P3NK-5132-02Z0

Fujitsu Network SR-X
コマンド設定事例集

V02

FUJITSU

はじめに

このたびは、本装置をお買い上げいただき、まことにありがとうございます。
サーバとの共存性を高めた、省スペース・省電力の本製品はサーバ間接続に最適です。

2014年 10月 初 版
2023年 5月 第2版

目次

本書の使いかた

本書では、ネットワークを構築するために、代表的な接続形態や本装置の機能を活用した接続形態について説明しています。

本書の読者と前提知識

本書は、ネットワーク管理を行っている方を対象に記述しています。

本書を利用するにあたって、ネットワークおよびインターネットに関する基本的な知識が必要です。

ネットワーク設定を初めて行う方でも「機能説明書」に分かりやすく記載していますので、安心してお読みいただけます。

マークについて

本書で使用しているマーク類は、以下のような内容を表しています。

	本装置をお使いになる際に、役に立つ知識をコラム形式で説明しています。
こんな事に気をつけて	本装置をご使用になる際に、注意していただきたいことを説明しています。
	操作手順で説明しているもののほかに、補足情報を説明しています。
	操作方法など関連事項を説明している箇所を示します。
	本装置の機能を使用する際に、対象となる機種名を示します。
	製造物責任法（PL）関連の警告事項を表しています。本装置をお使いの際は必ず守ってください。
	製造物責任法（PL）関連の注意事項を表しています。本装置をお使いの際は必ず守ってください。

設定例の記述について

コマンド例では configure コマンドを実行して、構成定義モードに入ったあとのコマンドを記述しています。
また、プロンプトは設定や機種によって変化するため、“#” に統一しています。

本書における商標の表記について

Microsoft、MS-DOS、Windows、Windows NTおよびWindows Vistaは、米国Microsoft Corporationの米国およびその他の国における登録商標です。

AdobeおよびReaderは、Adobe Systems Incorporated（アドビシステムズ社）の米国ならびに他の国における商標または登録商標です。

Netscapeは、米国Netscape Communications Corporationの商標です。

UNIXは、米国およびその他の国におけるオープン・グループの登録商標です。

本書に記載されているその他の会社名および製品名は、各社の商標または登録商標です。

製品名の略称について

本書で使用している製品名は、以下のように略して表記します。

なお、本文中では®を省略しています。

製品名称	本文中の表記
Microsoft® Windows® XP Professional operating system	Windows XP
Microsoft® Windows® XP Home Edition operating system	
Microsoft® Windows® 2000 Server Network operating system	Windows 2000
Microsoft® Windows® 2000 Professional operating system	
Microsoft® Windows NT® Server network operating system Version 4.0	Windows NT 4.0
Microsoft® Windows NT® Workstation operating system Version 4.0	
Microsoft® Windows Server® 2003, Standard Edition	Windows Server 2003
Microsoft® Windows Server® 2003 R2, Standard Edition	
Microsoft® Windows Server® 2003, Enterprise Edition	
Microsoft® Windows Server® 2003 R2, Enterprise Edition	
Microsoft® Windows Server® 2003, Datacenter Edition	
Microsoft® Windows Server® 2003 R2, Datacenter Edition	
Microsoft® Windows Server® 2003, Web Edition	
Microsoft® Windows Server® 2003, Standard x64 Edition	
Microsoft® Windows Server® 2003 R2, Standard Edition	
Microsoft® Windows Server® 2003, Enterprise x64 Edition	
Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition	
Microsoft® Windows Server® 2003, Enterprise Edition for Itanium-based systems	
Microsoft® Windows Server® 2003, Datacenter x64 Edition	
Microsoft® Windows Server® 2003 R2, Datacenter x64 Edition	
Microsoft® Windows Vista® Ultimate operating system	Windows Vista
Microsoft® Windows Vista® Business operating system	
Microsoft® Windows Vista® Home Premium operating system	
Microsoft® Windows Vista® Home Basic operating system	
Microsoft® Windows Vista® Enterprise operating system	
Microsoft® Windows® 7 64bit Home Premium	Windows 7
Microsoft® Windows® 7 32bit Professional	

本装置のマニュアルの構成

本装置の取扱説明書は、以下のとおり構成されています。使用する目的に応じて、お使いください。

マニュアル名称	内容
ご利用にあたって	本装置の設置方法やソフトウェアのインストール方法を説明しています。
機能説明書	本装置の便利な機能について説明しています。
トラブルシューティング	トラブルが起きたときの原因と対処方法を説明しています。
メッセージ集	システムログ情報などのメッセージの詳細な情報を説明しています。
仕様一覧	本装置のハード／ソフトウェア仕様とMIB/Trap一覧を説明しています。
コマンドユーザーズガイド	コマンドを使用して、時刻などの基本的な設定またはメンテナンスについて説明しています。
コマンド設定事例集（本書）	コマンドを使用した、基本的な接続形態または機能の活用方法を説明しています。
コマンドリファレンス	コマンドの項目やパラメタの詳細な情報を説明しています。
Webユーザーズガイド	Web画面を使用して、時刻などの基本的な設定またはメンテナンスについて説明しています。また、Web画面の項目の詳細な情報を説明しています。

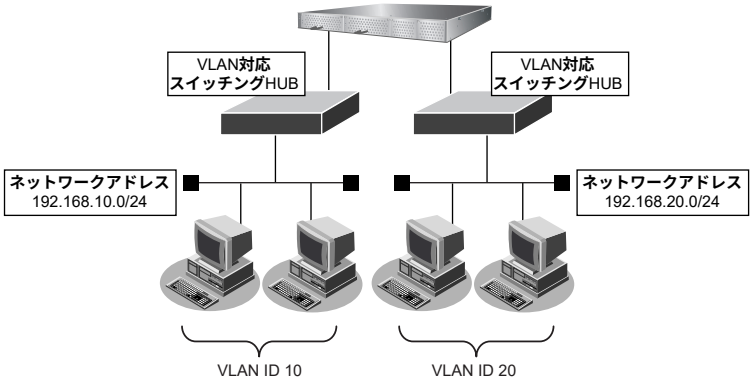
1　VLAN機能を使う

適用機種　全機種

1.1　ポートVLAN機能を使う

適用機種　全機種

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

- ETHER1、5ポートを使用する
- VLAN対応スイッチングHUBで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
  VLAN ID：20　　ネットワークアドレス：192.168.20.0/24

上記の設定条件に従って設定を行う場合のコマンド例を示します。

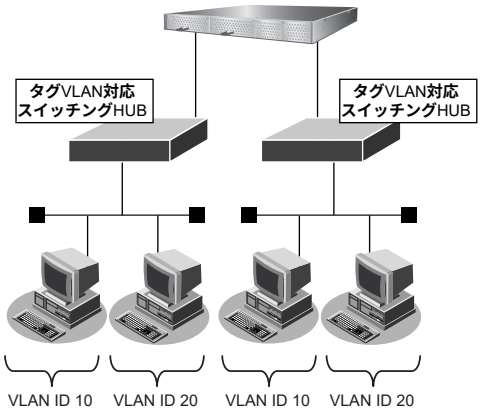
● コマンド

```
ETHER1 ポートを設定する
# ether 1 vlan untag 10

ETHER5 ポートを設定する
# ether 5 vlan untag 20

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

192.168.20.1/24 のネットワークを設定する
# lan 1 ip address 192.168.20.1/24 3
# lan 1 vlan 20

設定終了
# save
# commit
```

1.2 タグ VLAN 機能を使う

適用機種 全機種

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

- ETHER1、5ポートを使用する
- VLAN対応スイッチングHUBで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
  VLAN ID：20　　ネットワークアドレス：192.168.20.0/24

上記の設定条件に従って設定を行う場合のコマンド例を示します。

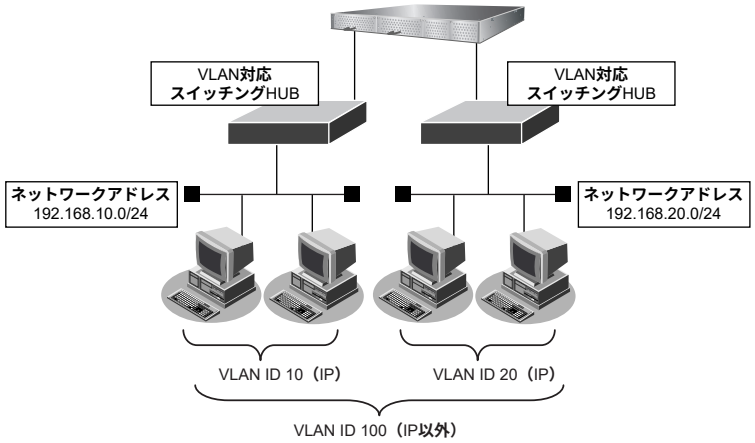
● コマンド

```
ETHER1 ポートを設定する
# ether 1 vlan tag 10,20

ETHER5 ポートを設定する
# ether 5 vlan tag 10,20

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

192.168.20.1/24 のネットワークを設定する
# lan 1 ip address 192.168.20.1/24 3
# lan 1 vlan 20

設定終了
# save
# commit
```

1.3 プロトコルVLAN機能を使う

適用機種 全機種

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

- ETHER1、5ポートを使用する
- VLAN対応スイッチングHUBで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
  VLAN ID：20　　ネットワークアドレス：192.168.20.0/24
  VLAN ID：100

上記の設定条件に従って設定を行う場合のコマンド例を示します。

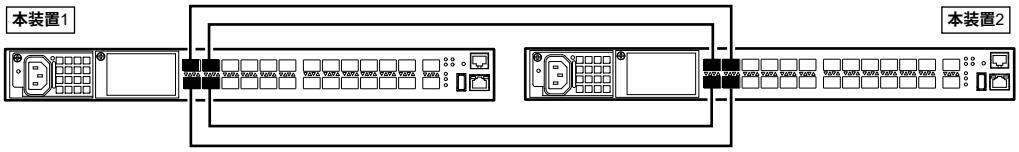
● コマンド

```
ETHER1 ポートを設定する
# ether 1 vlan untag 10,100

ETHER5 ポートを設定する
# ether 5 vlan untag 20,100

VLAN10、20 を IPv4 プロトコル VLAN に設定する
# vlan 10 protocol ipv4
# vlan 20 protocol ipv4

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

192.168.20.1/24 のネットワークを設定する
# lan 1 ip address 192.168.20.1/24 3
# lan 1 vlan 20

設定終了
# save
# commit
```

2　リンクアグリゲーション機能を使う

適用機種　全機種

ここではSR-X526R1の場合を例にして、4ポートの10G回線を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

- ETHER1～4ポートをリンクアグリゲーションする
- リンクアグリゲーションした4ポートにVLAN10のタグ付きフレームとVLAN20のタグ付きフレームが流れるように設定する
- 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
  VLAN ID：20　　ネットワークアドレス：192.168.20.0/24

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

[本装置1]

```
ETHER1～4ポートを設定する
# ether 1-4 vlan tag 10,20

ETHER1～4ポートをリンクアグリゲーションとして設定する
# ether 1-4 type linkaggregation 1

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

192.168.20.1/24のネットワークを設定する
# lan 1 ip address 192.168.20.1/24 3
# lan 1 vlan 20

設定終了
# save
# commit
```

[本装置2]

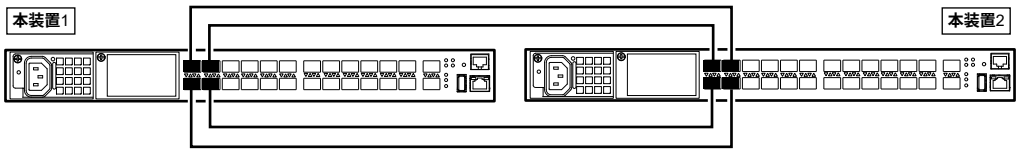
```
ETHER1～4ポートを設定する
# ether 1-4 vlan tag 10,20

ETHER1～4ポートをリンクアグリゲーションとして設定する
# ether 1-4 type linkaggregation 1

192.168.10.2/24のネットワークを設定する
# lan 0 ip address 192.168.10.2/24 3
# lan 0 vlan 10

192.168.20.2/24のネットワークを設定する
# lan 1 ip address 192.168.20.2/24 3
# lan 1 vlan 20

設定終了
# save
# commit
```

☛参照 マニュアル「機能説明書」

2.1 LACP機能を使う

適用機種 全機種

ここではSR-X526R1の場合を例にして、4ポートの10G回線を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

- ETHER1～4ポートをリンクアグリゲーションする
- リンクアグリゲーションした4ポートでLACPを実行する
- リンクアグリゲーションした4ポートにVLAN10のタグ付きフレームとVLAN20のタグ付きフレームが流れるように設定する
- 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
  VLAN ID：20　　ネットワークアドレス：192.168.20.0/24

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

[本装置1]

```
ETHER1～4ポートを設定する
# ether 1-4 vlan tag 10,20

ETHER1～4ポートをリンクアグリゲーションとして設定する
# ether 1-4 type linkaggregation 1

LACPを利用したリンクアグリゲーションとして設定する
# linkaggregation 1 mode active

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

192.168.20.1/24 のネットワークを設定する
# lan 1 ip address 192.168.20.1/24 3
# lan 1 vlan 20

設定終了
# save
# commit
```

[本装置2]

```
ETHER1～4ポートを設定する
# ether 1-4 vlan tag 10,20

ETHER1～4ポートをリンクアグリゲーションとして設定する
# ether 1-4 type linkaggregation 1

LACPを利用したリンクアグリゲーションとして設定する
# linkaggregation 1 mode active

192.168.10.2/24 のネットワークを設定する
# lan 0 ip address 192.168.10.2/24 3
# lan 0 vlan 10

192.168.20.2/24 のネットワークを設定する
# lan 1 ip address 192.168.20.2/24 3
# lan 1 vlan 20

設定終了
# save
# commit
```

☛参照 マニュアル「機能説明書」

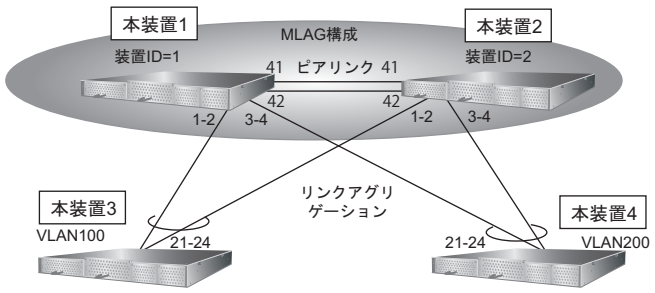
3　MLAG機能を使う

適用機種　***SR-X340TR1***

ここでは、MLAG機能を使用する場合の設定方法を説明します。

参照　マニュアル「機能説明書」

SR-X340TR1の場合を例にします。



● 設定条件

2台のSR-X340TR1でMLAGを構成し、配下のSR-X324T2と接続する。

- ドメインIDを1とする（初期値）
- 本装置1の装置IDを1、本装置2の装置IDを2とする
- ETHER41、42ポートをピアリンクポートとして使用する
- 本装置3はVLAN100、本装置4はVLAN200を収容する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

[本装置1]

```
MLAG機能を使用する
# mlag mode enable
# mlag id 1
# mlag peerlink 41,42

リンクアグリゲーション（グループ1）を設定する
# ether 1-2 type linkaggregation 1
# ether 1-2 vlan tag 100

リンクアグリゲーション（グループ2）を設定する
# ether 3-4 type linkaggregation 2
# ether 3-4 vlan tag 200

STP機能を無効にする
# stp mode disable

IPアドレスを設定する
# lan 0 ip address 192.168.100.1/24 3
# lan 0 vlan 100
# lan 1 ip address 192.168.200.1/24 3
# lan 1 vlan 200
```

```
設定終了
# save
# reset
```

[本装置2]

```
MLAG機能を使用する
# mlag mode enable
# mlag id 2
# mlag peerlink 41,42

リンクアグリゲーション（グループ1）を設定する
# ether 1-2 type linkaggregation 1
# ether 1-2 vlan tag 100

リンクアグリゲーション（グループ2）を設定する
# ether 3-4 type linkaggregation 2
# ether 3-4 vlan tag 200

STP機能を無効にする
# stp mode disable

IPアドレスを設定する
# lan 0 ip address 192.168.100.2/24 3
# lan 0 vlan 100
# lan 1 ip address 192.168.200.2/24 3
# lan 1 vlan 200

設定終了
# save
# reset
```

[本装置3]

```
リンクアグリゲーション（グループ1）を設定する
# ether 21-24 type linkaggregation 1 21
# ether 21-24 vlan tag 100

STP機能を無効にする
# stp mode disable

IPアドレスを設定する
# lan 0 ip address 192.168.100.10/24 3
# lan 0 vlan 100

設定終了
# save
# reset
```

[本装置4]

```
リンクアグリゲーション（グループ2）を設定する
# ether 21-24 type linkaggregation 2 21
# ether 21-24 vlan tag 200

STP機能を無効にする
# stp mode disable

IPアドレスを設定する
# lan 0 ip address 192.168.200.10/24 3
# lan 0 vlan 200

設定終了
# save
# reset
```

4　バックアップポート機能を使う

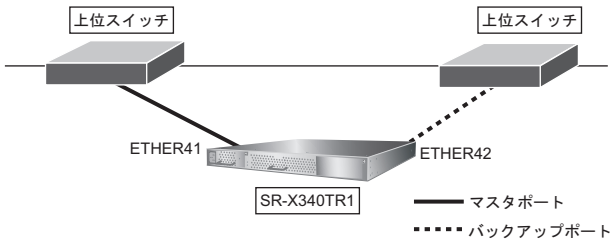
ここでは、アップリンクポートをバックアップポートとして利用する場合の設定方法について説明します。
アップリンクポートをそれぞれ異なるスイッチに接続することで、冗長アップリンクの形態にできます。

こんな事に気をつけて

切替通知フレームを受信する上位スイッチが正しくMACアドレスを再学習するために最適な切替通知フレームの送信条件は、上位スイッチの仕様に依存します。本機能を利用する際は、必ず実機確認を行い最適な送信条件を事前に確認してください。

4.1　マスタポートを優先的に使用する

ここでは、マスタポートを優先的に使用する場合の設定方法を説明します。
SR-X340TR1の場合を例にします。



● 設定条件

- ETHER41、42ポートをバックアップポートとして使用する
  （ETHER41をマスタポート、ETHER42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
- 稼動ポート切替発生時に、切替通知フレームをFDB-tableモードで送信する
  （100ミリ秒間隔で20フレームずつ、初回送信は500ミリ秒遅延させる）

上記の設定条件に従って設定を行う場合のコマンド例を示します。

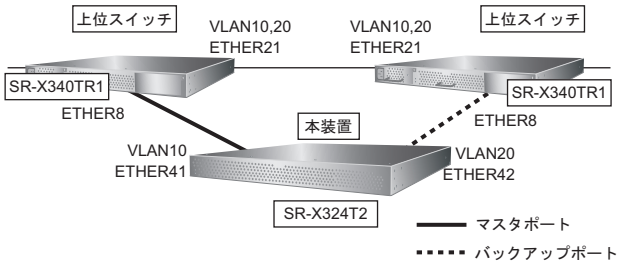
● コマンド

```
ETHER41ポート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
# ether 41 type backup 1 master

ETHER42ポート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
# ether 42 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
# backup 1 mode master

バックアップポートの切替通知動作を設定する
# backup 1 notify mode fdb-table
# backup 1 notify interval 100 20 500

設定終了
# save
# commit
```

4.2 VLANごとに両方のポートを同時に使用する

ここでは、バックアップポートをVLANごとに両方のポートを同時に稼動させる場合の設定方法を説明します。本設定では、マスタポートとバックアップポートがVLANごとに同時に稼動するため通信帯域を有効に利用できます。どちらかのポートがリンクダウンした場合は、残された稼動ポートがもう一方のポートのVLANも動的にバックアップします。

上位スイッチをSR-X340TR1 とし、SR-X324T2 をバックアップポートで接続する例とします。



こんな事に気をつけて

- Vlan-basedモード設定ではSTP機能と同時に使用できません。
- 上位スイッチの本装置接続ポートには、マスタポートとバックアップポート両方のタグVLANを設定する必要があります。

● 設定条件

2台のSR-X340TR1を上位スイッチとしてSR-X324T2を接続する。

[本装置]

- ETHER41、42ポートをバックアップポートとして使用する
  （ETHER41をマスタポート、ETHER42をバックアップポートとする）
- VLANごとに両方のポートを使用する
  （マスタポートでVLAN10、バックアップポートでVLAN20を優先使用する）
- 切替通知フレームをMAC-flushモードで送信する
  切替通知送信条件　：100ミリ秒間隔で10フレームずつ、初回送信は500ミリ秒遅延させる
  切替通知フレームの送信元MACアドレス
  　：00:aa:aa:aa:aa:aa

[上位スイッチ]

- MACテーブルフラッシュ機能を使用する
  監視MACアドレス　：00:aa:aa:aa:aa:aa
  学習テーブルの初期化　：VLANごとに初期化する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

[本装置]

```
ETHER41ポートをバックアップポート（グループ3）のマスタポート（VLAN10を優先動作）に設定する
# ether 41 type backup 3 master
# ether 41 vlan tag 10

ETHER42ポートをバックアップポート（グループ3）のバックアップポート（VLAN20を優先動作）に設定する
# ether 42 type backup 3 backup
# ether 42 vlan tag 20

バックアップグループ3をVLANごとに両方のポートを使用するモードに設定する
```

```
# backup 3 mode vlan-based

バックアップポートの切替通知動作を設定する
# backup 3 notify mode mac-flush
# backup 3 notify interval 100 10 500
# backup 3 notify mac 00:aa:aa:aa:aa:aa

STP機能を無効にする
# stp mode disable

設定終了
# save
# commit
```

[上位スイッチ]

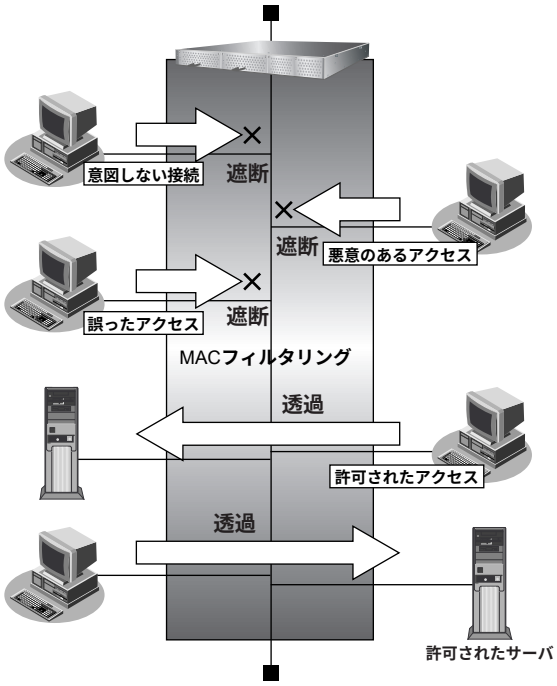
```
ETHER8ポートをSR-X324T2との接続ポートとしてVLAN設定する
# ether 8 vlan tag 10,20
# ether 8 stp use off

STP機能を無効にする
# stp mode disable

MACテーブルフラッシュ機能を設定する
# mac flush 0 address 00:aa:aa:aa:aa:aa
# mac flush 0 mode vlan

設定終了
# save
# commit
```

5　MACフィルタリング機能を使う

適用機種　全機種

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。

参照　マニュアル「機能説明書」



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。

- 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
- フィルタ処理の対象となるパケット入力ETHERポート
- 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

5.1 特定 MAC アドレスからのパケットだけを許可する

適用機種 全機種

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 ETHER1 ～ 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 ETHER1 ～ 4 ポートおよび ETHER9 ～ 12 ポートで構成されるポート VLAN で、ETHER1 ～ 4 ポートでタグ付き、ETHER9 ～ 12 ポートでタグなしである
- ETHER2 ポートの VLAN 10 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だけを許可し、その他はすべて禁止する

上記のフィルタリング設計に従って設定を行う場合のコマンド例を示します。

● 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）
# acl 100 mac 00:0b:01:02:03:04 any any
# 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）
# acl 110 vlan 10 any

ETHER2 ポートで（1）で設定した形式のパケットを透過させる
# ether 2 macfilter 0 pass 100

ETHER2 ポートで（2）で設定した形式のパケットを遮断する
# ether 2 macfilter 1 reject 110
```

5.2 特定MACアドレスへのパケットだけを許可する

適用機種 全機種

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ETHER1～8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ETHER1～4ポートおよびETHER9～12ポートで構成されるポートVLANで、ETHER1～4ポートでタグ付き、ETHER9～12ポートでタグなしである
- ETHER4～8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

上記のフィルタリング設計に従って設定を行う場合のコマンド例を示します。

● 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)
# acl 120 mac any 00:0b:01:02:03:04 any
# 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)
# acl 110 vlan 10 any

ETHER4～8ポートで（1）で設定した形式のパケットを透過させる
# ether 4-8 macfilter 0 pass 120

ETHER4～8ポートで（2）で設定した形式のパケットを遮断する
# ether 4-8 macfilter 1 reject 110
```

5.3 特定パケット形式のパケットだけを禁止する

適用機種 全機種

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ETHER1～8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ETHER1～4ポートおよびETHER9～12ポートで構成されるポートVLANで、ETHER1～4ポートでタグ付き、ETHER9～12ポートでタグなしである
- ETHER1～4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

上記のフィルタリング設計に従って設定を行う場合のコマンド例を示します。

● 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)
# acl 130 mac any any ether 0800
# acl 131 mac any any ether 0806
# acl 132 mac any any ether 8035

ETHER1～4ポートで（1）で作成したパケットのパターンを遮断する
# ether 1-4 macfilter 0 reject 130
# ether 1-4 macfilter 1 reject 131
# ether 1-4 macfilter 2 reject 132
```

5.4 VLAN単位で特定MACアドレス間の通信だけを遮断する

適用機種 全機種

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

- VLAN10はETHER1～4ポートでタグなし、ETHER5～8ポートでタグ付きで構成されるポートVLANである
- VLAN20はETHER1～4ポートでタグ付き、ETHER5～8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、VLAN 20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

上記のフィルタリング設計に従って設定を行う場合のコマンド例を示します。

● 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）
# acl 0 mac 00:0b:01:02:03:04 00:0b:11:12:13:14 any
# 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）
# acl 1 mac 00:0b:11:12:13:14 00:0b:01:02:03:04 any
# 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）
# acl 2 mac 00:0b:21:22:23:24 00:0b:31:32:33:34 any
# 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）
# acl 3 mac 00:0b:31:32:33:34 00:0b:21:22:23:24 any
# 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
# vlan 10 macfilter 0 reject 0
# 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
# vlan 20 macfilter 0 reject 2
# vlan 20 macfilter 1 reject 3
```

5.5 VLAN単位で特定パケット形式のパケットだけを許可する

適用機種 全機種

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

- VLAN10はETHER1～4ポートでタグなし、ETHER5～8ポートでタグ付きで構成されるポートVLANである
- VLAN20はETHER1～4ポートでタグ付き、ETHER5～8ポートでタグなしで構成されるポートVLANである
- VLAN10ではIPプロトコルの入力パケットだけを許可する
- VLAN 20ではFNAプロトコルの入力パケットだけを許可する

上記のフィルタリング設計に従って設定を行う場合のコマンド例を示します。

● コマンド

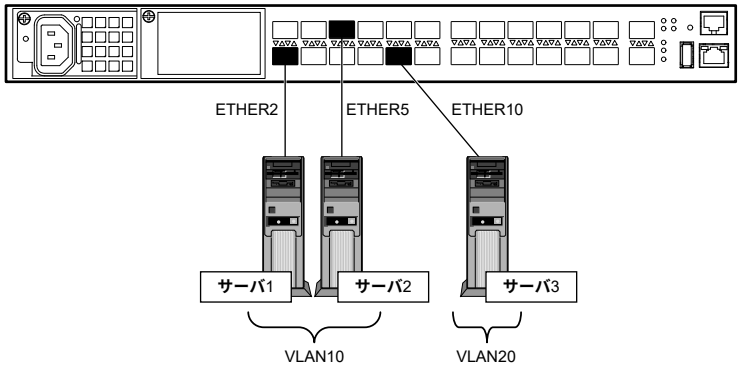
```
IP プロトコルのパケット（IP, ARP, Reverse ARP）の形式をACLで設定する　----（1）
# acl 10 mac any any ether 0800
# acl 11 mac any any ether 0806
# acl 12 mac any any ether 8035

FNAプロトコルのパケットの形式をACLで設定する　----（2）
# acl 20 mac any any llc 8080
# acl 21 mac any any llc 0000
# acl 22 mac any any llc 0001

全プロトコルのパケットの形式をACLで設定する　----（3）
# 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　----（4）
# vlan 10 macfilter 0 pass 10
# vlan 10 macfilter 1 pass 11
# vlan 10 macfilter 2 pass 12
# vlan 10 macfilter 3 reject 30

VLAN20で（2）で作成したパケットのパターン以外を遮断する　----（5）
# vlan 20 macfilter 0 pass 20
# vlan 20 macfilter 1 pass 21
# vlan 20 macfilter 2 pass 22
# vlan 20 macfilter 3 reject 30
```

6　スタティックMACフォワーディング機能を使う

適用機種　全機種

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

- ETHER2、5ポートにサーバ1、2を接続し、VLANを10とする
- ETHER10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

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
ETHER2、5ポートにVLAN10を設定する
# ether 2,5 vlan untag 10

ETHER10ポートにVLAN20を設定する
# ether 10 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
# vlan 10 forward 0 00:00:00:00:00:11 2
# 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
# vlan 20 forward 0 00:00:00:00:00:33 10

設定終了
# save
# commit
```

7　QoS機能を使う

適用機種　全機種

参照　マニュアル「機能説明書」

7.1　優先制御機能を使う

適用機種　全機種

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。

こんな事に気をつけて

- 本装置の初期設定は、マニュアル「機能説明書」の「優先制御機能」に関する記述を参照してください。
- SR-X316T2/324T2の場合のキューは4個、SR-X340TR1/526R1の場合のキューは8個となります。

SR-X316T2/324T2の場合

● 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	
	2	1
その他	1	
	0	0

上記の優先制御設定に従って設定を行う場合のコマンド例を示します。

● コマンド

```
優先制御を設定する
#qos cosmap 0 0
#qos cosmap 1 1
#qos cosmap 2 1
#qos cosmap 3 2
#qos cosmap 4 2
#qos cosmap 5 3
#qos cosmap 6 3
#qos cosmap 7 3
```

SR-X340TR1 の場合

● 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	4
	6	
音声	5	3
FAX／呼制御	4	2
映像	3	1
	2	
その他	1	0
	0	

上記の優先制御設定に従って設定を行う場合のコマンド例を示します。

● コマンド

```
優先制御を設定する
#qos cosmap 0 0
#qos cosmap 1 0
#qos cosmap 2 1
#qos cosmap 3 1
#qos cosmap 4 2
#qos cosmap 5 3
#qos cosmap 6 4
#qos cosmap 7 4
```

SR-X526R1 の場合

● 優先制御設計

パケットのタイプ	CoS 値	ETHER ポートの出力キュークラス		
		ETHER1～ETHER10	ETHER11～ETHER20	ETHER21～ETHER26
管理パケット	7	7（初期設定）	7（初期設定）	7（初期設定）
	6	3	3	6（初期設定）
音声	5	6	4	5（初期設定）
FAX／呼制御	4	5	5	4（初期設定）
映像	3	4	6	3（初期設定）
	2	1（初期設定）	1（初期設定）	1（初期設定）
	1	0（初期設定）	0（初期設定）	0（初期設定）
	0	2（初期設定）	2（初期設定）	2（初期設定）

上記の優先制御設定に従って設定を行う場合のコマンド例を示します。

● コマンド

```
優先制御を設定する
# ether 1-10 qos prioritymap 3 4
# ether 1-10 qos prioritymap 4 5
# ether 1-10 qos prioritymap 5 6
# ether 1-10 qos prioritymap 6 3
# ether 11-20 qos prioritymap 3 6
# ether 11-20 qos prioritymap 4 5
# ether 11-20 qos prioritymap 5 4
# ether 11-20 qos prioritymap 6 3
```

7.2 優先制御情報書き換え機能を使う

適用機種 ***SR-X340TR1, 526R1***

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。

- 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
- 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
- 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

- VLAN 10はETHER1～8ポートで構成されるポートVLANで、すべてタグ付きである
- ETHER1ポートでは全入力パケットのDSCP値を40に書き換える

上記の書き換え要求に従って設定を行う場合のコマンド例を示します。

● コマンド

```
すべてのパケットの形式をACLで設定する ----  (1)
# acl 120 mac any any any

ETHER1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
# ether 1 qos aclmap 0 dscp 40 120

設定終了
# save
# commit
```

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

- VLAN 10 は ETHER1 ～ 8 ポートで構成されるポート VLAN で、すべてタグ付きである
- VLAN 10 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

上記の書き換え要求に従って設定を行う場合のコマンド例を示します。

● 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)
# acl 150 vlan 10 5

VLAN10 に属する ETHER1 ～ 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
# ether 1-8 qos aclmap 0 tos 6 150

設定終了
# save
# commit
```

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 ETHER1 ～ 5 ポートで構成されるポート VLAN で、ETHER1 ～ 4 ポートでタグ付き、ETHER5 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

上記の書き換え要求に従って設定を行う場合のコマンド例を示します。

● 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)
# 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
# vlan 20 qos aclmap 0 queue 3 100

設定終了
# save
# commit
```

8 STP機能を使う

適用機種 全機種

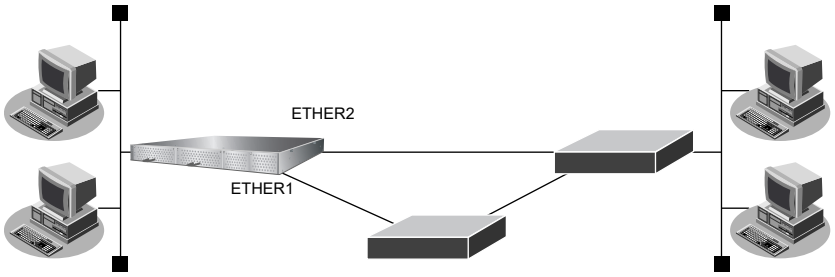
ここでは、STP機能を使用する場合の設定方法を説明します。

8.1 STPを使う

適用機種 全機種

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。

参照 マニュアル「機能説明書」



● 設定条件

- STPを使用する
- ETHER1、2ポートをVID 10のポートVLANとする

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
VLANを設定する
# ether 1 vlan untag 10
# ether 2 vlan untag 10

STPを設定する
# stp mode stp
# ether 1 stp use on
# ether 2 stp use on

設定終了
# save
# commit
```

8.2 MSTP を使う

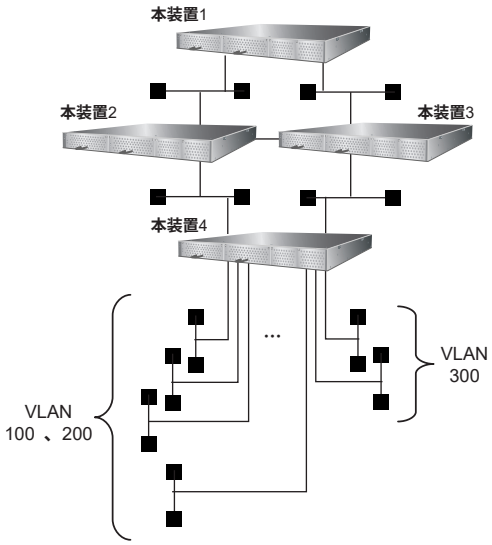
適用機種 全機種

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。

☛ 参照 マニュアル「機能説明書」

● 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　：本装置 1 →本装置 2 →本装置 3 →本装置 4

[インスタンス 1]

- ブリッジの優先順位　：本装置 1 →本装置 2 →本装置 3 →本装置 4
- VLAN 割り当て　：100、200

[インスタンス 2]

- ブリッジの優先順位　：本装置 1 →本装置 3 →本装置 2 →本装置 4
- VLAN 割り当て　：300

[本装置 1]

- ETHER19 ポートを本装置 2 に接続する
- ETHER26 ポートを本装置 3 に接続する
- ETHER19、26 ポートの STP パスコストを、全インスタンスで 20000 とする

[本装置 2]

- ETHER19 ポートを本装置 1 に接続する
- ETHER23 ポートを本装置 3 に接続する
- ETHER26 ポートを本装置 4 に接続する
- ETHER19、23、26 ポートの STP パスコストを、全インスタンスで 20000 とする

[本装置3]

- ETHER19 ポートを本装置 1 に接続する
- ETHER23 ポートを本装置 2 に接続する
- ETHER26 ポートを本装置 4 に接続する
- ETHER19、23、26 ポートの STP パスコストを、全インスタンスで 20000 とする

[本装置4]

- ETHER19 ポートを本装置 2 に接続する
- ETHER26 ポートを本装置 3 に接続する
- ETHER19、26 ポートの STP パスコストを、全インスタンスで 20000 とする
- ETHER20、21 ポートで VLAN100 の端末と接続する
- ETHER22 ポートで VLAN200 の端末と接続する
- ETHER24、25 ポートで VLAN300 の端末と接続する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

[本装置1]

```
ETHER19、23 ポートに STP パスコストを設定する
# ether 19,23 stp domain 0 cost 20000
# ether 19,23 stp domain 1 cost 20000
# ether 19,23 stp domain 2 cost 20000

VLAN を設定する
# ether 19,23 vlan tag 100,200,300

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

設定終了
# save
# commit
```

[本装置2]

```
ETHER19、23、26 ポートに STP パスコストを設定する
# ether 19,23,26 stp domain 0 cost 20000
# ether 19,23,26 stp domain 1 cost 20000
# ether 19,23,26 stp domain 2 cost 20000

VLAN を設定する
# ether 19,23,26 vlan tag 100,200,300

STP を設定する
# stp mode mstp
# stp domain 1 vlan 100,200
# stp domain 2 vlan 300
# stp domain 0 priority 8192
# stp domain 1 priority 8192
```

```
# stp domain 2 priority 12288

設定終了
# save
# commit
```

[本装置3]

```
ETHER19、23、26ポートにSTPパスコストを設定する
# ether 19,23,26 stp domain 0 cost 20000
# ether 19,23,26 stp domain 1 cost 20000
# ether 19,23,26 stp domain 2 cost 20000

VLANを設定する
# ether 19,23,26 vlan tag 100,200,300

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

設定終了
# save
# commit
```

[本装置4]

```
ETHER19、26ポートにSTPパスコストを設定する
# ether 19,26 stp domain 0 cost 20000
# ether 19,26 stp domain 1 cost 20000
# ether 19,26 stp domain 2 cost 20000

VLANを設定する
# ether 19,26 vlan tag 100,200,300

STPを設定する
# stp mode mstp
# stp domain 1 vlan 100,200
# stp domain 2 vlan 300
# stp domain 0 priority 32768
# stp domain 1 priority 32768
# stp domain 2 priority 32768

設定終了
# save
# commit
```

9　IGMPスヌープ機能を使う

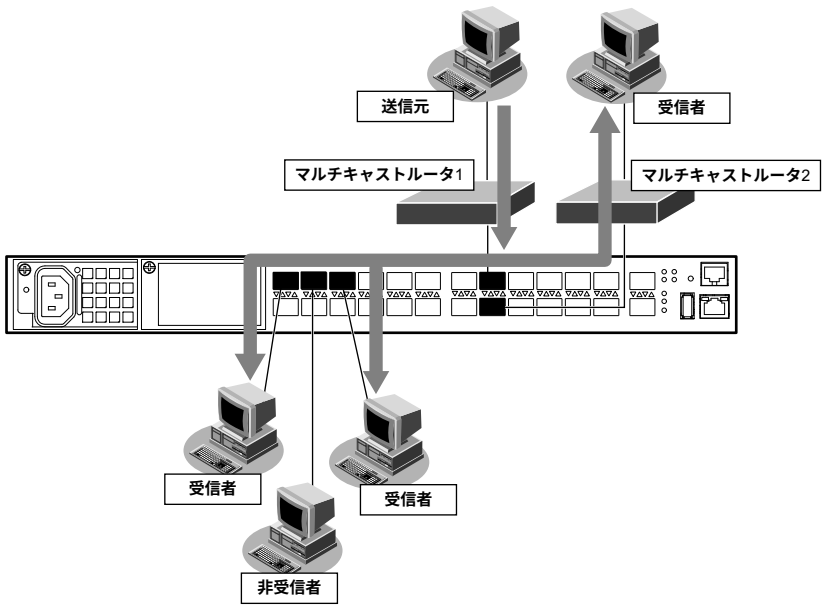
適用機種　全機種

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。

☛参照　マニュアル「機能説明書」

こんな事に気をつけて

- 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は、通信が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。詳細は、マニュアル「コマンドリファレンス」を参照してください。
- 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flooding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。
- 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。
- 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	：ETHER1、2 ポート
	VLAN	：10
リスナ端末 2	ポート	：ETHER3、4 ポート
	VLAN	：11
リスナ端末 3	ポート	：ETHER5、6 ポート
	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 ETHER15 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 ETHER16 に接続する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

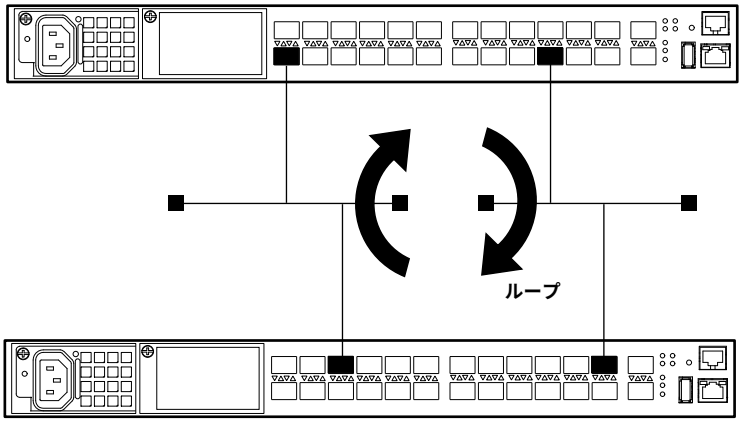
```
IGMP スヌープ機能を使用する
# igmpsnoop use on

ポートを設定する
# ether 1-2 vlan untag 10
# ether 3-4 vlan untag 11
# ether 5-6 vlan untag 12
# ether 15 vlan tag 10,11,12
# ether 16 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
# vlan 10 igmpsnoop router yes 15,16

設定終了
# save
# commit
```

10　ループ検出機能を使う

適用機種　全機種

ループ検出機能を利用すると、ネットワーク上でのパケットのループを防止するためにループ検出およびループしているポートを閉鎖または論理的に遮断することができます。

ここではループ検出機能の設定方法を説明します。



● 設定条件

- ループ検出機能を有効にする
- ポート閉塞を行う
- ループ検出用フレームの送信間隔　　：1分

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
ループ検出機能を設定する
# loopdetect use on
# loopdetect portdisable yes
# loopdetect interval 1m

設定終了
# save
# commit
```

こんな事に気をつけて

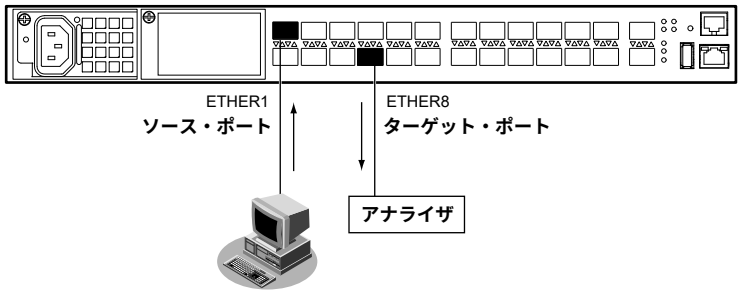
- 閉塞されたポートは自動では復旧しません。online コマンドで復旧させてください。
- トラフィックが高負荷状態になった場合、ループを検出することができません。ブロードキャスト／マルチキャストストーム制御を併用してください。
- STP 機能が有効なポートでは、ループ検出時にポートを論理的に遮断する指定はできません。

11　ポート・ミラーリング機能を使う

適用機種　全機種

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・ポートの受信トラフィックまたは送信トラフィックを監視することができます。

ここでは、ETHER1 ポートをソース・ポート、ETHER8 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。



● 設定条件

- ETHER1 ポートをソース・ポートとする（受信フレーム指定）
- ETHER8 ポートをターゲット・ポートとする

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
ETHER8 ポートのポート種別をミラーポートに設定する
# ether 8 type mirror 0 1 rx

設定終了
# save
# commit
```

12　ether L3 監視機能を使う

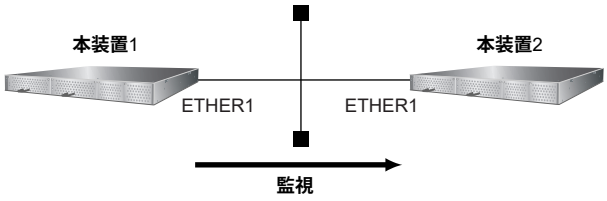
適用機種　全機種

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。

こんな事に気をつけて

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

- ETHER1 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

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

[本装置 1]

```
ETHER1 ポートを設定する
# ether 1 vlan untag 1

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

監視あて先 IP アドレスを設定する
# ether 1 icmpwatch address 192.168.10.2

監視間隔を設定する
# ether 1 icmpwatch interval 15s 40s 5s

設定終了
# save
# commit
```

[本装置2]

```
ETHER1 ポートを設定する
# ether 1 vlan untag 1

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

設定終了
# save
# commit
```

12.1 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

適用機種 全機種

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

- ETHER1～4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

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

[本装置1]

```
ETHER1～4ポートを設定する
# ether 1-4 vlan tag 10

ETHER1～4ポートをリンクアグリゲーションとして設定する
# ether 1-4 type linkaggregation 1

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

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

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

設定終了
# save
# commit
```

[本装置2]

```
ETHER1～4 ポートを設定する
# ether 1-4 vlan tag 10

ETHER1～4 ポートをリンクアグリゲーションとして設定する
# ether 1-4 type linkaggregation 1

192.168.10.1/24 のネットワークを設定する
# lan 0 ip address 192.168.10.2/24 3
# lan 0 vlan 10

設定終了
# save
# commit
```

13　ポート閉塞機能を使う

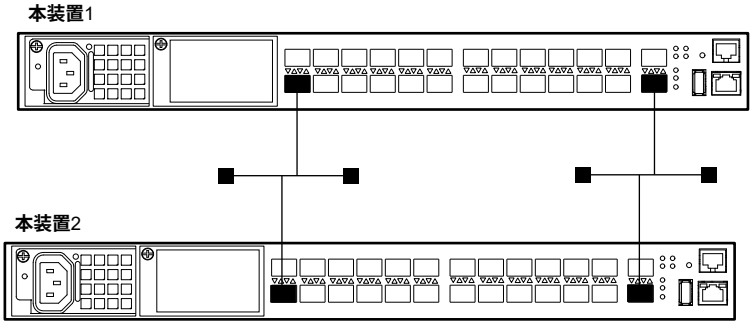
適用機種　全機種

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。

こんな事に気をつけて

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

[本装置 1]

- 各装置で ETHER2、26 ポートをバックアップポートとして使用する
  （ETHER2 をマスタポート、ETHER26 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

[本装置 2]

- 各装置で ETHER2、26 ポートをバックアップポートとして使用する
  （ETHER2 をマスタポート、ETHER26 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

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

[本装置1側]

```
ETHER2 ポートでリンクダウン回数の上限値を設定する
# ether 2 recovery limit 5

ETHER2 ポート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
# ether 2 type backup 1 master

ETHER26 ポート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
# ether 26 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
# backup 1 mode master

設定終了
# save
# commit
```

[本装置2側]

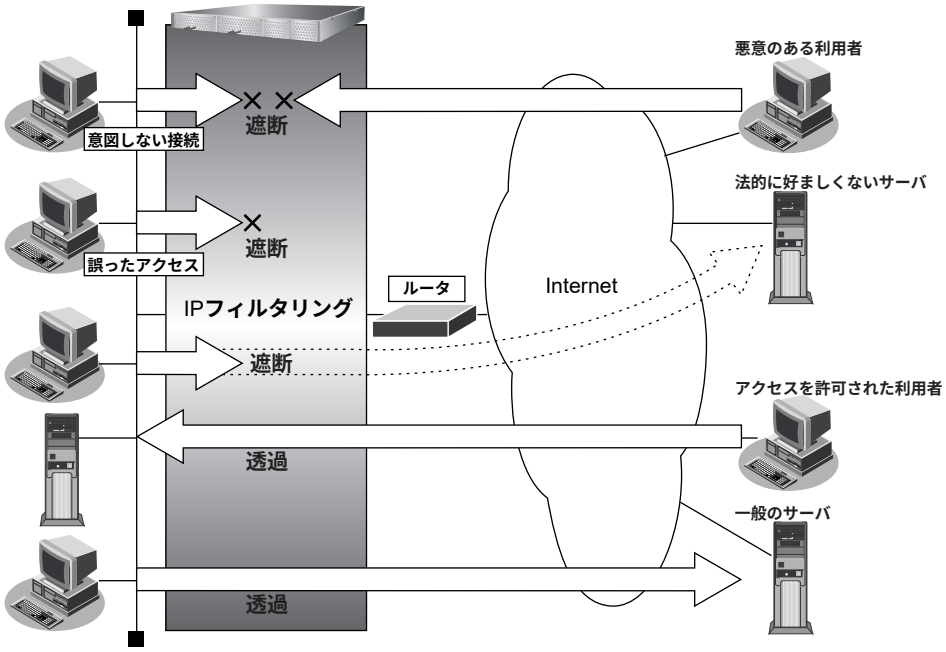
```
ETHER2 ポートでリンクダウン回数の上限値を設定する
# ether 2 recovery limit 5

ETHER2 ポート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
# ether 2 type backup 1 master

ETHER26 ポート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
# ether 26 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
# backup 1 mode master

設定終了
# save
# commit
```

14　IPフィルタリング機能を使う

適用機種　全機種

参照　マニュアル「機能説明書」

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

IP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

こんな事に気をつけて

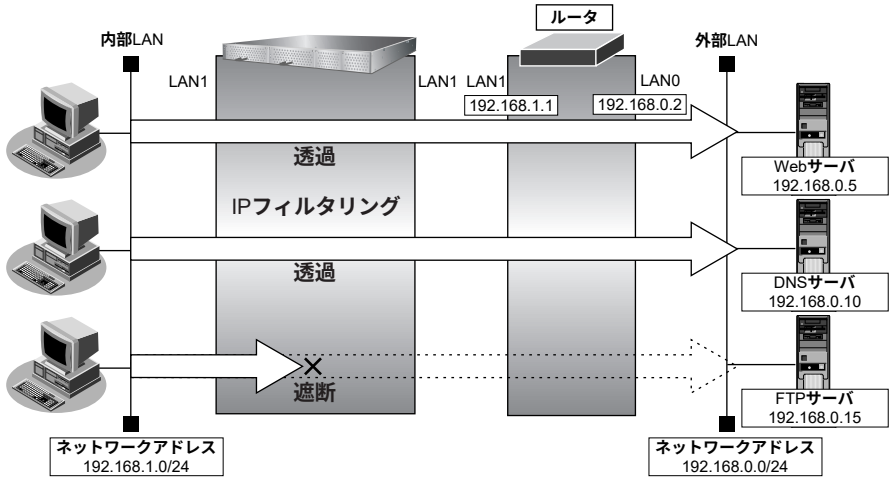
IP フィルタリング条件が複数存在する場合、それぞれの条件に優先順位がつき、数値の小さいものから優先的に採用されます。設定内容によっては通信できなくなる場合がありますので、優先順位を意識して設定してください。

14.1 外部の特定サービスへのアクセスだけを許可する

適用機種 全機種

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。

補足 DNSサーバに問い合わせが発生する場合、DNSサーバへのアクセスを許可する必要があります。
DNSサーバへのアクセスを許可することによって、Webサービス以外でドメイン名を指定した場合もDNSサーバへの発信が発生します。あらかじめ接続するWebサーバが決まっている場合は、本装置のDNSサーバ機能を利用することによって、DNSサーバへの発信を抑止することができます。



● 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

こんな事に気をつけて

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
  (2) Webサーバからの応答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
  (2) DNSサーバからの応答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

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

● コマンド

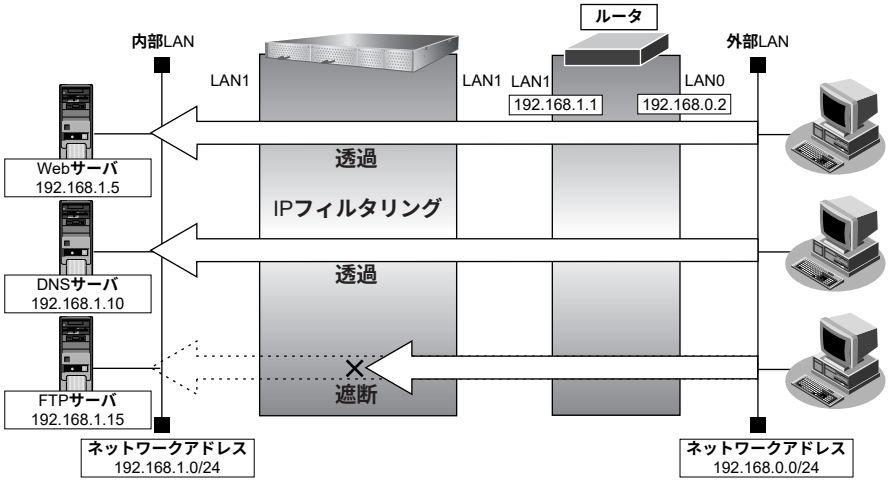
```
任意のWebサーバのポート80 へのTCPパケットを透過させる
# acl 0 ip 192.168.1.0/24 any 6 any
# acl 0 tcp any 80
# lan 1 ip filter 0 pass acl 0

Webサーバからの応答パケットを透過させる
# acl 1 ip any 192.168.1.0/24 6 any
# acl 1 tcp 80 any
# lan 1 ip filter 1 pass acl 1

DNSサーバのポート53へのUDPパケットを透過させる
# acl 2 ip 192.168.1.0/24 192.168.0.10/32 17 any
# acl 2 udp any 53
# lan 1 ip filter 2 pass acl 2

DNSサーバからの応答パケットを透過させる
# acl 3 ip 192.168.0.10/32 192.168.1.0/24 17 any
# acl 3 udp 53 any
# lan 1 ip filter 3 pass acl 3

ICMPのパケットを透過させる
# acl 4 ip any any 1 any
# lan 1 ip filter 4 pass acl 4

残りのパケットをすべて遮断する
# acl 5 ip any any any any
# lan 1 ip filter 5 reject acl 5

設定終了
# save
# commit
```

14.2 外部から特定サーバへのアクセスだけを許可する

適用機種 全機種

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。

補足 DNSサーバに問い合わせが発生する場合、DNSサーバへのアクセスを許可する必要があります。
DNSサーバへのアクセスを許可することによって、Web サービス以外でもドメイン名で指定されるとDNSサーバへの問い合わせが発生します。あらかじめ接続するWeb サーバが決まっている場合は、本装置のDNSサーバ機能を利用することで、DNSサーバへの問い合わせを抑止することができます。



● 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

こんな事に気をつけて

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
  (2) Webサーバからの応答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
  (2) DNSサーバからの応答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

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

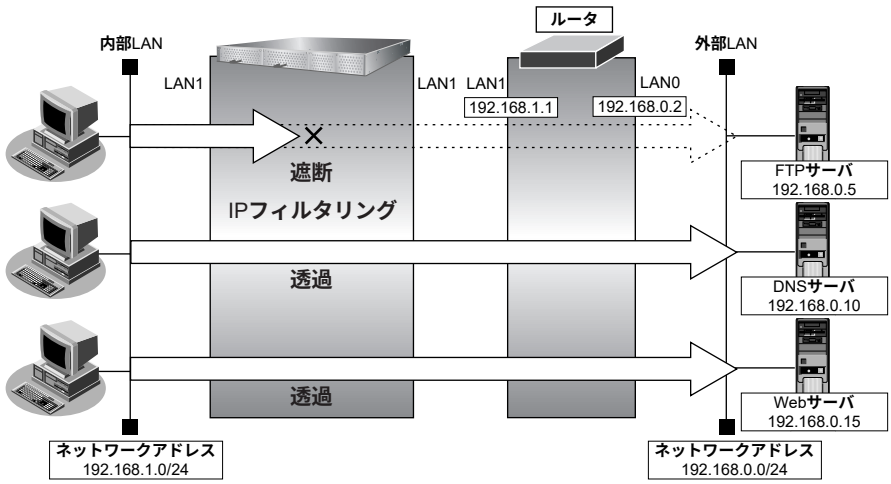
● コマンド

```
Webサーバのポート80へのTCPパケットを透過させる
# acl 0 ip 192.168.0.0/24 any 6 any
# acl 0 tcp any 80
# lan 1 ip filter 0 pass acl 0

Webサーバからの応答パケットを透過させる
# acl 1 ip any 192.168.0.0/24 6 any
# acl 1 tcp 80 any
# lan 1 ip filter 1 pass acl 1

DNSサーバのポート53へのUDPパケットを透過させる
# acl 2 ip 192.168.0.0/24 192.168.1.10/32 17 any
# acl 2 udp any 53
# lan 1 ip filter 2 pass acl 2

DNSサーバからの応答パケットを透過させる
# acl 3 ip 192.168.1.10/32 192.168.0.0/24 17 any
# acl 3 udp 53 any
# lan 1 ip filter 3 pass acl 3

ICMPのパケットを透過させる
# acl 4 ip any any 1 any
# lan 1 ip filter 4 pass acl 4

残りのパケットをすべて遮断する
# acl 5 ip any any any any
# lan 1 ip filter 5 reject acl 5

設定終了
# save
# commit
```

14.3 外部の特定サーバへのアクセスだけを禁止する

適用機種 全機種

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。



● 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

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

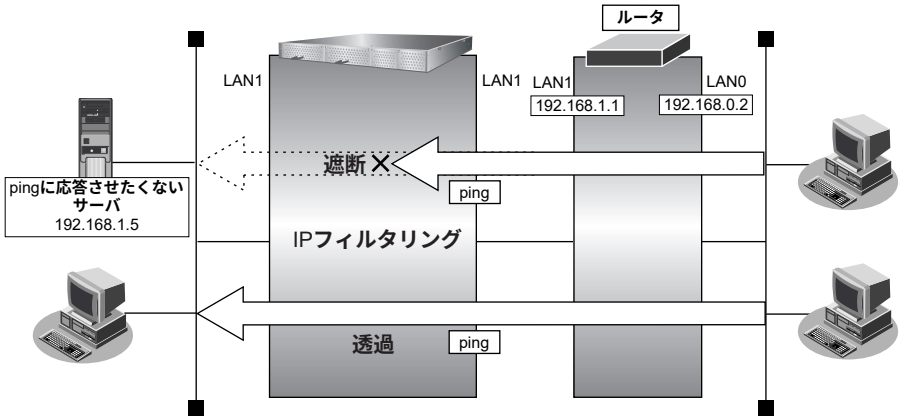
● コマンド

```
内部のLANから192.168.0.5へのFTPのパケットを遮断する
# acl 0 ip 192.168.1.0/24 192.168.0.5/32 6 any
# acl 0 tcp any 21
# lan 1 ip filter 0 reject acl 0

設定終了
# save
# commit
```

14.4 外部から特定サーバへのpingだけを禁止する

適用機種 全機種

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。



● 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

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

● コマンド

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

残りのパケットをすべて透過させる
# acl 1 ip any any any any
# lan 1 ip filter 1 pass acl 1

設定終了
# save
# commit
```

15　DSCP値書き換え機能を使う

適用機種　*SR-X340TR1, 526R1*

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ーに合わせることができます。

☛参照　マニュアル「機能説明書」

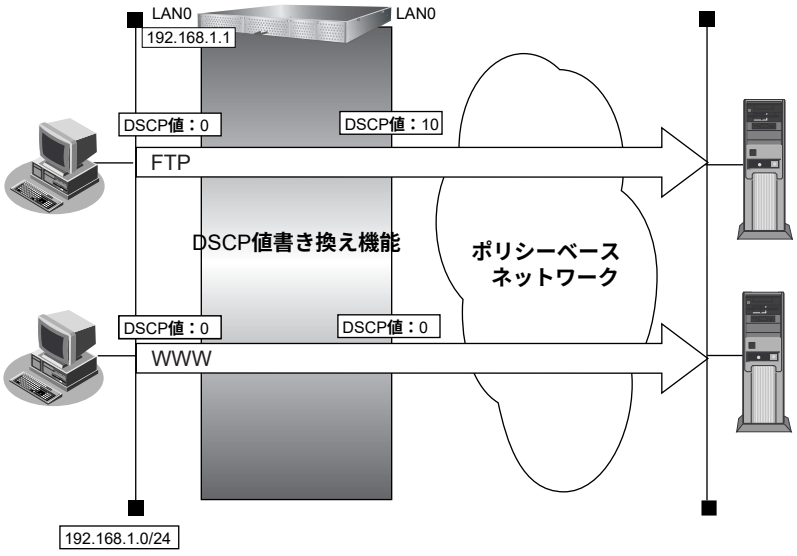
DSCP値書き換え機能の条件

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ポリシーベースネットワークのポリシーに合った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

ここではネットワークが以下のポリシー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

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● 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
# acl 0 ip 192.168.1.0/24 any 6 dscp 0
# acl 0 tcp any 20,21
# lan 0 ip dscp 0 acl 0 10

設定終了
# save
# commit
```

16　DNSサーバ機能を使う（ProxyDNS）

適用機種　全機種

本装置のProxyDNSには、以下の機能があります。

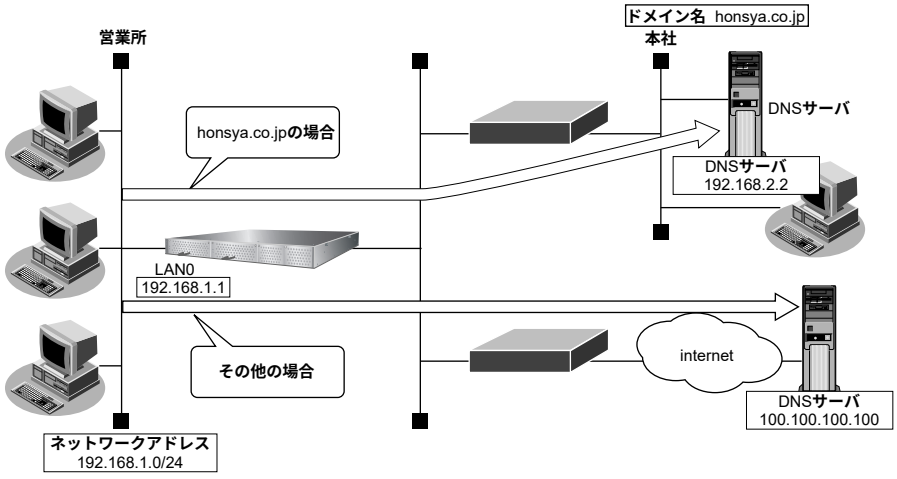
- DNSサーバの自動切り替え機能
- DNS問い合わせタイプフィルタ機能
- DNSサーバ機能

参照　マニュアル「機能説明書」

16.1　DNSサーバの自動切り替え機能（順引き）を使う

適用機種　全機種

ProxyDNSは、パソコン側で本装置のIPアドレスをDNSサーバのIPアドレスとして登録するだけで、ドメインごとに使用するDNSサーバを切り替えて中継できます。ここでは、順引きの場合の設定方法を説明します。



● 設定条件

- 会社のDNSサーバを使用する場合
  使用するドメイン　　：honsya.co.jp
  DNSサーバのIPアドレス　　：192.168.2.2
- インターネット上のDNSサーバを使用する場合
  使用するドメイン　　：honsya.co.jp以外
  DNSサーバのIPアドレス　　：100.100.100.100

こんな事に気をつけて

コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

参照　マニュアル「コマンドユーザーズガイド」の「コマンドで入力できる文字一覧」

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
DNS サーバ自動切り替え機能（順引き）を設定する
# proxydns domain 0 any *.honsya.co.jp any static 192.168.2.2
# proxydns domain 1 any * any static 100.100.100.100

設定終了
# save
# commit
```

パソコン側の設定を確認する

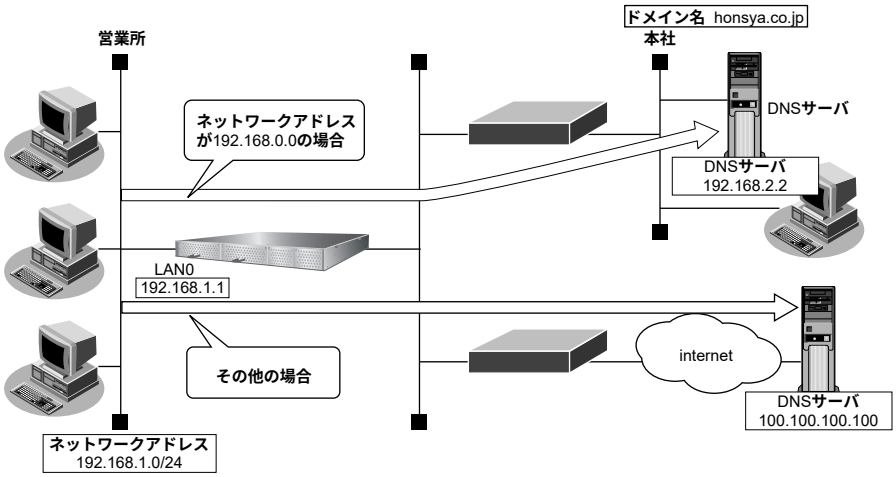
1. パソコン側が DHCP クライアントかどうか確認します。

DHCP クライアントでない場合は設定します。

16.2 DNSサーバの自動切り替え機能（逆引き）を使う

適用機種 全機種

ProxyDNSは、先に説明した順引きとは逆に、IPアドレスごとに使用するDNSサーバを切り替えて中継できます。ここでは、逆引きの場合の設定方法を説明します。



● 設定条件

- 会社のDNSサーバを使用する場合
  逆引き対象のネットワークアドレス　：192.168.0.0
  DNSサーバのIPアドレス　：192.168.2.2
- インターネット上のDNSサーバを使用する場合
  逆引き対象のネットワークアドレス　：192.168.0.0以外
  DNSサーバのIPアドレス　：100.100.100.100

こんな事に気をつけて

コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

☛参照 マニュアル「コマンドユーザーズガイド」の「コマンドで入力できる文字一覧」

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
DNSサーバ自動切り替え機能（逆引き）を設定する
# proxydns address 0 192.168.0.0/24 static 192.168.2.2
# proxydns address 1 any static 100.100.100.100

設定終了
# save
# commit
```

パソコン側の設定を確認する

1. パソコン側がDHCPクライアントかどうか確認します。

DHCPクライアントでない場合は設定します。

16.3 DNS問い合わせタイプフィルタ機能を使う

適用機種 全機種

端末が送信するDNSパケットのうち、特定の問い合わせタイプ（QTYPE）のパケットを破棄することができます。

こんな事に気をつけて

ProxyDNS機能を使用する場合、問い合わせタイプがA（1）のDNS問い合わせパケットを破棄するように指定にすると、正常な通信が行えなくなります。

● 設定条件

- ドメイン名　：＊
- 問い合わせタイプ　：SOA（6）
- 動作　：破棄する

こんな事に気をつけて

コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

☛参照 マニュアル「コマンドユーザーズガイド」の「コマンドで入力できる文字一覧」

上記の設定条件に従って設定を行う場合のコマンド例を示します。

本装置側を設定する

● コマンド

```
DNS問い合わせパケット破棄を設定する
# proxydns domain 0 6 * any reject

設定終了
# save
# commit
```

パソコン側の設定を行う

ここでは、Windows 2000の場合を例に説明します。

1. ［コントロールパネル］ウィンドウで［ネットワークとダイヤルアップ接続］アイコンをダブルクリックします。
2. ［ローカルエリア接続］アイコンを右クリックし、プロパティを選択します。
   ［ローカルエリア接続のプロパティ］ダイアログボックスが表示されます。
3. 一覧から「インターネットプロトコル（TCP/IP）」をクリックして選択します。
4. ［プロパティ］ボタンをクリックします。
5. 「次のDNSサーバーのアドレスを使う」を選択します。
6. 「優先DNSサーバー」に、本装置のIPアドレスを入力します。
7. ［OK］ボタンをクリックします。
8. ［はい］ボタンをクリックし、パソコンを再起動します。
   再起動後に、設定した内容が有効になります。

16.4 DNS サーバ機能を使う

適用機種 全機種

本装置のホストデータベースにホスト名と IP アドレスを登録します。登録したホストに対して DNS 要求があった場合は、ProxyDNS が DNS サーバの代わりに応答します。

● 設定条件

- ホスト名 ：host.com
- IPv4 アドレス ：192.168.1.2

こんな事に気をつけて

コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

☛ 参照 マニュアル「コマンドユーザーズガイド」の「コマンドで入力できる文字一覧」

上記の設定条件に従って設定を行う場合のコマンド例を示します。

本装置側を設定する

● コマンド

```
ホストデータベース情報を設定する
# host 0 name host.com
# host 0 ip address 192.168.1.2

設定終了
# save
# commit
```

補足 ホストデータベース情報は「DNS サーバ機能」で使われており、必要な項目だけを設定します。

パソコン側の設定を行う

パソコン側の設定を行います。

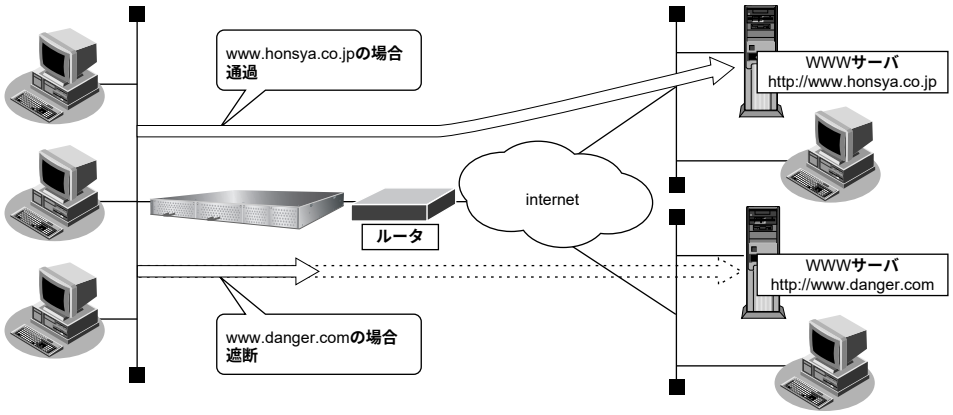
設定方法は、「16.3 DNS 問い合わせタイプフィルタ機能を使う」（P.58）の「 パソコン側の設定を行う」（P.59）を参照してください。

17　特定のURLへのアクセスを禁止する（URLフィルタ機能）

適用機種　全機種

URLフィルタ機能は、特定のURLへのアクセスを禁止することができます。本機能を使用する場合は、ProxyDNS情報で設定します。

以下にURLフィルタを行う場合の設定方法を説明します。



☛参照　マニュアル「機能説明書」

ここでは、会社のネットワークとプロバイダがすでに接続されていることを前提とします。また、ProxyDNS情報は何も設定されていないものとします。

● 設定条件

- アクセスを禁止するドメイン名　：www.danger.com
- DNSサーバのIPアドレス　：100.100.100.100

こんな事に気をつけて

- URLフィルタ機能を使用する場合は、LAN内のパソコンが本装置のIPアドレスをDNSサーバのIPアドレスとして登録する必要があります。
- コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

  ☛参照　マニュアル「コマンドユーザーズガイド」の「コマンドで入力できる文字一覧」

ヒント

◆「＊」は使えるの？

たとえば「www.danger.com」と「XXX.danger.com」の両方をURLフィルタの対象とする場合は「＊.danger.com」と指定することで両方を対象にできます。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

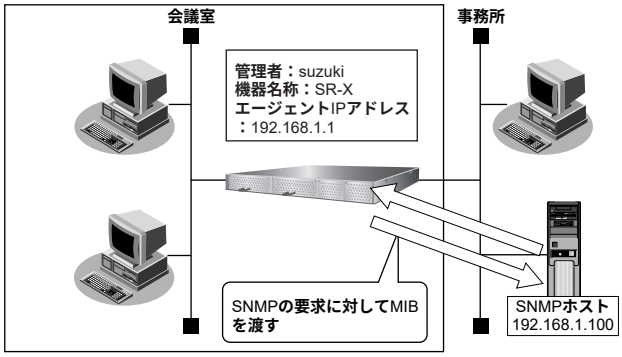
● コマンド

```
URLの情報を設定する
# proxydns domain 0 any www.danger.com any reject
# proxydns domain 1 any * any static 100.100.100.100

設定終了
# save
# commit
```

18　SNMP エージェント機能を使う

適用機種　全機種

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。



参照　マニュアル「機能説明書」

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。

参照　マニュアル「仕様一覧」

こんな事に気をつけて

- 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。

SNMPv1 または SNMPv2c でアクセスする場合の情報を設定する

SNMPv1 または SNMPv2c でアクセスする場合は、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　：SR-X
- 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

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
SNMP エージェント情報を設定する
# snmp agent contact suzuki
# snmp agent sysname SR-X
# snmp agent location 1F
# snmp agent address 192.168.1.1

SNMP ホスト情報を設定する
# snmp manager 0 192.168.1.100 public00 off disable

SNMP エージェント機能を使用する
# snmp service on

設定終了
# save
# commit
```

SNMPv3 でアクセスする場合の情報を設定する

SNMPv3 でアクセスする場合は、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　：SR-X
- 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。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
SNMP エージェント情報を設定する
# snmp agent contact suzuki
# snmp agent sysname SR-X
# snmp agent location 1F
# snmp agent address 192.168.1.1

SNMPv3 情報を設定する
# snmp user 0 name user00
# snmp user 0 address 0 192.168.1.100
# snmp user 0 notification 0 192.168.1.100

認証・暗号プロトコルを設定する
# snmp user 0 auth md5 auth_password
# snmp user 0 priv des priv_password

MIB ビュー情報を設定する
# snmp user 0 read view 0
# snmp user 0 notify view 0
# snmp view 0 subtree 0 include system
# snmp view 0 subtree 1 include interfaces
# snmp view 0 subtree 2 include linkdown
# snmp view 0 subtree 3 include linkup

SNMP エージェント機能を使用する
# snmp service on

設定終了
# save
# commit
```

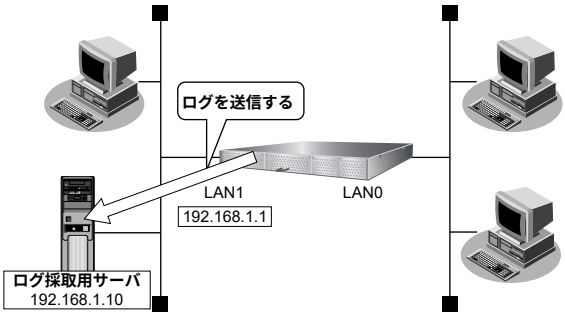
19　システムログを採取する

適用機種　全機種

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。また、セキュリティログとして以下のログを採取することができます。

- URL フィルタ（遮断したパケット）

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
- 以下のセキュリティログを採取する
  - Proxy DNS
- ログ受信用サーバの IP アドレス　：192.168.1.10

上記の設定条件に従ってシステムログを採取する場合のコマンド例を示します。

● コマンド

```
# syslog server 0 address 192.168.1.10

システムログを設定する
# syslog pri error,warn,notice,info
# syslog security proxydns

設定終了
# save
# commit
```

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。

20　スケジュール機能を使う

適用機種　全機種

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。

こんな事に気をつけて

設定前に本装置の内部時刻を正しくセットしてください。

☛参照　マニュアル「コマンドユーザーズガイド」

20.1　構成定義情報の切り替えを予約する

適用機種　全機種

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、2009年1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　　：2009年1月1日　6時30分
- 構成定義情報切り替え　　：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

上記の設定条件に従って構成定義情報を切り替える場合のコマンド例を示します。

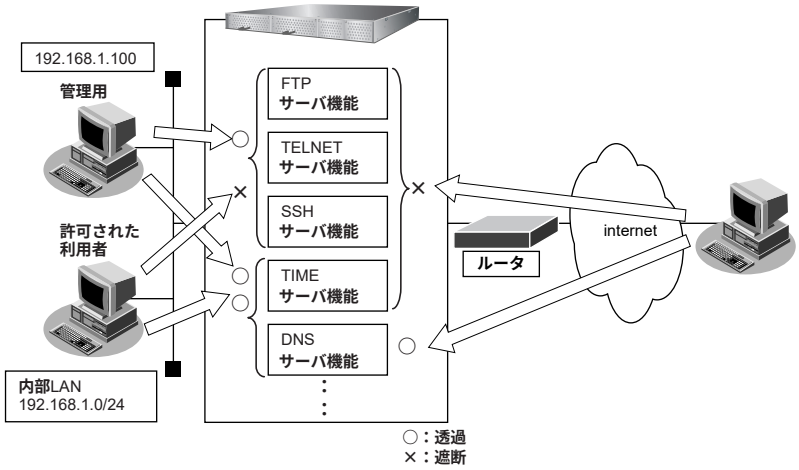
● コマンド

```
構成定義を切り替える
# addact 0 0901010630 reset config2

設定終了
# save
# commit
```

21　アプリケーションフィルタ機能を使う

適用機種　全機種

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。



ここでは、アプリケーションフィルタを利用して各サーバ機能へのアクセスを制限する場合の設定方法を説明します。

● 設定条件

- 管理用のホスト（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のホスト（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。

こんな事に気をつけて

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。

上記の設定条件に従ってアプリケーションフィルタを設定する場合のコマンド例を示します。

● 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
# serverinfo ftp filter default reject
# serverinfo telnet filter default reject
# serverinfo ssh filter default reject
# 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
# acl 0 ip 192.168.1.100/32 any any any
# serverinfo ftp filter 0 accept acl 0
# serverinfo telnet filter 0 accept acl 0
# 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
# acl 1 ip 192.168.1.0/24 any any any
# serverinfo time filter 0 accept acl 1
```

```
設定終了
# save
# commit
```

22 装置を保護する

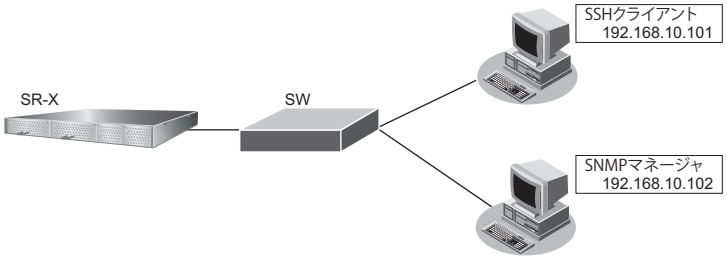
適用機種 全機種

本装置に対するセキュリティ対策として、以下の設定を行います。

- 管理者(admin)用パスワードの設定
- オートログアウトの設定
- Telnet/SSHおよびSNMP接続に対するアクセス制限
- 不要なサービスの停止

22.1 設定例

以下にそれぞれの設定を行う場合の例を示します。



● 設定条件

- 管理者(admin) パスワード ：srx_admin-2022
- IPアドレス ：192.168.10.100/24
- オートログアウトの設定（ログインしたままの状態で指定時間無操作だった際に自動切断を行う）
  コンソールのオートログアウト時間 ：5分
  SSHのオートログアウト時間 ：5分
  ※SSH のオートログアウト時間は ”telnetinfo autologout” と共通
- SNMP設定
  アクセス許可するSNMPマネージャ ：192.168.10.102
  コミュニティ名 ：private
  マネージャからの書き込み ：許可しない
- SSH接続を許可するホストのIPアドレス ：192.168.10.101
- Telnet接続 ：禁止
- 不要なサーバ機能はすべて停止
  ＃ serverinfo < サーバ機能名 > ip off
- IPv6アドレスをSR-Xに付与した際には、IPv6に関する不要なサーバ機能はすべて停止
  ＃ serverinfo < サーバ機能名 > ip6 off

```
adminパスワードをsrx_admin-2022に設定
# password admin set srx_admin-2022

コンソール接続のオートログアウト時間を5分に設定
# consoleinfo autologout 5m

Telnet/SSHのオートログアウトまでの無操作時間を5分に設定
# telnetinfo autologout 5m
```

```
自装置IPアドレスとVLANの設定
# lan 0 ip address 192.168.10.100/24 3
# lan 0 vlan 1

SNMPを有効、コミュニティ名をprivate、書き込み許可しない
# snmp service on
# snmp manager 0 192.168.10.102 private v1 disable

許可するホストからのSSH接続のみ許可する
# acl 0 ip 192.168.10.101/32 any any any
# serverinfo ssh filter 0 accept acl 0
# serverinfo ssh filter default reject

Telnetサーバ機能を停止
# serverinfo telnet ip off

不要なサーバ機能はすべて停止
# serverinfo ftp ip off
# serverinfo sftp ip off
# serverinfo http ip off
# serverinfo https ip off
# serverinfo dns ip off
# serverinfo sntp ip off
# serverinfo time ip tcp off
# serverinfo time ip udp off

設定終了
# save
# commit
```

索引

と

は

ふ

ほ

ま

ゆ

り

る

SR-X　コマンド設定事例集

P3NK-5132-02Z0

発行日　　2023年5月

発行責任　　富士通株式会社