FUJITSU

CA92344-0456-01

PRIMERGY

PRIMERGY スイッチブレード (10Gbps 18/8+2) 設定事例集

(PY-SW105)

FUJITSU

目次

1. VLAN 機能を使う

1.1 タグなし VLAN 機能を使う

ここでは、ポート単位でグループ化したタグなしパケットをポートVLANで送受信する場合の設定方法を説明します。

【設定条件】

Interface0/1 にタグなしで VLAN10 を割り当てる。

Interface0/5 にタグなしで VLAN20 を割り当てる。

VLAN ID:20 に 192.168.20.1/24 を設定する。

【コマンド】

Interface0/1 にタグなしで VLAN10 を割り当てる。

```
(config)#interface 0/1
(config-if)#vlan untag 10
```

Interface0/5 にタグなしで VLAN20 を割り当てる。

```
(config)#interface 0/5
(config-if)#vlan untag 20
```

VLAN ID:20 に 192.168.20.1/24 を設定する。

```
(config)#lan 0 ip address 192.168.20.1/24 3
(config)#lan 0 vlan20
```

設定を保存する。

```
(config)#save
```

1.2 タグ VLAN 機能を使う

ここでは、1 つのポートで、2 つのVLANからのタグ付きパケットを、それぞれのVLANで送受信する場合の設定方法を説明します。

【設定条件】

Interface0/1 にタグ付きで VLAN10 を割り当てる。

Interface0/5 にタグ付で VLAN20 を割り当てる。

VLAN ID:20 に 192.168.20.1/24 を設定する。

【コマンド】

Interface0/1 にタグ付きで VLAN10、20 を割り当てる。

```
(config)#interface 0/1
(config-if)#vlan tag 10,20
```

Interface0/5 にタグ付きで VLAN10、20 を割り当てる。

```
(config)#interface 0/5
(config-if)#vlan tag 10,20
```

VLAN ID:20 に 192.168.20.1/24 を設定する。

```
(config)#lan 0 ip address 192.168.20.1/24 3
(config)#lan 0 vlan20
```

設定を保存する。

```
(config)#save
```

1.3 プロトコル VLAN 機能を使う

ここでは、IP プロトコルのパケットをそれぞれのポートでVLAN10 およびVLAN20として送受信し、IP プロトコル以外のパケットについてはVLAN100 として送受信する場合の設定方法を説明します。

【設定条件】

Interface0/1 にタグなし VLAN10、100 を割り当てる。

Interface0/5 にタグなし VLAN20、100 を割り当てる。

VLAN10、20 を Ipv4 プロトコル VLAN に設定する。

VLAN ID:20 に 192.168.20.1/24 を設定する。

【コマンド】

Interface0/1 を VLAN10、20 に設定する。

```
(config)#interface 0/1
(config-if)#vlan untag 10,100
```

Interface0/5 を VLAN10、20 に設定する。

```
(config)#interface 0/5
(config-if)#vlan untag 20,100
```

VLAN10、20 を IPv4 プロトコル VLAN に設定する。

```
(config)#vlan 10 protocol ipv4
(config)#vlan 20 protocol ipv4
```

VLAN ID:20 に 192.168.20.1/24 を設定する。

```
(config)#lan 0 ip address 192.168.20.1/24 3
(config)#lan 0 vlan20
```

設定を保存する。

```
(config)#save
```

2. リンクアグリゲーション機能を使う

2.1 LACP 使わない

ここでは 4 ポートの回線をリンクアグリゲーションする場合の設定方法を説明します。

【設定条件】

Interface0/19～0/22 をリンクアグリゲーションに設定する。

VLAN ID:20 に 192.168.20.1/24 を設定する。

SBAX3#1

【コマンド】

Interface0/19～0/22 を VLAN10、20 に設定する。

```
(config)#interface range 0/19-0/22
(config-if)#vlan tag 10,20
```

Interface0/19～0/22 をリンクアグリゲーションとして設定する。

```
(config)#interface range 0/19-0/22 type linkaggregation 1
(config-if)#vlan untag 20
```

VLAN ID:20 に 192.168.20.1/24 を設定する。

```
(config)#lan 0 ip address 192.168.20.1/24 3
(config)#lan 0 vlan20
```

設定を保存する。

```
(config)#save
```

SBAX3#2

【コマンド】

Interface0/19 を VLAN10 に設定する。

```
(config)#interface range 0/19-0/22
(config-if)#vlan tag 10,20
```

Interface0/19～0/22 をリンクアグリゲーションとして設定する。

```
(config)#interface range 0/19-0/22
(config-if)#type linkaggregation 1
```

(config-if)#vlan untag 20

VLAN ID:20 に 192.168.20.1/24 を設定する。
(config)#lan 0 ip address 192.168.20.2/24 3
(config)#lan 0 vlan20

設定を保存する。
(config)#save

2.2 LACP 機能を使う

ここでは、4ポートをLACPを利用したリンクアグリゲーションとする場合の設定方法を説明します。

【設定条件】

Interface0/19～0/22 を LACP 利用のリンクアグリゲーションに設定する。

VLAN ID:20 に 192.168.20.1/24 を設定する。

SBAX3#1
【コマンド】

Interface0/19～0/22 を VLAN10、20 に設定する。
(config)#interface range 0/19-0/22
(config-if)#vlan tag 10,20

Interface0/19～0/22 をリンクアグリゲーションとして設定する。
(config)#interface range 0/19-0/22
(config-if)#type linkaggregation 1
(config)#llinkaggregation 1 mode active

VLAN ID:20 に 192.168.20.1/24 を設定する。
(config)#lan 0 ip address 192.168.20.1/24 3
(config)#lan 0 vlan20

設定を保存する。
(config)#save

SBAX3#2
【コマンド】

Interface0/19-0/22 を VLAN10 に設定する。

(config)#interface range 0/19-0/22
(config-if)#vlan tag 10,20

Interface0/19～0/22 をリンクアグリゲーションとして設定する。

(config)#interface range 0/19-0/22
(config-if)#type linkaggregation 1
(config)#llinkaggregation 1 mode active

VLAN ID:20 に 192.168.20.1/24 を設定する。

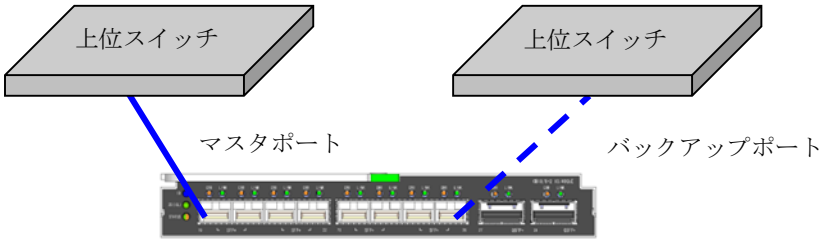
(config)#lan 0 ip address 192.168.20.2/24 3
(config)#lan 0 vlan20

設定を保存する。

(config)#save

3　バックアップポート機能を使う

ここではアップリンクポートをバックアップポートとして利用する場合の設定方法について説明します。
アップリンクポートをそれぞれ異なるスイッチに接続することで、冗長アップリンクの形態にできます。



【設定条件】

Interface0/19、0/26 をバックアップポートに設定する。

(Interface0/19 をマスタポート、Interface0/26 をバックアップポートとする。)

マスタポートを優先的に使用する。

SBAX3#1

【コマンド】

Interface0/19 をバックアップポート(グループ 1)のマスタポートに設定する。

```
SBAX3(config)#interface 0/19
SBAX3(config-if)#type backup 1 master
Jan 01 10:09:50 127.0.0.1 SBAX3: l2nsm: backup 1 definition is invalid. backup port is not defined.
```

(このようにバックアップグループで master または backup のみを定義した場合、他方が存在せず無効というメッセージが表示されます。バックアップグループには master と backup の両方を定義する必要があるためです。続けて他方の定義を行えばバックアップグループの機能が有効になります。)

Interface0/26 をバックアップポート(グループ 1)のバックアップポートに設定する。

```
(config)#interface 0/26
(config-if)#type backup 1 backup
```

バックアップグループ 1 をマスタポート優先モードに設定する。

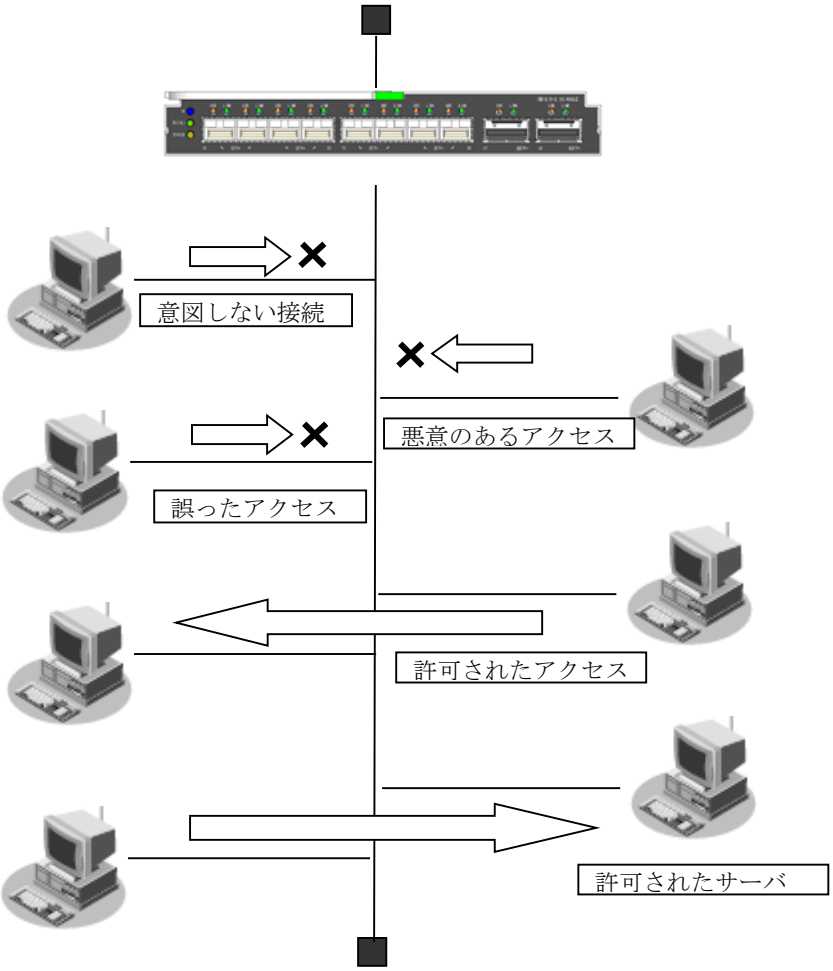
```
(config)#backup 1 mode master
```

設定を保存する。

```
(config)#save
```

4 MAC フィルタリング機能を使う

本装置を経由するパケットを、MACアドレス、パケット形式、ETHERNET タイプ、VLAN ID、COS値などの組み合わせで制御することによって、ネットワークのセキュリティを向上させたり、ネットワークへの負荷を軽減することができます。



フィルタリング条件

以下の条件を指定することによって、パケットデータの流れを制御できます。

1)ACLのMAC定義およびVLAN定義で指定した以下の情報

- 送信元MAC情報（MAC アドレス／パケット形式／ ETHERNET タイプ／ LSAP）
- あて先MAC情報（MAC アドレス／パケット形式／ ETHERNET タイプ／ LSAP）
- VLAN ID
- COS値
- 送信元IP 情報（IP アドレス／アドレスマスク）
- あて先IP 情報（IP アドレス／アドレスマスク）
- プロトコル

- TCP・UDPのポート番号
- ICMP TYPE、ICMP CODE
- IPパケットのTOS 値、DSCP値

2)フィルタ処理の対象となるパケット入力ETHERポート
3)フィルタ処理の対象となるパケットが入力ETHERポートに入力された場合の動作（遮断または透過）

フィルタリングの設計方針

フィルタリングの設計方針には大きく分類して以下の 2 つがあります。

A. 特定の条件のパケットだけを透過させ、その他はすべて遮断する。

B. 特定の条件のパケットだけを遮断し、その他はすべて透過させる。

ここでは、設計方針Aの例として、以下の設定例について説明します。

特定MACアドレスからのパケットだけを許可する

特定MACアドレスへのパケットだけを許可する

また、設計方針Bの例として、以下の設定例について説明します。

特定パケット形式のパケットだけを禁止する

こんなことに気をつけて

プロトコル VLAN 機能と併用した場合、プロトコル VLAN として認識されるフレームへの MAC フィルタリング機能は無効となります。

なお、プロトコル VLAN として認識されるフレームについては “vlan protocol” コマンド項目を参照してください。

4.1 特定 MAC アドレスからのパケットだけを許可する

ここでは、VLAN内の特定ポートで特定のMACアドレスを持つホストからの入力パケットだけを許可し、その他のホストからの入力パケットを禁止する場合の設定方法を説明します。

【フィルタリング設計】

VLAN 10はInterface0/1～0/8ポートで構成されるポートVLANで、それぞれのポートでタグなしである

•VLAN 20はInterface0/1～0/4ポートおよびInterface0/9～0/12 ポートで構成されるポートVLANで、Interface0/1～0/4ポー

トでタグ付き、Interface0/9～0/12ポートでタグなしである。

Interface0/4～0/8 ポートのVLAN 10ではMACアドレス00:0b:01:02:03:04のホストへの送信パケットだけを許可し、その他はすべて禁止する。

【コマンド】

VLAN ID が10 で送信元MACアドレスが00:0b:01:02:03:04 であるパケットの形式をACLで設定する ----（1）

```
(config)#acl 100 mac 00:0b:01:02:03:04 any any
(config)#acl 100 vlan 10 any
```

VLAN ID が10 のすべてのパケットの形式をACLで設定する ----（2）

```
(config)#acl 110 vlan 10 any
```

Interface0/2ポートで（1）で設定した形式のパケットを透過させる

```
(config)#interface 0/2
(config-if)#macfilter 0 pass 100
```

Interface0/2ポートで（2）で設定した形式のパケットを遮断する

```
(config)#interface 0/2
(config-if)#macfilter 1 reject 110
```

4.2 特定 MAC アドレスへのパケットだけを許可する

ここでは、VLAN内の特定ポートで特定のMACアドレスを持つホストへの送信パケットだけを許可し、その他のホストへの送信パケットを禁止する場合の設定方法を説明します。

【フィルタリング設計】

VLAN 10はInterface0/1～0/8 ポートで構成されるポートVLANで、それぞれのポートでタグなしである

VLAN 20 はInterface0/1～0/4ポートおよびInterface0/9～0/12ポートで構成されるポートVLANで、

Interafce0/1～0/4ポートでタグ付き、Interafce0/9～12 ポートでタグなしである。

Interface0/4～Interface0/8ポートのVLAN 10ではMACアドレス00:0b:01:02:03:04のホストへの送信パケットだけを許可し、その他はすべて禁止する。

【コマンド】

VLAN ID が10 で送信先MACアドレスが00:0b:01:02:03:04 であるパケットの形式をACLで設定する ----（1）

```
(config)#acl 120 mac any 00:0b:01:02:03:04 any
(config)#acl 120 vlan 10 any
```

VLAN ID が10 のすべてのパケットの形式をACLで設定する ---- （2）

```
(config)#acl 110 vlan 10 any
```

Interface0/4～0/8ポートで（1）で設定した形式のパケットを透過させる

```
(config)#interface range 0/4-0/8
(config-if)#macfilter 0 pass 120
```

Interface0/4～0/8ポートで（2）で設定した形式のパケットを遮断する

```
(config)#interface range 0/4-0/8
(config-if)#macfilter 1 reject 110
```

4.3 特定パケット形式のパケットだけを禁止する

ここでは、VLAN内の特定ポートで特定のパケット形式を持つ入力パケットだけを禁止し、その他の入力パケットを許可する場合の設定方法を説明します。

【フィルタリング設計】

VLAN 10はInterface0/1～0/8 ポートで構成されるポートVLANで、それぞれのポートでタグなしである

VLAN 20 はInterface0/1～0/4ポートおよびInterface0/9～0/12ポートで構成されるポートVLANで、

Interafce0/1～0/4ポートでタグ付き、Interafce0/9～0/12 ポートでタグなしである。

Interface0/1～Interface0/4ポートでは、IPプロトコルの入力パケットだけを禁止し、その他はすべて許可する。

【コマンド】

IP プロトコルのパケット(IP,ARP,Reverse ARP)の形式を ACL で設定する。----(1)

```
(config)#acl 130 mac any any ether 0800
(config)#acl 131 mac any any ether 0806
(config)#acl 132 mac any any ether 8035
```

Interface0/1～0/4で(1)で作成したパケットのパターンを遮断する。

Interface0/4～0/8ポートで（2）で設定した形式のパケットを遮断する

```
(config)#interface range 0/1-0/4
(config-if)#macfilter 0 reject 130
(config-if)#macfilter 1 reject 131
(config-if)#macfilter 2 reject 132
```

4.4 VLAN 単位で特定 MAC アドレス間の通信だけを遮断する

ここでは、VLAN内のポートで特定のMACアドレスを持つホスト間の通信だけを遮断する場合の設定方法を説明します。

【フィルタリング設計】

VLAN 10はInterface0/1～0/4 ポートでタグなし、Interface0/5～0/8ポートでタグ付きで構成されるポートVLANである

VLAN 20 はInterface0/1～0/4ポートでタグ付き、Interface0/5～0/8ポートでタグなしで構成されるポートVLANである

VLAN10ではMACアドレス00:0b:01:02:03:04のホストからMACアドレス00:0b:11:12:13:14間のTCP通信だけを禁止し、VLAN20ではMACアドレス00:0b:21:22:23:24のホストからMACアドレス00:0b:31:32:33:34間のUDP通信だけを禁止する。

【コマンド】

送信元MACアドレスが00:0b:01:02:03:04、送信先MACアドレスが00:0b:11:12:13:14であるTCPパケットの形式をACLで設定する。---------(1)

```
(config)#acl 0 mac 00:0b:01:02:03:04 00:0b:11:12:13:14 any
(config)#acl 0 ip any any 6 any
```

送信元MACアドレスが00:0b:11:12:13:14、送信先MACアドレスが00:0b:01:02:03:04であるTCPパケットの形式をACLで設定する。---------(2)

```
(config)#acl 1 mac 00:0b:11:12:13:14 00:0b:01:02:03:04 any
(config)#acl 1 ip any any 6 any
```

送信元MACアドレスが00:0b:21:22:23:24、送信先MACアドレスが00:0b:31:32:33:34であるUDPパケットの形式をACLで設定する。---------(3)

```
(config)#acl 2 mac 00:0b:21:22:23:24 00:0b:31:32:33:04 any
(config)#acl 2 ip any any 17 any
```

送信元MACアドレスが00:0b:31:32:33:34、送信先MACアドレスが00:0b:21:22:23:24であるUDPパケットの形式をACLで設定する。---------(4)

```
(config)#acl 3 mac 00:0b:21:22:23:24 00:0b:31:32:33:04 any
```

(config)#acl 3 ip any any 17 any

VLAN10で(1)、(2)で設定した形式のパケットを遮断する。
(config)#vlan 10 macfilter 0 reject 0
(config)#vlan 10 macfilter 1 reject 1

VLAN20で（3）、(4)で設定した形式のパケットを遮断する
(config)#vlan 20 macfilter 0 reject 2
(config)#vlan 20 macfilter 1 reject 3

4.5 VLAN 単位で特定パケット形式のパケットだけを許可する

ここでは、VLAN内のポートで特定のパケット形式を持つ入力パケットだけを許可し、その他の入力パケットを遮断する場合の設定方法を説明します。

【フィルタリング設計】
VLAN 10はInterface0/1～0/4 ポートでタグなし、Interface0/5～0/8ポートでタグ付きで構成されるポートVLANであるVLAN10ではIPプロトコルの入力だけを許可する

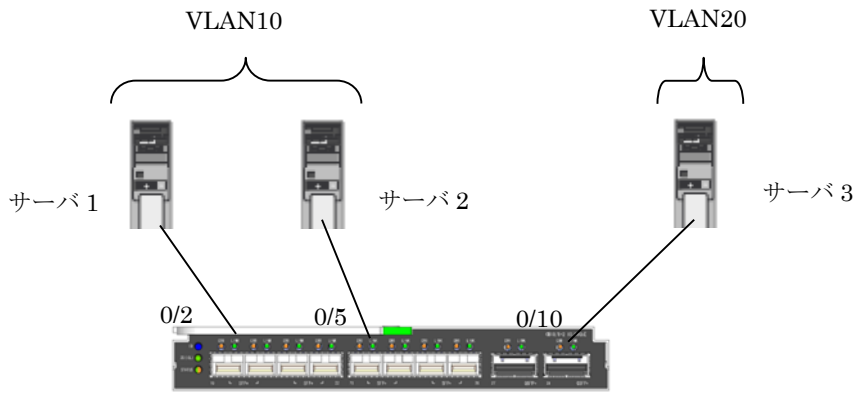
【コマンド】
IP プロトコルのパケット(IP,ARP,Reverse ARP)の形式を ACL で設定する。----(1)
(config)#acl 10 mac any any ether 0800
(config)#acl 11 mac any any ether 0806
(config)#acl 12 mac any any ether 8035

全プロトコルのパケットの形式を ACL で設定する。----(2)
(config)#acl 30 mac any any any

VLAN10で(1)で作成したパケットのパターン以外を遮断する。-----(3)
(config)#vlan 10 macfilter 0 pass 10
(config)#vlan 10 macfilter 1 pass 11
(config)#vlan 10 macfilter 2 pass 12
(config)#vlan 10 macfilter 3 reject 30

5　スタティック MAC フォワーディング機能を使う

スタティックMACフォワーディング機能を利用すると、構成定義によって、MACアドレスをスタティックにFDBに登録することができ、フラッディングによる余分なフレームがネットワーク上を流れることを防止できます。ここでは、各ETHERポートに接続されるサーバのMACアドレスをスタティックエントリとして設定する方法を説明します。



【設定条件】

Interface0/2、0/5 ポートにサーバ1、2 を接続し、VLANを10 とする

Interface0/10ポートにサーバ3 を接続し、VLANを20 とする

サーバ1 のMACアドレス：00:00:00:00:00:11

サーバ2 のMACアドレス：00:00:00:00:00:22

サーバ3 のMACアドレス：00:00:00:00:00:33

【コマンド】

Interface0/2、0/5 に VLAN10 を設定する。

```
(config)#interface range 0/2,0/5
(config-if)#vlan untag 10
```

Interface0/10 に VLAN20 を設定する。

```
(config)#interface 0/10
(config-if)#vlan untag 20
```

VLAN10 にスタティック MAC フォワーディングを設定する。

```
(config)#vlan 10 forward 0 00:00:00:00:00:11 2
(config)#vlan 10 forward 1 00:00:00:00:00:22 5
```

VLAN20 にスタティック MAC フォワーディングを設定する。

```
(config)#vlan 20 forward 0 00:00:00:00:00:33 10
```

設定を保存する。

```
(config)#save
```

6 QoS 機能を使う

優先制御機能を使う

本装置では、VLAN機能のユーザプライオリティ値に出力ポートの複数の優先度の異なるキューを対応付けることで、パケットの優先制御を行うことができます。

【優先制御設計】

パケットのタイプ	CoS 値	装置内部のキュークラス
管理パケット	7	3
	6	
音声	5	
FAX/呼制御	4	2
映像	3	1
	2	
その他	1	0
	0	

【コマンド】

```
(config)#qos cosmap 0 0
(config)#qos cosmap 1 0
(config)#qos cosmap 2 1
(config)#qos cosmap 3 1
(config)#qos cosmap 4 2
(config)#qos cosmap 5 3
(config)#qos cosmap 6 3
(config)#qos cosmap 7 3
```

優先制御情報書き換え機能を使う

本装置を経由して送出されるパケットをMACアドレス, パケット形式, ETHERNETタイプ, VLAN ID, COS値などの組み合わせで指定し、ETHERポートへの入力時に優先制御情報を書き換えることができます。

書き換え条件

以下の条件を指定することによって、優先制御情報を書き換えることができます。

1)ACLのMAC定義およびVLAN定義で指定した以下の情報

- 送信元MAC情報（MAC アドレス／パケット形式／ ETHERNET タイプ／ LSAP）
- あて先MAC情報（MAC アドレス／パケット形式／ ETHERNET タイプ／ LSAP）
- VLAN ID
- COS値
- 送信元IP 情報（IP アドレス／アドレスマスク）
- あて先IP 情報（IP アドレス／アドレスマスク）
- TCP・UDPのポート番号
- ICMP TYPE、ICMP CODE
- IPパケットのTOS 値、DSCP値

2)優先制御情報書き換えの対象となるパケット入力ETHERポート

3)優先制御情報書き換えの対象となるパケットが入力ETHERポートに入力された場合の以下の動作

- パケットのDSCP値を指定した値で書き換える
- パケットのip precedence 値を指定した値で書き換える
- 入力パケットが出力される際に使用される出力ポートのキューを指定したキューに変更する

パケットのDSCP値を指定した値で書き換える

ここでは、VLAN内の特定ポートですべての入力パケットのDSCP値を指定した値で書き換える方法を説明します。

【書き換え要求】

VLAN10はInterface0/1～0/8で構成されるポートVLANで、すべてタグ付きである。
Interface0/1ポートでは全入力パケットのDSCP値を40に書き換える。

【コマンド】

すべてのパケットの形式を ACL で設定する。 -----(1)

```
(config)#acl 120 mac any any any
```

Interface0/1 ポートで(1)で設定した形式のパケットの DSCP 値を 40 に書き換える。

```
(config)#interface 0/1
(config-if)#qos aclmap 0 dscp 40 120
```

設定を保存する。

```
(config)#save
```

パケットの **ip precedence** 値を指定した値で書き換える

ここでは、VLAN内の特定ポートで特定のCOS値の入力パケットのip precedence 値を指定した値に書き換える方法を説明します。

【書き換え要求】

VLAN10はInterface0/1～0/8で構成されるポートVLANで、すべてタグ付きである。
VLAN10 では COS 値 5 のパケットが入力された場合に、入力パケットの ip precedence 値を 6 に書き換える。

【コマンド】

VLAN ID が 10 で COS 値が 5 のパケットの形式を ACL で設定する-----(1)
(config)#acl 150 vlan 10 5

VLAN10 に属する Interface0/1～0/8 ポートで(1)で設定した形式のパケットの ip precedence 値を 6 に書き換える。
(config)#interface range 0/1-0/8
(config-if)#qos aclmap 0 tos 6 150

設定を保存する。
(config)#save

VLAN単位でパケットの出力キューを変更する

ここでは、VLAN内のポートで特定のMACアドレスを持つホストからの入力パケットが出力ポートから出力される際に使用されるキューを変更する方法を説明します。

【書き換え要求】

VLAN20はInterface0/1～0/5で構成されるポートVLANで、Interface0/1～0/4ポートでタグ付き、Interface0/5ポートでタグなしである。
VLAN20 では MAC アドレス 00:0b:01:02:03:04 のホストからの入力パケットが出力される際に使用される出力ポートのキューを 3 に変更する。

【コマンド】

送信元MACアドレスが00:0b:01:02:03:04であるパケットの形式をACLで設定する。---------(1)
(config)#acl 100 mac 00:0b:01:02:03:04 any any

VLAN20 で(1)で設定した形式のパケットが出力される際に使用されるキューを変更する。
(config)#vlan 20 qos aclmap 0 queue 3 100

設定を保存する。
(config)#save

こんなことに気をつけて

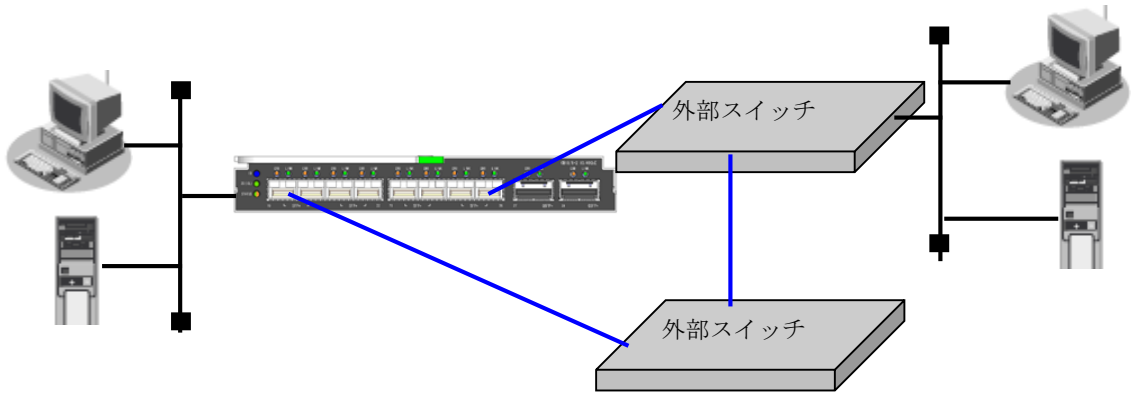
プロトコル VLAN 機能と併用した場合、プロトコル VLAN として認識されるフレームへの QoS 機能は無効となります。
なお、プロトコル VLAN として認識されるフレームについては “vlan protocol” コマンド項目を参照してください。
MAC フィルタリング機能と併用した場合、MAC フィルタリング機能に該当したパケットに対する QoS 機能は無効となります。

7 STP 機能を使う

ここでは、STP 機能を使用する場合の設定方法を説明します。

STP を使う

STP を使用すると、物理的にループしているネットワークでも、論理的にループしないようにすることができます。これによって、ネットワーク内のデータを円滑に流すことができます。



【設定条件】

STPを使用する。

Interface0/19、0/26 ポートをVID10のポートVLANとする。

【コマンド】

Interface0/19、0/26 に VLAN10 を設定する。

```
(config)#interface range 0/19,0/26
(config-if)#vlan untag 10
```

Interface0/19、0/26 に STP を設定する。

```
(config)#interface range 0/19,0/26
(config-if)#stp use on
```

設定を保存する。

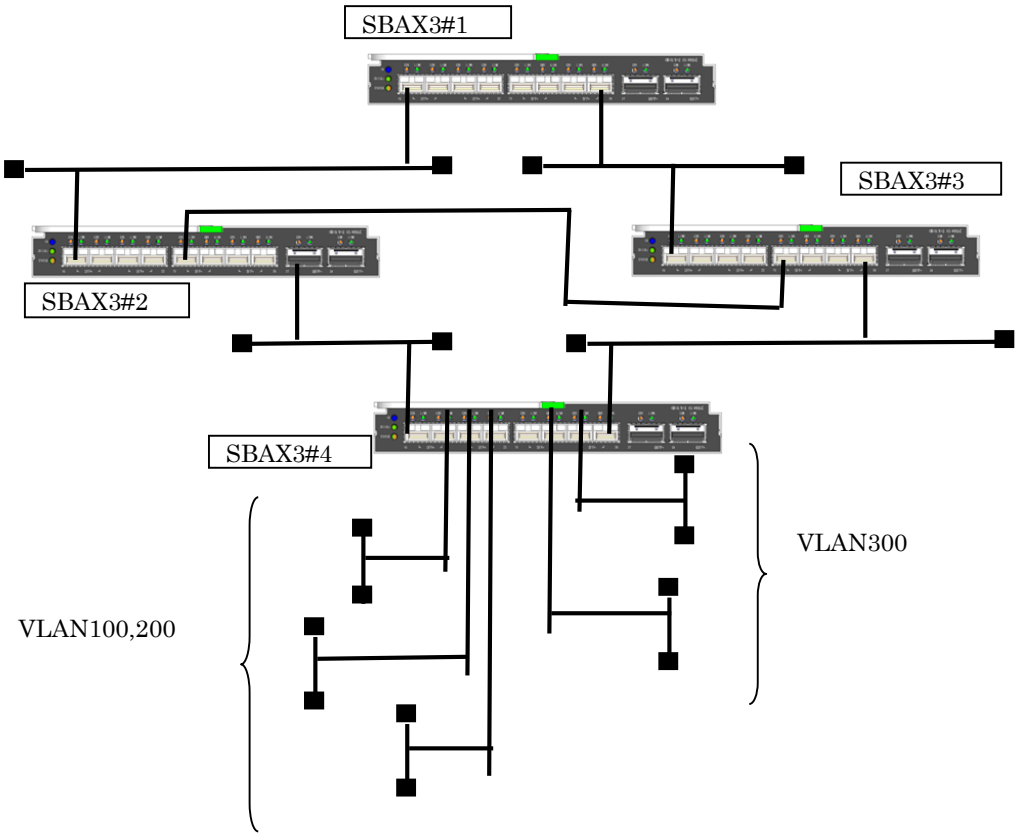
```
(config)#save
```

MSTP を使う

物理的にループしているネットワークでも、VLAN の構成によっては、論理的にループしない場合があります。STP ではループと判断して、一方の LAN を通信に使わないで動作しますが、MSTP では VLAN 単位に扱うことができるため、STP よりも効率的にネットワーク内のデータを流すことができます。

【設定条件】

以下のようなVLAN環境下でMSTPを併用したVLAN単位でフレームの制御を行う。



[インスタンス 0]
ブリッジの優先順位: SBAX3#1 -> SBAX3#2 -> SBAX3#3 -> SBAX3#4

[インスタンス 1]
ブリッジの優先順位: SBAX3#1 -> SBAX3#2 -> SBAX3#3 -> SBAX3#4
VLAN 割り当て 100、200

[インスタンス 2]
ブリッジの優先順位: SBAX3#1 -> SBAX3#3 -> SBAX3#2 -> SBAX3#4
VLAN 割り当て 300

<SBAX3#1>
interface0/19 を SBAX3#2 に接続する。
interafce0/26 を SBAX3#3 に接続する。
interface 0/19 と 0/26 の STP パスコストを全インスタンスで 20000 とする。

<SBAX3#2>
interface0/19 を SBAX3#1 に接続する。
interafce0/23 を SBAX3#3 に接続する。
interafce0/26 を SBAX3#4 に接続する。
interface 0/19、0/2３、0/26 の STP パスコストを全インスタンスで 20000 とする。

<SBAX3#3>
interface0/19 を SBAX3#1 に接続する。
interafce0/23 を SBAX3#2 に接続する。
interafce0/26 を SBAX3#4 に接続する。
interface 0/19、0/2３、0/26 の STP パスコストを全インスタンスで 20000 とする。

<SBAX3#4>
interface0/19 を SBAX3#2 に接続する。
interafce0/26 を SBAX3#3 に接続する。
interface 0/19、0/26 の STP パスコストを全インスタンスで 20000 とする。
Interface0/20-0/21 で VLAN100 の端末と接続する。
Interface0/22 で VLAN200 の端末と接続する。
Interface0/24-0/25 で VLAN300 の端末と接続する。

【コマンド】
<SBAX3#1>
interface0/19、0/23 に STP パスコストを設定する。
(config)#interface range 0/19,0/23
(config-if)#stp domain 0 cost 20000
(config-if)#stp domain 1 cost 20000

(config-if)#stp domain 2 cost 20000

VLAN を設定する。
(config)#interface range 0/19,0/23
(config-if)#vlan tag 100,200,300

STP を設定する。
(config)#stp mode mstp
(config)#stp domain 1 vlan 100,200
(config)#stp domain 2 vlan 300
(config)#stp domain 0 priority 4096
(config)#stp domain 1 priority 4096
(config)#stp domain 2 priority 4096

設定を保存する。
(config)#save

<SBAX3#2>
interface0/19、0/23、0/26 に STP パスコストを設定する。
(config)#interface range 0/19,0/23,0/26
(config-if)#stp domain 0 cost 20000
(config-if)#stp domain 1 cost 20000
(config-if)#stp domain 2 cost 20000

VLAN を設定する。
(config)#interface range 0/19,0/23,0/26
(config-if)#vlan tag 100,200,300

STP を設定する。
(config)#stp mode mstp
(config)#stp domain 1 vlan 100,200
(config)#stp domain 2 vlan 300
(config)#stp domain 0 priority 8192
(config)#stp domain 1 priority 8192
(config)#stp domain 2 priority 12288

設定を保存する。
(config)#save

<SBAX3#3>
interface0/19、0/23、0/26 に STP パスコストを設定する。
(config)#interface range 0/19,0/23,0/26
(config-if)#stp domain 0 cost 20000
(config-if)#stp domain 1 cost 20000
(config-if)#stp domain 2 cost 20000

VLAN を設定する。
(config)#interface range 0/19,0/23,0/26
(config-if)#vlan tag 100,200,300

STP を設定する。
(config)#stp mode mstp

```
(config)#stp domain 1 vlan 100,200
(config)#stp domain 2 vlan 300
(config)#stp domain 0 priority 12288
(config)#stp domain 1 priority 12288
(config)#stp domain 2 priority 8192
```

設定を保存する。

```
(config)#save
```

<SBAX3#4>

interface0/19、0/26 に STP パスコストを設定する。

```
(config)#interface range 0/19,0/26
(config-if)#stp domain 0 cost 20000
(config-if)#stp domain 1 cost 20000
(config-if)#stp domain 2 cost 20000
```

VLAN を設定する。

```
(config)#interface range 0/19,0/26
(config-if)#vlan tag 100,200,300
```

STP を設定する。

```
(config)#stp mode mstp
(config)#stp domain 1 vlan 100,200
(config)#stp domain 2 vlan 300
(config)#stp domain 0 priority 32768
(config)#stp domain 1 priority 32768
(config)#stp domain 2 priority 32768
```

設定を保存する。

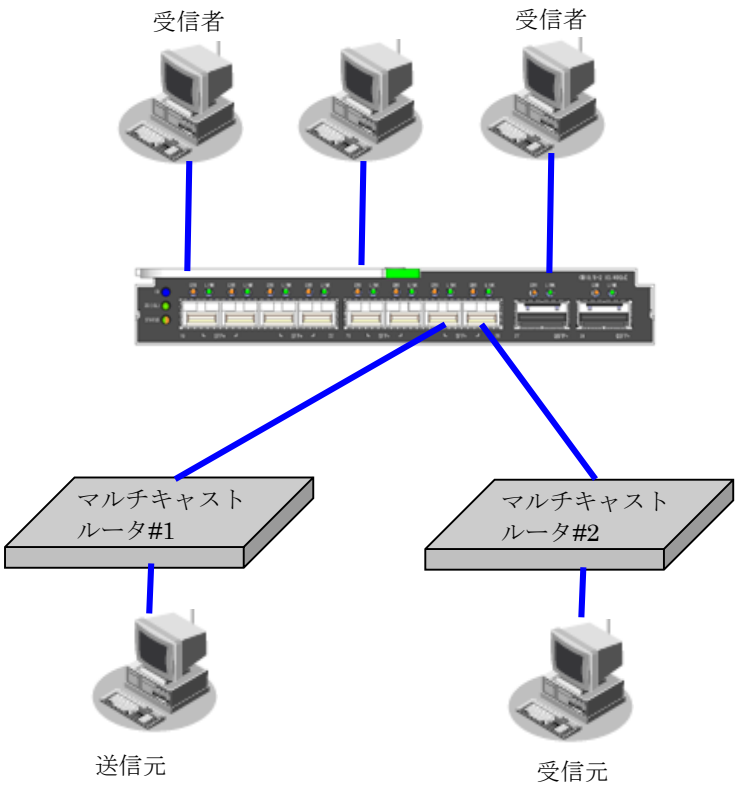
```
(config)#save
```

8 IGMP スヌープ機能を使う

IGMP スヌープ機能を使用すると、マルチキャスト・パケットを必要としているポートを IGMP パケットから検出し、そのポート以外へはマルチキャスト・パケットを転送しません。これにより、無用なトラフィックを端末やサーバに送出することが防止でき、マルチキャストを利用しているネットワークで端末やサーバの負荷を軽減することができます。

こんなことに気をつけて

- IGMP を利用しないでマルチキャスト通信を行っている場合、通信できなくなる可能性があります。
- IGMP スヌープが有効である装置と接続するポートは、構成定義でマルチキャストルータポートとして設定してください。
- マルチキャストルータが 2 台以上接続される場合は、マルチキャストルータポートを構成定義で設定してください。マルチキャストルータポートが正しく認識されなくなり、マルチキャストルータの先に接続される端末がマルチキャスト・パケットを受信できなくなる場合があります。
- 本装置では、一度登録されたグループアドレスはリスナ端末が存在しなくなった場合でもエントリ自体を消去しないで、出力ポートの情報だけを消去します。不要なグループアドレスが登録されている場合は、clear igmpsnoop group コマンドで消去することができます。
- 最大登録可能なマルチキャストグループアドレス数を超えた場合、超えたアドレスはすべて同一 VLAN 内にフラッディングされます。扱われるグループアドレスが最大登録可能数を超える場合は、IGMP スヌープ機能は利用しないでください。
- 本装置では 224.1.1.1 と 225.1.1.1 や 224.1.1.1 と 225.129.1.1 のように、IP アドレスの下位 23 ビットが同じアドレスについては、同一アドレスとして認識されます。そのため、これらのアドレスで待ち合わせする異なるリスナ端末が存在した場合でも両方のアドレスあてのパケットが転送されます。
- IGMP スヌープ機能を有効にすると、vlan igmpsnoop source 定義がないと送信元アドレスとして 0.0.0.0 を使用します。送信元アドレスが 0.0.0.0 である IGMP Query パケットを扱えない装置が接続されている場合、vlan igmpsnoop source 定義で送信元アドレスを設定してください。なお、マルチキャストルータが接続されているネットワークではマルチキャストルータのアドレスより大きな値となるアドレスを送信元アドレスとして指定してください。
- IGMP V1/V2 が混在する環境では、vlan igmpsnoop proxy 定義で off（代理応答しない）を選択してください。
- IPv4 マルチキャスト以外の通信（例：IPv6 通信）を利用するネットワークでは利用できません。IGMP スヌープ機能は有効にしないでください。
- マルチキャストルータが接続されないネットワークでは、vlan igmpsnoop querier コマンドで Querier 動作を無効としないでください。



【設定条件】

IGMPスヌープ機能を利用する

リスナ端末はそれぞれ以下に属する。

リスナ端末 1	ポート: Interface0/1、0/2 VLAN: 10
リスナ端末 2	ポート:Interface0/3、0/4 VLAN:11
リスナ端末 3	ポート:Interface0/5、0/6 VLAN:12

マルチキャストルータ1 はタグVLANを使用し、VLAN10 ～ 12 を設定する

ポートはInterface0/25に接続する

マルチキャストルータ2 はVLAN10 に属し、ポートはInterface0/26 に接続する

【コマンド】

IGMP スヌープ機能を使用する

```
(config)#igmpsnoop use on

(config)#interface range 0/1-0/2
(config-if)vlan untag 10
```

```
(config)#interface 0/3-0/4
(config-if)#vlan untag 11
(config)#interface 0/5-0/6
(config-if)#vlan untag 12
(config)#interface 0/25
(config-if)#vlan tag 10,11,12
(config)#interface 0/26
(config-if)#vlan untag 10
```

複数のマルチキャストルータが接続される VLAN10 にマルチキャストルータポートを設定する

```
(config)#vlan 10 igmpsnoop router yes 25,26
```

設定を保存する。

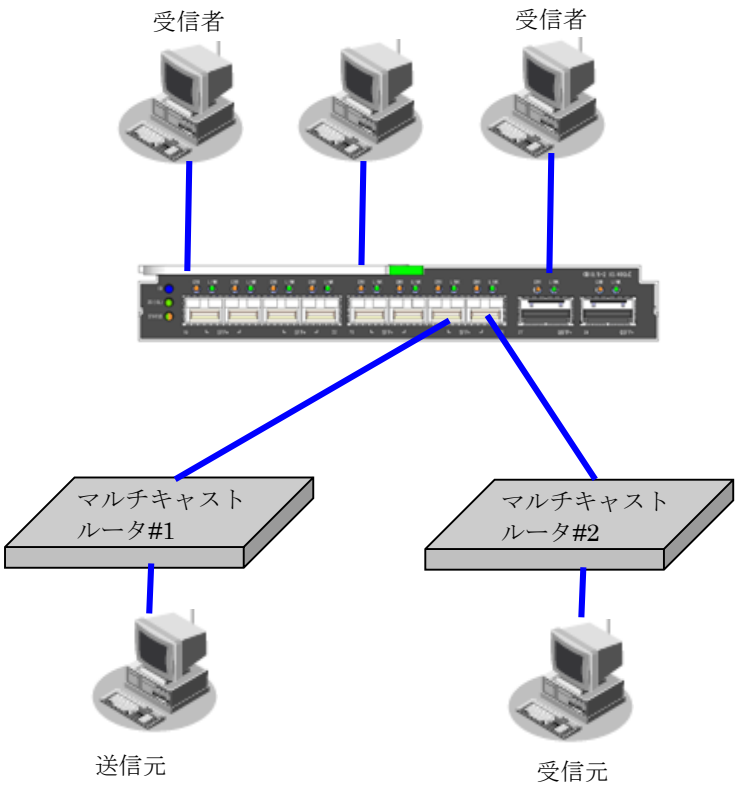
```
(config)#save
```

9 MLD スヌープ機能を使う

MLD スヌープ機能を使用すると、IPv6 マルチキャスト・パケットを必要としているポートを MLD パケットから検出し、そのポート以外へは IPv6 マルチキャスト・パケットを転送しません。これにより、無用なトラフィックを端末やサーバに送出することが防止でき、IPv6 マルチキャストを利用しているネットワークで端末やサーバの負荷を軽減することができます。

こんなことに気をつけて

- MLD を利用しないで IPv6 マルチキャスト通信を行っている場合、通信できなくなる可能性があります。
- MLD スヌープが有効である装置と接続するポートは、構成定義でマルチキャストルータポートとして設定してください。
- マルチキャストルータが 2 台以上接続される場合は、マルチキャストルータポートを構成定義で設定してください。マルチキャストルータポートが正しく認識されなくなり、マルチキャストルータの先に接続される端末が IPv6 マルチキャスト・パケットを受信できなくなる場合があります。
- 本装置では、一度登録されたグループアドレスはリスナ端末が存在しなくなった場合でもエントリ自体を消去しないで、出力ポートの情報だけを消去します。不要なグループアドレスが登録されている場合は、clear mldsnoop group コマンドで消去することができます。
- 最大登録可能なマルチキャストグループアドレス数を超えた場合、超えたアドレスはすべて同一 VLAN 内にフラッディングされます。扱われるグループアドレスが最大登録可能数を超える場合は、MLD スヌープ機能は利用しないでください。
- MLD スヌープ機能を有効にすると、vlan mldsnoop source 定義がないと送信元アドレスとして :: を使用します。送信元アドレスが :: である MLD Query パケットを扱えない装置が接続されている場合、vlan mldsnoop source 定義で送信元アドレスを設定してください。なお、マルチキャストルータが接続されているネットワークではマルチキャストルータのアドレスより大きな値となるアドレスを送信元アドレスとして指定してください。
- IPv4 マルチキャストを使用するネットワークでは IGMP スヌープ機能も有効にしてください。
- IP 以外のマルチキャスト通信を利用するネットワークでは利用できません。MLD スヌープ機能は有効にしないでください。
- マルチキャストルータが接続されないネットワークでは、vlan mldsnoop querier コマンドで Querier 動作を無効としないでください。



【設定条件】

MLDスヌープ機能を利用する

リスナ端末はそれぞれ以下に属する。

リスナ端末 1	ポート: Interface0/1、0/2 VLAN: 10
リスナ端末 2	ポート:Interface0/3、0/4 VLAN:11
リスナ端末 3	ポート:Interface0/5、0/6 VLAN:12

マルチキャストルータ1 はタグVLANを使用し、VLAN10 ～ 12 を設定する

ポートはInterface0/25に接続する

マルチキャストルータ2 はVLAN10 に属し、ポートはInterface0/26 に接続する

【コマンド】

MLD スヌープ機能を使用する

```
(config)#mldsnoop use on

(config)#interface range 0/1-0/2
(config-if)vlan untag 10
```

```
(config)#interface 0/3-0/4
(config-if)#vlan untag 11
(config)#interface 0/5-0/6
(config-if)#vlan untag 12
(config)#interface 0/25
(config-if)#vlan tag 10,11,12
(config)#interface 0/26
(config-if)#vlan untag 10
```

複数のマルチキャストルータが接続される VLAN10 にマルチキャストルータポートを設定する

```
(config)#vlan 10 mldsnoop router yes 25,26
```

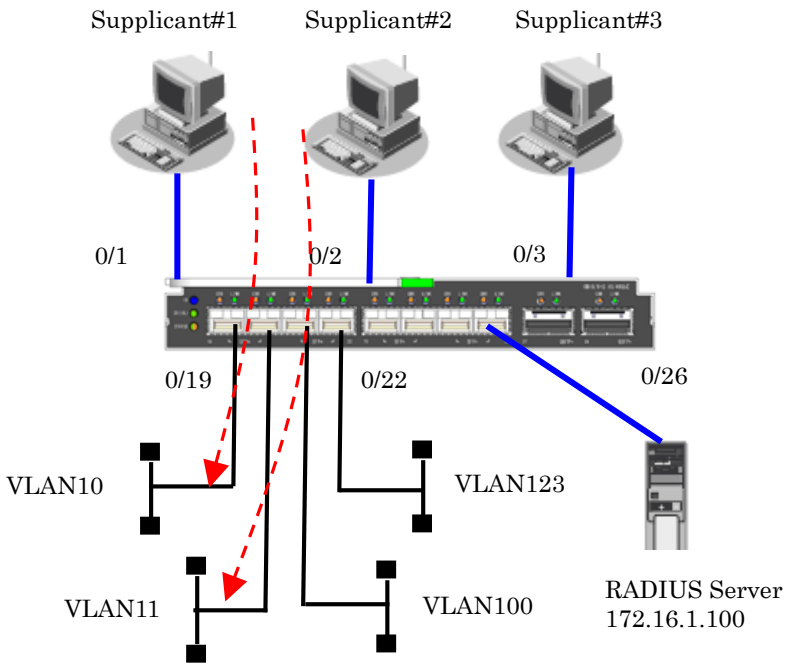
設定を保存する。

```
(config)#save
```

10　IEEE802.1X 認証機能を使う

IEEE802.1X 認証を使用すると、本装置に接続する端末ユーザがネットワークへのアクセス権限を持っているかを認証することができます。また、認証データベースで、ユーザごとに所属するVLAN ID を設定すると、認証されたユーザが所属するネットワークも同時に管理できます。これらの機能によりネットワークへのアクセスをユーザ単位で制御でき、ネットワークのセキュリティを向上することができます。

こんなことに気をつけて
IEEE802.1X 認証を利用するポートにはVLAN ID を設定しないでください。
IEEE802.1X 認証で利用するAAAのグループID を正しく設定してください。
ローカル認証で利用できる認証方式はEAP-MD5だけです。
1つの物理ポートで複数端末の認証を行う環境で確認済みのサプリカントソフトは富士通製
「Systemwalker Desktop
Inspection 802.1X サプリカント」です。
1つの物理ポートで複数端末の認証を行う環境では課金情報のうち以下の項目が正しく採取できません。
- 送信パケット数
- 受信パケット数
- 送信バイト数
- 受信バイト数



【設定条件】

Interface0/1～0/3ポートでIEEE802.1X 認証を使用する

Interface0/1～0/3ポートで利用する認証データベース

-Interface0/1、0/2ポート :RADIUSサーバ

-Interface0/3ポート :ローカルで設定した認証情報

AAAグループID

-Interface0/1、0/2ポート：0

-Interface0/3 ポート：1

Supplicant のMACアドレスごとに認証を行う

Inetrafce0/3 ポートで利用可能なユーザは以下のとおり

ユーザ ID	パスワード	割り当てる VLAN ID
Supp1	Supp1-pass	VLAN123
Supp2	Supp2-pass	VLAN100

RADIUS サーバの IP アドレス： 172.16.1.100

RADIUS サーバは VLAN13 に接続されている。

RADIUS サーバのシークレット:radius-secret

Interface0/1、0/2 ポートで利用する RADIUS サーバで、認証処理と課金情報（※）の収集を行う。

※)本装置がサポートする課金情報と対応する属性を以下に示します。

- 接続時間 Acct-Session-Time
- 送信パケット数 Acct-Output-Packets
- 受信パケット数 Acct-Input-Packets
- 送信バイト数 Acct-Output-Octets
- 受信バイト数 Acct-Input-Packets

こんなことに気をつけて

RADIUSサーバにはユーザにVLAN ID を割り当てるために以下の属性を設定してください。設定方法については

RADIUSサーバのマニュアルを参照してください。

名前	番号	属性値(※)
Tunnel-Type	64	VLAN (13)
Tunnel-Media-Type	65	802 (6)
Tunnel-Private-Group-ID	81	VLAN ID (10 進数表記を ASCII コードでコーディング)

※ ()内の数字は属性として設定される 10 進数の値

タグにより複数のトンネル属性が設定されている場合は、利用可能な値が指定されているもっとも小さなタグの情報がユーザに割り当てるVLAN情報として選択されます。

【コマンド】

IEEE802.1x 認証を使用する

```
(config)#dot1x use on
```

RADIUS サーバを接続するポートを設定する。

```
(config)#interface 0/26
(config-if)#vlan untag 13
```

RADIUS サーバの VLAN を設定する。

```
(config)#lan 0 vlan 13
(config)#lan 0 ip address 172.16.1.101/16 3
```

IEEE802.1X により認証された Supplicant が接続される VLAN 情報を設定する。

```
(config)#interface 0/19
(config-if)#vlan untag 10
(config)#interface 0/20
(config-if)#vlan untag 11
(config)#interface 0/21
(config-if)#vlan untag 100
(config)#interface 0/22
(config-if)#vlan untag 123
```

IEEE802.1X 認証ポートを設定する。

```
(config)#interface 0/1
(config-if)#dot1x aaa 0
(config-if)#dot1x use on
(config)#interface 0/2
(config-if)#dot1x aaa 0
(config-if)#dot1x use on
(config)#interface 0/3
(config-if)#dot1x aaa 1
(config-if)#dot1x use on
```

RADIUS サーバを利用する AAA グループ情報を設定する

```
(config)#aaa 0 name radiusAuth
(config)#aaa 0 radius service client both
(config)#aaa 0 radius auth source 172.16.1.101
(config)#aaa 0 radius client server-info auth secret radius-secret
(config)#aaa 0 radius client server-info auth address 172.16.1.100
(config)#aaa 0 radius client server-info accounting secret radius-secret
(config)#aaa 0 radius client server-info accounting address 172.16.1.100
```

ローカル認証情報を利用する AAA グループ情報を設定する。

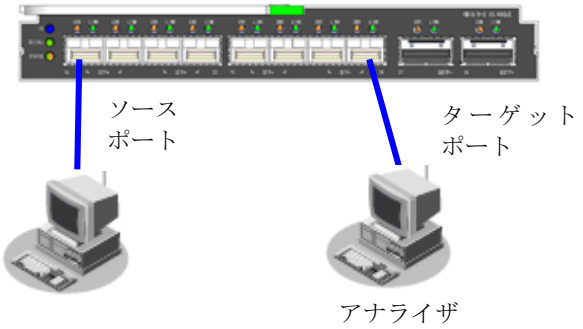
```
(config)# aaa 1 name localAuth
(config)# aaa 1 user 0 id Supp1
(config)# aaa 1 user 0 password Supp1-pass
(config)# aaa 1 user 0 supplicant vid 123
(config)# aaa 1 user 1 id Supp2
(config)# aaa 1 user 1 password Supp2-pass
(config)# aaa 1 user 1 supplicant vid 100
```

設定を保存する。

```
(config)#save
```

11　ポートミラーリング機能を使う

ポート・ミラーリング機能を利用すると、指定したターゲット・ポートから、指定したソース・ポートの受信/送信トラフィックを監視することができます。ここでは、Interface0/19ポートをソース・ポート、Interface0/26 ポートをターゲット・ポートとして設定し、ソース・ポートの受信トラフィックをターゲット・ポートへミラーリングする場合の設定方法を説明します。



<Configuration target>
Interface0/19 ポートをソースポートとする（受信フレーム指定）
Interace0/26 ポートをターゲットポートとする

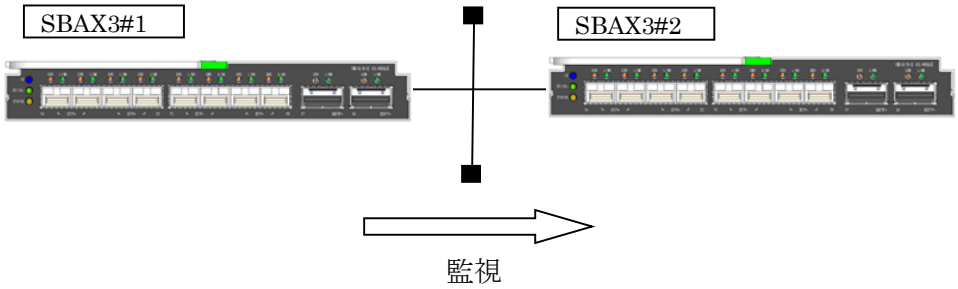
<Commands>
Interface0/26 のポートをミラーポートに設定する。
(config)#interface 0/26
(config-if)#type mirror port 0 19 rx

設定を保存する。
(config)#save

12　Ether L3 監視機能を使う

ether L3 監視機能を使用すると、指定したETHERポートから監視相手装置を監視することによって、経路上の
障害を検出および監視をしているポートを閉塞します。
ここでは、ether L3 監視機能を使用する場合の設定方法を説明します。

こんなことに気をつけて
閉塞されたポートは自動では復旧しません。online コマンドで復旧させてください。



【設定条件】

Interface0/19ポートを使用する

VLAN IDとネットワークアドレスを以下のように対応付ける

　　VLAN ID：1　　ネットワークアドレス：192.168.10.0/24

ether L3監視機能を使用する

【コマンド】

SBAX3#1

Interface0/19 ポートを設定する。

(config)#interface range 0/19
(config-if)#vlan untag 1

192.168.10.1/24 のネットワークを設定する

(config)#lan 0 ip address 192.168.10.1/24 3
(config)#lan 0 vlan 1

監視あて先 IP アドレスを設定する

(config)#interface 0/19
(config-if)#icmpwatch address 192.168.10.2

監視間隔を設定する。

(config)#interface 0/19
(config-if)#icmpwatch interval 15s 40s 5s

設定を保存する。

(config)#save

SBAX3#2

Interface0/19 ポートを設定する。

(config)#interface range 0/19
(config-if)#vlan untag 1

192.168.10.1/24 のネットワークを設定する
(config)#lan 0 ip address 192.168.10.2/24 3
(config)#lan 0 vlan 1

設定を保存する。
(config)#save

リンクアグリゲーション機能を使用した ether L3 監視機能を使う

ここではリンクアグリゲーション機能を利用したポートで ether L3 監視機能を使用する場合の設定方法を説明します。

【設定条件】
Interface0/1～0/4ポートを使用する
VLAN IDとネットワークアドレスを以下のように対応付ける
　　VLAN ID：10　　ネットワークアドレス：192.168.10.0/24
ether L3監視機能を使用する

【コマンド】
SBAX3#1
Interface0/1～0/4 ポートを設定する。
(config)#interface range 0/1-0/4
(config-if)#vlan tag 10

Interface0/1～0/4 ポートをリンクアグリゲーションとして設定する。
(config)# interface range 0/1-0/4
(config-if)#type linkaggregation 1

192.168.10.1/24 のネットワークを設定する
(config)#lan 0 ip address 192.168.10.1/24 3
(config)#lan 0 vlan 10

監視あて先 IP アドレスを設定する
(config)#linkaggregation 1 icmpwatch address 192.168.10.2

監視間隔を設定する。
(config)#linkaggregation 1 icmpwatch interval 15s 40s 5s

設定を保存する。
(config)#save

【コマンド】
SBAX3#2
Interface0/1～0/4 ポートを設定する。

(config)#interface range 0/1-0/4
(config-if)#vlan tag 10

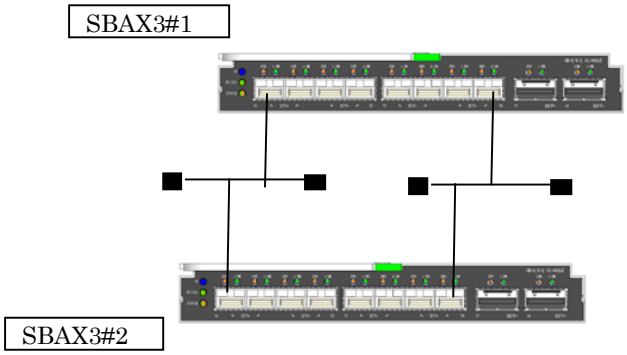
Interface0/1～0/4 ポートをリンクアグリゲーションとして設定する。
(config)# interface range 0/1-0/4
(config-if)#type linkaggregation 1

192.168.10.1/24 のネットワークを設定する
(config)#lan 0 ip address 192.168.10.1/24 3
(config)#lan 0 vlan 10

設定を保存する。
(config)#save

13　ポート閉塞機能を使う

ポート閉塞機能を利用すると、間欠障害発生時にも接続ポートが閉塞状態を保持するため、安定した通信を保つ
ことができます。
ここでは、バックアップポート機能と併用し、マスタポートの間欠障害発生時にはマスタポートを閉塞し、バッ
クアップポートだけを使用する場合を例に説明します。



【設定条件】
SBAX3#1
各装置でInterface0/19、0/26 ポートをバックアップポートとして使用する
（Interface0/19をマスタポート、Interface0/26 をバックアップポートとし、マスタポートを優先的に使用する）
• リンクダウン回数による閉塞を行う
• リンクダウン回数の上限値の設定

SBAX3#2
各装置でInterface0/19、0/26 ポートをバックアップポートとして使用する
（Interface0/19 をマスタポート、Interface0/26 をバックアップポートとし、マスタポートを優先的に使用する）
• リンクダウン回数による閉塞を行う
• リンクダウン回数の上限値の設定

【コマンド】
SBAX3#1
Interface0/19 ポートでリンクダウン回数の上限値を設定する。
(config)#interface 0/19
(config-if)#recovery limit 5

Interface 0/19 ポートをバックアップポート(グループ)のマスタポートに設定する。
(config)#interface 0/19
(config-if)#type backup 1 master

Jan 01 10:13:43 127.0.0.1 SBAX3: l2nsm: backup 1 definition is invalid. backup port is not defined.
(このようにバックアップグループで master または backup のみを定義した場合、他方が存在せず無効というメッセージが表示されます。バックアップグループには master と backup の両方を定義する必要があるためです。続けて他方の定義を行えばバックアップグループの機能が有効になります。)

Interface 0/26 ポートをバックアップポート(グループ)のバックアップポートに設定する。
(config)#interface 0/26
(config-if)#type backup 1 backup

バックアップグループ 1 をマスタポート優先モードに設定する。
(config)#backup 1 mode master

設定を保存する。
(config)#save

SBAX3#2
Interface0/19 ポートでリンクダウン回数の上限値を設定する。
(config)#interface 0/19
(config-if)#recovery limit 5

Interface 0/19 ポートをバックアップポート(グループ)のマスタポートに設定する。
(config)#interface 0/19
(config-if)#type backup 1 master
Jan 01 10:18:13 127.0.0.1 SBAX3: l2nsm: backup 1 definition is invalid. backup port is not defined.

Interface 0/26 ポートをバックアップポート(グループ)のバックアップポートに設定する。
(config)#interface 0/26
(config-if)#type backup 1 backup

バックアップグループ 1 をマスタポート優先モードに設定する。
(config)#backup 1 mode master

設定を保存する。
(config)#save

14　IP フィルタリング機能を使う

本装置を経由してインターネットに送出されるパケット、またはインターネットから受信したパケットを IP アドレスとポート番号の組み合わせで制御することによって、ネットワークのセキュリティを向上させることができます。

IP フィルタリングの条件

本装置では、ACL 番号で指定したACL 定義の中で、以下の条件を指定することによってデータの流れを制御できます。

- プロトコル
- 送信元情報（IP アドレス／アドレスマスク／ポート番号）
- あて先情報（IP アドレス／アドレスマスク／ポート番号）
- IPパケットのTOS 値DSCP値

ヒント

◆ IP アドレスとアドレスマスクの決め方

フィルタリング条件の要素には「IP アドレス」と「アドレスマスク」があります。制御対象となるパケッ
トは、本装置に届いたパケットのIP アドレスとアドレスマスクの論理積の結果が、指定したIPアドレスと一致したものに限ります。

IP フィルタリングの設計方針

IP フィルタリングの設計方針には大きく分類して以下の2つがあります。

A. 基本的にパケットをすべて遮断し、特定の条件のものだけを透過させる。

B. 基本的にパケットをすべて透過させ、特定の条件のものだけを遮断する。

ここでは、設計方針Aの例として、以下の設定例について説明します。

- 外部の特定サービスへのアクセスだけを許可する
- 外部から特定サーバへのアクセスだけを許可する

また、設計方針Bの例として、以下の設定例について説明します。

- 外部の特定サーバへのアクセスだけを禁止する
- 外部から特定サーバへのping だけを禁止する

こんなことに気をつけて

- IPフィルタリング条件が複数存在する場合、それぞれの条件に優先順位がつき、数値の小さいものから優先的に採用されます。設定内容によっては通信できなくなる場合がありますので、優先順位を意識して設定してください。

14.1 外部の特定サービスへのアクセスだけを許可する

ここでは、一時的にLANを作成し、外部LANのすべてのWeb サーバに対してアクセスすることだけを許可し、
ほかのサーバ（FTP サーバなど）へのアクセスを禁止する場合の設定方法を説明します。ただし、Web サーバ名を解決するために、DNSサーバへのアクセスは許可します。

【設定条件】

Interface0/1ポートを使用する

VLAN IDとネットワークアドレスを以下のように対応付ける

VLAN ID：10　　ネットワークアドレス：192.168.10.0/24

【フィルタリング設計】

内部LANのホスト(192.168.1.0/24)から外部LANのWebサーバへのアクセスを許可

内部LANのホスト(192.168.1.0/24)から外部LANのDNSサーバへのアクセスを許可

ICMPの通信を許可

その他はすべて遮断

こんなことに気をつけて

ICMPは、IP 通信を行う際にさまざまな制御メッセージを交換します。ICMPの通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPの通信を透過させる設定を行ってください。

【フィルタリングルール】

・Webサーバへのアクセスを許可するには

（1）192.168.1.0/24 の任意のポートから、任意のWeb サーバのポート80（http）へのTCPパケットを透過させる

・DNSサーバへのアクセスを許可するには

（1）192.168.1.0/24 の任意のポートから、DNSサーバのポート53（domain）へのUDPパケットを透過させる

・ICMPの通信を許可するためには

（1）ICMPパケットを透過させる

・その他をすべて遮断するには

（1）すべてのパケットを遮断する

【コマンド】

Interface0/1 ポートを設定する。

```
(config)#interface 0/1
(config-if)#vlan tag 10
```

192.168.10.0/24 のネットワークを設定する

```
(config)#lan 0 ip address 192.168.10.0/24 3
(config)#lan 0 vlan 10
```

任意の Web サーバのポート 80 への TCP パケットを透過させる

```
(config)#acl 0 ip 192.168.1.0/24 any 6 any
(config)#acl 0 tcp any 80
(config)#lan 0 ip filter 0 pass acl 0
```

DNS サーバのポート 53 への UDP パケットを透過させる

```
(config)#acl 1 ip 192.168.1.0/24 192.168.0.10/32 17 any
(config)#acl 1 udp any 53
(config)#lan 0 ip filter 1 pass acl 1
```

ICMP のパケットを透過させる

```
(config)#acl 2 ip any any 1 any
(config)#acl 2 icmp any any
(config)#lan 0 ip filter 2 pass acl 2
```

残りのパケットをすべて遮断する

```
(config)#acl 3 ip any any any
(config)#lan 0 ip filter 3 reject acl 3
```

設定を保存する。

```
(config)#save
```

14.2 外部の特定サービスへのアクセスだけを許可する(IPv6 フィルタリング)

ここでは、一時的に LAN を作成し、外部 LAN のすべての Web サーバに対してアクセスすることだけを許可し、ほかのサーバ（ftp サーバなど）へのアクセスを禁止する場合の設定方法を説明します。ただし、Web サーバ名を解決するために、DNS サーバへのアクセスは許可します。

【設定条件】
Interface0/1ポートを使用する
VLAN IDとネットワークアドレスを以下のように対応付ける
　　VLAN ID：10　　ネットワークアドレス：2001:db8:1::/64

【フィルタリング設計】
内部 LAN 上のホスト（2001:db8:1::/64）から任意の Web サーバへのアクセスを許可
内部 LAN 上のホスト（2001:db8:1::/64）から外部 LAN の DNS サーバへのアクセスを許可
ICMPv6 の通信を許可
その他はすべて遮断

こんなことに気をつけて
ICMPv6 は、IPv6 通信を行う際にさまざまな制御メッセージを交換します。ICMPv6 の通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPv6 の通信を透過させる設定を行ってください

【フィルタリングルール】
・Web サーバへのアクセスを許可するには
（1）2001:db8:1::/64 の任意のポートから、任意のアドレスのポート 80（http）への TCP パケットを透過させる
・DNS サーバへのアクセスを許可するには
（1）2001:db8:1::/64 の任意のポートから DNS サーバのポート 53（domain）への UDP パケットを透過させる
・ICMPv6 の通信を許可するためには
（1）ICMPv6 パケットを透過させる
・その他をすべて遮断するには
（1）すべてのパケットを遮断する

【コマンド】
Interface0/1 ポートを設定する。
(config)#interface 0/1
(config-if)#vlan tag 10

2001:db8:1::/64 のネットワークを設定する
(config)#lan 0 ip6 address 2001:db8:1::/64
(config)#lan 0 vlan 10

任意の Web サーバのポート 80 への TCP パケットを透過させる

```
(config)# acl 0 ip6 2001:db8:1::/64 any 6 any
(config)# acl 0 tcp any 80
(config)# lan 0 ip6 filter 0 pass acl 0
```

DNS サーバのポート 53 への UDP パケットを透過させる

```
(config)# acl 1 ip6 2001:db8:1::/64 any 17 any
(config)# acl 1 udp any 53
(config)# lan 0 ip6 filter 1 pass acl 1
```

ICMPv6 のパケットを透過させる

```
(config)# acl 2 ip6 any any 58
(config)# acl 2 icmp any any
(config)# lan 0 ip6 filter 2 pass acl 2
```

残りのパケットをすべて遮断する

```
(config)# acl 3 ip6 any any any any
(config)# lan 0 ip6 filter 3 reject acl 3
```

設定終了

```
(config)# save
```

14.3 外部から特定サーバへのアクセスだけを許可する

ここでは、内部LANの特定サーバに対するアクセスを許可し、ほかのサーバに対するアクセスを禁止する場合の設定方法を説明します。ただし、Web サーバ名を解決するためにDNSサーバへのアクセスは許可します。

【設定条件】
Interface0/1ポートを使用する
VLAN IDとネットワークアドレスを以下のように対応付ける
　　VLAN ID：10　　ネットワークアドレス：192.168.10.0/24

【フィルタリング設計】
内部 LAN のホスト（192.168.1.5/32）を Web サーバとして利用を許可
内部 LAN のネットワークへの DNS サーバへのアクセスを許可
ICMP の通信を許可
その他はすべて遮断

こんなことに気をつけて
ICMP は、IP 通信を行う際にさまざまな制御メッセージを交換します。ICMP の通信を遮断すると正常な通信ができなくなる場合がありますので、ICMP の通信を透過させる設定を行ってください。

【フィルタリングルール】
・内部 LAN のホストの Web サーバとしての利用を許可するには
（1）192.168.1.5/32 のポート 80（http）への TCP パケットを透過させる
・DNS サーバへのアクセスを許可するには
（1）192.168.0.0/24 の任意のポートから DNS サーバのポート 53（domain）への UDP パケットを透過させる
・ICMP の通信を許可するためには
（1）ICMP パケットを透過させる
・その他をすべて遮断するには
（1）すべてのパケットを遮断する

【コマンド】
Interface0/1 ポートを設定する。
(config)#interface 0/1
(config-if)#vlan tag 10

192.168.10.0/24 のネットワークを設定する
(config)#lan 0 ip address 192.168.10.0/24 3
(config)#lan 0 vlan 10

LAN 上のホストのポート 80 への TCP パケットを透過させる
(config)# acl 0 ip 192.168.0.0/24 any 6 any

```
(config)# acl 0 tcp any 80
(config)# lan 0 ip filter 0 pass acl 0
```

DNS サーバのポート 53 への UDP パケットを透過させる

```
(config)# acl 1 ip 192.168.0.0/24 192.168.1.10/32 17 any
(config)# acl 1 udp any 53
(config)# lan 0 ip filter 1 pass acl 1
```

ICMP のパケットを透過させる

```
(config)# acl 2 ip any any 1 any
(config)# acl 2 icmp any any
(config)# lan 0 ip filter 2 pass acl 2
```

残りのパケットをすべて遮断する

```
(config)# acl 3 ip any any any any
(config)# lan 0 ip filter 3 reject acl 3
```

設定終了

```
(config)# save
```

14.4 外部から特定サーバへのアクセスだけを禁止する

ここでは、外部 LAN の FTP サーバに対するアクセスを禁止する場合の設定方法を説明します。

【設定条件】

Interface0/1ポートを使用する

VLAN IDとネットワークアドレスを以下のように対応付ける

VLAN ID：10　　ネットワークアドレス：192.168.10.0/24

【フィルタリング設定】

内部 LAN のホスト（192.168.1.0/24）から外部 LAN の FTP サーバ（192.168.0.5）へのアクセスを禁止

【フィルタリングルール】

・FTP サーバへのアクセスを禁止するには

（1）192.168.1.0/24 から 192.168.0.5 のポート 21（ftp）への TCP パケットを遮断する

【コマンド】

Interface0/1 ポートを設定する。

```
(config)#interface 0/1
(config-if)#vlan tag 10
```

192.168.10.0/24 のネットワークを設定する

```
(config)#lan 0 ip address 192.168.10.0/24 3
(config)#lan 0 vlan 10
```

内部の LAN から 192.168.0.5 への FTP のパケットを遮断する

```
(config)# acl 0 ip 192.168.1.0/24 192.168.0.5/32 6 any
(config)# acl 0 tcp any 21
(config)# lan 0 ip filter 0 reject acl 0
```

設定終了

```
(config)# save
```

14.5 外部から特定サーバへの ping だけを禁止する

ここでは、内部 LAN の特定のサーバに対する ping（ICMP ECHO）を禁止し、この特定のサーバに対するほかの ICMP パケット、その他のプロトコルのパケットおよびほかのホストに対するパケットはすべて許可する場合の設定方法を説明します。

【設定条件】

Interface0/1ポートを使用する

VLAN IDとネットワークアドレスを以下のように対応付ける

VLAN ID：10　　ネットワークアドレス：192.168.10.0/24

【フィルタリング設定】

内部 LAN のサーバ（192.168.1.5/32）に対して外部からの ping（ICMP ECHO）を禁止

その他はすべて通過

【フィルタリングルール】

・内部 LAN のサーバ（192.168.1.5/32）に対して外部からの ping（ICMP ECHO）を禁止するには

（1）192.168.1.5/32 への ICMP TYPE 8 の ICMP パケットを遮断する

・その他のパケットを許可する

（1）すべてのパケットを透過させる

【コマンド】

Interface0/1 ポートを設定する。

```
(config)#interface 0/1
(config-if)#vlan tag 10
```

192.168.10.0/24 のネットワークを設定する

```
(config)#lan 0 ip address 192.168.10.0/24 3
(config)#lan 0 vlan 10
```

アドレス 192.168.1.5/32 への ICMP TYPE 8 の ICMP パケットを遮断する

```
(config)# acl 0 ip any 192.168.1.5/32 1 any
(config)# acl 0 icmp 8 any
(config)# lan 0 ip filter 0 reject acl 0
```

残りのパケットをすべて透過させる

```
(config)# acl 1 ip any any any any
(config)# lan 0 ip filter 1 pass acl 1
```

設定終了

```
(config)# save
```

15　DSCP 値書き換え機能を使う。

本装置を経由してネットワークに送信される、またはネットワークから受信したパケットをIP アドレスとポート番号の組み合わせでDSCP値を変更することにより、ポリシーベースネットワークのポリシに合わせることができます。

本装置では、ACL 番号で指定したACL 定義の中で、以下の条件を指定することによってポリシーベースネットワークのポリシに合ったDSCP値に書き換えることができます。

- プロトコル
- 送信元情報（IP アドレス／アドレスマスク／ポート番号）
- あて先情報（IP アドレス／アドレスマスク／ポート番号）
- IPパケットのTOS 値またはDSCP値（全機種）

または、

IPv6 パケットのTraffic Class 値またはDSCP値。

ここではネットワークが以下のポリシを持つ場合の設定方法を説明します。

- FTP（DSCP値10）を最優先とする
- その他はなし

【設定条件】

- 送信元IPアドレス/アドレスマスク　192.168.1.0/24
- 送信元ポート番号　指定しない
- あて先IPアドレス/アドレスマスク　指定しない
- あて先ポート番号　20 (ftp-dataのポート番号)、21(ftpのポート番号)
- プロトコル　TCP
- DSCP値　0

新DSCP値　10

【コマンド】

FTP サーバのアクセスで DSCP 値を 0 から 10 に書き換える

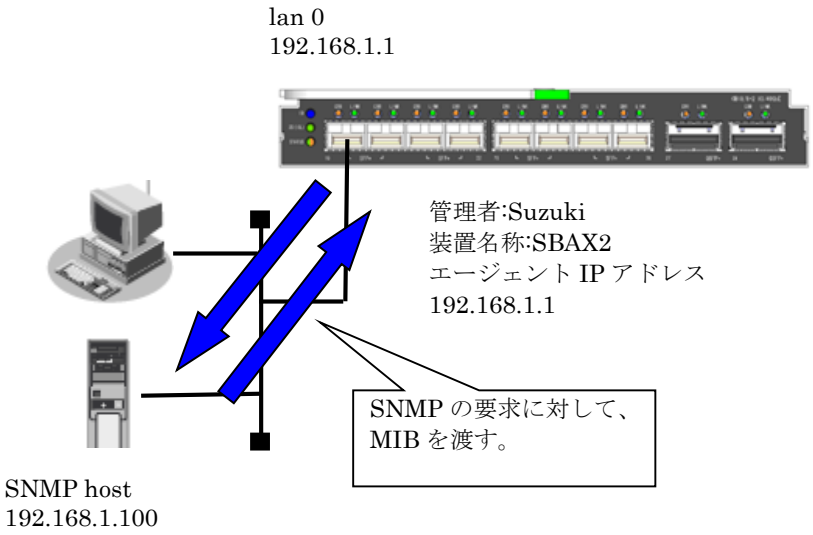
```
(config)#acl 0 ip 192.168.1.0/24 any 6 dscp 0
(config)#acl 0 tcp any 20,21
(config)#lan 0 ip dscp 0 acl 0 10
```

設定を保存する。

```
(config)#save
```

16　SNMP エージェント機能を使う

本装置は、SNMP（Simple Network Management Protocol）エージェント機能をサポートしています。
ここでは、SNMPホストに対してMIB情報を通知する場合の設定方法を説明します。



ヒント

◆ SNMPとは？

SNMP（Simple Network Management Protocol）は、ネットワーク管理用のプロトコルです。SNMPホストは、ネットワーク上の端末の稼動状態や障害状況を一元管理します。SNMPエージェントは、SNMPホストの要求に対してMIB（Management Information Base）という管理情報を返します。また、特定の情報についてはトラップという機能を用いて、SNMPエージェントからSNMPホストに対して非同期通知を行うことができます。

こんなことに気をつけて

エージェントアドレスには、本装置に設定されたどれかのインタフェースのIP アドレスを設定します。誤ったIP アドレスを設定した場合は、SNMPホストとの通信ができなくなります。

•認証プロトコルとパスワード、暗号プロトコルとパスワードは、SNMPホストの設定と同じ設定にします。誤ったプロトコルとパスワードを設定した場合は、SNMPホストとの通信ができなくなります。

•SNMPv3での認証／暗号プロトコルを使用する場合、snmp設定反映時の認証／暗号鍵生成に時間がかかります。

このとき、セッション監視タイムアウトが発生するなど、ほかの処理に影響する可能性があります。

•SNMPv3で使用されるsnmpEngineBoots 値は、装置再起動時に初期化（初期値：1）されます。そのため、MIB 情報

取得中に装置が再起動されると、SNMPホストによっては継続したMIB情報の取得ができないことがあります。

【設定条件】

SNMPエージェント機能を使用する

- 管理者：suzuki
- 機器名称：SBAX3
- 機器設置場所：1F（1 階）
- エージェントアドレス：192.168.1.1（自装置IP アドレス）
- SNMPホストアドレス：192.168.1.100
- コミュニティ名：public00

【コマンド】

SNMP エージェント情報を設定する。

```
(config)#snmp agent contact suzuki
(config)#snmp agent sysname SBAX3
(config)#snmp agent location 1F
(config)#snmp agent adress 192.168.1.1
```

SNMP ホスト情報を設定する。

```
(config)#snmp manager 0 192.168.1.100 public00 off disable
```

SNMP エージェント機能を使用する

```
(config)#snmp service on
```

設定を保存する。

```
(config)#save
```

SNMPv3でアクセス場合の情報を設定する

SNMPv3でアクセス場合は、以下の情報を設定します。

【設定条件】

SNMPエージェント機能を使用する

管理者：suzuki

機器名称：SBAX3

機器設置場所：1F（1 階）

エージェントアドレス：192.168.1.1（自装置IP アドレス）

SNMPホストアドレス：192.168.1.100

トラップ通知ホストアドレス：192.168.1.100

ユーザ名：user00

認証プロトコル：MD5

パスワード：auth_password

暗号プロトコル：DES

パスワード： priv_password

MIBビュー：MIB読み出しはsystem、interfaces グループのみ許可。

トラップ通知はlinkDown、linkUp トラップのみ許可。

【コマンド】

SNMP エージェント情報を設定する。

```
(config)#snmp agent contact suzuki
(config)#snmp agent sysname SBAX3
(config)#snmp agent location 1F
(config)#snmp agent adress 192.168.1.1
```

SNMPv3 情報を設定する。

```
(config)#snmp user 0 name user00
(config)#snmp user 0 address 0 192.168.1.100
(config)#snmp user 0 notification 0 192.168.1.100
```

認証・暗号プロトコルを設定する

```
(config)#snmp user 0 auth md5 auth_password
(config)#snmp user 0 priv des priv_password
```

MIB ビュー情報を設定する

```
(config)#snmp user 0 read view 0
(config)#snmp user 0 notify view 0
(config)#snmp view 0 subtree 0 include system
(config)#snmp view 0 subtree 1 include interfaces
(config)#snmp view 0 subtree 2 include linkdown
(config)#snmp view 0 subtree 3 include linkup
```

SNMP エージェント機能を使用する

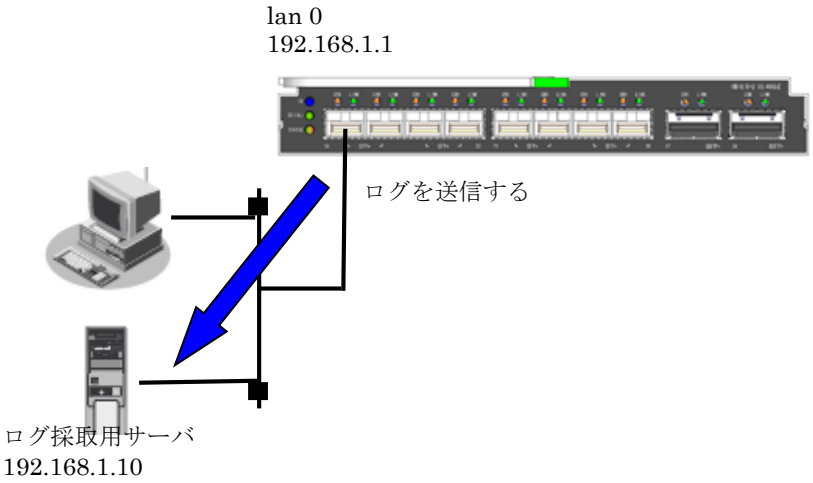
```
(config)#snmp service on
```

設定を保存する。

```
(config)#save
```

17　システムログを採取する

本装置では、各種システムログ（回線の接続／切断など）をネットワーク上のシステムログサーバに送信することができます。ここでは、システムログを採取する場合の設定方法を説明します。



【設定条件】

以下のプライオリティを設定する

-プライオリティ LOG_ERROR

-プライオリティ LOG_WARNING

-プライオリティ LOG_NOTICE

-プライオリティ LOG_INFO

•ログ受信用サーバのIP アドレス：192.168.1.10

【コマンド】

(config)#syslog server 192.168.1.10

システムログを設定する

(config)#syslog pri error,warm,notice,info

設定を保存する。

(config)#save

採取したシステムログを確認する

採取したシステムログの確認方法は、お使いのサーバによって異なります。

18　スケジュール機能を使う。

本装置のスケジュール機能は、以下のとおりです。

• 構成定義情報切り替え予約

本装置は、内部に2つ構成定義情報を持つことができます。運用構成の変更に備え、あらかじめ構成定義情
報を用意し、指定した日時に新しい構成定義に切り替えることができます。

構成定義の切り替え予約をする

本装置は、内部に構成定義情報を2 つ持つことができます。
ここでは、2006 年12 月1 日6 時30 分に構成定義情報を構成定義情報1 から構成定義情報2 に切り替える場合の設定方法を説明します。

【設定条件】

実行日時	2006 年 12 月 1 日　6 時 30 分
構成定義切り替え	構成定義情報 1 の構成定義情報→構成定義情報 2 の構成定義情報

【コマンド】

構成定義を切り替える
(config)#addact 0 0612010630 reset conifg 2

設定を保存する。
(config)#save

19　アプリケーションフィルタ機能を使う。

本装置上で動作する各サーバ機能に対してアクセス制限を行うことができます。
これにより、装置をメンテナンスまたは装置のサーバ機能を使用する端末を限定し、セキュリティを向上させることができます。

【設定条件】
管理用ホスト(192.168.1.100)からだけ TELNET/FTP/SSH サーバ機能へのアクセスを許可する。
内部 LAN ホスト(192.168.1.0/24)からだけ TIME サーバ機能へのアクセスを許可する。
その他のサーバ機能は制限しない。

こんなことに気をつけて
IP フィルタリングにより自装置へのパケットを遮断している場合、アプリケーションフィルタで許可する設定を行っていてもアクセスはできません。

【コマンド】
制限するサーバ機能に対し、デフォルトのアクセスを遮断する
(config)#serverinfo ftp filter default reject
(config)#serverinfo telnet filter default reject
(config)#serverinfo ssh filter default reject
(config)#serverinfo time filter default reject

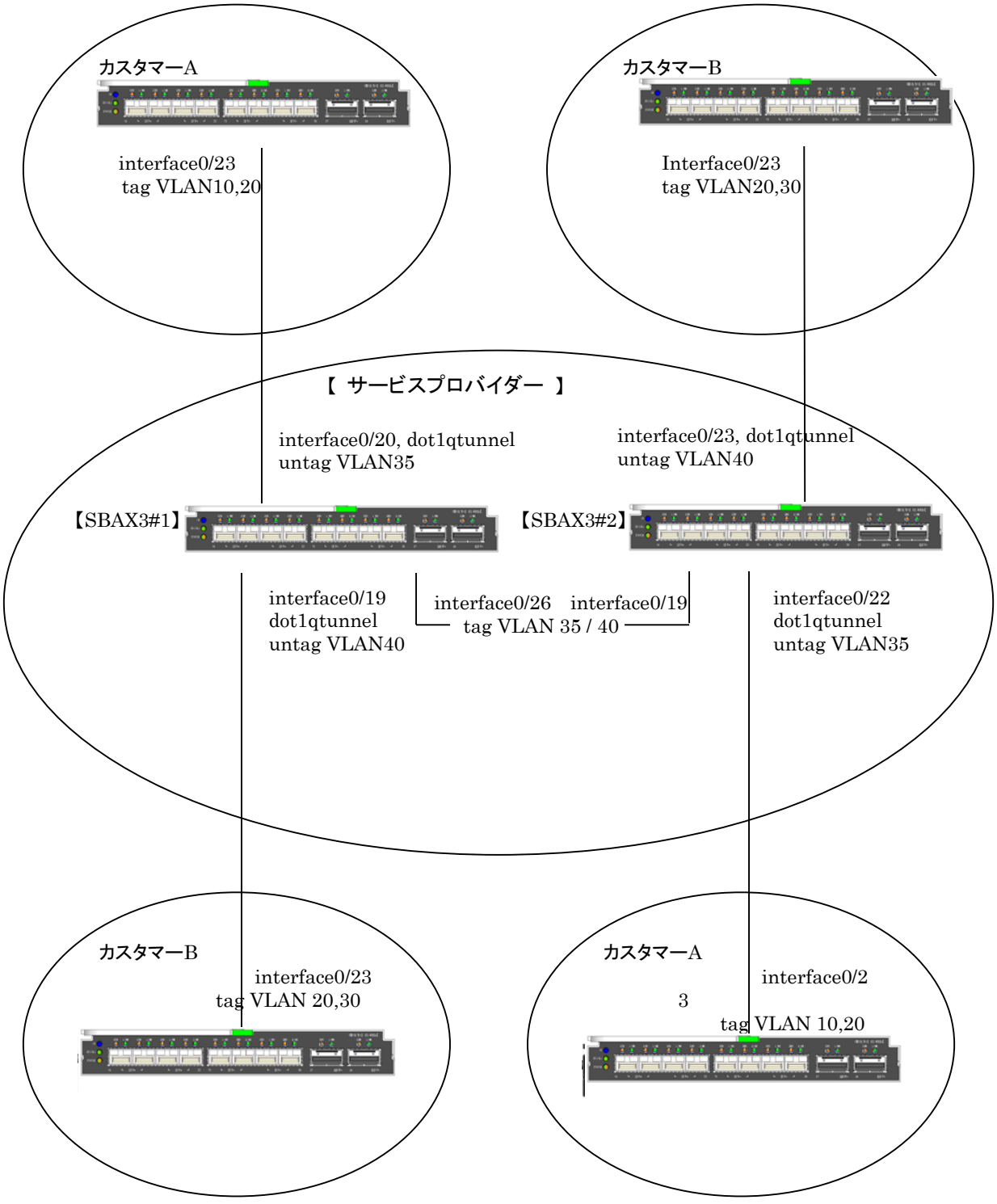
管理用のホストからの FTP/TELNET/SSH サーバ機能へのアクセスを許可する。
(config)#acl 0 ip 192.168.1.100/32 any any any
(config)#serverinfo ftp filter 0 accept acl 0
(config)#serverinfo telnet filter 0 accept acl 0
(config)#serverinfo ssh filter 0 accept acl 0

内部 LAN のホストからの TIME サーバ機能へのアクセスを許可する
(config)#acl 1 ip 192.168.1.0/24 any any any
(config)#serverinfo tme filter 0 accept acl 1

設定を保存する。
(config)#save

20　IEEE802.1Q トンネリング機能を使う。

ここでは、下図のカスタマーA、カスタマーB、SBAX3#1 および SBAX3#2 の設定方法を説明します。



【 設定条件 】

カスタマーA

Interface0/23 にタグ付きで VLAN10,20 を割り当てる。

カスタマーB

Interface0/23 にタグ付きで VLAN20,30 を割り当てる。

SBAX3#1

Interface0/19 にタグなしで VLAN40 を割り当てる。

Interface0/20 にタグなしで VLAN35 を割り当てる。

Interface0/26 にタグ付きで VLAN35 および 40 を割り当てる。

Interface0/19～0/20 に IEEE802.1Q トンネルポートを設定する。

IEEE802.1Q トンネルポートの使用を設定する。

SBAX3#2

Interface0/19 にタグ付きで VLAN35 および 40 を割り当てる。

Interface0/22 にタグなしで VLAN35 を割り当てる。

Interface0/23 にタグなしで VLAN40 を割り当てる。

Interface0/22～0/23 に IEEE802.1Q トンネルポートを設定する。

IEEE802.1Q トンネルポートの使用を設定する。

【 コマンド 】

カスタマーA

Interface0/23 にタグ付きで VLAN10,20 を割り当てる。

```
(config)#interface 0/23
(config-if)#vlan tag 10,20
```

カスタマーB

Interface0/23 にタグ付きで VLAN20,30 を割り当てる。

```
(config)#interface 0/23
(config-if)#vlan tag 20,30
```

SBAX3# 1

Interface0/19 にタグなしで VLAN40 を割り当てる。

```
(config)#interface 0/19
(config-if)#vlan untag 40
```

Interface0/20 にタグなしで VLAN35 を割り当てる。

```
(config)#interface 0/20
(config-if)#vlan untag 35
```

Interface0/26 にタグ付きで VLAN35 および 40 を割り当てる。

(config)#interface 0/26
(config-if)#vlan tag 35,40

Interface0/19～0/20 に IEEE802.1Q トンネルポートを設定する。
(config)#interface range 0/19-0/20
(config-if)#dot1qtunnel use on

IEEE802.1Q トンネルポートの使用を設定する。
(config)#dot1qtunnel use on

SBAX3#2
Interface0/19 にタグ付きで VLAN35 および 40 を割り当てる。
(config)#interface 0/19
(config-if)#vlan tag 35,40

Interface0/22 にタグなしで VLAN35 を割り当てる。
(config)#interface 0/22
(config-if)#vlan untag 35

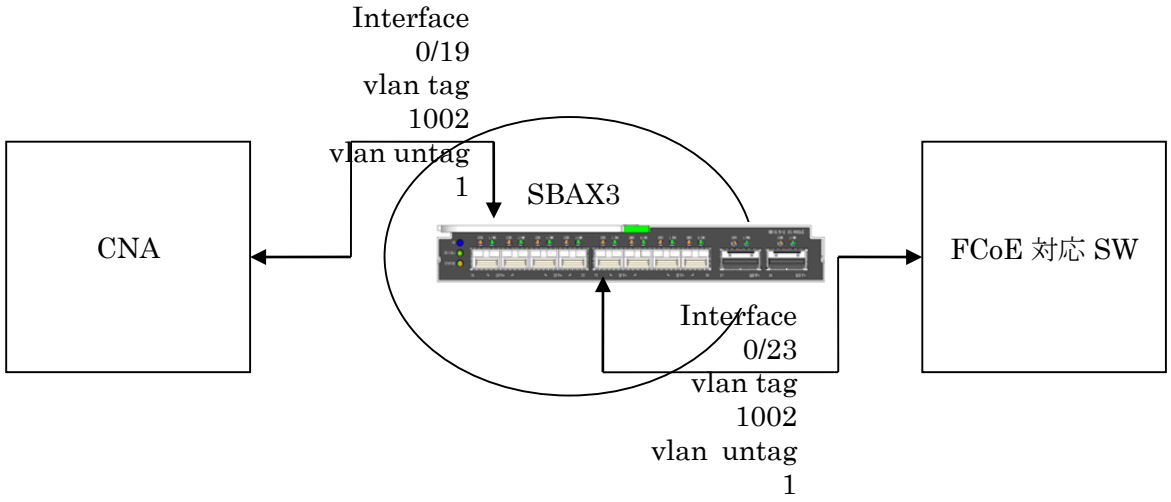
Interface0/23 にタグなしで VLAN40 を割り当てる。
(config)#interface 0/23
(config-if)#vlan untag 40

Interface0/22～0/23 に IEEE802.1Q トンネルポートを設定する。
(config)#interface range 0/22-0/23
(config-if)#dot1qtunnel use on

IEEE802.1Q トンネルポートの使用を設定する。
(config)#dot1qtunnel use on

21 CEE 機能を使う。

ここでは、下図の各機の設定方法を説明します。



【 設定条件 】

CNA

SBAX3 と接続しているポートが、SBAX3 の DCBX 設定を受け入れられるような設定をする (willing bit を立てる)。

SBAX3 / FCoE 対応 SW

CEE ポートにタグ付きで VLAN1002 を割り当てる。

CEE ポートに FIP フレーム転送用にタグ無しで VLAN1 を割り当てる。

CEE ポートの CEE プライオリティグループ 1 を帯域幅 40 で設定する。

CEE ポートの CEE プライオリティグループ 2 を帯域幅 60 で設定する。

CEE ポートの CEE プライオリティグループ 2 の PFC を有効にする。

CEE ポートの CEE プライオリティマップをプライオリティ 3 のみプライオリティグループ 2 に、他プライオリティはプライオリティグループ 1 に割り当てる設定する。

CEE ポートの FCoE のプライオリティを、プライオリティ 3 のみ指定する。

CEE 機能を有効にする。

【 コマンド 】

SBAX3

装置のプライオリティグループ 1、2 を有効にする。

```
(config)# cee priority group 1 use on
(config)# cee priority group 2 use on
```

プライオリティ 3 のみプライオリティグループ 2 に、他プライオリティはプライオリティグループ 1 に割り当てる設定する。
(config)# cee priority map 1 1 1 2 1 1 1 1

Interface 0/19, 0/23 にタグ付きで VLAN1002 を割り当てる。
(config)# interface range 0/19,0/23
(config-if)# vlan tag 1002

Interface 0/19、0/23 に FIP フレーム転送用にタグ無しで VLAN1 を割り当てる。
(config-if)# vlan untag 1

Interface 0/19, 0/23 で LLDP 情報の送受信を行うよう設定する。
(config-if)# lldp mode enable

Interface 0/19, 0/23 の CEE プライオリティグループ 1 の weight 値を 40 に設定する。
(config-if)# cee priority group 1 weight 40

Interface 0/19, 0/23 の CEE プライオリティグループ 2 の weight 値を 60 に設定する。
(config-if)# cee priority group 2 weight 60

Interface 0/19, 0/23 の CEE プライオリティグループ 2 の PFC を有効にする。
(config-if)# cee priority group 2 pfc on

Interface 0/19, 0/23 の CEE ポートの FCoE のプライオリティを、プライオリティ 3 のみ指定する。
(config-if)# dcbx fcoe-priority3

Interface 0/19, 0/23 の CEE 機能を有効にする。
(config-if)# cee use on

装置の CEE 機能を有効にする。
(config-if)# end
(config)# cee mode on