

Fujitsu Network SR-S コマンド設定事例集

V20

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。

認証機能などによりセキュリティを強化して、安全なネットワークを提供するために、本装置をご利用ください。

2020年1月 初 版

2021年2月 第2版

2022年11月 第3版

2023年4月 第4版

本ドキュメントには「外国為替及び外国貿易管理法」に基づく特定技術が含まれています。

従って本ドキュメントを輸出または非居住者に提供するとき、同法に基づく許可が必要となります。

Microsoft Corporationのガイドラインに従って画面写真を使用しています。

Copyright Fujitsu Limited 2020-2023

目次

はじめに	2
本書の使いかた	6
本書の読者と前提知識	6
本書における商標の表記について	7
本装置のマニュアルの構成	8
1 VLAN 機能を使う	9
1.1 ポート VLAN 機能を使う	9
1.2 タグ VLAN 機能を使う	10
1.3 プロトコル VLAN 機能を使う	11
2 リンクアグリゲーション機能を使う	12
2.1 LACP 機能を使う	13
3 MLAG 機能を使う	15
4 バックアップポート機能を使う	18
4.1 マスタポートを優先的に使用する	18
4.2 VLAN ごとに両方のポートを同時に使用する	19
5 MAC フィルタリング機能を使う	21
5.1 特定 MAC アドレスからのパケットだけを許可する	22
5.2 特定 MAC アドレスへのパケットだけを許可する	23
5.3 特定パケット形式のパケットだけを禁止する	24
5.4 VLAN 単位で特定 MAC アドレス間の通信だけを遮断する	25
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	26
6 スタティック MAC フォワーディング機能を使う	27
7 QoS 機能を使う	28
7.1 優先制御機能を使う	28
7.2 優先制御情報書き換え機能を使う	30
8 STP 機能を使う	34
8.1 STP を使う	34
8.2 MSTP を使う	35
9 DHCP スヌープ機能を使う	39
10 IGMP スヌープ機能を使う	41
11 IEEE802.1X 認証機能を使う	43
12 Web 認証機能を使う	46
12.1 AAA でローカル認証を行う	46
12.2 AAA でリモート認証を行う	49
12.3 認証ログイン画面のカスタマイズを行う	52
13 MAC アドレス認証機能を使う	53
14 接続端末数制限機能を使う	56
15 ARP 認証機能を使う	58
16 ループ検出機能を使う	60
17 ポート・ミラーリング機能を使う	61
18 ether L3 監視機能を使う	62
18.1 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	63
19 ポート閉塞機能を使う	65
20 LAN をネットワーク間接続する	67
21 IPv4 のネットワークに IPv6 ネットワークを追加する	69
22 RIP を使用したネットワークを構築する (IPv4)	71
23 RIP の経路を制御する (IPv4)	73
23.1 特定の経路情報の送信を許可する	75

23.2	特定の経路情報のメトリック値を変更して送信する	76
23.3	特定の経路情報の受信を許可する	77
23.4	特定の経路情報のメトリック値を変更して受信する	78
23.5	特定の経路情報の送信を禁止する	79
23.6	特定の経路情報の受信を禁止する	80
24	RIP の経路を制御する (IPv6)	81
24.1	特定の経路情報の送信を許可する	83
24.2	特定の経路情報のメトリック値を変更して送信する	84
24.3	特定の経路情報の受信を許可する	85
24.4	特定の経路情報のメトリック値を変更して受信する	86
24.5	特定の経路情報の送信を禁止する	87
24.6	特定の経路情報の受信を禁止する	88
25	OSPF を使用したネットワークを構築する (IPv4)	89
25.1	バーチャルリンクを使う	94
25.2	スタブエリアを使う	98
26	OSPF の経路を制御する (IPv4)	101
26.1	OSPF ネットワークでエリアの経路情報 (LSA) を集約する	101
26.2	AS 外部経路を集約して OSPF ネットワークに広報する	103
26.3	エリア境界ルータで不要な経路情報 (LSA) を遮断する	105
27	OSPF 機能を使う (IPv6)	107
27.1	OSPF ネットワークを構築する	107
27.2	エリア境界ルータでエリア内部経路を集約する	109
27.3	エリア境界ルータで不要な経路情報を遮断する	110
28	マルチキャスト機能を使う	111
28.1	マルチキャスト機能 (PIM-DM) を使う	111
28.2	マルチキャスト機能 (PIM-SM) を使う	114
28.3	マルチキャスト機能 (スタティックルーティング) を使う	120
29	IP フィルタリング機能を使う	123
29.1	外部の特定サービスへのアクセスだけを許可する	125
29.2	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)	127
29.3	外部から特定サーバへのアクセスだけを許可する	129
29.4	外部の特定サーバへのアクセスだけを禁止する	131
29.5	外部から特定サーバへの ping だけを禁止する	132
30	DSCP 値書き換え機能を使う	133
31	VRRP 機能を使う	135
31.1	簡易ホットスタンバイ機能を使う	136
31.2	クラスタリング機能を使う	139
32	ECMP 機能を使う	142
33	DHCP 機能を使う	144
33.1	DHCP サーバ機能を使う	144
33.2	DHCP スタティック機能を使う	146
33.3	DHCP リレーエージェント機能を使う	148
33.4	IPv6 DHCP サーバ機能を使う	150
33.5	IPv6 DHCP リレーエージェント機能を使う	152
34	DNS サーバ機能を使う (ProxyDNS)	153
34.1	DNS サーバの自動切り替え機能 (順引き) を使う	153
34.2	DNS サーバの自動切り替え機能 (逆引き) を使う	155
34.3	DNS 問い合わせタイプフィルタ機能を使う	156
34.4	DNS サーバ機能を使う	158
35	特定の URL へのアクセスを禁止する (URL フィルタ機能)	159
36	SNMP エージェント機能を使う	161
37	システムログを採取する	164

38	スケジュール機能を使う	165
38.1	構成定義情報の切り替えを予約する	165
39	アプリケーションフィルタ機能を使う	166
40	無線 LAN 管理機能を使う	168
40.1	無線 LAN 管理機能の環境を設定する	168
40.2	アクセスポイントモニタリングを行う	171
40.3	クライアントモニタリングを行う	172
40.4	無線 LAN アクセスポイントに MAC アドレスフィルタを配布する (MAC アドレスフィルタ配布)	173
40.5	無線 LAN アクセスポイントの電波出力を調整する (電波出力自動調整)	174
40.6	無線 LAN アクセスポイントの無線 LAN チャンネルを調整する	176
41	端末可視化機能を使う	177
42	NXconcierge と連携する	179
43	装置を保護する	182
43.1	設定例	182
索引	184

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

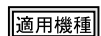
本書で使用しているマーク類は、以下のような内容を表しています。


 **ヒント** 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。

 **補足** 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。

 **参照** 操作方法など関連事項を説明している箇所を示します。

 **適用機種** 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。

 **警告** 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。

 **注意** 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

Windows 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。

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。

製品名称	本文中の表記
Microsoft® Windows® 10 Home 64ビット版	Windows 10 または Windows
Microsoft® Windows® 10 Pro 64ビット版	

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。
SR-S 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。
Web 設定事例集	Web 画面を使用した、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。
Web リファレンス	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

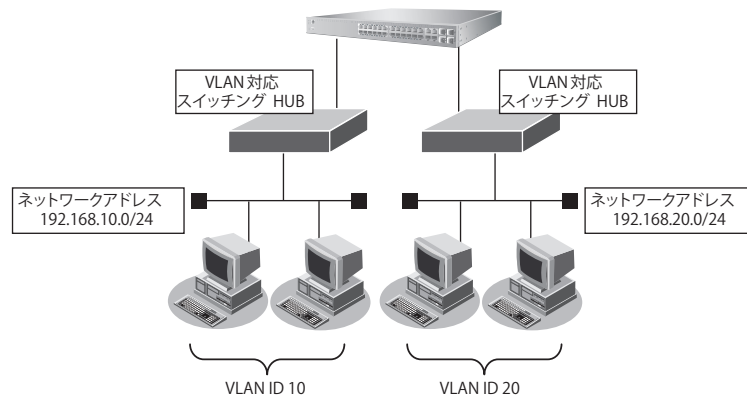
適用機種 全機種

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。

SR-S332TR1 の場合を例にします。



● 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

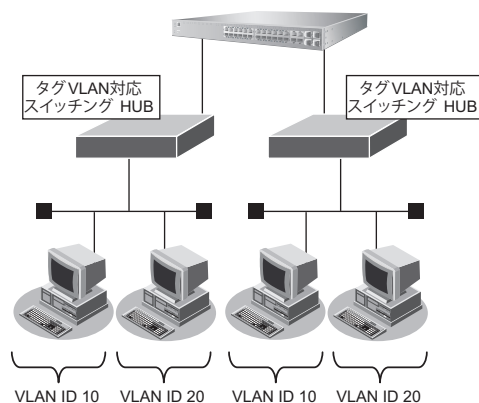
設定終了
# save
# commit
```

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。

SR-S332TR1の場合を例にします。



● 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

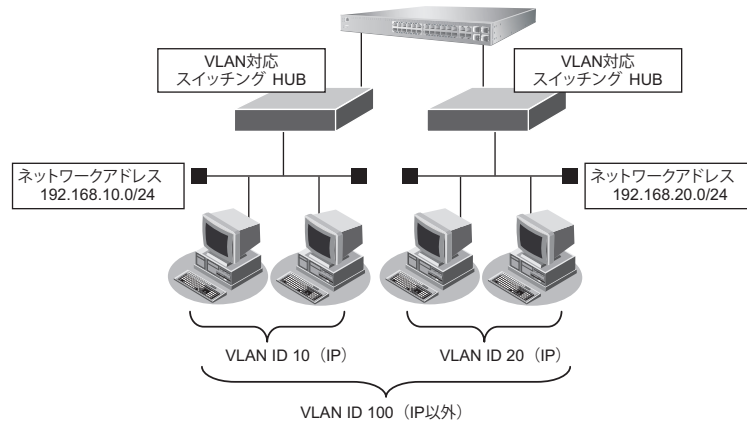
設定終了
# save
# commit
```

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。

SR-S332TR1の場合を例にします。



● 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

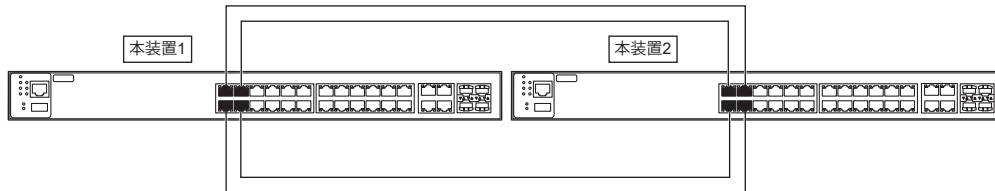
192.168.20.1/24のネットワークを設定する
# lan 1 ip address 192.168.20.1/24 3
# lan 1 vlan 20

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、4ポートの1000M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。
SR-S332TR1の場合を例にします。



● 設定条件

- ETHER1～4ポートを使用する
- 通信速度を1000Mbps固定に変更する
- 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 mode 1000
# 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 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 mode 1000
# 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 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

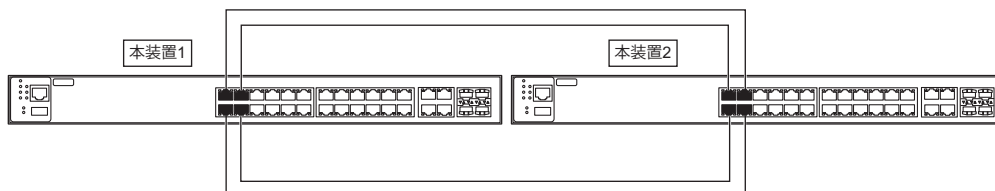
```

☞ 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、4ポートの1000M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。SR-S332TR1の場合を例にします。



● 設定条件

- ETHER1～4ポートを使用する
- 通信速度を1000Mbps固定に変更する
- 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 mode 1000
# 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 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 mode 1000
# 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 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」

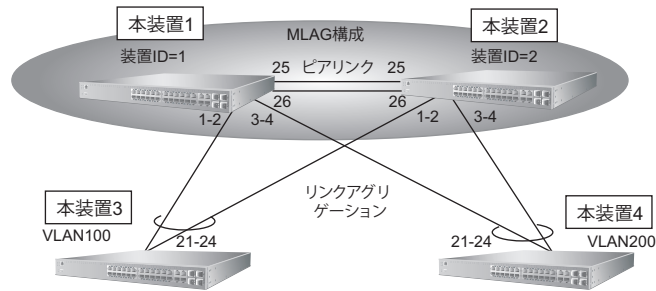
3 MLAG 機能を使う

適用機種 SR-S332TR1, 352TR1

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-S332TR1 の場合を例にします。



● 設定条件

2台のSR-S332TR1でMLAGを構成し、配下のSR-S332TR1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
- ETHER25、26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 25,26

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 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 3
# ether 3-4 vlan tag 200

STP 機能を無効にする
# stp mode disable

MAC アドレス学習テーブルのHITDA 機能を有効にする
# mac hitda on
    
```

```
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 25,26

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 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 3
# ether 3-4 vlan tag 200

STP 機能を無効にする
# stp mode disable

MAC アドレス学習テーブルのHITDA 機能を有効にする
# mac hitda on

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

適用機種 全機種

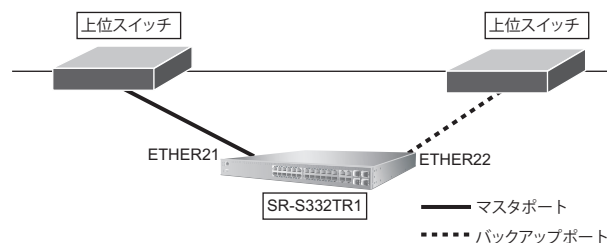
ここでは、アップリンクポートをバックアップポートとして利用する場合の設定方法について説明します。アップリンクポートをそれぞれ異なるスイッチに接続することで、冗長アップリンクの形態にできます。

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-S332TR1 の場合を例にします。



● 設定条件

- ETHER21、22 ポートをバックアップポートとして使用する (ETHER21 をマスタポート、ETHER22 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

```
ETHER21 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 21 type backup 1 master

ETHER22 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 22 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

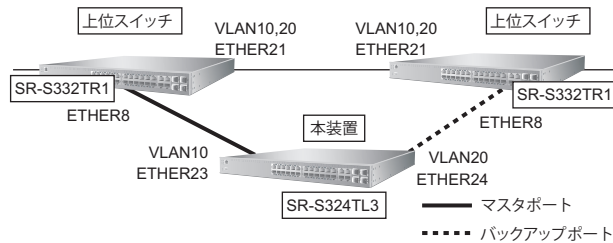
バックアップポートの切替通知動作を設定する
# backup 1 notify mode fdb-table
# backup 1 notify interval 100 20 500

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働させる場合の設定方法を説明します。本設定では、マスターポートとバックアップポートがVLANごとに同時に稼働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、残された稼働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-S332TR1とし、SR-S324TL3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、マスター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-S332TR1を上位スイッチとしてSR-S324TL3を接続する。

[本装置]

- ETHER23、24ポートをバックアップポートとして使用する
(ETHER23をマスターポート、ETHER24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
(マスターポートで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]

```
ETHER23ポートをバックアップポート (グループ3) のマスターポート (VLAN10を優先動作) に設定する
# ether 23 type backup 3 master
# ether 23 vlan tag 10
```

```
ETHER24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 24 type backup 3 backup
# ether 24 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-S332TR1 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

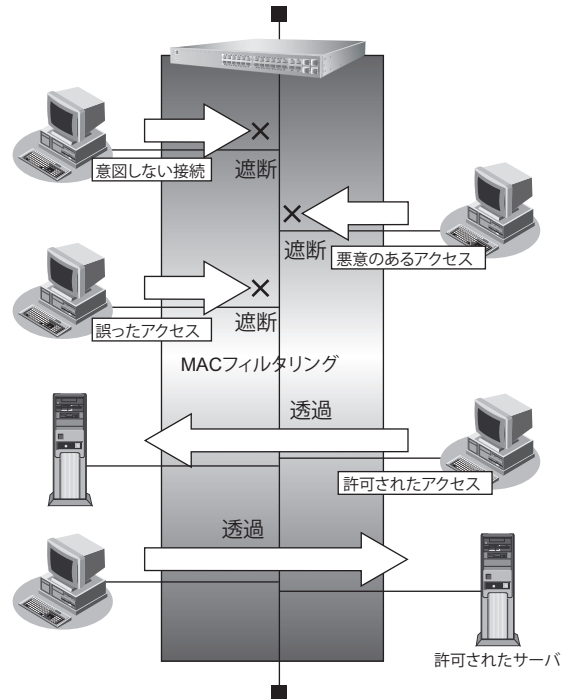
```
# save
# commit
```

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。

こんな事に気をつけて

SR-S312LE1/320LE1/324LE1 では、以下の機能を同時に使用することができません。

MAC フィルタ機能を有効にするためには、"resource filter distribution filter ipv4" を設定する必要があります。

- MAC フィルタ機能 (IPv4) / IP フィルタリング機能 (IPv4)
- MAC フィルタ機能 (IPv6 フィルタ) / IP フィルタリング機能 (IPv6)
- 優先制御情報書き換え機能 (IPv4) / DSCP 値書き換え機能 (IPv4)
- 優先制御情報書き換え機能 (IPv6) / DSCP 値書き換え機能 (IPv6)

● 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。

こんな事に気をつけて

SR-S312LE1/320LE1/324LE1では、以下の機能を同時に使用することができません。

MACフィルタ機能を有効にするためには、"resource filter distribution filter ipv4"を設定する必要があります。

- MACフィルタ機能 (IPv4) / IPフィルタリング機能 (IPv4)
- MACフィルタ機能 (IPv6フィルタ) / IPフィルタリング機能 (IPv6)
- 優先制御情報書き換え機能 (IPv4) / DSCP値書き換え機能 (IPv4)
- 優先制御情報書き換え機能 (IPv6) / DSCP値書き換え機能 (IPv6)

● 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。

こんな事に気をつけて

SR-S312LE1/320LE1/324LE1では、以下の機能を同時に使用することができません。

MACフィルタ機能を有効にするためには、"resource filter distribution filter ipv4"を設定する必要があります。

- MACフィルタ機能 (IPv4) / IPフィルタリング機能 (IPv4)
- MACフィルタ機能 (IPv6フィルタ) / IPフィルタリング機能 (IPv6)
- 優先制御情報書き換え機能 (IPv4) / DSCP値書き換え機能 (IPv4)
- 優先制御情報書き換え機能 (IPv6) / DSCP値書き換え機能 (IPv6)

● 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をSR-S332TR1を例にして示します。

● 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。

こんな事に気をつけて

SR-S312LE1/320LE1/324LE1では、以下の機能を同時に使用することができません。

MACフィルタ機能を有効にするためには、"resource filter distribution filter ipv4"を設定する必要があります。

- MACフィルタ機能 (IPv4) / IPフィルタリング機能 (IPv4)
- MACフィルタ機能 (IPv6フィルタ) / IPフィルタリング機能 (IPv6)
- 優先制御情報書き換え機能 (IPv4) / DSCP値書き換え機能 (IPv4)
- 優先制御情報書き換え機能 (IPv6) / DSCP値書き換え機能 (IPv6)

● 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、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

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。

こんな事に気をつけて

SR-S312LE1/320LE1/324LE1では、以下の機能を同時に使用することができません。

MACフィルタ機能を有効にするためには、"resource filter distribution filter ipv4"を設定する必要があります。

- MACフィルタ機能 (IPv4) / IPフィルタリング機能 (IPv4)
- MACフィルタ機能 (IPv6フィルタ) / IPフィルタリング機能 (IPv6)
- 優先制御情報書き換え機能 (IPv4) / DSCP値書き換え機能 (IPv4)
- 優先制御情報書き換え機能 (IPv6) / DSCP値書き換え機能 (IPv6)

● 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

```
# 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

```
# 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

```
# vlan 20 macfilter 0 pass 20
# vlan 20 macfilter 1 pass 21
# vlan 20 macfilter 2 pass 22
# vlan 20 macfilter 3 reject 30
```

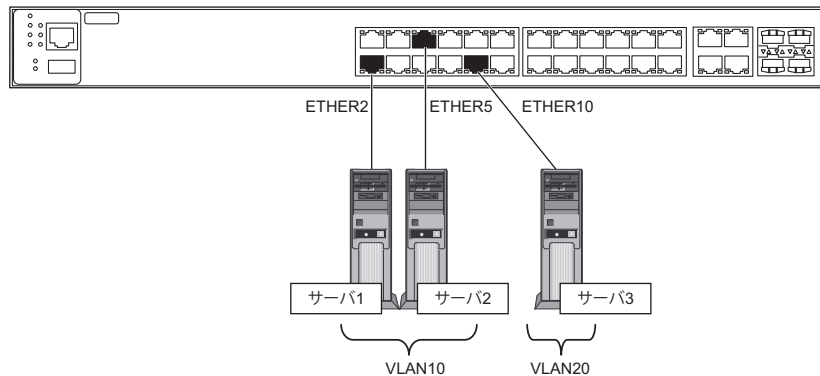
6 スタティック MAC フォワーディング機能を使う

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。

SR-S332TR1 の場合を例にします。



● 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（自装置あてポート含む）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-S312LE1/320LE1/324LE1 の場合のキューは 4 個、SR-S332TR1/352TR1/732TR1/752TR1 の場合のキューは 8 個となります。

SR-S312LE1/320LE1/324LE1 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	2
	4	
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 2
#qos cosmap 4 2
#qos cosmap 5 3
#qos cosmap 6 3
#qos cosmap 7 3
```

SR-S332TR1/352TR1/732TR1/752TR1 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
    
```

7.2 優先制御情報書き換え機能を使う

適用機種 全機種

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。

こんな事に気をつけて

SR-S312LE1/320LE1/324LE1では、以下の機能を同時に使用することができません。

優先制御情報書き換え機能を有効にするためには、"resource filter distribution qos ipv4"を設定する必要があります。

- MACフィルタ機能 (IPv4) / IPフィルタリング機能 (IPv4)
- MACフィルタ機能 (IPv6フィルタ) / IPフィルタリング機能 (IPv6)
- 優先制御情報書き換え機能 (IPv4) / DSCP値書き換え機能 (IPv4)
- 優先制御情報書き換え機能 (IPv6) / DSCP値書き換え機能 (IPv6)

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COS値を指定した値で書き換える
 - パケットのCOS値をパケットのip precedence値で書き換える
 - 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
 - パケットのip precedence値をパケットのCOS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

以下に設定例を示します。

パケットの COS 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MACアドレスを持つホストからの入力パケットのCOS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 20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
- ETHER5ポートのVLAN 20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のCOS値を5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

```
VLAN IDが20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 20 any
```

```
ETHER5ポートで(1)で設定した形式のパケットのCOS値を5に書き換える
# ether 5 qos aclmap 0 cos 5 100
```

パケットの COS 値をパケットの ip precedence 値で書き換える

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のCOS値をパケットのip precedence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のCOS値をパケットのip precedence値で書き換える

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 110 mac any 00:0b:01:02:03:04 any
# acl 110 vlan 10 any
```

```
ETHER1ポートで(1)で設定した形式のパケットのCOS値をパケットのip precedence値で書き換える
# ether 1 qos aclmap 0 cos tos 110
```

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
```

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
```


パケットの ip precedence 値をパケットの COS 値で書き換える

ここでは、VLAN内の特定ポートで特定のVLANからの入力パケットの ip precedence 値をパケットの COS 値で書き換える方法を説明します。

● 書き換え要求

- ETHER10 ポートは VLAN10、VLAN20、VLAN30 にタグ付き、VLAN100 にタグなしで属する
- ETHER10 ポートからの VLAN 20、VLAN30、VLAN100 からの入力パケットの ip precedence 値をパケットの COS 値に書き換える

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 20、30、100 のパケットの形式をそれぞれ ACL で設定する ---- (1)
# acl 100 vlan 20 any
# acl 110 vlan 30 any
# acl 120 vlan 100 any
```

```
ETHER10 ポートで (1) で作成した形式のパケットの ip precedence 値をパケットの COS 値に書き換える
# ether 10 qos aclmap 0 tos cos 100
# ether 10 qos aclmap 1 tos cos 110
# ether 10 qos aclmap 2 tos cos 120
```

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
```

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。

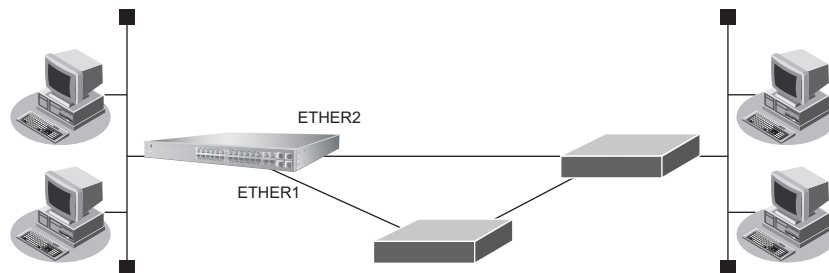
8.1 STP を使う

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」

SR-S332TR1 の場合を例にします。



● 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
# 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

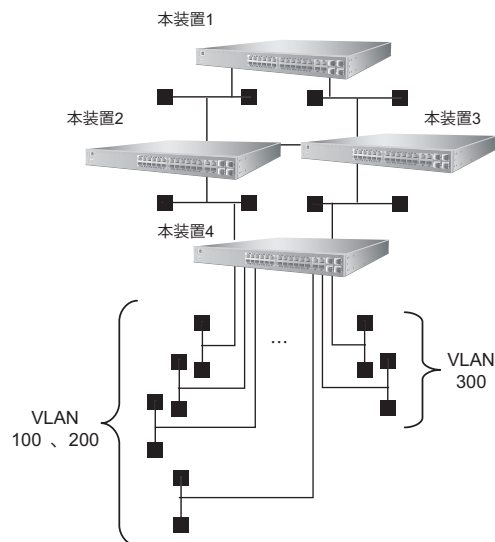
物理的にループしているネットワークでも、VLANの構成によっては、論理的にループしない場合があります。STPではループと判断して、一方のLANを通信に使わないで動作しますが、MSTPではVLAN単位に扱うことができるため、STPよりも効率的にネットワーク内のデータを流すことができます。

☛ 参照 マニュアル「機能説明書」

SR-S332TR1 の場合を例にします。

● 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
- 本装置1－本装置2間は1Gとする
- 本装置1－本装置3間は100Mとし、トラフィック量が多いものは本装置1－2間に流す
- 装置間の回線はクロスケーブルを使用する



[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]

- ETHER1ポートで本装置2と接続し、回線速度は1Gとする
- ETHER2ポートで本装置3と接続し、回線速度は100Mとする
- ETHER1、2ポートのSTPパスコストは、全インスタンス20000とする

[本装置 2]

- ETHER1 ポートで本装置 1 と接続し、回線速度は 1G とする
- ETHER2 ポートで本装置 3 と接続し、回線速度は 100M とする
- ETHER3 ポートで本装置 4 と接続し、回線速度は 1G とする
- ETHER1～3 ポートの STP パスコストは、全インスタンス 20000 とする

[本装置 3]

- ETHER1 ポートで本装置 1 と接続し、回線速度は 100M とする
- ETHER2 ポートで本装置 2 と接続し、回線速度は 100M とする
- ETHER3 ポートで本装置 4 と接続し、回線速度は 100M とする
- ETHER1～3 ポートの STP パスコストは、全インスタンス 20000 とする

[本装置 4]

- ETHER1 ポートで本装置 2 と接続し、回線速度は 1G とする
- ETHER2 ポートで本装置 3 と接続し、回線速度は 100M とする
- ETHER1、2 ポートの STP パスコストは、全インスタンス 20000 とする
- ETHER3～9 ポートで VID100 の端末と接続し、回線速度は 100M とする
- ETHER10～14 ポートで VID200 の端末と接続し、回線速度は 100M とする
- ETHER15、16 ポートで VID300 の端末と接続し、回線速度は 100M 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

[本装置 1]

```
MDI を設定する
# ether 1,2 mdi mdix

ETHER1、2 ポートの STP パスコストを設定する
# ether 1-2 stp domain 0 cost 20000
# ether 1-2 stp domain 1 cost 20000
# ether 1-2 stp domain 2 cost 20000

ETHER1、2 ポートを設定する
# ether 1 mode 1000
# ether 2 mode 100

VLAN を設定する
# ether 1-2 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]

```
MDIを設定する
# ether 1-3 mdi mdix

ETHER1～3ポートのSTPパスコストを設定する
# ether 1-3 stp domain 0 cost 20000
# ether 1-3 stp domain 1 cost 20000
# ether 1-3 stp domain 2 cost 20000

ETHER1～3ポートを設定する
# ether 1 mode 1000
# ether 2 mode 100
# ether 3 mode 1000

VLANを設定する
# ether 1-3 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]

```
MDIを設定する
# ether 1-3 mdi mdix

ETHER1～3ポートのSTPパスコストを設定する
# ether 1-3 stp domain 0 cost 20000
# ether 1-3 stp domain 1 cost 20000
# ether 1-3 stp domain 2 cost 20000

ETHER1～3ポートを設定する
# ether 1-3 mode 100

VLANを設定する
# ether 1-3 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]

```
MDIを設定する
# ether 1-16 mdi mdix

ETHER1、2ポートのSTPパスコストを設定する
# ether 1-2 stp domain 0 cost 20000
# ether 1-2 stp domain 1 cost 20000
# ether 1-2 stp domain 2 cost 20000

ETHER1～16ポートを設定する
# ether 1 mode 1000
# ether 2-16 mode 100

VLANを設定する
# ether 1 vlan tag 100,200,300
# ether 2 vlan tag 100,200,300
# ether 3-9 vlan untag 100
# ether 10-14 vlan untag 200
# ether 15,16 vlan untag 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 DHCP スヌープ機能を使う

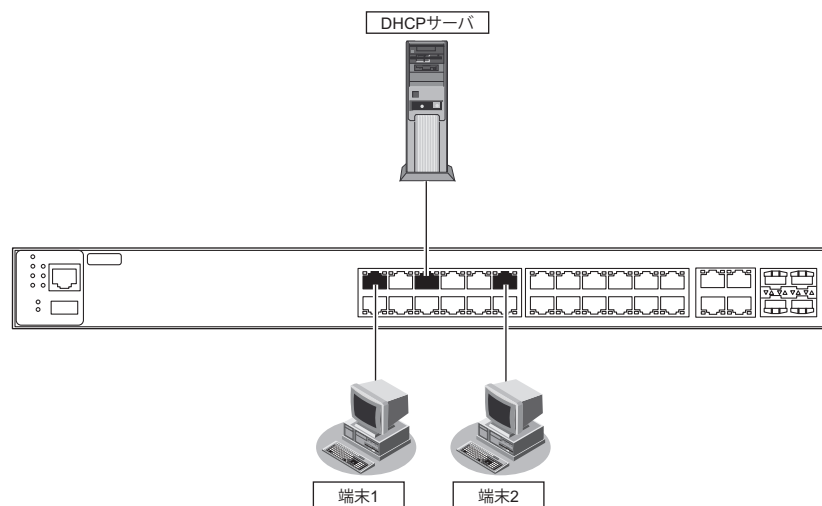
適用機種 全機種

DHCP スヌープ機能を使用すると、DHCP で IP アドレスが割り当てられた端末だけ通信を許可することができ、管理外の不正端末によるネットワークへの不正アクセスを防止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

- 本機能は IPv4 の場合に使用できます。
- DHCP サーバは trusted に設定されたポートに接続してください。
- 同一 VLAN 内で IPv4 DHCP 機能を有効に設定した場合、この VLAN では本機能が無効になり、すべての端末が通信可能となります。
- untrusted に設定されたポートで以下の条件に一致する場合、このポートでは本機能が無効になり、すべての端末が通信可能となります。
 - IEEE802.1X 認証、Web 認証および MAC アドレス認証のどれかが有効に設定されている場合
 - リンクアグリゲーションとして設定されている場合
 - タグ VLAN が設定されている場合
 - プロトコル VLAN が設定されている場合
- 本装置では、一度登録された許可端末が存在しなくなってもエントリ自体はリース期間の満了まで消去しません。DHCP サーバでリース期間を適切に設定してください。
また、不要なエントリが登録されている場合は、clear dhcp snoop コマンドで消去することができます。
- 監視可能な DHCP クライアント数を超えた場合、受信した DHCP パケットは破棄されエントリ登録されません。また、最大エントリ数に満たない場合でも登録できないことがあります。エントリ登録に失敗した場合は、登録に失敗したことを示すシステムログが記録されます。
- 本機能は DHCP パケットの往復を監視して動作します。DHCP クライアントとサーバ間の通信は必ず本装置を経由するようなネットワーク構成にしてください。
- 設定反映、または装置リセットを実行した場合、エントリが破棄される場合があります。この場合、端末が DHCP で IP アドレスを再取得するまで通信できなくなります。



● 設定条件

- VLAN10でDHCPスヌープ機能を使用する
- ETHERポートの通信許可

ETHER1ポート	: DHCPでIPアドレスを割り当てられた端末のみ
ETHER5ポート	: すべての端末
ETHER11ポート	: DHCPでIPアドレスを割り当てられた端末のみ

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

```

DHCPスヌープ機能を使用する
# vlan 10 dhcpsnoop use on

DHCPクライアントの接続ポートを設定する
# ether 1 vlan untag 10
# ether 1 dhcpsnoop trust untrusted
# ether 11 vlan untag 10
# ether 11 dhcpsnoop trust untrusted

DHCPサーバの接続ポートを設定する
# ether 5 vlan untag 10
# ether 5 dhcpsnoop trust trusted

設定終了
# save
# commit
    
```


10 IGMP スヌープ機能を使う

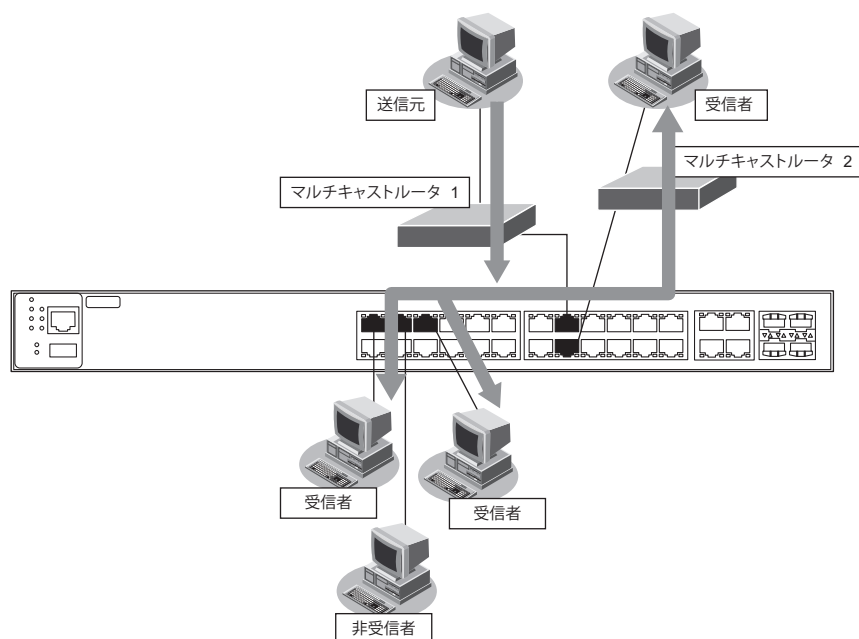
適用機種 全機種

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

- マルチキャストルーティング機能が有効であるlan 定義が存在する場合、IGMP スヌープ機能は無効となり、動作しません。
- 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破棄されます。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。
- 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 : 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
  
```

11 IEEE802.1X 認証機能を使う

適用機種 全機種

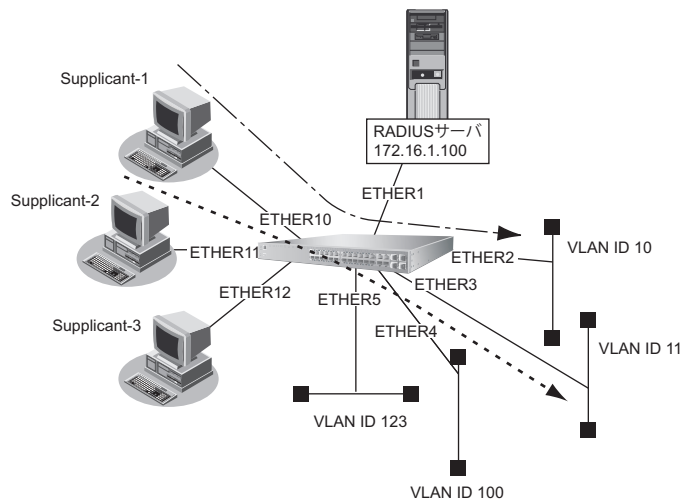
IEEE802.1X 認証を使用すると、本装置に接続する端末ユーザがネットワークへのアクセス権を持っているかを認証することができます。また、認証データベースで、ユーザごとに所属する VLAN ID を設定すると、認証されたユーザが所属するネットワークも同時に管理できます。これらの機能によりネットワークへのアクセスをユーザ単位で制御でき、ネットワークのセキュリティを向上することができます。

☛ 参照 マニュアル「機能説明書」

こんな事に気をつけて

- IEEE802.1X 認証を利用するポートでは、事前に VLAN を設定できません。ただし、以下の場合はその限りではありません。
 - Web 認証機能が併用されている場合の、Web 認証用のタグなしのポート VLAN 設定
 - VLAN タグ付きフレームを認証しないで透過する場合の、タグ VLAN 設定
- 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

SR-S332TR1 の場合を例にします。



● **設定条件**

- ETHER10～12ポートでIEEE802.1X認証を使用する
- ETHER10～12ポートで利用する認証データベース
 ETHER10、11ポート : RADIUSサーバ
 ETHER12ポート : ローカルで設定した認証情報
- AAAグループID
 ETHER10、11ポート : 0
 ETHER12ポート : 1
- SupplicantのMACアドレスごとに認証を行う
- ETHER12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
- ETHER10、11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

こんな事に気をつけて

- 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。

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

```
IEEE802.1X 認証を使用する
# dot1x use on

RADIUS サーバの VLAN を設定する
# lan 0 vlan 13
# lan 0 ip address 172.16.1.101/16 3

RADIUS サーバを接続するポートを設定する
# ether 1 vlan untag 13

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
# ether 2 vlan untag 10
# ether 3 vlan untag 11
# ether 4 vlan untag 100
# ether 5 vlan untag 123

IEEE802.1X 認証ポートを設定する
# ether 10 dot1x use on
# ether 10 dot1x aaa 0
# ether 11 dot1x use on
# ether 11 dot1x aaa 0
# ether 12 dot1x use on
# ether 12 dot1x aaa 1

RADIUS サーバを利用する AAA グループ情報を設定する
# aaa 0 name radiusAuth
# aaa 0 radius service client both
# aaa 0 radius auth source 172.16.1.101
# aaa 0 radius client server-info auth secret radius-secret
# aaa 0 radius client server-info auth address 172.16.1.100
# aaa 0 radius client server-info account secret radius-secret
# aaa 0 radius client server-info account 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
# aaa 1 name localAuth
# aaa 1 user 0 id Supp1
# aaa 1 user 0 password Supp1-pass
# aaa 1 user 0 supplicant vid 123
# aaa 1 user 1 id Supp2
# aaa 1 user 1 password Supp2-pass
# aaa 1 user 1 supplicant vid 100

設定終了
# save
# commit
```

12 Web 認証機能を使う

適用機種 全機種

Web 認証機能を使用すると、認証が成功した場合だけ外部のネットワークに接続するため、セキュリティを向上させることができます。

☛ 参照 マニュアル「機能説明書」

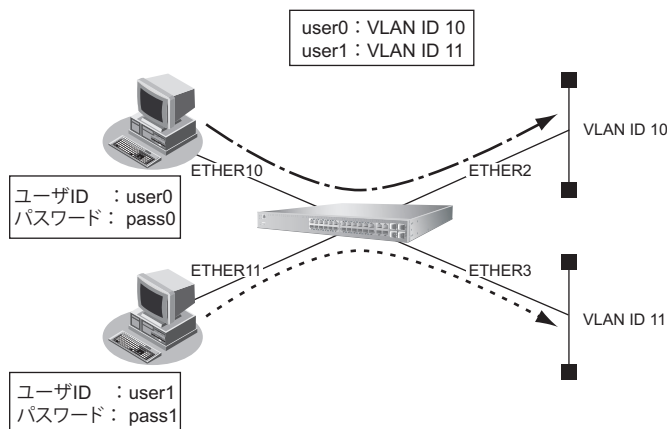
こんな事に気をつけて

- Web 認証を利用するポートでは、Web 認証機能で用いるための VLAN として、タグなしのポート VLAN だけ指定できます。タグ VLAN およびプロトコル VLAN は設定しないでください。ただし、VLAN タグ付きフレームを認証しないで透過する場合、タグ VLAN 設定はその限りではありません。
- 認証用 VLAN への経路を広報しないように経路フィルタを設定してください。
- 認証用 VLAN から外部へ IP パケットが透過しないように IP フィルタを設定してください。

12.1 AAA でローカル認証を行う

適用機種 全機種

SR-S732TR1 の場合を例にします。



● 設定条件

- ETHER10、11 ポートで Web 認証機能を用いて、AAA グループ ID は 1 を使用する
- ETHER10、11 ポートの認証方法

ETHER10 ポート	: MAC アドレス
ETHER11 ポート	: ポート
- 認証プロトコルとして MD5-CHAP を使用する
- 認証用 VLAN の VLAN ID : 500
- 認証用 VLAN の LAN0 の IP アドレス : 192.168.1.0/24
- 認証用 VLAN では DHCP で IP アドレスを割り当てる

割り当てる IP アドレス	: 192.168.1.2/24 から 100 個
リース期間	: 10 秒
DNS サーバ IP アドレス	: 192.168.1.1 (本装置の IP アドレス)

- ログイン画面のリダイレクト動作 : 有効
- ログイン画面のリダイレクト動作プロトコル : HTTPS
- 認証用VLANのLAN0で許可する通信
 - 送信元IPアドレス : 192.168.1.0/24
 - 宛先IPアドレス : 192.168.1.1/32
- VLAN ID 10が割り当てられた場合は、ETHER2ポートと通信する
- VLAN ID 11が割り当てられた場合は、ETHER3ポートと通信する
- ユーザuser0とuser1をAAAグループ1に登録する
 - user0で割り当てるVLAN ID 10
 - user1で割り当てるVLAN ID 11

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

```

IP フォワーディング機能を有効に設定する
# ip routing enable

Web 認証機能を使用する
# webauth use on

認証プロトコルとして MD5-CHAP を使用する
# webauth type chap_md5

認証用 VLAN の VID に 500 を設定する
# lan 0 vlan 500

DHCP サーバ機能を設定する
# lan 0 ip address 192.168.1.1/24 3
# lan 0 ip dhcp service server
# lan 0 ip dhcp info dns 192.168.1.1
# lan 0 ip dhcp info address 192.168.1.2/24 100
# lan 0 ip dhcp info time 10s

認証ログイン画面のリダイレクト動作を設定する
# lan 0 ip webauth redirect enable

認証ログイン画面のリダイレクト動作プロトコルを設定する
# webauth protocol https

IP フィルタリング機能を設定する
# acl 0 ip 192.168.1.0/24 192.168.1.1/32 any
# lan 0 ip filter 0 pass acl 0
# acl 1 ip any 255.255.255.255/32 any
# lan 0 ip filter 1 pass acl 1
# acl 2 ip any any any
# lan 0 ip filter 2 reject acl 2

ETHER10、11 ポートでは STP を使用しない
# ether 10 stp use off
# ether 11 stp use off

ETHER10、11 ポートで Web 認証機能を使用する
# ether 10 vlan untag 500
# ether 10 webauth use on
# ether 10 webauth aaa 1
# ether 11 vlan untag 500
# ether 11 webauth use on
  
```

```
# ether 11 webauth aaa 1
# ether 11 webauth mode port
```

Web 認証後、VLAN ID が割り当てられたときに ETHER ポートと通信する

```
# ether 2 vlan untag 10
# ether 3 vlan untag 11
```

LAN1 を VLAN ID 100 に割り当てる

```
# lan 1 vlan 100
# lan 1 ip address 172.16.1.102/24 3
```

外部と通信する LAN1 では RIP を使用してダイナミックルーティングを行う

```
# lan 1 ip rip use v2m v2 0 off
```

RIP を使用するインタフェースでは認証用 VLAN の 192.168.1.0/24 に対する経路を配布しない

```
# rip ip redistrib 0 reject 192.168.1.0/24 exact
# rip ip redistrib 1 pass any
```

AAA 情報を設定する

```
# aaa 1 name home
# aaa 1 user 0 id user0
# aaa 1 user 0 password pass0
# aaa 1 user 0 supplicant vid 10
# aaa 1 user 1 id user1
# aaa 1 user 1 password pass1
# aaa 1 user 1 supplicant vid 11
```

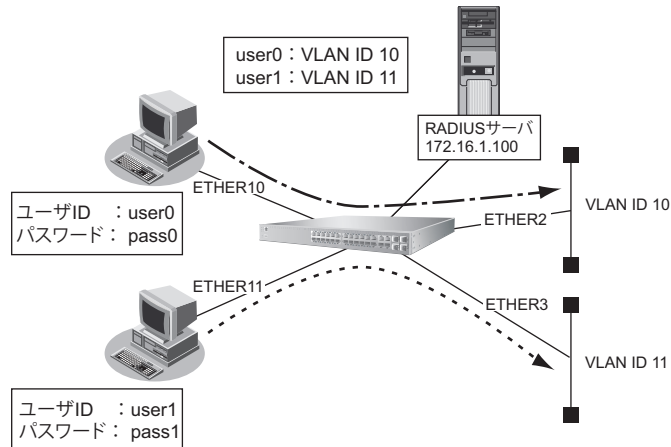
設定終了

```
# save
# reset
```


12.2 AAAでリモート認証を行う

適用機種 全機種

SR-S732TR1 の場合を例にします。



● 設定条件

- ETHER10、11 ポートで Web 認証機能を用いて、AAA グループ ID は 1 を使用する
- ETHER10、11 ポートの認証方法

ETHER10 ポート	: MAC アドレス
ETHER11 ポート	: ポート
- RADIUS サーバの IP アドレス : 172.16.1.100
- 認証プロトコルとして MD5-CHAP を使用する
- 認証用 VLAN の LAN0 の IP アドレス : 192.168.1.0/24
- 認証用 VLAN では DHCP で IP アドレスを割り当てる

割り当てる IP アドレス	: 192.168.1.2/24 から 100 個
リース期間	: 10 秒
DNS サーバ IP アドレス	: 192.168.1.1 (本装置の IP アドレス)
- ログイン画面のリダイレクト動作 : 有効
- ログイン画面のリダイレクト動作プロトコル : HTTPS
- 認証用 VLAN の LAN0 で許可する通信

送信元 IP アドレス	: 192.168.1.0/24
あて先 IP アドレス	: 192.168.1.1/32
- 認証成功後にリダイレクトする URL : <http://jp.fujitsu.com/>
- 認証成功後にリダイレクトする時間 : 15 秒

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

IP フォワーディング機能を有効に設定する
ip routing enable

Web 認証機能を使用する
webauth use on

認証プロトコルとして MD5-CHAP を使用する
webauth type chap_md5

認証用 VLAN の VID に 500 を設定する
lan 0 vlan 500

DHCP サーバ機能を設定する
lan 0 ip address 192.168.1.1/24 3
lan 0 ip dhcp service server
lan 0 ip dhcp info dns 192.168.1.1
lan 0 ip dhcp info address 192.168.1.2/24 100
lan 0 ip dhcp info time 10s

認証ログイン画面のリダイレクト動作を設定する
lan 0 ip webauth redirect enable

認証ログイン画面のリダイレクト動作プロトコルを設定する
webauth protocol https

認証成功後にリダイレクトさせる URL を設定する
webauth success redirect url http://jp.fujitsu.com/

認証成功後にリダイレクトする時間を設定する
webauth success redirect time 15s

IP フィルタリング機能を設定する
acl 0 ip 192.168.1.0/24 192.168.1.1/32 any
lan 0 ip filter 0 pass acl 0
acl 1 ip 0.0.0.0/32 255.255.255.255/32 any
lan 0 ip filter 1 pass acl 1
acl 2 ip any any any
lan 0 ip filter 2 reject acl 2

ETHER10、11 ポートでは STP を使用しない
ether 10 stp use off
ether 11 stp use off

ETHER10、11 ポートで Web 認証機能を使用する
ether 10 vlan untag 500
ether 10 webauth use on
ether 10 webauth aaa 1
ether 11 vlan untag 500
ether 11 webauth use on
ether 11 webauth aaa 1
ether 11 webauth mode port

Web 認証後、VLAN ID が割り当てられたときに ETHER ポートと通信する
ether 2 vlan untag 10
ether 3 vlan untag 11

LAN1 を VLAN ID 100 に割り当てる

```
# lan 1 vlan 100
```

```
# lan 1 ip address 172.16.1.102/24 3
```

外部と通信する LAN1 では RIP を使用してダイナミックルーティングを行う

```
# lan 1 ip rip use v2m v2 0 off
```

RIP を使用するインターフェースでは認証用 VLAN の 192.168.1.0/24 に対する経路を配布しない

```
# rip ip redistrib 0 reject 192.168.1.0/24 exact
```

```
# rip ip redistrib 1 pass any
```

AAA 情報を設定する

```
# aaa 1 name home
```

```
# aaa 1 radius service client both
```

```
# aaa 1 radius client server-info auth secret test
```

```
# aaa 1 radius client server-info auth address 172.16.1.100
```

設定終了

```
# save
```

```
# reset
```

12.3 認証ログイン画面のカスタマイズを行う

適用機種 全機種

こんな事に気をつけて

- カスタマイズされた画面は装置起動時にダウンロードされます。また webauthctl コマンドにて運用中に更新することも可能です。
- カスタマイズする画面ファイルは以下の弊社ホームページよりサンプルファイルを取得し利用ください。

☛ 参照 URL: <https://www.fujitsu.com/jp/products/network/download/sr-s/firm/>

● 設定条件

- カスタマイズ認証ログイン画面の取得先 : FTP サーバ
- FTP サーバの IP アドレス : 172.16.1.100
- FTP サーバのユーザ ID : user-id
- FTP サーバのユーザパスワード : user-pass
- カスタマイズするログイン画面ファイル : /webauth/login.html
- カスタマイズするロゴ画像ファイル : /webauth/logo.gif

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。



ここでは認証動作の設定は省略します。

認証動作の設定については、「12.1AAA でローカル認証を行う」(P.46)、「12.2AAA でリモート認証を行う」(P.49)を参照してください。

● コマンド

```
認証ログイン画面のカスタマイズファイル取得先の設定
# webauth customize mode ftp
```

```
FTP サーバの設定
# webauth customize server address 172.16.1.100
# webauth customize server user user-id
# webauth customize server password user-pass
```

```
カスタマイズファイルの設定
# webauth customize page /webauth/login.html
# webauth customize logo /webauth/logo.gif
```

```
設定終了
# save
# reset
```

13 MAC アドレス認証機能を使う

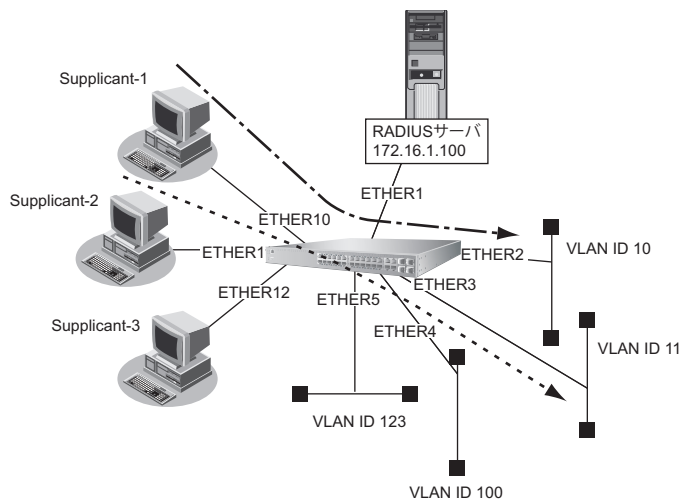
適用機種 全機種

MAC アドレス認証機能を使用すると、本装置に接続する端末がネットワークへのアクセス権を持っているかを認証することができます。

こんな事に気をつけて

- MAC アドレス認証を利用するポートでは、事前に VLAN を設定できません。ただし、以下の場合はその限りではありません。
 - Web 認証機能が併用されている場合の、Web 認証用のタグなしのポート VLAN 設定
 - VLAN タグ付きフレームを認証しないで透過する場合の、タグ VLAN 設定
- MAC アドレス認証で利用する AAA のグループ ID を正しく設定してください。

SR-S332TR1 の場合を例にします。



● 設定条件

- ETHER10～12 ポートで MAC アドレス認証を使用する
- ETHER10～12 ポートで利用する認証データベース
 - ETHER10、11 ポート : RADIUS サーバ
 - ETHER12 ポート : ローカルで設定した認証情報
- AAA グループ ID
 - ETHER10、11 ポート : 0
 - ETHER12 ポート : 1
- Supplicant の MAC アドレスごとに認証を行う
- ETHER12 ポートで利用可能なユーザは以下のとおり

MAC アドレス	割り当てる VLAN ID
00:11:11:00:00:01	VLAN123
00:22:22:00:00:02	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
- 認証プロトコルとして MD5-CHAP を使用する

こんな事に気をつけて

- 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。

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

```

MACアドレス認証を使用する
# macauth use on

MACアドレス認証で使用するパスワードを設定する
# macauth password macauth-pass

認証プロトコルとしてMD5-CHAPを使用する
# macauth type chap_md5

RADIUSサーバのVLANを設定する
# lan 0 vlan 13
# lan 0 ip address 172.16.1.101/16 3

RADIUSサーバを接続するポートを設定する
# ether 1 vlan untag 13

MACアドレス認証により認証されたSupplicantが接続されるVLAN情報を設定する
# ether 2 vlan untag 10
# ether 3 vlan untag 11
# ether 4 vlan untag 100
# ether 5 vlan untag 123

MACアドレス認証ポートを設定する
# ether 10 macauth use on
# ether 10 macauth aaa 0
# ether 11 macauth use on
# ether 11 macauth aaa 0
# ether 12 macauth use on
# ether 12 macauth aaa 1

RADIUSサーバを利用するAAAグループ情報を設定する
# aaa 0 name radiusAuth
# aaa 0 radius service client auth
# aaa 0 radius auth source 172.16.1.101
# aaa 0 radius client server-info auth secret radius-secret
# aaa 0 radius client server-info auth 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

```
# aaa 1 name localAuth
# aaa 1 user 0 id 001111000001
# aaa 1 user 0 password macauth-pass
# aaa 1 user 0 supplicant vid 123
# aaa 1 user 1 id 002222000002
# aaa 1 user 1 password macauth-pass
# aaa 1 user 1 supplicant vid 100
```

設定終了

```
# save
# commit
```

14 接続端末数制限機能を使う

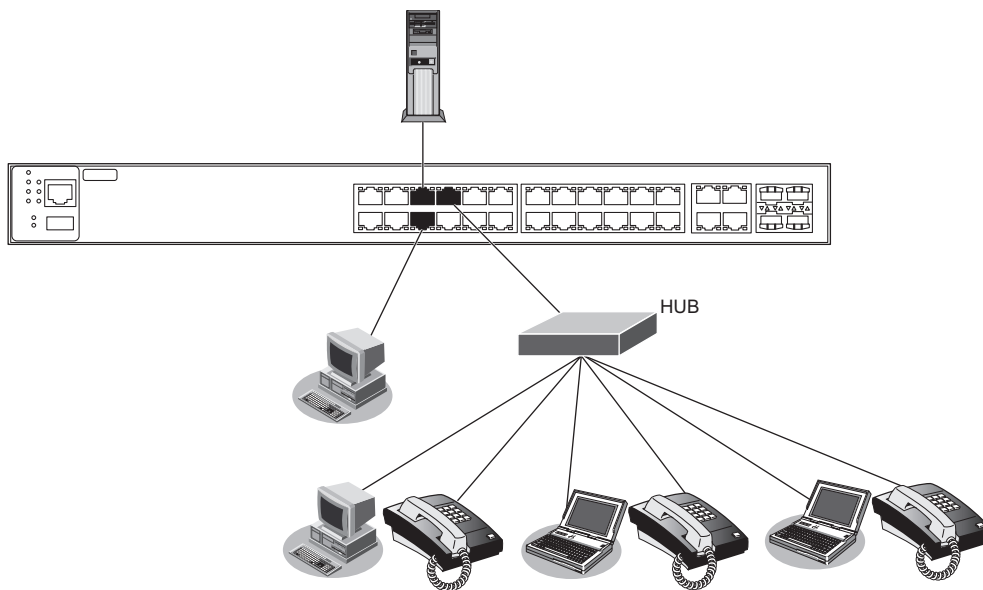
適用機種 全機種

接続端末数制限機能を使用すると、簡易的に本装置への不正接続を検出することができます。

こんな事に気をつけて

- 本機能は、不正接続を検出する機能であり、不正接続とみなした端末に対する通信の遮断は行いません。不正な接続を検出した際に通信を遮断したい場合はポート閉塞モードを有効にしてください。
- IEEE802.1X 認証、Web 認証および MAC アドレス認証のどれかを有効にしたポートでは、本機能は無効となります。
- リンクアグリゲーションとして設定されたポートでは、本機能は無効となります。
- 閉塞されたポートは自動では復旧しません。online ether コマンドで復旧させてください。

SR-S332TR1 の場合を例にします。



● 設定条件

- ETHER5～7 ポートで接続端末数制限機能を使用する
- 接続許容端末数

ETHER5、6 ポート	: 1
ETHER7 ポート	: 6
- ポート閉塞モード

ETHER5、6 ポート	: 閉塞する
ETHER7 ポート	: 閉塞しない

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

接続端末数制限機能を使用する
ether 5-7 mac detection use on

接続許容最大数を設定する
ether 7 mac detection max_user 6

ポート閉塞モードを設定する
ether 5-6 mac detection portdisable yes

設定終了
save
commit

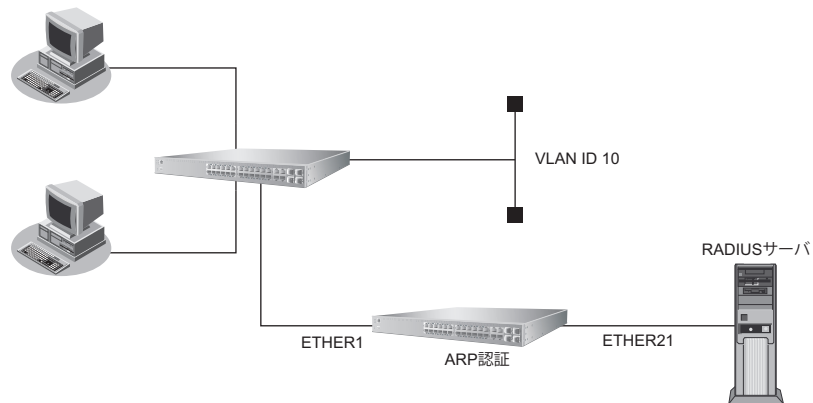
15 ARP 認証機能を使う

適用機種 全機種

ここでは、既存のネットワークに本装置を追加して、ARP 認証を行う場合の設定方法を説明します。

こんな事に気をつけて

ARP 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。



SR-S332TR1 の場合を例にします。

● 設定条件

- VLAN10 で ARP 認証を使用する
- ARP 認証で利用する認証データベース : RADIUS サーバ
- AAA グループの ID : 0
- RADIUS サーバの IP アドレス : 172.16.1.100
- RADIUS サーバは VLAN20 に接続されている
- RADIUS サーバのシークレット : radius-secret
- 認証失敗時の通信妨害を行う
- 通信妨害のための ARP パケット送信間隔 : 10 秒

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

```
RADIUS サーバの VLAN を設定する
# lan 0 vlan 20
# lan 0 ip address 172.16.1.200/16 3

メディア種別を設定する
# ether 21 media metal

RADIUS サーバを接続するポートを設定する
# ether 21 vlan untag 20

ARP 認証が動作する VLAN を設定する
# ether 1 vlan untag 10
```

ARP 認証を設定する

```
# vlan 10 arpauth use on
# vlan 10 arpauth aaa 0
# vlan 10 arpauth obstruction enable 10s
```

RADIUS サーバを利用する AAA グループ情報を設定する

```
# aaa 0 name RADIUS
# aaa 0 radius service client auth
# aaa 0 radius auth source 172.16.1.200
# aaa 0 radius client server-info auth 0 secret radius-secret
# aaa 0 radius client server-info auth 0 address 172.16.1.100
```

設定終了

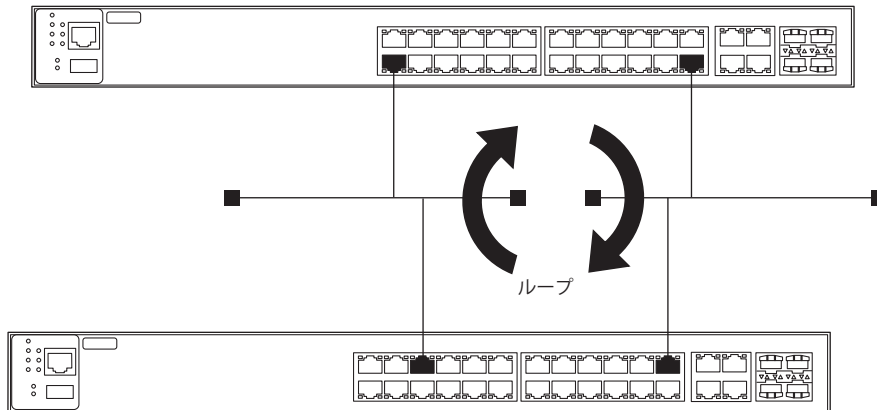
```
# save
# commit
```

16 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

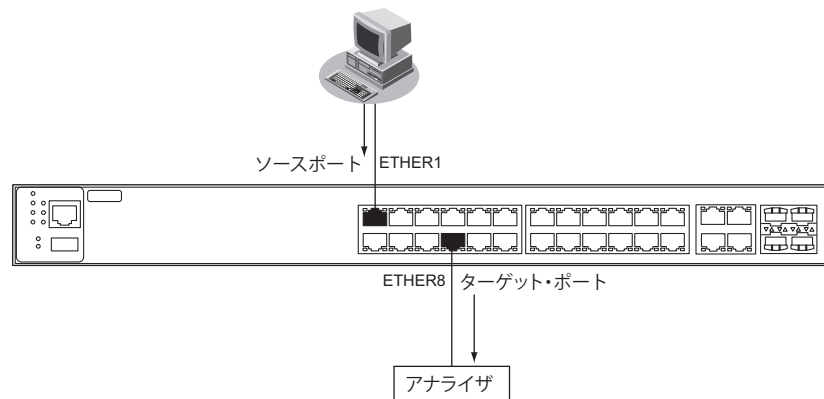
- 閉塞されたポートは自動では復旧しません。online ether コマンドで復旧させてください。
- トラフィックが高負荷状態になった場合、ループを検出することができません。ブロードキャスト/マルチキャスト ストーム制御を併用してください。
- STP 機能が有効なポートでは、ループ検出時にポートを論理的に遮断する指定はできません。

17 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／送信／送受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
```


[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
```

18.1 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。

SR-S332TR1 の場合を例にします。

● 設定条件

- ETHER1～4 ポートを使用する
- 通信速度を 1000Mbps 固定に変更する
- 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 mode 1000
# 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 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 mode 1000
# 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 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
```


19 ポート閉塞機能を使う

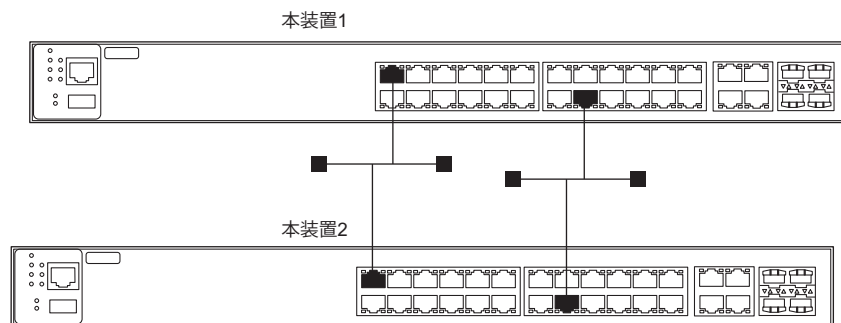
適用機種 全機種

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 ether 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ETHER1、16ポートをバックアップポートとして使用する
(ETHER1をマスタポート、ETHER16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ETHER1、16ポートをバックアップポートとして使用する
(ETHER1をマスタポート、ETHER16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]**

```
ETHER1ポートでリンクダウン回数の上限値を設定する
# ether 1 recovery limit 5

ETHER1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 1 type backup 1 master

ETHER16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 16 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]

```
ETHER1ポートでリンクダウン回数の上限値を設定する
# ether 1 recovery limit 5

ETHER1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 1 type backup 1 master

ETHER16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 16 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
```

20 LANをネットワーク間接続する

適用機種 SR-S732TR1, 752TR1

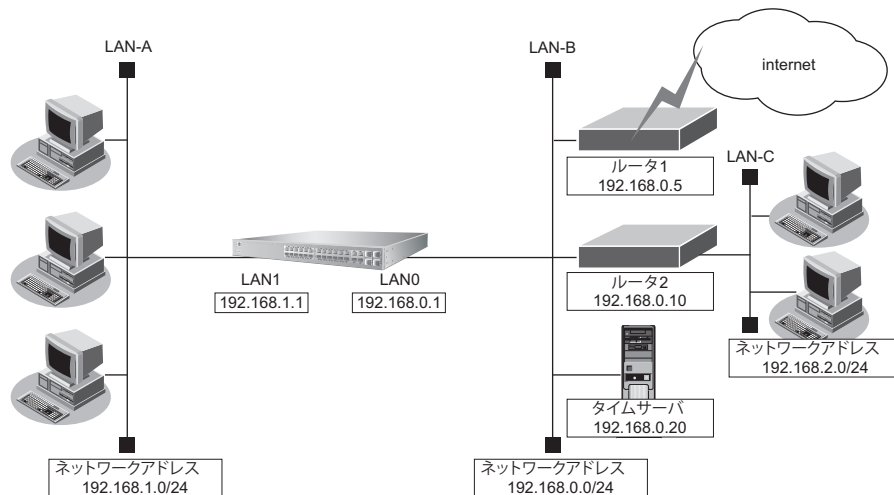
ここでは、既存のLAN-Bに新規のLAN-Aをネットワーク間接続し、静的に経路情報を設定する場合を例に説明します。

こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかつたり手順どおり設定しても通信できないことがあります。

☞ 参照 マニュアル「トラブルシューティング」

SR-S732TR1の場合を例にします。



● 設定条件

【LAN-A側】

- ・ 転送レートは自動認識
- ・ VLANはタグなし
- ・ 本装置のLAN1側のIPアドレス : 192.168.1.1
- ・ ネットワークアドレス/ネットマスク : 192.168.1.0/24
- ・ DHCP機能を使用する

【LAN-B側】

- ・ 転送レートは自動認識
- ・ VLANはタグなし
- ・ 本装置のLAN0側のIPアドレス : 192.168.0.1
- ・ ネットワークアドレス/ネットマスク : 192.168.0.0/24
- ・ DHCP機能を使用しない
- ・ ルーティングプロトコルとしてRIP-V1を使用する
- ・ インターネットにつながるルータ1と、事業所内のその他のネットワークにつながるルータ2が存在し、静的に経路情報を登録する
 - ルータ1のIPアドレス : 192.168.0.5
 - ルータ2のIPアドレス : 192.168.0.10
- ・ LAN-Cのネットワークアドレス/ネットマスク : 192.168.2.0/24

[その他の条件]

- 自動時刻設定にする

タイムサーバ	: 使用する
サーバ設定	: 設定する
プロトコル	: TIME プロトコル
タイムサーバのアドレス	: 192.168.0.20

ヒント

◆ TIME プロトコル、SNTP とは？

TIME プロトコル (RFC868) はネットワーク上で時刻情報を配布するプロトコルです。SNTP (Simple Network Time Protocol、RFC1361、RFC1769) は NTP (Network Time Protocol) のサブセットで、パソコンなど末端のクライアントマシンの時刻を同期させるのに適しています。

こんな事に気をつけて

本装置の IP アドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。

● コマンド

IP フォワーディング機能を有効に設定する

```
# ip routing enable
```

VLAN を設定する

```
# ether 1 vlan untag 10
```

```
# ether 2 vlan untag 20
```

```
# lan 0 vlan 10
```

```
# lan 1 vlan 20
```

LAN0 情報を設定する

```
# lan 0 ip address 192.168.0.1/24 3
```

```
# lan 0 ip dhcp service off
```

```
# lan 0 ip route 0 192.168.2.0/24 192.168.0.10 1 1
```

```
# lan 0 ip route 1 default 192.168.0.5 1 1
```

```
# lan 0 ip rip use v1 v1 0 off
```

LAN1 情報を設定する

```
# lan 1 ip address 192.168.1.1/24 3
```

```
# lan 1 ip dhcp service server
```

```
# lan 1 ip dhcp info dns 192.168.1.1
```

```
# lan 1 ip dhcp info address 192.168.1.2/24 253
```

```
# lan 1 ip dhcp info time 1d
```

```
# lan 1 ip dhcp info gateway 192.168.1.1
```

自動時刻を設定する

```
# time auto server 0 address 192.168.0.20 time
```

```
# time auto interval start
```

設定終了

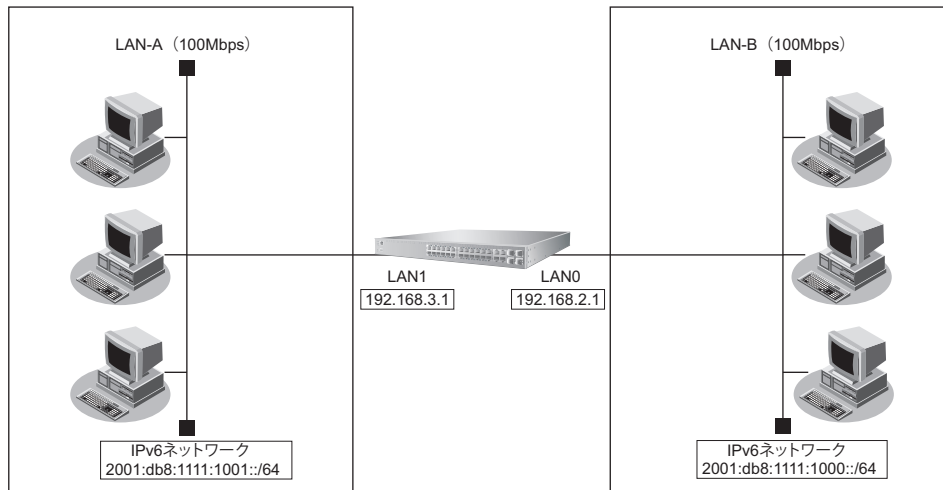
```
# save
```

```
# reset
```

21 IPv4のネットワークにIPv6ネットワークを追加する

適用機種 SR-S732TR1, 752TR1

ここでは、IPv4で通信しているネットワーク環境にIPv6ルーティング設定を追加する例について説明します。



● 設定条件

[LAN-A側]

- プレフィックス/プレフィックス長 : 2001:db8:1111:1001::/64
- RA送信を行う
- VLANはタグなし

[LAN-B側]

- プレフィックス/プレフィックス長 : 2001:db8:1111:1000::/64
- RA送信を行う
- VLANはタグなし

こんな事に気をつけて

- IPv4のネットワークをすでに使用している場合の設定例です。新規にIPv6だけのネットワーク構成を設定する場合は、etherポートへのVLAN設定などが必要になります。
- IPv6フォワーディング機能有効時は、装置リセットが必要となります。

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

IPv6 フォワーディング機能を有効に設定する
ip6 routing enable

LAN0 情報を設定する
lan 0 ip6 use on
lan 0 ip6 address 0 2001:db8:1111:1000::/64
lan 0 ip6 ra prefix 0 2001:db8:1111:1000::/64 30d 7d c0
lan 0 ip6 ra mode send

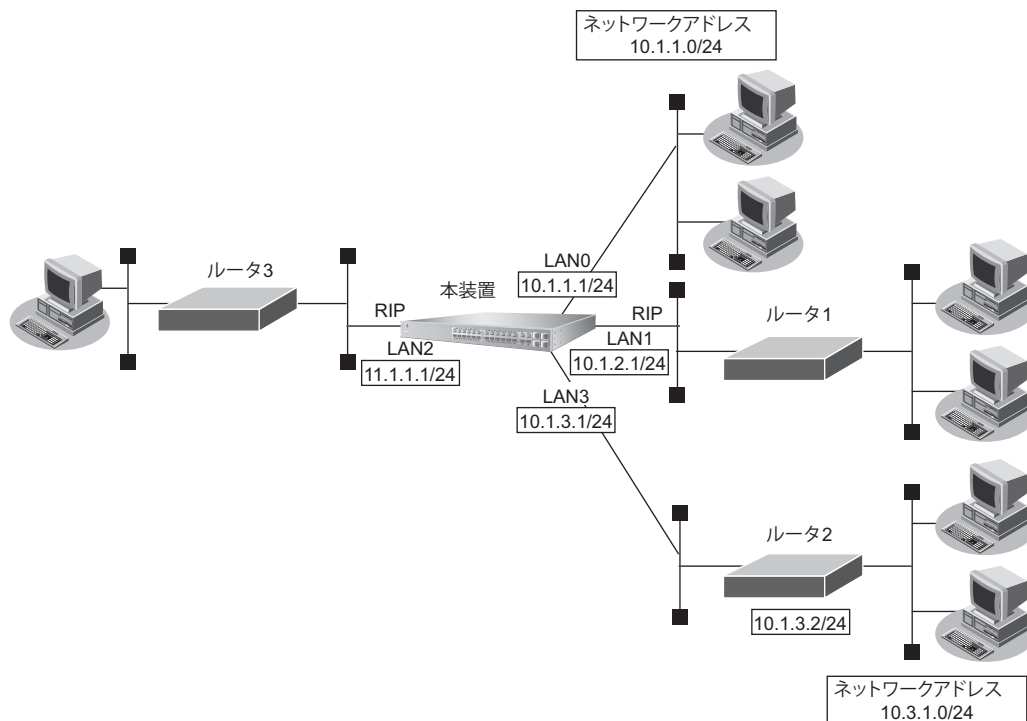
LAN1 情報を設定する
lan 1 ip6 use on
lan 1 ip6 address 0 2001:db8:1111:1001::/64
lan 1 ip6 ra prefix 0 2001:db8:1111:1001::/64 30d 7d c0
lan 1 ip6 ra mode send

設定終了
save
reset

22 RIP を使用したネットワークを構築する (IPv4)

適用機種 SR-S732TR1, 752TR1

ここでは、RIPv2 を使用したダイナミックルーティングのネットワーク設定について説明します。



● 前提条件

- すべてのインタフェースに IP アドレスの設定がされている
- IP フォワーディング機能を使用する設定がされている

● 設定条件

- LAN0 のネットワークは、RIP ネットワークに広報する
- LAN1 で RIPv2 を使用する
- LAN2 で RIPv2 を使用する
- LAN3 でルータ 2 を経由するネットワークはスタティック経路で設定し、このスタティック経路を RIP ネットワークに広報する

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。

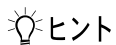
● コマンド

```
RIP基本情報を設定する
# lan 1 ip rip use v2m v2 0 off
# lan 2 ip rip use v2m v2 0 off

ルータ2を経由する経路をスタティック経路で設定する
# lan 3 ip route 0 10.3.1.0/24 10.1.3.2 1 1

RIPへの再配布経路を設定する
# routemanage ip redistrib rip connected on
# routemanage ip redistrib rip static on

設定完了
# save
# commit
```



◆ RIPユニキャスト送信

RIPの経路広報は通常マルチキャスト/ブロードキャストパケットを使用して行われますが、ユニキャストフレームを使用して広報することができます。

ユニキャスト送信は、以下のコマンドで設定します。

- ユニキャスト送信の設定 : rip ip neighbor
- RIP基本情報の設定 : lan ip rip use

ユニキャスト送信先に対して、加算メトリック、認証機能およびRIP機能を使用する場合は、送信先ネットワークが属するインタフェースの設定を行います。

◆ RIPマルチパス機能

RIPを利用した冗長ネットワークで通信経路に障害が発生した場合は、ルーティングテーブルから障害経路が削除されても、新しい経路情報をRIP定期広報などで受信するまでは経路が切り替わりません。そこで、マルチパス機能を利用し、バックアップ経路として冗長な経路を1つ保持することで、障害経路が削除された直後に経路を切り替えることができます。

マルチパス機能は、以下のコマンドで設定します。

- RIPマルチパスの設定 : rip ip multipath

こんな事に気をつけて

- 本装置の初期設定では、インタフェース経路とスタティック経路をRIPに再配布する設定となっています。再配布が不要な場合は、再配布しない設定を行ってください。
- メトリック値が同じ冗長経路を受信した場合、先に受信したRIP経路を優先経路として扱います。ECMPとしては動作しません。
- 複数のインタフェースでRIPを利用する場合、以下の条件式の範囲で広報RIPパケット数を設計してください。
 条件式 : 広報RIPパケット数×RIP利用インタフェース数 ≤ 243
 広報RIPパケット数は、広報RIP経路数を25で割り、小数点以下を切り上げた値です。広報RIP経路数は、経路フィルタにより減らすことができます。「広報RIPパケット数×RIP利用インタフェース数」の値は、本装置が集中して受信するRIPパケット数であり、この値が243に近ければRIP受信パケットの破棄など通信に影響が出る場合があります。このため、243よりも十分小さくなるように設計してください。
 なお、破棄されたパケット数は、統計情報表示 (show ip traffic udp) の統計値「dropped due to full socket buffers」で確認できます。

23 RIPの経路を制御する (IPv4)

適用機種 SR-S732TR1, 752TR1

本装置を経由して、ほかのルータに送受信する経路情報に対して、IPアドレスや方向を組み合わせで指定することによって、特定のあて先への経路情報だけを広報する、または不要な経路情報を遮断することができます。

経路情報のフィルタリング条件

対象となる経路情報

- RIPによる経路情報

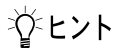
指定条件

本装置では、以下の条件を指定することによって、経路情報を制御することができます。

- 動作
- 方向
- フィルタリング条件 (IPアドレス/アドレスマスク)
- メトリック値



メトリック値は指定メトリック値の経路情報をフィルタリングするのではなく、フィルタリング後の経路情報のメトリック値を変更する場合に指定します。0を指定すると変更は行いません。経路情報のフィルタリング条件にany以外を指定した場合に有効です。送信方向のメトリック値に1～16を指定した場合、インタフェースに設定したRIPの加算メトリック値は加算されません。



◆ 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。制御対象となる経路情報は、経路情報のIPアドレスとアドレスマスクが指定したIPアドレスとアドレスマスクと一致したもののだけです。

例) 指定値 : 172.21.0.0/16の場合
 経路情報 : 172.21.0.0/16は制御対象となる
 172.21.0.0/24は制御対象とならない

また、フィルタリング条件のIPアドレスと指定したIPアドレスが、指定したアドレスマスクまで一致した場合に制御対象とすることもできます。

指定値 : 172.21.0.0/16の場合
 経路情報 : 172.21.0.0/24は制御対象となる
 172.21.10.0/24は制御対象となる

こんな事に気をつけて

RIPv1を使用している場合もアドレスマスクの設定が必要です。この場合、インタフェースのアドレスマスクを指定してください。また、アドレスクラスが異なる経路情報を制御する場合は、ナチュラルマスク値を指定してください。

例) `lan 0 ip address 192.168.1.1/24`に10.0.0.0の経路情報を制御する場合は、10.0.0.0/8を指定します。

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. 特定の条件の経路情報だけを透過させ、その他はすべて遮断する
- B. 特定の条件の経路情報だけを遮断し、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。

- 特定の経路情報の送信を許可する
- 特定の経路情報のメトリック値を変更して送信する
- 特定の経路情報の受信を許可する
- 特定の経路情報のメトリック値を変更して受信する

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。

- 特定の経路情報の送信を禁止する
- 特定の経路情報の受信を禁止する

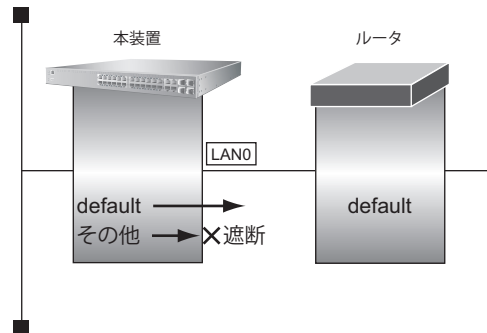
こんな事に気をつけて

- フィルタリング条件には、優先度を示す定義番号があり、小さいほど、より高い優先度を示します。
 - RIP 受信時には、優先順位の高い定義から順に受信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。一致した以降の条件は参照されません。また、受信方向のすべての条件に一致しないRIP 経路情報は遮断されます。
 - RIP 送信時には、優先順位の高い定義から順に送信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。一致した以降の条件は参照されません。また、送信方向のすべての条件に一致しないRIP 経路情報は遮断されます。
-

23.1 特定の経路情報の送信を許可する

適用機種 SR-S732TR1, 752TR1

ここでは、本装置からルータへのデフォルトルートの送信だけを許可し、それ以外の経路情報の送信を禁止する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースにIPアドレスとRIPv2を使用する設定がされている
- IPフォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置からルータへのデフォルトルートの送信だけを許可
- その他はすべて遮断

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● コマンド

```

デフォルトルートを透過させる
# lan 0 ip rip filter 0 act pass out
# lan 0 ip rip filter 0 route default

その他の経路情報はすべて遮断する
# lan 0 ip rip filter 1 act reject out
# lan 0 ip rip filter 1 route any

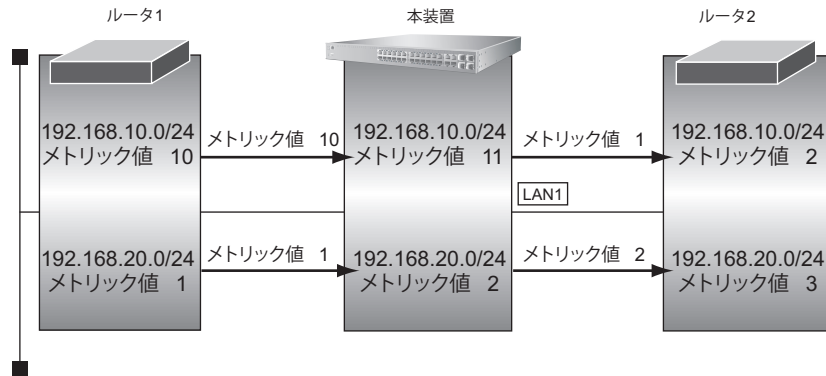
設定終了
# save
# commit
    
```

23.2 特定の経路情報のメトリック値を変更して送信する

適用機種 SR-S732TR1, 752TR1

ここでは、本装置がルータ2へ 192.168.10.0/24、メトリック値 1 の経路情報を送信する場合の設定方法を説明します。

なお、本装置は、ルータ1から 192.168.10.0/24 のメトリック値 10 と 192.168.20.0/24 のメトリック値 1 の経路情報を受信するものとします。



● 前提条件

- すべてのインタフェースに IP アドレスと RIPv2 を使用する設定がされている
- IP フォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置から 192.168.10.0/24 の送信を許可する場合、メトリック値 1 に変更
- 192.168.10.0/24 以外の経路情報は、メトリック値を変更しない

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● コマンド

```
192.168.10.0/24 をメトリック値 1 で送信する
# lan 1 ip rip filter 0 act pass out
# lan 1 ip rip filter 0 route 192.168.10.0/24
# lan 1 ip rip filter 0 set metric 1
```

```
その他の経路情報はメトリック値を変更しないで送信する
残りの経路情報は、すべて送信する
# lan 1 ip rip filter 1 act pass out
# lan 1 ip rip filter 1 route any
```

```
設定終了
# save
# commit
```

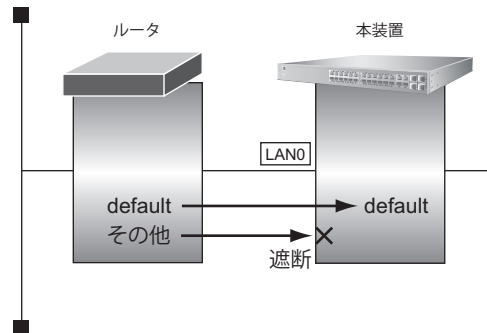
こんな事に気をつけて

- 送信方向でメトリック値が設定されている場合、インタフェースのRIP加算メトリック値の加算は行われません。
- 送信方向でメトリック値が設定されていても、メトリック値 16 の経路情報のメトリック値は変更されません。

23.3 特定の経路情報の受信を許可する

適用機種 SR-S732TR1, 752TR1

ここでは、本装置はルータからデフォルトルートの受信だけを許可し、それ以外の経路情報の受信を禁止する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースにIPアドレスとRIPv2を使用する設定がされている
- IPフォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置はデフォルトルートの受信だけを許可
- その他はすべて遮断

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● コマンド

```
デフォルトルートを透過させる
# lan 0 ip rip filter 0 act pass in
# lan 0 ip rip filter 0 route default
```

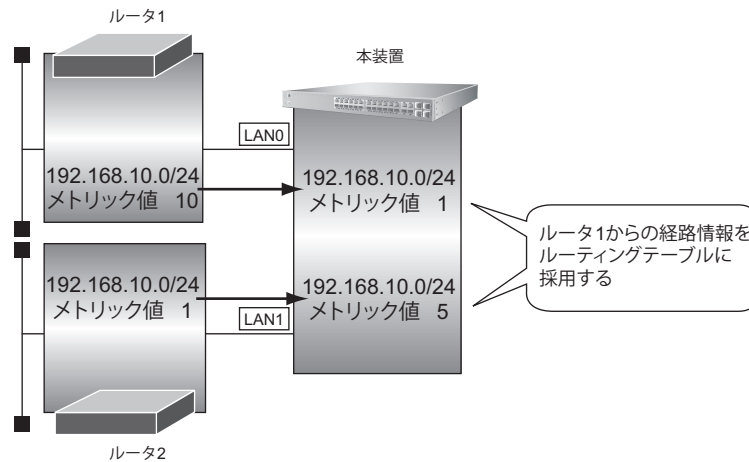
```
その他の経路情報はすべて遮断する
# lan 0 ip rip filter 1 act reject in
# lan 0 ip rip filter 1 route any
```

```
設定終了
# save
# commit
```

23.4 特定の経路情報のメトリック値を変更して受信する

適用機種 SR-S732TR1, 752TR1

ここでは、本装置が、ルータ1とルータ2から同じ先への経路情報 192.168.10.0/24 を受信した場合に、ルータ1から受信した経路情報を採用する場合の設定方法を説明します。



● 前提条件

- すべてのインターフェースにIPアドレスとRIPv2を使用する設定がされている
- IPフォワーディング機能を使用する設定がされている

● フィルタリング設計

- ルータ1から、192.168.10.0/24の経路情報を受信した場合、メトリック値1に変更
- ルータ2から、192.168.10.0/24の経路情報を受信した場合、メトリック値5に変更
- 上記以外の経路情報は、メトリック値を変更しない

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● コマンド

```
LAN0から192.168.10.0/24を受信した場合、メトリック値1で受信する
# lan 0 ip rip filter 0 act pass in
# lan 0 ip rip filter 0 route 192.168.10.0/24
# lan 0 ip rip filter 0 set metric 1

LAN0からのその他の経路情報はすべて受信する
# lan 0 ip rip filter 1 act pass in
# lan 0 ip rip filter 1 route any

lan1から192.168.10.0/24を受信した場合、メトリック値5で受信する
# lan 1 ip rip filter 0 act pass in
# lan 1 ip rip filter 0 route 192.168.10.0/24
# lan 1 ip rip filter 0 set metric 5

lan1からのその他の経路情報はすべて受信する
# lan 1 ip rip filter 1 act pass in
# lan 1 ip rip filter 1 route any

設定終了
# save
# commit
```

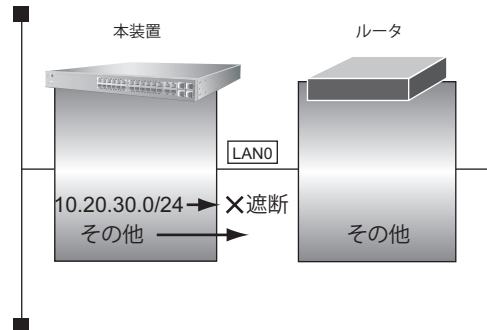
こんな事に気をつけて

受信方向でメトリック値が設定されていても、メトリック値16の経路情報のメトリック値は変更されません。

23.5 特定の経路情報の送信を禁止する

適用機種 SR-S732TR1, 752TR1

ここでは、本装置からルータへの 10.20.30.0/24 の送信を禁止し、それ以外の経路情報の送信を許可する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースにIPアドレスとRIPv2を使用する設定がされている
- IPフォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置からルータへの 10.20.30.0/24 の送信を禁止
- その他はすべて透過

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● コマンド

```

10.20.30.0/24 を遮断する
# lan 0 ip rip filter 0 act reject out
# lan 0 ip rip filter 0 route 10.20.30.0/24

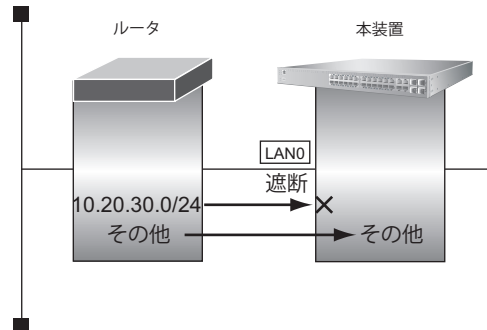
その他の経路情報はすべて透過させる
# lan 0 ip rip filter 1 act pass out
# lan 0 ip rip filter 1 route any

設定終了
# save
# commit
    
```

23.6 特定の経路情報の受信を禁止する

適用機種 SR-S732TR1, 752TR1

ここでは、本装置は、ルータから 10.20.30.0/24 の経路情報の受信を禁止し、それ以外の経路情報の受信を許可する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースにIPアドレスとRIPv2を使用する設定がされている
- IPフォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置は 10.20.30.0/24 の受信を禁止
- その他はすべて透過

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● コマンド

```
10.20.30.0/24 を遮断する
# lan 0 ip rip filter 0 act reject in
# lan 0 ip rip filter 0 route 10.20.30.0/24

その他の経路情報はすべて透過させる
# lan 0 ip rip filter 1 act pass in
# lan 0 ip rip filter 1 route any

設定終了
# save
# commit
```


24 RIP の経路を制御する (IPv6)

適用機種 SR-S732TR1, 752TR1

本装置を経由して、ほかのルータに送信する経路情報や、ほかのルータから受信する経路情報に対して、経路情報や方向を組み合わせて指定することによって、特定のあて先への経路情報だけを広報する、または、不要な経路情報を遮断することができます。

経路情報のフィルタリング条件

対象となる経路情報

- RIPによる経路情報 (IPv6)

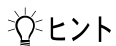
指定条件

本装置では、以下の条件を指定することによって、経路情報を制御することができます。

- 動作
- 方向
- フィルタリング条件 (プレフィックス/プレフィックス長)
- メトリック値



メトリック値は指定メトリック値の経路情報をフィルタリングするのではなく、フィルタリング後の経路情報のメトリック値を変更する場合に指定します。0を指定すると変更は行いません。経路情報のフィルタリング条件にany以外を指定した場合に有効です。送信方向のメトリック値に1～16を指定した場合、インタフェースに設定したRIPの加算メトリック値は加算されません。



◆ プレフィックスとプレフィックス長の決め方

フィルタリング条件の要素には、「プレフィックス」と「プレフィックス長」があります。制御対象となる経路情報は、経路情報のプレフィックスとプレフィックス長が指定したプレフィックスとプレフィックス長と一致したものです。

例) 指定値 : 2001:db8:1111::/32 の場合
 経路情報 : 2001:db8:1111::/32 は制御対象となる
 2001:db8:1111::/64 は制御対象とはならない

また、経路情報のプレフィックスと指定したプレフィックスが、指定したプレフィックス長まで一致した場合に制御対象とすることもできます。

指定値 : 2001:db8::/16 の場合
 経路情報 : 2001:db8::/32 は制御対象となる
 2001:db8:1111::/32 は制御対象となる

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. 特定の条件の経路情報だけを透過させ、その他はすべて遮断する
- B. 特定の条件の経路情報だけを遮断し、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。

- 特定の経路情報の送信を許可する
- 特定の経路情報のメトリック値を変更して送信する
- 特定の経路情報の受信を許可する
- 特定の経路情報のメトリック値を変更して受信する

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。

- 特定の経路情報の送信を禁止する
- 特定の経路情報の受信を禁止する

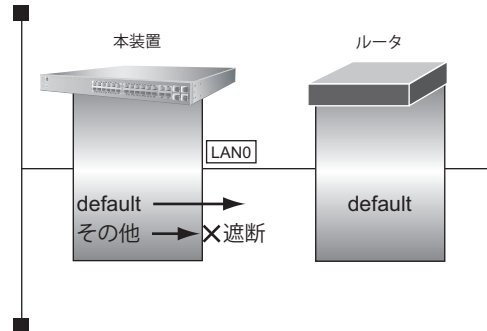
こんな事に気をつけて

- フィルタリング条件には、優先度を示す定義番号があり、小さいほど、より高い優先度を示します。
 - RIP受信時には、優先順位の高い定義から順に受信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。一致した以降の条件は参照されません。また、受信方向のすべての条件に一致しないRIP経路情報は遮断されます。
 - RIP送信時には、優先順位の高い定義から順に送信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。一致した以降の条件は参照されません。また、送信方向のすべての条件に一致しないRIP経路情報は遮断されます。
-

24.1 特定の経路情報の送信を許可する

適用機種 SR-S732TR1, 752TR1

ここでは、本装置からルータへのデフォルトルートの送信だけを許可し、それ以外の経路情報の送信を禁止する場合の設定方法を説明しています。



● 前提条件

- すべてのインタフェースにIPv6機能とRIP (IPv6) を使用する設定がされている
- IPv6 フォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置からルータへのデフォルトルートの送信だけを許可
- その他はすべて遮断

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● コマンド

```
デフォルトルートを透過させる
# lan 0 ip6 rip filter 0 act pass out
# lan 0 ip6 rip filter 0 route default
```

```
その他の経路情報はすべて遮断する
# lan 0 ip6 rip filter 1 act reject out
# lan 0 ip6 rip filter 1 route any
```

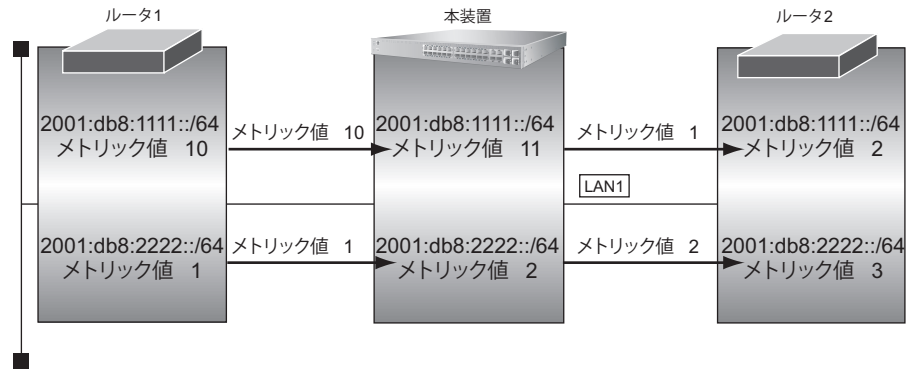
```
設定終了
# save
# commit
```

24.2 特定の経路情報のメトリック値を変更して送信する

適用機種 SR-S732TR1, 752TR1

ここでは、本装置がルータ2へ2001:db8:1111::/64、メトリック値1の経路情報を送信する場合の設定方法を説明します。

なお、本装置は、ルータ1から2001:db8:1111::/64のメトリック値10と2001:db8:2222::/64のメトリック値1の経路情報を受信するものとします。



● 前提条件

- すべてのインタフェースにIPv6機能とRIP (IPv6) を使用する設定がされている
- IPv6 フォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置から2001:db8:1111::/64の送信を許可する場合、メトリック値1に変更
- 2001:db8:1111::/64以外の経路情報は、メトリック値を変更しない

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● コマンド

```
2001:db8:1111::/64 をメトリック値1で送信する
# lan 1 ip6 rip filter 0 act pass out
# lan 1 ip6 rip filter 0 route 2001:db8:1111::/64
# lan 1 ip6 rip filter 0 set metric 1
```

```
その他の経路情報はメトリック値を変更しないで送信する
# lan 1 ip6 rip filter 1 act pass out
# lan 1 ip6 rip filter 1 route any
```

```
設定終了
# save
# commit
```

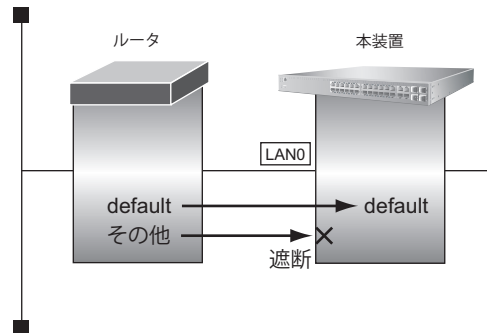
こんな事に気をつけて

- 送信方向でメトリック値が設定されている場合、インタフェースのRIP加算メトリック値の加算は行われません。
- 送信方向でメトリック値が設定されていても、メトリック値16の経路情報のメトリック値は変更されません。

24.3 特定の経路情報の受信を許可する

適用機種 SR-S732TR1, 752TR1

ここでは、本装置はルータからデフォルトルートの受信だけを許可し、それ以外の経路情報の受信を禁止する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースにIPv6機能とRIP (IPv6) を使用する設定がされている
- IPv6 フォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置はデフォルトルートの受信だけを許可
- その他はすべて遮断

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● コマンド

```
デフォルトルートを透過させる
# lan 0 ip6 rip filter 0 act pass in
# lan 0 ip6 rip filter 0 route default
```

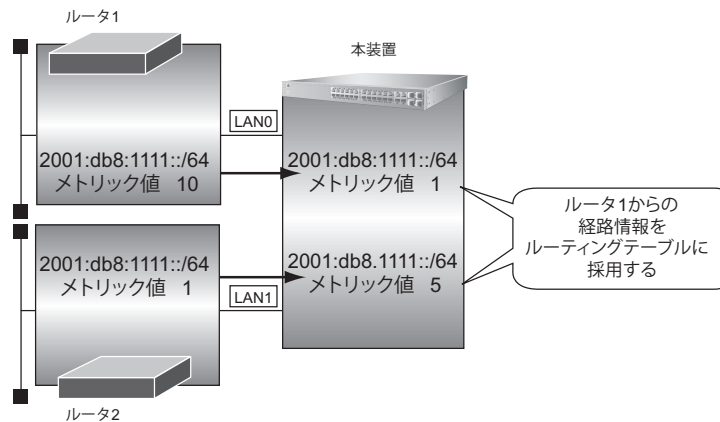
```
その他の経路情報はすべて遮断する
# lan 0 ip6 rip filter 1 act reject in
# lan 0 ip6 rip filter 1 route any
```

```
設定終了
# save
# commit
```

24.4 特定の経路情報のメトリック値を変更して受信する

適用機種 SR-S732TR1, 752TR1

ここでは、本装置が、ルータ1とルータ2から同じ先への経路情報 2001:db8:1111::/64 を受信した場合に、ルータ1から受信した経路情報を採用する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースにIPv6機能とRIP (IPv6) を使用する設定がされている
- IPv6 フォワーディング機能を使用する設定がされている

● フィルタリング設計

- ルータ1から、2001:db8:1111::/64の経路情報を受信した場合、メトリック値1に変更
- ルータ2から、2001:db8:1111::/64の経路情報を受信した場合、メトリック値5に変更
- 上記以外の経路情報は、メトリック値を変更しない

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● コマンド

```
LAN0から2001:db8:1111::/64を受信した場合、メトリック値1で受信する
# lan 0 ip6 rip filter 0 act pass in
# lan 0 ip6 rip filter 0 route 2001:db8:1111::/64
# lan 0 ip6 rip filter 0 set metric 1

LAN0からのその他の経路情報はすべて受信する
# lan 0 ip6 rip filter 1 act pass in
# lan 0 ip6 rip filter 1 route any

lan1から2001:db8:1111::/64を受信した場合、メトリック値5で受信する
# lan 1 ip6 rip filter 0 act pass in
# lan 1 ip6 rip filter 0 route 2001:db8:1111::/64
# lan 1 ip6 rip filter 0 set metric 5

lan1からのその他の経路情報はすべて受信する
# lan 1 ip6 rip filter 1 act pass in
# lan 1 ip6 rip filter 1 route any

設定終了
# save
# commit
```

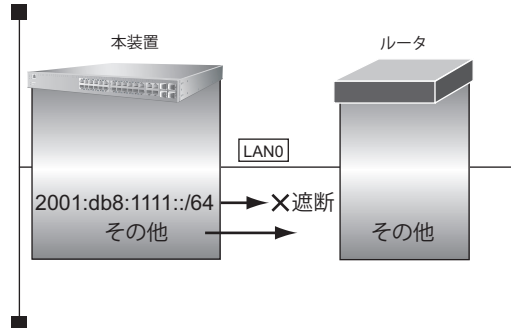
こんな事に気をつけて

受信方向でメトリック値が設定されていても、メトリック値16の経路情報のメトリック値は変更されません。

24.5 特定の経路情報の送信を禁止する

適用機種 SR-S732TR1, 752TR1

ここでは、本装置からルータへの 2001:db8:1111::/64 の送信を禁止し、それ以外の経路情報の送信を許可する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースにIPv6機能とRIP (IPv6) を使用する設定がされている
- IPv6 フォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置からルータへの 2001:db8:1111::/64 の送信を禁止
- その他はすべて透過

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● コマンド

```

2001:db8:1111::/64 を遮断する
# lan 0 ip6 rip filter 0 act reject out
# lan 0 ip6 rip filter 0 route 2001:db8:1111::/64

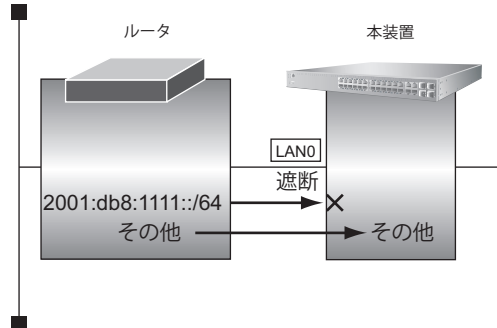
その他の経路情報はすべて透過させる
# lan 0 ip6 rip filter 1 act pass out
# lan 0 ip6 rip filter 1 route any

設定終了
# save
# commit
    
```

24.6 特定の経路情報の受信を禁止する

適用機種 SR-S732TR1, 752TR1

ここでは、本装置は、ルータから 2001:db8:1111::/64 の経路情報の受信を禁止し、それ以外の経路情報の受信を許可する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースに IPv6 機能と RIP (IPv6) を使用する設定がされている
- IPv6 フォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置は 2001:db8:1111::/64 の受信を禁止
- その他はすべて透過

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● コマンド

```

2001:db8:1111::/64 を遮断する
# lan 0 ip6 rip filter 0 act reject in
# lan 0 ip6 rip filter 0 route 2001:db8:1111::/64

その他の経路情報はすべて透過させる
# lan 0 ip6 rip filter 1 act pass in
# lan 0 ip6 rip filter 1 route any

設定終了
# save
# commit
    
```


25 OSPF を使用したネットワークを構築する (IPv4)

適用機種 SR-S732TR1, 752TR1

ここでは、OSPFv2を使用したダイナミックルーティングのネットワークの設定方法について説明します。

OSPFを使用するネットワークは、バックボーンエリアとその他のエリアに分割して管理します。

エリアには、エリアごとにエリアIDを設定します。バックボーンエリアには必ず0.0.0.0のエリアIDを設定し、ほかのエリアには重複しないように0.0.0.0以外のエリアIDを設定します。

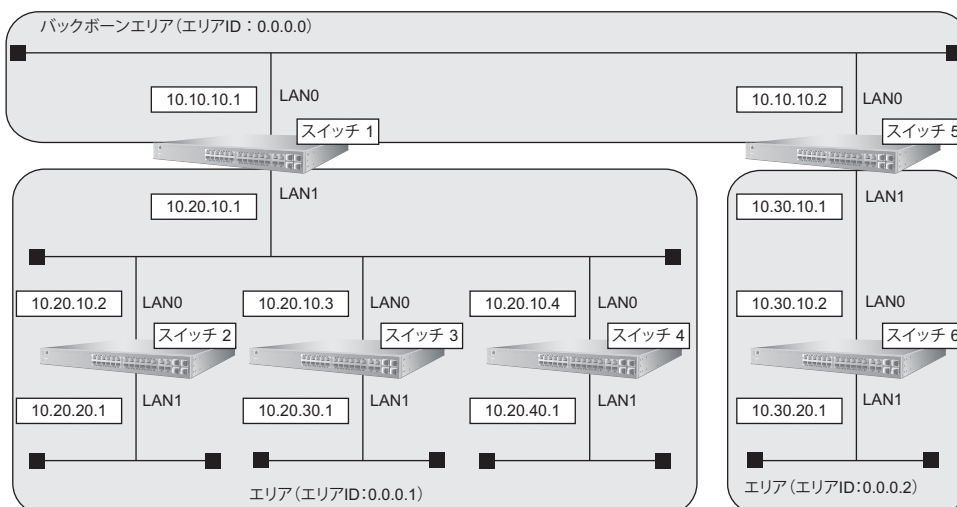
エリア境界ルータでは、エリア内の経路情報を集約して広報することができます。

☛ 参照 マニュアル「機能説明書」

こんな事に気をつけて

- OSPFを使用するインタフェースは、それぞれ異なったネットワークに属するIPアドレスを設定する必要があります。同じネットワークに属するIPアドレスを設定した場合、OSPFを使用しないと判断されます。
- ルータは、各エリアに50台まで設置することができます。ただし、複数のエリアの境界ルータとして使用する場合は、2つ以上のエリアの指定ルータ (Designated Router) とならないように設定してください。
- 隣接するOSPFルータ同士は、同じMTU値を設定してください。
- 経路情報を最大値まで保持した場合、OSPF以外の経路情報の減少によって経路情報に空きができて、OSPFの経路は、経路情報に反映されません。
- 本装置で保有できるLSA数には上限値があります。この上限値を超えるネットワークで本装置を使用した場合、正しく通信することができません (LSDBオーバーフロー)。また、LSA生成元のルータの停止などによって、LSA数が本装置の上限値以下まで減少した場合、本装置の電源再投入、commit / reset コマンド実行にかかわらず、正常に通信ができるまでに最大60分かかることがあります。
- OSPF使用中にcommitコマンドを実行した場合、自装置が広報したすべてのLSAに対してMaxAgeで再広報を行ったあとに、OSPFネットワークへの経路情報が再作成されることがあります。
- OSPFで使用するインタフェースは、以下の条件で使用してください。

本装置がDRを兼務する場合	本装置がDRを兼務しない場合
(25000+本装置保有LSA数) 未満	(50000+本装置保有LSA数) 未満



● **前提条件**

- すべてのスイッチのすべてのインタフェースにIPアドレスの設定がされている
- すべてのスイッチにIP フォワーディング機能を使用する設定がされている

● **設定条件**

[スイッチ1でのルーティングプロトコル情報]

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : OSPF
- LAN0でのOSPFエリアID : 0.0.0.0
- LAN1でのOSPFエリアID : 0.0.0.1
- LAN1でのルータ優先度 : 0
- エリア0.0.0.1への集約経路設定 : 10.20.0.0/16

[スイッチ2でのルーティングプロトコル情報]

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : OSPF
- LAN0でのOSPFエリアID : 0.0.0.1
- LAN1でのOSPFエリアID : 0.0.0.1
- LAN0でのルータ優先度 : 1
- LAN1でのpassive-interface設定 : 設定する

[スイッチ3でのルーティングプロトコル情報]

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : OSPF
- LAN0でのOSPFエリアID : 0.0.0.1
- LAN1でのOSPFエリアID : 0.0.0.1
- LAN0でのルータ優先度 : 255
- LAN1でのpassive-interface設定 : 設定する

[スイッチ4でのルーティングプロトコル情報]

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : OSPF
- LAN0でのOSPFエリアID : 0.0.0.1
- LAN1でのOSPFエリアID : 0.0.0.1
- LAN0でのルータ優先度 : 1
- LAN1でのpassive-interface設定 : 設定する

[スイッチ5でのルーティングプロトコル情報]

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : OSPF
- LAN0でのOSPFエリアID : 0.0.0.0
- LAN1でのOSPFエリアID : 0.0.0.2
- エリア0.0.0.2への集約経路設定 : 10.30.0.0/16

[スイッチ6でのルーティングプロトコル情報]

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : OSPF

- LAN0でのOSPFエリアID : 0.0.0.2
- LAN1でのOSPFエリアID : 0.0.0.2
- LAN1でのpassive-interface設定 : 設定する

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。

スイッチ1を設定する

● コマンド

```

LAN情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 1
# lan 1 ip ospf priority 0

OSPF情報を設定する
# ospf ip area 0 id 0.0.0.0
# ospf ip area 1 id 0.0.0.1
# ospf ip area 1 range 0 10.20.0.0/16

設定終了
# save
# commit
    
```

スイッチ2を設定する

● コマンド

```

LAN情報を設定する
# lan 0 ip ospf use on 0
# lan 0 ip ospf priority 1
# lan 1 ip ospf use on 0
# lan 1 ip ospf passive on

OSPF情報を設定する
# ospf ip area 0 id 0.0.0.1

設定終了
# save
# commit
    
```

スイッチ 3 を設定する

● コマンド

```

LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 0 ip ospf priority 255
# lan 1 ip ospf use on 0
# lan 1 ip ospf passive on

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.1

設定終了
# save
# commit
    
```

スイッチ 4 を設定する

● コマンド

```

LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 0 ip ospf priority 1
# lan 1 ip ospf use on 0
# lan 1 ip ospf passive on

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.1

設定終了
# save
# commit
    
```

スイッチ 5 を設定する

● コマンド

```

LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 1

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.0
# ospf ip area 1 id 0.0.0.2
# ospf ip area 1 range 0 10.30.0.0/16

設定終了
# save
# commit
    
```

スイッチ 6 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 0
# lan 1 ip ospf passive on

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.2

設定終了
# save
# commit
```

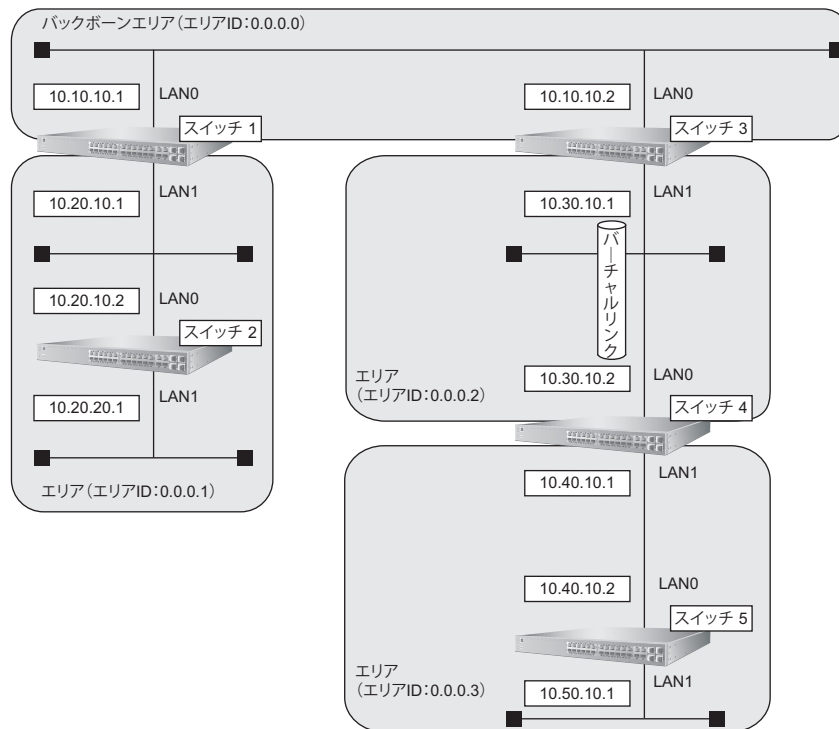
25.1 バーチャルリンクを使う

適用機種 SR-S732TR1, 752TR1

バックボーンエリアと直接接続できないエリアを、バーチャルリンクを使用して接続する設定方法について説明します。

こんな事に気をつけて

- バーチャルリンクは、スタブエリア、準スタブエリアを経由して使用することはできません。
- バーチャルリンクを使用する場合は、OSPF ルータ ID を設定する必要があります。設定する際は、OSPF ルータ ID が重複しないように設定してください。



● 前提条件

- すべてのスイッチのすべてのインタフェースにIPアドレスの設定がされている
- すべてのスイッチにIP フォワーディング機能を使用する設定がされている

● 設定条件

[スイッチ1でのルーティングプロトコル情報]

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : OSPF
- LAN0でのOSPFエリアID : 0.0.0.0
- LAN1でのOSPFエリアID : 0.0.0.1

[スイッチ2でのルーティングプロトコル情報]

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : OSPF
- LAN0でのOSPFエリアID : 0.0.0.1
- LAN1でのOSPFエリアID : 0.0.0.1

[スイッチ3でのルーティングプロトコル情報]

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : OSPF
- LAN0でのOSPFエリアID : 0.0.0.0
- LAN1でのOSPFエリアID : 0.0.0.2
- OSPFルータID : 10.30.10.1
- バーチャルリンク接続先OSPFルータID : 10.40.10.1

[スイッチ4でのルーティングプロトコル情報]

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : OSPF
- LAN0でのOSPFエリアID : 0.0.0.2
- LAN1でのOSPFエリアID : 0.0.0.3
- OSPFルータID : 10.40.10.1
- バーチャルリンク接続先OSPFルータID : 10.30.10.1

[スイッチ5でのルーティングプロトコル情報]

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : OSPF
- LAN0でのOSPFエリアID : 0.0.0.3
- LAN1でのOSPFエリアID : 0.0.0.3

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。

スイッチ1を設定する

● コマンド

```

LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 1

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.0
# ospf ip area 1 id 0.0.0.1

設定終了
# save
# commit
    
```

スイッチ 2 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 0

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.1

設定終了
# save
# commit
```

スイッチ 3 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 1

OSPF 情報を設定する
# ospf ip id 10.30.10.1
# ospf ip area 0 id 0.0.0.0
# ospf ip area 1 id 0.0.0.2
# ospf ip area 1 vlink 0 id 10.40.10.1

設定終了
# save
# commit
```

スイッチ 4 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 1

OSPF 情報を設定する
# ospf ip id 10.40.10.1
# ospf ip area 0 id 0.0.0.2
# ospf ip area 0 vlink 0 id 10.30.10.1
# ospf ip area 1 id 0.0.0.3

設定終了
# save
# commit
```


スイッチ 5 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 0

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.3

設定終了
# save
# commit
```

25.2 スタブエリアを使う

適用機種 SR-S732TR1, 752TR1

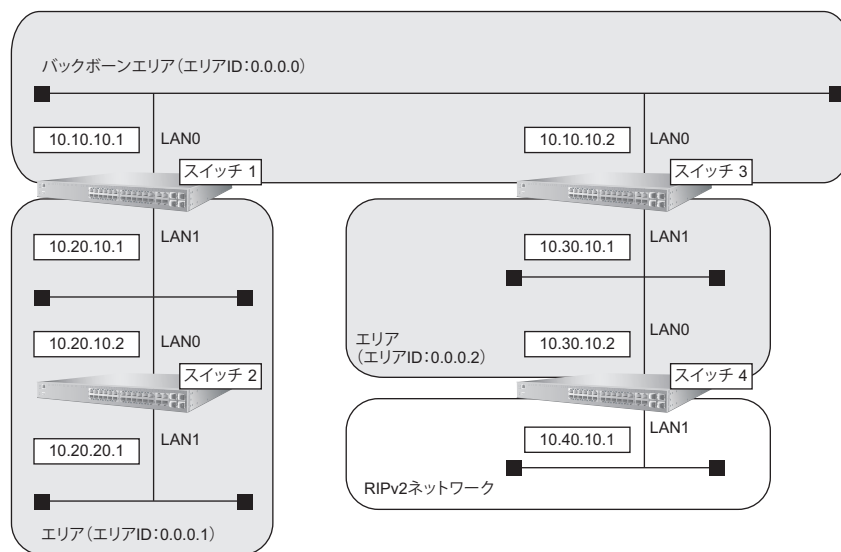
OSPF以外のルーティングプロトコルを使用したネットワークとの接続の設定について説明します。

OSPFは、RIPで受信した経路情報、スタティック経路情報およびインタフェース経路情報をOSPFネットワークに取り入れることができます。また、OSPFの経路情報をRIPで広報することができます。

OSPF以外のネットワークと接続する場合、スタブエリアとして運用すると、OSPFネットワーク外の経路としてデフォルトルートを使用するため、エリア内の経路情報を少なくすることができます。スタブエリアからOSPF以外のネットワークに直接接続することはできません。直接、接続する場合は、準スタブエリア (NSSA) として運用します。

こんな事に気をつけて

OSPF以外のネットワークと接続する場合、OSPF以外のネットワークで使用するインタフェース経路情報をOSPFネットワークに取り入れるように設定する必要があります。



● 前提条件

- すべてのスイッチのすべてのインタフェースにIPアドレスの設定がされている
- すべてのスイッチにIPフォワーディング機能を使用する設定がされている

● 設定条件

[スイッチ1でのルーティングプロトコル情報]

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : OSPF
- LAN0でのOSPFエリアID : 0.0.0.0
- LAN1でのOSPFエリアID : 0.0.0.1
- エリアID 0.0.0.1のエリアタイプ : stub

[スイッチ2でのルーティングプロトコル情報]

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : OSPF
- LAN0でのOSPFエリアID : 0.0.0.1
- LAN1でのOSPFエリアID : 0.0.0.1
- エリアID 0.0.0.1のエリアタイプ : stub

[スイッチ3でのルーティングプロトコル情報]

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : OSPF
- LAN0でのOSPFエリアID : 0.0.0.0
- LAN1でのOSPFエリアID : 0.0.0.2
- エリアID 0.0.0.2のエリアタイプ : nssa

[スイッチ4でのルーティングプロトコル情報]

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : RIP V2,OSPF
- LAN0でのOSPFエリアID : 0.0.0.2
- LAN1での passive-interface 設定 : 設定する
- エリアID0.0.0.2のエリアタイプ : nssa
- OSPF 経路のRIPでの広報 : 再配布する
- RIP 経路のOSPFでの広報 : 再配布する

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。

スイッチ1を設定する

● コマンド

```

LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 1

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.0
# ospf ip area 1 id 0.0.0.1
# ospf ip area 1 type stub

設定終了
# save
# commit
    
```

スイッチ2を設定する

● コマンド

```

LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 0

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.1
# ospf ip area 0 type stub

設定終了
# save
# commit
    
```

スイッチ 3 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 1

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.0
# ospf ip area 1 id 0.0.0.2
# ospf ip area 1 type nssa

設定終了
# save
# commit
```

スイッチ 4 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip rip use v2m v2 0 off
# lan 1 ip ospf use on 0
# lan 1 ip ospf passive on

ルーティングマネージャ情報を設定する
# routemanage ip redistrib ospf rip on
# routemanage ip redistrib rip ospf on

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.2
# ospf ip area 0 type nssa

設定終了
# save
# commit
```

26 OSPF の経路を制御する (IPv4)

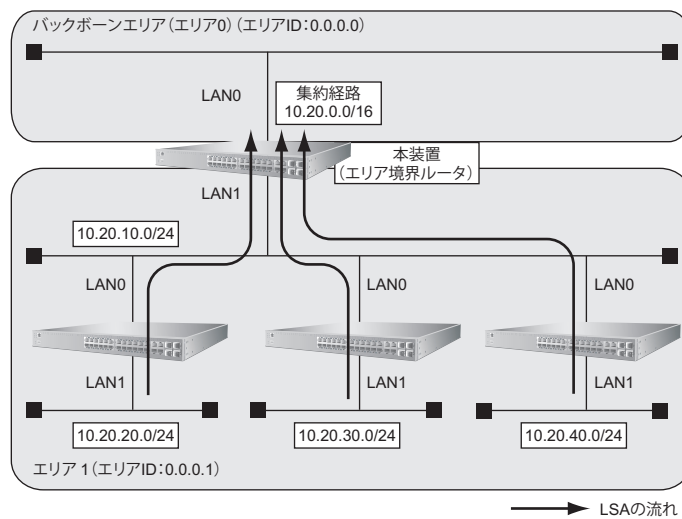
適用機種 SR-S732TR1, 752TR1

本装置で、ほかのルータから受信する経路情報 (LSA) に変更を加えることで、本装置で保有する経路情報や広報する経路情報の数を制御することができます。

26.1 OSPF ネットワークでエリアの経路情報 (LSA) を集約する

適用機種 SR-S732TR1, 752TR1

エリア内の LSA を、本装置 (エリア境界ルータ) で集約して、バックボーンエリアへ取り込む場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースに IP アドレスの設定がされている
- IP フォワーディング機能を使用する設定がされている

● 経路情報の設計

- エリア内の LSA を、本装置 (エリア境界ルータ) で集約してバックボーンエリアに取り込む

● 設定条件

- LAN0 でのルーティングプロトコル : OSPF
- LAN1 でのルーティングプロトコル : OSPF
- LAN0 でのエリア ID : 0.0.0.0
- LAN1 でのエリア ID : 0.0.0.1
- バックボーンエリアへの集約経路設定 : 10.20.0.0/16

上記の経路情報に従って設定する場合のコマンド例を示します。

● コマンド

OSPF で使用するインタフェースを設定する

```
# lan 0 ip ospf use on 0
```

```
# lan 1 ip ospf use on 1
```

エリア情報を設定する

```
# ospf ip area 0 id 0.0.0.0
```

```
# ospf ip area 1 id 0.0.0.1
```

集約経路を設定する

```
# ospf ip area 1 range 0 10.20.0.0/16
```

設定終了

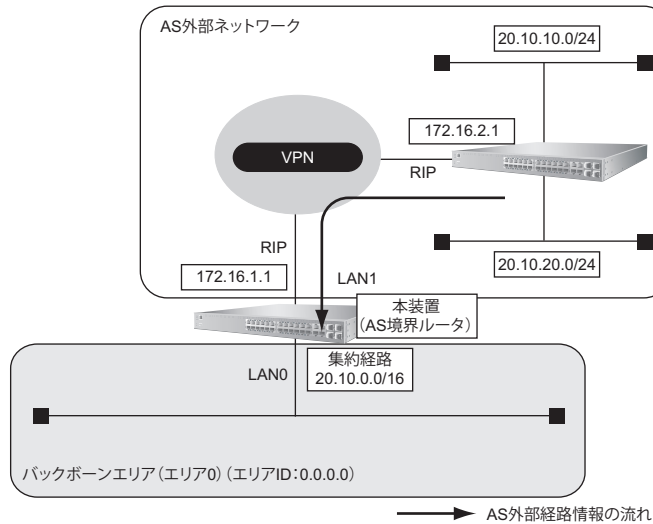
```
# save
```

```
# commit
```

26.2 AS 外部経路を集約して OSPF ネットワークに広報する

適用機種 SR-S732TR1, 752TR1

AS 外部 (OSPF 以外) のネットワークの経路情報を本装置 (AS 境界ルータ) で集約して、バックボーンエリアに広報する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースに IP アドレスの設定がされている
- IPv6 フォワーディング機能を使用する設定がされている
- LAN1 インタフェースに RIPv2 を使用する設定がされている
- IP フォワーディング機能を使用する設定がされている

● 経路情報の設計

- AS 外部経路情報を本装置 (AS 境界ルータ) で集約して OSPF ネットワーク (バックボーンエリア) に広報する
- その他の AS 外部経路情報はすべて遮断する

● 設定条件

- LAN0 でのルーティングプロトコル : OSPF
- LAN0 でのエリア ID : 0.0.0.0
- バックボーンエリアへの集約経路設定 : 20.10.0.0/16
- OSPF に再配布する RIP 経路 : 20.10.0.0/16 でマスクした結果が一致する経路だけを再配布

上記の経路情報に従って設定する場合のコマンド例を示します。

● コマンド

OSPF で使用するインターフェースを設定する
lan 0 ip ospf use on 0

エリア情報を設定する
ospf ip area 0 id 0.0.0.0

OSPF に広報する AS 外部経路を設定する
routemanage ip redistrib ospf rip on

集約経路を設定する
ospf ip summary 0 20.10.0.0/16

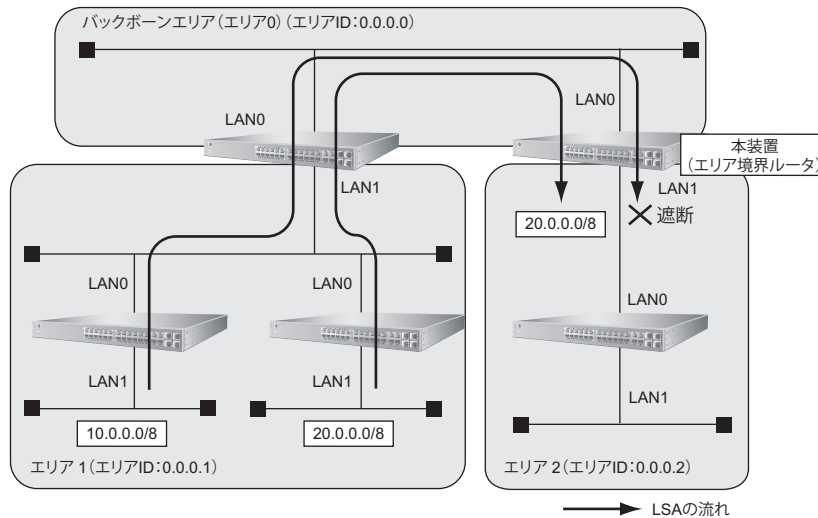
不要な AS 外部経路情報を遮断する
ospf ip redistrib 0 pass 20.10.0.0/16 inexact
ospf ip redistrib 1 reject any

設定終了
save
commit

26.3 エリア境界ルータで不要な経路情報 (LSA) を遮断する

適用機種 SR-S732TR1, 752TR1

エリア境界ルータで、通信に使用しないTYPE3 サマリ LSA の経路情報を遮断する設定方法を説明します。



● 前提条件

- すべてのインターフェースに IP アドレスの設定がされている
- IP フォワーディング機能を使用する設定がされている

● 経路情報の設計

- エリア 1 の 10.0.0.0/8 のネットワークとエリア 2 のネットワークでは通信を行わないため、10.0.0.0/8 の経路情報を遮断する
- その他はすべて透過させる

● 設定条件

- LAN0 でのルーティングプロトコル : OSPF
- LAN1 でのルーティングプロトコル : OSPF
- LAN0 でのエリア ID : 0.0.0.0
- LAN1 でのエリア ID : 0.0.0.2
- 10.0.0.0/8 の LSA を遮断

上記の経路情報に従って設定する場合のコマンド例を示します。

● コマンド

```
OSPF で使用するインターフェースを設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 1

エリア情報を設定する
# ospf ip area 0 id 0.0.0.0
# ospf ip area 1 id 0.0.0.2

エリア 2 に注入する経路情報を制限する
# ospf ip area 1 type3-lsa 0 reject 10.0.0.0/8 in exact
# ospf ip area 1 type3-lsa 1 pass any in
```

```
設定終了  
# save  
# commit
```

27 OSPF 機能を使う (IPv6)

適用機種 SR-S732TR1, 752TR1

27.1 OSPF ネットワークを構築する

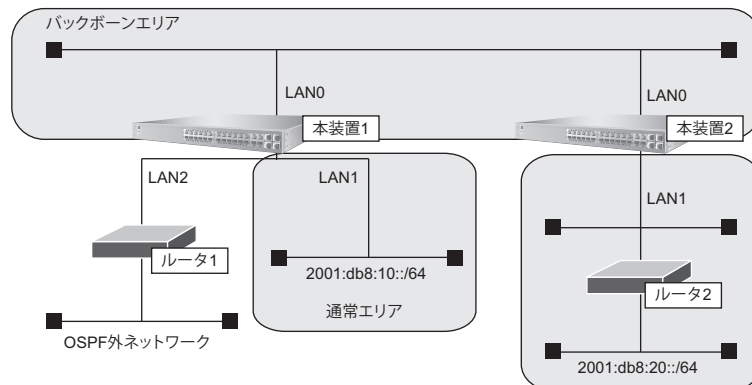
適用機種 SR-S732TR1, 752TR1

OSPF (IPv6) を使用したネットワークの構築について説明します。

こんな事に気をつけて

- ルータは、各エリアに30台まで設置することができます。ただし、複数のエリアの境界ルータとして使用する場合は、2つ以上のエリアの指定ルータ (DR : Designated Router) とならないように設定してください。
- LANを使用した隣接 OSPF ルータと MTU 値が一致しない場合は、隣接関係を構築できません。
- 経路情報を最大値まで保持した場合、OSPF 以外の経路情報の減少によって経路情報に空きができて、OSPF の経路は、経路情報に反映されません。
- 本装置で保有できる LSA 数には上限値があります。この上限値を超えるネットワークで本装置を使用した場合、正しく通信することができません (LSDB オーバフロー)。また、LSA 生成元のルータの停止などによって、LSA 数が本装置の上限値以下まで減少した場合、本装置の電源再投入、commit/reset コマンドの実行にかかわらず、正常に通信ができるまでに最大60分かかることがあります。
- OSPF で使用するインタフェースは、以下の条件で使用してください。

本装置がDRを兼務する場合	本装置がDRを兼務しない場合
(10000+ 本装置保有 LSA 数) 未満	(20000+ 本装置保有 LSA 数) 未満



● 前提条件

- 本装置1、2のすべてのインタフェースでIPv6機能を利用する設定 (lan ip6 use on) がされている
- 本装置1、2にIPv6 フォワーディング機能を使用する設定がされている
- 本装置1のLAN1には、グローバルアドレスが設定されている
- 本装置1のLAN2には、OSPF外ネットワークへの経路がスタティック設定されている

● 設定条件

- 本装置1はバックボーンエリアと通常エリアのエリア境界ルータであり、かつ、OSPF外ネットワークへ到達するためのAS境界ルータとして運用する
- 本装置2はバックボーンエリアとスタブエリアのエリア境界ルータとして運用する。また、バックボーンエリアでは指定ルータとして運用する

- 各エリア ID は、以下のとおり
- | | |
|-----------|-----------|
| バックボーンエリア | : 0.0.0.0 |
| 通常エリア | : 0.0.0.1 |
| スタブエリア | : 0.0.0.2 |

[本装置 1]

- LAN0 はバックボーンエリアに属する
- LAN1 は通常エリアに属し、ほかにルータが接続されていないため、Passive-interface として OSPF パケットを送信しないようにする
- OSPF ルータ ID は 100.0.0.1 とする
- スタティック経路を OSPF に再配布する

[本装置 2]

- LAN0 はバックボーンエリアに属し、バックボーンエリアの指定ルータとするため、指定ルータ優先度に 255 を設定する
- LAN1 はスタブエリアとする
- OSPF ルータ ID は 100.0.0.2 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。

本装置 1 を設定する

● コマンド

```

LAN 情報を設定する
# lan 0 ip6 ospf use on 0
# lan 1 ip6 ospf use on 1
# lan 1 ip6 ospf passive on

OSPF 情報を設定する
# ospf ip6 id 100.0.0.1
# ospf ip6 area 0 id 0.0.0.0
# ospf ip6 area 1 id 0.0.0.1

ルーティングマネージャ情報を設定する
# routemanage ip6 redistrib ospf static on

設定終了
# save
# commit
    
```

本装置 2 を設定する

● コマンド

```

LAN 情報を設定する
# lan 0 ip6 ospf use on 0
# lan 0 ip6 ospf priority 255
# lan 1 ip6 ospf use on 1

OSPF 情報を設定する
# ospf ip6 id 100.0.0.2
# ospf ip6 area 0 id 0.0.0.0
# ospf ip6 area 1 id 0.0.0.2
    
```

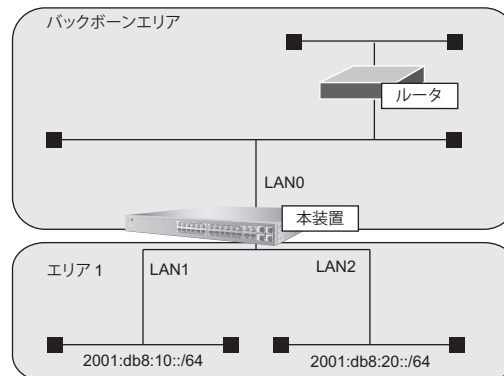
```
# ospf ip6 area 1 type stub
```

```
設定終了
# save
# commit
```

27.2 エリア境界ルータでエリア内部経路を集約する

適用機種 SR-S732TR1, 752TR1

エリア境界ルータで、エリア内経路を集約してほかのエリアに広報する設定について説明します。



● 前提条件

- 本装置のすべてのインタフェースでIPv6機能を利用する設定 (lan ip6 use on) がされている
- IPv6 フォワーディング機能を使用する設定がされている
- 本装置はバックボーンエリアとエリア1のエリア境界ルータとして運用し、LAN0、LAN1、LAN2でOSPFを使用する
- OSPFルータIDは、100.0.0.1
- 各エリアIDは、以下のとおり

バックボーンエリア	: 0.0.0.0 (エリア定義番号0)
エリア1	: 0.0.0.1 (エリア定義番号1)
- 各インタフェースのIPアドレスは、以下のとおり

LAN1	: 2001:db8:10::1/64
LAN2	: 2001:db8:20::1/64

● 設定条件

- エリア1のエリア内部経路 (2001:db8:10::/64、2001:db8:20::/64) は、集約経路 (2001:db8::/32、コスト100) としてバックボーンエリアに広報する

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。

本装置を設定する

● コマンド

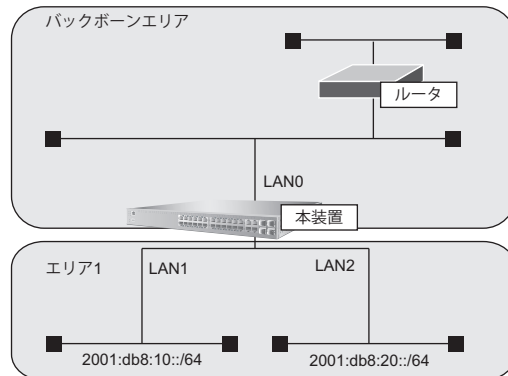
```
OSPF情報を設定する
# ospf ip6 area 1 range 0 2001:db8::/32 100
```

```
設定終了
# save
# commit
```

27.3 エリア境界ルータで不要な経路情報を遮断する

適用機種 SR-S732TR1, 752TR1

エリア境界ルータで、ほかのエリアに対し特定のエリア内経路（エリア間プレフィックスLSA）を遮断して広報する設定について説明します。



● 前提条件

- 本装置のすべてのインタフェースでIPv6機能を利用する設定（lan ip6 use on）がされている
- IPv6 フォワーディング機能を使用する設定がされている
- 本装置はバックボーンエリアとエリア1のエリア境界ルータとして運用し、LAN0、LAN1、LAN2でOSPFを使用する
- OSPFルータIDは、100.0.0.1
- 各エリアIDは、以下のとおり
 バックボーンエリア : 0.0.0.0（エリア定義番号0）
 エリア1 : 0.0.0.1（エリア定義番号1）
- 各インタフェースのIPアドレスは、以下のとおり
 LAN1 : 2001:db8:10::1/64
 LAN2 : 2001:db8:20::1/64

● 設定条件

- エリア1からバックボーンエリアへの広報で、2001:db8:20::/64は破棄し、その他のエリア内部経路は透過させる

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。

本装置を設定する

● コマンド

```
OSPF情報を設定する
# ospf ip6 area 1 inter-area-prefix 0 reject 2001:db8:20::/64 out
# ospf ip6 area 1 inter-area-prefix 1 pass any out
```

```
設定終了
# save
# commit
```

28 マルチキャスト機能を使う

適用機種 SR-S732TR1, 752TR1

本装置には、マルチキャスト機能を動作させるために以下の2種類のプロトコルがあります。

- PIM-DM プロトコル
- PIM-SM プロトコル

また、本装置では、ルーティングプロトコルは使用しないで、スタティックにマルチキャスト経路を設定することもできます。

☛ 参照 マニュアル「機能説明書」

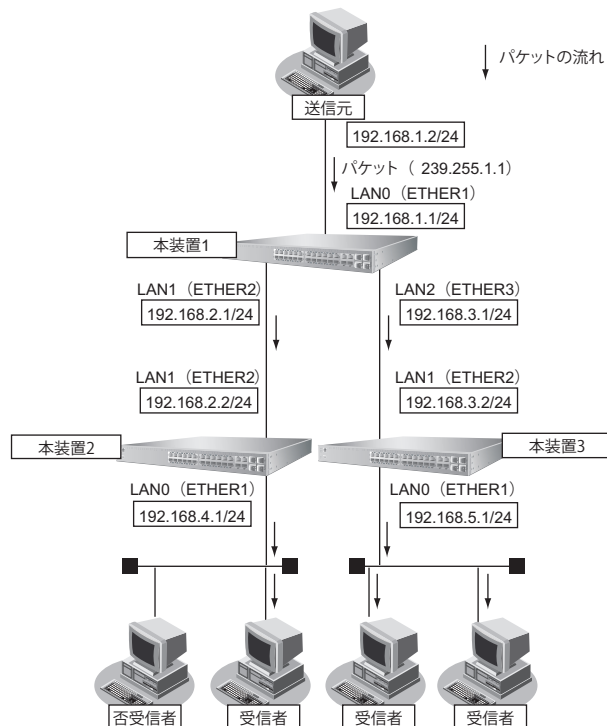
28.1 マルチキャスト機能 (PIM-DM) を使う

適用機種 SR-S732TR1, 752TR1

マルチキャスト機能 (PIM-DM) を使用すると、会社などの LAN 内で、動画や音声などを配送することができます。

こんな事に気をつけて

マルチキャストでパケットを配送するルータは、すべて PIM-DM に対応している必要があります。また、ルータ上ではユニキャストのルーティングテーブルが作成されている必要があります。



ここでは、PIM-DMを利用してマルチキャストパケットを転送する場合の設定方法を説明します。

● 設定条件

- マルチキャスト・ルーティングプロトコルにはPIM-DMを利用する

[本装置1]

- マルチキャストパケットを転送するインタフェースとしてLAN0、LAN1、LAN2を使用し、それぞれ、ETHER1、ETHER2、ETHER3に割り当てる
- ユニキャストのルーティングテーブルの作成にRIPを使用する
- LAN0のIPアドレス : 192.168.1.1/24
- LAN1のIPアドレス : 192.168.2.1/24
- LAN2のIPアドレス : 192.168.3.1/24

[本装置2]

- マルチキャストパケットを転送するインタフェースとしてLAN0、LAN1を使用し、それぞれ、ETHER1、ETHER2に割り当てる
- ユニキャストのルーティングテーブルの作成にRIPを使用する
- LAN0のIPアドレス : 192.168.4.1/24
- LAN1のIPアドレス : 192.168.2.2/24

[本装置3]

- マルチキャストパケットを転送するインタフェースとしてLAN0、LAN1を使用し、それぞれ、ETHER1、ETHER2に割り当てる
- ユニキャストのルーティングテーブルの作成にRIPを使用する
- LAN0のIPアドレス : 192.168.5.1/24
- LAN1のIPアドレス : 192.168.3.2/24

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]

```
ETHER ポートを削除する
# delete ether

LAN インタフェースを削除する
# delete lan

ETHER1～3 ポートを設定する
# ether 1 vlan untag 1
# ether 2 vlan untag 2
# ether 3 vlan untag 3

192.168.1.0/24のネットワークを設定する
# lan 0 vlan 1
# lan 0 ip address 192.168.1.1/24 3
# lan 0 ip multicast mode pimdm

192.168.2.0/24のネットワークを設定する
# lan 1 vlan 2
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ip rip use v2 v2 0 on
# lan 1 ip multicast mode pimdm

192.168.3.0/24のネットワークを設定する
# lan 2 vlan 3
```



```
# lan 2 ip address 192.168.3.1/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimdm
```

```
設定終了
# save
# commit
```

[本装置 2]

```
ETHER ポートを削除する
# delete ether
```

```
LAN インタフェースを削除する
# delete lan
```

```
ETHER1、2 ポートを設定する
# ether 1 vlan untag 1
# ether 2 vlan untag 2
```

```
192.168.4.0/24 のネットワークを設定する
# lan 0 vlan 1
# lan 0 ip address 192.168.4.1/24 3
# lan 0 ip multicast mode pimdm
```

```
192.168.2.0/24 のネットワークを設定する
# lan 1 vlan 2
# lan 1 ip address 192.168.2.2/24 3
# lan 1 ip rip use v2 v2 0 on
# lan 1 ip multicast mode pimdm
```

```
設定終了
# save
# commit
```

[本装置 3]

```
ETHER ポートを削除する
# delete ether
```

```
LAN インタフェースを削除する
# delete lan
```

```
ETHER1、2 ポートを設定する
# ether 1 vlan untag 1
# ether 2 vlan untag 2
```

```
192.168.5.0/24 のネットワークを設定する
# lan 0 vlan 1
# lan 0 ip address 192.168.5.1/24 3
# lan 0 ip multicast mode pimdm
```

```
192.168.3.0/24 のネットワークを設定する
# lan 1 vlan 2
# lan 1 ip address 192.168.3.2/24 3
# lan 1 ip rip use v2 v2 0 on
# lan 1 ip multicast mode pimdm
```

```
設定終了
# save
# commit
```

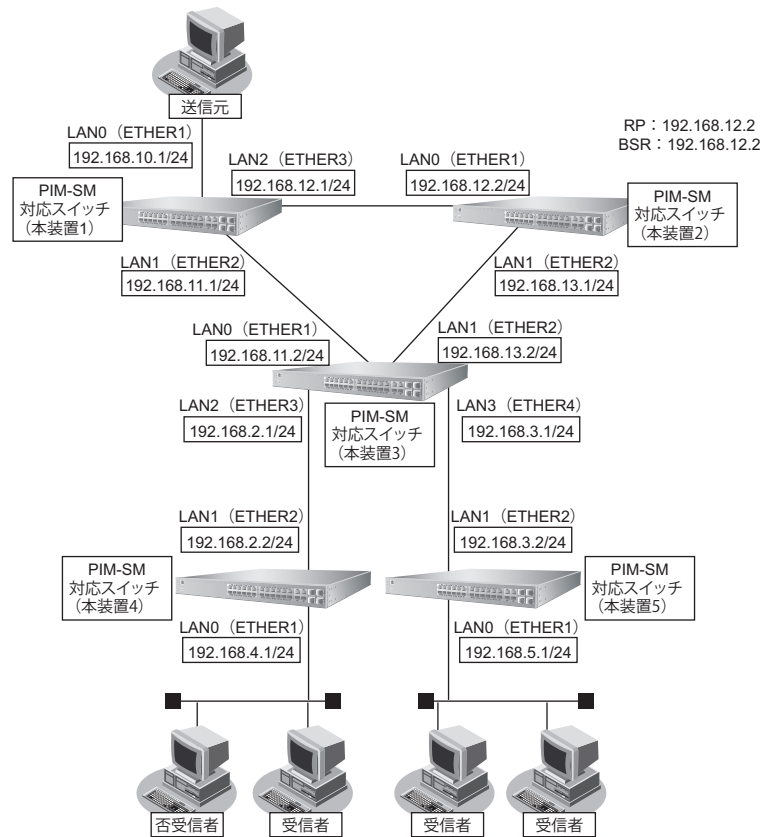
28.2 マルチキャスト機能 (PIM-SM) を使う

適用機種 SR-S732TR1, 752TR1

マルチキャスト機能 (PIM-SM) を使用すると、インターネットなど、十分な帯域を保証されないネットワーク上で、マルチキャストパケットを配送することができます。

こんな事に気をつけて

- マルチキャストパケットを配送するルータは、すべて PIM-SM に対応している必要があります。また、ルータ上ではユニキャストのルーティングテーブルが作成されている必要があります。
- ネットワーク内に BSR (Bootstrap Router : ブートストラップルータ) として動作するルータを 1 台以上置く必要があります。BSR は RP (Rendezvous Point : ランデブーポイント) の情報を広報します。
- ネットワーク内に RP として動作するルータを 1 台以上置く必要があります。パケットの配送は、RP を配送樹の頂点として開始され、その後、最短経路 (SPT : Shortest Path Tree) に切り替わります。
- PIM-SM ではマルチキャストパケットの配送を、RP を配送樹の頂点として開始するため、RP はネットワークの中心付近に置くことをお勧めします。



ここでは、PIM-SMを利用してマルチキャストパケットを転送する場合の設定方法を説明します。

マルチキャストパケットは、はじめはRPである本装置2を経由して、本装置1→本装置2→本装置3→本装置4の順に配送されます（一度、本装置1から本装置2に送られ、本装置2を配送樹の頂点として配送されます）。本装置4へのパケット転送開始直後に、本装置4はSPTへの切り替えを開始します。切り替えが行われると、本装置1→本装置3→本装置4のように、最短経路を利用して配送されます（本装置1を配送樹の頂点として配送されます）。同様の切り替えが本装置5でも行われます。

● 設定条件

- マルチキャスト・ルーティングプロトコルには PIM-SM を利用する
ユニキャストのルーティングテーブルの作成に RIP を使用する
RP : 本装置2 (192.168.12.2)
BSR : 本装置2 (192.168.12.2)
- SPTへの切り替えを行う（初期値）

【本装置1】

- マルチキャストパケットを転送するインターフェースとして LAN0、LAN1、LAN2 を使用し、それぞれ、ETHER1、ETHER2、ETHER3に割り当てる
- LAN0のIPアドレス : 192.168.10.1/24
- LAN1のIPアドレス : 192.168.11.1/24
- LAN2のIPアドレス : 192.168.12.1/24

【本装置2】

- マルチキャストパケットを転送するインターフェースとして LAN0、LAN1 を使用し、それぞれ、ETHER1、ETHER2に割り当てる
- LAN0のIPアドレス : 192.168.12.2/24
- LAN1のIPアドレス : 192.168.13.1/24
- RP : 192.168.12.2
- BSR : 192.168.12.2

【本装置3】

- マルチキャストパケットを転送するインターフェースとして LAN0、LAN1、LAN2、LAN3 を使用し、それぞれ、ETHER1、ETHER2、ETHER3、ETHER4に割り当てる
- LAN0のIPアドレス : 192.168.11.2/24
- LAN1のIPアドレス : 192.168.13.2/24
- LAN2のIPアドレス : 192.168.2.1/24
- LAN3のIPアドレス : 192.168.3.1/24

【本装置4】

- マルチキャストパケットを転送するインターフェースとして LAN0、LAN1 を使用し、それぞれ、ETHER1、ETHER2に割り当てる
- LAN0のIPアドレス : 192.168.4.1/24
- LAN1のIPアドレス : 192.168.2.2/24

【本装置5】

- マルチキャストパケットを転送するインターフェースとして LAN0、LAN1 を使用し、それぞれ、ETHER1、ETHER2に割り当てる
- LAN0のIPアドレス : 192.168.5.1/24
- LAN1のIPアドレス : 192.168.3.2/24

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]**

```
ETHER ポートを削除する
# delete ether

LAN インタフェースを削除する
# delete lan

ETHER1～3 ポートを設定する
# ether 1 vlan untag 1
# ether 2 vlan untag 2
# ether 3 vlan untag 3

192.168.10.0/24 のネットワークを設定する
# lan 0 vlan 1
# lan 0 ip address 192.168.10.1/24 3
# lan 0 ip multicast mode pimsm

192.168.11.0/24 のネットワークを設定する
# lan 1 vlan 2
# lan 1 ip address 192.168.11.1/24 3
# lan 1 ip rip use v2 v2 0 on
# lan 1 ip multicast mode pimsm

192.168.12.0/24 のネットワークを設定する
# lan 2 vlan 3
# lan 2 ip address 192.168.12.1/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimsm

設定終了
# save
# commit
```

[本装置 2]

```
ETHER ポートを削除する
# delete ether

LAN インタフェースを削除する
# delete lan

ETHER1、2 ポートを設定する
# ether 1 vlan untag 1
# ether 2 vlan untag 2

192.168.12.0/24 のネットワークを設定する
# lan 0 vlan 1
# lan 0 ip address 192.168.12.2/24 3
# lan 0 ip rip use v2 v2 0 on
# lan 0 ip multicast mode pimsm

192.168.13.0/24 のネットワークを設定する
# lan 1 vlan 2
# lan 1 ip address 192.168.13.1/24 3
# lan 1 ip rip use v2 v2 0 on
# lan 1 ip multicast mode pimsm

マルチキャストを設定する
# multicast ip pimsm candrp mode on
# multicast ip pimsm candrp address 192.168.12.2
# multicast ip pimsm candbsr mode on
# multicast ip pimsm candbsr address 192.168.12.2

設定終了
# save
# commit
```

[本装置 3]

```
ETHER ポートを削除する
# delete ether

LAN インタフェースを削除する
# delete lan

ETHER1～4 ポートを設定する
# ether 1 vlan untag 1
# ether 2 vlan untag 2
# ether 3 vlan untag 3
# ether 4 vlan untag 4

192.168.11.0/24 のネットワークを設定する
# lan 0 vlan 1
# lan 0 ip address 192.168.11.2/24 3
# lan 0 ip rip use v2 v2 0 on
# lan 0 ip multicast mode pimsm

192.168.13.0/24 のネットワークを設定する
# lan 1 vlan 2
# lan 1 ip address 192.168.13.2/24 3
# lan 1 ip rip use v2 v2 0 on
# lan 1 ip multicast mode pimsm
```

```
192.168.2.0/24 のネットワークを設定する
# lan 2 vlan 3
# lan 2 ip address 192.168.2.1/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimsm

192.168.3.0/24 のネットワークを設定する
# lan 3 vlan 4
# lan 3 ip address 192.168.3.1/24 3
# lan 3 ip rip use v2 v2 0 on
# lan 3 ip multicast mode pimsm

設定終了
# save
# commit
```

[本装置 4]

```
ETHER ポートを削除する
# delete ether

LAN インタフェースを削除する
# delete lan

ETHER1、2 ポートを設定する
# ether 1 vlan untag 1
# ether 2 vlan untag 2

192.168.4.0/24 のネットワークを設定する
# lan 0 vlan 1
# lan 0 ip address 192.168.4.1/24 3
# lan 0 ip multicast mode pimsm

192.168.2.0/24 のネットワークを設定する
# lan 1 vlan 2
# lan 1 ip address 192.168.2.2/24 3
# lan 1 ip rip use v2 v2 0 on
# lan 1 ip multicast mode pimsm

設定終了
# save
# commit
```

[本装置 5]

```
ETHER ポートを削除する
# delete ether

LAN インタフェースを削除する
# delete lan

ETHER1、2 ポートを設定する
# ether 1 vlan untag 1
# ether 2 vlan untag 2

192.168.5.0/24 のネットワークを設定する
# lan 0 vlan 1
# lan 0 ip address 192.168.5.1/24 3
# lan 0 ip multicast mode pimsm

192.168.3.0/24 のネットワークを設定する
# lan 1 vlan 2
```

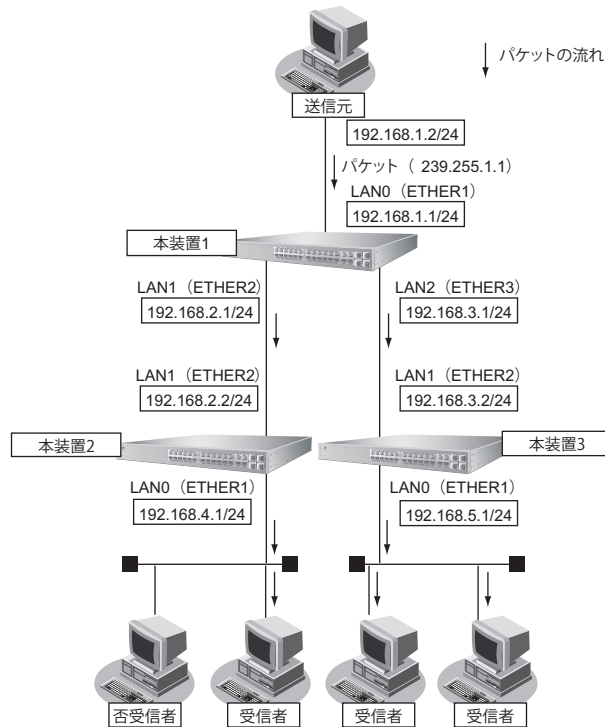
```
# lan 1 ip address 192.168.3.2/24 3  
# lan 1 ip rip use v2 v2 0 on  
# lan 1 ip multicast mode pimsm
```

```
設定終了  
# save  
# commit
```

28.3 マルチキャスト機能（スタティックルーティング）を使う

適用機種 SR-S732TR1, 752TR1

マルチキャスト機能（スタティックルーティング）を利用すると、マルチキャストパケットが配送される経路を静的に設定することができます。



ここでは、スタティックルーティングを利用してマルチキャストパケットの転送を行う場合を例に説明します。

● 設定条件

- マルチキャスト・スタティックルーティングを利用する
- マルチキャストパケットの送信元アドレスは 192.168.1.2 とする
- マルチキャストパケットのグループアドレスは 239.255.1.1 とする

【本装置1】

- マルチキャストパケットを転送するインターフェースとして LAN0、LAN1、LAN2 を使用し、それぞれ、ETHER1、ETHER2、ETHER3 に割り当てる
- LAN0のIPアドレス : 192.168.1.1/24
- LAN1のIPアドレス : 192.168.2.1/24
- LAN2のIPアドレス : 192.168.3.1/24

【本装置2】

- マルチキャストパケットを転送するインターフェースとして LAN0、LAN1 を使用し、それぞれ、ETHER1、ETHER2 に割り当てる
- LAN0のIPアドレス : 192.168.4.1/24
- LAN1のIPアドレス : 192.168.2.2/24

[本装置 3]

- マルチキャストパケットを転送するインタフェースとして LAN0, LAN1 を使用し、それぞれ、ETHER1、ETHER2 に割り当てる
- LAN0 の IP アドレス : 192.168.5.1/24
- LAN1 の IP アドレス : 192.168.3.2/24

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]

```

ETHER ポートを削除する
# delete ether

LAN インタフェースを削除する
# delete lan

ETHER1～3 ポートを設定する
# ether 1 vlan untag 1
# ether 2 vlan untag 2
# ether 3 vlan untag 3

192.168.1.0/24 のネットワークを設定する
# lan 0 vlan 1
# lan 0 ip address 192.168.1.1/24 3
# lan 0 ip multicast mode static

192.168.2.0/24 のネットワークを設定する
# lan 1 vlan 2
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ip multicast mode static

192.168.3.0/24 のネットワークを設定する
# lan 2 vlan 3
# lan 2 ip address 192.168.3.1/24 3
# lan 2 ip multicast mode static

マルチキャスト・スタティックルーティングの設定をする
# multicast ip route 0 static 192.168.1.2 239.255.1.1 lan0 lan1-lan2

設定終了
# save
# commit
    
```

[本装置 2]

```
ETHER ポートを削除する
# delete ether

LAN インタフェースを削除する
# delete lan

ETHER1、2 ポートを設定する
# ether 1 vlan untag 1
# ether 2 vlan untag 2

192.168.4.0/24 のネットワークを設定する
# lan 0 vlan 1
# lan 0 ip address 192.168.4.1/24 3
# lan 0 ip multicast mode static

192.168.2.0/24 のネットワークを設定する
# lan 1 vlan 2
# lan 1 ip address 192.168.2.2/24 3
# lan 1 ip multicast mode static

マルチキャスト・スタティックルーティングの設定をする
# multicast ip route 0 static 192.168.1.2 239.255.1.1 lan1 lan0

設定終了
# save
# commit
```

[本装置 3]

```
ETHER ポートを削除する
# delete ether

LAN インタフェースを削除する
# delete lan

ETHER1、2 ポートを設定する
# ether 1 vlan untag 1
# ether 2 vlan untag 2

192.168.5.0/24 のネットワークを設定する
# lan 0 vlan 1
# lan 0 ip address 192.168.5.1/24 3
# lan 0 ip multicast mode static

192.168.3.0/24 のネットワークを設定する
# lan 1 vlan 2
# lan 1 ip address 192.168.3.2/24 3
# lan 1 ip multicast mode static

マルチキャスト・スタティックルーティングの設定をする
# multicast ip route 0 static 192.168.1.2 239.255.1.1 lan1 lan0

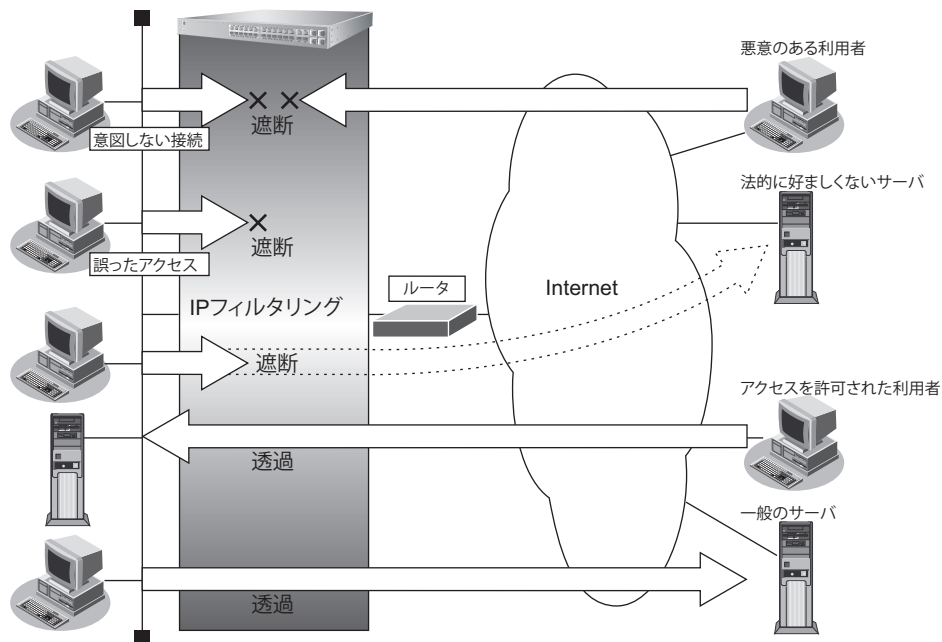
設定終了
# save
# commit
```

29 IP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。

☞ 参照 マニュアル「機能説明書」



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。

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 フィルタリングでDHCP（ポート番号 67、68）でのアクセスを制限する設定を行った場合、DHCP 機能が使用できなくなる場合があります。
 - 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。
-

29.1 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。



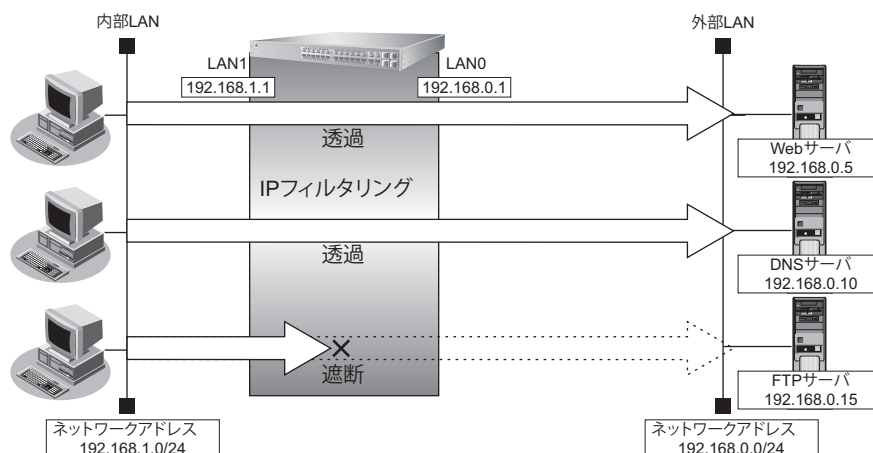
DNSサーバに問い合わせが発生する場合、DNSサーバへのアクセスを許可する必要があります。DNSサーバへのアクセスを許可することによって、Webサービス以外でドメイン名を指定した場合もDNSサーバへの発信が発生します。あらかじめ接続するWebサーバが決まっている場合は、本装置のDNSサーバ機能を利用することによって、DNSサーバへの発信を抑制することができます。

こんな事に気をつけて

SR-S312LE1/320LE1/324LE1では、以下の機能を同時に使用することができません。

IPフィルタリング機能(IPv4)を有効にするためには、"resource filter distribution filter ipv4"を設定する必要があります。

- MACフィルタ機能 (IPv4) / IPフィルタリング機能 (IPv4)
- MACフィルタ機能 (IPv6フィルタ) / IPフィルタリング機能 (IPv6)
- 優先制御情報書き換え機能 (IPv4) / DSCP値書き換え機能 (IPv4)
- 優先制御情報書き換え機能 (IPv6) / DSCP値書き換え機能 (IPv6)



● 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
- 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

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
```

DNS サーバのポート 53 への UDP パケットを透過させる

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

ICMP のパケットを透過させる

```
# acl 2 ip any any 1 any
# lan 1 ip filter 2 pass acl 2
```

残りのパケットをすべて遮断する

```
# acl 3 ip any any any any
# lan 1 ip filter 3 reject acl 3
```

設定終了

```
# save
# commit
```

29.2 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)

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。



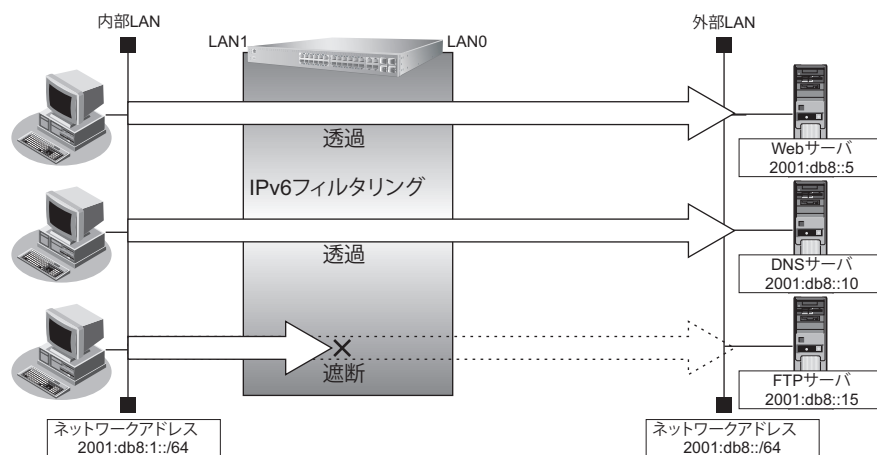
DNS サーバに問い合わせが発生する場合、DNS サーバへのアクセスを許可する必要があります。DNS サーバへのアクセスを許可することによって、Web サービス以外でドメイン名を指定した場合も DNS サーバへの発信が発生します。あらかじめ接続する Web サーバが決まっている場合は、本装置の DNS サーバ機能を利用することによって、DNS サーバへの発信を抑止することができます。

こんな事に気をつけて

SR-S312LE1/320LE1/324LE1 では、以下の機能を同時に使用することができません。

IP フィルタリング機能 (IPv6) を有効にするためには、"resource filter distribution filter ipv6" を設定する必要があります。

- MAC フィルタ機能 (IPv4) / IP フィルタリング機能 (IPv4)
- MAC フィルタ機能 (IPv6 フィルタ) / IP フィルタリング機能 (IPv6)
- 優先制御情報書き換え機能 (IPv4) / DSCP 値書き換え機能 (IPv4)
- 優先制御情報書き換え機能 (IPv6) / DSCP 値書き換え機能 (IPv6)



● 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

こんな事に気をつけて

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

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 ip6 2001:db8:1::/64 any 6 any
# acl 0 tcp any 80
# lan 1 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

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

ICMPv6 のパケットを透過させる

```
# acl 2 ip6 any any 58
# acl 2 icmp any any
# lan 1 ip6 filter 2 pass acl 2
```

残りのパケットをすべて遮断する

```
# acl 3 ip6 any any any any
# lan 1 ip6 filter 3 reject acl 3
```

設定終了

```
# save
# commit
```


29.3 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。



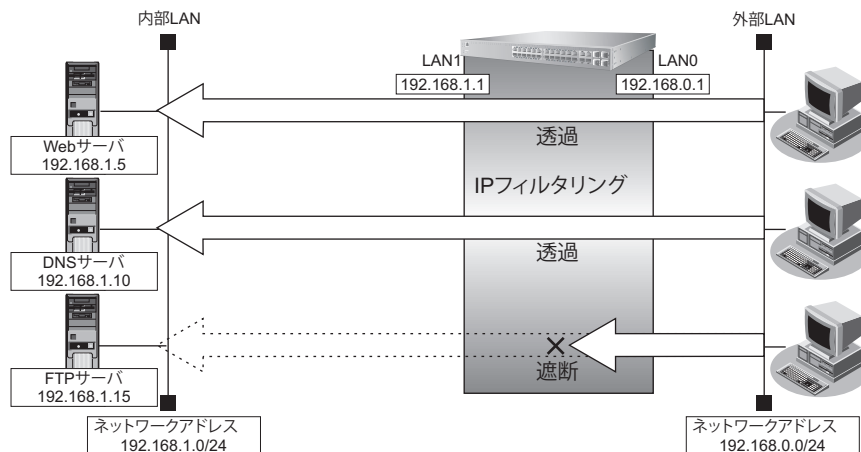
DNSサーバに問い合わせが発生する場合、DNSサーバへのアクセスを許可する必要があります。DNSサーバへのアクセスを許可することによって、Webサービス以外でもドメイン名で指定されるとDNSサーバへの問い合わせが発生します。あらかじめ接続するWebサーバが決まっている場合は、本装置のDNSサーバ機能を利用することで、DNSサーバへの問い合わせを抑制することができます。

こんな事に気をつけて

SR-S312LE1/320LE1/324LE1では、以下の機能を同時に使用することができません。

IPフィルタリング機能 (IPv4) を有効にするためには、"resource filter distribution filter ipv4" を設定する必要があります。

- MACフィルタ機能 (IPv4) / IPフィルタリング機能 (IPv4)
- MACフィルタ機能 (IPv6フィルタ) / IPフィルタリング機能 (IPv6)
- 優先制御情報書き換え機能 (IPv4) / DSCP値書き換え機能 (IPv4)
- 優先制御情報書き換え機能 (IPv6) / DSCP値書き換え機能 (IPv6)



● 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
- 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

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

LAN 上のホストのポート 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 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

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

ICMP のパケットを透過させる

```
# acl 2 ip any any 1 any
# lan 0 ip filter 2 pass acl 2
```

残りのパケットをすべて遮断する

```
# acl 3 ip any any any any
# lan 0 ip filter 3 reject acl 3
```

設定終了

```
# save
# commit
```

29.4 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

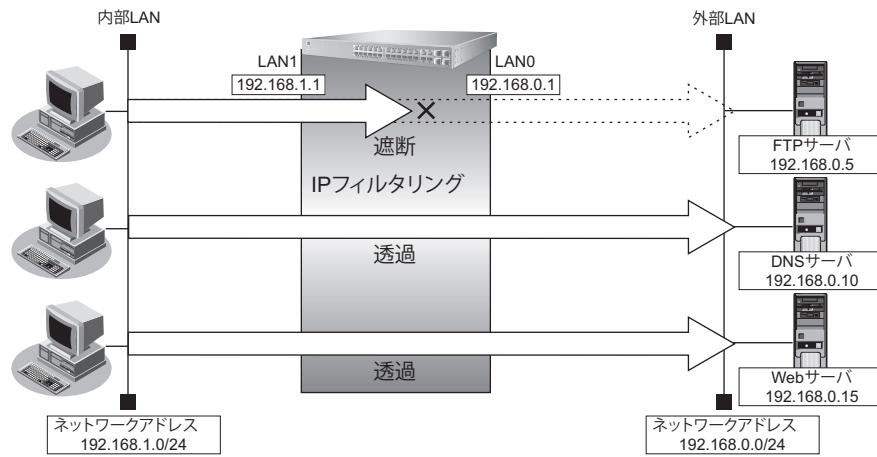
ここでは、外部LANのFTPサーバに対するアクセスを禁止する場合の設定方法を説明します。

こんな事に気をつけて

SR-S312LE1/320LE1/324LE1 では、以下の機能を同時に使用することができません。

IPフィルタリング機能 (IPv4) を有効にするためには、"resource filter distribution filter ipv4" を設定する必要があります。

- MACフィルタ機能 (IPv4) / IPフィルタリング機能 (IPv4)
- MACフィルタ機能 (IPv6フィルタ) / IPフィルタリング機能 (IPv6)
- 優先制御情報書き換え機能 (IPv4) / DSCP値書き換え機能 (IPv4)
- 優先制御情報書き換え機能 (IPv6) / DSCP値書き換え機能 (IPv6)



● 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
```

29.5 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

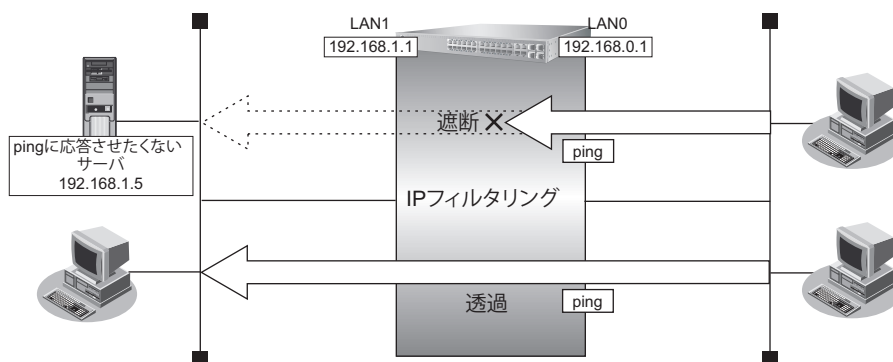
ここでは、内部LANの特定のサーバに対する ping (ICMP ECHO) を禁止し、この特定のサーバに対するほかの ICMP パケット、その他のプロトコルのパケットおよびほかのホストに対するパケットはすべて許可する場合の設定方法を説明します。

こんな事に気をつけて

SR-S312LE1/320LE1/324LE1 では、以下の機能を同時に使用することができません。

IP フィルタリング機能 (IPv4) を有効にするためには、"resource filter distribution filter ipv4" を設定する必要があります。

- MAC フィルタ機能 (IPv4) / IP フィルタリング機能 (IPv4)
- MAC フィルタ機能 (IPv6 フィルタ) / IP フィルタリング機能 (IPv6)
- 優先制御情報書き換え機能 (IPv4) / DSCP 値書き換え機能 (IPv4)
- 優先制御情報書き換え機能 (IPv6) / DSCP 値書き換え機能 (IPv6)



● フィルタリング設計

- 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 0 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 0 ip filter 1 pass acl 1
```

```
設定終了
# save
# commit
```

30 DSCP 値書き換え機能を使う

適用機種 全機種

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事ができます。

☞ 参照 マニュアル「機能説明書」

こんな事に気をつけて

SR-S312LE1/320LE1/324LE1では、以下の機能を同時に使用することができません。

DSCP 値書き換え機能 (IPv4) を有効にするためには、"resource filter distribution qos ipv4" を設定する必要があります。

- MACフィルタ機能 (IPv4) / IPフィルタリング機能 (IPv4)
- MACフィルタ機能 (IPv6フィルタ) / IPフィルタリング機能 (IPv6)
- 優先制御情報書き換え機能 (IPv4) / DSCP 値書き換え機能 (IPv4)
- 優先制御情報書き換え機能 (IPv6) / DSCP 値書き換え機能 (IPv6)

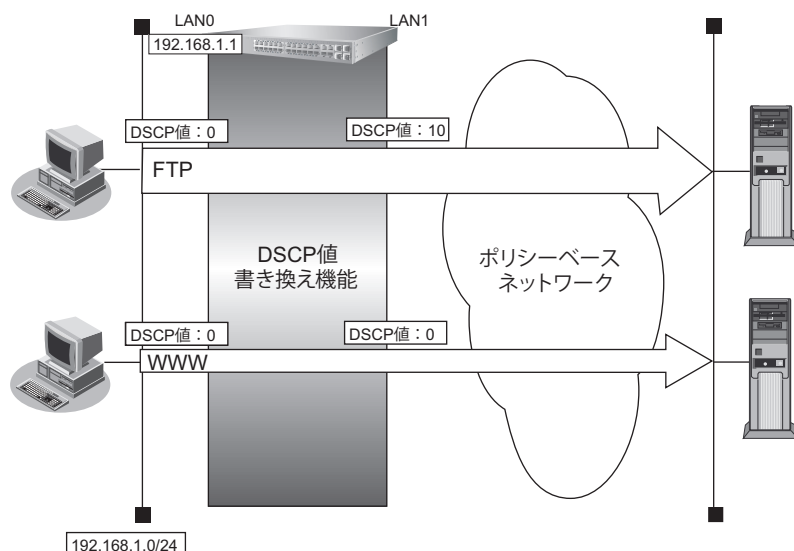
DSCP 値書き換え機能の条件

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 (全機種)
または、
IPv6パケットのTraffic Class値またはDSCP値 (全機種)

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
```

31 VRRP 機能を使う

適用機種 SR-S732TR1, 752TR1

VRRP 機能は2つ以上のルータがグループを形成し、1台のルータ（仮想ルータ）のように動作します。グループ内の各ルータには優先度が設定されており、その優先度に従ってマスタールータ（実際に経路情報を処理する装置）とバックアップルータ（マスタールータで異常を検出したときに経路情報の処理を引き継ぐ装置）を決定します。本装置には、以下のVRRP 機能があります。

- 簡易ホットスタンバイ機能
動的に経路制御（RIP など）できない端末から、別のネットワークへの通信に使用しているルータがなんらかの理由で中継できなくなった場合、自動でほかのルータが通信をバックアップします。
- クラスタリング機能
VRRP のグループを複数設定することで、通信の負荷分散と冗長構成を実現します。本装置では、2台のルータを組み合わせることで簡易ホットスタンバイによる信頼性の高い通信を実現できます。

☞ 参照 マニュアル「機能説明書」

こんな事に気をつけて

- 本装置の電源の投入、マスタールータでの設定反映、または装置リセットを実行した場合、バックアップルータがマスタールータとなることがあります。プリエンプトモードが on の場合は自動で切り戻りますが、プリエンプトモードが off の場合は、vrrp preempt-permit コマンドで切り戻しを行う必要があります。
- 優先度の値が大きい方が優先的にマスタールータとなります。
- LAN に接続される装置はデフォルトルートとして仮想 IP アドレスを設定してください。
- VRRP 機能では、VRRP-AD メッセージに以下のパケットを使用します。IP フィルタ設定時には、このパケットを遮断しないように設定する必要があります。

IPv4-VRRP

あて先 IP アドレス: 224.0.0.18

プロトコル番号: 112

IPv6-VRRP

あて先 IP アドレス: ff02::12

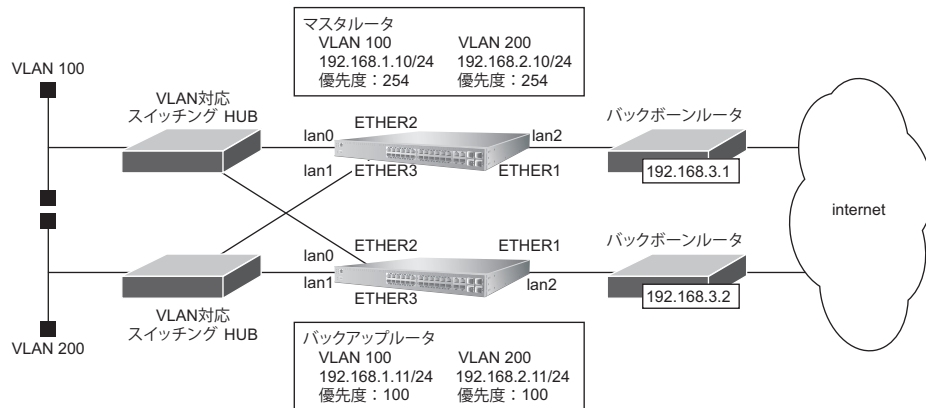
IPv6 Next Header: 112

31.1 簡易ホットスタンバイ機能を使う

適用機種 SR-S732TR1, 752TR1

本装置では、2台のルータを組み合わせることで簡易ホットスタンバイ機能による信頼性の高い通信を実現することができます。

ここでは、インターネット側へはバックボーンルータを経由、ローカルLAN側をVLAN構成とする場合の設定方法を説明します。



● 設定条件

- ・ 障害発生後の切り戻しは手動で行う
- ・ マスタルータはインターネット側経路をノードダウントリガによって監視する

[VLAN 100]

- ・ グループ ID : 10
- ・ 仮想 IP アドレス : 192.168.1.1

[VLAN 200]

- ・ グループ ID : 20
- ・ 仮想 IP アドレス : 192.168.2.1

[マスタルータ]

- ・ バックボーンルータへの接続ポート : ETHER1 ポート
- ・ VLAN 100 への接続ポート : ETHER2 ポート
- ・ VLAN 200 への接続ポート : ETHER3 ポート
- ・ 本装置の IP アドレス/ネットマスク : 192.168.1.10/24
- ・ ノードダウントリガの監視 IP アドレス : 202.168.2.1 (プロバイダ側の DNS サーバアドレスなど)

[バックアップルータ]

- ・ バックボーンルータへの接続ポート : ETHER1 ポート
- ・ VLAN 100 への接続ポート : ETHER2 ポート
- ・ VLAN 200 への接続ポート : ETHER3 ポート
- ・ 本装置の IP アドレス/ネットマスク : 192.168.1.11/24

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**[マスタールータの設定]**

物理ポート/VLANを設定する

```
# ether 1 vlan untag 10
# ether 2 vlan tag 100
# ether 3 vlan tag 200
# lan 0 vlan 100
# lan 1 vlan 200
# lan 2 vlan 10
```

STP機能を無効に設定する

```
# stp mode disable
```

ルーティング機能を有効に設定する

```
# ip routing enable
```

本装置のIPアドレスを設定する (DNSサーバアドレスへのスタティック経路を設定する)

```
# lan 0 ip address 192.168.1.10/24 3
# lan 1 ip address 192.168.2.10/24 3
# lan 2 ip address 192.168.3.10/24 3
# lan 2 ip route 0 default 192.168.3.1
```

VRRPを設定する (ノードダウントリガを使用する)

```
# lan 0 vrrp use on
# lan 0 vrrp group 0 id 10 254 192.168.1.1
# lan 0 vrrp group 0 preempt off
# lan 0 vrrp group 0 trigger 0 node 202.168.2.1 any
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 20 254 192.168.2.1
# lan 1 vrrp group 0 preempt off
# lan 1 vrrp group 0 trigger 0 node 202.168.2.1 any
```

設定終了

```
# save
```

設定反映

```
# reset
```

本設定で、インタフェースダウントリガを使用してバックボーンルータ側インタフェース状態を監視する場合は、以下の設定を追加します。

● コマンド**[マスタールータの設定]**

```
# lan 0 vrrp group 0 trigger 1 ifdown lan2
# lan 1 vrrp group 0 trigger 1 ifdown lan2
```

[バックアップルータの設定]

物理ポート/VLANを設定する

```
# ether 1 vlan untag 10
# ether 2 vlan tag 100
# ether 3 vlan tag 200
# lan 0 vlan 100
# lan 1 vlan 200
# lan 2 vlan 10
```

STP機能を無効に設定する

```
# stp mode disable
```

ルーティング機能を有効に設定する

```
# ip routing enable
```

本装置のIPアドレスを設定する

```
# lan 0 ip address 192.168.1.11/24 3
# lan 1 ip address 192.168.2.11/24 3
# lan 2 ip address 192.168.3.11/24 3
# lan 2 ip route 0 default 192.168.3.2
```

VRRPを設定する

```
# lan 0 vrrp use on
# lan 0 vrrp group 0 id 10 100 192.168.1.1
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 20 100 192.168.2.1
```

設定終了

```
# save
```

設定反映

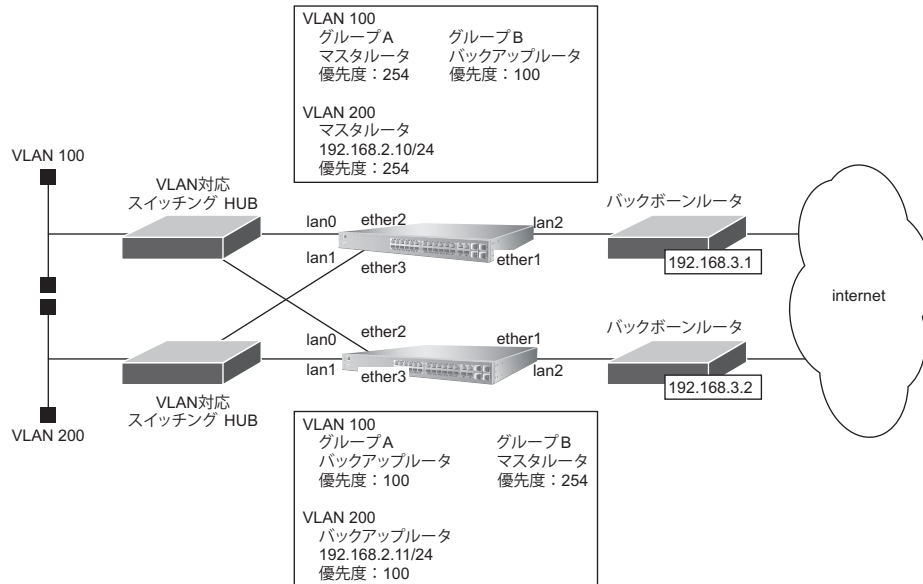
```
# reset
```

31.2 クラスタリング機能を使う

適用機種 SR-S732TR1, 752TR1

本装置では、2台のルータに複数のグループIDを設定することで、信頼性を高めると同時に通信の負荷分散を実現できます。

ここでは、インターネット側へはバックボーンルータを経由、ローカルLAN側をVLAN構成とする場合の設定方法を説明します（VLAN 100のみクラスタリング機能を使用する）。



● 設定条件

- 故障発生後の切り戻しは手動で行う
- マスタールータはバックボーンルータ側のインタフェースをインタフェースダウントリガにより監視する

[VLAN 100]

- [グループA]
 - グループID : 10
 - 仮想IPアドレス : 192.168.1.1
- [グループB]
 - グループID : 11
 - 仮想IPアドレス : 192.168.1.2

[VLAN 200]

- グループID : 20
- 仮想IPアドレス : 192.168.2.1

[マスタールータ]

- バックボーンルータへの接続ポート : ETHER1 ポート
- VLAN 100 への接続ポート : ETHER2 ポート
- VLAN 200 への接続ポート : ETHER3 ポート
- 本装置のIPアドレス/ネットマスク : 192.168.1.10/24

[バックアップルータ]

- バックボーンルータへの接続ポート : ETHER1 ポート
- VLAN 100 への接続ポート : ETHER2 ポート
- VLAN 200 への接続ポート : ETHER3 ポート
- 本装置の IP アドレス/ネットマスク : 192.168.1.11/24

こんな事に気をつけて

クラスティング機能を有効に利用するには、端末からのトラフィック量に応じて、端末側で設定するデフォルトルートの定義を適切に分散してください。

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

[マスタルータの設定]

物理ポート/VLAN を設定する

```
# ether 1 vlan untag 10
# ether 2 vlan tag 100
# ether 3 vlan tag 200
# lan 0 vlan 100
# lan 1 vlan 200
# lan 2 vlan 10
```

STP 機能を無効に設定する

```
# stp mode disable
```

ルーティング機能を有効に設定する

```
# ip routing enable
```

本装置の IP アドレスを設定する

```
# lan 0 ip address 192.168.1.10/24 3
# lan 1 ip address 192.168.2.10/24 3
# lan 2 ip address 192.168.3.10/24 3
# lan 2 ip route 0 default 192.168.3.1
```

VRRP を設定する (インタフェースダウントリガを使用する)

```
# lan 0 vrrp use on
# lan 0 vrrp group 0 id 10 254 192.168.1.1
# lan 0 vrrp group 0 preempt off
# lan 0 vrrp group 0 trigger 0 ifdown lan2 254
# lan 0 vrrp group 1 id 11 100 192.168.1.2
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 20 254 192.168.2.1
# lan 1 vrrp group 0 preempt off
# lan 1 vrrp group 0 trigger 0 ifdown lan2 254
```

設定終了

```
# save
```

設定反映

```
# reset
```

[バックアップルータの設定]

物理ポート/VLANを設定する

```
# ether 1 vlan untag 10
# ether 2 vlan tag 100
# ether 3 vlan tag 200
# lan 0 vlan 100
# lan 1 vlan 200
# lan 2 vlan 10
```

STP機能を無効に設定する

```
# stp mode disable
```

ルーティング機能を有効に設定する

```
# ip routing enable
```

本装置のIPアドレスを設定する

```
# lan 0 ip address 192.168.1.11/24 3
# lan 1 ip address 192.168.2.11/24 3
# lan 2 ip address 192.168.3.11/24 3
# lan 2 ip route 0 default 192.168.3.2
```

VRRPを設定する

```
# lan 0 vrrp use on
# lan 0 vrrp group 0 id 10 100 192.168.1.1
# lan 0 vrrp group 1 id 11 254 192.168.1.2
# lan 0 vrrp group 1 preempt off
# lan 0 vrrp group 1 trigger 0 ifdown lan2 254
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 20 100 192.168.2.1
```

設定終了

```
# save
```

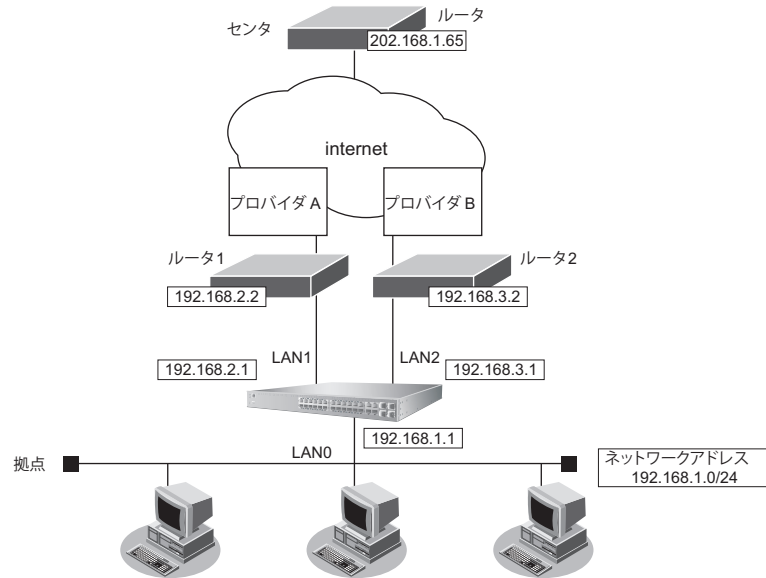
設定反映

```
# reset
```

32 ECMP 機能を使う

適用機種 SR-S732TR1, 752TR1

ここでは、ECMP 機能を利用した負荷分散通信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」

● 設定条件

- 拠点では、センタへの通信は、ルータ1とルータ2を利用して負荷分散して送信します。

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

```
ETHER15でルータ1、ETHER16でルータ2と接続し、残りのETHERを端末との接続に使用する
すべてのETHERをタグなしとする
# ether 1-14 vlan untag 10
# lan 0 vlan 10
# ether 15 vlan untag 11
# lan 1 vlan 11
# ether 16 vlan untag 12
# lan 2 vlan 12

LANのIPアドレスを設定する
# lan 0 ip address 192.168.1.1/24 3
# lan 1 ip address 192.168.2.1/24 3
# lan 2 ip address 192.168.3.1/24 3

経路を設定する
# lan 1 ip route 202.168.1.0/24 192.168.2.2 1 1
# lan 2 ip route 202.168.1.0/24 192.168.3.2 1 1

ECMPを設定する
# routemanage ip ecmp mode hash
```


```
設定終了  
# save  
# commit
```

33 DHCP機能を使う

適用機種 全機種

本装置のDHCPには、以下の機能があります。

- DHCPサーバ機能
- DHCPスタティック機能
- DHCPリレーエージェント機能 (SR-S732TR1/752TR1のみ)

 **参照** マニュアル「機能説明書」

本装置では、それぞれのインタフェースでDHCP機能が使用できます。

こんな事に気をつけて

- 1つのインタフェースでは、1つの機能だけ動作します。同時に複数の機能を動作することはできません。
- 本装置のDHCPサーバは、リレーエージェントを経由して運用することはできません。

33.1 DHCPサーバ機能を使う

適用機種 全機種

DHCPサーバ機能は、ネットワークに接続されているパソコンに対して、IPアドレスの自動割り当てを行う機能です。管理者はパソコンが増えるたびにIPアドレスが重複しないように設定する必要があります。

この機能を利用すると、DHCPクライアント機能を持つパソコンはIPアドレスの設定が不要になり、管理者の手間を大幅に省くことができます。

本装置のDHCPサーバ機能は、以下の情報を広報することができます。

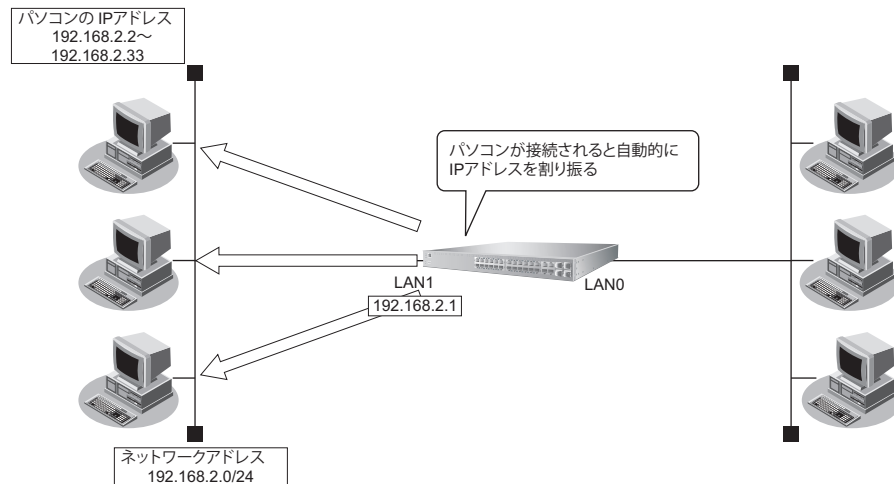
- IPアドレス
- ネットマスク
- リース期間
- デフォルトルータのIPアドレス
- DNSサーバのIPアドレス
- ドメイン名

こんな事に気をつけて

本装置のDHCPサーバ機能は、DHCPリレーエージェントのサーバにはなれません。

ここでは、SR-S732TR1 の場合を例にして、DHCP サーバ機能を使用する場合の設定方法を説明します。

補足 DHCP サーバ機能で割り当てることのできる IP アドレスの最大数は 253 個です。



● 前提条件

- LAN0 が設定されている
- LAN1 は VLAN が設定されている

● 設定条件

- 本装置の IP アドレス : 192.168.2.1
- ブロードキャストアドレス : 3 (ネットワークアドレス+オール1)
- パソコンに割り当てる IP アドレス : 192.168.2.2 ~ 192.168.2.33
- パソコンに割り当て可能 IP アドレス数 : 32
- ネットワークアドレス/ネットマスク : 192.168.2.0/24
- DHCP サーバ機能を使用する

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

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

DHCP サーバ機能を設定する
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ip dhcp info dns 192.168.2.1
# lan 1 ip dhcp info address 192.168.2.2/24 32
# lan 1 ip dhcp info time 1d
# lan 1 ip dhcp info gateway 192.168.2.1
# lan 1 ip dhcp service server

設定終了
# save
# commit
```

33.2 DHCP スタティック機能を使う

適用機種 全機種

DHCP サーバは、使用していない IP アドレスを一定期間（またはパソコンが IP アドレスを返却するまで）割り当てます。不要になった IP アドレスは自動的に再利用されるため、パソコンの IP アドレスが変わることがあります。本装置では、IP アドレスと MAC アドレスを対応付けることによって、登録されたパソコンから DHCP 要求が発行されると、常に同じ IP アドレスを割り当てることができます。これを DHCP スタティック機能と言います。

DHCP スタティック機能を利用する場合は、ホストデータベース情報に IP アドレスと MAC アドレスを設定してください。

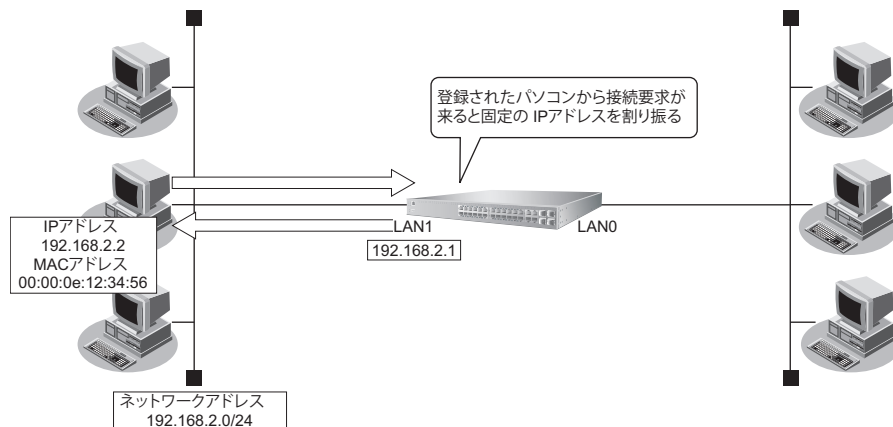


- MAC アドレスとは、LAN 機器に設定されていて世界中で重複されないように管理されている固有のアドレスです。
- 本装置がサポートしている IP フィルタリング機能などはパソコンの IP アドレスが固定されていないと使いにくい場合があります。これらの機能と DHCP サーバ機能の併用を実現するために、本装置では「DHCP スタティック機能」をサポートしています。

ここでは、SR-S732TR1 の場合を例にして、DHCP スタティック機能を使用する場合の設定方法を説明します。



- ホストデータベース情報は、「DHCP スタティック機能」、「DNS サーバ機能」で使われており、それぞれ必要な項目だけを設定します。
- DHCP スタティック機能で設定できるホストの最大数は 100 個です。



● 設定条件

- ネットワークアドレス/ネットマスク : 192.168.2.0/24
- IP アドレスを固定するパソコンの MAC アドレス : 00:00:0e:12:34:56
- 割り当て IP アドレス : 192.168.2.2
- DHCP サーバ機能を使用する

こんな事に気をつけて

DHCP サーバ機能を使用するコマンドを実行していない場合、DHCP スタティック機能の設定は無効となります。

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

VLAN を設定する

```
# ether 1 vlan untag 10
```

```
# lan 1 vlan 10
```

DHCP サーバ機能を設定する

```
# lan 1 ip address 192.168.2.1/24 3
```

```
# lan 1 ip dhcp info dns 192.168.2.1
```

```
# lan 1 ip dhcp info address 192.168.2.2/24 32
```

```
# lan 1 ip dhcp info time 1d
```

```
# lan 1 ip dhcp info gateway 192.168.2.1
```

```
# lan 1 ip dhcp service server
```

DHCP スタティック機能を設定する

```
# host 0 ip address 192.168.2.2
```

```
# host 0 mac 00:00:0e:12:34:56
```

設定終了

```
# save
```

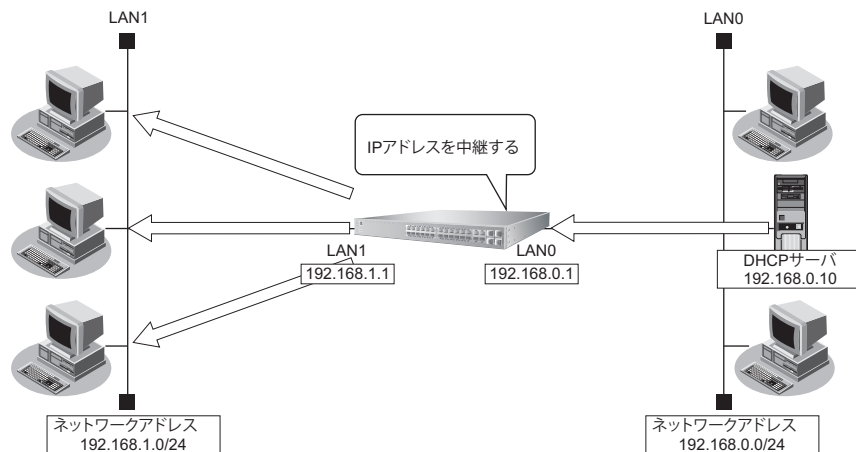
```
# commit
```

33.3 DHCP リレーエージェント機能を使う

適用機種 SR-S732TR1, 752TR1

DHCPクライアントは、同じネットワーク上にあるサーバから、IPアドレスなどの情報を獲得することができます。DHCPリレーエージェントは、遠隔地にあるDHCPクライアントの要求をDHCPサーバが配布する情報を中継する機能です。この機能を利用することで、遠隔地の別のネットワークにDHCPサーバが存在する場合も同様に情報を獲得することができます。

ここでは、DHCPリレーエージェント機能を使用する場合の設定方法を説明します。



● 前提条件

- LAN0が設定されている
- LAN1はVLANが設定されている

● 設定条件

[LAN1]

- 本装置のIPアドレス : 192.168.1.1
- DHCPリレーエージェント機能を使用する

[LAN0]

- 本装置のIPアドレス : 192.168.0.1
- DHCPサーバ : 192.168.0.10

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

```
VLANを設定する
# ether 1 vlan untag 10
# ether 2 vlan untag 20
# lan 0 vlan 10
# lan 1 vlan 20

本装置のIPアドレスを設定する
# lan 0 ip address 192.168.0.1/24 3
# lan 1 ip address 192.168.1.1/24 3
```

```
DHCP リレーエージェント機能を設定する  
# lan 1 ip dhcp service relay 192.168.0.10
```

```
設定終了  
# save  
# commit
```

33.4 IPv6 DHCP サーバ機能を使う

適用機種 全機種

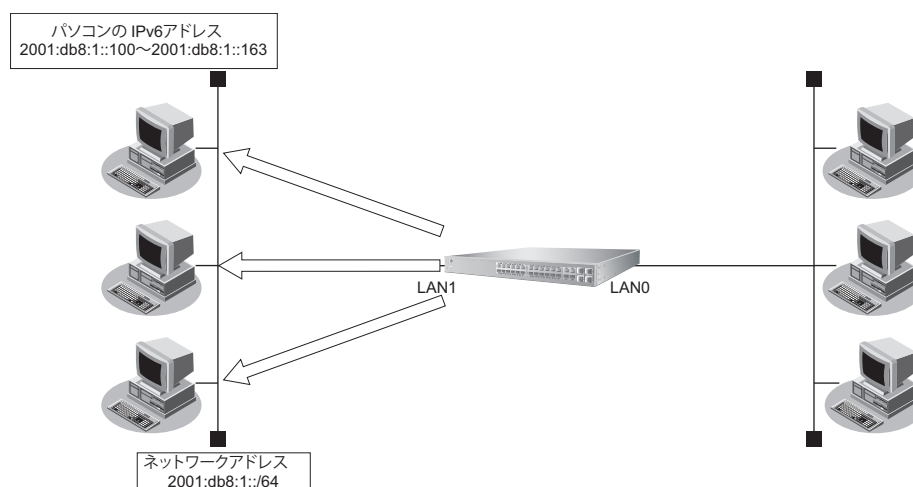
本装置のIPv6 DHCP サーバ機能は、以下の情報を広報することができます。

- IPv6 アドレス
- IPv6 プレフィックス
- DNS サーバのIPv6 アドレス
- DNS ドメイン名

こんな事に気をつけて

本装置のIPv6 DHCP サーバ機能は、IPv6 DHCP リレーエージェントのサーバにはなれません。

IPv6 DHCP サーバ機能を使用する場合の設定方法を説明します。



● 設定条件

- | | |
|--------------------------|-------------------------------------|
| • 本装置の IP アドレス | : 2001:db8:1::1 |
| • パソコンに割り当てる IPv6 アドレス | : 2001:db8:1::100 ~ 2001:db8:1::163 |
| • パソコンに割り当て可能 IPv6 アドレス数 | : 100 |
| • ネットワークアドレス/プレフィックス長 | : 2001:db8:1::/64 |
| • Valid Lifetime | : 30 日 |
| • Preferred Lifetime | : 7 日 |
| • DNS サーバの IPv6 アドレス | : 2001:db8:1::53 |

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

IPv6 DHCP サーバの動作するインタフェースを設定する

```
# lan 1 ip6 use on
```

```
# lan 1 ip6 address 0 2001:db8:1::1/64
```

IPv6 DHCP サーバ機能を設定する

```
# lan 1 ip6 dhcp service server
```

```
# lan 1 ip6 dhcp server info address 2001:db8:1::100 100 30d 7d
```

```
# lan 1 ip6 dhcp server info dns 2001:db8:1::53
```

設定終了

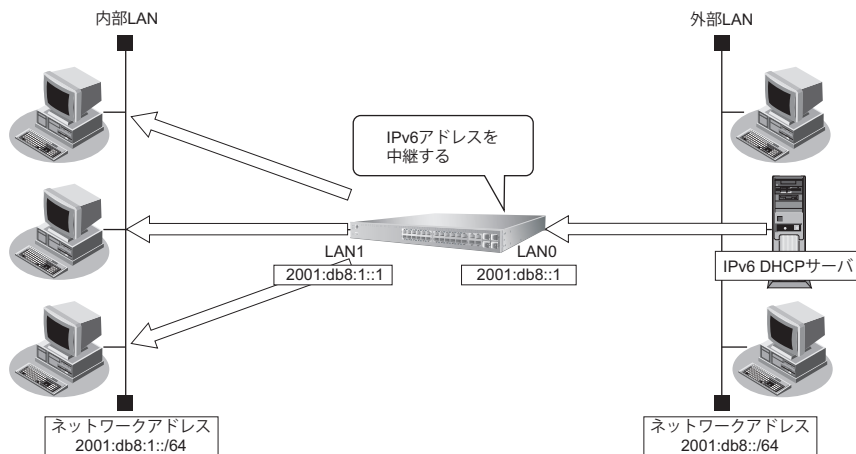
```
# save
```

```
# commit
```

33.5 IPv6 DHCP リレーエージェント機能を使う

適用機種 SR-S732TR1, 752TR1

ここでは、IPv6 DHCP リレーエージェント機能を使用する場合の設定方法を説明します。



● 設定条件

[内部 LAN 側]

- 本装置の IPv6 アドレス : 2001:db8:1::1
- IPv6 DHCP リレーエージェント機能を使用する

[外部 LAN 側]

- 本装置の IPv6 アドレス : 2001:db8::1

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

```

本装置のインタフェースを設定する
# lan 0 ip6 use on
# lan 0 ip6 address 0 2001:db8::1/64
# lan 1 ip6 use on
# lan 1 ip6 address 0 2001:db8:1::1/64
# lan 1 ip6 ra mode send
# lan 1 ip6 ra flags c0

IPv6 DHCP リレーエージェント機能を設定する
# lan 1 ip6 dhcp service relay
# lan 1 ip6 dhcp relay interface lan0

設定終了
# save
# commit
    
```


34 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。

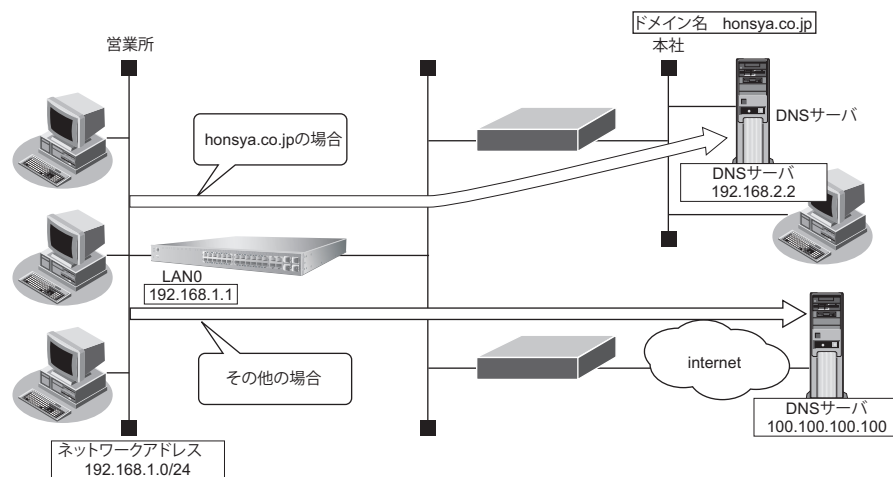
- DNS サーバの自動切り替え機能
- DNS 問い合わせタイプフィルタ機能
- DNS サーバ機能

☞ 参照 マニュアル「機能説明書」

34.1 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「コマンドユーザズガイド」

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
```

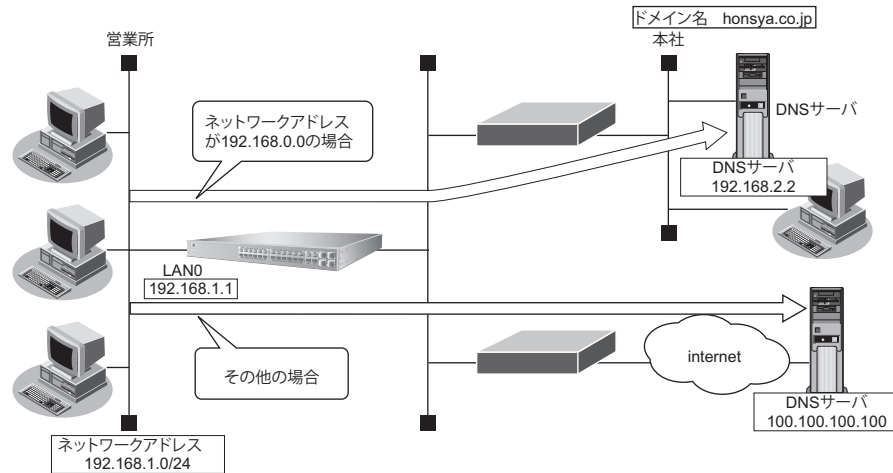
パソコン側の設定を確認する

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。

34.2 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「コマンドユーザズガイド」

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。

34.3 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」

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 10の場合を例に説明します。

1. [Windows ロゴ] ボタン、[Windows システムツール]、[コントロールパネル] の順にクリックします。
2. [ネットワークとインターネット] をクリックします。
3. [ネットワークと共有センター] をクリックします。
4. [アダプターの設定の変更] をクリックします。
5. [イーサネット] アイコンを右クリックし、[プロパティ] ボタンをクリックします。
[イーサネットのプロパティ] ダイアログボックスが表示されます。
6. 一覧から「インターネットプロトコルバージョン4 (TCP/IPv4)」を選択します。
7. [プロパティ] ボタンをクリックします。
[インターネットプロトコルバージョン4 (TCP/IPv4) のプロパティ] ダイアログボックスが表示されます。
8. 「次のDNS サーバーのアドレスを使う」を選択します。
9. 「優先DNS サーバー」に、本装置のIPアドレスを入力します。
10. [OK] ボタンをクリックします。
[イーサネットのプロパティ] ダイアログボックスに戻ります。
11. [閉じる] ボタンをクリックします。
設定した内容が有効になります。

34.4 DNS サーバ機能を使う

 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「コマンドユーザズガイド」


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
```

 ホストデータベース情報は「DHCPスタティック機能」、「DNSサーバ機能」で使われており、それぞれ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。

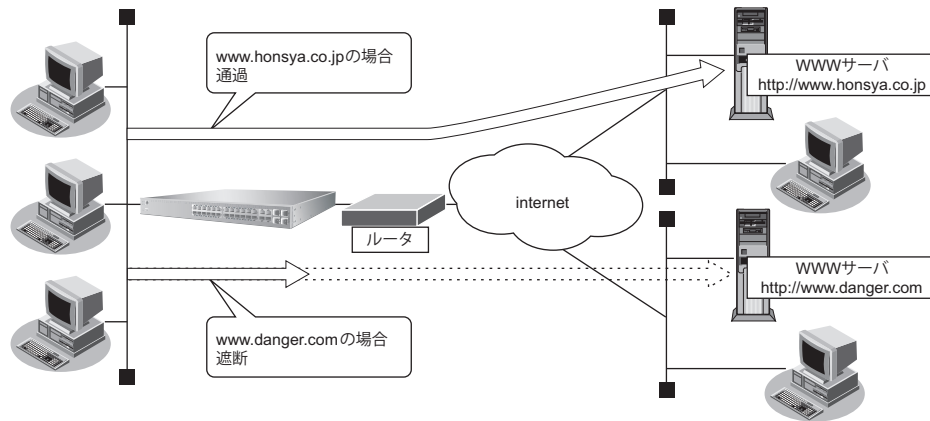
設定方法は、[「34.3DNS 問い合わせタイプフィルタ機能を使う」\(P.156\)](#) の「[パソコン側の設定を行う](#)」(P.157) を参照してください。

35 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」の「DNSサーバ機能」に関する記述

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」

💡 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**

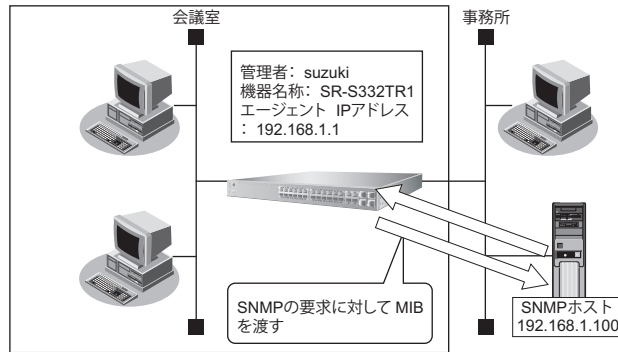
```
URL の情報を設定する
# proxydns domain 0 any www.danger.com any reject
# proxydns domain 1 any * any static 100.100.100.100

設定終了
# save
# commit
```

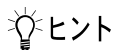

36 SNMP エージェント機能を使う

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」



◆ 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働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-S332TR1
- 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-S332TR1
# 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-S332TR1
- 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-S332TR1
# 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
```

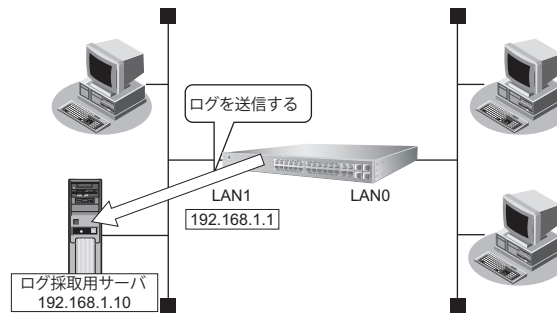
37 システムログを採取する

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syslog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）
- DHCP（配布したIPv4アドレス）

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
 - DHCP
 - 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 dhcp,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。

38 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「コマンドユーザズガイド」

38.1 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、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 0612010630 reset config2

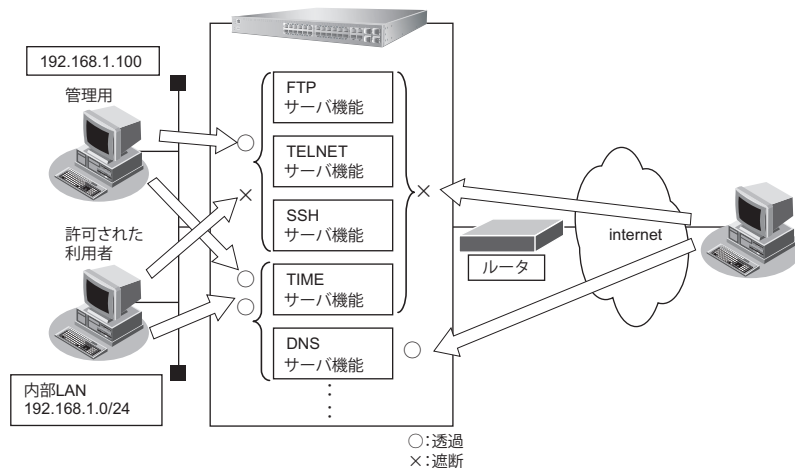
設定終了
# save
# commit
```

39 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
```

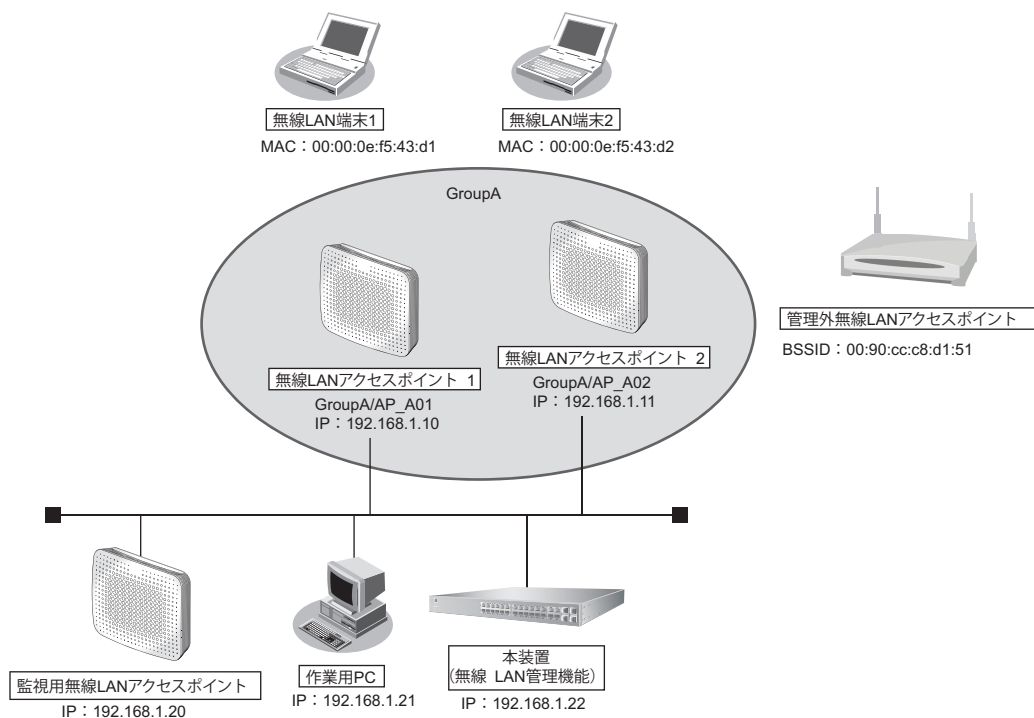
40 無線 LAN 管理機能を使う

適用機種 全機種

40.1 無線 LAN 管理機能の環境を設定する

適用機種 全機種

ここでは、複数の無線 LAN アクセスポイントによって構成されたネットワークを無線 LAN 管理機能で管理する場合の設定方法を説明します。



無線 LAN の監視を実施する場合は、1 台以上の無線 LAN アクセスポイントを監視用に設定してください。

無線 LAN 管理機能で監視できる無線 LAN チャンネルは、監視用に設定した無線 LAN アクセスポイントの周辺アクセスポイント検出機能の設定に依存します。周辺アクセスポイント検出機能の設定方法は、弊社製の無線 LAN アクセスポイント (SR-M50AP1/20AP1/20AP2) のマニュアルを参照してください。

こんな事に気をつけて

- 管理機器のログイン時の入力プロンプトは、システムデフォルトのままとしてください。管理機器のログイン時の入力プロンプトを変更された場合、無線 LAN 管理機器の動作は不定となります。
- 管理機器で nodemgr アカウントの情報を変更した場合、無線 LAN 管理機能の対応するアカウント情報も同時に変更するようにしてください。

● 設定条件

- 無線 LAN 管理対象
 - 管理グループ
 - グループ名 : GroupA
 - 無線 LAN アクセスポイント 1
 - 管理機器名 : AP_A01
 - IP アドレス : 192.168.1.10
 - アカウント : ユーザ ID : nodemgr、パスワード : nodemgr1
 - 無線 LAN アクセスポイント 2
 - 管理機器名 : AP_A02
 - IP アドレス : 192.168.1.11
 - アカウント : ユーザ ID : nodemgr、パスワード : nodemgr2
- 監視用無線 LAN アクセスポイント
 - 周辺アクセスポイント検出機能をスキャン専用モードで運用
 - 使用する無線 LAN モジュール : ieee80211 1、ieee80211 2
 - 管理機器名 : Watcher
 - IP アドレス : 192.168.1.20
 - 監視用アカウント : ユーザ ID : nodemgr、パスワード : nodemgr3
- 管理外無線 LAN アクセスポイント
 - MAC アドレス : 00:90:cc:c8:d1:51
- 管理情報取得の時間パラメタ (アクセスポイントモニタリング用)
 - 情報取得間隔 : 10 秒
 - 情報取得待機間隔 : 10 秒
 - 情報取得タイムアウト時間 : 5 秒
- 監視のパラメタ (アクセスポイントモニタリング用)
 - 有線 LAN
 - 稼動監視間隔 : 10 秒
 - 稼動監視待機間隔 : 10 秒
 - 稼動監視タイムアウト時間 : 5 秒
 - 稼動監視 通信異常判定しきい値 : 6 回
 - 無線 LAN
 - スキャンレポート取得間隔 : 10 秒
 - スキャンレポート取得待機間隔 : 10 秒
 - スキャンレポート取得タイムアウト時間 : 1 分
 - 無線 LAN 監視 通信異常判定しきい値 : 6 回
- 監視ログのパラメタ (アクセスポイントモニタリング/クライアントモニタリング用)
 - 監視ログ保持件数 : 100 件
- 無線 LAN 端末の RSSI 監視のパラメタ (クライアントモニタリング用)
 - RSSI 評価母数 : 10 個
 - RSSI 最低しきい値 : 20

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

```
管理グループを設定する
# nodemanager group 0 name GroupA

無線LAN アクセスポイントを設定する
# nodemanager node 0 name AP_A01
# nodemanager node 0 group 0
# nodemanager node 0 address 192.168.1.10
# nodemanager node 0 user nodemgr nodemgr1
# nodemanager node 0 wlan scan disable
# nodemanager node 1 name AP_A02
# nodemanager node 1 group 0
# nodemanager node 1 address 192.168.1.11
# nodemanager node 1 user nodemgr nodemgr2
# nodemanager node 1 wlan scan disable

監視用無線LAN アクセスポイントを設定する
# nodemanager node 4 name Watcher
# nodemanager node 4 address 192.168.1.20
# nodemanager node 4 user nodemgr nodemgr3
# nodemanager node 4 wlan scan enable
# nodemanager node 4 wlan sta disable

管理外無線LAN アクセスポイントを設定する
# nodemanager wlan scan unmanaged 0 UMAP01 00:90:cc:c8:d1:51

管理情報取得の時間パラメタを設定する
# nodemanager collect interval 10s 10s 5s

有線LAN、無線LANの監視パラメタを設定する
# nodemanager icmpwatch interval 10s 10s 5s
# nodemanager icmpwatch threshold 6
# nodemanager wlan scan interval 10s 10s 1m
# nodemanager wlan scan error threshold 6

監視ログのパラメタを設定する
# nodemanager log 100

無線LAN 端末のRSSI 監視のパラメタを設定する
# nodemanager wlan sta rssi 10 20

設定終了
# save
# commit
```

40.2 アクセスポイントモニタリングを行う

適用機種 全機種

無線LAN管理機能は、アクセスポイントモニタリングをすることができます。



- モニタリングは各管理機器にアクセスして収集した結果を出力していますので、構成定義の設定直後や、ネットワークの状況によっては収集が完了しておらず、途中の状態が表示される場合があります。この場合は、しばらく時間を置いたあと、再度モニタリング結果を表示してみてください。
- 使用目的が明確で管理不要な無線LANアクセスポイントを管理外無線LANアクセスポイントとして設定すると、不明無線LANアクセスポイントのモニタリングが容易となります。

ここでは、「[40.1 無線LAN管理機能の環境を設定する](#)」(P.168) で構築した環境に対するアクセスポイントモニタリングのコマンド例を示します。

☛ 参照 各コマンドの表示結果については、マニュアル「コマンドリファレンス」を参照してください。

● コマンド

管理無線LANアクセスポイントのモニタリング結果の一覧を表示する
show nodemanager logging wlan scan managed brief

管理無線LANアクセスポイントの有線LAN、無線LANのモニタリング結果を表示する
show nodemanager node node 0
show nodemanager node node 1

管理無線LANアクセスポイントの無線LANのモニタリング結果を表示する
show nodemanager logging wlan scan managed group 0

管理外無線LANアクセスポイントのモニタリング結果を表示する
show nodemanager logging wlan scan unmanaged

不明無線LANアクセスポイントのモニタリング結果を表示する
show nodemanager logging wlan scan unknown

監視ログを表示する
show nodemanager logging wlan scan

40.3 クライアントモニタリングを行う

適用機種 全機種

無線LAN管理機能は、無線LANアクセスポイントと接続している無線LAN端末のクライアントモニタリングをすることができます。



モニタリングは各管理機器にアクセスして収集した結果を出力していますので、構成定義の設定直後や、ネットワークの状況によっては収集が完了しておらず、途中の状態が表示される場合があります。この場合は、しばらく時間を置いたあと、再度モニタリング結果を表示してみてください。

ここでは、「[40.1 無線LAN管理機能の環境を設定する](#)」(P.168)で構築した環境に対するクライアントモニタリングのコマンド例を示します。

☛ 参照 各コマンドの表示結果については、マニュアル「コマンドリファレンス」を参照してください。

● コマンド

無線LAN端末の受信信号強度のモニタリング結果を表示する
show nodemanager logging wlan sta rssi group 0

無線LAN端末の接続状況をモニタリングする
show nodemanager logging wlan sta group 0

無線LAN端末の接続拒否情報をモニタリングする
show nodemanager logging wlan reject group 0

無線LANインタフェースのトレース情報をモニタリングする
show nodemanager logging wlan trace group 0

監視ログを表示する
show nodemanager logging wlan scan

40.4 無線 LAN アクセスポイントに MAC アドレスフィルタを配布する (MAC アドレスフィルタ配布)

適用機種 全機種

無線 LAN 管理機能は、無線 LAN アクセスポイントへの無線 LAN 端末の (MAC アドレスによる) 接続許可情報を一括管理して配布することができます。

補足 管理機器の MAC アドレスフィルタをクリアしたい場合は、MAC アドレスフィルタを設定していない MAC アドレスフィルタセットを配布してください。

● 設定条件

- 無線 LAN の接続を許可する端末
 - 無線 LAN 端末 1 (MAC アドレス : 00:00:0e:f5:43:d1)
 - 無線 LAN 端末 2 (MAC アドレス : 00:00:0e:f5:43:d2)
- 無線 LAN の接続を拒否する端末
 - 上記以外
- MAC アドレスフィルタの配布先
 - 無線 LAN アクセスポイント 1
 - 無線 LAN アクセスポイント 2

ここでは、「[40.1 無線 LAN 管理機能の環境を設定する](#)」(P.168) で構築した環境に対する MAC アドレスフィルタ配布のコマンド例を示します。

参照 各コマンドの実行結果については、マニュアル「コマンドリファレンス」を参照してください。

● コマンド

```
接続を許可する無線 LAN 端末の MAC アドレスを MAC アドレスフィルタに設定する
# nodemanager wlan filterset 0 filter 0 mac 00:00:0e:f5:43:d1 pass
# nodemanager wlan filterset 0 filter 0 description STATION_001
# nodemanager wlan filterset 0 filter 1 mac 00:00:0e:f5:43:d2 pass
# nodemanager wlan filterset 0 filter 1 description STATION_002
# nodemanager wlan filterset 0 filter 2 mac any reject
```

```
設定完了
# save
# commit
```

```
無線 LAN アクセスポイントに MAC アドレスフィルタを配布する
# nodemanagerctl update wlan filterset 0 group 0
```

40.5 無線 LAN アクセスポイントの電波出力を調整する (電波出力自動調整)

適用機種 全機種

無線 LAN 管理機能は、無線 LAN アクセスポイントの電波出力を調整することができます。



近隣管理機器には、電波出力自動調整機能で設定対象の無線 LAN アクセスポイントの無線を到達させたい無線 LAN アクセスポイントを設定します。ただし、電波出力自動調整による送信出力の調整には時間がかかりますので、必要以上に近隣管理機器を設定しないようにしてください。電波出力自動調整は、構成定義で設定した“電波自動調整の RSSI 最低しきい値”に近い値になるまで、以下の処理を繰り返します。

1. 近隣管理機器での周辺アクセスポイント情報の取得
必要時間：約 60 秒 × 近隣管理機器の台数
2. 電波出力の確認
RSSI 最低しきい値に近い値であれば終了
3. 無線 LAN アクセスポイントの無線送信出力の設定
必要時間：約 10 秒
4. 無線送信出力の安定待ち
必要時間：約 90 秒
5. 手順 1. の処理から繰り返し

こんな事に気をつけて

- 電波出力自動調整は、無線 LAN インタフェースの動作タイプが AP のみ (未設定を含む) で構成される無線 LAN アクセスポイントを対象とするようにしてください。
- 電波出力自動調整の近隣機器には、以下の条件を満たす無線 LAN アクセスポイントを指定してください。
 - 調整対象と同じ無線 LAN モジュールが動作している。
 - その無線 LAN モジュールの動作タイプは、AP、SCANONLY または未設定のみから構成される。
- 電波出力自動調整の実施中は、無線の状態が不安定になる可能性があります。よって、メンテナンスなどの通常運用時以外で電波出力自動調整を行うようにしてください。

● 設定条件

- 電波出力を調整する無線 LAN アクセスポイント
無線 LAN アクセスポイント 1
無線 LAN アクセスポイント 2
- 無線 LAN アクセスポイント 1 の近隣管理機器
無線 LAN アクセスポイント 2、監視用無線 LAN アクセスポイント
- 無線 LAN アクセスポイント 2 の近隣管理機器
無線 LAN アクセスポイント 1、監視用無線 LAN アクセスポイント
- 電波出力自動調整の RSSI の最低しきい値 : 20

ここでは、「[40.1 無線 LAN 管理機能の環境を設定する](#)」(P.168) で構築した環境に対する電波出力自動調整のコマンド例を示します。

☛ 参照 各コマンドの実行結果については、マニュアル「コマンドリファレンス」を参照してください。

● コマンド

近隣管理機器を設定する

```
# nodemanager node 0 wlan neighbor 1 4
```

```
# nodemanager node 1 wlan neighbor 0 4
```

電波出力自動調整のRSSIの最低しきい値を設定する

```
# nodemanager wlan autotxpower rssi 20
```

設定完了

```
# save
```

```
# commit
```

電波出力自動調整を行う

```
# nodemanagerctl wlan autotxpower group 0
```

40.6 無線 LAN アクセスポイントの無線 LAN チャンネルを調整する

適用機種 全機種

無線 LAN 管理機能は、無線 LAN アクセスポイントの無線 LAN チャンネルを自動的に調整することができます。

こんな事に気をつけて

無線 LAN チャンネル自動調整の実施中は、無線の状態が不安定になる可能性があります。よって、メンテナンスなどの通常運用時以外で無線 LAN チャンネル自動調整を行うようにしてください。

● 設定条件

- 5GHz 帯のチャンネル自動調整の割当範囲 : w52/53/56
- 2.4GHz 帯のチャンネル自動調整の判定用 RSSI しきい値 : 20
- 2.4GHz 帯のチャンネル自動調整のレイアウト
 - 開始チャンネル : 1
 - チャンネル割当間隔 : 5
- IEEE802.11n 通信時に使用する帯域幅 : 40

ここでは、[\[40.1 無線 LAN 管理機能の環境を設定する\]](#) (P.168) で構築した環境に対する無線 LAN チャンネル自動調整のコマンド例を示します。

☞ **参照** 各コマンドの実行結果については、マニュアル「コマンドリファレンス」を参照してください。

● コマンド

```
5GHz 帯のチャンネル自動調整の割当範囲を設定する
# nodemanager wlan autochannel channel w52/53/56

2.4GHz 帯のチャンネル自動調整の判定用 RSSI しきい値を設定する
# nodemanager wlan autochannel rssi 20

2.4GHz 帯のチャンネル自動調整のレイアウトを設定する
# nodemanager wlan autochannel layout 1 5

IEEE802.11n 通信時の通信帯域幅を設定する
# nodemanager wlan autochannel bandwidth 40

設定終了
# save
# commit

無線 LAN アクセスポイントの使用チャンネルを自動調整する
# nodemanagerctl wlan autochannel group 0
```


41 端末可視化機能を使う

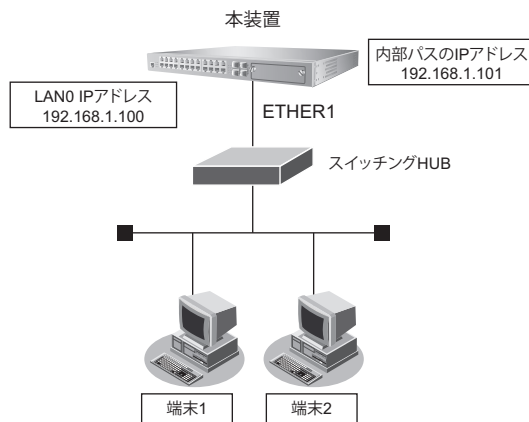
適用機種 SR-S332TR1, 352TR1, 732TR1, 752TR1

端末可視化機能を使用すると、ネットワーク上にどのような端末が接続されているかを詳細に把握することができます。

こんな事に気をつけて

- IPv4 を使用していないネットワーク上では端末情報を正しく検出できません。
- 本機能は ARP パケットを使用して端末の検出を行います。ARP パケットに応答しない機器は検出できません。
- 機器種別は本機能により推定した結果であり、実際の機器種別と異なる場合があります。
- ベンダー名、機器種別は、識別できない場合があります。
なお、識別したいベンダー名、機器種別は、ユーザが任意の識別情報を設定することも可能です。
- 本装置の OUI 辞書に登録されていない OUI を検出した場合、ベンダー名には "Unknown" と表示されます。
- 本機能では ASCII 文字以外は認識できません。検出した情報に認識できない文字が含まれる場合、"Unrecognized" と表示されます。
- IEEE802.1X 認証機能または不正端末アクセス防止機能 (MAC アドレス認証) 機能と本機能を併用する場合、認証されていない端末は検出できません。
- 本機能は装置内の内部バスを使用してパケットを監視するため、内部バスの設定が必要になります。
内部バスには本機能で可視化対象とする VLAN ID および IP アドレスを設定します。
- 接続する端末が、ランダムな MAC アドレスを使用する場合、以下の点に注意してください。
 - MAC アドレスが変更されるごとに、異なる端末として端末情報が収集されます。なお、一定時間を経過した端末情報を削除するには、devscan age コマンドを使用してください。
 - ベンダー名は識別されません。

SR-S332TR1 の場合を例にします。



● 設定条件

- VLAN10 で端末可視化機能を使用する
- LAN0 の VLAN ID : 10
- LAN0 の IP アドレス : 192.168.1.100
- 内部バスの VLAN ID : 10
- 内部バスの IP アドレス : 192.168.1.101
- 端末情報のエージングアウト時間 : 1 日

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
```

LAN0のIPアドレスを設定する

```
# lan 0 ip address 192.168.1.100/24 3
```

```
# lan 0 vlan 10
```

VLAN10で端末可視化機能を設定する

```
# devscan use on
```

```
# devscan vlan 10
```

内部パスインターフェースのVLANとIPアドレスを設定する

```
# internal-path 0 vlan 10
```

```
# internal-path 0 ip address 192.168.1.101/24 3
```

端末情報のエイジングアウト時間を1日に設定する

```
# devscan age 1d
```

設定終了

```
# save
```

```
# commit
```

42 NXconciierge と連携する

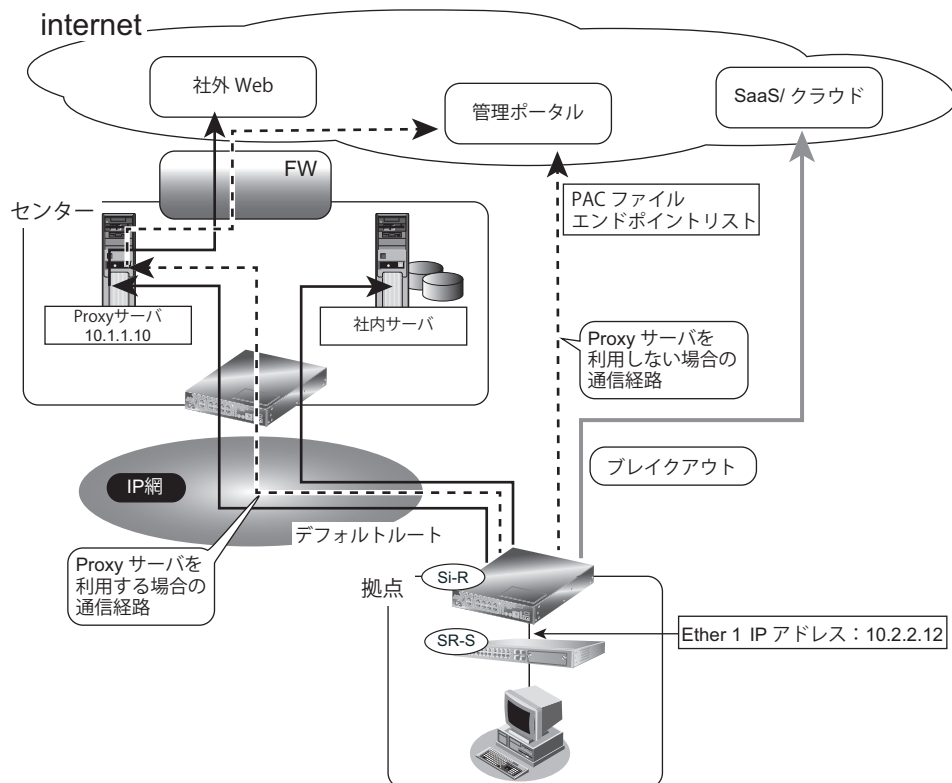
適用機種 SR-S332TR1, 352TR1, 732TR1, 752TR1

NXconciierge とは、ネットワーク機器を集中管理する Web アプリケーションサーバです。

本装置は、NXconciierge によるネットワーク機器の管理に対応したエージェント機能を搭載しており、NXconciierge と連携することで、ネットワーク経由で機器の集中管理を実現することができます。

こんな事に気をつけて

NXconciierge エージェント機能に割り当てる IP アドレスは、装置の物理ポートに割り当てた IP アドレスと同一のアドレスを設定します。



● 前提条件

- 時刻設定
 - 現在時刻が設定済み
- ルータから、管理ポータルへの経路は、ルータの設定に依存します。

エージェントと NXconciierge サーバとの通信時に Proxy サーバを利用する場合の設定方法を説明します。

● 設定条件

- LAN1 の VLAN ID : 10
- LAN1 の IP アドレス : 10.2.2.12
- デフォルトゲートウェイの IP アドレス : 10.2.2.2
- エージェントの IP アドレス : 10.2.2.12
- Proxy サーバの IP アドレス : 10.1.1.10
- SNMP 連携 : 有効
- 端末可視化機能 : 有効

● コマンド

ETHER1ポートを設定する

```
# ether 1 vlan untag 10
```

LANアドレスを設定する

```
# lan 0 ip address 10.2.2.12/24 3
```

```
# lan 0 vlan 10
```

```
# lan 0 ip route 0 default 10.2.2.2 1 1
```

SNMP連携を設定する

```
# snmp service on
```

```
# snmp agent address 10.2.2.12
```

```
# snmp manager 0 0.0.0.0 public off disable
```

端末可視化の設定

```
# internal-path 0 ip address 10.2.2.13/24 3
```

```
# internal-path 0 vlan 30
```

```
# devscan use on
```

```
# devscan vlan 30
```

```
# devscan scan-interval 1h
```

```
# devscan age 14d
```

```
# proxydns domain 0 any * any static 10.2.2.2
```

エージェント設定を行う

```
# management-agent mode agent
```

```
# management-agent tenantkey key
```

```
# management-agent serverlogin proxy address 10.1.1.10 8080
```

```
# management-agent serverlogin proxy auth send id pass
```

```
# management-agent ip address 10.2.2.12
```

次に、エージェントとNXconciergeサーバとの通信時にProxyサーバを利用せず、直接インターネット経由で通信する場合の設定方法を説明します。

● 設定条件

- LAN1のVLAN ID : 10
- LAN1のIPアドレス : 10.2.2.12
- デフォルトゲートウェイのIPアドレス : 10.2.2.2
- エージェントのIPアドレス : 10.2.2.12
- SNMP連携 : 有効
- 端末可視化機能 : 有効

● コマンド

ETHER1ポートを設定する

```
# ether 1 vlan untag 10
```

LANアドレスを設定する

```
# lan 0 ip address 10.2.2.12/24 3
```

```
# lan 0 vlan 10
```

```
# lan 0 ip route 0 default 10.2.2.2 1 1
```

SNMP連携を設定する

```
# snmp service on
```

```
# snmp agent address 10.2.2.12
```

```
# snmp manager 0 0.0.0.0 public off disable
```

端末可視化の設定

```
# internal-path 0 ip address 10.2.2.13/24 3
```

```
# internal-path 0 vlan 30
```

```
# devscan use on
```

```
# devscan vlan 30
```

```
# devscan scan-interval 1h
```

```
# devscan age 14d
```

```
# proxydns domain 0 any * any static 10.2.2.2
```

エージェント設定を行う

```
# management-agent mode agent
```

```
# management-agent tenantkey key
```

```
# management-agent ip address 10.2.2.12
```

43 装置を保護する

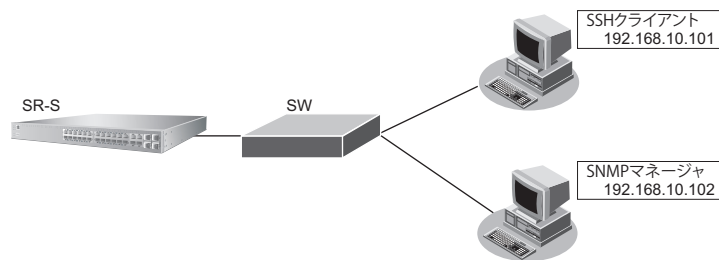
適用機種 全機種

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

43.1 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 : srs_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-S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srs_admin-2022に設定
# password admin set srs_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 snmp ip off  
# serverinfo time ip tcp off  
# serverinfo time ip udp off
```

索引

A

ACL 番号	123, 133
ARP 認証機能	58
AS 外部経路	103
AS 境界ルータ	103

B

BSR (ブートストラップルータ)	114
-------------------------	-----

D

DHCP 機能	144
DHCP サーバ機能	144
DHCP スタティック機能	146
DHCP スヌープ機能	39
DHCP リレーエージェント機能	148
DNS サーバ機能	158
DNS サーバの自動切り替え機能 (逆引き)	155
DNS サーバの自動切り替え機能 (順引き)	153
DNS 問い合わせタイプフィルタ機能	156
DSCP 値	123, 133
DSCP 値書き換え機能	133

E

ECMP 機能	142
ether L3 監視機能	62

I

IEEE802.1X 認証機能	43
IGMP スヌープ機能	41
IGMP パケット	41
IPv6 ネットワークの追加	69
IP アドレス	73, 123
IP アドレスの自動割り当て	144
IP フィルタリング機能	123
IP フィルタリングの条件	123
IP フィルタリングの設計方針	124

L

LACP 機能	13
LAN のネットワーク間接続	67
LSA	101

M

MAC アドレス	146
MAC アドレス認証機能	53

MAC アドレスフィルタ配布	173
MAC フィルタリング機能	21
MIB	161
MLAG 機能	15
MSTP	35

N

NXconciierge	179
--------------------	-----

O

OSPFv2 でネットワークを構築	89
OSPF 機能 (IPv4)	101
OSPF 機能 (IPv6)	107
OSPF 経路の制御	101

P

PIM-DM	111
PIM-SM	114
ProxyDNS	153

Q

QoS 機能	28
--------------	----

R

RIP 経路の制御 (IPv4)	73
RIP 経路の制御 (IPv6)	81
RIP マルチパス機能	72
RIP ユニキャスト	72
RIP を使用したネットワーク	71
RP (ランデブーポイント)	114

S

SNMP	161
SNMP エージェント機能	161
SNTP	68
SPT (最短経路)	114
STP	34

T

TIME プロトコル	68
TOS 値	123, 133

U

URL フィルタ機能	159
------------------	-----

V

VLAN 機能	9
VRPP 機能	135

W

Web 認証機能	46
----------	----

あ

アクセスポイントモニタリング	171
あて先情報	123, 133
アドレスマスク	73, 123
アプリケーションフィルタ機能	166

え

エリア ID	89
エリア境界ルータ	101

か

簡易ホットスタンバイ機能	135, 136
--------------	----------

き

逆引き	155
-----	-----

く

クライアントモニタリング	172
クラスタリング機能	135, 139
グループ ID	139

こ

構成定義情報切り替え予約	165
--------------	-----

し

システムログ	164
システムログの確認	164
準スタブエリア	98
順引き	153

す

スイッチング HUB	9
スケジュール機能	165
スタティック MAC フォワーディング機能	27
スタティックルーティング	120
スタブエリア	98

せ

制御	123
セキュリティ	123
接続端末数制限機能	56

そ

ソースポート	61
送信元情報	123, 133

た

ターゲット・ポート	61
タグ VLAN 機能	10
端末可視化機能	177

て

電波出力自動調整	174
----------	-----

と

動画・音声	111
ドメイン	153

は

バックアップポート機能	18
バックアップルータ	135
バックボーンエリア	89, 101

ふ

フィルタリング条件 (ルーティング)	73
フィルタリングの設計方針 (ルーティング)	74, 82
負荷分散通信	142
プロトコル	123, 133
プロトコル VLAN 機能	11

ほ

ポート VLAN 機能	9
ポート閉塞機能	65
ポート・ミラーリング機能	61
方向	73, 81
ホストデータベース	158
ホストデータベース情報	146
ポリシーベースネットワーク	133

ま

マスタルータ	135
マニュアル構成	8
マルチキャスト機能	111
マルチキャストパケット	41, 114

む

無線 LAN 管理機能	168
無線 LAN チャンネルの自動調整	176

め

メトリック値	73, 81
--------------	--------

ゆ

優先順位	124
優先制御機能	28
優先制御情報書き換え機能	30
ユニキャスト	111

り

リモート認証	49
リンクアグリゲーション機能	12

る

ループ検出機能	60
---------------	----

ろ

ローカル認証	46
--------------	----

SR-S コマンド設定事例集

P3NK-7102-04Z0

発行日 2023年4月

発行責任 富士通株式会社

- 本書の一部または全部を無断で他に転載しないよう、お願いいたします。
- 本書は、改善のために予告なしに変更することがあります。
- 本書に記載されたデータの使用に起因する第三者の特許権、その他の権利、損害については、弊社はその責を負いません。