドレスの owner として設定できます。このルータでは、仮想ルータ IP アドレスを、そのルータの実インタフェースアドレスとしてもちます。このルータは、ICMP ping、TCP 接続など、この仮想ルータの IP アドレスに向けられたパケットに応答します。

VRRP ルータが IP アドレスの owner になるための要件はありません。ほとんどの VRRP の構築では IP アドレスの owner の実装を選択しません。本章では、IP アドレスの owner ではない VRRP ルータを renter と呼びます。

マスタとバックアップ仮想ルータ

仮想ルータの内、1 台の VRRP ルータがマスタ仮想ルータとして選択されます。選択プロセスについては、「マスタ VRRP ルータの選択」を参照してください。

> **注**: IP アドレス owner を使用している場合、その仮想ルータがマスタになります。

マスタは仮想ルータに送信されたパケットを転送します。また、仮想ルータの IP アドレスに送信された ARP 要求にも応答します。また、マスタは自身が稼動中であることと、プライオリティを他の VRRP ルータに定期的に知らせます。

仮想ルータ内でマスタに選択されていない VRRP ルータをバックアップ仮想ルータといいます。マスタ仮想ルータで障害が発生した場合、バックアップ仮想ルータの内 1 台がマスタとなり、処理を受け継ぎます。

仮想インタフェースルータ(VIR)

レイヤ 3 では、仮想インタフェースルータ(VIR)により、2 台の VRRP ルータが 1 つの IP アドレスを共有できます。VIR からアップストリームルータに対し単一の宛先 IP(DIP)や、仮想デフォルトゲートウェイを提供できます。

> **注**：各 VIR に 1 つの IP インタフェースを、各 IP インタフェースに 1 つの VLAN を割り当てる必要があります。ある VLAN 内のすべてのポートがリンクアップしていない場合、その VLAN の IP インタフェースは停止しています。また、ある VIR の IP インタフェースが停止している場合、その VIR は INIT 状態になります。

VRRP の動作

マスタ仮想ルータのみが ARP 要求に応答します。したがって、アップストリームルータはマスタのみにパケットを転送します。マスタは ICMP ping 要求にも応答します。一方、バックアップはトラフィックの転送も、ARP 要求への応答も行いません。

マスタが利用できなくなると、バックアップがマスタになって、パケット転送と ARP 要求への応答を受け継ぎます。

マスタ VRRP ルータの選択

各 VRRP ルータに 1～254 の優先順位を設定します。選定プロセスにより、VRRP ルータからマスタ（プライオリティが最も高い VRRP ルータ）が決まります。

マスタは IP マルチキャストアドレスに定期的に通知を出します。その通知を受信している限り、バックアップはバックアップ状態のままです。バックアップは、3 回の通知送信間隔のあいだに通知を受信しない場合、選定プロセスを開始して、どの VRRP ルータのプライオリティが一番高く、マスタを受け継ぐかを決定します。

バックアップは、現在のマスタよりプライオリティが高いと判断した場合、マスタに代わって自分がマスタになります（そうしない設定になっている場合は除きます）。交代すると、バックアップがマスタの役割を受け継ぎ、通知の送信を開始します。それまでのマスタはバックアップのプライオリティが高いことを確認して、マスタとしての機能を停止します。

バックアップルータは、次の 2 つのうちのいずれかの理由で通知の受信ができなくなります。マスタがダウンしたか、もしくは、マスタとバックアップの間のすべての通信リンクが停止したときです。

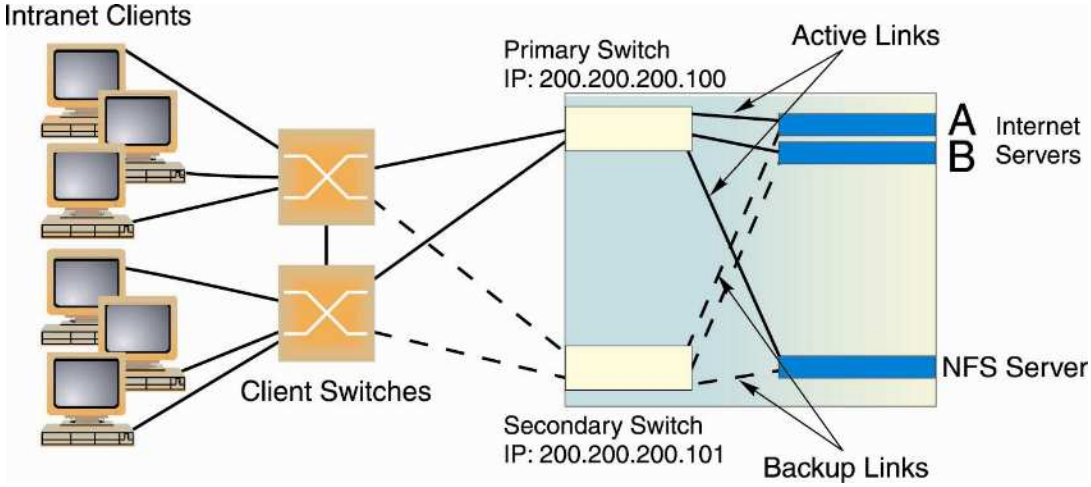
> **注**：マスタが正常でも、マスタとバックアップ間が不通になった場合、仮想ルータ内のマスタが 2 台になります。これを防止するためには、仮想ルータを形成するスイッチ間で冗長リンクにします。

フェイルオーバ方法

インターネットにてサービスの可用性が非常に注目されているため、サービスプロバイダは、冗長構成にして、アプリケーションスイッチなどのインターネットトラフィック制御デバイスの展開を拡大しています。従来、冗長構成は、一方のスイッチがアクティブで、他方のスイッチがスタンバイモードの、ホットスタンバイ構成をとっています。

VRRP 未対応のホットスタンバイ構成を次の図に示します。

図24　VRRP 未対応のホットスタンバイ構成



ホットスタンバイ構成は、single point-of-failure (SPOF)を解消することにより可用性が向上しますが、1 台のアプリケーションスイッチが障害が発生するまで待機状態で使用されないため、サービスプロバイダは、ネットワーク資源の利用が効率的でないという見方を強めています。サービスプロバイダがベンダに求めているのは、正常なデバイスすべてがトラフィックを処理してスループットを向上し、ユーザ応答時間を短縮し、冗長構成をサポートする装置です。

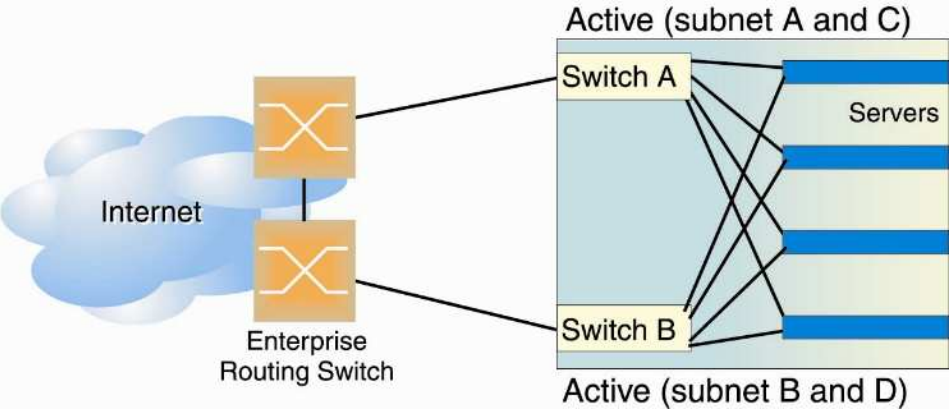
本スイッチの高可用性の構成は、VRRP に基づいています。本スイッチでは高可用性を実現する VRRP のアクティブ－アクティブ構成をサポートします。

アクティブ－アクティブ冗長構成

次の図に示すアクティブ－アクティブ冗長構成の場合、2 台のスイッチが互いに冗長性を提供し、2 台が同時にアクティブです。各スイッチが別々のサブネットでトラフィックを処理します。一方で障害が発生すると、正常なスイッチがすべてのサブネットのトラフィックを処理します。

次の図にアクティブ－アクティブ構成の例を示します。

図25　アクティブ－アクティブ冗長構成



VRRP の拡張

この節では、本スイッチのソフトウェアに実装されている VRRP 拡張機能について説明します。

VRRP ルータプライオリティのトラッキング

本スイッチは、現在の状態に基づいて VRRP ルータのプライオリティを動的に変更するトラッキング機能をサポートしています。トラッキングの目的は、可能な限り、ある LAN 上のマスタ仮想ルータを同じスイッチに集中させることです。トラッキングにより、選択したスイッチが最適なネットワークパフォーマンスを提供できます。トラッキングを使用する場合、preemption を有効にする必要があります。

本スイッチでは、次に示すパラメータでトラッキングを使用できます。

表23 VRRP トラッキングパラメータ

パラメータ	説明
スイッチ上でアクティブ(稼動)となっている IP インタフェースの数 /cfg/l3/vrrp/track/ifs	使用可能な経路を最も多く持つ仮想ルータをマスタとして選択するのに役立ちます。（同じ VLAN 上にアクティブポートが少なくとも 1 つある場合、IP インタフェースはアクティブと見なします。）このパラメータは、仮想インタフェースルータ内の VRRP ルータのプライオリティに影響します。
同じ VLAN 上のアクティブポート数 /cfg/l3/vrrp/track/ports	使用可能なポートを最も多く持つ仮想ルータをマスタとして選択するのに役立ちます。このパラメータは、仮想インタフェースルータ内の VRRP ルータのプライオリティに影響します。
スイッチ上でマスタモードの仮想ルータ数 /cfg/l3/vrrp/track/vrs	特定のクライアント-サーバペアのトラフィックが同じスイッチで処理されるようにして、ルーティング効率を向上するのに有効です。このパラメータは、仮想インタフェースルータ内の VRRP ルータのプライオリティに影響します。

トラッキングの各パラメータには、ユーザ設定可能な重み付けができます。トラッキングの各パラメータが増減すると、各パラメータの重み付けに従って、VRRP ルータのプライオリティが増減します。スタンバイのプライオリティが現在のマスタより高くなると、スタンバイがマスタの役割を受け継ぎます。

VRRP プライオリティをトラッキングする設定例については、「スイッチのトラッキング設定」を参照してください。

仮想ルータの配置

仮想ルータを配置する際のネットワークトラブルを防止するため、本節で説明する次の項目を確認してください。

- VRRP 仮想ルータ ID の割当て
- スイッチのトラッキング設定

VRRP 仮想ルータ ID の割当て

スイッチでフェイルオーバが有効になっている場合、ソフトウェアアップグレードプロセス時、VRRP 仮想ルータ ID が自動的に割り当てられます。アップグレード後、仮想ルータを設定する場合、仮想ルータ ID 番号(/cfg/l3/vrrp/vr #/vrid)を割り当てる必要があります。仮想ルータ ID は 1～255 の任意の番号に設定できます。

スイッチのトラッキング設定

トラッキング設定は、ユーザによる優先付けとネットワーク環境に大きく依存します。図 25 で示した構成で、ネットワークで以下の動作を想定します。

- 初期設定で、マスタルータはスイッチ A とします。
- スイッチ A がマスタで、アクティブサーバがスイッチ B より 1 台少ない場合でも、マスタはスイッチ A とします。
  新しいマスタに交代し、処理中のすべてのコネクションを切断するよりも、稼動しているサーバを 1 台停止するほうが影響が少ないためです。
- スイッチ A がマスタで、アクティブサーバがスイッチ B より 2 台以上少ない場合、スイッチ B をマスタにします。
- スイッチ B がマスタで、スイッチ A でサーバが復旧しても（サーバが 1 台だけ少ないか同数）、マスタはスイッチ B とします。
- スイッチ B がマスタで、アクティブサーバがスイッチ A より 1 台少なくなると、スイッチ A をマスタにします。

スイッチを次のように設定することで、上記の動作を実現できます。

1. スイッチ A のプライオリティを 101 に設定します。
2. スイッチ B のプライオリティをデフォルトの 100 のままにします。
3. 両スイッチで、ポート(ports)、インタフェース(ifs)、または仮想ルータ(vr)に基づいてトラッキングを有効にします。トラッキングパラメータは、ネットワークの構成に基づいて、任意に組み合わせることができます。

注：トラッキングパラメータの設定に簡単な方法はありません。目標を最初に設定し、各種構成やシナリオを分析して、目標を実現するための設定を見つける必要があります。

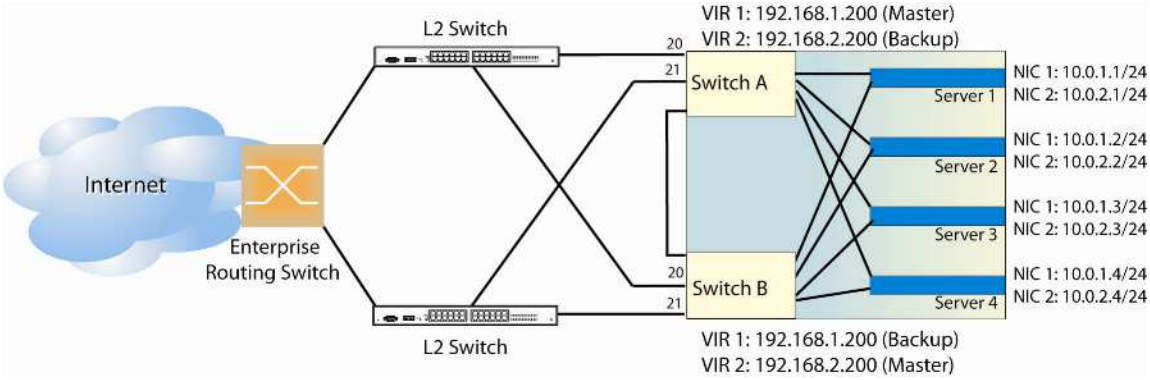
高可用性構成

本スイッチでは柔軟な冗長構成を提供できます。本節ではアクティブ－アクティブ構成について説明します。

アクティブ－アクティブ構成

次の図に、アクティブ－アクティブ構成で 2 台のスイッチを VRRP ルータとして使用する例を示します。この構成では、両方のスイッチがパケットに応答します。

図26　アクティブ－アクティブ高可用性構成



この例ではスイッチを 2 台のみ示していますが、冗長構成で使用するスイッチ数に制限はありません。LAN 内のすべての VRRP 対応スイッチでアクティブ－アクティブ構成を実装できます。

アクティブ－アクティブ構成では各 VRRP 対応スイッチは自律しています。仮想ルータ内のスイッチを同じ設定にする必要はありません。

図の例では、IP アドレス 10.0.1.1 宛のトラフィックは図の上側のレイヤ 2 スイッチを通過し、スイッチ A のポート 20 に入ります。戻りのトラフィックはデフォルトゲートウェイ 1(192.168.1.1)を使用しています。スイッチ A とレイヤ 2 スイッチ間のリンクが失敗した場合、プライオリティが高いスイッチ B がマスタになり、トラフィックはスイッチ B に転送されます。戻りのトラフィックはデフォルトゲートウェイ 2(192.168.2.1)を使用し、図の下側のレイヤ 2 スイッチを通じて転送されます。

アクティブ－アクティブの例を実装するには、スイッチを次のように設定します。

タスク 1：スイッチ A の設定（AOS CLI の例）

1. ポートを設定します。

```
/cfg/l2/vlan 10                                 (Select VLAN 10)
>> VLAN 10# ena                                 (Enable VLAN 10)
>> VLAN 10# add 20                              (Add port 20 to VLAN 10)
>> VLAN 10# ..
>> Layer 2# vlan 20                             (Select VLAN 20)
>> VLAN 20# ena                                 (Enable VLAN 20)
>> VLAN 20# add 21                              (Add port 21 to VLAN 20)
```

2. クライアントとサーバのインタフェースを設定します。

```
/cfg/l3/if 1                                              (Select interface 1)
>> IP Interface 1# addr 192.168.1.100       (Define IP address for interface 1)
>> IP Interface 1# vlan 10                      (Assign VLAN 10 to interface 1)
>> IP Interface 1# ena                                    (Enable interface 1)
>> IP Interface 1# ..
>> Layer 3# if 2                                          (Select interface 2)
>> IP Interface 2# addr 192.168.2.101       (Define IP address for interface 2)
>> IP Interface 2# vlan 20                      (Assign VLAN 20 to interface 2)
>> IP Interface 2# ena                                    (Enable interface 2)
>> IP Interface 2# ..
>> Layer 3# if 3                                          (Select interface 3)
```

```
>> IP Interface 3# addr 10.0.1.100          (Define IP address for interface 3)
>> IP Interface 3# mask 255.255.255.0      (Define subnet mask for interface 3)
>> IP Interface 3# ena                                  (Enable interface 3)
>> IP Interface 3# ..
>> Layer 3# if 4                                        (Select interface 4)
>> IP Interface 4# addr 10.0.2.101          (Define IP address for interface 4)
>> IP Interface 4# mask 255.255.255.0      (Define subnet mask for interface 4)
>> IP Interface 4# ena                                  (Enable interface 4)
```

3. **デフォルトゲートウェイを設定します。各デフォルトゲートウェイはレイヤ 2 ルータの一方を指します。**

```
/cfg/l3/gw 1                                        (Select default gateway 1)
>> Default gateway 1# addr 192.168.1.1   (Point gateway to the first L2 router)
>> Default gateway 1# ena                    (Enable the default gateway)
>> Default gateway 1# ..
>> Layer 3# gw 2                                  (Select default gateway 2)
>> Default gateway 2# addr 192.168.2.1     (Point gateway to the second router)
>> Default gateway 2# ena                    (Enable the default gateway)
```

4. VRRP **を有効にして、2 台の仮想インタフェースルータを設定します。**

```
/cfg/l3/vrrp/on                                                 (Turn VRRP on)
>> Virtual Router Redundancy Protocol# vr 1          (Select virtual router 1)
>> VRRP Virtual Router 1# vrid 1                              (Set VRID to 1)
>> VRRP Virtual Router 1# if 1                              (Set interface 1)
>> VRRP Virtual Router 1# addr 192.168.1.200              (Define IP address)
>> VRRP Virtual Router 1# ena                        (Enable virtual router 1)
>> VRRP Virtual Router 1# ..                         (Enable virtual router 1)
>> Virtual Router Redundancy Protocol# vr 2          (Select virtual router 2)
>> VRRP Virtual Router 2# vrid 2                              (Set VRID to 2)
>> VRRP Virtual Router 2# if 2                              (Set interface 2)
>> VRRP Virtual Router 2# addr 192.168.2.200              (Define IP address)
>> VRRP Virtual Router 2# ena                        (Enable virtual router 2)
```

5. **ポートのトラッキングを有効にします。仮想ルータ 1 がマスタになるように、プライオリティを 101 に設定します。**

```
/cfg/l3/vrrp/vr 1                                (Select VRRP virtual router 1)
>> VRRP Virtual Router 1# track/ports/ena               (Set tracking on ports)
>> VRRP Virtual Router 1 Priority Tracking# ..
>> VRRP Virtual Router 1# prio 101                     (Set the VRRP priority)
>> VRRP Virtual Router 1# ..
>> Virtual Router Redundancy Protocol# vr 2      (Select VRRP virtual router 2)
>> VRRP Virtual Router 2# track/ports/ena               (Set tracking on ports)
```

6. **スパニングツリープロトコルをグローバルにオフに、設定を適用、保存します。**

```
/cfg/l2/stg 1/off                                               (Turn off STG)
>> Spanning Tree Group 1# apply
>> Spanning Tree Group 1# save
```

タスク 2**：スイッチ** B **の設定（**AOS CLI **の例）**

1. **ポートを設定します。**

```
/cfg/l2/vlan 10                                     (Select VLAN 10)
>> VLAN 10# ena                                     (Enable VLAN 10)
>> VLAN 10# add 20                                  (Add port 20 to VLAN 10)
>> VLAN 10# ..
>> Layer 2# vlan 20                                 (Select VLAN 20)
>> VLAN 20# ena                                     (Enable VLAN 20)
>> VLAN 20# add 21                                  (Add port 21 to VLAN 20)
```

2. **クライアントとサーバのインタフェースを設定します。**

```
/cfg/l3/if 1                                                (Select interface 1)
>> IP Interface 1# addr 192.168.1.101      (Define IP address for interface 1)
>> IP Interface 1# vlan 10                    (Assign VLAN 10 to interface 1)
>> IP Interface 1# ena                                  (Enable interface 1)
>> IP Interface 1# ..
>> Layer 3# if 2                                        (Select interface 2)
```

```
>> IP Interface 2# addr 192.168.2.100       (Define IP address for interface 2)
>> IP Interface 2# vlan 20                     (Assign VLAN 20 to interface 2)
>> IP Interface 2# ena                                  (Enable interface 2)
>> IP Interface 2# ..
>> Layer 3# if 3                                        (Select interface 3)
>> IP Interface 3# addr 10.0.1.101          (Define IP address for interface 3)
>> IP Interface 3# mask 255.255.255.0      (Define subnet mask for interface 3)
>> IP Interface 3# ena                                  (Enable interface 3)
>> IP Interface 3# ..
>> Layer 3# if 4                                        (Select interface 4)
>> IP Interface 4# addr 10.0.2.100          (Define IP address for interface 4)
>> IP Interface 4# mask 255.255.255.0      (Define subnet mask for interface 4)
>> IP Interface 4# ena                                  (Enable interface 4)
```

3. **デフォルトゲートウェイを設定します。各デフォルトゲートウェイはレイヤ 2 ルータの一方を指します。**

```
/cfg/l3/gw 1                                        (Select default gateway 1)
>> Default gateway 1# addr 192.168.2.1   (Point gateway to the first L2 router)
>> Default gateway 1# ena                  (Enable the default gateway)
>> Default gateway 1# ..
>> Layer 3# gw 2                                    (Select default gateway 2)
>> Default gateway 2# addr 192.168.1.1    (Point gateway to the second router)
>> Default gateway 2# ena                  (Enable the default gateway)
```

4. VRRP **を有効にして、仮想インタフェースルータを** 2 **台設定します。**

```
/cfg/l3/vrrp/on                                                (Turn VRRP on)
>> Virtual Router Redundancy Protocol# vr 1          (Select virtual router 1)
>> VRRP Virtual Router 1# vrid 1                              (Set VRID to 1)
>> VRRP Virtual Router 1# if 1                            (Set interface 1)
>> VRRP Virtual Router 1# addr 192.168.1.200             (Define IP address)
>> VRRP Virtual Router 1# ena                        (Enable virtual router 1)
>> VRRP Virtual Router 1# ..                         (Enable virtual router 1)
>> Virtual Router Redundancy Protocol# vr 2          (Select virtual router 2)
>> VRRP Virtual Router 2# vrid 2                              (Set VRID to 2)
>> VRRP Virtual Router 2# if 2                            (Set interface 2)
>> VRRP Virtual Router 2# addr 192.168.2.200             (Define IP address)
>> VRRP Virtual Router 2# ena                        (Enable virtual router 2)
```

5. **ポートのトラッキングを有効にします。仮想ルータ** 2 **がマスタになるよう、プライオリティを** 101 **に設定します。**

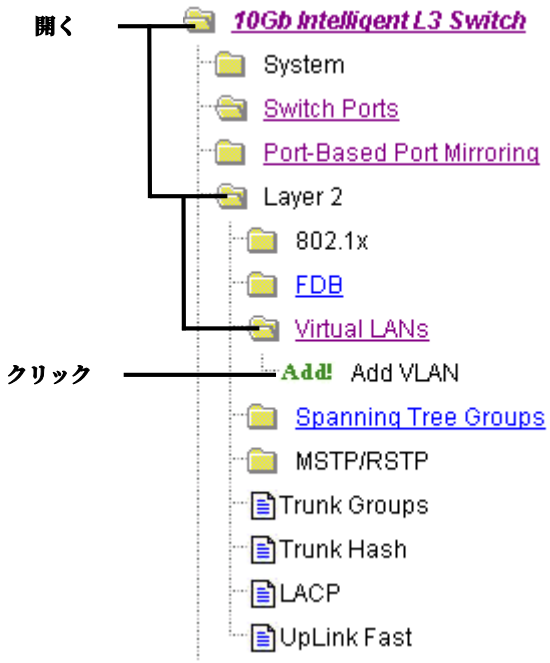
```
/cfg/l3/vrrp/vr 1                              (Select VRRP virtual router 1)
>> VRRP Virtual Router 1# track/ports/ena             (Set tracking on ports)
>> VRRP Virtual Router 1 Priority Tracking# ..
>> VRRP Virtual Router 1# ..
>> Virtual Router Redundancy Protocol# vr 2      (Select VRRP virtual router 2)
>> VRRP Virtual Router 2# track/ports/ena             (Set tracking on ports)
>> VRRP Virtual Router 2 Priority Tracking# ..
>> VRRP Virtual Router 2# prio 101                    (Set the VRRP priority)
```

6. **スパニングツリープロトコルをグローバルにオフに、設定を適用、保存します。**

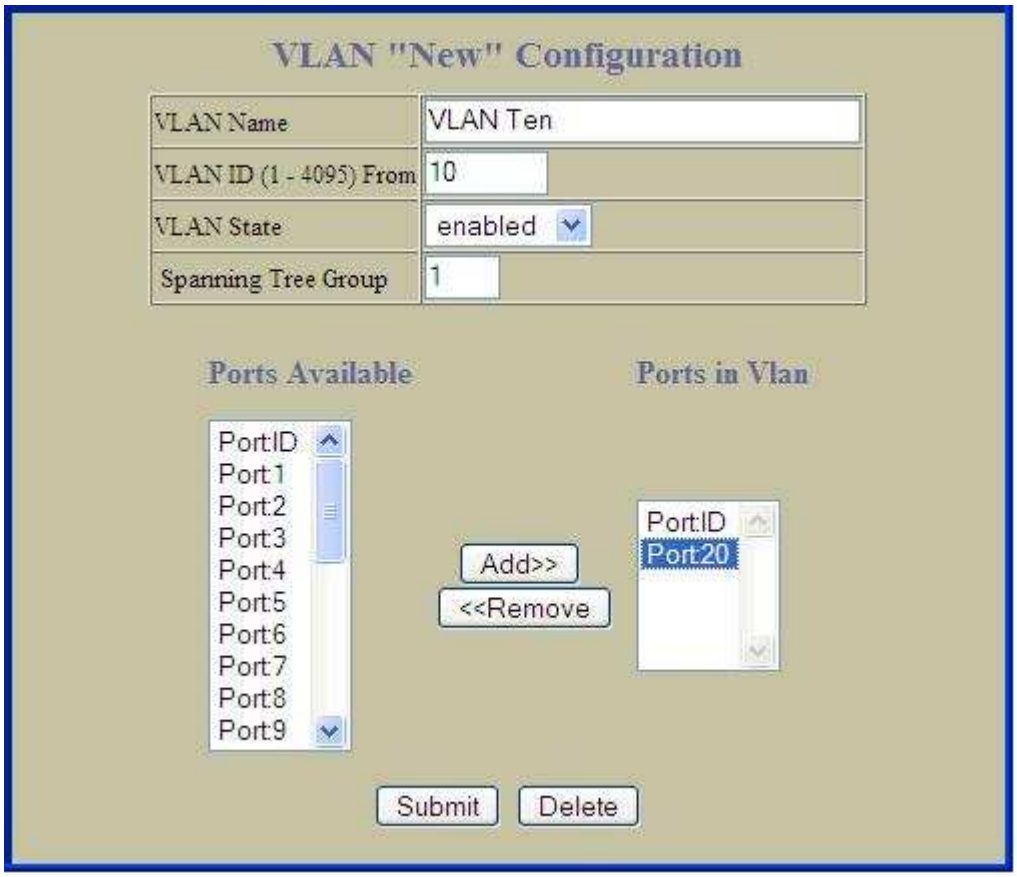
```
/cfg/l2/stg 1/off                                              (Turn off STG)
>> Spanning Tree Group 1# apply
>> Spanning Tree Group 1# save
```

タスク１：スイッチＡの設定（BBI の例）

1. ポートと VLAN を設定します。
   a. CONFIGURE ボタンをクリックします。
   b. Virtual LANs フォルダを開き、Add VLAN を選択します。



c. ポート 20 を VLAN10 のメンバに、ポート 21 を VLAN20 のメンバとして設定し、各 VLAN を有効にします。

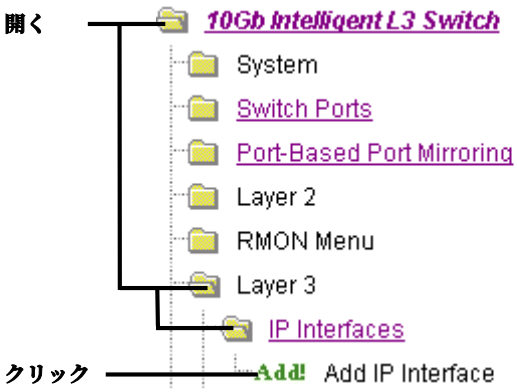


d. Sumbit をクリックします。

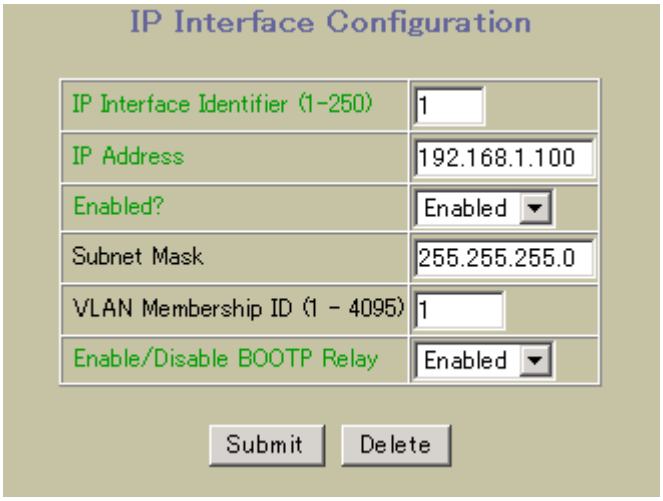
2. 次のクライアントとサーバのインタフェースを設定します。

- IF 1
  IP address = 192.168.1.100
  Subnet mask = 255.255.255.0
  VLAN 10
- IF 2
  IP address = 192.168.2.101
  Subnet mask = 255.255.255.0
  VLAN 20
- IF 3
  IP address = 10.0.1.100
  Subnet mask = 255.255.255.0
- IF 4
  IP address = 10.0.2.101
  Subnet mask = 255.255.255.0

a. IP Interfaces フォルダを開き、Add IP Interface を選択します。



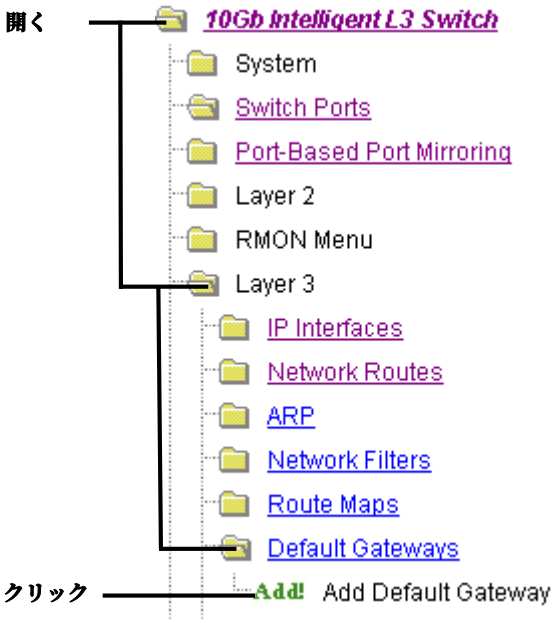
b. IP インタフェースを設定します。IP アドレス、サブネットマスク、VLAN ID を入力し、インタフェースを有効にします。



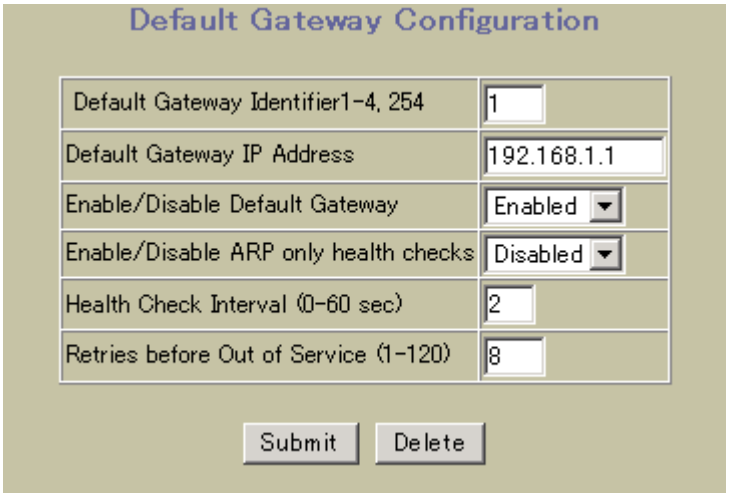
c. Submit をクリックします。

3. デフォルトゲートウェイを設定します。各デフォルトゲートウェイはレイヤ 2 ルータの一方を指します。

a. Default Gateways フォルダを開き、Add Default Gateway を選択します。



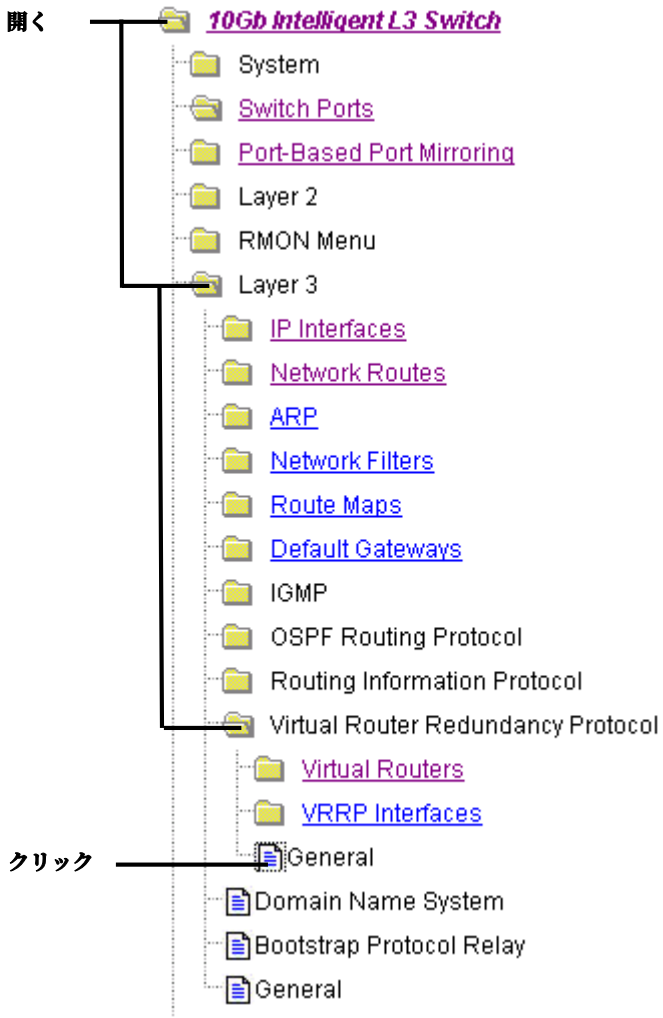
b. 各デフォルトゲートウェイに IP アドレスを設定し、有効にします。



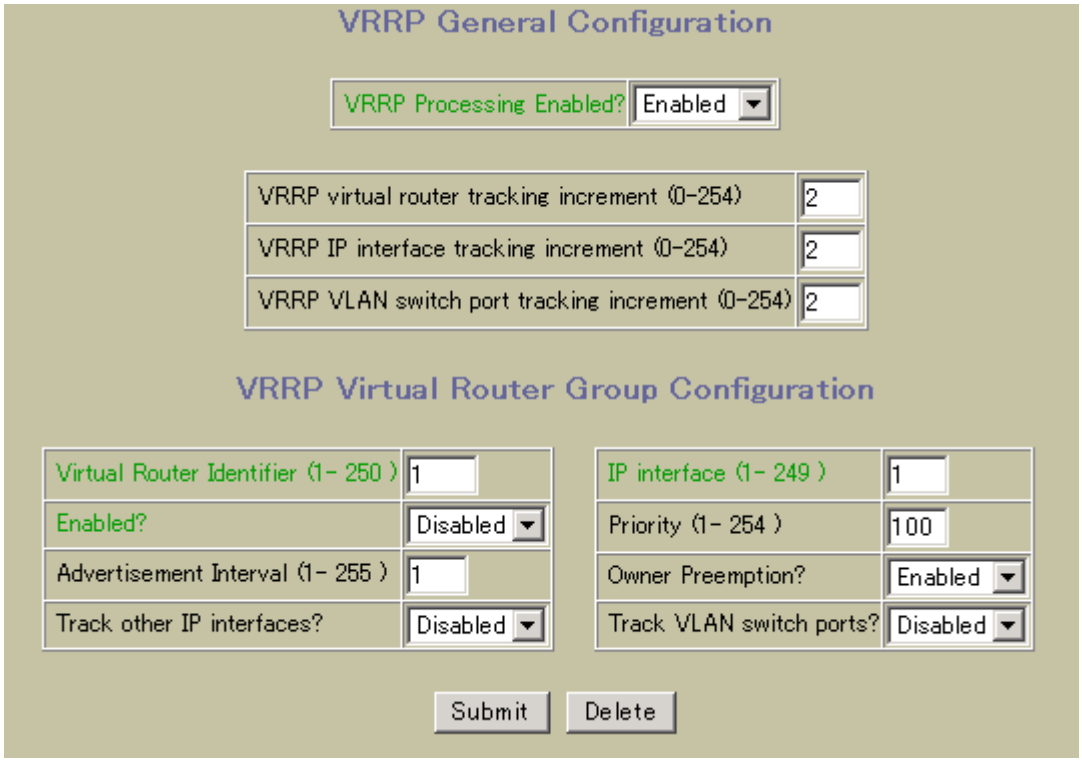
c. Submit をクリックします。

4. VRRP を有効にし、2 つの仮想インタフェースルータを設定します。

a. Virtual Router Redundancy Protocol フォルダを開き、General を選択します。

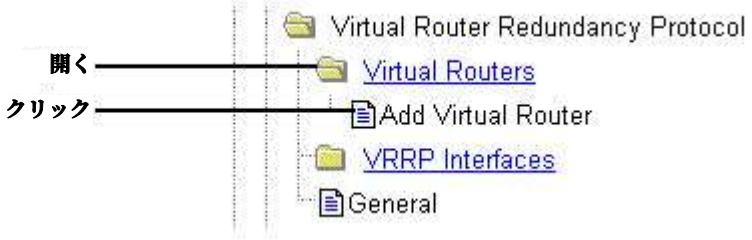


b. VRRP processing を有効にします。

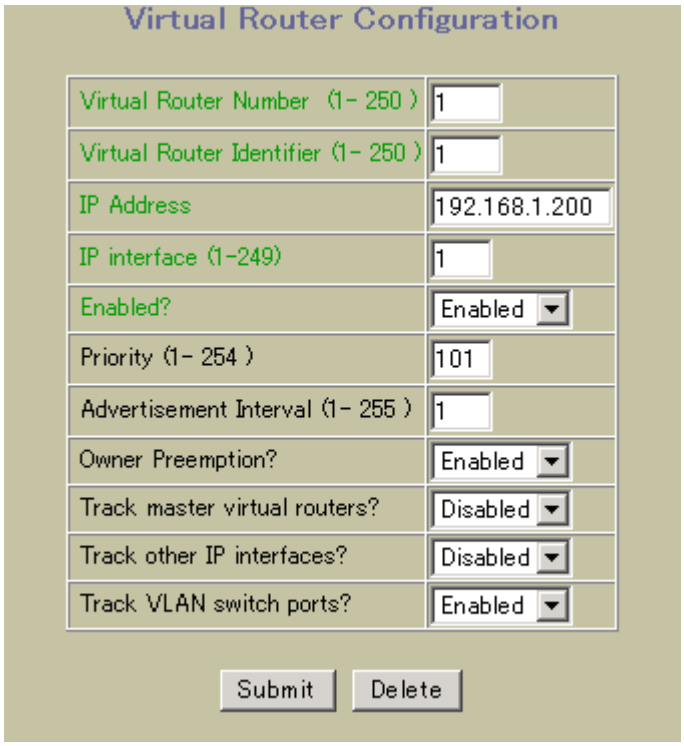


c. Submit をクリックします。

d. Virtual Routers フォルダを開き、Add Virtual Router を選択します。

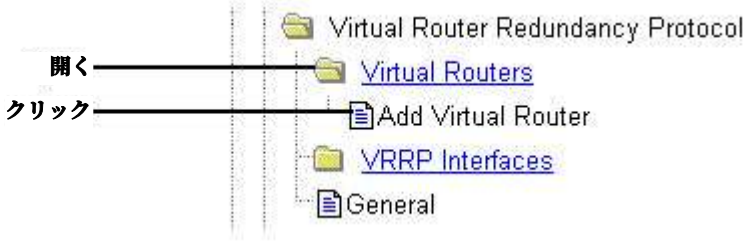


e. 仮想ルータ 1 の IP アドレスを設定します。ポートのトラッキングを有効、プライオリティを 101 にし、仮想ルータを有効にします。

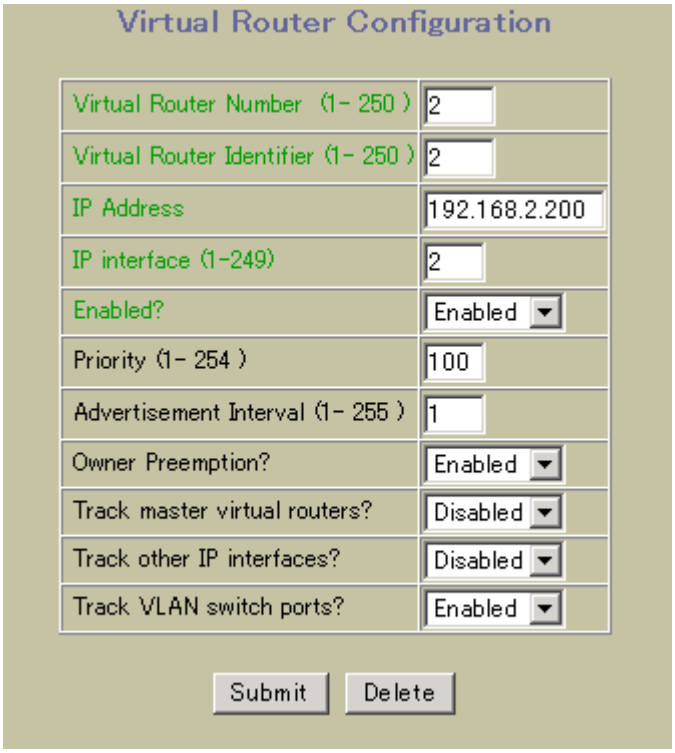


f. Submit をクリックします。

g. Add Virtual Router を選択します。



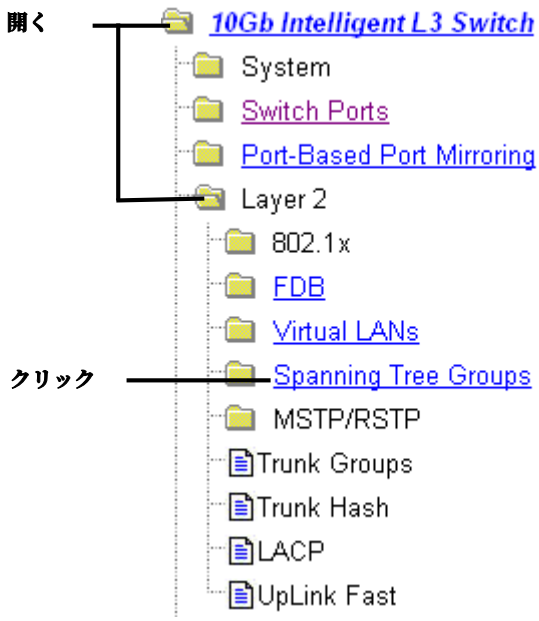
h. 仮想ルータ 2 の IP アドレスを設定します。ポートのトラッキングを有効にし、プライオリティをデフォルトの 100 に設定し、仮想ルータを有効にします。



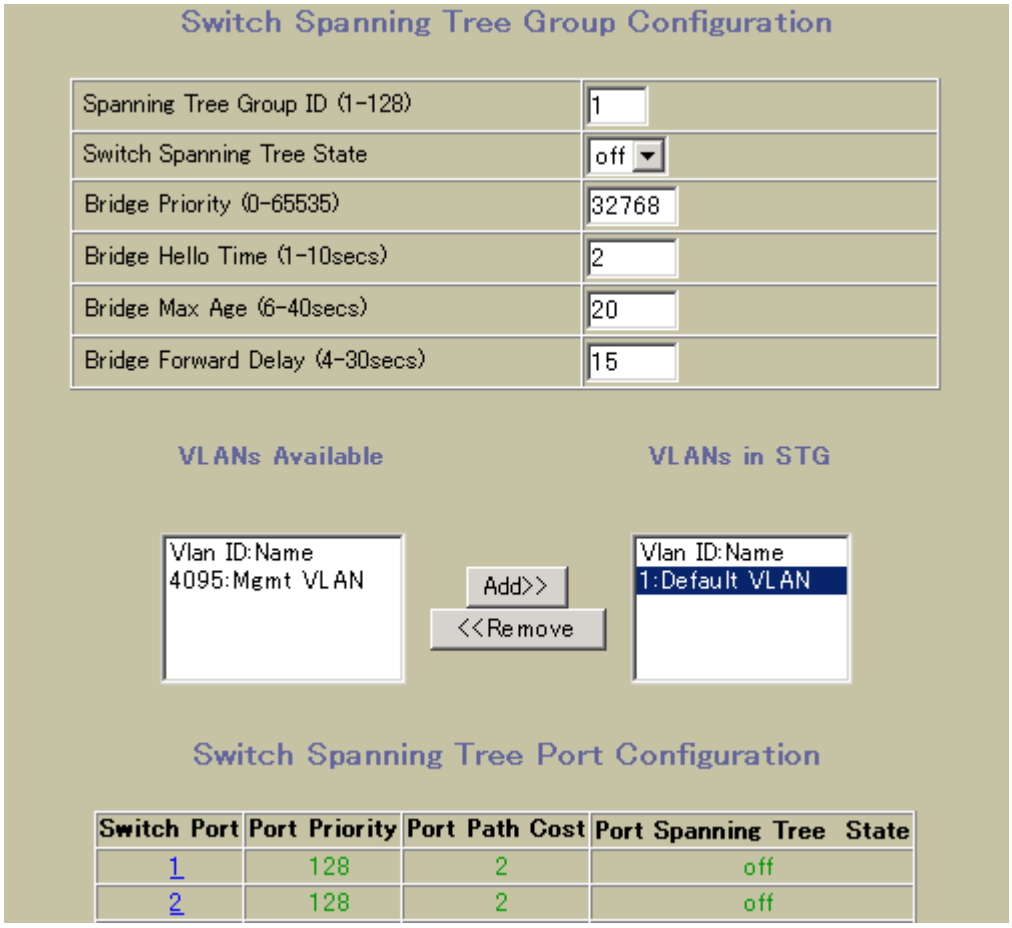
i. Submit をクリックします。

5. スパニングツリーを無効にします。

a. Spanning Tree Groups を選択します。

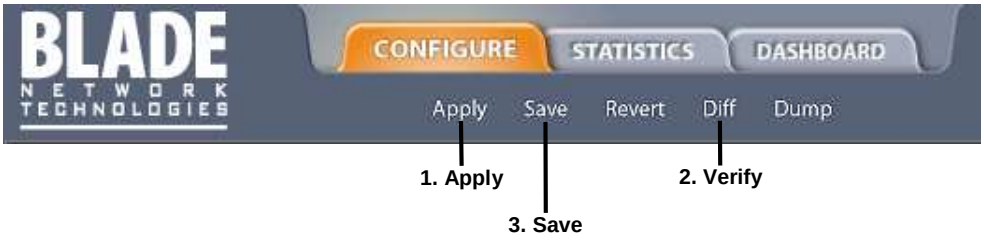


b. Spanning Tree Group ID に 1 を入力し、Switch Spanning Tree State を off に設定します。



c. Submit をクリックします。

6. 設定を適用、確認、保存します。



Troubleshooting tools

はじめに

この章では、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。

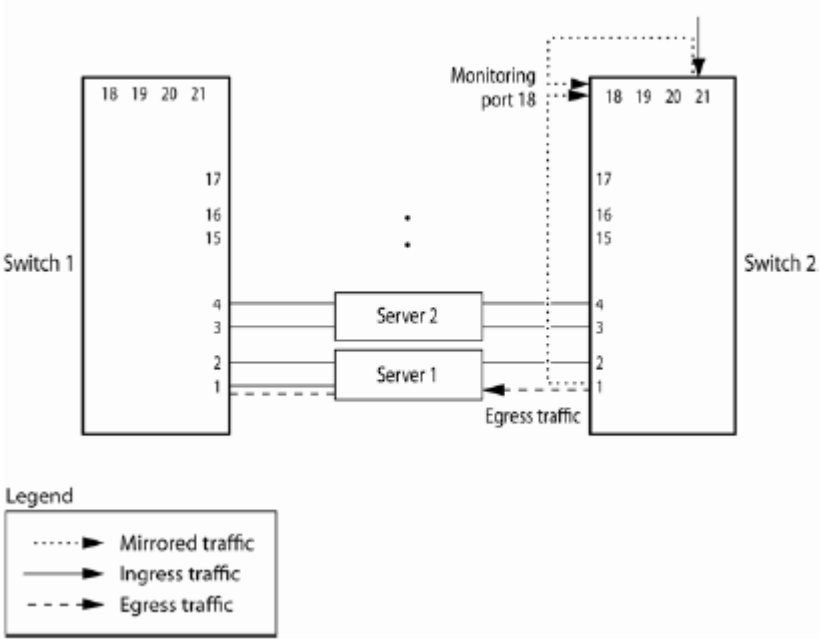
ポートミラーリング

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 18 でポート 21 の Ingress 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 Egress 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 18 に接続すれば、ポート 21 と 1 のトラフィックをモニタできます。

図27　ポートモニタリング



この図は、2 つのポートを 1 つのポートでモニタしているケースです。同様に、1 つのポートを 1 ポートで、もしくは多数のポートを 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。

Ingress トラフィックは、処理前に二重化して、モニタポートに送られます。Egress トラフィックは、処理後に二重化して、モニタ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. モニタポートを指定します。

```
>> # /cfg/pmirr/monport 18            (Select port 18 for monitoring)
```

2. ミラーリングするポートを選択します。

```
>> Port 18 # add 21                        (Select port 21 to mirror)
>> Enter port mirror direction [in, out, or both]: in
(Monitor ingress traffic on port 21)
>> Port 18 # add 1                         (Select port 1 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。

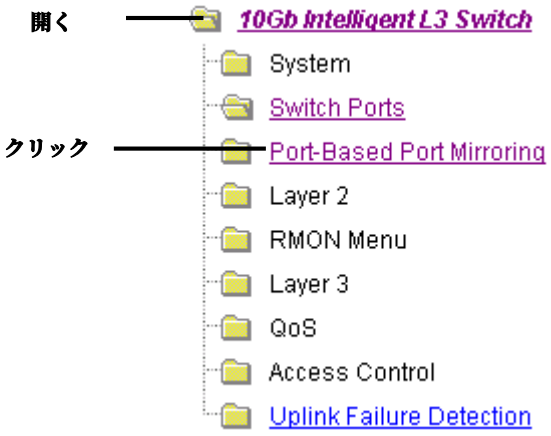
```
>> PortMirroring# apply                (Apply the configuration)
>> PortMirroring# save                  (Save the configuration)
```

5. 現在の設定を確認します。

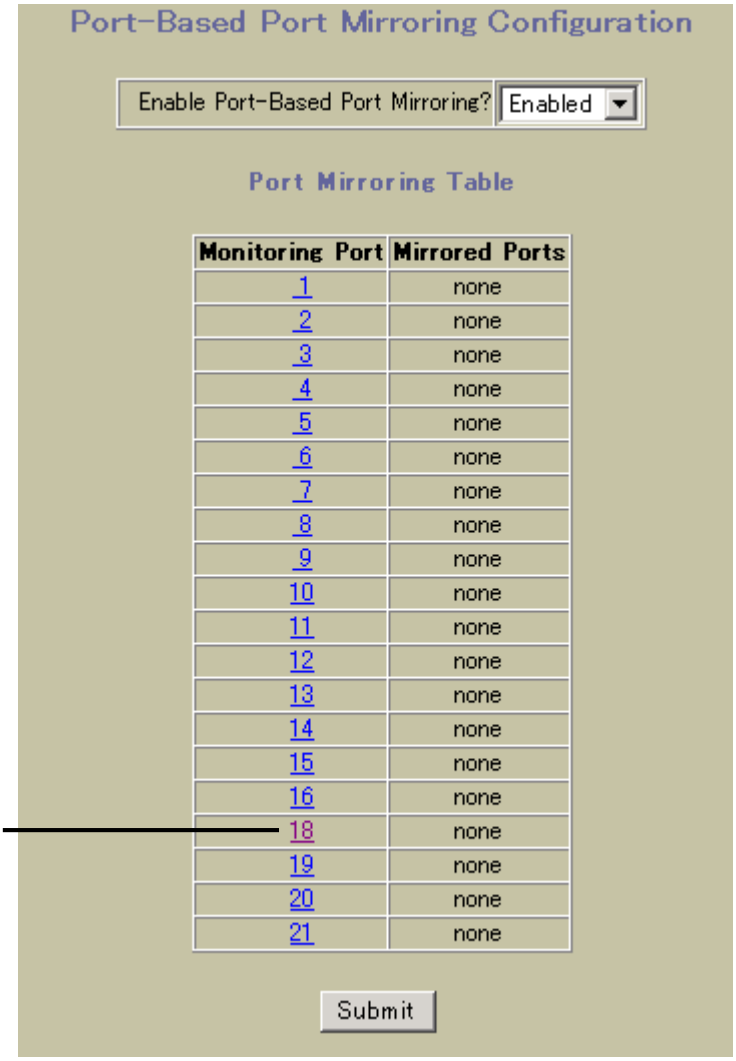
```
>> PortMirroring# cur              (Display the current settings)
Port mirroring is enabled
Monitoring Ports Mirrored Ports
1     none
2     none
3     none
4     none
5     none
   :
   :
16    none
18    none
20 (21, in) (1, out)
21    none
```

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）。

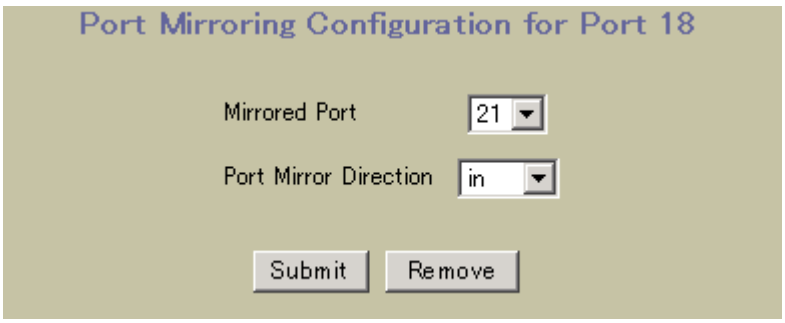


   c. ポート番号をクリックしてモニタポートを選択します。



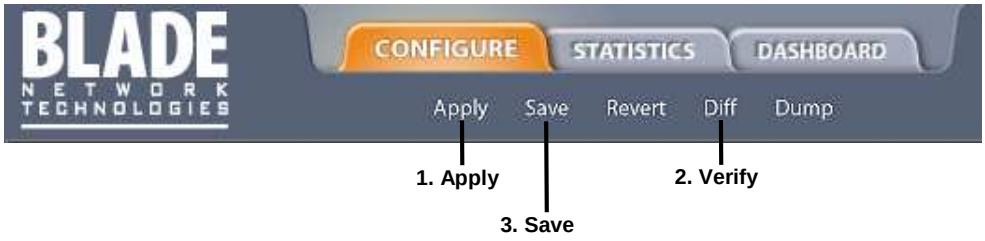
d. Add Mirrored Port をクリックします。

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

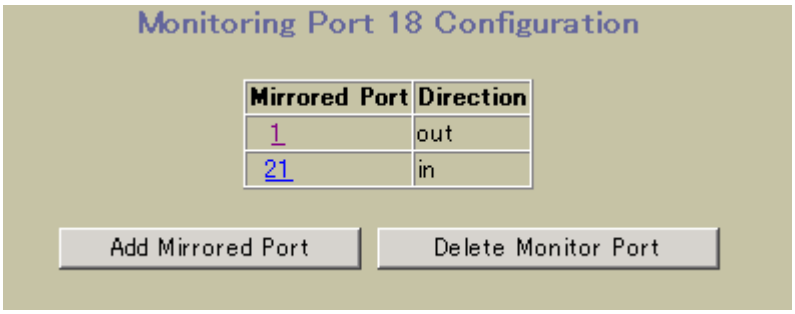


f. Submit をクリックします。

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 ]] [-m|-mgt|-d|-data]
```

`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。デフォルトでは、マネジメントポートが使用されます。データポートを使用する場合は、-d もしくは-data オプションを指定します。

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。