P3NK-2182-01Z0

GeoStream Si-R シリーズ

コマンド設定事例集

V32

FUJITSU

はじめに

このたびは、本装置をお買い上げいただき、まことにありがとうございます。
インターネットやLANをさらに活用するために、本装置をご利用ください。

2006年 9月初版

目次

本書の構成と使いかた

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。

また、CD-ROMの中のREADMEファイルには大切な情報が記載されていますので、併せてお読みください。

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。

本書の構成

以下に、本書の構成と各章の内容を示します。

章タイトル	内　容
第1章　導入例	この章では、本装置の代表的な接続形態を紹介します。
第2章　活用例	この章では、本装置の便利な機能の活用方法について説明します。

マークについて

本書で使用しているマーク類は、以下のような内容を表しています。

本装置をお使いになる際に、役に立つ知識をコラム形式で説明しています。

こんな事に気をつけて　本装置をご使用になる際に、注意していただきたいことを説明しています。

操作手順で説明しているものの他に、補足情報を説明しています。

操作方法など関連事項を説明している箇所を示します。

本装置の機能を使用する際に、対象となる機種名を示します。

製造物責任法（PL）関連の注意事項をあらわしています。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。

参照　Si-Rシリーズ　コマンドユーザーズガイド「1.1 コマンドの運用手順」（P.8）

本書における商標の表記について

Microsoft、Windows および Windows NT 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。

Hi/fn および LZS は、Hi/fn,inc. の登録商標です。

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

Windows® 2000 の正式名称は、Microsoft® Windows® 2000 Server Network operating system、または Microsoft® Windows® 2000 Professional operating system です。

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
Si-R 効率化運用ツール使用手引書	Si-R 効率化運用ツールを使用する方法を説明しています。
Si-R180　ご利用にあたって	Si-R180 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。
Si-R220B　ご利用にあたって	Si-R220B 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。
Si-R240　ご利用にあたって	Si-R240 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。
Si-R260B　ご利用にあたって	Si-R260B 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。
Si-R370　ご利用にあたって	Si-R370 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。
Si-R570　ご利用にあたって	Si-R570 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。
Si-R シリーズ　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。
Si-R シリーズ　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。
Si-R シリーズ　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。
Si-R シリーズ　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。
Si-R シリーズ　コマンドユーザーズガイド	コマンドを使用して、時計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。
Si-R シリーズ　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。
Si-R シリーズ　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。
Si-R シリーズ　Web ユーザーズガイド	Web 画面を使用して、時計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。
Si-R シリーズ　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。
Si-R シリーズ　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。

第1章　導入例

この章では、本装置の代表的な接続形態を紹介します。

1.1　プライベートLANを構築する

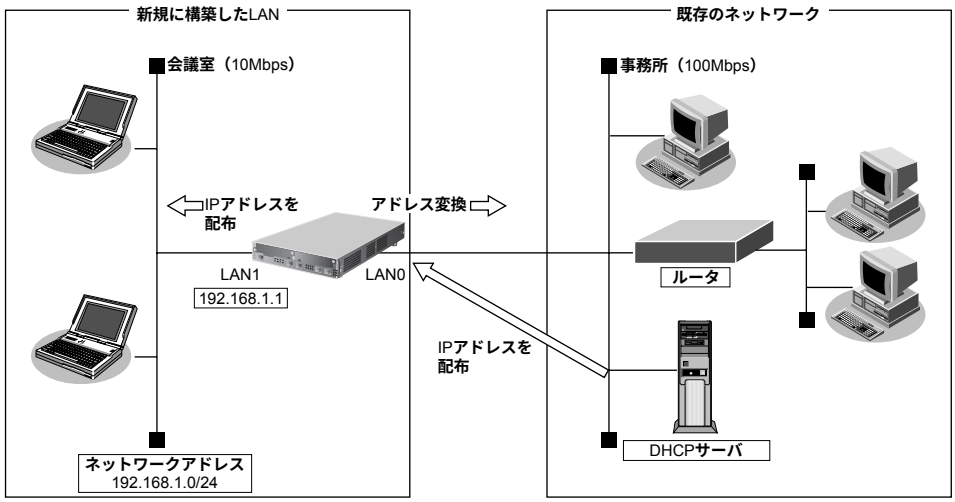
適用機種　全機種

ここでは、以下の条件で会議室 LAN を一時的に構築し、事務所ネットワークと接続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っ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　Si-R シリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.49）



● 設定条件

[事務所側 LAN]

- LAN0 ポートを使用する
- 転送レート　：自動認識
- IP アドレス　：DHCP サーバから自動的に取得
- マルチ NAT を使用する
  グローバルアドレス　：事務所側の DHCP サーバから割り当てられた IP アドレスを使用する
  アドレス個数　：1
  アドレス割当てタイマ　：5 分

[会議室側 LAN]

- LAN1 ポートを使用する
- 転送レート　：自動認識
- IP アドレス/ネットマスク　：192.168.1.1/24
- DHCP サーバ機能を使用する
  割当て先頭 IP アドレス　：192.168.1.2
  割当てアドレス数　：253
  リース期間　：1 日
  デフォルトルータ広報　：192.168.1.1
  DNS サーバ広報　：192.168.1.1

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 Si-R シリーズ　コマンドユーザーズガイド「1.7 コマンドで入力できる文字一覧」（P.26）

- **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

事務所側の LAN 情報を設定する
```
# delete lan 0
# lan 0 mode auto
# lan 0 ip dhcp service client
# lan 0 ip rip use off v1 0 off
# lan 0 ip nat mode multi any 1
```

会議室側の LAN 情報を設定する
```
# lan 1 mode auto
# 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
# lan 1 ip rip use v1 v1 0 off
```

設定終了
```
# save
```

再起動
```
# reset
```

本装置の設定が終了したら、設定を有効にするためにパソコンのシステムを終了し、パソコンおよび本装置の電源を切断します。各装置を LAN ケーブルで正しく接続したあと、本装置、パソコンの順に電源を投入します。

こんな事に気をつけて

本装置の DHCP サーバ機能を使用する場合は、以下の点に注意してください。

- **本装置の DHCP サーバ機能を利用する LAN 側のパソコンは、IP アドレスを自動的に取得する設定にしてください。固定の IP アドレスを設定していると、本装置が配布する IP アドレスと重なり、矛盾が生じる場合があります。**
- **パソコンに固定の IP アドレスを割り当てる場合は、「2.22.2 DHCP スタティック機能を使う」（P.304）を参考にして、IP アドレスと MAC アドレスを設定してください。**

1.2　プライベートLANを構築する（Si-R180）

適用機種　*Si-R180*

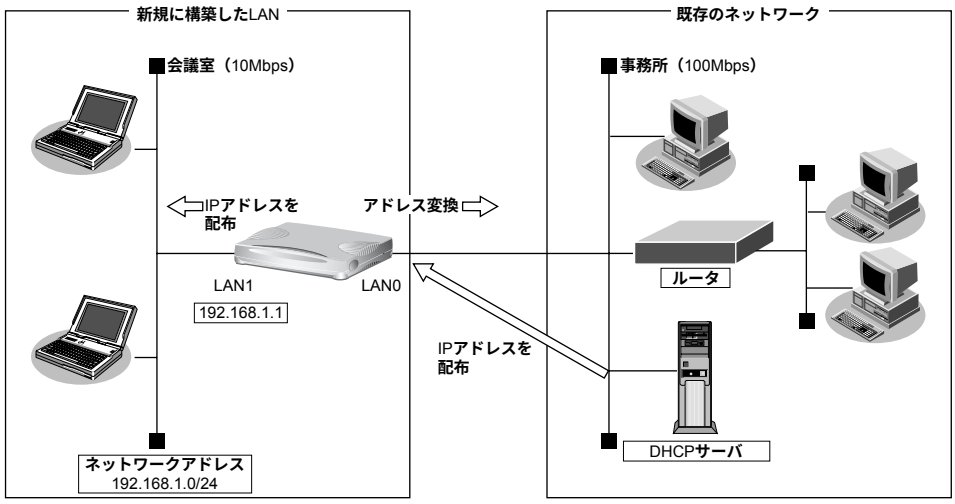
プライベートLANでは、マルチNAT機能を使用することで、割り当てられた1つのグローバルアドレスを使って、複数台のパソコンからネットワークにアクセスすることができます。

また、DHCPサーバ機能が動作しているため、パソコンのIPアドレス管理が必要ありません。そのため、簡単にLANを構築することができます。

ここでは、以下の条件で会議室LANを一時的に構築し、事務所ネットワークと接続する場合を例に説明します。

本装置のIPアドレスを変更しない場合

本装置がご購入時の状態の場合、本装置の電源を投入するだけで通信できます。



● 設定条件

[事務所側]

- 転送レートは自動認識
- IPアドレスはDHCPサーバから自動的に取得する

[会議室側]

- 転送レートは自動認識
- 本装置の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

[その他の条件]

- パスワードを設定する
  パスワード　：himitu

☛ 参照　Si-Rシリーズ　コマンドユーザーズガイド「1.3 パスワード情報を設定する」（P.13）

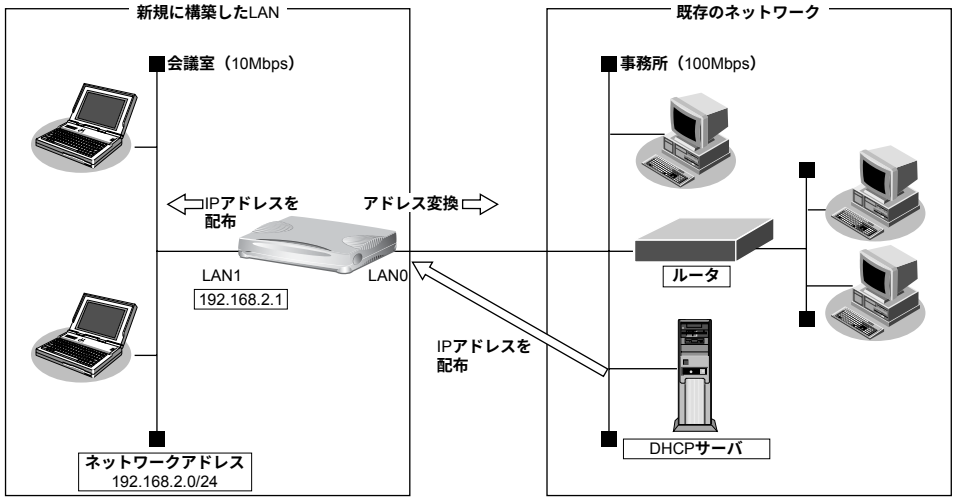
こんな事に気をつけて

- **パスワードを設定することを強く推奨します。設定しない場合、ネットワーク上のだれからでもアクセスできるため非常に危険です。**
- **「プライベート LAN 構築」で DHCP サーバを使用すると設定した場合は、DHCP サーバが広報する情報（デフォルトルータ、DNS サーバ、ドメイン名）に、DHCP サーバが動作するインタフェース側のネットワーク構成に応じた情報を設定してください。**
- **Si-R180 でスイッチポート（SW1 ～ 4）を利用する場合は、「2.40 スイッチポートを使う」（P.391）を参照してください。**

本装置の IP アドレスを変更する場合

「プライベート LAN 構築」では、プライベート LAN 側のネットワークアドレスを変更することができます。

以下に、プライベート LAN 側（LAN1 側）のネットワークアドレスを 192.168.2.0/24 に変更する手順を示します。



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　Si-R シリーズ　コマンドユーザーズガイド「1.7 コマンドで入力できる文字一覧」（P.26）

- **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。**

● 設定条件

[プライベート側ネットワーク]

- IP アドレス　：192.168.2.1
- ネットマスク　：24
- DHCP サーバ　：192.168.2.1
- デフォルトルータ広報　：192.168.2.1

● コマンド

```
プライベート側 LAN 情報を設定する
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ip dhcp service server
# lan 1 ip dhcp info dns 192.168.2.1
# lan 1 ip dhcp info address 192.168.2.2/24 253
# lan 1 ip dhcp info gateway 192.168.2.1

設定終了
# save

再起動
# reset
```

こんな事に気をつけて

- 本装置の IP アドレスを変更した場合、以下に示す 2 つの操作が必要です。
  - 本装置に接続しているパソコンの IP アドレスも変わります。再度、DHCP サーバから割り当ててもらう必要があります。
  - 再起動後に本装置にアクセスするためには、telnet で指定する IP アドレスに変更後の IP アドレスを指定する必要があります。
- 本装置に接続するネットワーク上のパソコンは、IP アドレスを自動的に取得する設定にしてください。IP アドレスを固定的に設定していると、本装置が配布する IP アドレスと重なり、矛盾が生じる場合があります。なお、常時同じ IP アドレスを取得する場合は、「2.22.2 DHCP スタティック機能を使う」（P.304）で IP アドレスと MAC アドレスを設定してください。
- ご購入時は、LAN1 ポートからだけ設定できます。

1.3　CATV インターネットに接続する

適用機種　全機種

CATV インターネット接続とは、CATV 事業者が提供するインターネット接続サービスです。CATV インターネット接続には、ケーブルモデム接続とダイヤルアップ接続の 2 つの接続形態があります。ケーブルモデム接続は、ケーブルテレビ網を利用したもので、CATV 事業者が提供するケーブルモデムに接続する形態です。ダイヤルアップ接続とは、CATV 電話サービスを利用したもので、パソコンにモデムを接続する形態です。本装置を使用して CATV インターネット接続する場合は、「ケーブルモデム接続」の形態となり、CATV 事業者との契約が必要です。接続にあたっては、CATV 事業者の指示に従ってください。

ヒント

◆ ケーブルモデムとは？

ケーブルテレビ網に接続するための専用モデムで、CATV インターネット接続サービスに必要な機器です。パソコン（LAN ボード）とは LAN ケーブルで接続します。通常、CATV サービス加入時に CATV 事業者より貸し出され、宅内工事の際に設置されます。

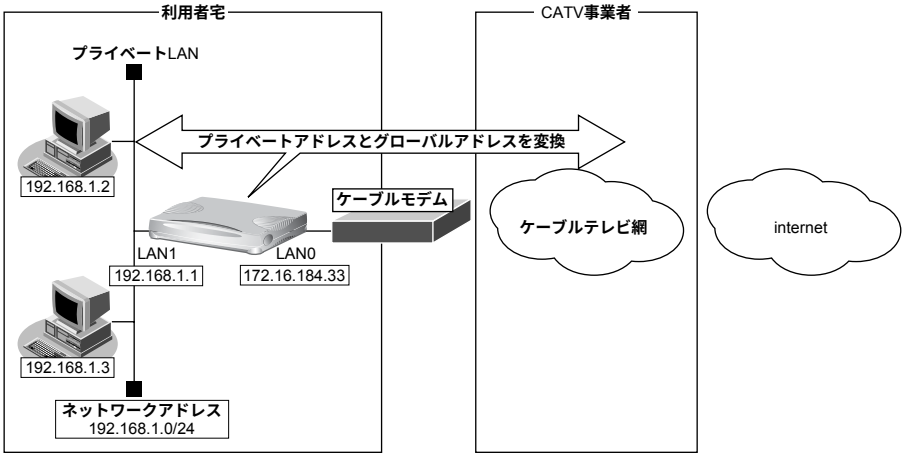
本装置を使った CATV インターネット接続は、CATV 事業者が提供するインターネット接続サービスをプライベート LAN 上の複数のパソコンから利用するための接続形態です。本装置と CATV 事業者が提供するケーブルモデムを接続することで、プライベート LAN 上のパソコンからインターネット接続サービスを利用できます。

本装置のアドレス変換機能が CATV 事業者側のネットワークと利用者側のプライベート LAN との間で動作し、プライベート LAN 側の IP アドレスを外部から隠すため、セキュリティが確保できます。

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っ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　Si-R シリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.49）



● 設定条件

[CATV 事業者側]

- LAN0 ポートを使用する
- IP アドレス　：172.16.184.33
- ネットワークアドレス/ネットマスク　：172.16.184.0/24
- デフォルトルータ　：172.16.184.100
- DNS サーバ　：192.10.10.10

[プライベート LAN 側]

- 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 サーバ機能を使用する

こんな事に気をつけて

- **契約した CATV 事業者によって設定方法が異なります。実際の設定は、CATV 事業者の指示に従ってください。**
- **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。**
- **Si-R180 でスイッチポートを利用する場合は、「2.40 スイッチポートを使う」（P.391）を参照してください。**

● コマンド

CATV 事業者側を設定する

```
# delete lan
# lan 0 ip address 172.16.184.33/24 3
# lan 0 ip dhcp info time 1d
# lan 0 ip route 0 default 172.16.184.100 1 0
# lan 0 ip rip use off v1 0 off
# lan 0 ip nat mode multi any 1 5m
```

プライベート LAN 側を設定する

```
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip dhcp service server
# lan 1 ip dhcp info dns 192.10.10.10
# 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
# lan 1 ip rip use v1 v1 0 off
```

ProxyDNS を設定する

```
# proxydns domain 0 any * any static 192.10.10.10
# proxydns address 0 any static 192.10.10.10
```

設定終了

```
# save
```

再起動

```
# reset
```

1.4　LAN をネットワーク間接続する

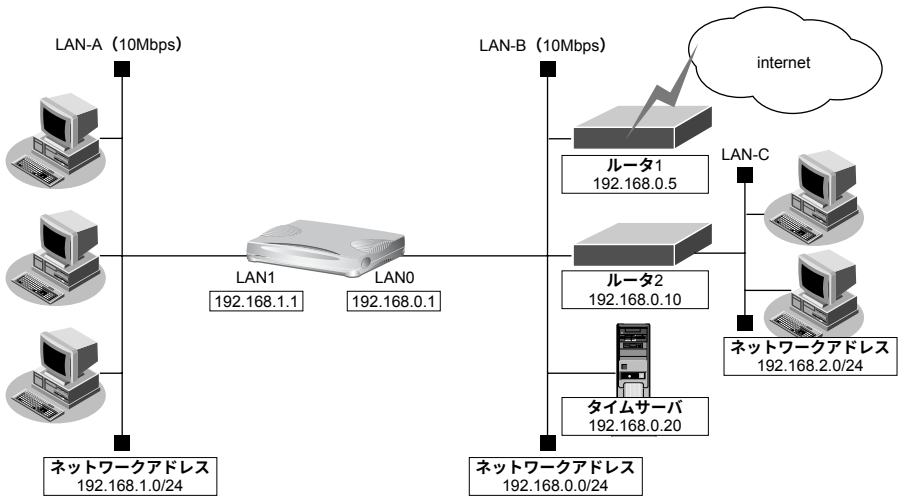
適用機種　全機種

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っ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　Si-R シリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.49）



● 設定条件

[LAN-A 側]

- 転送レートは自動認識
- 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
- NAT を使用しない

[LAN-B 側]

- 転送レートは自動認識
- 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
- NAT は使用しない

[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。
- Si-R180 でスイッチポートを利用する場合は、「2.40 スイッチポートを使う」（P.391）を参照してください。

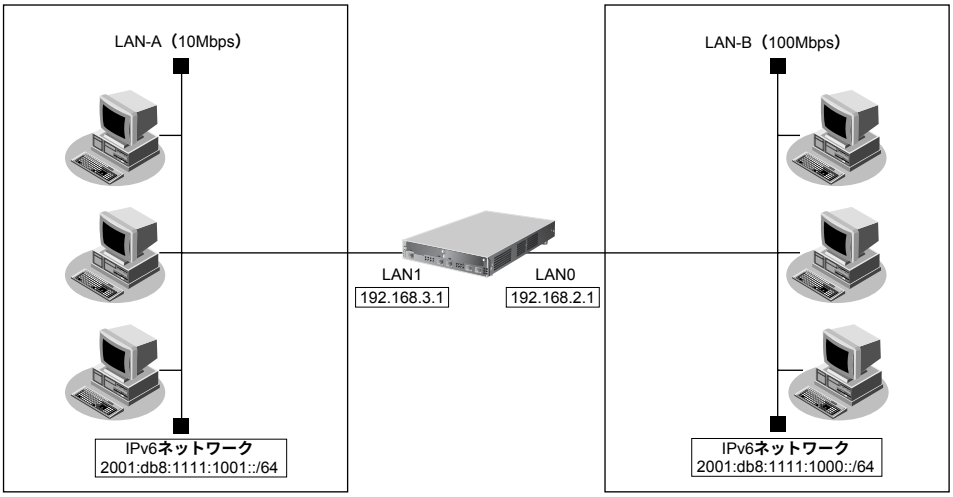
● コマンド

```
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 0
# lan 0 ip route 0 default 192.168.0.5 1 0
# 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
# lan 1 ip rip use v1 v1 0 off

自動時刻を設定する
# time auto server 192.168.0.20 time
# time auto interval start

設定終了
# save

再起動
# reset
```

1.5　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　全機種

ここでは、IPv4 で通信しているネットワーク環境に IPv6 通信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

【LAN-B 側】

- プレフィックス/プレフィックス長　：2001:db8:1111:1000::/64

こんな事に気をつけて

Si-R180 でスイッチポートを利用する場合は、「2.40 スイッチポートを使う」（P.391）を参照してください。

● コマンド

```
LAN0 情報を設定する
# lan 0 ip6 use on
# lan 0 ip6 address 0 2001:db8:1111:1000::/64 30d 7d c0
# lan 0 ip6 ra mode send
# lan 0 ip6 rip use on on 0
# lan 0 ip6 rip site-local on

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

設定終了
# save
# commit
```

1.6　インターネットへ専用線で接続する

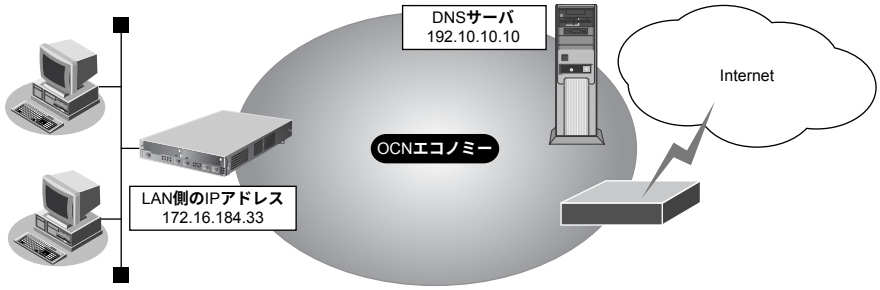
適用機種　***Si-R220B,370,570***

ここでは、以下の設定条件で専用線を利用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っ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　Si-R シリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.49）



● 設定条件

- SLOT0 に実装された BRI 拡張モジュール L2 または基本ボード上の ISDN ポート（Si-R220B の場合）で OCN エコノミー専用線（128Kbps）を使用する
- LAN0 を使用して、新規に LAN を構築する
- OCN 側の DNS サーバを使用　：192.10.10.10
- OCN より提示されたドメイン名　：domain.ocn.ne.jp
- 接続するパソコンの台数は OCN から割り当てられた IP アドレスよりも少ない
- 割り当て IP アドレス
  ネットワークアドレス/ネットマスク　：172.16.184.32/29
  ホストアドレス　：172.16.184.33 ～ 172.16.184.38
  ブロードキャストアドレス　：172.16.184.39
  本装置の LAN 側の IP アドレス　：172.16.184.33
- 接続ネットワーク名　：internet

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　Si-R シリーズ　コマンドユーザーズガイド「1.7 コマンドで入力できる文字一覧」（P.26）

- **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。**
- **Si-R220B では、利用物理回線設定でスロット番号に “mb” を指定してください。**

● コマンド

回線情報を設定する
wan 0 bind 0
wan 0 line hsd 128k

本装置の IP アドレスを設定する
lan 0 ip address 172.16.184.33/29 3

DHCP **サーバを設定する**
lan 0 ip dhcp info dns 192.10.10.10
lan 0 ip dhcp info address 172.16.184.34/29 6
lan 0 ip dhcp info gateway 172.16.184.33
lan 0 ip dhcp info domain domain.ocn.ne.jp
lan 0 ip dhcp service server

接続先の情報を設定する
remote 0 name internet
remote 0 ip route 0 default 1
remote 0 ap 0 name ISP-1
remote 0 ap 0 datalink bind wan 0
remote 0 ap 0 ip dns 192.10.10.10

設定終了
save

再起動
reset

1.7　インターネットへ PPPoE で接続する

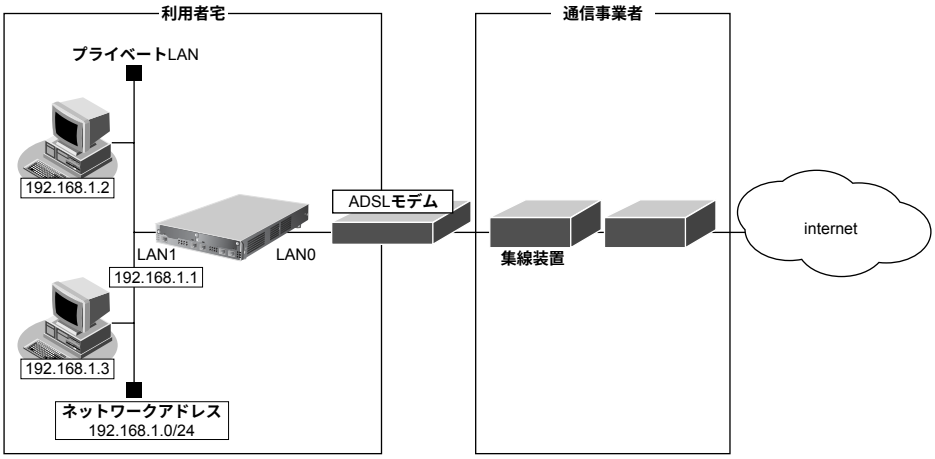
適用機種　全機種

ここでは、PPPoE 接続を使ってフレッツ・ADSL などのサービスを利用し、インターネットへ接続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っ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　Si-R シリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.49）



● 設定条件

[通信事業者側]

- ユーザ認証 ID　：userid（プロバイダから提示された内容）
- ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- LAN0 ポートを使用する

[プライベート LAN 側]

- 本装置の 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

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　Si-R シリーズ　コマンドユーザーズガイド「1.7 コマンドで入力できる文字一覧」（P.26）

- **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。**
- **PPPoE で利用する相手情報の MTU 値は、接続先から指定された MTU 値を設定します。一般的には、1454 を設定すれば問題ありません。**
- **PPPoE を利用する物理インタフェースの LAN 情報設定では、lan mode コマンドで動作モードを必ず設定してください。lan mode コマンドで動作モードの設定がなく、その他の lan 情報で設定する値もすべて初期値とした場合、その LAN 情報は保存されないため、通信できなくなります。**

● コマンド

ADSL モデムに接続するインタフェースを設定する
delete lan 0
lan 0 mode auto

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

DHCP サーバを設定する
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
lan 1 ip dhcp service server
lan 1 ip nat mode off

接続先の情報を設定する
remote 0 name internet
remote 0 mtu 1454
remote 0 autodial enable
remote 0 ppp ipcp vjcomp disable
remote 0 ip route 0 default 1
remote 0 ip rip use off off 0 off
remote 0 ip nat mode multi any 1 5m
remote 0 ip msschange 1414
remote 0 ap 0 name ISP-1
remote 0 ap 0 datalink bind lan 0
remote 0 ap 0 ppp auth send userid userpass

ProxyDNS を設定する
proxydns domain 0 any * any to 0
proxydns address 0 any to 0

設定終了
save

再起動
reset

1.8　インターネットへデータ通信カードを使用して接続する

適用機種　*Si-R240*

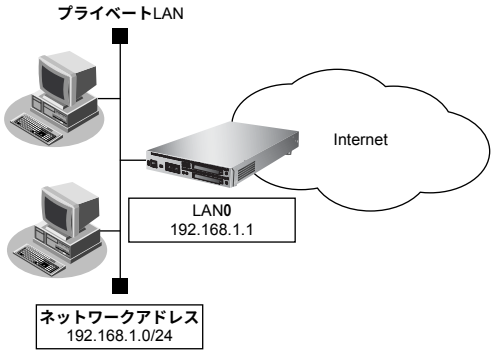
ここでは、データ通信カードを使用して、インターネットへ接続する場合を例に説明します。

参照　動作検証済みのデータ通信カード（富士通ホームページ）
http://fenics.fujitsu.com/products/sir/sir240/supportcard.html

こんな事に気をつけて

- **データ通信カードは、SLOT0 のみ動作します。**
- **データ通信カードは、電源投入前に挿入してください。また、電源投入後の抜き差しはしないでください。**
- **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ったり手順どおりに設定しても通信できないことがあります。**

参照　Si-R シリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.49）



● 設定条件

[Internet 側]

- 認証 ID　：hoge（通信事業者から提示された内容）
- 認証パスワード　：hogehoge（通信事業者から提示された内容）
- 電話番号　：*99# （通信事業者から提示された内容）
- 無通信監視タイマ　：無通信監視時間を 1 分とする
- 強制切断　：100000 パケット（128 バイト単位）を超えた場合に回線を切断し、以降自動発信を行わない

[プライベート LAN 側]

- 本装置の IP アドレス　：192.168.1.1
- ネットワークアドレス/マスク　：192.168.1.0/24

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。だたし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

  ☛ 参照 Si-R シリーズ　コマンドユーザーズガイド「1.7 コマンドで入力できる文字一覧」（P.26）

- 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。
- データ通信カード接続では、以下の機能は動作しません。
  - テンプレート機能
  - 金額による課金制御機能
  - 常時接続機能
  - シェーピング機能
- データ通信カードで通信できるプロトコルは、IPv4、IPv6、ブリッジだけです。
- データ通信カードによる発信は課金が発生するため、課金情報（アカウント情報）を監視して超過課金が発生していないか、こまめに確認してください。
  また、超過課金を防止する場合は、課金制御機能の累計接続時間か累計パケット数を設定してください。
- 課金制御機能（強制切断）による回線切断が発生した場合、以下のシステムログが出力されます。

  protocol: [<line>] forced disconnection <target> <reason>

  ☛ 参照 Si-R シリーズ　メッセージ集「課金制御機能による強制切断」

  課金制御機能（強制切断）により切断した場合、以降の手動および自動発信を禁止します。
  接続するにはデータ通信カードのアカウント情報のクリア（clear modem account）を実行する必要があります。
- パケット数による強制切断のパケット数は、累計送受信バイト数（PPP パケット長）を 128 で割った値を用います。
  パケット数による強制切断のパケット数は目安であり、通信事業者でのパケット数と異なる場合があります。

● 設定コマンド

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

DHCP サーバを設定する
```
# lan 0 ip dhcp info dns 192.168.1.1
# lan 0 ip dhcp info address 192.168.1.2/24 253
# lan 0 ip dhcp info time 1d
# lan 0 ip dhcp info gateway 192.168.1.1
# lan 0 ip dhcp service server
```

回線情報を設定する
```
# wan 0 bind 0
# wan 0 line cardmodem
```

接続先の情報を設定する
```
# remote 0 name internet
# remote 0 autodial enable
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip route 0 default 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind wan 0
# remote 0 ap 0 ppp auth send hoge hogehoge
# remote 0 ap 0 dial 0 number *99#
# remote 0 ap 0 idle 1m
```

課金制御機能を設定する
```
# remote 0 ap 0 disconnect packet 100000 per128
```

ProxyDNS を設定する
```
# proxydns domain 0 any * any to 0
# proxydns address 0 any to 0
```

設定終了
save

再起動
reset

補足 各通信事業者の認証 ID、認証パスワード、電話番号を以下に示します。
詳細については、各通信事業者にお問い合わせください。

通信事業者	認証 ID	認証パスワード	電話番号
ウィルコム PRIN つなぎ放題[PRO]	prin	prin	0570570711##64
NTT ドコモ mopera	（任意の文字列）	（任意の文字列）	*99***1#
au by KDDI au.NET	au@au-win.ne.jp	au	*99**24#
ボーダフォン （ソフトバンクモバイル） アクセスインターネット	vodafone@connect	vodafone	*99#

1.9　事業所 LAN を ISDN で接続する

適用機種　*Si-R220B,370,570*

ここでは、ISDN 回線を介して 2 つの事業所（東京、川崎）のネットワークを接続する場合を例に説明します。

こんな事に気をつけて

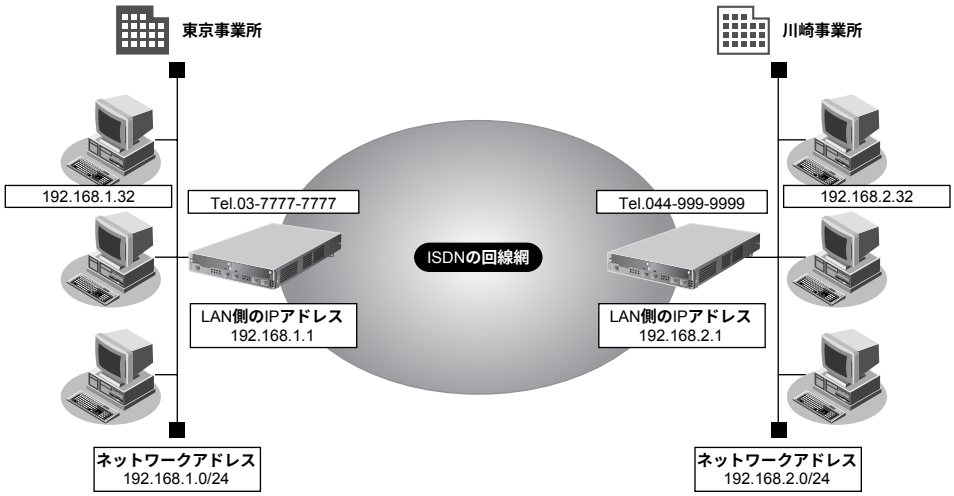
この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。

☛ 参照　Si-R シリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.49）

- **双方の事業所から同時に発信が行われた場合、両方の接続が成立することでその接続が超過課金（2 倍）になる場合があります。これは、接続優先制御機能を利用して片方の接続のみが存続するようにすることで防ぐことができます。**

☛ 参照　Si-R シリーズ　コマンドリファレンス「remote ap connect priority」

この機能を利用する場合は、双方の事業所の装置で同じ接続優先設定を行わないでください。同時発信の際に接続ができなくなります。この機能を利用する場合は、以下の設定を奨励します。
- **一方の装置で着信接続を優先する。**
- **一方の装置で接続優先制御を行わない。**



● 設定条件

- SLOT0 に実装された BRI 拡張モジュール L2 または基本ボード上の ISDN ポート（Si-R220B の場合）で ISDN 回線（64Kbps）を使用する
- スタティック経路機能を使用する
- 接続ネットワーク名　：intranet
- 無通信監視時間を 1 分とする

[東京事業所]

- 本装置の IP アドレス/ネットマスク　：192.168.1.1/24
- 電話番号　：03-7777-7777
- ユーザ認証 ID とユーザ認証パスワード
  発信　：tokyo、tokyopass
  着信　：kawasaki、kawapass

[川崎事業所]

- 本装置の IP アドレス/ネットマスク　：192.168.2.1/24
- 電話番号　：044-999-9999

- ユーザ認証 ID とユーザ認証パスワード
  発信　：kawasaki、kawapass
  着信　：tokyo、tokyopass

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。**
- **Si-R220B では、利用物理回線設定でスロット番号に“mb”を指定してください。**

東京事業所の本装置を設定する

● コマンド

回線情報を設定する
wan 0 bind 0
wan 0 line isdn

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

接続先の情報を設定する
remote 0 name intranet
remote 0 ip route 0 192.168.2.0/24 1
remote 0 ap 0 name kawasaki
remote 0 ap 0 datalink bind wan 0
remote 0 ap 0 dial 0 number 044-999-9999
remote 0 ap 0 dial 0 speed 64K
remote 0 ap 0 ppp auth type any
remote 0 ap 0 ppp auth send tokyo tokyopass
remote 0 ap 0 ppp auth receive kawasaki kawapass
remote 0 ap 0 idle 1m

設定終了
save

再起動
reset

川崎事業所の本装置を設定する

● コマンド

回線情報を設定する
wan 0 bind 0
wan 0 line isdn

本装置の IP アドレスを設定する
lan 0 ip address 192.168.2.1/24 3

接続先の情報を設定する
remote 0 name intranet
remote 0 ip route 0 192.168.1.0/24 1
remote 0 ap 0 name tokyo
remote 0 ap 0 datalink bind wan 0
remote 0 ap 0 dial 0 number 03-7777-7777
remote 0 ap 0 dial 0 speed 64K
remote 0 ap 0 ppp auth type any
remote 0 ap 0 ppp auth send kawasaki kawapass
remote 0 ap 0 ppp auth receive tokyo tokyopass
remote 0 ap 0 idle 1m

設定終了
save

再起動
reset

1.10 事業所 LAN を専用線で接続する

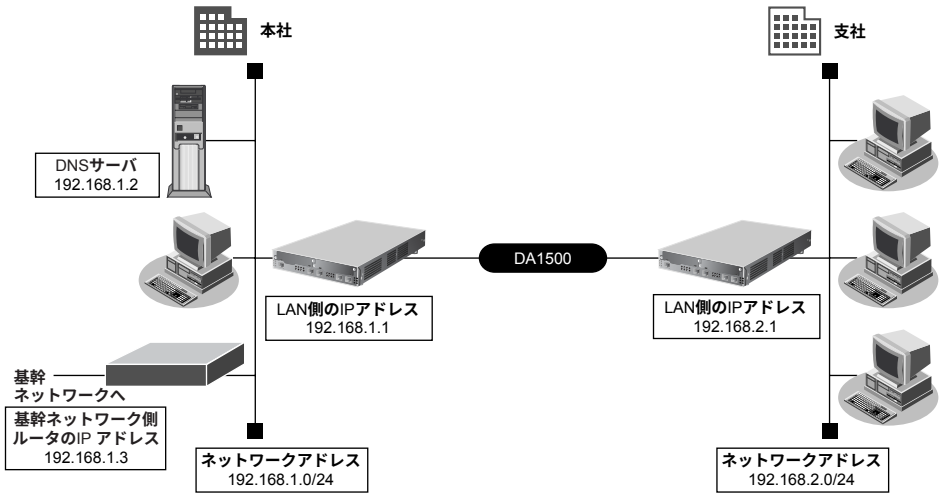
適用機種　*Si-R220B,370,570*

ここでは、高速ディジタル専用線を介して 2 つの事業所（本社、支社）のネットワークを接続する場合について Si-R370 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っ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　Si-R シリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.49）



● 設定条件

- SLOT0 に実装された PRI 拡張モジュール L2 で専用線（1.5Mbps）を使用する
- DHCP サーバ機能は使用しない

[本社]

- 接続ネットワーク名　：honsya
- 接続先名　：honsya-1
- ネットワークアドレス/ネットマスク　：192.168.1.0/24
- 本装置の LAN 側の IP アドレス　：192.168.1.1
- DNS サーバ　：192.168.1.2
- 基幹ネットワーク側ルータ IP アドレス　：192.168.1.3

[支社]

- 接続ネットワーク名　：shisya1
- 接続先名　：shisya-1
- ネットワークアドレス/ネットマスク　：192.168.2.0/24
- 本装置の LAN 側の IP アドレス　：192.168.2.1

補足　この例では、本社に DNS サーバが存在し、IP アドレスを固定にする必要があります。そのため、本社側では DHCP サーバ機能は使用しない条件にします。

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 Si-R シリーズ　コマンドユーザーズガイド「1.7 コマンドで入力できる文字一覧」（P.26）

- **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。**

本社の本装置を設定する

● コマンド

```
回線情報を設定する
# wan 0 bind 0
# wan 0 line hsd 1.5m

LAN 情報を設定する
# lan 0 ip address 192.168.1.1/24 3
# lan 0 ip route 0 default 192.168.1.3 1

接続先の情報を設定する
# remote 0 name shisya1
# remote 0 ip route 0 192.168.2.1/24 1
# remote 0 ap 0 name shisya-1
# remote 0 ap 0 datalink bind wan 0

設定終了
# save

再起動
# reset
```

支社の本装置を設定する

● コマンド

```
回線情報を設定する
# wan 0 bind 0
# wan 0 line hsd 1.5m

LAN 情報を設定する
# lan 0 ip address 192.168.2.1/24 3

接続先の情報を設定する
# remote 0 name honsya
# remote 0 ap 0 name honsya-1
# remote 0 ap 0 datalink bind wan 0
# remote 0 ip route 0 default 1

設定終了
# save

再起動
# reset
```

補足 「1.6 インターネットへ専用線で接続する」（P.20）では、デフォルトルートを設定しています。
この設定例では、本社のネットワーク内に基幹ネットワークにつながるルータが存在します。このため、本社側への経路をデフォルトルートとする必要があります。よって、ここでは「インターネットへ専用線で接続する」のネットワーク設計を利用しています。ただし、このネットワーク設計の場合は DHCP サーバ機能が動作するので、DHCP サーバ機能を使用しないように設定を変更してください。

1.11 複数の事業所 LAN をフレームリレーで接続する

適用機種 ***Si-R220B,370,570***

ここでは、フレームリレーで複数の事業所を接続する場合を例に説明します。

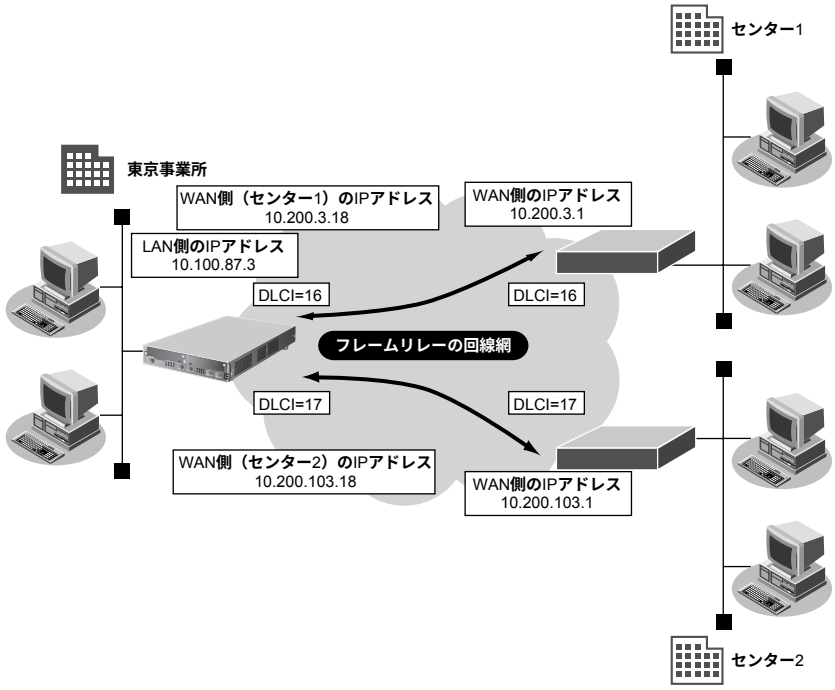
フレームリレーを利用すると複数の事業所の LAN と接続できるため、データを高速に転送することができます。

また、相手ごとに固定的な回線を接続するので、公衆網であるフレームリレー網に閉域ネットワークを構築することができ、セキュリティの確保にも適しています。

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っ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 Si-R シリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.49）



● 設定条件

- SLOT0 に実装された BRI 拡張モジュール L2 または基本ボード上の ISDN ポート（Si-R220B の場合）でフレームリレー（128Kbps）を使用する
- RIPv1 を使用する
- 本装置の LAN 側の IP アドレス/ネットマスク　：10.100.87.3/24

[センター 1 と接続する条件]

- ネットワーク名　：center1
- 接続先名　：ap1
- WAN の自側 IP アドレス　：10.200.3.18
- WAN の相手側 IP アドレス　：10.200.3.1
- DLCI　：16
- CIR　：64Kbps

[センター 2 と接続する条件]

- ネットワーク名　：center2
- 接続先名　：ap2
- WAN の自側 IP アドレス　：10.200.103.18
- WAN の相手側 IP アドレス　：10.200.103.1
- DLCI　：17
- CIR　：64Kbps

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。**
- **Si-R220B では、利用物理回線設定でスロット番号に“mb”を指定してください。**
- **BRI4 ポート拡張モジュールは、フレームリレーに対応していません。**

● コマンド

回線情報を設定する
wan 0 bind 0
wan 0 line fr 128k

本装置の LAN 側の IP アドレスを設定する
lan 0 ip address 10.100.87.3/24 3

RIP 情報を設定する
lan 0 ip rip use v1 v1 0 off

接続先（センター 1）の情報を設定する
remote 0 name center1
remote 0 ip address local 10.200.3.18
remote 0 ip address remote 10.200.3.1
remote 0 ip rip use v1 v1 0 off
remote 0 ap 0 name ap1
remote 0 ap 0 datalink bind wan 0
remote 0 ap 0 fr dlci 16
remote 0 ap 0 fr cir 64

接続先（センター 2）の情報を設定する
remote 1 name center2
remote 1 ip address local 10.200.103.18
remote 1 ip address remote 10.200.103.1
remote 1 ip rip use v1 v1 0 off
remote 1 ap 0 name ap2
remote 1 ap 0 datalink bind wan 0
remote 1 ap 0 fr dlci 17
remote 1 ap 0 fr cir 64

設定終了
save

再起動
reset

1.12 複数の事業所 LAN を ATM で接続する

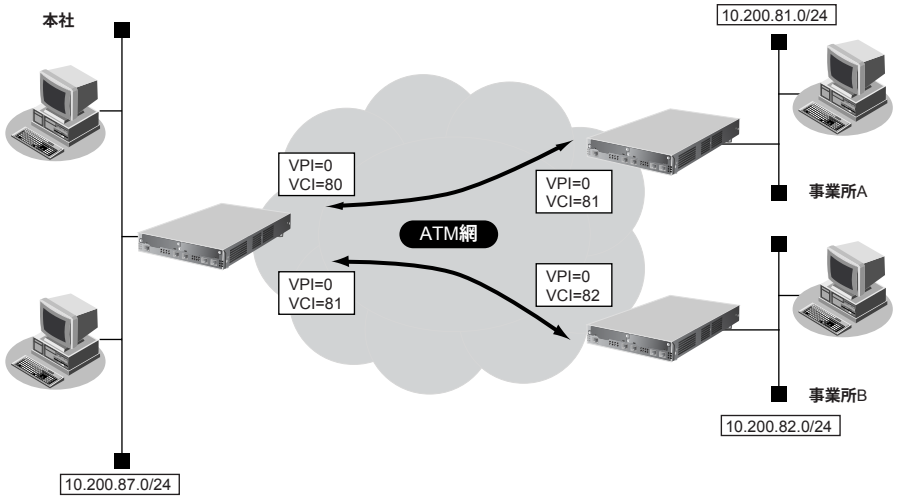
適用機種　*Si-R260B,370,570*

ここでは、ATM 網を利用して複数の事業所のネットワークを接続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っ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　Si-R シリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.49）



● 設定条件

[本社]

- slot0 に実装された ATM25M または ATM155M 拡張モジュール L2、または本装置に内蔵の ATM インタフェース（Si-R260B の場合）で ATM 網を使用する
- LAN 側の IP アドレス　：10.200.87.3/24
- 事業所 A 向け接続ネットワーク名　：JigyoA
- 事業所 A 向け接続先名　：jigyo-a
- 事業所 A 向け VPI/VCI　：0/80
- 事業所 A 向けサービスクラス　：CBR（VC 速度：6Mbps）
- 事業所 B 向け接続ネットワーク名　：JigyoB
- 事業所 B 向け接続先名　：jigyo-b
- 事業所 B 向け VPI/VCI　：0/81
- 事業所 B 向けサービスクラス　：CBR（VC 速度：4Mbps）

[事業所 A]

- slot0 に実装された ATM25M または ATM155M 拡張モジュール L2、または本装置に内蔵の ATM インタフェース（Si-R260B の場合）で ATM 網を使用する
- LAN 側の IP アドレス　：10.200.81.1/24
- 接続ネットワーク名　：Honsya
- 接続先名　：honsya-1

- VPI/VCI　：0/81
- サービスタイプ　：CBR（VC 速度：6Mbps）

[事業所 B]

- slot0 に実装された ATM25M または ATM155M 拡張モジュール L2、または本装置に内蔵の ATM インタフェース（Si-R260B の場合）で ATM 網を使用する
- LAN 側の IP アドレス　：10.200.82.1/24
- 接続ネットワーク名　：Honsya
- 接続先名　：honsya-2
- VPI/VCI　：0/82
- サービスタイプ　：CBR（VC 速度：4Mbps）

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。**
- **Si-R260B では、利用物理回線設定でスロット番号に“mb”を指定してください。**

● コマンド

[本社]

```
VPC の情報を設定する
# wan 0 bind 0
# wan 0 line atm
# wan 0 atm vpi 0

本装置の IP アドレスを設定する
# lan 0 ip address 10.200.87.3/24 3

事業所 A 向け情報を設定する
# remote 0 name JigyoA
# remote 0 ip route 0 10.200.81.0/24
# remote 0 ap 0 name jigyo-a
# remote 0 ap 0 datalink bind wan 0
# remote 0 ap 0 atm vci 80
# remote 0 ap 0 atm rate 6m
# remote 0 ap 0 atm ast cbr

事業所 B 向け情報を設定する
# remote 1 name JigyoB
# remote 1 ip route 0 10.200.82.0/24
# remote 1 ap 0 name jigyo-b
# remote 1 ap 0 datalink bind wan 0
# remote 1 ap 0 atm vci 81
# remote 1 ap 0 atm rate 4m
# remote 1 ap 0 atm ast cbr

設定終了
# save

再起動
# reset
```

こんな事に気をつけて

使用する拡張モジュールによって、以下の点に注意して設定してください。Si-R260B の ATM25 インタフェースは ATM25 拡張モジュール L2 と同じです。

拡張モジュール	注意点
ATM25M ／ ATM155M 拡張モジュール L2	• VP ／ VC 速度を設定する場合は、64Kbps ～ 25Mbps の範囲で 8Kbps または 50Kbps 刻みで指定します。 • VP シェーピングを前提とした運用を本装置で行う場合は、以下のように設定してください。 - VPC が 1VPC の場合にだけ、VP シェーピングと VC シェーピングを同時に利用することができます。 - VP シェーピングを行う VPC と VP シェーピングを行わない VPC は、同一拡張モジュール内で同時に利用することはできません。 • 本装置で複数 VPC を使って ATM 網を利用する場合は、以下のように設定してください。 - 複数 VPC で VP シェーピングが必要となる場合は、1VPC あたり 1VCC となるようにネットワークを設計してください。このとき、16VPC まで利用することができます。 - VP 速度は設定しないでください。契約時の VP 速度は VC 速度として設定し、サービスタイプを CBR に設定してください。 • VP シェーピングを必要としない場合は、複数 VPC 上で複数 VC シェーピングを行うことができます。 • VP シェーピング時は、VC 速度（CBR、GFR+）、平均速度（SCR）および最低速度（UBR+）の総和が VP 速度を超えないようにように設定してください。 • VC シェーピング時は、VC 速度（CBR、GFR+）、平均速度（SCR）および最低速度（UBR+）の総和が 25Mbps を超えないようにように設定してください。
ATM25M 拡張モジュール H1	• VP ／ VC 速度を設定する場合は、以下の設定範囲で設定してください。 - 64Kbps ～ 25Mbps の範囲で 8Kbps または 50Kbps 刻みで指定します。 • VP シェーピングを前提とした運用を本装置で行う場合は、以下のように設定してください。 - VP 速度の総和を 25Mbps 以下に設定してください。 - 1-VPC での VP ／ VC シェーピング時以外で、サービスタイプ UBR+ は設定できません。複数 VPC での VP ／ VC シェーピング時は VBR を設定してください。 - サービスタイプが VBR の場合は、平均速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが CBR の場合は、VC 速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが UBR+ の場合は、最低速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが GFR+ の場合は、VC 速度の総和が VP 速度を超えないように設定してください。 - VP シェーピングを行う VPC と VP シェーピングを行わない VPC は、同一拡張モジュール内で同時に利用することはできません。

拡張モジュール	注意点
ATM155M 拡張モジュール H1	• VP ／ VC 速度を設定する場合は、以下の設定範囲で設定してください。 - VP 速度は、200Kbps ～ 50Mbps の範囲で 8Kbps または 50Kbps 刻みで指定できます。 - VC 速度は、64Kbps ～ 100Mbps の範囲で 8Kbps または 50Kbps 刻みで指定できます。 • VP シェーピングを前提とした運用を本装置で行う場合は、以下のように設定してください。 - VP 速度の総和を 50Mbps 以下に設定してください。 - 1-VPC での VP ／ VC シェーピング時以外ではサービスタイプ UBR+ は設定できません。複数 VPC での VP ／ VC シェーピング時は VBR を設定してください。 - サービスタイプが VBR の場合は、平均速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが CBR の場合は、VC 速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが UBR+ の場合は、最低速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが GFR+ の場合は、VC 速度の総和が VP 速度を超えないように設定してください。 - VPC 内の VC 速度の最高速度は 50Mbps になります。 - VP シェーピングを行う VPC と VP シェーピングを行わない VPC は、同一拡張モジュール内で同時に利用することはできません。 • DSU 接続する場合は、atm send clock コマンドで送信クロックの設定を recovery にしてください。 `atm <slot> send clock recovery`

[事業所 A]

```
# wan 0 bind 0
# wan 0 line atm
# wan 0 atm vpi 0
# lan 0 ip address 10.200.81.1/24 3
# remote 0 name Honsya
# remote 0 ip route 0 default 1
# remote 0 ap 0 name honsya-1
# remote 0 ap 0 datalink bind wan 0
# remote 0 ap 0 atm vci 81
# remote 0 ap 0 atm rate 6m
# remote 0 ap 0 atm ast cbr
# save
# reset
```

[事業所 B]

```
# wan 0 bind 0
# wan 0 line atm
# wan 0 atm vpi 0
# lan 0 ip address 10.200.82.1/24 3
# remote 0 name Honsya
# remote 0 ip route 0 default 1
# remote 0 ap 0 name honsya-2
# remote 0 ap 0 datalink bind wan 0
# remote 0 ap 0 atm vci 82
# remote 0 ap 0 atm rate 4m
# remote 0 ap 0 atm ast cbr
# save
# reset
```

1.13　複数の事業所 LAN を IP-VPN 網を利用して接続する

適用機種　全機種

ここでは、プロトコル BGP4 を使用して、IP-VPN 網で複数の事業所を接続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

- **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っ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　Si-R シリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.49）

- **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　Si-R シリーズ　コマンドユーザーズガイド「1.7 コマンドで入力できる文字一覧」（P.26）

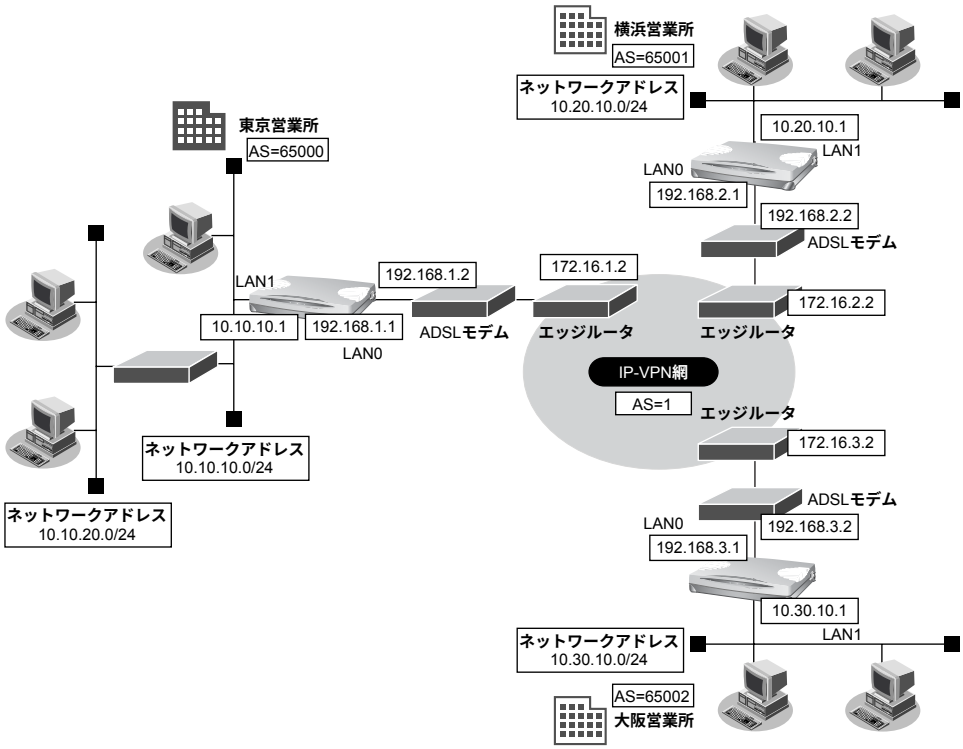
- **NAT 機能と併用することはできません。**
- **バージョン 4 だけをサポートしています。**
- **BGP で利用できるセッション数は使用する装置ごとに異なります。**

  ☛ 参照　Si-R シリーズ　仕様一覧「2.3 システム最大値一覧」（P.37）

- **経路情報を最大値まで保持している状態では、受信した BGP パケットは破棄されます。破棄した BGP パケットの経路情報は、その後、経路情報に空きができた場合でも反映されません。**
- **BGP 使用中に commit コマンドを実行した場合、接続中のセッションが一度切断されることがあります。**
- **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。**

1.13.1　ADSL モデムを使用して IP-VPN 網と接続する

適用機種　全機種



● 設定条件

- LAN0 ポートを ADSL モデムに接続する

[IP-VPN 網]

- 東京営業所向け IP アドレス　：172.16.1.2
- 横浜営業所向け IP アドレス　：172.16.2.2
- 大阪営業所向け IP アドレス　：172.16.3.2
- AS 番号　：1

[東京営業所]

- IP-VPN 網側ポート　：LAN0
- LAN0 側 IP アドレス　：192.168.1.1
- LAN0 側ネットワークアドレス/ネットマスク　：192.168.1.0/24
- LAN1 側 IP アドレス　：10.10.10.1
- LAN1 側ネットワークアドレス/ネットマスク　：10.10.10.0/24
- AS 番号　：65000
- 営業所内のルーティングプロトコル　：RIPv2

[横浜営業所]

- IP-VPN 網側ポート　：LAN0
- LAN0 側 IP アドレス　：192.168.2.1
- LAN0 側ネットワークアドレス/ネットマスク　：192.168.2.0/24
- LAN1 側 IP アドレス　：10.20.10.1

- LAN1 側ネットワークアドレス/ネットマスク　：10.20.10.0/24
- AS 番号　：65001

[大阪営業所]

- IP-VPN 網側ポート　：LAN0
- LAN0 側 IP アドレス　：192.168.3.1
- LAN0 側ネットワークアドレス/ネットマスク　：192.168.3.0/24
- LAN1 側 IP アドレス　：10.30.10.1
- LAN1 側ネットワークアドレス/ネットマスク　：10.30.10.0/24
- AS 番号　：65002

こんな事に気をつけて

Si-R180 でスイッチポートを利用する場合は、「2.40 スイッチポートを使う」（P.391）を参照してください。

東京営業所を設定する

● コマンド

Si-R180 の場合は、まず以下のコマンドで LAN ポートを削除します。

```
LAN ポートを削除する
# delete lan
```

Si-R180 以外の機種の場合は、以下のコマンドから設定します。

```
LAN 情報を設定する
# lan 0 ip address 192.168.1.1/24 3
# lan 0 ip route 0 172.16.1.0/24 192.168.1.2 1
# lan 1 ip address 10.10.10.1/24 3
# lan 1 ip rip use v2m v2 0 off

ルーティングプロトコル情報を設定する
# routemanage ip redist rip bgp on
# routemanage ip redist bgp rip on
# bgp as 65000
# bgp network route 0 10.10.10.0/24
# bgp neighbor 0 address 172.16.1.2
# bgp neighbor 0 as 1
# bgp neighbor 0 ebgp-multihop 2

設定終了
# save
# commit
```

横浜営業所を設定する

● コマンド

Si-R180の場合は、まず以下のコマンドでLANポートを削除します。

```
LANポートを削除する
# delete lan
```

Si-R180以外の機種の場合は、以下のコマンドから設定します。

```
LAN情報を設定する
# lan 0 ip address 192.168.2.1/24 3
# lan 0 ip nat mode off
# lan 0 ip dhcp service off
# lan 0 ip route 0 172.16.2.0/24  192.168.2.2 1
# lan 1 ip address 10.20.10.1/24 3

ルーティングプロトコル情報を設定する
# bgp as 65001
# bgp network route 0 10.20.10.0/24
# bgp neighbor 0 address 172.16.2.2
# bgp neighbor 0 as 1
# bgp neighbor 0 ebgp-multihop 2

設定終了
# save
# commit
```

大阪営業所を設定する

● コマンド

Si-R180の場合は、まず以下のコマンドでLANポートを削除します。

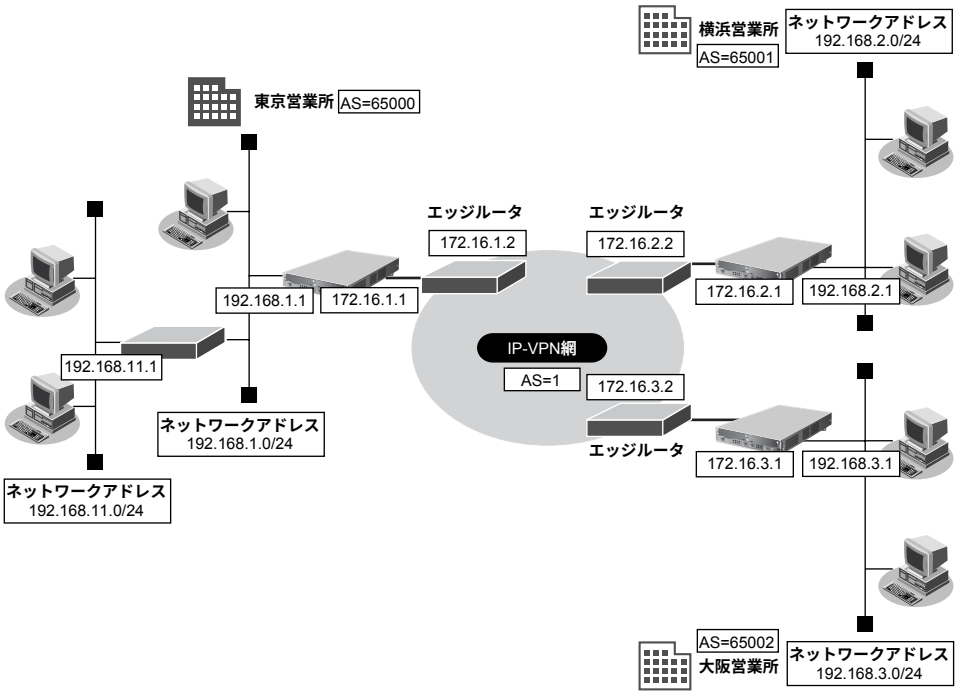
```
LANポートを削除する
# delete lan
```

Si-R180以外の機種の場合は、以下のコマンドから設定します。

```
LAN情報を設定する
# lan 0 ip address 192.168.3.1/24 3
# lan 0 ip nat mode off
# lan 0 ip dhcp service off
# lan 0 ip route 0 172.16.3.0/24 192.168.3.2 1
# lan 1 ip address 10.30.10.1/24 3

ルーティングプロトコル情報を設定する
# bgp as 65002
# bgp network route 0 10.30.10.0/24
# bgp neighbor 0 address 172.16.3.2
# bgp neighbor 0 as 1
# bgp neighbor 0 ebgp-multihop 2

設定終了
# save
# commit
```

1.13.2　高速ディジタル専用線を使用して IP-VPN 網と接続する

適用機種　*Si-R220B,370,570*



● 設定条件

- SLOT0 に実装された BRI 拡張モジュール L2 または基本ボード上の ISDN ポート（Si-R220B の場合）で専用線に接続する

[IP-VPN 網]

- 東京営業所向け IP アドレス　：172.16.1.2
- 横浜営業所向け IP アドレス　：172.16.2.2
- 大阪営業所向け IP アドレス　：172.16.3.2
- AS 番号　：1

[東京営業所]

- LAN 側の IP アドレス　：192.168.1.1
- LAN 側のネットワークアドレス/ネットマスク　：192.168.1.0/24
- サブ LAN 側のネットワークアドレス/ネットマスク　：192.168.11.0/24
- サブ LAN 側のルーティングプロトコル　：RIPv2
- WAN 側の IP アドレス　：172.16.1.1
- AS 番号　：65000

[横浜営業所]

- LAN 側の IP アドレス　：192.168.2.1
- LAN 側のネットワークアドレス/ネットマスク　：192.168.2.0/24
- WAN 側の IP アドレス　：172.16.2.1
- AS 番号　：65001

[大阪営業所]

- LAN 側の IP アドレス　：192.168.3.1
- LAN 側のネットワークアドレス/ネットマスク　：192.168.3.0/24
- WAN 側の IP アドレス　：172.16.3.1
- AS 番号　：65002

こんな事に気をつけて

Si-R220B では、利用物理回線設定でスロット番号に“mb”を指定してください。

東京営業所を設定する

● コマンド

```
回線情報を設定する
# wan 0 bind 0
# wan 0 line hsd 128k

LAN 情報を設定する
# lan 0 ip address 192.168.1.1/24 3
# lan 0 ip rip use v2m v2 0 off

接続先の情報を設定する
# remote 0 name IP-VPN
# remote 0 ap 0 name ip-vpn
# remote 0 ap 0 datalink bind wan 0
# remote 0 ip address local 172.16.1.1
# remote 0 ip address remote 172.16.1.2

ルーティングプロトコル情報を設定する
# routemanage ip redist rip bgp on
# routemanage ip redist bgp rip on
# bgp as 65000
# bgp network route 0 192.168.1.0/24
# bgp neighbor 0 address 172.16.1.2
# bgp neighbor 0 as 1

設定終了
# save
# commit
```

横浜営業所を設定する

● コマンド

```
回線情報を設定する
# wan 0 bind 0
# wan 0 line hsd 128k

LAN 情報を設定する
# lan 0 ip address 192.168.2.1/24 3

接続先の情報を設定する
# remote 0 name IP-VPN
# remote 0 ap 0 name ip-vpn
# remote 0 ap 0 datalink bind wan 0
# remote 0 ip address local 172.16.2.1
# remote 0 ip address remote 172.16.2.2

ルーティングプロトコル情報を設定する
# bgp as 65001
# bgp network route 0 192.168.2.0/24
# bgp neighbor 0 address 172.16.2.2
# bgp neighbor 0 as 1

設定終了
# save
# commit
```

大阪営業所を設定する

● コマンド

```
回線情報を設定する
# wan 0 bind 0
# wan 0 line hsd 128k

LAN 情報を設定する
# lan 0 ip address 192.168.3.1/24 3

接続先の情報を設定する
# remote 0 name IP-VPN
# remote 0 ap 0 name ip-vpn
# remote 0 ap 0 datalink bind wan 0
# remote 0 ip address local 172.16.3.1
# remote 0 ip address remote 172.16.3.2

ルーティングプロトコル情報を設定する
# bgp as 65002
# bgp network route 0 192.168.3.0/24
# bgp neighbor 0 address 172.16.3.2
# bgp neighbor 0 as 1

設定終了
# save
# commit
```

⚠注意

- **BGP4 機能を使用する場合、定期的にパケットを送信します。このため、定額制でない回線を使用している場合は、超過課金の原因となることがあります。このような環境では、BGP4 機能を使用しないでください。**
- **BGP セッションで使用する WAN インタフェースのインタフェース経路（ホストルート）を BGP で広報した場合、BGP セッションの接続・切断を繰り返す場合があります。該当するインタフェース経路は BGP で広報しないように設定してください。該当しないインタフェース経路を BGP で広報する場合は、以下のどちらかを設定してください。**
  - **BGP にインタフェース経路を再配布しないで、広報するインタフェース経路を BGP ネットワークとして設定します。**
  - **BGP にインタフェース経路を再配布し、該当するインタフェース経路を BGP フィルタリングで送信を破棄するように設定します。**

1.14 複数の事業所 LAN を VPN（IPsec）で接続する

適用機種　全機種

ここでは、VPN（IPsec）で複数の事業所を接続する場合を例に説明します。

1.14.1 NAT と併用しない固定 IP アドレスでの VPN（自動鍵交換）

IPsec 機能を使って自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社 A および支社 B は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社 A（PPPoE 常時接続）]

- ローカルネットワーク IP アドレス　：192.168.1.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス　：202.168.1.66/24
- PPPoE ユーザ認証 ID　：userid1（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass1（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[支社 B（PPPoE 常時接続）]

- ローカルネットワーク IP アドレス　：192.168.3.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス　：202.168.3.66/24
- PPPoE ユーザ認証 ID　：userid3（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass3（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IP アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IP アドレス　：202.168.2.65

こんな事に気をつけて

Si-R180 でスイッチポートを利用する場合は、「2.40 スイッチポートを使う」（P.391）を参照してください。

● 設定コマンド

[支社 A（PPPoE 常時接続）]

```
# delete lan 0
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid1 userpass1
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.1.66
```

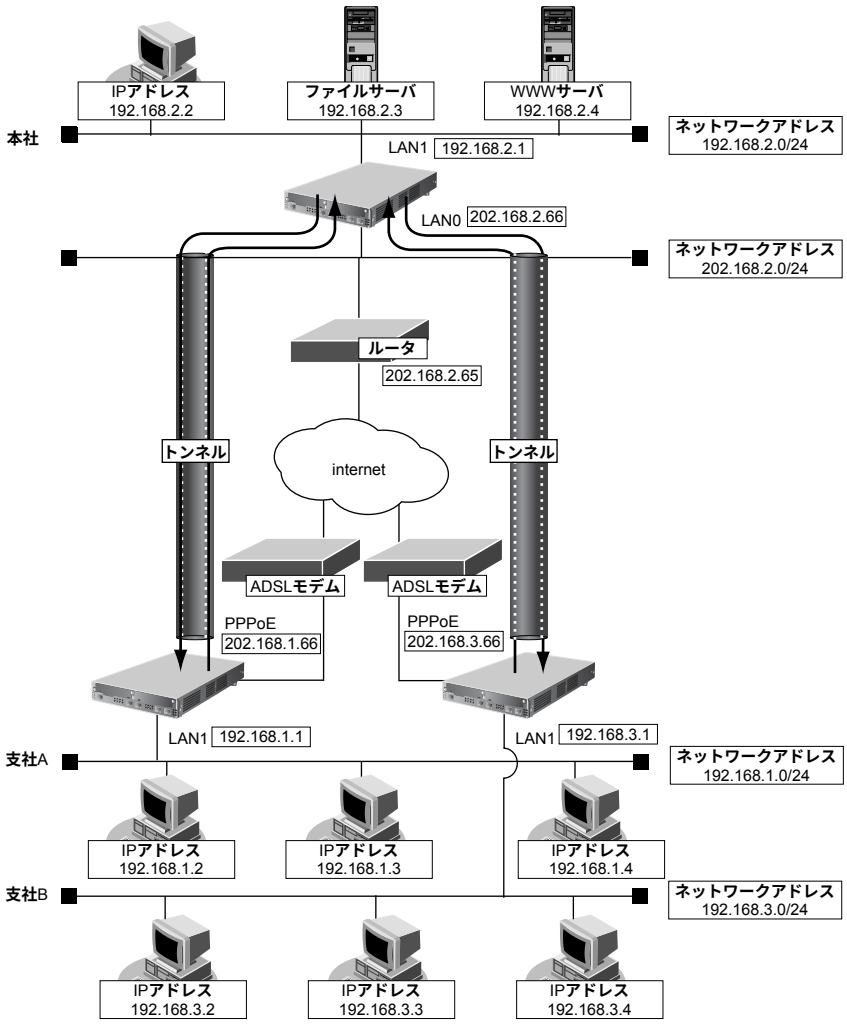
```
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
```

[支社 B（PPPoE 常時接続）]

```
# delete lan 0
# lan 0 mode auto
# lan 1 ip address 192.168.3.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid3 userpass3
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.3.66
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 1 ip address 192.168.2.1/24 3
```



● 設定条件

[支社 A]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：202.168.1.66 - 202.168.2.66
- IPsec 対象範囲　：192.168.1.0/24-any4

[支社 B]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：202.168.3.66 - 202.168.2.66
- IPsec 対象範囲　：192.168.3.0/24-any4

[本社]

- ネットワーク名　：vpn-shiA
- 接続先名　：shisyaA
- IPsec/IKE 区間　：202.168.2.66 - 202.168.1.66
- IPsec 対象範囲　：any4-192.168.1.0/24
- ネットワーク名　：vpn-shiB
- 接続先名　：shisyaB
- IPsec/IKE 区間　：202.168.2.66 - 202.168.3.66
- IPsec 対象範囲　：any4-192.168.3.0/24

[共通 A]

- 鍵交換タイプ　：Main Mode
- IPsec プトロコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

[共通 B]

- 鍵交換タイプ　：Main Mode
- IPsec プトロコル　：esp
- IPsec 暗号アルゴリズム　：3des-cbc
- IPsec 認証アルゴリズム　：hmac-sha1
- IPsec DH グループ　：なし
- IKE 認証鍵　：ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：3des-cbc
- IKE 認証アルゴリズム　：hmac-sha1
- IKE DH グループ　：modp1024

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

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。

支社 A を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.1.0/24 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

支社 B を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.3.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.3.0/24 any4
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024
```

設定終了
save
commit

本社を設定する

● コマンド

VPN を設定する
remote 0 name vpn-shiA
remote 0 ip route 0 192.168.1.0/24 1 0
remote 0 ap 0 name shisyaA
remote 0 ap 0 datalink type ipsec
remote 0 ap 0 tunnel local 202.168.2.66
remote 0 ap 0 tunnel remote 202.168.1.66
remote 0 ap 0 ipsec type ike
remote 0 ap 0 ipsec ike protocol esp
remote 0 ap 0 ipsec ike range any4 192.168.1.0/24
remote 0 ap 0 ipsec ike encrypt des-cbc
remote 0 ap 0 ipsec ike auth hmac-md5
remote 0 ap 0 ike mode main
remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
remote 0 ap 0 ike proposal encrypt des-cbc
remote 1 name vpn-shiB
remote 1 ip route 0 192.168.3.0/24 1 0
remote 1 ap 0 name shisyaB
remote 1 ap 0 datalink type ipsec
remote 1 ap 0 tunnel local 202.168.2.66
remote 1 ap 0 tunnel remote 202.168.3.66
remote 1 ap 0 ipsec type ike
remote 1 ap 0 ipsec ike protocol esp
remote 1 ap 0 ipsec ike range any4 192.168.3.0/24
remote 1 ap 0 ipsec ike encrypt 3des-cbc
remote 1 ap 0 ipsec ike auth hmac-sha1
remote 1 ap 0 ike mode main
remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
remote 1 ap 0 ike proposal encrypt 3des-cbc
remote 1 ap 0 ike proposal hash hmac-sha1
remote 1 ap 0 ike proposal pfs modp1024

設定終了
save
commit

1.14.2　NAT と併用した固定 IP アドレスでの VPN（自動鍵交換）

IPsec 機能を使って自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社 A および支社 B は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社 A（PPPoE 常時接続）]

- ローカルネットワーク IP アドレス　：192.168.1.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス　：202.168.1.66/24
- グローバルネットワーク IP アドレス　：10.0.1.1/24
- PPPoE ユーザ認証 ID　：userid1（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass1（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[支社 B（PPPoE 常時接続）]

- ローカルネットワーク IP アドレス　：192.168.3.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス　：202.168.3.66/24
- グローバルネットワーク IP アドレス　：10.0.3.1/24
- PPPoE ユーザ認証 ID　：userid3（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass3（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IP アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IP アドレス　：202.168.2.65

こんな事に気をつけて

Si-R180 でスイッチポートを利用する場合は、「2.40 スイッチポートを使う」（P.391）を参照してください。

● 設定コマンド

[支社 A（PPPoE 常時接続）]

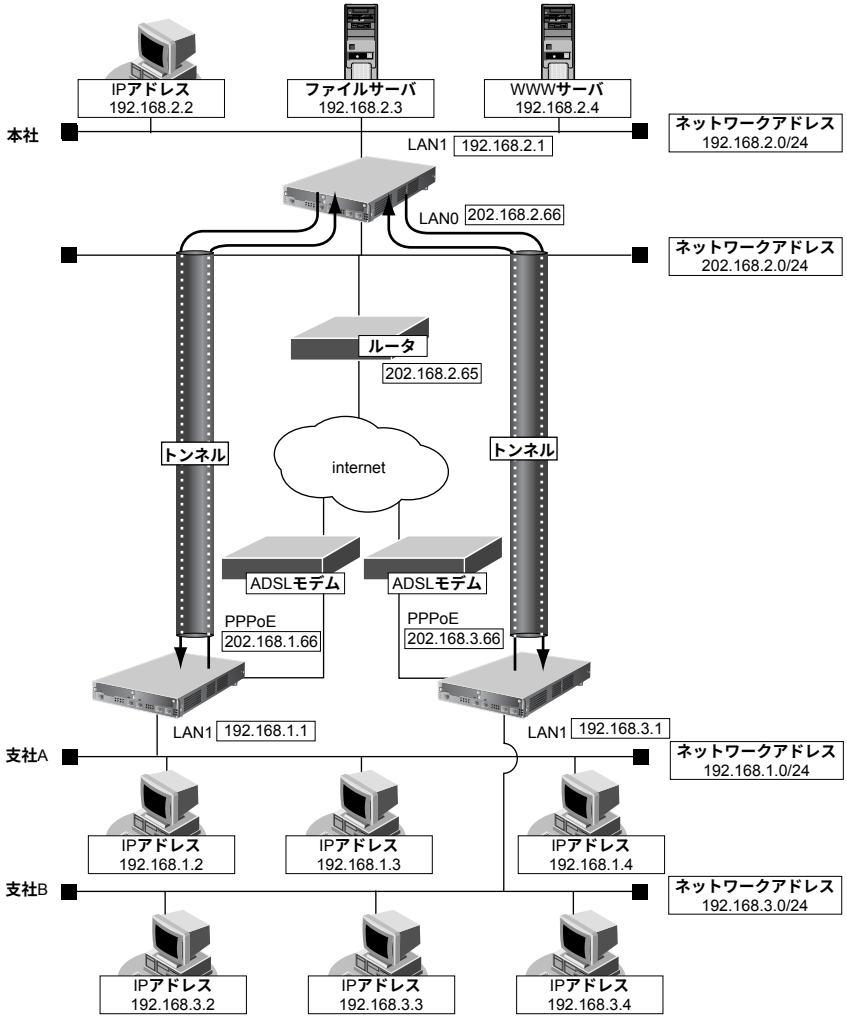
```
# delete lan 0
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid1 userpass1
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 0
# remote 0 ip nat mode multi 10.0.1.1 1 5m
# remote 0 ip msschange 1414
```

[支社 B（PPPoE 常時接続）]

```
# delete lan 0
# lan 0 mode auto
# lan 1 ip address 192.168.3.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid3 userpass3
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.3.66
# remote 0 ip route 0 default 1 0
# remote 0 ip nat mode multi 10.0.3.1 1 5m
# remote 0 ip msschange 1414
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 1 ip address 192.168.2.1/24 3
```



● 設定条件

[支社 A]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：10.0.1.1 - 202.168.2.66
- IPsec 対象範囲　：192.168.1.0/24-any4

[支社 B]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：10.0.3.1 - 202.168.2.66
- IPsec 対象範囲　：192.168.3.0/24-any4

[本社]

- ネットワーク名　：vpn-shiA
- 接続先名　：shisyaA
- IPsec/IKE 区間　：202.168.2.66 - 10.0.1.1
- IPsec 対象範囲　：any4-192.168.1.0/24
- ネットワーク名　：vpn-shiB
- 接続先名　：shisyaB
- IPsec/IKE 区間　：202.168.2.66 - 10.0.3.1
- IPsec 対象範囲　：any4-192.168.3.0/24

[共通 A]

- 鍵交換タイプ　：Main Mode
- IPsec プトロコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

[共通 B]

- 鍵交換タイプ　：Main Mode
- IPsec プトロコル　：esp
- IPsec 暗号アルゴリズム　：3des-cbc
- IPsec 認証アルゴリズム　：hmac-sha1
- IPsec DH グループ　：なし
- IKE 認証鍵　：ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：3des-cbc
- IKE 認証アルゴリズム　：hmac-sha1
- IKE DH グループ　：modp1024

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

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。

支社 A を設定する

● コマンド

```
インターネットへ IPsec/IKE パケットを送信する設定をする
# remote 0 ip nat static 0 202.168.1.66 500 10.0.1.1 500 17
# remote 0 ip nat static 1 202.168.1.66 any 10.0.1.1 any 50

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.1.0/24 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

支社 B を設定する

● コマンド

```
インターネットへ IPsec/IKE パケットを送信する設定をする
# remote 0 ip nat static 0 202.168.3.66 500 10.0.3.1 500 17
# remote 0 ip nat static 1 202.168.3.66 any 10.0.3.1 any 50

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.3.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
```

```
# remote 1 ap 0 ipsec ike range 192.168.3.0/24 any4
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024

設定終了
# save
# commit
```

本社を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shiA
# remote 0 ip route 0 192.168.1.0/24 1 0
# remote 0 ap 0 name shisyaA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 tunnel remote 10.0.1.1
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 192.168.1.0/24
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode main
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 1 name vpn-shiB
# remote 1 ip route 0 192.168.3.0/24 1 0
# remote 1 ap 0 name shisyaB
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ap 0 tunnel remote 10.0.3.1
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 192.168.3.0/24
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024

設定終了
# save
# commit
```

1.14.3　NAT と併用した可変 IP アドレスでの VPN（自動鍵交換）

接続するたびに IP アドレスが変わる環境で VPN を構築する場合の設定方法を説明します。

ここでは、以下のコマンドによって、支社 A および支社 B は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社 A（PPPoE 接続）]

- ローカルネットワーク IP アドレス　：192.168.1.1/24
- PPPoE ユーザ認証 ID　：userid1（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass1（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[支社 B（PPPoE 接続）]

- ローカルネットワーク IP アドレス　：192.168.3.1/24
- PPPoE ユーザ認証 ID　：userid3（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass3（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IP アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IP アドレス　：202.168.2.65

こんな事に気をつけて

Si-R180 **でスイッチポートを利用する場合は、**「2.40 スイッチポートを使う」（P.391）**を参照してください。**

● 設定コマンド

[支社 A（PPPoE 接続）]

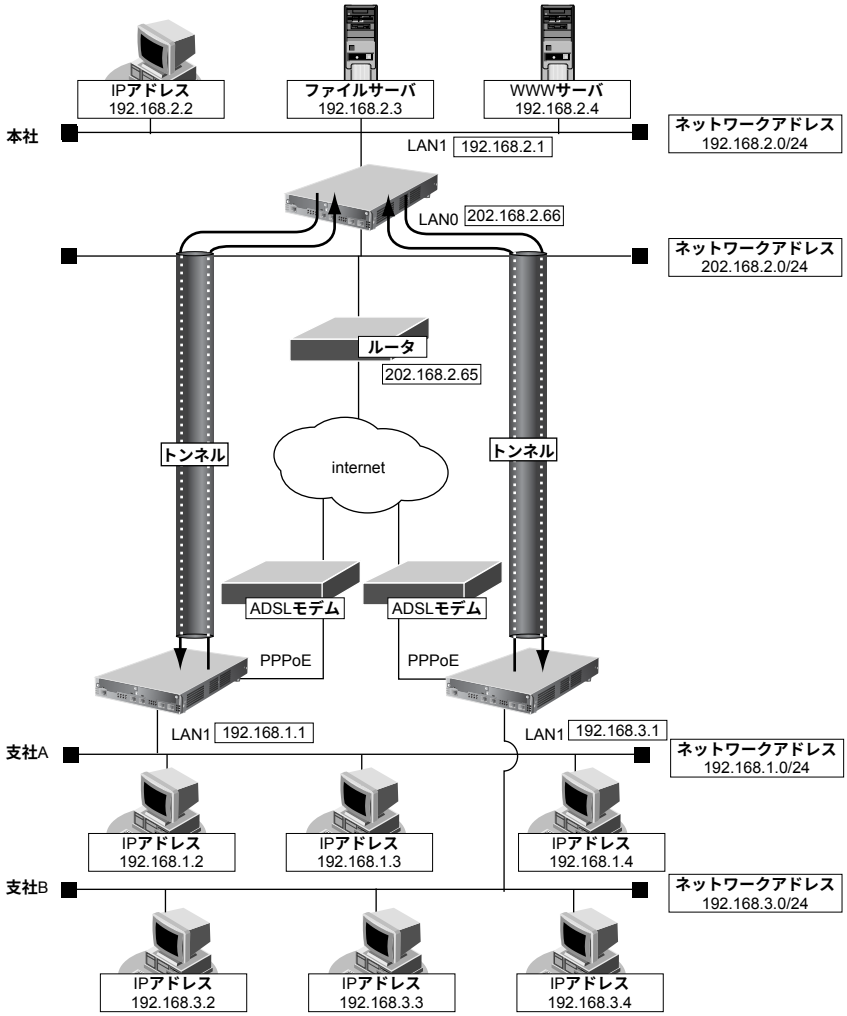
```
# delete lan 0
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 0
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid1 userpass1
```

[支社 B（PPPoE 接続)]

```
# delete lan 0
# lan 0 mode auto
# lan 1 ip address 192.168.3.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 0
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid3 userpass3
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 1 ip address 192.168.2.1/24 3
```



● 設定条件

[支社 A（Initiator)]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：支社 A - 202.168.2.66
- IPsec 対象範囲　：192.168.1.0/24-any4
- IKE（UDP：500 番ポート）のプライベートアドレス　：192.168.1.1
- ESP のプライベートアドレス　：192.168.1.1

[支社 B（Initiator)]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：支社 B - 202.168.2.66
- IPsec 対象範囲　：192.168.3.0/24-any4
- IKE（UDP：500 番ポート）のプライベートアドレス　：192.168.3.1
- ESP のプライベートアドレス　：192.168.3.1

[本社]

- ネットワーク名　：vpn-shiA
- 接続先名　：shisyaA
- IPsec/IKE 区間　：202.168.2.66 - 支社 A
- IPsec 対象範囲　：any4-192.168.1.0/24
- ネットワーク名　：vpn-shiB
- 接続先名　：shisyaB
- IPsec/IKE 区間　：202.168.2.66 - 支社 B
- IPsec 対象範囲　：any4-192.168.3.0/24

[共通 A]

- 鍵交換タイプ　：Aggressive Mode
- IPsec プトロコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 支社 A ID ／ ID タイプ　：shisyaA（自装置名）／ FQDN
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

[共通 B]

- 鍵交換タイプ　：Aggressive Mode
- IPsec プトロコル　：esp
- IPsec 暗号アルゴリズム　：3des-cbc
- IPsec 認証アルゴリズム　：hmac-sha1
- IPsec DH グループ　：なし
- IKE 支社 B ID ／ ID タイプ　：shisyaB（自装置名）／ FQDN
- IKE 認証鍵　：ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：3des-cbc
- IKE 認証アルゴリズム　：hmac-sha1
- IKE DH グループ　：modp1024

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは？

Aggressive Mode **の場合に、ネゴシエーションで使用する自装置を識別する** ID **の種別です。相手** VPN **装置の設定に合わせます。**

こんな事に気をつけて

可変 IP アドレスでの VPN 接続を行うときは、インターネットプロバイダから割り当てられる IP アドレスが不定であるため、ローカルネットワーク IP アドレスで IKE ネゴシエーションを行う場合があります。このような運用では、送出インタフェースで NAT 機能を使用してください。

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。

支社 A（Initiator）を設定する

● コマンド

```
インターネットから IPsec/IKE パケットを受信する設定をする
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.1.0/24 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisyaA
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

支社 B（Initiator）を設定する

● コマンド

```
インターネットから IPsec/IKE パケットを受信する設定をする
# remote 0 ip nat static 0 192.168.3.1 500 any 500 17
# remote 0 ip nat static 1 192.168.3.1 any any any 50

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.3.0/24 any4
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisyaB
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024

設定終了
# save
# commit
```

本社（Responder）を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shiA
# remote 0 ip route 0 192.168.1.0/24 1 0
# remote 0 ap 0 name shisyaA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 192.168.1.0/24
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode aggressive
# remote 0 ap 0 ike name remote shisyaA
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 1 name vpn-shiB
# remote 1 ip route 0 192.168.3.0/24 1 0
# remote 1 ap 0 name shisyaB
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 192.168.3.0/24
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name remote shisyaB
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024

設定終了
# save
# commit
```

1.15 IPv6の事業所LANをISDNで接続する

適用機種 *Si-R220B,370,570*

ここでは、ISDN回線を介して2つの事業所（東京、川崎）のIPv6ネットワークを接続する場合を例に説明します。

こんな事に気をつけて

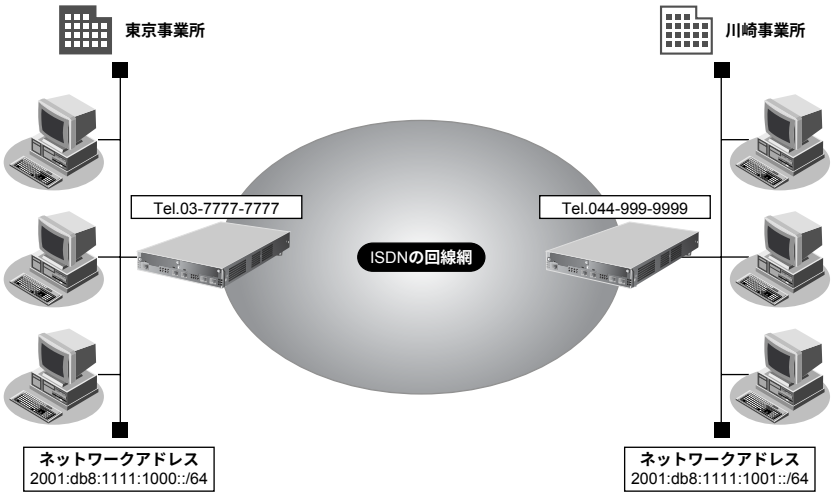
この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。

☛ 参照 Si-Rシリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.49）

- **双方の事業所から同時に発信が行われた場合、両方の接続が成立することでその接続が超過課金（2倍）になる場合があります。これは、接続優先制御機能を利用して片方の接続のみが存続するようにすることで防ぐことができます。**

☛ 参照 Si-Rシリーズ　コマンドリファレンス「remote ap connect priority」

この機能を利用する場合は、双方の事業所の装置で同じ接続優先設定を行わないでください。同時発信の際に接続ができなくなります。この機能を利用する場合は、以下の設定を奨励します。
- **一方の装置で着信接続を優先する。**
- **一方の装置で接続優先制御を行わない。**



● 設定条件

- SLOT0 に実装された BRI 拡張モジュール L2 または基本ボード上の ISDN ポート（Si-R220B の場合）で ISDN（64Kbps）を使用する
- IPv6 を使用する
- スタティック経路機能を使用する
- 接続ネットワーク名　：kaisya
- 無通信監視時間を 1 分とする

[東京事業所]

- ネットワークアドレス/プレフィックス長　：2001:db8:1111:1000::/64
- 接続先名　：tokyo
- 電話番号　：03-7777-7777
- ユーザ認証 ID とユーザ認証パスワード
  発信　：tokyo、tokyopass
  着信　：kawasaki、kawapass

[川崎事業所]

- ネットワークアドレス/プレフィックス長　：2001:db8:1111:1001::/64
- 接続先名　：kawasaki
- 電話番号　：044-999-9999
- ユーザ認証 ID とユーザ認証パスワード
  発信　：kawasaki、kawapass
  着信　：tokyo、tokyopass

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 Si-R シリーズ　コマンドユーザーズガイド「1.7 コマンドで入力できる文字一覧」（P26）

- **Si-R220B では、利用物理回線設定でスロット番号に "mb" を指定してください。**

東京事業所の本装置を設定する

● コマンド

```
回線情報を設定する
# wan 0 bind 0
# wan 0 line isdn

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

接続先の情報を設定する
# remote 0 name kaisya
# remote 0 ap 0 name kawasaki
# remote 0 ap 0 datalink bind wan 0
# remote 0 ap 0 dial 0 number 044-999-9999
# remote 0 ap 0 dial 0 speed 64K
# remote 0 ap 0 ppp auth type any
# remote 0 ap 0 ppp auth send tokyo tokyopass
# remote 0 ap 0 ppp auth receive kawasaki kawapass
# remote 0 ap 0 idle 1m
# remote 0 ip6 use on
# remote 0 ip6 route 0 2001:db8:1111:1001::/64 1

設定終了
# save

再起動
# reset
```

⚠注意

ISDN またはフレームリレーの場合、RIP（IPv6）を送信しないでください。RIP（IPv6）を送信すると、思わぬ課金（定期発信または長時間接続）が発生します。

川崎事業所の本装置を設定する

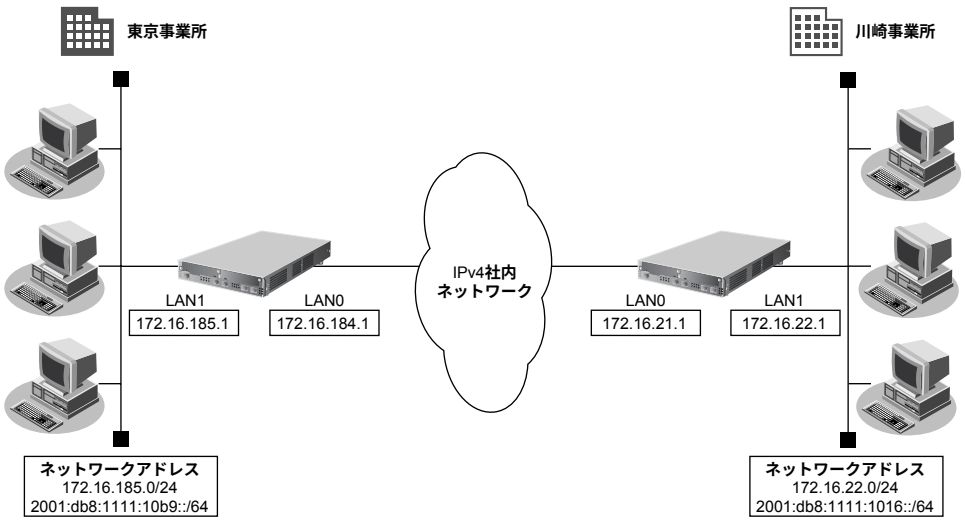
● コマンド

```
回線情報を設定する
# wan 0 bind 0
# wan 0 line isdn

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

接続先の情報を設定する
# remote 0 name kaisya
# remote 0 ap 0 name tokyo
# remote 0 ap 0 datalink bind wan 0
# remote 0 ap 0 dial 0 number 03-7777-7777
# remote 0 ap 0 dial 0 speed 64K
# remote 0 ap 0 ppp auth type any
# remote 0 ap 0 ppp auth send kawasaki kawapass
# remote 0 ap 0 ppp auth receive tokyo tokyopass
# remote 0 ap 0 idle 1m
# remote 0 ip6 use on
# remote 0 ip6 route 0 2001:db8:1111:1000::/64 1

設定終了
# save

再起動
# reset
```

1.16 IPv6の事業所LANをIPv6トンネルで接続する

適用機種　全機種

ここでは、IPv4で構築されたイントラネットを介して、2つの事業所（東京、川崎）のIPv6ネットワークどうしを接続（トンネリング）する場合を例に説明します。



● 設定条件

[東京事業所]

- ダイナミックルーティングを使用する
- LAN0側のIPv4アドレス　：172.16.184.1
- LAN1側のIPv4アドレス　：172.16.185.1
- LAN1側のIPv6プレフィックス/プレフィックス長　：2001:db8:1111:10b9::/64（※）

[川崎事業所]

- ダイナミックルーティングを使用する
- LAN0側のIPv4アドレス　：172.16.21.1
- LAN1側のIPv4アドレス　：172.16.22.1
- LAN1側のIPv6プレフィックス/プレフィックス長　：2001:db8:1111:1016::/64（※）

※）　この例では、プライベートアドレス（IPv4）／ドキュメント記述用アドレス（IPv6）を使用しています。

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 Si-Rシリーズ　コマンドユーザーズガイド「1.7 コマンドで入力できる文字一覧」（P.26）

- **IPv6 over IPv4トンネルを利用する場合は、カプセル化されたIPv4パケットのフラグメントを防ぐため、トンネルに利用する相手情報のMTUに1280を設定してください。**
- **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。**
- **Si-R180でスイッチポートを利用する場合は、「2.40 スイッチポートを使う」（P.391）を参照してください。**

東京事業所を設定する

● コマンド

```
IPv4 で事業所間を接続する
# lan 0 ip address 172.16.184.1/24 3
# lan 0 ip rip use v1 v1 0
# lan 0 ip dhcp service off
# lan 0 ip nat mode off
# lan 1 ip address 172.16.185.1/24 3
# lan 1 ip rip use v1 v1 0
# lan 1 ip dhcp service off
# lan 1 ip nat mode off

IPv6 情報を設定する
# lan 1 ip6 use on
# lan 1 ip6 ifid auto
# lan 1 ip6 address 0 2001:db8:1111:10b9::/64 30d 7d c0
# lan 1 ip6 ra mode send

IP トンネル接続（川崎事業所）の情報を設定する
# remote 0 name v6kawasa
# remote 0 mtu 1280
# remote 0 ap 0 name tun-kawa
# remote 0 ap 0 datalink type ip
# remote 0 ap 0 tunnel local 172.16.184.1
# remote 0 ap 0 tunnel remote 172.16.21.1
# remote 0 ip6 use on
# remote 0 ip6 route 0 2001:db8:1111:1016::/64 1

設定終了
# save

再起動
# reset
```

川崎事業所を設定する

● コマンド

```
IPv4 で事業所間を接続する
# lan 0 ip address 172.16.21.1/24 3
# lan 0 ip rip use v1 v1 0 off
# lan 0 ip dhcp service off
# lan 0 ip nat mode off
# lan 1 ip address 172.16.22.1/24 3
# lan 1 ip rip use v1 v1 0
# lan 1 ip dhcp service off
# lan 1 ip nat mode off

IPv6 情報を設定する
# lan 1 ip6 use on
# lan 1 ip6 ifid auto
# lan 1 ip6 address 0 2001:db8:1111:1016::/64 30d 7d c0
# lan 1 ip6 ra mode send

IP トンネル接続（東京事業所）の情報を設定する
# remote 0 name v6tokyo
# remote 0 mtu 1280
# remote 0 ap 0 name tun-tkyo
# remote 0 ap 0 datalink type ip
# remote 0 ap 0 tunnel local 172.16.21.1
# remote 0 ap 0 tunnel remote 172.16.184.1
# remote 0 ip6 use on
# remote 0 ip6 route 0 2001:db8:1111:10b9::/64 1

設定終了
# save

再起動
# reset
```

ヒント

◆ NAT と IPv6 over IPv4 トンネルを併用する

IPv4 環境の NAT と、IPv6 over IPv4 トンネルを利用した IPv6 通信環境を併用する場合は、IPv4 環境の NAT の処理によって、IPv4 アドレスがどのように変換処理されるかを判断して IPv6 over IPv4 トンネル通信の設定を行う必要があります。

本装置では、トンネル処理は NAT 処理の内側（プライベートアドレス側）で行われますので、以下のように設定します。

設定項目	設定内容
自側エンドポイント	以下の IP アドレスのどちらかを設定します。 • LAN に設定された IP アドレスまたはセカンダリ IP アドレス • remote ip address local コマンドで設定した自側 IP アドレス ※）PPP で割り当てられる IP アドレスは利用できません。
相手側エンドポイント	相手トンネル GW の IP アドレス
静的 NAT	IPv6 over IPv4 トンネル通信が相手トンネル GW 側から開始されることがある場合は、静的 NAT の設定が必要となります。 • プライベート IP 情報 IP アドレス　自側エンドポイントに設定したアドレス ポート番号　すべて • グローバル IP 情報 IP アドレス　相手トンネル GW に設定された、本装置側のアドレス ポート番号　すべて • プロトコル　IPv6 over IPv4

具体例を以下に示します。

条件：

- 本装置の NAT 変換で利用するグローバルアドレスに 172.16.0.1 を利用
- 本装置のプライベート LAN 側に 192.168.1.1 を利用
- 相手トンネル GW の IP アドレスに 172.31.0.1 を利用

IPv6 over IPv4 トンネル接続：

- 本装置のトンネル通信の設定：
  192.168.1.1 と 172.31.0.1 の間でトンネル通信を行うことを前提に、以下のとおり設定します。
  remote 0 ap 0 tunnel local 192.168.1.1
  remote 0 ap 0 tunnel remote 172.31.0.1

静的 NAT 設定：

- lan 0 ip nat static 0 192.168.1.1 any 172.16.0.1 any 41

なお、この具体例で、相手トンネル GW の設定は、以下のとおりです。

172.16.0.1 と 172.31.0.1 の間でトンネル通信を行うことを前提とします。

相手トンネル GW に Si-R シリーズ（NAT 未使用）を利用する場合は、相手側の Si-R に以下を設定します。

remote 0 ap 0 tunnel local 172.31.0.1
remote 0 ap 0 tunnel remote 172.16.0.1

第２章　活用例

この章では、本装置の便利な機能の活用方法について説明します。

2.1　RIP の経路を制御する（IPv4）

適用機種　全機種

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

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

補足　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。

ヒント

◆ IP アドレスとアドレスマスクの決め方

フィルタリング条件の要素には、「IP アドレス」と「アドレスマスク」があります。制御対象となる経路情報は、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

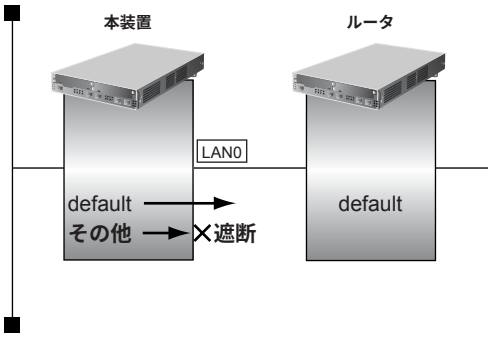
こんな事に気をつけて

- **フィルタリング条件には、優先度を示す定義番号があり、小さい値ほど、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。**

2.1.1　特定の経路情報の送信を許可する

適用機種　全機種

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。



● 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

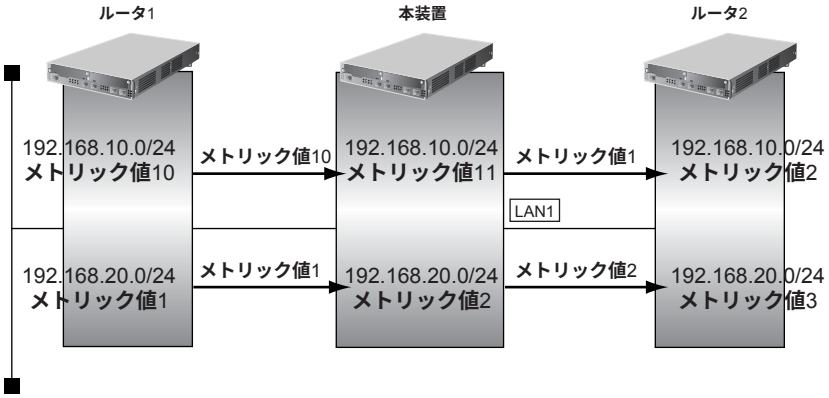
```
デフォルトルートを透過させる
# lan 0 ip rip filter 0 act pass out
# lan 0 ip rip filter 0 route default

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
```

2.1.2　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　全機種

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。



● 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
# lan 1 ip rip filter 1 act pass out
# lan 1 ip rip filter 1 route any

設定終了
# save
# commit
```

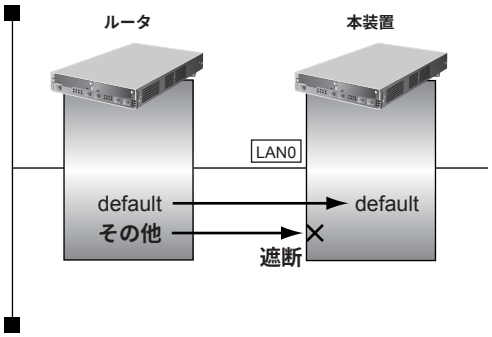
こんな事に気をつけて

- **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。**

2.1.3　特定の経路情報の受信を許可する

適用機種　全機種

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。



● 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。

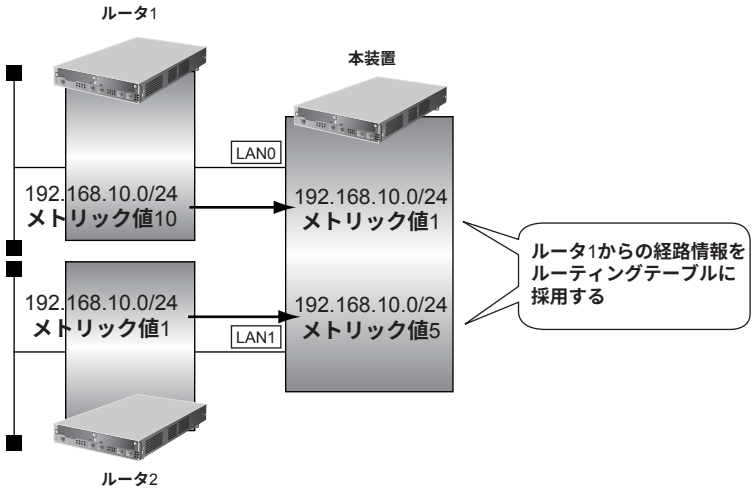
● コマンド

```
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
```

2.1.4　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　全機種

ここでは、本装置が、ルータ 1 とルータ 2 から同じあて先への経路情報 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。



● 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
```

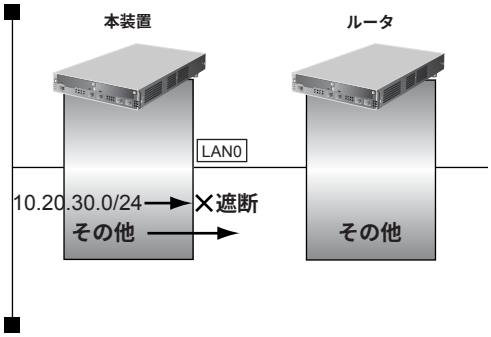
こんな事に気をつけて

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。

2.1.5　特定の経路情報の送信を禁止する

適用機種　全機種

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。



● 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。

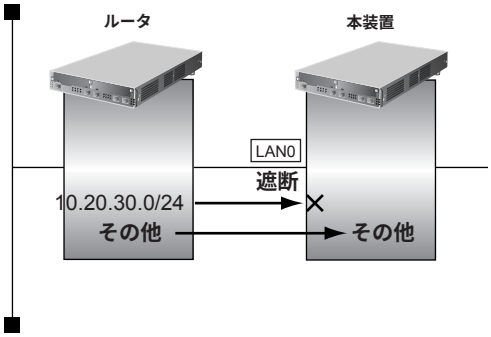
● コマンド

```
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
```

2.1.6　特定の経路情報の受信を禁止する

適用機種　全機種

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。



● 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
```

2.2　RIP の経路を制御する（IPv6）

適用機種　全機種

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

補足　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。

ヒント

◆ 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だけです。

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

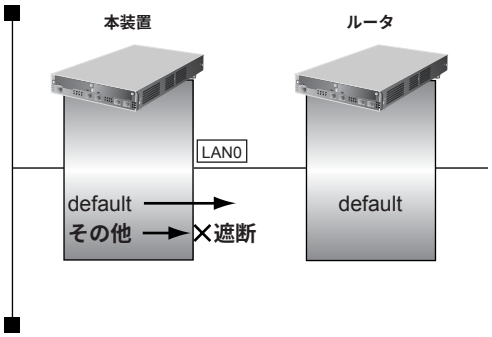
こんな事に気をつけて

フィルタリング条件には、優先度を示す定義番号があり、小さい値ほど、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。

2.2.1　特定の経路情報の送信を許可する

適用機種　全機種

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。



● 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

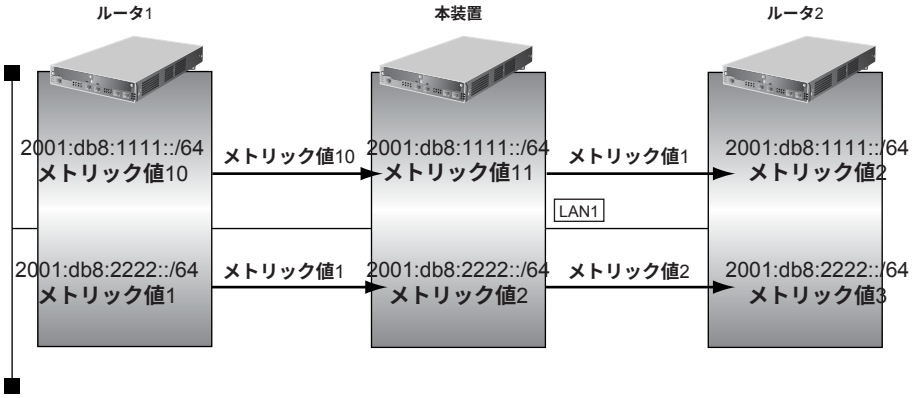
```
デフォルトルートを透過させる
# lan 0 ip6 rip filter 0 act pass out
# lan 0 ip6 rip filter 0 route default

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
```

2.2.2　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　全機種

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。



● 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
```

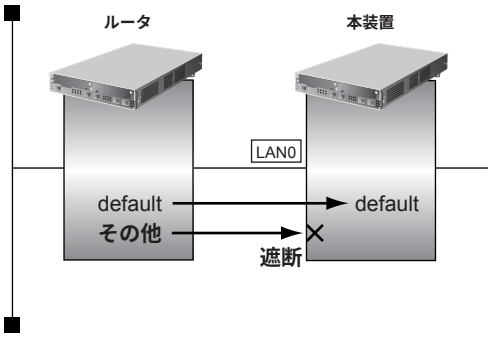
こんな事に気をつけて

- **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。**

2.2.3　特定の経路情報の受信を許可する

適用機種　全機種

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。



● 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。

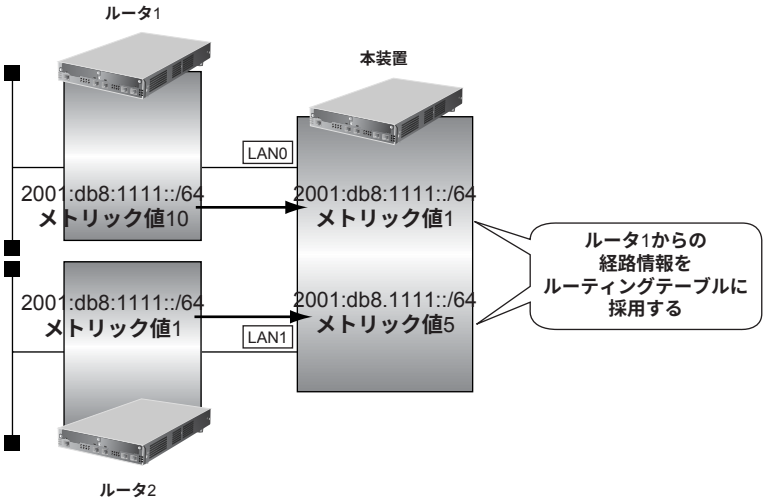
● コマンド

```
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
```

2.2.4　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　全機種

ここでは、本装置が、ルータ 1 とルータ 2 から同じあて先への経路情報 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。



● 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
```

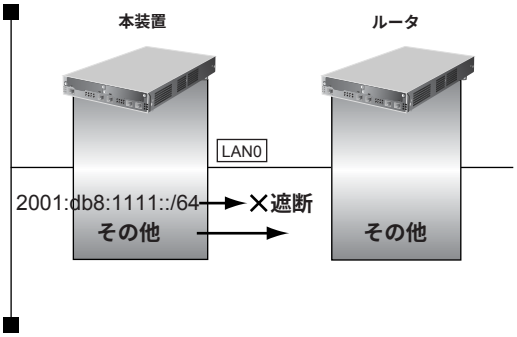
こんな事に気をつけて

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。

2.2.5　特定の経路情報の送信を禁止する

適用機種　全機種

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。



● 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。

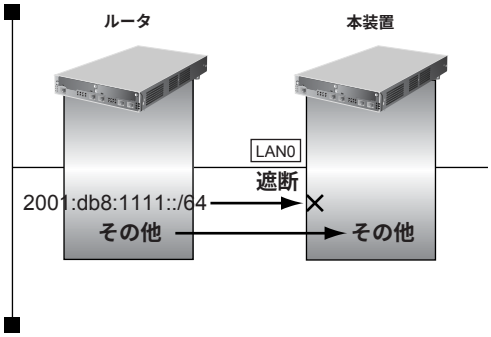
● コマンド

```
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
```

2.2.6　特定の経路情報の受信を禁止する

適用機種　全機種

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。



● 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
```

2.3 OSPFv2 を使用したネットワークを構築する（IPv4）

適用機種　全機種

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。

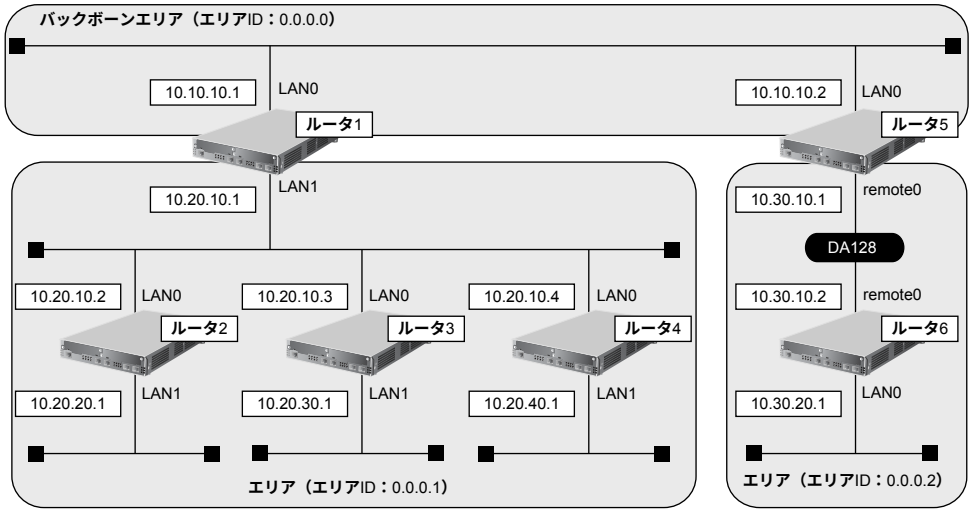
エリア境界ルータでは、エリア内の経路情報を集約して広報することができます。

参照　Si-R シリーズ　機能説明書「2.5 OSPF 機能」（P.34）

こんな事に気をつけて

- NAT 機能と併用することはできません。
- 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 ルータどうしは、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も、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。

	Si-R180、220B、240、260B	Si-R370、570
インタフェース数	（30000 ÷本装置保有 LSA 数）未満	（50000 ÷本装置保有 LSA 数）未満
通信速度	15Kbps 以上の通信帯域を確保する必要があります。	



ここでは、ルータ 5 とルータ 6 が専用線（remote 定義）で接続され、以下のとおりに設定されていることを前提とします。

● 前提条件

- ルータ 1 からルータ 6 のすべてのインタフェースに IP アドレスを設定する
- ルータ 1 からルータ 6 のすべてのインタフェースで NAT 機能および DHCP クライアント機能を使用しない

● 設定条件

- ルータ 5 およびルータ 6 は、SLOT0 に実装された BRI 拡張モジュール L2 または基本ボード上の ISDN ポート（Si-R220B の場合）で専用線に接続する

[ルータ 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

[ルータ 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

[ルータ 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

[ルータ 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
- LAN1 での passive-interface 設定　：設定する
- LAN0 でのルータ優先度　：1

[ルータ 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
- remote0 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
- remote0 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

[ルータ 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
- remote0 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
- remote0 での OSPF エリア ID　：0.0.0.2
- LAN0 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。

ルータ 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
```

ルータ 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
```

ルータ 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
```

ルータ 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
```

ルータ 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

接続先の情報を設定する
# remote 0 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
```

ルータ 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 0 ip ospf passive on

接続先の情報を設定する
# remote 0 ip ospf use on 0

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

設定終了
# save
# commit
```

こんな事に気をつけて

WAN 回線で使用する場合は、WAN 側 IP アドレスを必ず設定してください。

⚠注意

OSPF 機能を使用する場合、定期的にパケットを送信します。このため、定額制でない回線を使用している場合は、超過課金の原因となることがあります。このような環境では、OSPF 機能は使用しないでください。

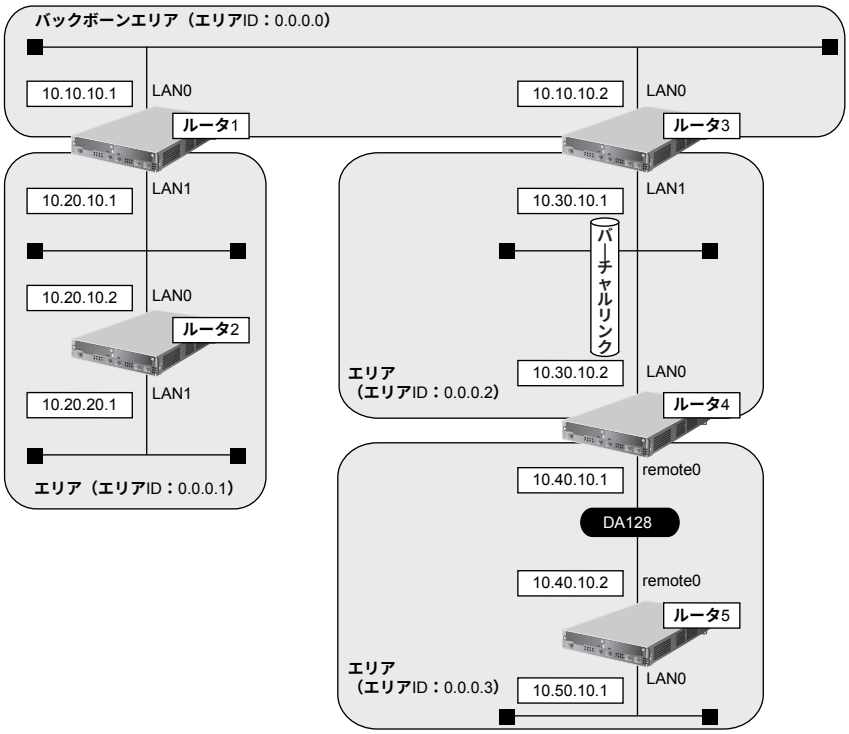
2.3.1　バーチャルリンクを使う

適用機種　全機種

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。**



ここでは、ルータ 4 とルータ 5 が専用線（remote 定義）で接続され、以下のとおりに設定されていることを前提とします。

● 前提条件

- ルータ 1 からルータ 5 のすべてのインタフェースに IP アドレスを設定する
- ルータ 1 からルータ 5 のすべてのインタフェースで NAT 機能および DHCP クライアント機能を使用しない

● 設定条件

- ルータ 4 およびルータ 5 は、SLOT0 に実装された BRI 拡張モジュール L2 または基本ボード上の ISDN ポート（Si-R220B の場合）で専用線に接続する

[ルータ 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

[ルータ 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

[ルータ 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

[ルータ 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
- remote0 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
- remote0 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

[ルータ 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
- remote0 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
- remote0 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。

ルータ 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
```

ルータ 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
```

ルータ 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
```

ルータ 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

接続先（ルータ 5）の情報を設定する
# remote 0 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
```

ルータ 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

接続先（ルータ 4）の情報を設定する
# remote 0 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
```

2.3.2　スタブエリアを使う

適用機種　全機種

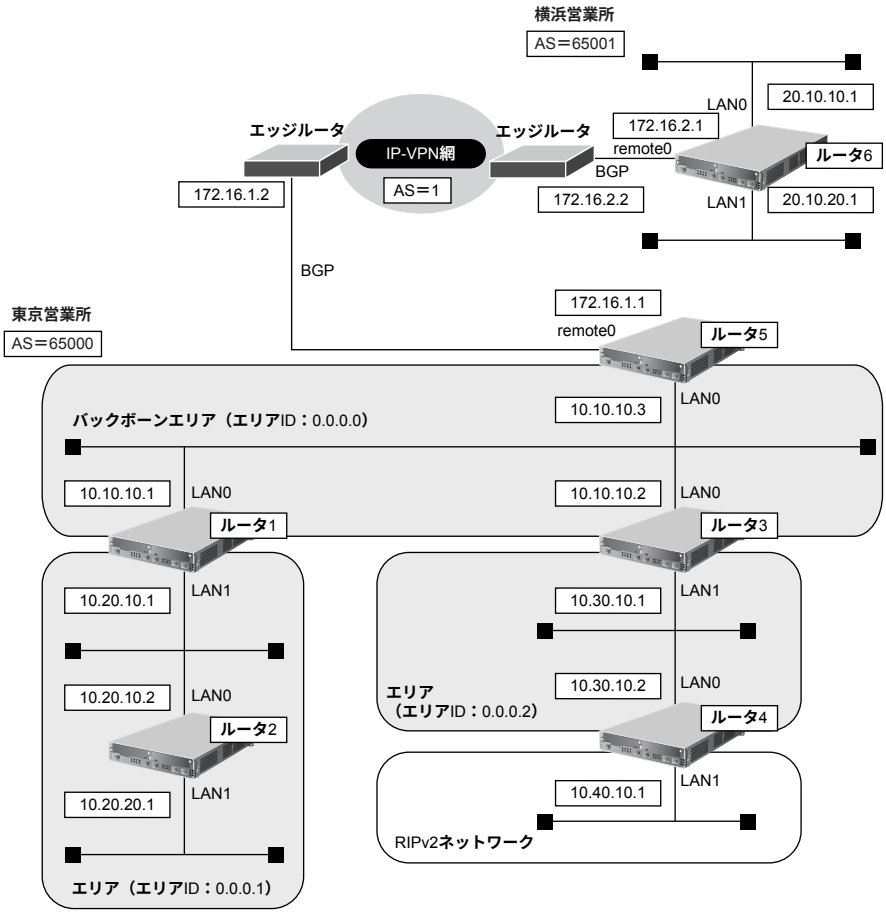
OSPF 以外のルーティングプロトコルを使用したネットワークとの接続の設定について説明します。

OSPF は、RIP または BGP 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 および BGP 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。



ここでは、ルータ 5 とルータ 6 が専用線（remote 定義）で IP-VPN 網に接続され、以下のとおりに設定されていることを前提とします。

● 前提条件

- ルータ 1 からルータ 6 のすべてのインタフェースに IP アドレスを設定する
- ルータ 1 からルータ 6 のすべてのインタフェースで NAT 機能および DHCP クライアント機能を使用しない

● 設定条件

- ルータ 5 およびルータ 6 は、SLOT0 に実装された BRI 拡張モジュール L2 または基本ボード上の ISDN ポート（Si-R220B の場合）で専用線に接続する

[東京営業所]

[ルータ 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

[ルータ 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

[ルータ 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

[ルータ 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

[ルータ 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
- remote0 でのルーティングプロトコル　：BGP
- LAN0 での OSPF エリア ID　：0.0.0.0
- BGP 経路の OSPF での広報　：再配布する
- BGP AS 番号　：65000
- BGP ネットワークの IGP との同期　：同期させる
- BGP ネットワーク　：10.10.10.0/24
- BGP 集約経路　：10.0.0.0/8
- AS 外部経路の集約　：20.10.0.0/16

[横浜営業所]

[ルータ 6 でのルーティングプロトコル情報]

- BGP AS 番号　：65001
- BGP ネットワークの IGP との同期　：同期させる
- BGP ネットワーク　：20.10.10.0/24、20.10.20.0/24

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。

ルータ 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
```

ルータ 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
```

ルータ 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
```

ルータ 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 redist ospf rip on
# routemanage ip redist 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
```

ルータ 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

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

BGP 情報を設定する
# bgp as 65000
# bgp neighbor 0 address 172.16.1.2
# bgp neighbor 0 as 1
# bgp network igp on
# bgp network route 0 10.10.10.0/24
# bgp aggregate 0 10.0.0.0/8 summary-only

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.0
# ospf ip summary 0 20.10.0.0/16

設定終了
# save
# commit
```

ルータ 6 を設定する

● コマンド

```
BGP 情報を設定する
# bgp as 65001
# bgp neighbor 0 address 172.16.2.2
# bgp neighbor 0 as 1
# bgp network igp on
# bgp network route 0 20.10.10.0/24
# bgp network route 1 20.10.20.0/24

設定終了
# save
# commit
```

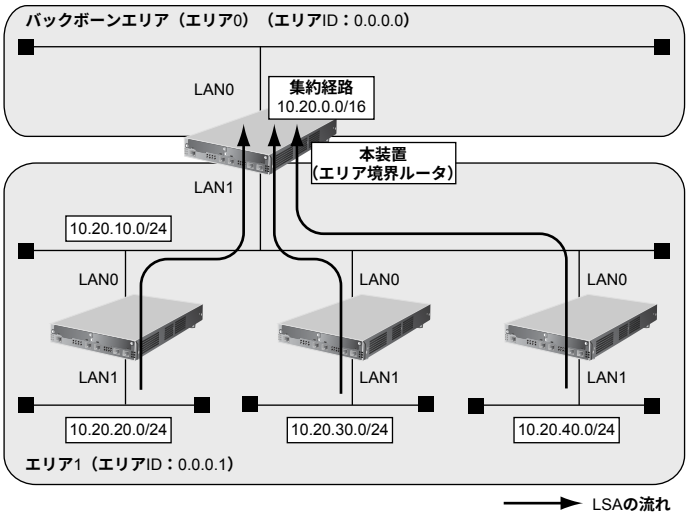
2.4　OSPFの経路を制御する（IPv4）

適用機種　全機種

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。

2.4.1　OSPFネットワークでエリアの経路情報（LSA）を集約する

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。



● 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

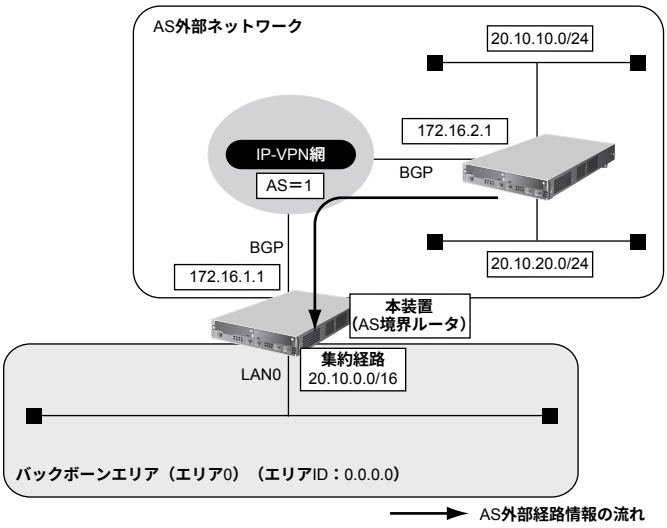
上記の経路情報に従って設定する場合のコマンド例を示します。

● 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
```

2.4.2　AS 外部経路を集約して OSPF ネットワークに広報する

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。



● 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
- remote0 でのルーティングプロトコル　：BGP
- 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

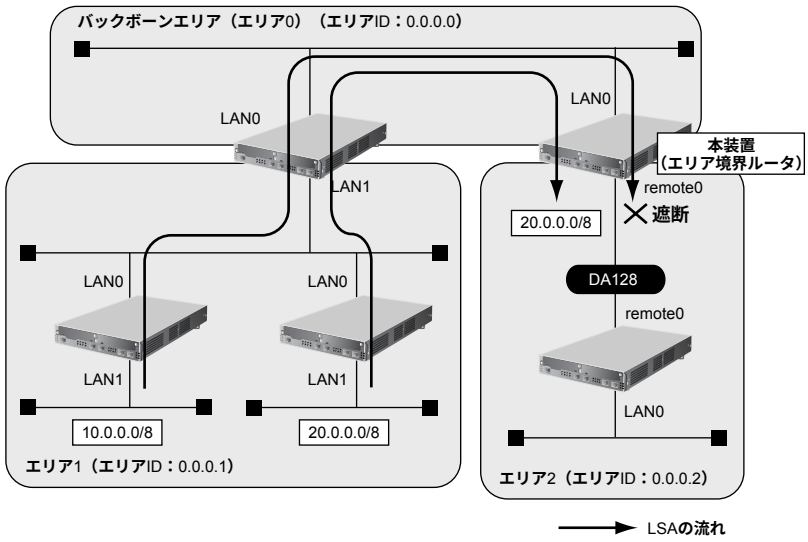
上記の経路情報に従って設定する場合のコマンド例を示します。

● 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

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 redist ospf bgp 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 redist 0 pass 20.10.0.0/16 inexact
# ospf ip redist 1 reject any

設定終了
# save
# commit
```

2.4.3　エリア境界ルータで不要な経路情報（LSA）を遮断する

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。



● 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
- remote0 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
- remote0 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 で使用するインタフェースを設定する
# lan 0 ip ospf use on 0
# remote 0 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
```

2.5　BGP の経路を制御する（IPv4）

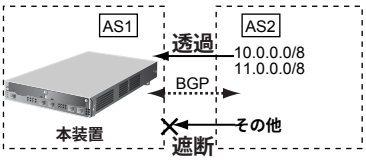
適用機種　全機種

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変更を加えることで、意図的にトラフィックを制御することができます。

参照 Si-R シリーズ　機能説明書「2.4 BGP4 機能」（P.31）

2.5.1　特定の経路情報の受信を透過させる

通信が必要なネットワークに限定して経路を透過させる場合の設定方法を説明します。



● 経路情報の設計

- 10.0.0.0/8 のネットワークの経路情報を透過
- 11.0.0.0/8 のネットワークの経路情報を透過
- その他はすべてを遮断

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。

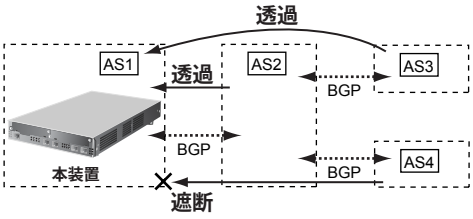
● コマンド

```
フィルタリング条件を設定する
# bgp neighbor 0 filter 0 act pass in
# bgp neighbor 0 filter 0 route 10.0.0.0/8
# bgp neighbor 0 filter 1 act pass in
# bgp neighbor 0 filter 1 route 11.0.0.0/8
# bgp neighbor 0 filter 2 act reject in
# bgp neighbor 0 filter 2 route any

設定終了
# save
# commit
```

2.5.2　特定の AS からの経路情報の受信を遮断する

適用機種　全機種

フルルートを受信するネットワーク（トランジット）に接続されている場合、特定の経路情報を遮断する場合の設定方法を説明します。



● 経路情報の設計

- AS4 からの経路情報を遮断
- その他はすべて透過

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

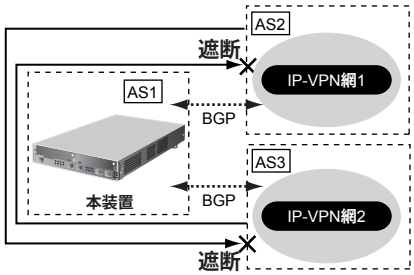
フィルタリング条件を設定する
bgp neighbor 0 filter 0 act reject in
bgp neighbor 0 filter 0 as 4
bgp neighbor 0 filter 1 act pass in
bgp neighbor 0 filter 1 route any

設定終了
save
commit

2.5.3　IP-VPN 網からの受信情報の他 IP-VPN 網への送信を遮断する

適用機種　全機種

異なる IP-VPN 網を使用し、冗長化ネットワークを構成する場合、IP-VPN 網 1 から受信した経路情報の IP-VPN 網 2 への送信を遮断、および IP-VPN 網 2 から受信した経路情報の IP-VPN 網 1 への送信を遮断する場合の設定方法を説明します。



● 経路情報の設計

- AS2 から AS3 への経路情報を遮断
- AS3 から AS2 への経路情報を遮断

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

フィルタリング条件を設定する

IP-VPN 網 1 への送信を遮断する
```
# bgp neighbor 0 filter 0 act reject out
# bgp neighbor 0 filter 0 as 3
# bgp neighbor 0 filter 1 act pass out
# bgp neighbor 0 filter 1 route any
```

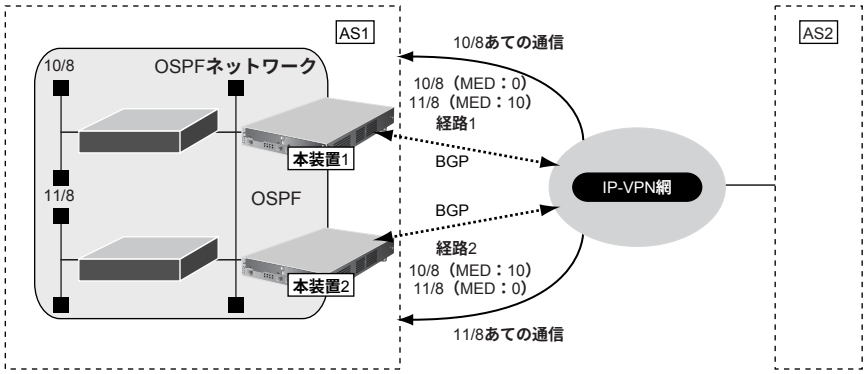
IP-VPN 網 2 への送信を遮断する
```
# bgp neighbor 1 filter 0 act reject out
# bgp neighbor 1 filter 0 as 2
# bgp neighbor 1 filter 1 act pass out
# bgp neighbor 1 filter 1 route any
```

設定終了
```
# save
# commit
```

2.5.4　冗長構成の通信経路を使用する

適用機種　全機種

IP-VPN 網に接続する経路を 2 つ使用した冗長構成で、通信の負荷分散および通信網異常による経路切り替えを行う場合の設定方法を説明します。



● 経路情報の設計

- OSPF ネットワークである AS1 で IP-VPN 網を経由した AS2 への通信経路を冗長化する
- 10/8 への通信は経路 1 を優先経路とし、11/8 への通信経路は経路 2 を優先経路とする。それぞれの経路で異常が発生した場合、異常が発生していない経路に切り替わる。優先順位を設定するときは MED メトリック値を使用する
- AS1 内の OSPF ネットワークでの経路変更は BGP で AS2 に広報する

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

[本装置 1]

```
経路情報に MED メトリック値を付加する
# bgp neighbor 0 filter 0 act pass out
# bgp neighbor 0 filter 0 route 10.0.0.0/8
# bgp neighbor 0 filter 0 set medmetric 0
# bgp neighbor 0 filter 1 act pass out
# bgp neighbor 0 filter 1 route 11.0.0.0/8
# bgp neighbor 0 filter 1 set medmetric 10

その他のすべての経路は透過する
# bgp neighbor 0 filter 2 act pass out
# bgp neighbor 0 filter 2 route any

BGP で OSPF 経路を広報する
# routemanage ip redist bgp ospf on

設定終了
# save
# commit
```

[本装置 2]

```
経路情報に MED メトリック値を付加する
# bgp neighbor 0 filter 0 act pass out
# bgp neighbor 0 filter 0 route 10.0.0.0/8
# bgp neighbor 0 filter 0 set medmetric 10
# bgp neighbor 0 filter 1 act pass out
# bgp neighbor 0 filter 1 route 11.0.0.0/8
# bgp neighbor 0 filter 1 set medmetric 0

その他のすべての経路は透過する
# bgp neighbor 0 filter 2 act pass out
# bgp neighbor 0 filter 2 route any

BGP で OSPF 経路を広報する
# routemanage ip redist bgp ospf on

設定終了
# save
# commit
```

こんな事に気をつけて

- すべてのフィルタリング条件に一致しない経路情報は破棄されます。
- BGP/MPLS VPN 機能では、BGP フィルタリング情報は無効となります。
- 送信時のフィルタを設定した場合、相手装置に広報する MED メトリック値、AS パスプリペンドはフィルタの設定値が使用されます。
- MED メトリック値の設定は、送信時のフィルタでだけ有効となります。受信時のフィルタでは、無効となります。
- AS パスプリペンドの設定は、送信時のフィルタでだけ有効となります。受信時のフィルタでは、無効となります。
- BGP 使用中に commit コマンドを実行した場合、接続中のセッションが一度切断されることがあります。

2.6　事業所間をMPLS接続サービスを利用して接続する

適用機種　全機種

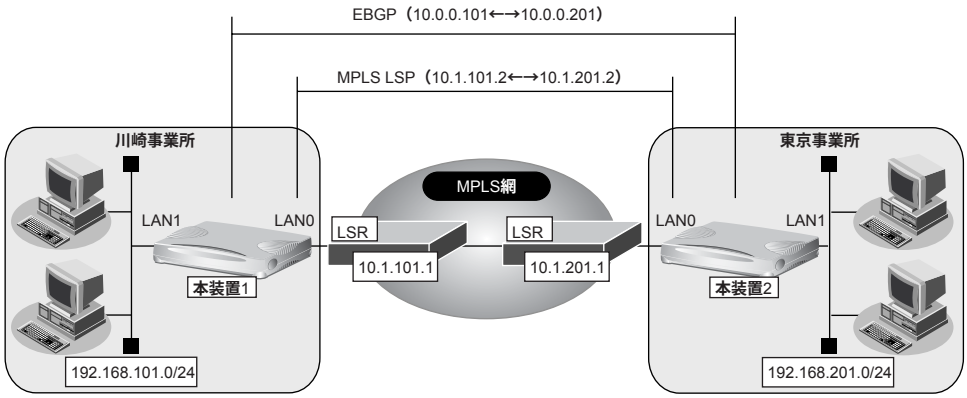
本装置ではMPLSのLSP（label Switching Path：トンネルラベルスイッチングパス）をトンネルとしてインタフェースに対応させるため、シェーピングや帯域制御などの機能をLSPごとに使用することができます（MPLS LSP トンネル）。

ここでは、MPLS接続サービス（キャリアなどから提供されるMPLSをユーザインタフェースとするデータ伝送サービスを想定しています）と本装置のMPLS LSP トンネルを使用して、事業所の間を接続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

- **隣接LSRは、ダイナミックルーティングを用いて最適経路から決定することはできません。**MPLS LSP**の送出先の設定と**MPLS LSP**での次ホップのラベルスイッチルータの設定で静的に指定する必要があります。**
- MPLS LSP**トンネルでは、**IPv4、IPv6**のプロトコルだけをサポートしています。ブリッジは使用できません。**MPLS LSP**トンネル上にさらにラベルをスタックできるのは、**BGP/MPLS VPN**機能だけです。**LDP over LDP**の形態はサポートしていません。**MPLS LSP**トンネルを使用するインタフェースでは、**MPLSを利用しないように設定してください。
- MPLS LSP**トンネルで**IPv6**通信を行う場合は、2層目のラベルスタックに**IPv6 Explicit NULL**ラベルを用いた多重スタックとなります。また、**MPLS TTL**伝達の設定で指定した値に関係なく、**TTLの継承は行われません。
- **複数の**MPLS LSP**トンネルを使用する場合は、それぞれ別の自側トンネルエンドポイントアドレスと相手側トンネルエンドポイントアドレスを設定してください。同じ自側トンネルエンドポイントアドレスが複数設定されている場合は、それぞれのLSPで受信したパケットが期待したLSPのインタフェースとは別のインタフェースで受信されてしまうため、受信インタフェースに依存して動作するIPフィルタリング機能、TOS値書き換え機能、NAT機能、マルチキャスト機能、ダイナミックルーティング（RIP、OSPF）機能などは正しく動作しません。
- **複数の**MPLS LSP**トンネルで相手側トンネルエンドポイントアドレスの設定が同じアドレスであった場合は、**MPLS LSP**の送出先の設定と**MPLS LSP**での次ホップのラベルスイッチルータは同じ値を設定してください。違う値を設定した場合、どれかの値だけが使用されます。**
- MPLS**通信で、優先制御機能、**EXP**値書き換え機能、およびシェーピング機能を利用する場合は、**MPLS LSP**トンネルを使用してください。**

2.6.1 トンネルエンドポイントをインタフェースアドレスにして MPLS LSP を使用する



● 前提条件

[本装置 1]

- LAN0 は MPLS 網、LAN1 は事業所内 LAN とする
- 接続する MPLS 網の次ホップ LSR とは、インタフェースアドレスでコネクションを確立する
- MPLS 網とのラベル交換はインタフェースアドレスに対して行う
- 本装置 1 と本装置 2 の間は、EBGP でループバックインタフェースどうしで経路情報を交換する

[本装置 2]

- LAN0 は MPLS 網、LAN1 は事業所内 LAN とする
- 接続する MPLS 網の次ホップ LSR とは、インタフェースアドレスでコネクションを確立する
- MPLS 網とのラベル交換は、インタフェースアドレスに対して行う
- 本装置 2 と本装置 1 の間は、EBGP でループバックインタフェースどうしで経路情報を交換する

● 設定条件

[本装置 1]

- LAN0（MPLS 網側）の IP アドレス　：10.1.101.2
- 接続する MPLS 網の次ホップ LSR の IP アドレス　：10.1.101.1
- LAN1（事業所内側）の IP アドレス　：192.168.101.1
- ループバックインタフェースの IP アドレス　：10.0.0.101
- 本装置 1 の属する AS 番号　：101
- 本装置 2 の属する AS 番号　：201

[本装置 2]

- LAN0（MPLS 網側）の IP アドレス　：10.1.201.2
- 接続する MPLS 網の次ホップ LSR の IP アドレス　：10.1.201.1
- LAN1（事業所内側）の IP アドレス　：192.168.201.1
- ループバックインタフェースの IP アドレス　：10.0.0.201
- 本装置 2 の属する AS 番号　：201
- 本装置 1 の属する AS 番号　：101

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]

```
MPLS 網との接続情報を設定する
# lan 0 ip address 10.1.101.2/24 3
# lan 0 mpls use on
# mpls ip propagate-ttl off
# mpls ldp router-id 10.1.101.2
# mpls ldp ip transport 10.1.101.2
# routemanage ip redist ldp connected off
# routemanage ip redist ldp rip off
# routemanage ip redist ldp ospf off

MPLS トンネルを設定する
# remote 0 name tokyo
# remote 0 ap 0 name lsp1
# remote 0 ap 0 datalink type mpls
# remote 0 ap 0 mpls to lan 0
# remote 0 ap 0 mpls nexthop 10.1.101.1
# remote 0 ap 0 tunnel local 10.1.101.2
# remote 0 ap 0 tunnel remote 10.1.201.2

ループバックインタフェースを設定する
# loopback ip address 10.0.0.101

LAN1 を設定する
# lan 1 ip address 192.168.101.1/24 3

本装置 2 との間で経路交換をする設定をする
# bgp as 101
# bgp neighbor 0 address 10.0.0.201
# bgp neighbor 0 as 201
# bgp neighbor 0 enforce-multihop on
# bgp neighbor 0 source 10.0.0.101
# bgp network igp on
# bgp network route 0 192.168.101.0/24
# remote 0 ip route 0 10.0.0.201/32

設定終了
# save
# commit
```

[本装置 2]

MPLS 網との接続情報を設定する
lan 0 ip address 10.1.201.2/24 3
lan 0 mpls use on
mpls ip propagate-ttl off
mpls ldp router-id 10.1.201.2
mpls ldp ip transport 10.1.201.2
routemanage ip redist ldp connected off
routemanage ip redist ldp rip off
routemanage ip redist ldp ospf off

MPLS トンネルを設定する
remote 0 name kawasaki
remote 0 ap 0 name lsp1
remote 0 ap 0 datalink type mpls
remote 0 ap 0 mpls to lan 0
remote 0 ap 0 mpls nexthop 10.1.201.1
remote 0 ap 0 tunnel local 10.1.201.2
remote 0 ap 0 tunnel remote 10.1.101.2

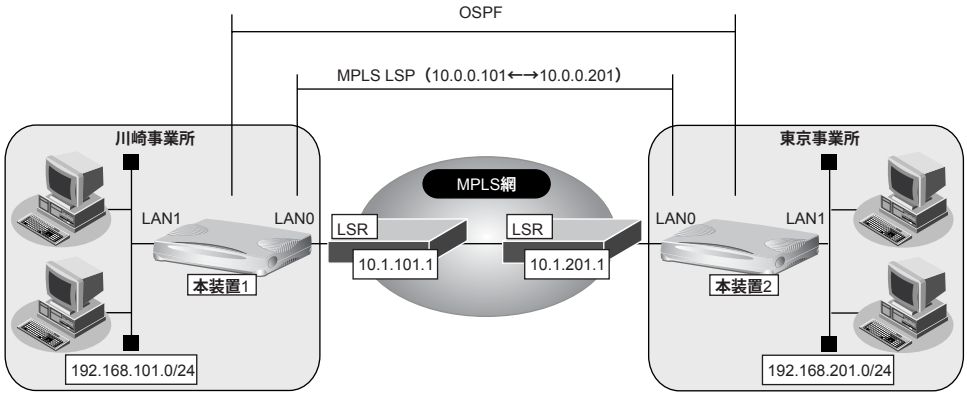
ループバックインタフェースを設定する
loopback ip address 10.0.0.201

LAN1 を設定する
lan 1 ip address 192.168.201.1/24 3

本装置 1 との間で経路交換をする設定をする
bgp as 201
bgp neighbor 0 address 10.0.0.101
bgp neighbor 0 as 101
bgp neighbor 0 enforce-multihop on
bgp neighbor 0 source 10.0.0.201
bgp network igp on
bgp network route 0 192.168.201.0/24
remote 0 ip route 0 10.0.0.101/32

設定終了
save
commit

2.6.2　トンネルエンドポイントをインタフェースアドレスとは別のアドレスにしてMPLS LSPを使用する



● 前提条件

[本装置 1]

- LAN0はMPLS網、LAN1は事業所内LANとする
- 接続するMPLS網の次ホップLSRとは、インタフェースアドレスでコネクションを確立する
- MPLS網とのラベル交換はインタフェースアドレスを使用しないで別のアドレスを使用する
- 本装置1と本装置2の間は、LSP上でOSPFを用いて経路情報を交換する
- MPLS網を使用したLSP上の通信は5Mbpsに帯域を制限する
- LSPでセッション監視を行い、セッションの切断を検知する

[本装置 2]

- LAN0はMPLS網、LAN1は事業所内LANとする
- 接続するMPLS網の次ホップLSRとは、インタフェースアドレスでコネクションを確立する
- MPLS網とのラベル交換はインタフェースアドレスを使用しないで別のアドレスを使用する
- 本装置1と本装置2の間は、LSP上でOSPFを用いて経路情報を交換する
- MPLS網を使用したLSP上の通信は5Mbpsに帯域を制限する
- LSPでセッション監視を行い、セッションの切断を検知する

● 設定条件

[本装置 1]

- LAN0（MPLS網側）のIPアドレス　：10.1.101.2
- 接続するMPLS網の次ホップLSRのIPアドレス　：10.1.101.1
- LAN1（事業所内側）のIPアドレス　：192.168.101.1
- MPLSトンネルの自側IPアドレス　：10.0.0.101
- MPLSトンネルの相手側IPアドレス　：10.0.0.201

[本装置 2]

- LAN0（MPLS網側）のIPアドレス　：10.1.201.2
- 接続するMPLS網の次ホップLSRのIPアドレス　：10.1.201.1
- LAN1（事業所内側）のIPアドレス　：192.168.201.1
- MPLSトンネルの自側IPアドレス　：10.0.0.201
- MPLSトンネルの相手側IPアドレス　：10.0.0.101

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]

```
MPLS 網との接続情報を設定する
# lan 0 ip address 10.1.101.2/24 3
# lan 0 mpls use on
# mpls ip propagate-ttl off
# mpls ldp router-id 10.1.101.2
# mpls ldp ip transport 10.1.101.2
# routemanage ip redist ldp connected off
# routemanage ip redist ldp rip off
# routemanage ip redist ldp ospf off

MPLS トンネルを設定する
# remote 0 name tokyo
# remote 0 ap 0 name lsp1
# remote 0 ap 0 datalink type mpls
# remote 0 ap 0 mpls to lan 0
# remote 0 ap 0 mpls nexthop 10.1.101.1
# remote 0 ap 0 tunnel local 10.0.0.101
# remote 0 ap 0 tunnel remote 10.0.0.201
# remote 0 ip address local 10.0.0.101
# remote 0 ip address remote 10.0.0.201

MPLS トンネルでシェーピングを行う
# remote 0 shaping on 5m

MPLS トンネルでセッション監視を行う
# remote 0 ap 0 sessionwatch address 10.0.0.101 10.0.0.201
# remote 0 ap 0 sessionwatch ttl 1

LAN1 を設定する
# lan 1 ip address 192.168.101.1/24 3

本装置 2 との間で経路交換をする設定をする
# remote 0 ip ospf use on 0
# lan 1 ip ospf use on 0
# lan 1 ip ospf passive on
# ospf ip area 0 id 0.0.0.0

設定終了
# save
# commit
```

[本装置 2]

MPLS 網との接続情報を設定する
lan 0 ip address 10.1.201.2/24 3
lan 0 mpls use on
mpls ip propagate-ttl off
mpls ldp router-id 10.1.201.2
mpls ldp ip transport 10.1.201.2
routemanage ip redist ldp connected off
routemanage ip redist ldp rip off
routemanage ip redist ldp ospf off

MPLS トンネルを設定する
remote 0 name kawasaki
remote 0 ap 0 name lsp1
remote 0 ap 0 datalink type mpls
remote 0 ap 0 mpls to lan 0
remote 0 ap 0 mpls nexthop 10.1.201.1
remote 0 ap 0 tunnel local 10.0.0.201
remote 0 ap 0 tunnel remote 10.0.0.101
remote 0 ip address local 10.0.0.201
remote 0 ip address remote 10.0.0.101

MPLS トンネルでシェーピングを行う
remote 0 shaping on 5m

MPLS トンネルでセッション監視を行う
remote 0 ap 0 sessionwatch address 1.0.0.201 10.0.0.101
remote 0 ap 0 sessionwatch ttl 2

LAN1 を設定する
lan 1 ip address 192.168.201.1/24 3

本装置 1 との間で経路交換をする設定をする
remote 0 ip ospf use on 0
lan 1 ip ospf use on 0
lan 1 ip ospf passive on
ospf ip area 0 id 0.0.0.0

設定終了
save
commit

2.7 MPLS を使用したレイヤ 2VPN（EoMPLS）を構築する

適用機種　全機種

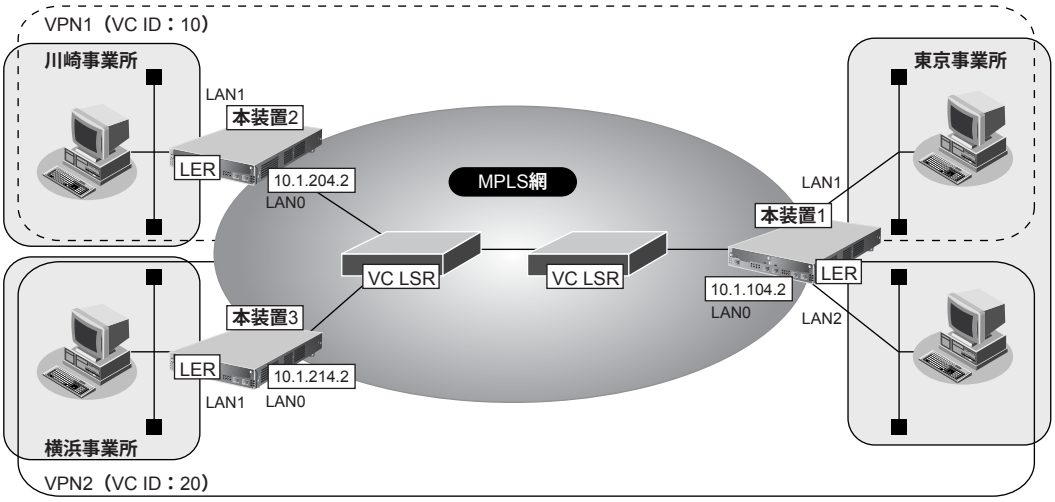
本装置では、MPLS 網を経由することによって、公衆ネットワーク上に仮想的なプライベートネットワーク（閉域網）を構築することができ、遠隔地のネットワークを同じオフィス内のネットワークと同じように利用することができます。また、少ない設備で、業務単位で隔離したネットワークを実現することができます。

参照 Si-R シリーズ　機能説明書「2.7.1 MPLS を使用したレイヤ 2VPN（EoMPLS）」（P.40）

ここでは、MPLS 接続サービス（キャリアなどから提供される MPLS をユーザインタフェースとするデータ伝送サービスを想定しています）と、MPLS LSP トンネルを使用して事業所でレイヤ 2VPN を EoMPLS で構築する事例を紹介します。

こんな事に気をつけて

- **複数のインタフェースを同一の VC に含めることはできません。**
- **トンネル LSP を使用するインタフェースでは、MPLS を利用する設定にしてください。**
- **VC インタフェースでは、シェーピング機能、LAN ポートバックアップ機能および VLAN 機能を併用して動作させることができます。IP 機能、IPv6 機能、ブリッジ機能（MAC フィルタ機能を含む）、VRRP 機能は動作できません。**
- **EoMPLS 通信を行う場合は、MAC 学習や STP のサポートを行わないため、パケットのループが発生しないように構成してください。Ethernet フレームがループし続けて通信できなくなります。また、EoMPLS 通信を用いて冗長構成を行う場合も、LAN インタフェース側に、STP などを使用できるスイッチ装置を設置し、Ethernet フレームがループしないように設定してください。**
- **VLAN Tag が異なる VLAN インタフェースどうしで VC を構成し、LAN 側で STP を使用する場合は、VLAN Tag の値をそろえてください。**



● 前提条件

[本装置 1]

- LAN0 は MPLS 網とし、LAN1、LAN2 は事業所内 LAN とする
- 接続する MPLS 網の次ホップ LSR とは、ループバックアドレスでコネクションを確立する
- MPLS 網とのラベル交換はループバックに対して行う
- 拠点間はスタティックルートで通信を行う

[本装置 2]

- LAN0 は MPLS 網とし、LAN1 は事業所内 LAN とする
- 接続する MPLS 網の次ホップ LSR とは、ループバックアドレスでコネクションを確立する
- MPLS 網とのラベル交換はループバックに対して行う
- 拠点間はスタティックルートで通信を行う

[本装置 3]

- LAN0 は MPLS 網とし、LAN1 は事業所内 LAN とする
- 接続する MPLS 網の次ホップ LSR とは、ループバックアドレスでコネクションを確立する
- MPLS 網とのラベル交換はループバックに対して行う
- 拠点間はスタティックルートで通信を行う

● 設定条件

[本装置 1]

- LAN0（MPLS 網側）の IP アドレス：10.1.104.2
- ループバックの IP アドレス　：10.0.0.104
- LAN1 の VC 番号　：10
- LAN2 の VC 番号　：20

[本装置 2]

- LAN0（MPLS 網側）の IP アドレス：10.1.204.2
- ループバックの IP アドレス　：10.0.0.204
- LAN1 の VC 番号　：10

[本装置 3]

- LAN0（MPLS 網側）の IP アドレス：10.1.214.2
- ループバックの IP アドレス　：10.0.0.214
- LAN1 の VC 番号　：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。

本装置 1 を設定する

● コマンド

```
MPLS 網との接続情報を設定する
# lan 0 ip address 10.1.104.2/24 3
# lan 0 ip route 0 10.0.0.204/32 10.1.104.1 1 0
# lan 0 ip route 1 10.0.0.214/32 10.1.104.1 1 0
# lan 0 mpls use on
# mpls ldp ip transport 10.0.0.104
# mpls ldp router-id 10.0.0.104
# loopback ip address 10.0.0.104
# loopback mpls ldp interface-label on

各拠点への VC を設定する
# lan 1 mpls l2-circuit vc 10 10.0.0.204
# lan 2 mpls l2-circuit vc 20 10.0.0.214

設定終了
# save
# commit
```

本装置 2 を設定する

● コマンド

```
MPLS 網との接続情報を設定する
# lan 0 ip address 10.1.204.2/24 3
# lan 0 ip route 0 10.0.0.104/32 10.1.204.1 1 0
# lan 0 mpls use on
# mpls ldp ip transport 10.0.0.204
# mpls ldp router-id 10.0.0.204
# loopback ip address 10.0.0.204
# loopback mpls ldp interface-label on

各拠点への VC を設定する
# lan 1 mpls l2-circuit vc 10 10.0.0.104

設定終了
# save
# commit
```

本装置 3 を設定する

● コマンド

```
MPLS 網との接続情報を設定する
# lan 0 ip address 10.1.214.2/24 3
# lan 0 ip route 0 10.0.0.104/32 10.1.214.1 1 0
# lan 0 mpls use on
# mpls ldp ip transport 10.0.0.214
# mpls ldp router-id 10.0.0.214
# loopback ip address 10.0.0.214
# loopback mpls ldp interface-label on

各拠点への VC を設定する
# lan 1 mpls l2-circuit vc 20 10.0.0.104

設定終了
# save
# commit
```

⚠注意

MPLS LSP トンネルの REMOTE インタフェースを使用し、EoMPLS 通信の相手装置のアドレスがトンネルエンドポイントと同じである場合は、REMOTE インタフェースの設定で、MPLS を使用する、LDP Multicast Hello パケットを送信しない、と設定してください。

2.8 MPLS を使用したレイヤ 3VPN（BGP/MPLS VPN）を構築する

適用機種　全機種

本装置では、MPLS 網を経由することによって、公衆ネットワーク上に仮想的なプライベートネットワーク（閉域網）を構築することができ、遠隔地のネットワークを同じオフィス内のネットワークと同じように利用することができます。また、少ない設備で、業務単位で隔離したネットワークを実現することができます。

☛ 参照　Si-R シリーズ　機能説明書「2.7.2 MPLS を使用したレイヤ 3VPN（BGP/MPLS VPN）」（P.42）

ここでは、MPLS を使用した VPN ネットワークを構築する場合の設定方法を説明します。

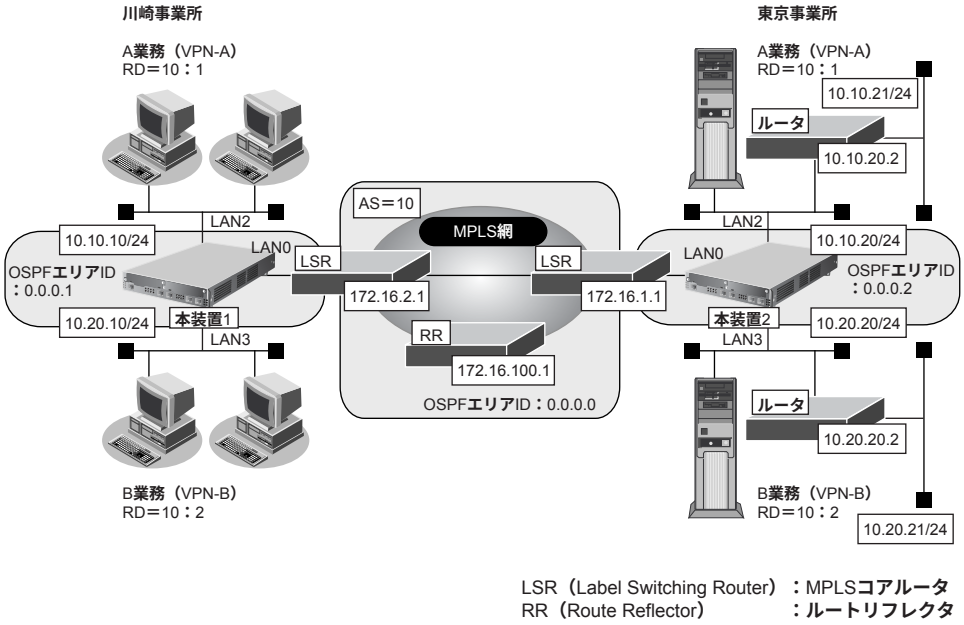
東京事業所と川崎事業所が MPLS 網に接続し、業務ごとに異なる VPN ネットワークを構築します。このとき、本装置 1、2 がそれぞれの前提条件を満たしていることを前提とします。

こんな事に気をつけて

- BGP/MPLS VPN 機能は IPv4 の場合だけ利用できます。IPv6 では使用できません。
- BGP で接続できる相手は 1 セッションだけです。このため、ルートリフレクタと接続する必要があります。
- IP-VPN 接続と併用することはできません。
- BGP ネットワーク、BGP 集約経路および BGP フィルタリングの機能は使用できません。
- BGP/MPLS VPN 機能と NAT 機能を併用することはできません。
- 本装置は、LER としてだけ動作します。
- BGP/MPLS VPN で構成された VPN ネットワーク内では、EBGP、OSPF および RIP は使用できません。
- 異なる VPN を収容する場合、VPN のインタフェースに設定した IP アドレスおよび属するネットワークアドレスを他 VPN インタフェースに設定できません。必ず異なるネットワークアドレスを設定してください。
- MPLS 網と接続するインタフェースで RIP を使用する場合、VPN で使用するインタフェース経路を RIP で広報します。MPLS への広報に対してフィルタリングを行ってください。
- LER では、受信した IP パケットを IP 処理層を通さずにラベルを付加します。IP フィルタリング機能、TOS 値書き換え機能およびソートフラグメント機能は、VPN に設定したインタフェースへの入力に限り動作します。ただし、VPN からの入力を IPsec によって暗号化し、対向ルータに送信する運用や帯域制御（WFQ）機能、イコールコストマルチパスなどの他 IP 機能を使用した運用は行うことはできません。
- VRRP と併用する場合は、トリガとしてインタフェースダウントリガまたはルートダウントリガ（VPN 内経路は対象外）が利用できます。ノードダウントリガは利用できません。
- BGP/MPLS VPN 構成では、LER は MTU 長の設定にかかわらず、IP パケットのフラグメント処理を行いません。受信したパケットはそのままラベルを付加して送信します。このため、MTU 長を調整する必要がある運用（VoIP 通信でのインターリーブなど）はできません。
- ループバックインタフェースで設定した IP アドレスを BGP の自側 IP アドレスとして使用しなければいけません。
- IP アドレスが設定されていないインタフェースでは MPLS は使用できません。隣接 MPLS 装置間で LDP セッションを構築する際、インタフェースのアドレスを用いる場合があります。
- BRI などの低速回線での高負荷時や装置の転送能力を超える高負荷が発生する場合、LDP セッションが切断されることがあります。LDP の Hello ホールドタイマを長め（例：30 秒）に設定してください。
- MPLS を利用すると、Ethernet フレームに 4 バイトのシムヘッダが最大 2 つ付加されます。最大 1526 バイトの Ethernet フレームが送出されることになります。通常の Ethernet フレームの最大サイズは 1518 バイトです。1526 バイトのフレームに対応していない機器と接続する場合は、MPLS を利用するインタフェースの MTU サイズを初期値の 1500 バイトから 1492 バイトに変更することで通信することができます。
- VPN 通信で使用するネットワークアドレスと、本装置に設定するすべてのネットワークアドレスが重複しないように設定してください。たとえば、本装置の MPLS ドメイン側 IP アドレスが 10.1.1.1/24 のとき、10.1.1.0/24 のネットワークを VPN として収容することはできません。
- VPN 以外の SNMP マネージャは VPN 内の装置を管理することはできません。
- BGP セッションの通信に使用するループバックインタフェースに設定したアドレスへの経路は集約しないでください。集約すると、トンネル LSP が正しく生成されません。

2.8.1　MPLS網とLAN を使用して接続する

適用機種　全機種



LSR（Label Switching Router）：MPLSコアルータ
RR（Route Reflector）：ルートリフレクタ

● 前提条件

[本装置 1]

- 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 : 2　　ネットワークアドレス：10.10.10.0/24
  VLAN ID : 3　　ネットワークアドレス：10.20.10.0/24
- LAN1 はVLAN 出力先としてだけ使用し、通常のLAN としては使用しない
- LAN2、LAN3 はVLAN とし、出力先の物理インタフェースはLAN1 とする
- LAN0 のIP アドレス　　：172.16.2.2
- LAN2 のIP アドレス　　：10.10.10.1
- LAN3 のIP アドレス　　：10.20.10.1
- LAN0 ～3 では、NAT 機能およびDHCP クライアント機能は使用しない

[本装置 2]

- 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 : 2　　ネットワークアドレス：10.10.20.0/24
  VLAN ID : 3　　ネットワークアドレス：10.20.20.0/24
- LAN1 はVLAN 出力先としてだけ使用し、通常のLAN としては使用しない
- LAN2、LAN3 はVLAN とし、出力先の物理インタフェースはLAN1 とする
- LAN0 のIP アドレス　　：172.16.1.2
- LAN2 のIP アドレス　　：10.10.20.1
- LAN3 のIP アドレス　　：10.20.20.1
- LAN0 ～3 では、NAT 機能およびDHCP クライアント機能は使用しない

● 設定条件

- MPLS 網の使用条件
  BGP AS 番号　：10
  RR の IP アドレス　：172.16.100.1
  MPLS 網で使用する IPv4 ネットワーク　：OSPF
  　：バックボーンエリア
- VPN-A の使用条件
  ルート識別子　：10:1
  使用するネットワーク　：10.10.10/24 川崎事業所
  　：10.10.20/24 東京事業所
  　：10.10.21/24 東京事業所
- VPN-B の使用条件
  ルート識別子　：10:2
  使用するネットワーク　：10.20.10/24 川崎事業所
  　：10.20.20/24 東京事業所
  　：10.20.21/24 東京事業所

[本装置 1]

- ループバックインタフェースの IP アドレス　：10.1.1.1
- ループバックインタフェースでのルーティングプロトコル　：OSPF
- ループバックインタフェースでの OSPF エリア ID　：0.0.0.1
- LAN0 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
- LAN2 で使用する VPN　：VPN-A
- LAN3 で使用する VPN　：VPN-B

[本装置 2]

- ループバックインタフェースの IP アドレス　：10.2.1.1
- ループバックインタフェースでのルーティングプロトコル　：OSPF
- ループバックインタフェースでの OSPF エリア ID　：0.0.0.2
- LAN0 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
- LAN2 で使用する VPN　：VPN-A
- LAN2 で使用する BGP/MPLS VPN スタティック経路情報
  あて先 IP アドレス　：10.10.21.0/24
  中継ルータアドレス　：10.10.20.2
- LAN3 で使用する VPN　：VPN-B
- LAN3 で使用する BGP/MPLS VPN スタティック経路情報
  あて先 IP アドレス　：10.20.21.0/24
  中継ルータアドレス　：10.20.20.2

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

```
ループバックインタフェースを設定する
# loopback ip address 0 10.1.1.1

MPLS 網との接続情報を設定する
# lan 0 mpls use on
# mpls ldp router-id 10.1.1.1
# mpls ldp ip transport 10.1.1.1
# lan 0 ip ospf use on 0
# ospf ip area 0 id 0.0.0.1
# loopback ip ospf use on 0

RR との接続情報を設定する
# bgp as 10
# bgp id 10.1.1.1
# bgp neighbor 0 address 172.16.100.1
# bgp neighbor 0 as 10
# bgp neighbor 0 family vpnv4
# bgp neighbor 0 source 10.1.1.1

VPN-A 情報として VRF0 情報を設定する
# bgp vrf 0 rd 10 1
# routemanage ip redist bgp vrf 0 connected on

VPN-B 情報として VRF1 情報を設定する
# bgp vrf 1 rd 10 2
# routemanage ip redist bgp vrf 1 connected on

LAN2 に VPN-A（VRF0）を設定する
# lan 2 ip vrf use on 0

LAN3 に VPN-B（VRF1）を設定する
# lan 3 ip vrf use on 1

設定終了
# save
# commit
```

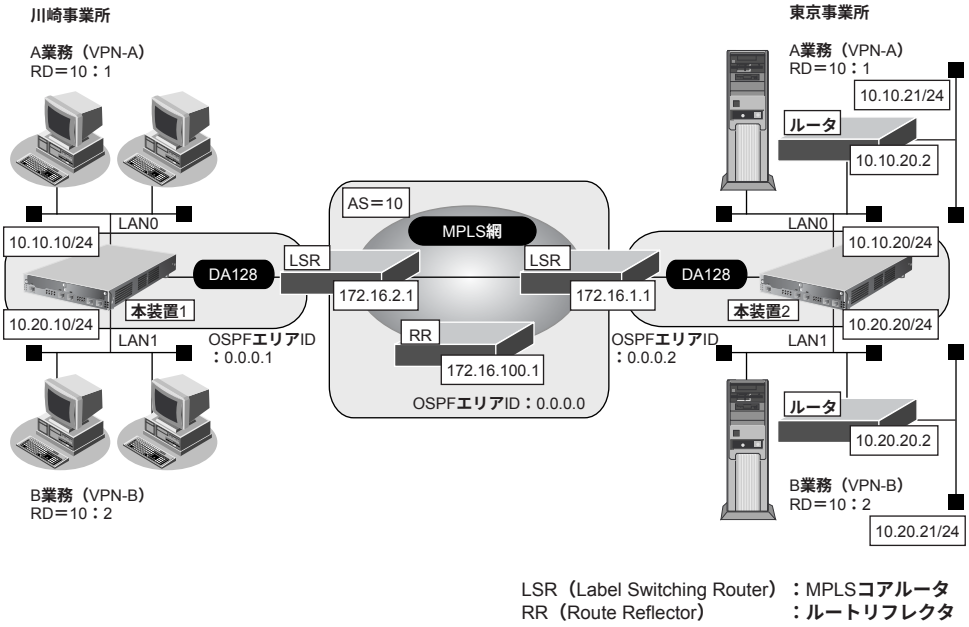
本装置 2 を設定する

● コマンド

```
ループバックインタフェースを設定する
# loopback ip address 0 10.2.1.1

MPLS 網との接続情報を設定する
# lan 0 mpls use on
# mpls ldp router-id 10.2.1.1
# mpls ldp ip transport 10.2.1.1
# lan 0 ip ospf use on 0
# ospf ip area 0 id 0.0.0.2
# loopback ip ospf use on 0

RR との接続情報を設定する
# bgp as 10
# bgp id 10.2.1.1
# bgp neighbor 0 address 172.16.100.1
# bgp neighbor 0 as 10
# bgp neighbor 0 family vpnv4
# bgp neighbor 0 source 10.2.1.1

VPN-A 情報として VRF0 情報を設定する
# bgp vrf 0 rd 10 1
# routemanage ip redist bgp vrf 0 static on
# routemanage ip redist bgp vrf 0 connected on

VPN-B 情報として VRF1 情報を設定する
# bgp vrf 1 rd 10 2
# routemanage ip redist bgp vrf 1 static on
# routemanage ip redist bgp vrf 1 connected on

LAN2 に VPN-A（VRF0）を設定する
# lan 2 ip vrf use on 0
# lan 2 ip vrf route 0 10.10.21.0/24 10.10.20.2

LAN3 に VPN-B（VRF1）を設定する
# lan 3 ip vrf use on 1
# lan 3 ip vrf route 0 10.20.21.0/24 10.20.20.2

設定終了
# save
# commit
```

2.8.2　MPLS網と専用線を使用して接続する

適用機種　***Si-R220B,370,570***



LSR（Label Switching Router）：MPLSコアルータ
RR（Route Reflector）　：ルートリフレクタ

● 前提条件

- すべてのインタフェースにIPアドレスを設定する
- すべてのインタフェースでNAT機能およびDHCPクライアント機能を使用しない

● 設定条件

- MPLS網の使用条件
  BGP AS番号　：10
  RRのIPアドレス　：172.16.100.1
  MPLS網で使用するIPv4ネットワーク　：OSPF
  　：バックボーンエリア
- VPN-Aの使用条件
  ルート識別子　：10:1
  使用するネットワーク　：10.10.10/24 川崎事業所
  　：10.10.20/24 東京事業所
  　：10.10.21/24 東京事業所
- VPN-Bの使用条件
  ルート識別子　：10:2
  使用するネットワーク　：10.20.10/24 川崎事業所
  　：10.20.20/24 東京事業所
  　：10.20.21/24 東京事業所

[本装置 1]

- ループバックインタフェースの IP アドレス　：10.1.1.1
- ループバックインタフェースでのルーティングプロトコル　：OSPF
- ループバックインタフェースでの OSPF エリア ID　：0.0.0.1
- rmt0 でのルーティングプロトコル　：OSPF
- rmt0 での OSPF エリア ID　：0.0.0.1
- LAN0 で使用する VPN　：VPN-A
- LAN1 で使用する VPN　：VPN-B

[本装置 2]

- ループバックインタフェースの IP アドレス　：10.2.1.1
- ループバックインタフェースでのルーティングプロトコル　：OSPF
- ループバックインタフェースでの OSPF エリア ID　：0.0.0.2
- rmt0 でのルーティングプロトコル　：OSPF
- rmt0 での OSPF エリア ID　：0.0.0.2
- LAN0 で使用する VPN　：VPN-A
- LAN0 で使用する BGP/MPLS VPN スタティック経路情報
  あて先 IP アドレス　：10.10.21.0/24
  中継ルータアドレス　：10.10.20.2
- LAN1 で使用する VPN　：VPN-B
- LAN1 で使用する BGP/MPLS VPN スタティック経路情報
  あて先 IP アドレス　：10.20.21.0/24
  中継ルータアドレス　：10.20.20.2

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

```
ループバックインタフェースを設定する
# loopback ip address 0 10.1.1.1

MPLS 網との接続情報を設定する
# remote 0 mpls use on
# mpls ldp router-id 10.1.1.1
# mpls ldp ip transport 10.1.1.1
# remote 0 ip ospf use on 0
# ospf ip area 0 id 0.0.0.1
# loopback ip ospf use on 0

RR との接続情報を設定する
# bgp as 10
# bgp id 10.1.1.1
# bgp neighbor 0 address 172.16.100.1
# bgp neighbor 0 as 10
# bgp neighbor 0 family vpnv4
# bgp neighbor 0 source 10.1.1.1

VPN-A 情報として VRF0 情報を設定する
# bgp vrf 0 rd 10 1
# routemanage ip redist bgp vrf 0 connected on

VPN-B 情報として VRF1 情報を設定する
# bgp vrf 1 rd 10 2
# routemanage ip redist bgp vrf 1 connected on

LAN0 に VPN-A（VRF0）を設定する
# lan 0 ip vrf use on 0
# lan 0 ip address 10.10.10.1/24 3

LAN1 に VPN-B（VRF1）を設定する
# lan 1 ip vrf use on 1
# lan 1 ip address 10.20.10.1/24 3

設定終了
# save
# commit
```

本装置 2 を設定する

● コマンド

```
ループバックインタフェースを設定する
# loopback ip address 0 10.2.1.1

MPLS 網との接続情報を設定する
# remote 0 mpls use on
# mpls ldp router-id 10.2.1.1
# mpls ldp ip transport 10.2.1.1
# remote 0 ip ospf use on 0
# ospf ip area 0 id 0.0.0.2
# loopback ip ospf use on 0

RR との接続情報を設定する
# bgp as 10
# bgp id 10.2.1.1
# bgp neighbor 0 address 172.16.100.1
# bgp neighbor 0 as 10
# bgp neighbor 0 family vpnv4
# bgp neighbor 0 source 10.2.1.1

VPN-A 情報として VRF0 情報を設定する
# bgp vrf 0 rd 10 1
# routemanage ip redist bgp vrf 0 static on
# routemanage ip redist bgp vrf 0 connected on

VPN-B 情報として VRF1 情報を設定する
# bgp vrf 1 rd 10 2
# routemanage ip redist bgp vrf 1 static on
# routemanage ip redist bgp vrf 1 connected on

LAN0 に VPN-A（VRF0）を設定する
# lan 0 ip vrf use on 0
# lan 0 ip address 10.10.20.1/24 3
# lan 0 ip vrf route 0 10.10.21.0/24 10.10.20.2

LAN1 に VPN-B（VRF1）を設定する
# lan 1 ip vrf use on 1
# lan 1 ip address 10.20.20.1/24 3
# lan 1 ip vrf route 0 10.20.21.0/24 10.20.20.2

設定終了
# save
# commit
```

こんな事に気をつけて

サポートインタフェースは PRI（ISDN、HSD）、BRI（ISDN、HSD）、ATM と LAN です。モデムや FR には対応していません。

⚠注意

MPLS、BGP、OSPF および RIP を使用する場合、定期的にパケットを送信します。このため、定額制でない回線を使用している場合は、超過課金の原因となることがあります。このような環境では、BGP/MPLS VPN 機能は使用しないでください。

2.9　マルチリンク機能を使う

適用機種　***Si-R220B,370,570***

ISDN によって相手装置と接続するときに、マルチリンク機能を使用することができます。マルチリンク機能では、B チャネル（64Kbps）を論理的に複数本束ねることによって、最大 1472Kbps で通信できます。また、回線使用率によって動的にチャネル数を増減することができ、回線を効率良く利用することができます。

参照　Si-R シリーズ　機能説明書「2.8 マルチリンク機能」（P.45）

ここでは、ISDN 接続をネットワーク 0（remote 0）で定義してある環境に対してマルチリンクを行う場合の設定方法を説明します。

● 設定条件

- ネットワーク 0（remote 0）で ISDN による通信環境が設定済み
- 接続直後のリンク数は 2 チャンネル
- 最大リンク数は 4 チャネル（2 本の INS ネット 64 回線を利用する）
- チャネルの使用率 90% 以上が 10 秒以上続いたら、チャネルを増加する
- チャネルの使用率 40% 以下が 60 秒以上続いたら、チャネルを減少する
- 受信順序制御機能（MP）を使用する

上記の設定条件に従ってマルチリンクを行う場合のコマンド例を示します。

● コマンド

```
回線の自局番号を設定する
# wan 0 isdn number 0 03-7777-7777
# wan 1 isdn number 1 03-7777-7778

装置のすべての ISDN 回線を利用するように設定する
# remote 0 ap 0 datalink bind any

マルチリンク機能を有効にする
# remote 0 ap 0 ppp mp use on

BAP/BACP 機能を有効にする
# remote 0 ap 0 ppp mp bap use on

接続時に自動的に 2 チャンネル接続するように設定する
# remote 0 ppp mp start 2

最大リンク数を設定する
# remote 0 ppp mp max 4

トラフィックによる自動増減を設定する
# remote 0 ppp mp traffic use on
# remote 0 ppp mp traffic increase 90 10s
# remote 0 ppp mp traffic decrease 40 60s

受信順序制御機能を設定する
# remote 0 ppp mp order on

設定終了
# save
# commit
```

こんな事に気をつけて

- 複数の ISDN 回線を利用してマルチリンク機能を利用する場合は、以下のどちらかが必要です。
  - 着信側回線で代表取り扱いサービスを契約し、同じ番号でどちらの回線でも着信できるようにする。
  - 装置に自局電話番号を正しく設定したうえで、BAP を利用する。
- 初期接続時はすべて同じ電話番号に発信するため、相手側が電話番号の異なる複数の回線で構成される場合は、指定された初期接続回線数まで増やせないことがあります。この場合は着信側回線で代表取り扱いサービスを契約し、同じ番号でどちらの回線でも着信できるようにしてください。

2.10 マルチキャスト機能を使う

適用機種　全機種

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　Si-R シリーズ　機能説明書「2.9 マルチキャスト機能」（P.46）

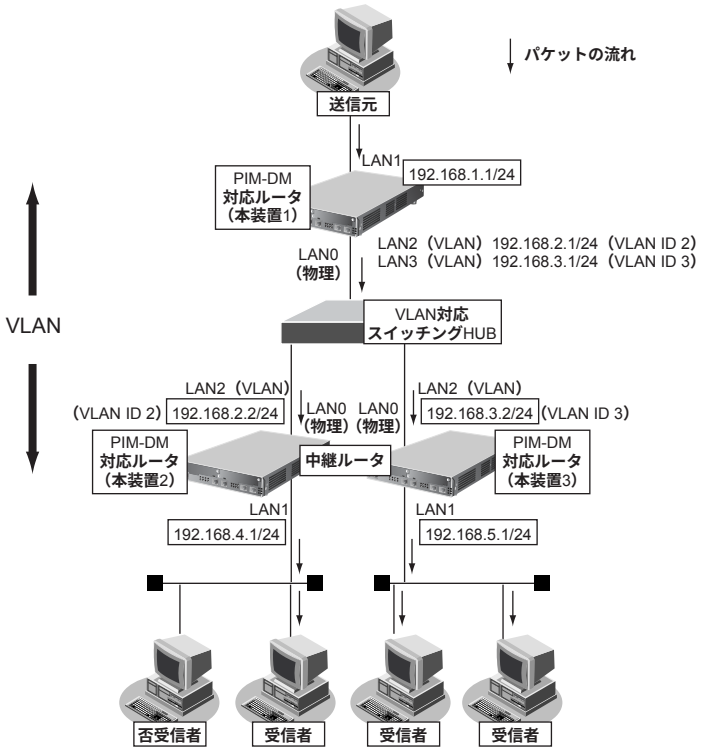
2.10.1 マルチキャスト機能（PIM-DM）を使う

適用機種　全機種

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。**
- **IP アドレスが設定されていないインタフェース上ではマルチキャストを利用することはできません。また、リモートインタフェース上でマルチキャストを動作させる場合は、自側 IP アドレスと相手側 IP アドレスの両方を正しく設定する必要があります。**



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

- 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：2　　ネットワークアドレス：192.168.2.0/24
  VLAN ID：3　　ネットワークアドレス：192.168.3.0/24
- 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 LAN1、LAN2、LAN3 を使用する
- LAN0 は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2、LAN3 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- 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
- LAN1 の IP アドレス　　：192.168.1.1/24
- 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 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 LAN1、LAN2 を使用する
- LAN0 は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- 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
- LAN1 の IP アドレス　　：192.168.4.1/24
- LAN2 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 LAN1、LAN2 を使用する
- LAN0 は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- 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
- LAN1 の IP アドレス　　：192.168.5.1/24
- LAN2 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]

```
LAN0 ポートを削除する
# delete lan 0

LAN 0 ポートを設定する
# lan 0 mode auto

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

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

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

設定終了
# save
# commit
```

[本装置 2]

```
LAN0 ポートを削除する
# delete lan 0

LAN 0 ポートを設定する
# lan 0 mode auto

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

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

設定終了
# save
# commit
```

[本装置 3]

```
LAN0 ポートを削除する
# delete lan 0

LAN 0 ポートを設定する
# lan 0 mode auto

192.168.5.0/24 のネットワークを設定する
# lan 1 ip address 192.168.5.1/24 3
# 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 ip address 192.168.3.2/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimdm
# lan 2 vlan bind 0
# lan 2 vlan tag vid 3

設定終了
# save
# commit
```

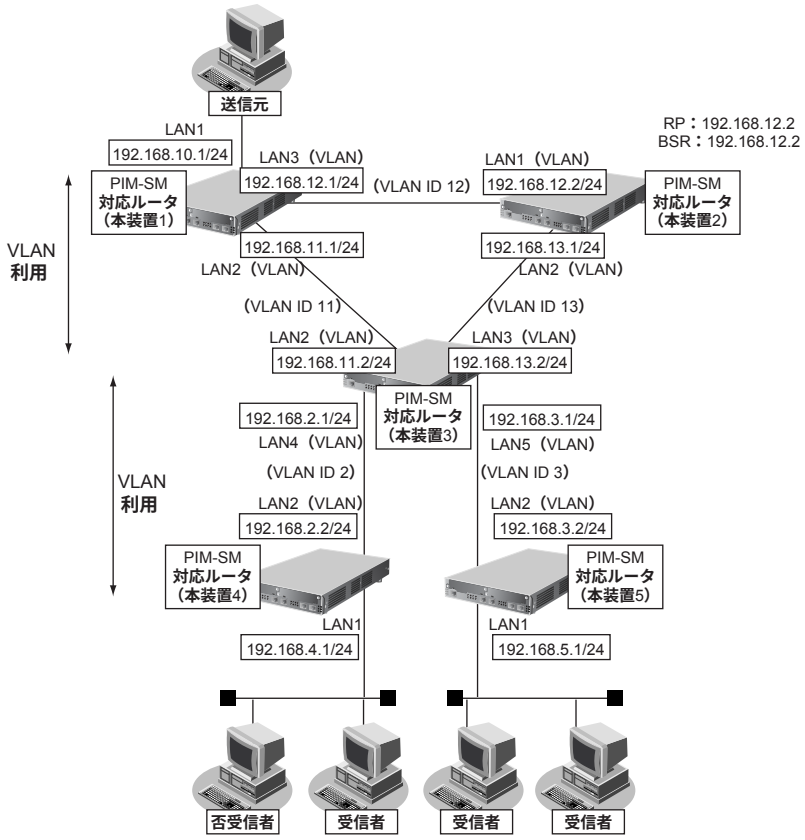
2.10.2 マルチキャスト機能（PIM-SM）を使う

適用機種　全機種

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。**
- **IP アドレスが設定されていないインタフェース上ではマルチキャストを利用することはできません。また、リモートインタフェース上でマルチキャストを動作させる場合は、自側 IP アドレスと相手側 IP アドレスの両方を正しく設定する必要があります。**
- **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。**
- **SPT への切り替えは、マルチキャスト・パケットの受信者の直前のルータ（lasthop router）が行います。**lasthop router **で設定することで** SPT **への切り替えを無効にすることができます。**



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。

この設定例では、VLAN を利用して、上図のネットワークを仮想的に構築します。

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

- 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：2　ネットワークアドレス：192.168.2.0/24
  VLAN ID：3　ネットワークアドレス：192.168.3.0/24
  VLAN ID：11　ネットワークアドレス：192.168.11.0/24
  VLAN ID：12　ネットワークアドレス：192.168.12.0/24
  VLAN ID：13　ネットワークアドレス：192.168.13.0/24
- 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フェースとして LAN1、LAN2、LAN3 を使用する
- LAN0 は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2、LAN3 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- LAN1 の IP アドレス　：192.168.10.1/24
- LAN2 の IP アドレス　：192.168.11.1/24
- LAN3 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フェースとして LAN1、LAN2 を使用する
- LAN0 は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN1、LAN2 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- LAN1 の IP アドレス　：192.168.12.2/24
- LAN2 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フェースとして LAN2、LAN3、LAN4、LAN5 を使用する
- LAN0、LAN1 は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2、LAN3 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- LAN4、LAN5 は VLAN とし、出力先の物理インタフェースは LAN1 とする
- LAN2 の IP アドレス　：192.168.11.2/24
- LAN3 の IP アドレス　：192.168.13.2/24
- LAN4 の IP アドレス　：192.168.2.1/24
- LAN5 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フェースとして LAN1、LAN2 を使用する
- LAN0 は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- LAN1 の IP アドレス　：192.168.4.1/24
- LAN2 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フェースとして LAN1、LAN2 を使用する
- LAN0 は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- LAN1 の IP アドレス　：192.168.5.1/24
- LAN2 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]

```
LAN0 ポートを削除する
# delete lan 0

LAN 0 ポートを設定する
# lan 0 mode auto

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

192.168.11.0/24 のネットワークを設定する
# lan 2 ip address 192.168.11.1/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimsm
# lan 2 vlan bind 0
# lan 2 vlan tag vid 11

192.168.12.0/24 のネットワークを設定する
# lan 3 ip address 192.168.12.1/24 3
# lan 3 ip rip use v2 v2 0 on
# lan 3 ip multicast mode pimsm
# lan 3 vlan bind 0
# lan 3 vlan tag vid 12

設定終了
# save
# commit
```

[本装置 2]

```
LAN0 ポートを削除する
# delete lan 0

LAN 0 ポートを設定する
# lan 0 mode auto

192.168.12.0/24 のネットワークを設定する
# lan 1 ip address 192.168.12.2/24 3
# lan 1 ip rip use v2 v2 0 on
# lan 1 ip multicast mode pimsm
# lan 1 vlan bind 0
# lan 1 vlan tag vid 12

192.168.13.0/24 のネットワークを設定する
# lan 2 ip address 192.168.13.1/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimsm
# lan 2 vlan bind 0
# lan 2 vlan tag vid 13

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]

LAN0 、LAN1 ポートを削除する
delete lan 0

LAN 0、LAN 1 ポートを設定する
lan 0 mode auto
lan 1 mode auto

192.168.11.0/24 のネットワークを設定する
lan 2 ip address 192.168.11.2/24 3
lan 2 ip rip use v2 v2 0 on
lan 2 ip multicast mode pimsm
lan 2 vlan bind 0
lan 2 vlan tag vid 11

192.168.13.0/24 のネットワークを設定する
lan 3 ip address 192.168.13.2/24 3
lan 3 ip rip use v2 v2 0 on
lan 3 ip multicast mode pimsm
lan 3 vlan bind 0
lan 3 vlan tag vid 13

192.168.2.0/24 のネットワークを設定する
lan 4 ip address 192.168.2.1/24 3
lan 4 ip rip use v2 v2 0 on
lan 4 ip multicast mode pimsm
lan 4 vlan bind 1
lan 4 vlan tag vid 2

192.168.2.0/24 のネットワークを設定する
lan 5 ip address 192.168.3.1/24 3
lan 5 ip rip use v2 v2 0 on
lan 5 ip multicast mode pimsm
lan 5 vlan bind 1
lan 5 vlan tag vid 3

設定終了
save
commit

[本装置 4]

```
LAN0 ポートを削除する
# delete lan 0

LAN 0 ポートを設定する
# lan 0 mode auto

192.168.4.0/24 のネットワークを設定する
# lan 1 ip address 192.168.4.1/24 3
# 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 ip address 192.168.2.2/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimsm
# lan 2 vlan bind 0
# lan 2 vlan tag vid 2

設定終了
# save
# commit
```

[本装置 5]

```
LAN0 ポートを削除する
# delete lan 0

LAN 0 ポートを設定する
# lan 0 mode auto

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

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

設定終了
# save
# commit
```

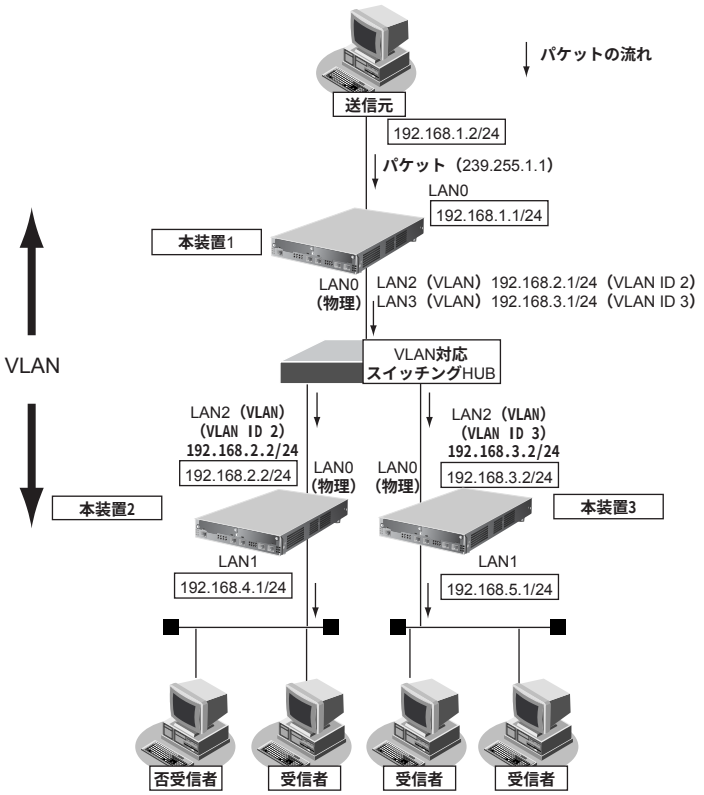
2.10.3 マルチキャスト機能（スタティックルーティング）を使う

適用機種　全機種

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。

こんな事に気をつけて

マルチキャスト・スタティックルーティングでは、入力インタフェースでの IGMP グループ参加を指定することができます。
上流側に PIM-DM などの IGMP 参加要求を受け付けるマルチキャスト・ルータが存在する場合は、入力インタフェースで IGMP グループ参加を行うこと、パケットを強制的に転送させることができます。



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

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 2　：ネットワークアドレス 192.168.2.0/24

VLAN ID 3　：ネットワークアドレス 192.168.3.0/24

- 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
- 入力インタフェースでの IGMP グループ参加は行わない

[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 LAN1、LAN2、LAN3 を使用する
- LAN0 はVLANの出力先としてだけ使用し、通常のLANとしては使用しない
- LAN2、LAN3 はVLANとし、出力先の物理インタフェースは LAN0 とする
- LAN1のIPアドレス　：192.168.1.1/24
- 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 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LAN1、LAN2 を使用する
- LAN0 はVLANの出力先としてだけ使用し、通常のLANとしては使用しない
- LAN2 はVLANとし、出力先の物理インタフェースは LAN0 とする
- LAN1のIPアドレス　：192.168.4.1/24
- LAN2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LAN1、LAN2 を使用する
- LAN0 はVLANの出力先としてだけ使用し、通常のLANとしては使用しない
- LAN2 はVLANとし、出力先の物理インタフェースは LAN0 とする
- LAN1のIPアドレス　：192.168.5.1/24
- LAN2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]

```
LAN0 ポートを削除する
# delete lan 0

LAN0 ポートを設定する
# lan 0 mode auto

192.168.1.0/24 のネットワークの設定をする
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip multicast mode static

192.168.2.0/24 のネットワークの設定をする
# lan 2 ip address 192.168.2.1/24 3
# lan 2 ip multicast mode static
# lan 2 vlan bind 0
# lan 2 vlan tag vid 2

192.168.3.0/24 のネットワークの設定をする
# lan 3 ip address 192.168.3.1/24 3
# lan 3 ip multicast mode static
# lan 3 vlan bind 0
# lan 3 vlan tag vid 3

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 0 192.168.1.2 239.255.1.1 lan1 lan2-lan3 off

設定終了
# save
# commit
```

[本装置 2]

```
LAN0 ポートを削除する
# delete lan 0

LAN0 ポートを設定する
# lan 0 mode auto

192.168.4.0/24 のネットワークの設定をする
# lan 1 ip address 192.168.4.1/24 3
# lan 1 ip multicast mode static

192.168.2.0/24 のネットワークの設定をする
# lan 2 ip address 192.168.2.2/24 3
# lan 2 ip multicast mode static
# lan 2 vlan bind 0
# lan 2 vlan tag vid 2

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 0 192.168.1.2 239.255.1.1 lan2 lan1

設定終了
# save
# commit
```

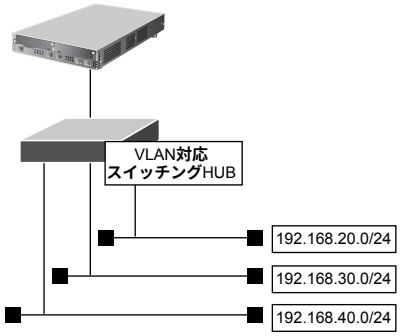
[本装置 3]

```
LAN0 ポートを削除する
# delete lan 0

LAN0 ポートを設定する
# lan 0 mode auto

192.168.5.0/24 のネットワークの設定をする
# lan 1 ip address 192.168.5.1/24 3
# lan 1 ip multicast mode static

192.168.3.0/24 のネットワークの設定をする
# lan 2 ip address 192.168.3.2/24 3
# lan 2 ip multicast mode static
# lan 2 vlan bind 0
# lan 2 vlan tag vid 3

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 0 192.168.1.2 239.255.1.1 lan2 lan1

設定終了
# save
# commit
```

2.11 VLAN 機能を使う

適用機種　全機種

ここでは、VLAN 機能を利用して、1 つの物理ポートで 3 つのネットワークを組む場合を例に説明します。



参照 Si-R シリーズ　機能説明書「2.10 VLAN 機能」（P.49）

● 設定条件

- LAN0 ポートを使用する
- VLAN ID として 2、3、4 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：2　　ネットワークアドレス：192.168.20.0/24
  VLAN ID：3　　ネットワークアドレス：192.168.30.0/24
  VLAN ID：4　　ネットワークアドレス：192.168.40.0/24

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

```
LAN0 ポートを設定する
# delete lan
# lan 0 mode auto

VLAN ID 2 のネットワークを設定する
# lan 1 ip address 192.168.20.1/24 3
# lan 1 ip rip use v1 v1 0 off
# lan 1 vlan bind 0
# lan 1 vlan tag vid 2

VLAN ID 3 のネットワークを設定する
# lan 2 ip address 192.168.30.1/24 3
# lan 2 ip rip use v1 v1 0 off
# lan 2 vlan bind 0
# lan 2 vlan tag vid 3

VLAN ID 4 のネットワークを設定する
# lan 3 ip address 192.168.40.1/24 3
# lan 3 ip rip use v1 v1 0 off
# lan 3 vlan bind 0
# lan 3 vlan tag vid 4

設定終了
# save

再起動
# reset
```

こんな事に気をつけて

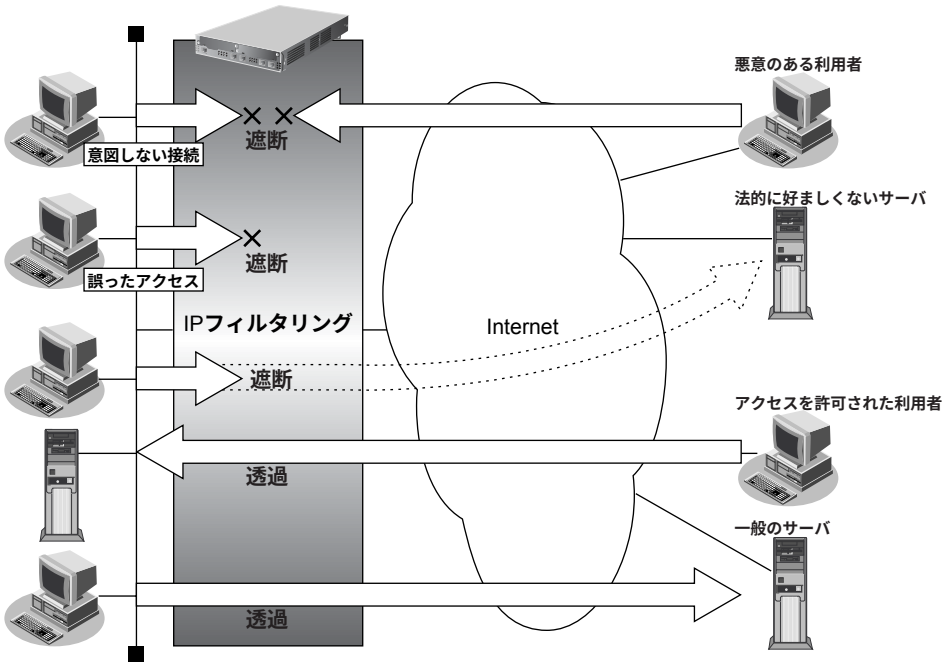
- VLAN 機能を利用すると、Ethernet フレームに 4 バイトの VLAN タグが付加され、最大 1522 バイトの Ethernet フレームが送出されることになります。通常の Ethernet フレームの最大サイズは 1518 バイトです。そのため、その状態では 1522 バイトのフレームに対応していない機器とは接続することはできません。1522 バイトのフレームに対応していない機器と接続する場合は、VLAN インタフェースの MTU サイズを 1496 に変更してください。
- VLAN インタフェース上では、シェーピングおよび帯域制御（WFQ）の機能を利用することはできません。
- VLAN の物理インタフェースに、VLAN インタフェースを使用することはできません。
- 同じ物理インタフェースを使用する複数の VLAN インタフェース上で、重複する VLAN ID を使用することはできません。
- VLAN 対応スイッチング HUB やルータ製品の中には、VLAN が設定されていない LAN ポートで、VLAN タグ付きフレームを受信してしまう装置があります。
  このような装置と接続する際には、スイッチング HUB（またはルータ）の設定を「VLAN あり」から「VLAN なし」に設定を変更してください。
  また、フレームを送信する PC の arp エントリが本装置に残っていると、arp エントリの生存時間中だけ通信するという現象が発生する場合があります。これを防ぐために、設定後に本装置で commit コマンドを実行してください。
- VLAN を利用する物理インタフェースの LAN 情報では、lan mode コマンドで動作モードを必ず設定してください。
  lan mode コマンドで動作モードの設定がなく、その他の LAN 情報で設定する値もすべて初期値とした場合、その LAN 情報は保存されないため、通信ができなくなります。

2.12 IP フィルタリング機能を使う

適用機種　全機種

参照　Si-R シリーズ　機能説明書「2.11 IP フィルタリング機能」（P.50）

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たり、回線への超過課金を防止することができます。



IP フィルタリングの条件

本装置では、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。

- 動作
- 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）
- TCP 接続要求
- TOS 値
- 方向

ヒント

◆ TCP 接続要求とは

TCP プロトコルでのコネクション確立要求を、フィルタリングの対象にするかどうか指定するものです。フィルタリングの動作に透過、プロトコルに TCP を指定した場合に有効です。TCP プロトコルはコネクション型であるため、コネクション確立要求を発行し、それに対する応答を受信することによって、コネクションを開設します。したがって、一方からのコネクションを禁止する場合でも、コネクション確立要求だけを遮断し、その他の応答や通常データなどを透過させるように設定しないと通信できません。

次に、TCP パケットとフラグ設定について説明します。TCP パケット内には SYN フラグと ACK フラグの 2 つの制御フラグがあります。このフラグの組み合わせによって、TCP パケットの内容が分かります。以下に、対応表を示します。

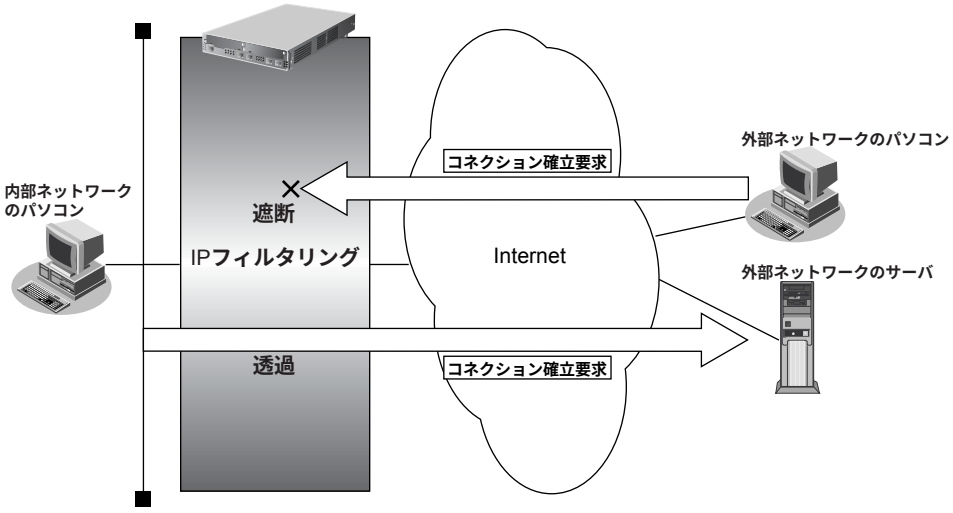
制御フラグ		TCP パケットの内容
SYN	ACK	
1	0	コネクションの確立要求
1	1	確立後の承認応答
0	1	確認応答、通常のデータ

この表から、制御フラグの組み合わせが SYN ＝ 1、ACK ＝ 0 の場合に、TCP パケットがコネクションの確立要求を行うことが分かります。つまり、IP パケットが禁止されている IP アドレスからの送信を禁止すれば、TCP/IP サービスのフィルタリングを行えます。

以下に、telnet（ポート番号 23）を例に説明します。

・外部ネットワークからのコネクション確立要求は遮断

・内部ネットワークからのコネクション確立要求は透過



◆ IP アドレスとアドレスマスクの決め方

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

◆ IP フィルタリングの方向

IP フィルタリングの方向に「リバース（reverse)」を指定すると、入力パケットと出力パケットの両方がフィルタリング対象になります。ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。

- 送信元 IP アドレス／アドレスマスクとあて先 IP アドレス／アドレスマスク
- 送信元ポート番号とあて先ポート番号

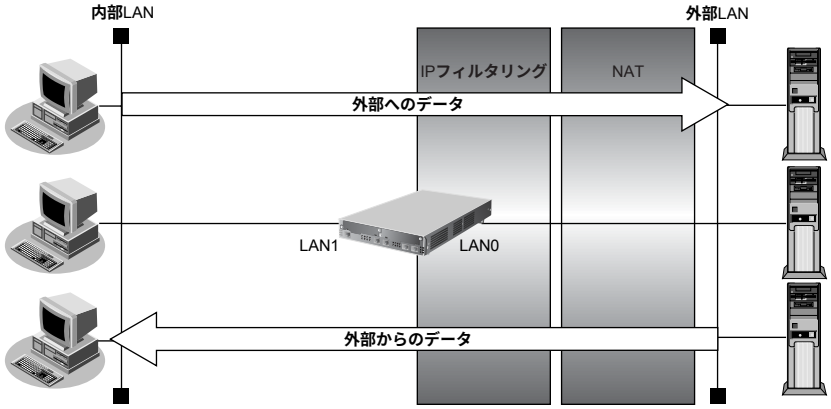
補足 IP フィルタリング機能と NAT 機能を併用する場合、回線切断時に NAT 機能の情報が消えてしまうため、回線切断後に再度接続しても、サーバからの応答が正しくアドレス変換されず、IP フィルタリング機能によってパケットは破棄されてしまいます。

ヒント

◆ アドレス変換（NAT）機能利用時の IP フィルタリングのかかるタイミング

内部 LAN から外部 LAN に向かう場合は、アドレス変換でアドレスが変更される前に IP フィルタリング処理を通過します。また、外部 LAN から内部 LAN に向かう場合は、アドレス変換でアドレスが変更されたあとで、IP フィルタリング処理を通過します。つまり、IP フィルタリングは「プライベートアドレス」を対象に行います。

本装置の IP フィルタリングとアドレス変換の位置付けは以下のとおりです。



IP フィルタリングの設計方針

IP フィルタリングの設計方針には大きく分類して以下の 2 つがあります。

A. 基本的にパケットをすべて遮断し、特定の条件のものだけを透過させる。

B. 基本的にパケットをすべて透過させ、特定の条件のものだけを遮断する。

ここでは、設計方針 A の例として、以下の設定例について説明します。

- 外部の特定サービスへのアクセスだけを許可する
- 外部から特定サーバへのアクセスだけを許可する
- 外部から特定サーバへのアクセスだけ許可して SPI を併用する
- 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）

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
- 利用者が意図しない発信を防ぐ
- 回線が接続しているときだけ許可する

補足 TCP 接続要求の設定は、プロトコルに TCP またはすべてを指定した場合にだけ有効です。それ以外のプロトコルを指定した場合は無効となります。

こんな事に気をつけて

- **IP フィルタリングで WWW（ポート番号 80）でのアクセスを制限する設定を行った場合、外部の WWW ブラウザから設定ができなくなる場合があります。**
- **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。PPPoE の場合は、remote 側にフィルタをかけるようにしてください。**
- **IP フィルタリングの方向に「reverse」を指定すると、入力パケットと出力パケットの両方がフィルタリング対象になります。ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。**
  - **送信元 IP アドレス／アドレスマスクとあて先 IP アドレス／アドレスマスク**
  - **送信元ポート番号とあて先ポート番号**

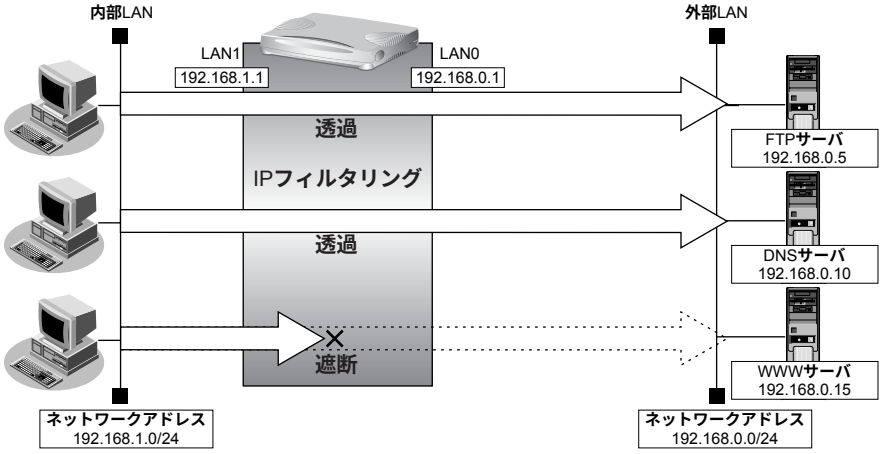
2.12.1　外部の特定サービスへのアクセスだけ許可する

適用機種　全機種

LAN 定義の場合

ここでは、一時的に LAN を作成し、外部 LAN のすべての FTP 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（WWW 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、FTP サーバ名を解決するために、DNS サーバへのアクセスは許可します。

補足
- ftp でホスト名を指定する場合、DNS サーバに問い合わせが発生するため、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、ftp 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 FTP 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。
- 本装置は ftp-data 転送に関するフィルタリングルールを自動的に作成します。



● フィルタリング設計

- 内部 LAN のホスト（192.168.1.0/24）から外部 LAN の FTP 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 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

- FTP 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 FTP サーバのポート 21（ftp）への TCP パケットを透過させる
  (2) (1) の応答パケットを透過させる
- DNS サーバへのアクセスを許可するには

  (1) 192.168.1.0/24 の任意のポートから、DNS サーバのポート 53（domain）への UDP パケットを透過させる
  (2) (1) の応答パケットを透過させる
- ICMP の通信を許可するためには

  (1) ICMP パケットを透過させる
- その他をすべて遮断するには

  (1) すべてのパケットを遮断する

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

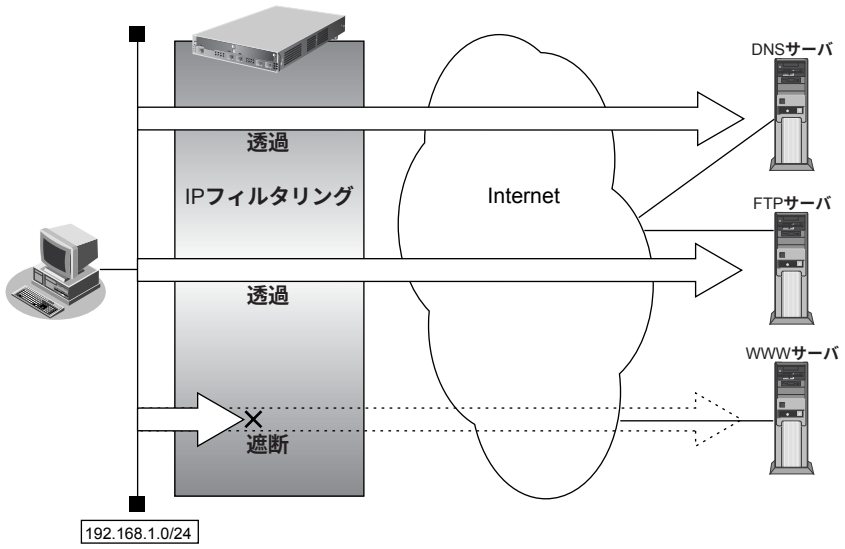
● コマンド

```
任意の FTP サーバのポート 21 への TCP パケットを透過させる
# acl 0 ip 192.168.1.0/24 any 6
# acl 0 tcp any 21 yes
# lan 0 ip filter 0 pass acl 0 any

FTP サーバからの応答パケットを透過させる
# acl 1 ip any 192.168.1.0/24 6
# acl 1 tcp 21 any no
# lan 0 ip filter 1 pass acl 1 any

DNS サーバのポート 53 への UDP パケットを透過させる
# acl 2 ip 192.168.1.0/24 192.168.0.10/32 17
# acl 2 udp any 53
# lan 0 ip filter 2 pass acl 2 any

DNS サーバからの応答パケットを透過させる
# acl 3 ip 192.168.0.10/32 192.168.1.0/24 17
# acl 3 udp 53 any
# lan 0 ip filter 3 pass acl 3 any

ICMP のパケットを透過させる
# acl 4 ip any any 1
# acl 4 icmp any any
# lan 0 ip filter 4 pass acl 4 any

残りのパケットをすべて遮断する
# acl 5 ip any any any
# lan 0 ip filter 5 reject acl 5 any

設定終了
# save
# commit
```

リモート定義の場合

ここでは、LAN 上のパソコンからインターネット上のすべての FTP 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（WWW 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、FTP サーバ名を解決するために、DNS サーバへのアクセスは許可します。

補足
- ftp でホスト名を指定する場合、DNS サーバに問い合わせが発生するため、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、ftp 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 FTP 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。
- 本装置は、ftp-data の転送に関するフィルタリングルールを自動的に作成します。



● フィルタリング設計

- LAN 上のホスト（192.168.1.0/24）から任意の FTP サーバへのアクセスを許可
- LAN 上のホスト（192.168.1.0/24）から WAN の先の 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

- FTP 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 FTP サーバのポート 21（ftp）への TCP パケットを透過させる
  (2)(1) の応答パケットを透過させる
- DNS サーバへのアクセスを許可するには

  (1)192.168.1.0/24 の任意のポートから、DNS サーバのポート 53（domain）への UDP パケットを透過させる
  (2)(1) の応答パケットを透過させる
- ICMP の通信を許可するためには

  (1)ICMP パケットを透過させる
- その他をすべて遮断するには

  (1)すべてのパケットを遮断する

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

● コマンド

```
任意の FTP サーバのポート 21 への TCP パケットを透過させる
# acl 0 ip 192.168.1.0/24 any 6
# acl 0 tcp any 21 yes
# remote 0 ip filter 0 pass acl 0 any

FTP サーバからの応答パケットを透過させる
# acl 1 ip any 192.168.1.0/24 6
# acl 1 tcp 21 any no
# remote 0 ip filter 1 pass acl 1 any

DNS サーバのポート 53 への UDP パケットを透過させる
# acl 2 ip 192.168.1.0/24 any 17
# acl 2 udp any 53
# remote 0 ip filter 2 pass acl 2 any

DNS サーバからの応答パケットを透過させる
# acl 3 ip any 192.168.1.0/24 17
# acl 3 udp 53 any
# remote 0 ip filter 3 pass acl 3 any

ICMP のパケットを透過させる
# acl 4 ip any any 1
# acl 4 icmp any any
# remote 0 ip filter 4 pass acl 4 any

残りのパケットをすべて遮断する
# acl 5 ip any any any
# remote 0 ip filter 5 reject acl 5 any

設定終了
# save
# commit
```

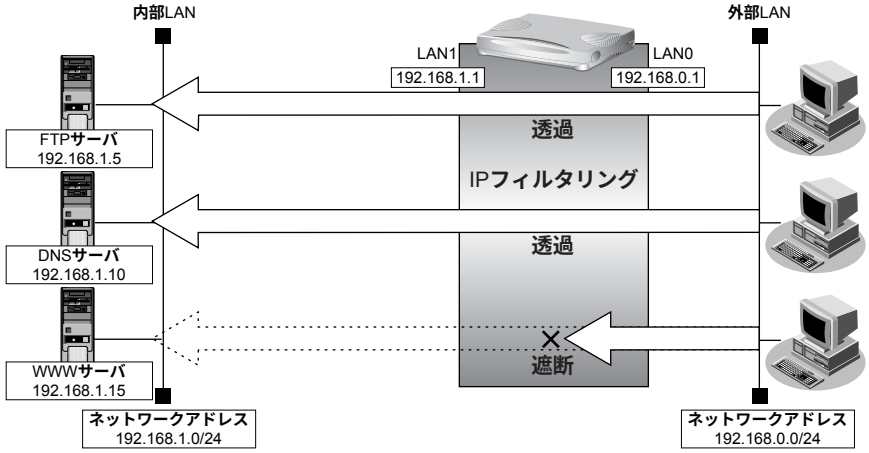
2.12.2　外部から特定サーバへのアクセスだけ許可する

適用機種　全機種

LAN 定義の場合

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、FTP サーバ名を解決するために DNS サーバへのアクセスは許可します。

補足
- ftp でホスト名を指定する場合、DNS サーバに問い合わせが発生するため、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、ftp 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 ftp サーバが決まっている場合は、本装置の DNS サーバ機能を利用することで、DNS サーバへの問い合わせを抑止することができます。
- 本装置は ftp-data 転送に関するフィルタリングルールを自動的に作成します。



● フィルタリング設計

- 内部 LAN のホスト（192.168.1.5/32）を FTP 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 FTP 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 21（ftp）への TCP パケットを透過させる
  （2）（1）の応答パケットを透過させる
- DNS サーバへのアクセスを許可するには
  （1）192.168.0.0/24 の任意のポートから DNS サーバのポート 53（domain）への UDP パケットを透過させる
  （2）（1）の応答パケットを透過させる
- ICMP の通信を許可するためには
  （1）ICMP パケットを透過させる
- その他をすべて遮断するには
  （1）すべてのパケットを遮断する

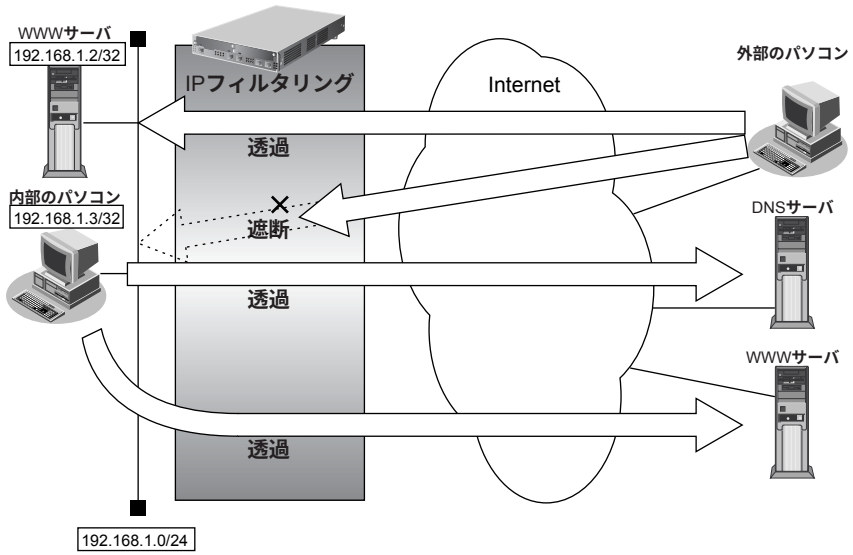
上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

● コマンド

```
LAN 上のホストのポート 21 への TCP パケットを透過させる
# acl 0 ip 192.168.0.0/24 192.168.1.5/32 6
# acl 0 tcp any 21 yes
# lan 0 ip filter 0 pass acl 0 any

LAN 上のホストからの応答パケットを透過させる
# acl 1 ip 192.168.1.5/32 192.168.0.0/24 6
# acl 1 tcp 21 any no
# lan 0 ip filter 1 pass acl 1 any

DNS サーバのポート 53 への UDP パケットを透過させる
# acl 2 ip 192.168.0.0/24 192.168.1.10/32 17
# acl 2 udp any 53
# lan 0 ip filter 2 pass acl 2 any

DNS サーバからの応答パケットを透過させる
# acl 3 ip 192.168.1.10/32 192.168.0.0/24 17
# acl 3 udp 53 any
# lan 0 ip filter 3 pass acl 3 any

ICMP のパケットを透過させる
# acl 4 ip any any 1
# acl 4 icmp any any
# lan 0 ip filter 4 pass acl 4 any

残りのパケットをすべて遮断する
# acl 5 ip any any any
# lan 0 ip filter 5 reject acl 5 any

設定終了
# save
# commit
```

リモート定義の場合

ここでは、LAN 上の WWW サーバに対する外部のパソコンからのアクセスを許可し、LAN 上のほかのパソコンへのアクセスは禁止する場合の設定方法を説明します。また、LAN 上のほかのパソコンはインターネット上の WWW サーバに対してアクセスすると想定されるため、そのアクセスには制限をつけません。



● フィルタリング設計

- LAN 上のホスト（192.168.1.2/32）を WWW サーバとして利用することを許可
- LAN 上のホスト（192.168.1.3/32）から任意の WWW サーバへのアクセスを許可
- LAN 上のホスト（192.168.1.0/24）から WAN の先の 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

- LAN 上のホストの WWW サーバとしての利用を許可するには
  （1）192.168.1.2/32 のポート 80（www-http）へのパケットを透過させる
  （2）（1）の応答パケットを透過させる
- 任意の WWW サーバへのアクセスを許可するには
  （1）192.168.1.3/32 の任意のポートから任意の WWW サーバのポート 80（www-http）へのパケットを透過させる
  （2）（1）の応答パケットを透過させる
- DNS サーバへのアクセスを許可するには
  （1）192.168.1.0/24 の任意のポートから DNS サーバのポート 53（domain）への UDP パケットを透過させる
  （2）（1）の応答パケットを透過させる
- ICMP の通信を許可するためには
  （1）ICMP パケットを透過させる
- その他をすべて遮断するには
  （1）すべてのパケットを遮断する

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

● コマンド

```
LAN 上のホストのポート 80 へのパケットを透過させる
# acl 0 ip any 192.168.1.2/32 6
# acl 0 tcp any 80 yes
# remote 0 ip filter 0 pass acl 0 any

LAN 上のホストからの応答パケットを透過させる
# acl 1 ip 192.168.1.2/32 any 6
# acl 1 tcp 80 any no
# remote 0 ip filter 1 pass acl 1 any

任意の WWW サーバのポート 80 へのパケットを透過させる
# acl 2 ip 192.168.1.3/32 any 6
# acl 2 tcp any 80 yes
# remote 0 ip filter 2 pass acl 2 any

任意の WWW サーバからの応答パケットを透過させる
# acl 3 ip any 192.168.1.3/32 6
# acl 3 tcp 80 any no
# remote 0 ip filter 3 pass acl 3 any

DNS サーバのポート 53 への UDP パケットを透過させる
# acl 4 ip 192.168.1.0/24 any 17
# acl 4 udp any 53
# remote 0 ip filter 4 pass acl 4 any

DNS サーバからの応答パケットを透過させる
# acl 5 ip any 192.168.1.0/24 17
# acl 5 udp 53 any
# remote 0 ip filter 5 pass acl 5 any

ICMP のパケットを透過させる
# acl 6 ip any any 1
# acl 6 icmp any any
# remote 0 ip filter 6 pass acl 6 any

残りのパケットをすべて遮断する
# acl 7 ip any any any
# remote 0 ip filter 7 reject acl 7 any

設定終了
# save
# commit
```

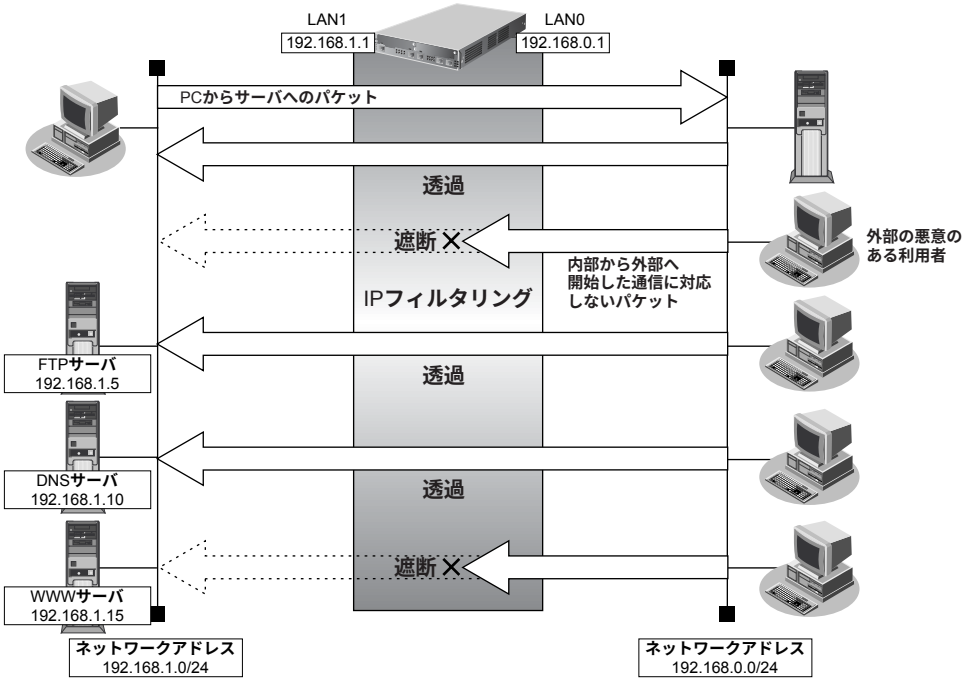
2.12.3 外部から特定サーバへのアクセスだけ許可して SPI を併用する

適用機種　全機種

LAN 定義の場合

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し、SPI を利用して外部へアクセスする場合の設定方法を説明します。ただし、FTP サーバ名を解決するために DNS サーバへのアクセスは許可します。

補足
- ftp でホスト名を指定する場合、DNS サーバに問い合わせが発生するため、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、ftp 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 ftp サーバが決まっている場合は、本装置の DNS サーバ機能を利用することで、DNS サーバへの問い合わせを抑止することができます。
- 本装置は ftp-data 転送に関するフィルタリングルールを自動的に作成します。



● フィルタリング設計

- 内部 LAN のホスト（192.168.1.5/32）を FTP 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
- 内部 LAN から外部へ開始するアクセスを許可し、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 FTP 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 21（ftp）への TCP パケットを透過させる
  （2）（1）の応答パケットを透過させる
- DNS サーバへのアクセスを許可するには
  （1）192.168.0.0/24 の任意ポートから DNS サーバのポート 53（domain）への UDP パケットを透過させる
  （2）（1）の応答パケットを透過させる
- ICMP の通信を許可するためには
  （1）ICMP パケットを透過させる
- 内部 LAN から外部へ開始するアクセスは許可し、その他をすべて遮断するには
  （1）残りのパケットに SPI を利用して IP フィルタリングを行う

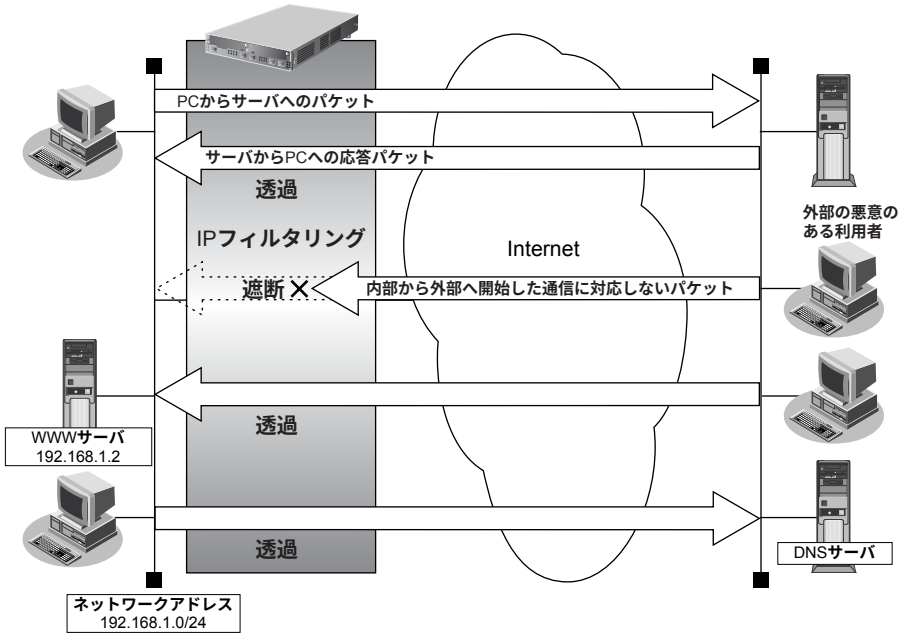
上記のフィルタリングルールに従って設定する場合のコマンド例を示します。

● コマンド

```
LAN 上のホストのポート 21 への TCP パケットを透過させる
# acl 0 ip 192.168.0.0/24 192.168.1.5/32 6
# acl 0 tcp any 21 yes
# lan 0 ip filter 0 pass acl 0 any

LAN 上のホストからの応答パケットを透過させる
# acl 1 ip 192.168.1.5/32 192.168.0.0/24 6
# acl 1 tcp 21 any no
# lan 0 ip filter 1 pass acl 1 any

DNS サーバのポート 53 への UDP パケットを透過させる
# acl 2 ip 192.168.0.0/24 192.168.1.10/32 17
# acl 2 udp any 53
# lan 0 ip filter 2 pass acl 2 any

DNS サーバからの応答パケットを透過させる
# acl 3 ip 192.168.1.10/32 192.168.0.0/24 17
# acl 3 udp 53 any
# lan 0 ip filter 3 pass acl 3 any

ICMP のパケットを透過させる
# acl 4 ip any any 1
# acl 4 icmp any any
# lan 0 ip filter 4 pass acl 4 any

残りのパケットに SPI を利用して IP フィルタリングを行う
# lan 0 ip filter default spi

設定終了
# save
# commit
```

リモート定義の場合

ここでは、外部からLAN上のWWWサーバに対するアクセスを許可し、ほかのLAN上のパソコンへのアクセスを禁止する場合の設定方法を説明します。また、LAN上のほかのパソコンはインターネット上のサーバに対してアクセスしますが、これらのアクセスに対してはSPIによるIPフィルタリングの対象とします。



● フィルタリング設計

- LAN上のホスト（192.168.1.2/32）をWWWサーバとして利用を許可
- ICMPの通信を許可
- 内部LANから外部へ開始するアクセスは許可し、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WWWサーバとしての利用を許可するには
  （1）192.168.1.2/32のポート80（www-http）へのTCPパケットを透過させる
  （2）（1）の応答パケットを透過させる
- ICMPの通信を許可するためには
  （1）ICMPパケットを透過させる
- 内部LANから外部へ開始するアクセスは許可し、その他をすべて遮断するには
  （1）残りのパケットにSPIを利用してIPフィルタリングを行う

上記のフィルタリングルール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

```
LAN 上のホストのポート 80 へのパケットを透過させる
# acl 0 ip any 192.168.1.2/32 6
# acl 0 tcp any 80 yes
# remote 0 ip filter 0 pass acl 0 any

LAN 上のホストからの応答パケットを透過させる
# acl 1 ip 192.168.1.2/32 any 6
# acl 1 tcp 80 any no
# remote 0 ip filter 1 pass acl 1 any

ICMP のパケットを透過させる
# acl 2 ip any any 1
# acl 2 icmp any any
# remote 0 ip filter 2 pass acl 2 any

残りのパケットに SPI を利用して IP フィルタリングを行う
# remote 0 ip filter default spi

設定終了
# save
# commit
```

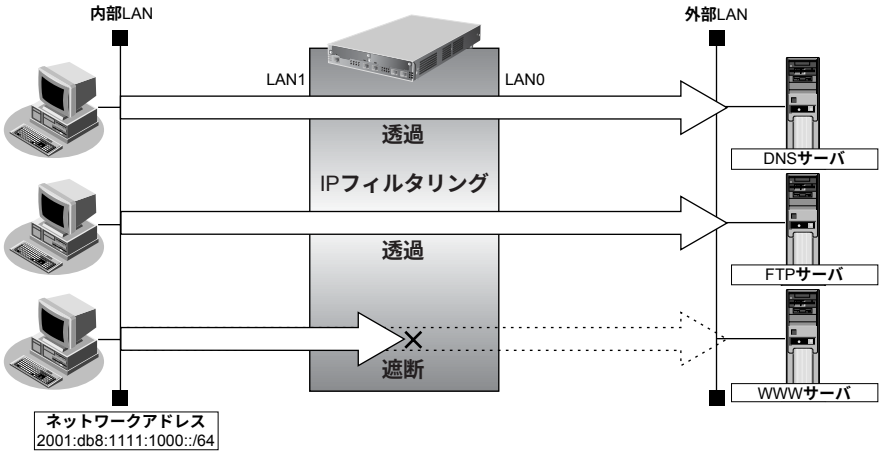
2.12.4 外部の特定サービスへのアクセスだけ許可する（IPv6 フィルタリング）

適用機種　全機種

LAN 定義の場合

ここでは、IPv6 フィルタリングを使って、内部 LAN 上のパソコンから外部 LAN 上のすべての FTP 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（WWW 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、FTP サーバ名を解決するために DNS サーバへのアクセスを許可する設定にします。

補足
- ftp でホスト名を指定する場合、DNS サーバに問い合わせが発生するため、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、ftp サービス以外でもドメイン名で指定されると DNS サーバへの通信が発生します。
- 本装置は ftp-data 転送に関するフィルタリングルールを自動的に作成します。



● フィルタリング設計

- 内部 LAN 上のホスト（2001:db8:1111:1000::/64）から任意の FTP サーバへのアクセスを許可
- 内部 LAN 上のホスト（2001:db8:1111:1000::/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

- FTP サーバへのアクセスを許可するには

  （1）2001:db8:1111:1000::/64 の任意のポートから、任意のアドレスのポート 21（ftp）への TCP パケットを透過させる

  （2）（1）の応答パケットを透過させる
- DNS サーバへのアクセスを許可するには

  （1）2001:db8:1111:1000::/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

  （2）（1）の応答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。

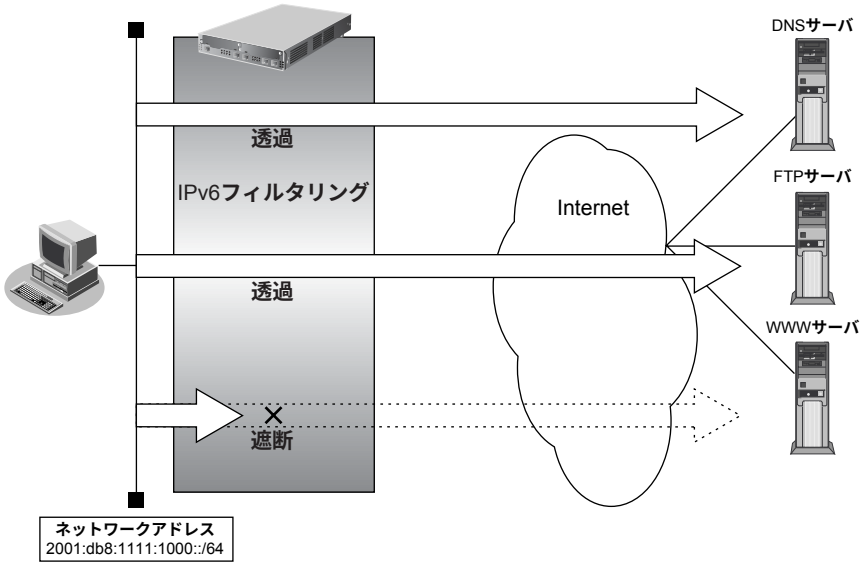
● コマンド

```
任意の FTP サーバのポート 21 への TCP パケットを透過させる
# acl 0 ip6 2001:db8:1111:1000::/64 any 6
# acl 0 tcp any 21 yes
# lan 0 ip6 filter 0 pass acl 0 any

FTP サーバからの応答パケットを透過させる
# acl 1 ip6 any 2001:db8:1111:1000::/64 6
# acl 1 tcp 21 any no
# lan 0 ip6 filter 1 pass acl 1 any

DNS サーバのポート 53 への UDP パケットを透過させる
# acl 2 ip6 2001:db8:1111:1000::/64 any 17
# acl 2 udp any 53
# lan 0 ip6 filter 2 pass acl 2 any

DNS サーバからの応答パケットを透過させる
# acl 3 ip6 any 2001:db8:1111:1000::/64 17
# acl 3 udp 53 any
# lan 0 ip6 filter 3 pass acl 3 any

ICMPv6 のパケットを透過させる
# acl 4 ip6 any any 58
# acl 4 icmp any any
# lan 0 ip6 filter 4 pass acl 4 any

残りのパケットをすべて遮断する
# acl 5 ip6 any any any
# lan 0 ip6 filter 5 reject acl 5 any

設定終了
# save
# commit
```

リモート定義の場合

ここでは、IPv6 フィルタリングを使って、LAN 上のパソコンからイントラネット上のすべての FTP 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（WWW 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、FTP サーバ名を解決するために DNS サーバへのアクセスを許可する設定にします。

補足
- ftp でホスト名を指定する場合、DNS サーバに問い合わせが発生するため、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、ftp サービス以外でドメイン名を指定する場合も DNS サーバへの発信が発生します。
- 本装置は ftp-data 転送に関するフィルタリングルールを自動的に作成します。



● フィルタリング設計

- LAN 上のホスト（2001:db8:1111:1000::/64）から任意の FTP サーバへのアクセスを許可
- LAN 上のホスト（2001:db8:1111:1000::/64）から WAN の先の 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

- FTP サーバへのアクセスを許可するには
  （1）2001:db8:1111:1000::/64 の任意のポートから、任意の FTP サーバのポート 21（ftp）への TCP パケットを透過させる
  （2）（1）の応答パケットを透過させる
- DNS サーバへのアクセスを許可するには
  （1）2001:db8:1111:1000::/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
  （2）（1）の応答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

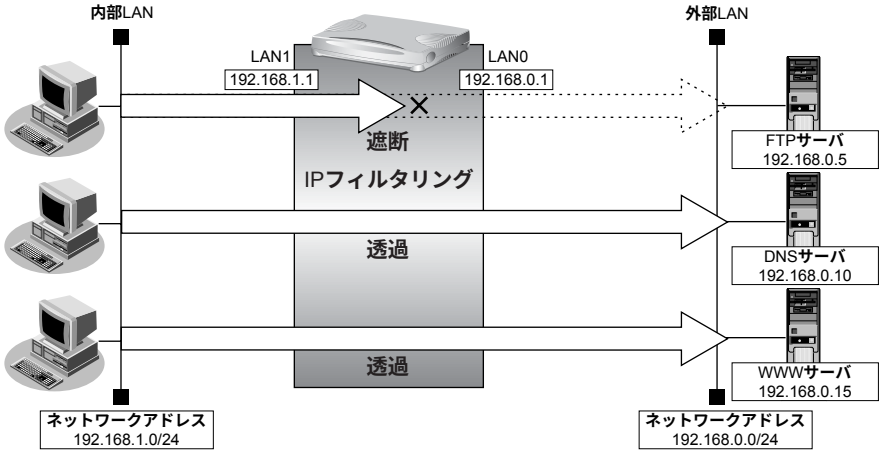
```
任意の FTP サーバのポート 21 への TCP パケットを透過させる
# acl 0 ip6 2001:db8:1111:1000::/64 any 6
# acl 0 tcp any 21 yes
# remote 0 ip6 filter 0 pass acl 0 any

FTP サーバからの応答パケットを透過させる
# acl 1 ip6 any 2001:db8:1111:1000::/64 6
# acl 1 tcp 21 any no
# remote 0 ip6 filter 1 pass acl 1 any

DNS サーバのポート 53 への UDP パケットを透過させる
# acl 2 ip6 2001:db8:1111:1000::/64 any 17
# acl 2 udp any 53
# remote 0 ip6 filter 2 pass acl 2 any

DNS サーバからの応答パケットを透過させる
# acl 3 ip6 any 2001:db8:1111:1000::/64 17
# acl 3 udp 53 any
# remote 0 ip6 filter 3 pass acl 3 any

ICMPv6 のパケットを透過させる
# acl 4 ip6 any any 58
# acl 4 icmp any any
# remote 0 ip6 filter 4 pass acl 4 any

残りのパケットをすべて遮断する
# acl 5 ip6 any any any
# remote 0 ip6 filter 5 reject acl 5 any

設定終了
# save
# commit
```

2.12.5　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

LAN 定義の場合

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



● フィルタリング設定

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

● フィルタリングルール

- FTP サーバへのアクセスを禁止するには

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

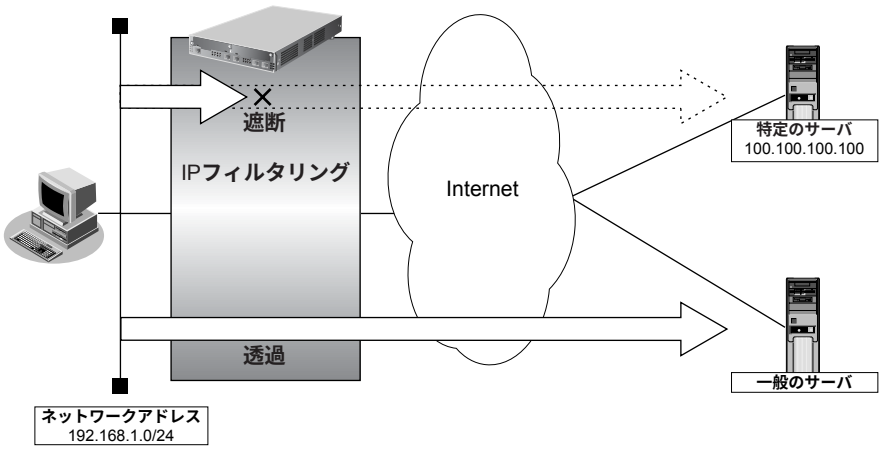
上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

● コマンド

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

設定終了
# save
# commit
```

リモート定義の場合

ここでは、インターネット上の特定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。



● フィルタリング設計

- LAN 上のホスト（192.168.1.0/24）からアドレス 100.100.100.100 へのアクセスを禁止

● フィルタリングルール

- 特定アドレスへのアクセスを禁止するには
  （1）192.168.1.0/24 から 100.100.100.100 の任意のポートへの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

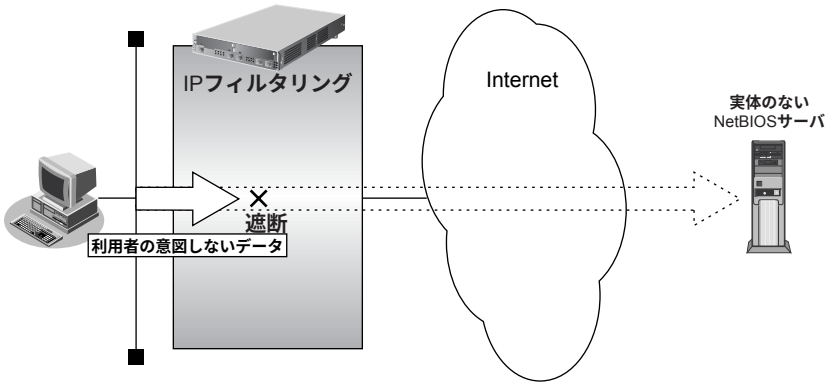
```
アドレス 100.100.100.100 へのすべてのパケットを遮断する
# acl 0 ip 192.168.1.0/24 100.100.100.100/32 any
# remote 0 ip filter 0 reject acl 0 any

設定終了
# save
# commit
```

2.12.6　利用者が意図しない発信を防ぐ

適用機種　全機種

LAN 上のパソコンは、利用者の意志とは無関係に、実体のない NetBIOS サーバにアクセスすることがあります。その際、回線が接続され、利用者が意識しないところで通信料金がかかってしまいます。

ここでは、上記のような、回線に対するむだな発信を抑止する場合のフィルタリング設定方法を説明します。



● フィルタリング設計

- ポート 137 ～ 139（NetBIOS サービス）へのアクセスを禁止

● フィルタリングルール

- ポート 137 ～ 139 へのアクセスを禁止するには

  (1) ポート 137 ～ 139 へのすべてのパケットを遮断する

  (2) ポート 137 ～ 139 からのすべてのパケットを遮断する

補足　Windows® (TCP 上の NetBIOS) 環境のネットワークでは、セキュリティ上の問題とむだな課金を抑えるために、ポート番号 137 ～ 139 の外向きの転送経路をふさいでおく必要があります。

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

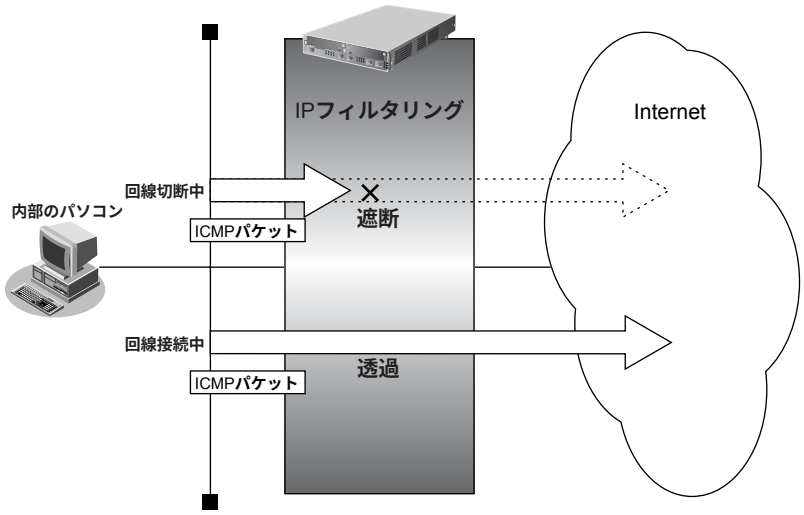
```
ポート137～139へのすべてのTCPパケットを遮断する
# acl 0 ip any any 6
# acl 0 tcp any 137-139 yes
# remote 0 ip filter 0 reject acl 0 any

ポート137～139からのすべてのTCPパケットを遮断する
# acl 1 ip any any 6
# acl 1 tcp 137-139 any yes
# remote 0 ip filter 1 reject acl 1 any

ポート137～139へのすべてのUDPパケットを遮断する
# acl 2 ip any any 17
# acl 2 udp any 137-139
# remote 0 ip filter 2 reject acl 2 any

ポート137～139からのすべてのUDPパケットを遮断する
# acl 3 ip any any 17
# acl 3 udp 137-139 any
# remote 0 ip filter 3 reject acl 3 any

設定終了
# save
# commit
```

2.12.7　回線が接続しているときだけ許可する

適用機種　全機種

一部のパソコンでは、ネットワークの設定によって、ログイン時に自動的にPINGを発行してPPPoEまたはISDN回線を接続してしまうものがあります。回線接続を必要とするICMPパケットを遮断することによって、意図しないPINGによるむだな発信を抑止することができます。ここでは、回線が接続されているときにだけICMPパケットを透過させる場合の設定方法を説明します。

補足　IPアドレスを直接指定せず、DNSによる名前アドレス変換を利用した場合、発信を抑止することはできません。



● フィルタリング設計

- すでに回線が接続している場合にだけPINGを許可

● フィルタリングルール

- すでに回線が接続している場合にだけPINGを許可するには
  (1)回線接続中だけICMP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

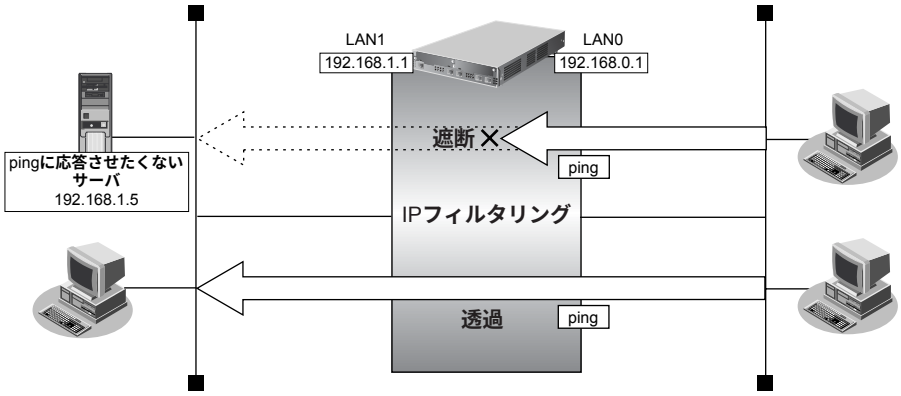
```
回線が接続しているときだけICMPパケットを透過させる
# acl 0 ip any any 1
# acl 0 icmp any any
# remote 0 ip filter 0 restrict acl 0 any

設定終了
# save
# commit
```

2.12.8　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

LAN 定義の場合

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



● フィルタリング設定

- 内部 LAN のサーバ（192.168.1.5/32）に対して外部からの ping（ICMP ECHO）を禁止
- その他はすべて通過

● フィルタリングルール

- 内部 LAN のサーバ（192.168.1.5/32）に対して外部からの ping（ICMP ECHO）を禁止するには
  (1) 192.168.1.5/32 への ICMP TYPE 8 の ICMP パケットを遮断する
- その他のパケットを許可する
  (1) すべてのパケットを透過させる

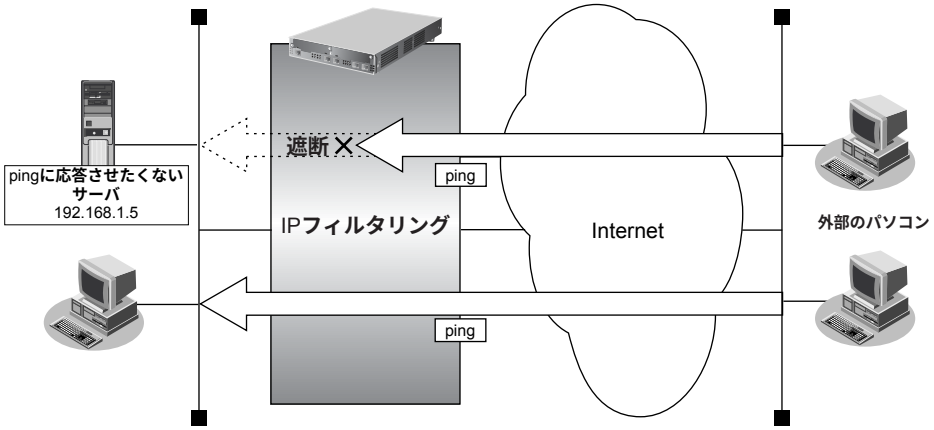
上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

● コマンド

```
アドレス 192.168.1.5/32 への ICMP TYPE 8 の ICMP パケットを遮断する
# acl 0 ip any 192.168.1.5/32 1
# acl 0 icmp 8 any
# lan 0 ip filter 0 reject acl 0 any

残りのパケットをすべて透過させる
# acl 1 ip any any any
# lan 0 ip filter 1 pass acl 1 any

設定終了
# save
# commit
```

リモート定義の場合

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



● フィルタリング設計

- LAN 上のサーバ（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

- LAN 上のサーバ（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 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
acl 0 icmp 8 any
remote 0 ip filter 0 reject acl 0 any

残りのパケットをすべて透過させる
acl 1 ip any any any
remote 0 ip filter 1 pass acl 1 any

設定終了
save
commit

2.13 IPsec機能を使う

適用機種　全機種

VPN（Virtual Private Network）は、インターネットを利用して遠隔地のLANをつなぐと、遠隔地のLAN上のアプリケーションやデータが、あたかも同じオフィスのLANのように利用できる機能です。また、認証情報や暗号情報を設定することにより、インターネット上を流れるデータのセキュリティを確保することができます。

本装置では、VPNを実現するためにIPsecというプロトコルを使用して、以下の接続形態が利用できます。

- 固定IPアドレスでのVPN（手動鍵交換）
  固定IPアドレスで送信元、送信先のIPアドレス範囲を指定してVPN通信を行います。
  認証情報、暗号情報の鍵は手動で設定します。
- 固定IPアドレスでのVPN（自動鍵交換）
  固定IPアドレスで送信元、送信先のIPアドレス範囲を指定してVPN通信を行います。
  認証情報、暗号情報の鍵は自動で交換します。
- 可変IPアドレスでのVPN（自動鍵交換）
  自側のIPアドレスが動的に割り当てられる環境で、経路情報（送信先のIPアドレス）に従ってVPN通信を行います。認証情報、暗号情報の鍵は自動で交換します。
- 1つのIKEセッションに複数のIPsecトンネル構成でのVPN（自動鍵交換）
  複数のIPsec対象範囲が存在し、IPsec対象範囲をすべて（any）とすることができない環境で、IKEセッション（トンネル）を1つとしてVPN通信を行います。
  認証情報、暗号情報の鍵は自動で交換します。
- IPsec機能と他機能との併用
  IPsec機能と他機能を併用する場合のいくつかの設定例を説明します。
- 固定IPアドレスでバックアップ用に使用するVPN（自動鍵交換）（Si-R370、570）
  固定IPアドレスでのVPNに加えて、異常を検出した場合に、自動でバックアップを行い、処理を引き継ぐことができます。
- テンプレート着信機能（AAA認証）を使用した固定IPアドレスでのVPN（自動鍵交換）
  IKE不特定着信のIKE認証鍵取得にAAA認証機能を使用してVPN通信を行います。認証情報および暗号情報の鍵は自動で交換します。
- テンプレート着信機能（AAA認証）を使用した可変IPアドレスでのVPN（自動鍵交換）
  相手側のIPアドレスが動的に割り当てられる環境で、IKE不特定着信のIKE認証鍵取得にAAA認証機能を使用してVPN通信を行います。認証情報および暗号情報の鍵は自動で交換します。
- テンプレート着信機能（RADIUS認証）を使用した固定IPアドレスでのVPN（自動鍵交換）
  IKE不特定着信のIKE認証鍵取得にRADIUS認証機能を使用してVPN通信を行います。認証情報および暗号情報の鍵は自動で交換します。
- テンプレート着信機能（RADIUS認証）を使用した可変IPアドレスでのVPN（自動鍵交換）
  相手側のIPアドレスが動的に割り当てられる環境で、IKE不特定着信のIKE認証鍵取得にRADIUS認証機能を使用してVPN通信を行います。認証情報および暗号情報の鍵は自動で交換します。
- テンプレート着信機能（動的VPN）を使用した固定IPアドレスでのVPN（自動鍵交換）
  動的VPN接続契機パケットを監視して動的にVPN通信を行います。
  自装置のIPsecトンネルIPアドレス、IPsec対象範囲、IPsec経路情報および接続先監視アドレスは、動的VPN情報交換機能で自動的に交換されます。
- NATトラバーサルを使用した可変IPアドレスでのVPN（自動鍵交換）
  自側のIPアドレスが動的に割り当てられる環境で、IKE区間にあるNATを介したIPsec通信を可能にするために、NATトラバーサル機能を使用してVPN通信を行います。

- テンプレート着信機能（AAA 認証）および NAT トラバーサルを使用した可変 IP アドレスでの VPN（自動鍵交換）
  相手側の IP アドレスが動的に割り当てられる環境で、IKE 不特定着信の IKE 認証鍵取得に AAA 認証機能を使用し、また IKE 区間にある NAT を介した IPsec 通信を可能にするために、NAT トラバーサル機能を使用して VPN 通信を行います。認証情報および暗号情報の鍵は自動で交換します。

☛ 参照 Si-R シリーズ　機能説明書「2.13 IPsec 機能」（P.61）

こんな事に気をつけて

- IPsec は IPv4、IPv6 で使用できます。
- NAT 変換には、IPsec の前の変換と IPsec のあとの変換があります。IPsec 前に変換する場合は IPsec 用の remote ip nat コマンドで設定します。IPsec 後に変換する場合は、プロバイダ接続用の remote ip nat コマンドで設定します。
- インターネット VPN では、VPN 装置どうしがインターネットを介して通信する必要があるため、VPN 装置にはインターネット上で使用可能なグローバルな IP アドレスを使用してください（NAT を使用している場合は、マルチ NAT（静的 NAT）で IP アドレスを割り当てます）。
- VPN 相互接続するアドレスがプライベートアドレスの場合、重複しないように設計してください。
- IPsec では、IPv4、IPv6 パケット通信だけをサポートしています。IPv4、IPv6 パケット以外は VPN の対象とならないため中継されません。
- 暗号パケットが多重に暗号化される形態で使用しないでください。暗号パケットが二重に暗号化され、復号処理が正常に行えないため通信異常となります。
- IPsec と NAT 機能を併用する場合は、マルチ NAT を使用してください。
- IPsec とマルチ NAT を併用する場合は、静的 NAT の設定が必要となることがあります。
- 経路情報を設定する場合、IPsec/IKE ネゴシエーションパケットが VPN のトンネルに入らないように設定してください。
- 複数の接続先情報定義に同じ IPsec トンネルアドレスを定義しないでください。
- IKE セッションに対して複数の IPsec トンネル構成を使用する場合は、同じ IPsec 対象範囲がないように設定してください。
- IPsec 対象範囲が複数ネットワーク存在し、IPsec 対象範囲にすべて（any）を設定できない環境の場合だけ、“IKE セッションに対して複数の IPsec トンネル構成”を使用することをお勧めします。ネットワークごとに IPsec SA を作成する構成や IPsec 対象範囲にすべて（any）を定義できない装置と接続する場合は、“IKE セッションに対して複数の IPsec トンネル構成”を使用してください。
- テンプレート着信機能（AAA 認証および RADIUS 認証）を使用した IPsec では、IKE セッションに対して複数の IPsec トンネル構成を使用することはできません。
- テンプレート着信機能（AAA 認証および RADIUS 認証）を使用した IPsec では、初回 IKE ネゴシエーションは Responder でのみ動作します。
- RADIUS および AAA の登録情報を変更して IPsec が接続できない場合は、手動切断を行い、再度テンプレート着信機能で接続してください。
- テンプレート着信機能（AAA 認証および RADIUS 認証）を使用した IPsec では、自側トンネルエンドポイントアドレスに IPv6 DHCP クライアントが取得したプレフィックスを使用することはできません。
- テンプレート着信機能（AAA 認証および RADIUS 認証）を使用した IPsec では、テンプレート定義の接続先監視アドレスに IPv6 DHCP クライアントが取得したプレフィックスを使用することはできません。
- テンプレート着信機能（AAA 認証および RADIUS 認証）を使用した IPsec では、AAA 設定または RADIUS 認証サーバ側のユーザ ID とユーザ認証パスワードを同じに設定してください。
- 動的 VPN 情報交換機能を使用する場合、システム全体で一意となるユーザ ID を設定してください。
- テンプレート着信機能（動的 VPN）を使用した IPsec では、IKE セッションに対して複数の IPsec トンネル構成を使用することはできません。
- テンプレート着信機能（動的 VPN）を使用した IPsec では、IKE モードは Main Mode で動作します。
- テンプレート着信機能（動的 VPN）を使用した IPsec では、動的 VPN で作成されたインタフェースにスタティック経路情報が設定されるように動的 VPN 接続契機パケットを監視するインタフェースの経路情報を設定してください。
- テンプレート着信機能（動的 VPN）を使用した IPsec を行う場合は、動的 VPN サーバを V31 ファームウェアにする必要があります。
- V31 ファームウェアと V30 ファームウェアでテンプレート着信機能（動的 VPN）を使用した IPsec を行う場合は、V31 ファームウェアの動的 VPN クライアント情報設定で交換情報のエンコードタイプに "off" を指定する必要があります。
- 動的 VPN で接続する自側ネットワークを異るアドレスファミリで設定した場合、拡張 IPsec 対象範囲が 1 定義分追加されます。

- 拡張 IPsec 対象範囲機能未対応版数（V30）の装置と動的 VPN 接続を行う場合、動的 VPN で接続する自側ネットワークに異なるアドレスファミリを設定しないでください。
- 拡張 IPsec 対象範囲機能を使用して IPsec パケットを通過させた場合、IPsec 対象範囲をチェックする相手装置の場合は IPsec が遮断されます。この場合は、拡張 IPsec 対象範囲機能を使用することはできません。
- 拡張 IPsec 対象範囲を使用して双方向通信を行う場合、相手装置側にも同様の設定が必要です。相手装置側に、自側装置と同様の設定が存在しない場合、片側通信のみ暗号化し、折り返しの通信は暗号化されない場合があります。
- NAT トラバーサル機能を利用するときは、以下の点に注意してください。
  - IKE を行う双方の装置で設定してください。片方の装置での利用や NAT トラバーサルのバージョンが異なると、NAT トラバーサルはできません。
    NAT トラバーサルは、以下の RFC、Internet Draft のバージョンをサポートします。
    “Negotiation of NAT-Traversal in the IKE”
    RFC3947
    draft-ietf-ipsec-nat-t-ike-03
    draft-ietf-ipsec-nat-t-ike-02
    “UDP Encapsulation of IPsec ESP Packets”
    RFC3948
  - IPsec トンネルに存在する NAT 装置の変換テーブルが解放されると、NAT トラバーサルは動作できなくなります。変換テーブルを保持するために、接続先監視機能と併用することを推奨します。
  - IPsec 通信プロトコルは暗号（ESP）を使用するように設定してください。IPsec 通信プロトコルが認証（AH）の場合は動作しません。
  - 自側トンネルエンドポイントアドレス、および相手側エンドポイントアドレスに IPv4 アドレスを設定してください。IPv6 アドレスを設定した場合は動作しません。
  - IKE を使用する設定をしてください。動的 VPN（dvpn）および手動鍵（manual）を設定した場合は動作しません。
  - 初回 IKE ネゴシエーションが、initiator 装置側で NAT される環境でのみ動作します。
  - テンプレート着信機能（AAA 認証および RADIUS 認証）を使用した IPsec では、IKE モードを Aggressive Mode で設定してください。Main Mode で設定した場合は動作しません。

ヒント

◆ VPN とは？

暗号化技術や認証技術を使って、インターネットを仮想的な専用線として利用する技術です。また、VPN を使ってつないだルータ間の通信経路のことをトンネルと言います。

◆ 自動鍵交換とは？

IPsec の通信に使用される暗号化・認証用の鍵素材を、自動で作成・更新します。鍵素材を定期的に自動更新させることにより、セキュリティの強度を高めることができます。自動鍵交換を使用しない場合は、手動で鍵を設定する必要があります。

◆ NAT と IPsec を併用する

IPsec で使用するグローバルアドレスで NAT を使用している場合（IPsec 後の NAT 変換後）は、IPsec パケットが NAT を通過できるように、実回線の LAN または remote 定義で、以下の静的 NAT を設定します。

利用形態	設定内容
固定 IP アドレスでの VPN（手動鍵交換）	ESP パケットの受信を設定します。 ・プライベート IP 情報 IP アドレス　自側エンドポイントに設定したアドレス ポート番号　すべて ・グローバル IP 情報 IP アドレス　相手 VPN 装置に設定された本装置側の IP アドレス ポート番号　すべて ・プロトコル　ESP

利用形態	設定内容
固定 IP アドレスでの VPN（自動鍵交換）	IKE パケットの受信を設定します。 ・プライベート IP 情報 IP アドレス　自側エンドポイントに設定したアドレス ポート番号　500 ・グローバル IP 情報 IP アドレス　相手 VPN 装置に設定された本装置側の IP アドレス ポート番号　500 ・プロトコル　UDP ESP パケットの受信を設定します。 ・プライベート IP 情報 IP アドレス　自側エンドポイントに設定したアドレス ポート番号　すべて ・グローバル IP 情報 IP アドレス　相手 VPN 装置に設定された本装置側の IP アドレス ポート番号　すべて ・プロトコル　ESP 例） 本装置の WAN の自側 IP アドレスが 202.168.1.66（固定）であり、202.168.1.66（自側）と 202.168.2.66（相手側）の間で IPsec/IKE 通信を行う場合、IPsec/IKE 通信の自側エンドポイントに 202.168.1.66 を設定します。このとき静的 NAT のプライベートアドレスおよびグローバルアドレスには、202.168.1.66 を設定します。
可変 IP アドレスでの VPN（Initiator）	IKE パケットの受信を設定します。 ・プライベート IP 情報 IP アドレス　本装置の LAN 側 IP アドレス ポート番号　500 ・グローバル IP 情報 IP アドレス　指定しない ポート番号　500 ・プロトコル　UDP
可変 IP アドレスでの VPN（Initiator）	ESP パケットの受信を設定します。 ・プライベート IP 情報 IP アドレス　本装置の LAN 側 IP アドレス ポート番号　すべて ・グローバル IP 情報 IP アドレス　指定しない ポート番号　すべて ・プロトコル　ESP

2.13.1　IPv4 over IPv4で固定IPアドレスでのVPN（手動鍵交換）

適用機種　全機種

IPsec 機能を使って手動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社（PPPoE 常時接続)]

- ローカルネットワーク IP アドレス　：192.168.1.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス　：202.168.1.66/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IP アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IP アドレス　：202.168.2.65

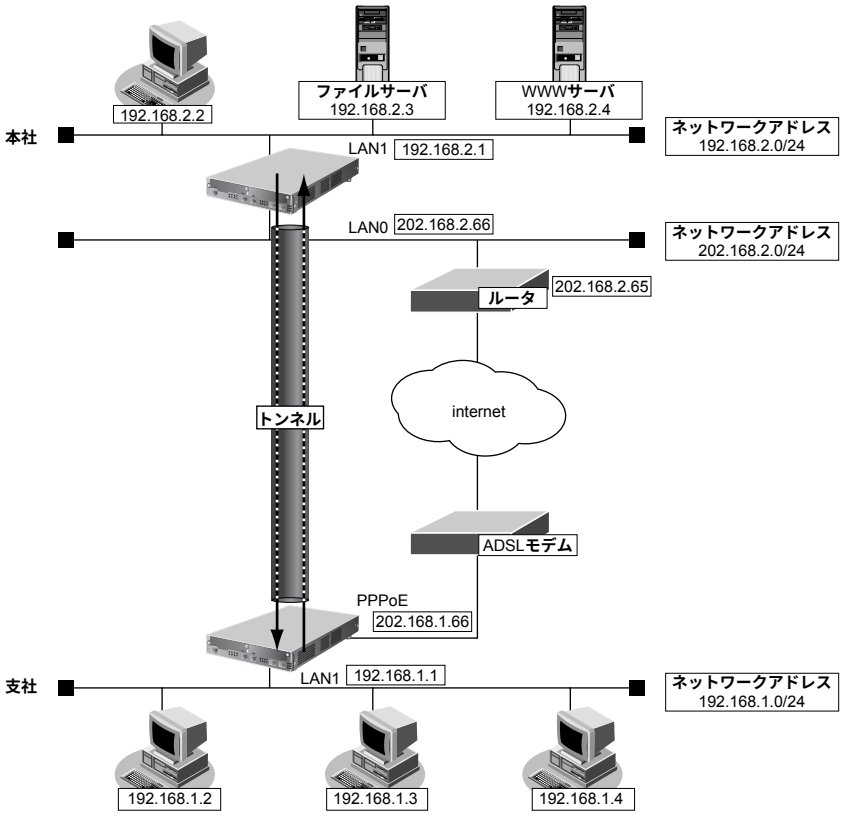
● 設定コマンド

[支社（PPPoE 常時接続)]

```
# delete lan 0
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1
# remote 0 ip address local 202.168.1.66
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1
# lan 1 ip address 192.168.2.1/24 3
```



● 設定条件

[支社]

- IPsec区間　：202.168.1.66 - 202.168.2.66
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット
- IPsecプロトコル　：esp
- IPsec送信用SPI　：100（16進数）
- IPsec送信用SA暗号アルゴリズムと暗号秘密鍵　：des-cbc、0123456789（16進数）
- IPsec送信用SA認証アルゴリズムと認証秘密鍵　：hmac-md5、123456789a（16進数）
- IPsec受信用SPI　：101（16進数）
- IPsec受信用SA暗号アルゴリズムと暗号秘密鍵　：des-cbc、23456789ab（16進数）
- IPsec受信用SA認証アルゴリズムと認証秘密鍵　：hmac-md5、3456789abc（16進数）

[本社]

- IPsec区間　：202.168.2.66 - 202.168.1.66
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット
- IPsecプロトコル　：esp
- IPsec送信用SPI　：101（16進数）
- IPsec送信用SA暗号アルゴリズムと暗号秘密鍵　：des-cbc、23456789ab（16進数）
- IPsec送信用SA認証アルゴリズムと認証秘密鍵　：hmac-md5、3456789abc（16進数）
- IPsec受信用SPI　：100（16進数）
- IPsec受信用SA暗号アルゴリズムと暗号秘密鍵　：des-cbc、0123456789（16進数）
- IPsec受信用SA認証アルゴリズムと認証秘密鍵　：hmac-md5、123456789a（16進数）

ヒント

◆ SPI とは？

トンネルの識別子です。SPI はトンネルの往路と復路でそれぞれ異なる値を設定します。トンネルをつなぐ本装置を設定するときには、同じ方向のトンネルには同じ SPI を設定します。

こんな事に気をつけて

- **暗号アルゴリズムに des-cbc を選択する場合、鍵に単純な文字列（同じ文字だけ、文字列の繰り返しなど）を指定すると、暗号強度が低下するおそれがあるので指定しないでください。暗号アルゴリズムに 3des-cbc を選択する場合は、鍵を 16 桁ごとに 3 つに分割した、それぞれ 3 つの暗号強度が低下する鍵（弱い鍵）にならないように指定してください。des-cbc で弱い鍵として具体的に知られているものには以下のようなものがあります。本装置は、これらの文字列で始まる鍵で通信できないようにしています。**
  0101 0101 0101 0101、1F1F 1F1F E0E0 E0E0、E0E0 E0E0 1F1F 1F1F、FEFE FEFE FEFE FEFE、
  01FE 01FE 01FE 01FE、1FE0 1FE0 0EF1 0EF1、01E0 01E0 01F1 01F1、FE01 FE01 FE01 FE01、
  E01F E01F F10E F10E、E001 E001 F101 F101、1FFE 1FFE 0EFE 0EFE、011F 011F 010E 010E、
  E0FE E0FE F1FE F1FE、FE1F FE1F FE0E FE0E、1F01 1F01 0E01 0E01、FEE0 FEE0 FEF1 FEF1
- **暗号アルゴリズムに 3des を選択する場合は、以下のように鍵を 16 桁ごとに 3 つに分割し、鍵 1 ≠鍵 2 ≠鍵 3 となるように鍵を設定してください。**
  鍵:　1122334455667788　9900aabbccddeeff　1122334455667788
  鍵 1（16 桁）　鍵 2（16 桁）　鍵 3（16 桁）
  鍵 1 ＝鍵 3 のように鍵を設定すると、16 バイトの鍵で暗号化するのと同じ結果になります。また、鍵 1 ＝鍵 2、鍵 2 ＝鍵 3 のように鍵を設定すると、それぞれ鍵 3、鍵 1 の des-cbc 暗号と同じ結果になります（鍵 1 ＝鍵 2 ＝鍵 3 の場合も同様です）。

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。

支社を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ap 0 name honten
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type manual

送信用 SA を設定する
# remote 1 ap 0 ipsec send protocol esp
# remote 1 ap 0 ipsec send spi 100
# remote 1 ap 0 ipsec send encrypt des-cbc hex 0123456789
# remote 1 ap 0 ipsec send auth hmac-md5 hex 123456789a

受信用 SA を設定する
# remote 1 ap 0 ipsec receive protocol esp
# remote 1 ap 0 ipsec receive spi 101
# remote 1 ap 0 ipsec receive encrypt des-cbc hex 23456789ab
# remote 1 ap 0 ipsec receive auth hmac-md5 hex 3456789abc

設定終了
# save
# commit
```

本社を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shi
# remote 0 ip route 0 192.168.1.0/24 1 0
# remote 0 ap 0 name shiten
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 tunnel remote 202.168.1.66
# remote 0 ap 0 ipsec type manual

送信用 SA を設定する
# remote 0 ap 0 ipsec send protocol esp
# remote 0 ap 0 ipsec send spi 101
# remote 0 ap 0 ipsec send encrypt des-cbc hex 23456789ab
# remote 0 ap 0 ipsec send auth hmac-md5 hex 3456789abc

受信用 SA を設定する
# remote 0 ap 0 ipsec receive protocol esp
# remote 0 ap 0 ipsec receive spi 100
# remote 0 ap 0 ipsec receive encrypt des-cbc hex 0123456789
# remote 0 ap 0 ipsec receive auth hmac-md5 hex 123456789a

設定終了
# save
# commit
```

2.13.2　IPv4 over IPv6 で固定 IP アドレスでの VPN（自動鍵交換）

IPsec 機能を使って IPv4 ローカルネットワーク間を IPv6 インターネットで結び、自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社（PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス
  ：202.168.1.66/24
- インターネットプロバイダから割り当てられた固定 IPv6 アドレス
  ：2001:db8:1111:1::66/64
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから割り当てられた固定 IPv6 アドレス　：2001:db8:1111:2::66/64
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65
- インターネットプロバイダから指定されたデフォルトルートの IPv6 アドレス：2001:db8:1111:2::65

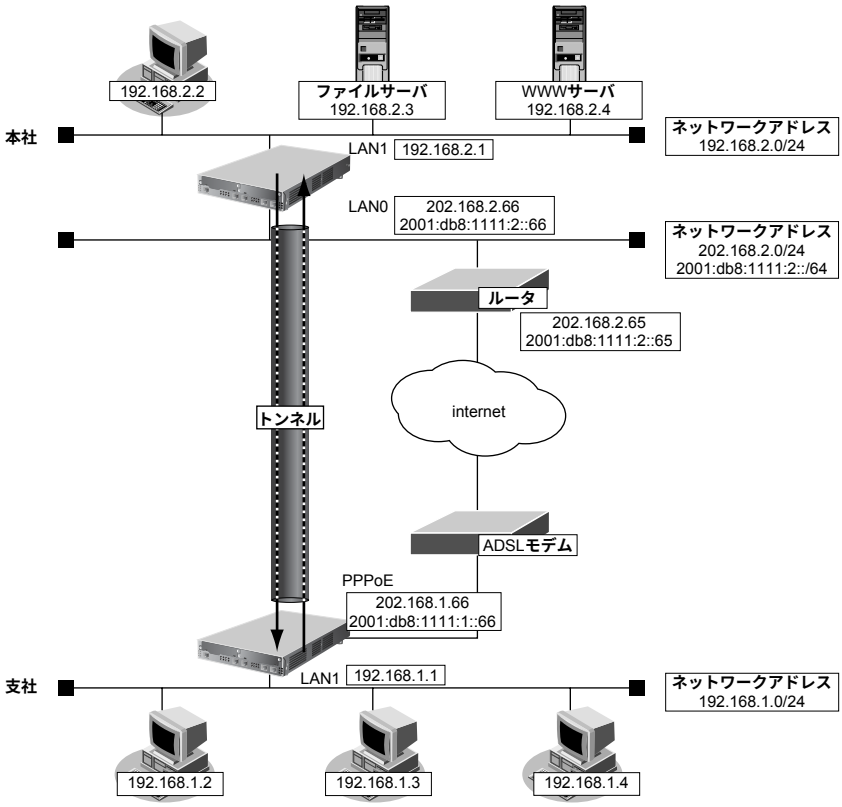
● 設定コマンド

[支社（PPPoE 常時接続)]

```
# delete lan 0
# lan 0 mode auto
# lan 0 ip6 use on
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 0
# remote 0 ip6 use on
# remote 0 ip6 address 0 2001:db8:1111:1::66/64 infinity infinity c0
# remote 0 ip6 route 0 default 1
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 0 ip6 use on
# lan 0 ip6 address 0 2001:db8:1111:2::66/64 infinity infinity c0
# lan 0 ip6 route 0 default 2001:db8:1111:2::65 1
# lan 1 ip address 192.168.2.1/24 3
```



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：2001:db8:1111:1::66-2001:db8:1111:2::66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[本社]

- ネットワーク名　：vpn-shi
- 接続先名　：shisya
- IPsec/IKE 区間　：2001:db8:1111:2::66-2001:db8:1111:1::66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Main Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

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。

支社を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 2001:db8:1111:1::66
# remote 1 ap 0 tunnel remote 2001:db8:1111:2::66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

本社を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shi
# remote 0 ip route 0 192.168.1.0/24 1 0
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 2001:db8:1111:2::66
# remote 0 ap 0 tunnel remote 2001:db8:1111:1::66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode main
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

2.13.3 IPv4 over IPv6 で可変 IP アドレスでの VPN（自動鍵交換）

接続するたびに IP アドレスが変わる環境で VPN を構築する場合の設定方法を説明します。

IPv4 ローカルネットワーク間を IPv6 インターネットで結んで IPsec を行います。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社（PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから割り当てられた固定 IPv6 アドレス　：2001:db8:1111:2::66/64
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65
- インターネットプロバイダから指定されたデフォルトルートの IPv6 アドレス：2001:db8:1111:2::65

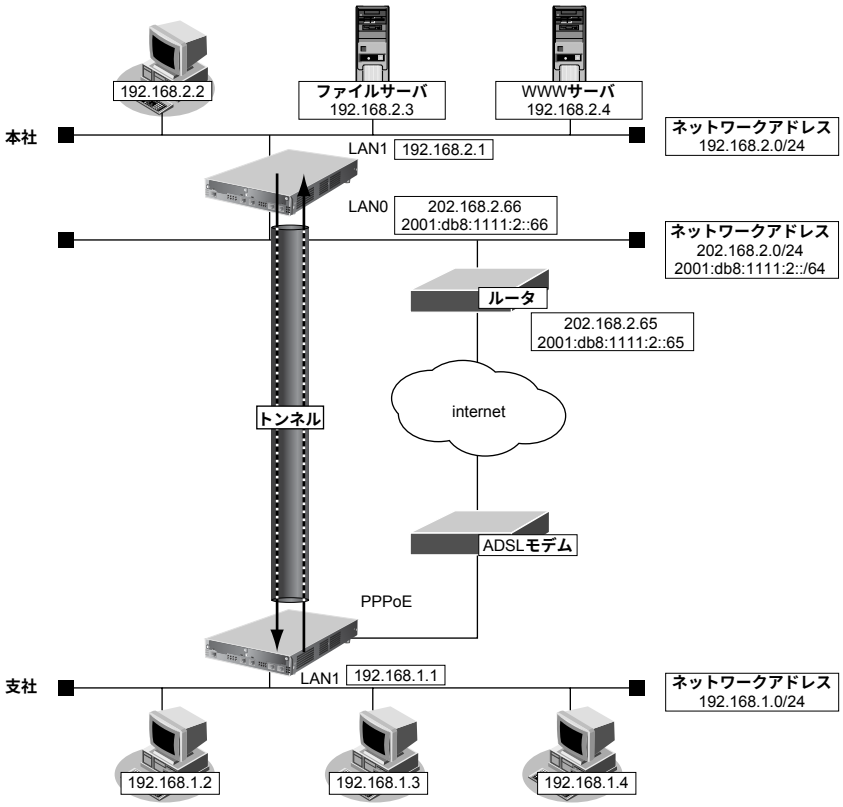
● 設定コマンド

[支社（PPPoE 常時接続)]

```
# delete lan 0
# lan 0 mode auto
# lan 0 ip6 use on
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 0
# remote 0 ip6 use on
# remote 0 ip6 route 0 default 1
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 0 ip6 use on
# lan 0 ip6 route 0 default 2001:db8:1111:2::65 1
# lan 0 ip6 address 0 2001:db8:1111:2::66/64 infinity infinity c0
# lan 1 ip address 192.168.2.1/24 3
```



● 設定条件

[支社（Initiator)]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：支社-2001:db8:1111:2::66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- IKE（UDP:500 番ポート）のプライベートアドレス
  ：2001:db8:1111:1::66
  （インターネットプロバイダから割り当てられた IPv6 アドレス）
- ESP のプライベートアドレス　：2001:db8:1111:1::66
  （インターネットプロバイダから割り当てられた IPv6 アドレス）

[本社]

- ネットワーク名　：vpn-shi
- 接続先名　：shisya
- IPsec/IKE 区間　：2001:db8:1111:2::66-支社
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Aggressive Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 支社 ID/ID タイプ　：shisya（自装置名）/FQDN

- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは？

Aggressive Mode **の場合に、ネゴシエーションで使用する自装置を識別する** ID **の種別です。相手** VPN **装置の設定に合わせます。**

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。

支社（Initiator）を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel remote 2001:db8:1111:2::66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

本社（Responder）を設定する

● コマンド

VPN を設定する
remote 0 name vpn-shi
remote 0 ip route 0 192.168.1.0/24 1 0
remote 0 ap 0 name shisya
remote 0 ap 0 datalink type ipsec
remote 0 ap 0 tunnel local 2001:db8:1111:2::66
remote 0 ap 0 ipsec type ike
remote 0 ap 0 ipsec ike protocol esp
remote 0 ap 0 ipsec ike encrypt des-cbc
remote 0 ap 0 ipsec ike auth hmac-md5
remote 0 ap 0 ike mode aggressive
remote 0 ap 0 ike name remote shisya
remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
remote 0 ap 0 ike proposal encrypt des-cbc

設定終了
save
commit

2.13.4　IPv6 over IPv4 で固定 IP アドレスでの VPN（自動鍵交換）

IPsec 機能を使って IPv6 ローカルネットワーク間を IPv4 インターネットで結び、自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社（PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- ローカルネットワーク IPv6 アドレス　：2001:db8:1111:1::1/64
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.1.66/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- ローカルネットワーク IPv6 アドレス　：2001:db8:1111:2::1/64
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス　：202.168.2.65

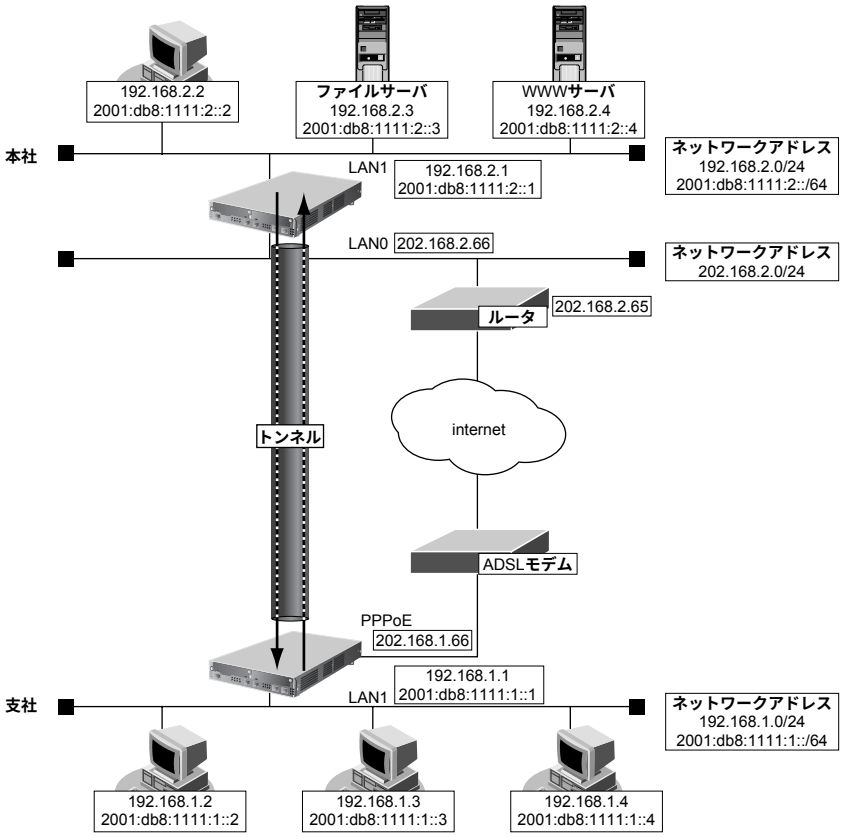
● 設定コマンド

[支社（PPPoE 常時接続)]

```
# delete lan 0
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip6 use on
# lan 1 ip6 address 0 2001:db8:1111:1::1/64 infinity infinity c0
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ip6 use on
# lan 1 ip6 address 0 2001:db8:1111:2::1/64 infinity infinity c0
```



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：202.168.1.66-202.168.2.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[本社]

- ネットワーク名　：vpn-shi
- 接続先名　：shisya
- IPsec/IKE 区間　：202.168.2.66-202.168.1.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Main Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

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。

支社（Initiator）を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip6 use on
# remote 1 ip6 route 0 2001:db8:1111:2::/64 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

本社を設定する

● コマンド

```
VPNを設定する
# remote 0 name vpn-shi
# remote 0 ip6 use on
# remote 0 ip6 route 0 2001:db8:1111:1::/64 1
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 tunnel remote 202.168.1.66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any6 any6
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode main
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

2.13.5　IPv6 over IPv4 で可変 IP アドレスでの VPN（自動鍵交換）

接続するたびに IP アドレスが変わる環境で VPN を構築する場合の設定方法を説明します。

IPv6 ローカルネットワーク間を IPv4 インターネットで結んで IPsec を行います。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社（PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- ローカルネットワーク IPv6 アドレス　：2001:db8:1111:1::1/64
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- ローカルネットワーク IPv6 アドレス　：2001:db8:1111:2::1/64
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65

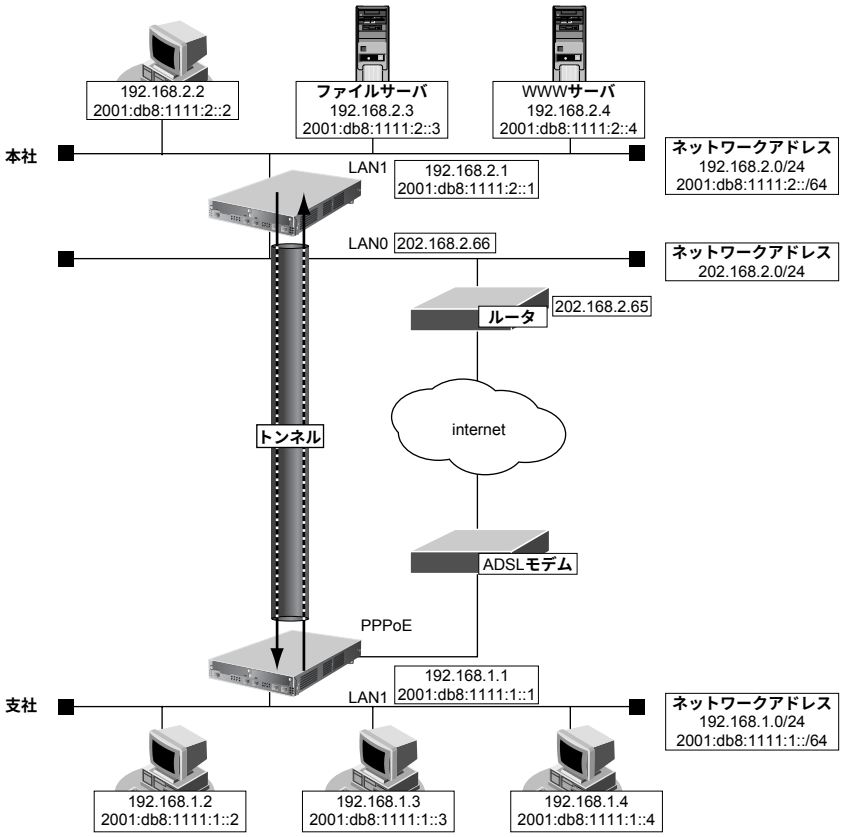
● 設定コマンド

[支社（PPPoE 常時接続)]

```
# delete lan 0
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip6 use on
# lan 1 ip6 address 0 2001:db8:1111:1::1/64 infinity infinity c0
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 0
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ip6 use on
# lan 1 ip6 address 0 2001:db8:1111:2::1/64 infinity infinity c0
```



● 設定条件

[支社（Initiator)]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：支社-202.168.2.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- IKE（UDP:500 番ポート）のプライベートアドレス：192.168.1.1
- ESP のプライベートアドレス　：192.168.1.1

[本社]

- ネットワーク名　：vpn-shi
- 接続先名　：shisya
- IPsec/IKE 区間　：202.168.2.66-支社
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Aggressive Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 支社 ID/ID タイプ　：shisya（自装置名）/FQDN
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared

- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは？

Aggressive Mode **の場合に、ネゴシエーションで使用する自装置を識別する** ID **の種別です。相手** VPN **装置の設定に合わせます。**

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。

支社（Initiator）を設定する

● コマンド

```
インターネットから IPsec/IKE パケットを受信する設定をする
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip6 use on
# remote 1 ip6 route 0 2001:db8:1111:2::/64 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

本社（Responder）を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shi
# remote 0 ip6 use on
# remote 0 ip6 route 0 2001:db8:1111:1::/64 1
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any6 any6
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode aggressive
# remote 0 ap 0 ike name remote shisya
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

2.13.6　IPv6 over IPv6 で固定 IP アドレスでの VPN（自動鍵交換）

IPsec 機能を使って IPv6 で自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社（PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- ローカルネットワーク IPv6 アドレス　：2001:db8:1111:3::1/64
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス
  ：202.168.1.66/24
- インターネットプロバイダから割り当てられた固定 IPv6 アドレス
  ：2001:db8:1111:1::66/64
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- ローカルネットワーク IPv6 アドレス　：2001:db8:1111:4::1/64
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから割り当てられた固定 IPv6 アドレス　：2001:db8:1111:2::66/64
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65
- インターネットプロバイダから指定されたデフォルトルートの IPv6 アドレス：2001:db8:1111:2::65

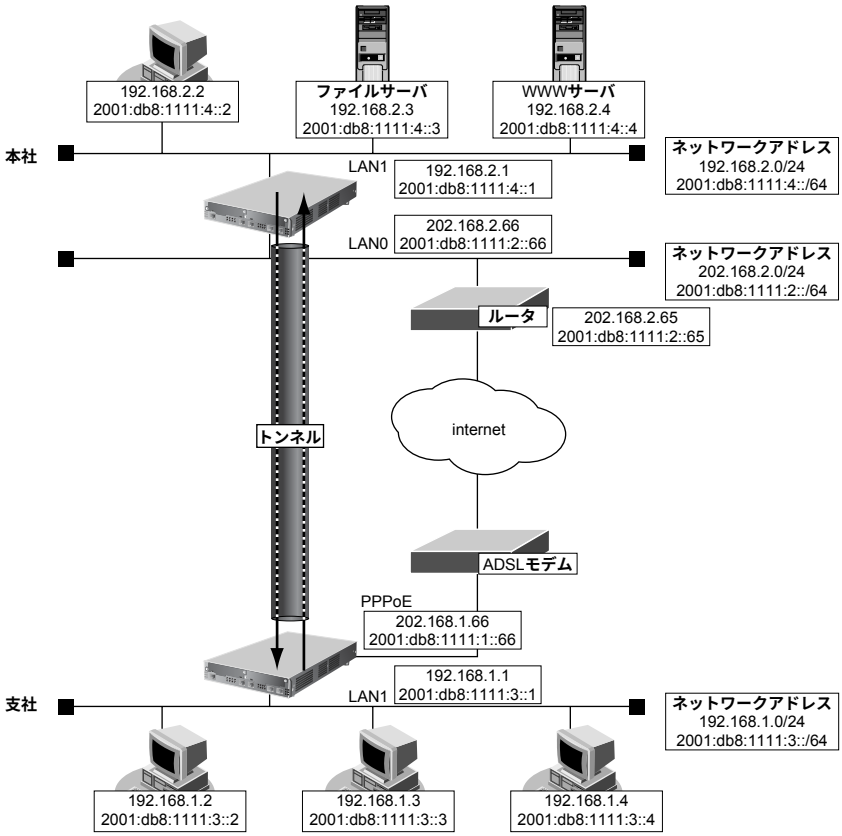
● 設定コマンド

[支社（PPPoE 常時接続)]

```
# delete lan 0
# lan 0 mode auto
# lan 0 ip6 use on
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip6 use on
# lan 1 ip6 address 0 2001:db8:1111:3::1/64 infinity infinity c0
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 0
# remote 0 ip6 use on
# remote 0 ip6 route 0 default 1
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 0 ip6 use on
# lan 0 ip6 address 0 2001:db8:1111:2::66/64 infinity infinity c0
# lan 0 ip6 route 0 default 2001:db8:1111:2::65 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ip6 use on
# lan 1 ip6 address 0 2001:db8:1111:4::1/64 infinity infinity c0
```



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：2001:db8:1111:1::66-2001:db8:1111:2::66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[本社]

- ネットワーク名　：vpn-shi
- 接続先名　：shisya
- IPsec/IKE 区間　：2001:db8:1111:2::66-2001:db8:1111:1::66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Main Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc

- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

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。

支社を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ip6 use on
# remote 1 ip6 route 0 2001:db8:1111:4::/64 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 2001:db8:1111:1::66
# remote 1 ap 0 tunnel remote 2001:db8:1111:2::66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

本社を設定する

● コマンド

VPN を設定する
remote 0 name vpn-shi
remote 0 ip route 0 192.168.1.0/24 1 0
remote 0 ip6 use on
remote 0 ip6 route 0 2001:db8:1111:3::/64 1
remote 0 ap 0 name shisya
remote 0 ap 0 datalink type ipsec
remote 0 ap 0 tunnel local 2001:db8:1111:2::66
remote 0 ap 0 tunnel remote 2001:db8:1111:1::66
remote 0 ap 0 ipsec type ike
remote 0 ap 0 ipsec ike protocol esp
remote 0 ap 0 ipsec ike range any6 any6
remote 0 ap 0 ipsec ike encrypt des-cbc
remote 0 ap 0 ipsec ike auth hmac-md5
remote 0 ap 0 ike mode main
remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
remote 0 ap 0 ike proposal encrypt des-cbc

設定終了
save
commit

2.13.7　IPv6 over IPv6 で可変 IP アドレスでの VPN（自動鍵交換）

接続するたびに IPv6 アドレスが変わる環境で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社（PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- ローカルネットワーク IPv6 アドレス　：2001:db8:1111:3::1/64
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- ローカルネットワーク IPv6 アドレス　：2001:db8:1111:4::1/64
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから割り当てられた固定 IPv6 アドレス　：2001:db8:1111:2::66/64
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65
- インターネットプロバイダから指定されたデフォルトルートの IPv6 アドレス：2001:db8:1111:2::65

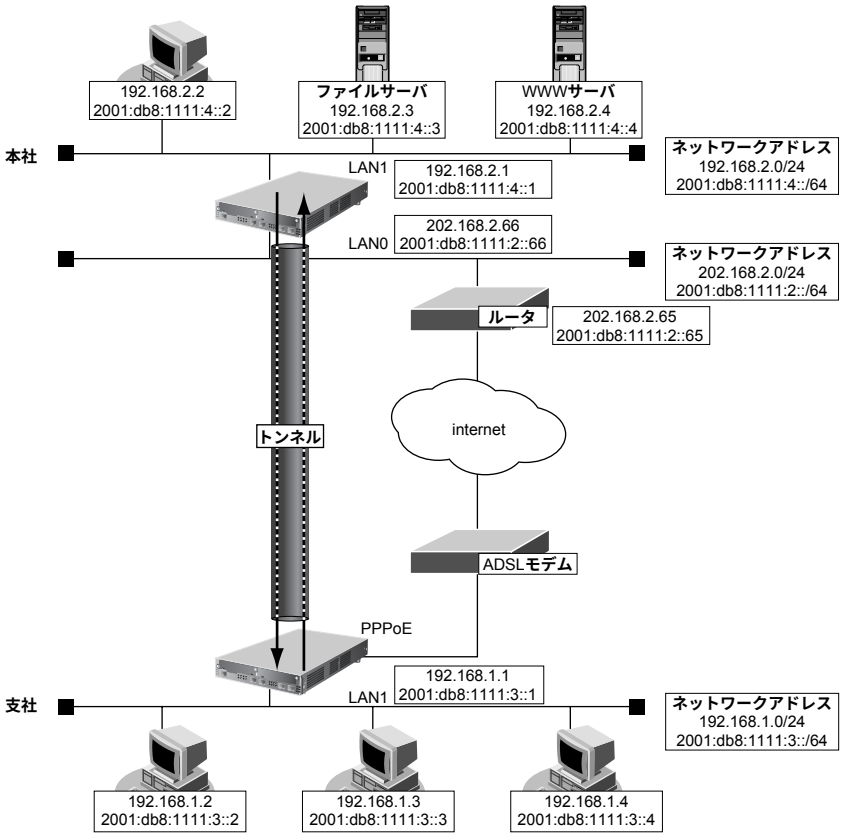
● 設定コマンド

[支社（PPPoE 常時接続)]

```
# delete lan 0
# lan 0 mode auto
# lan 0 ip6 use on
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip6 use on
# lan 1 ip6 address 0 2001:db8:1111:3::1/64 infinity infinity c0
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 0
# remote 0 ip6 use on
# remote 0 ip6 route 0 default 1
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 0 ip6 use on
# lan 0 ip6 route 0 default 2001:db8:1111:2::65 1
# lan 0 ip6 address 0 2001:db8:1111:2::66/64 infinity infinity c0
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ip6 use on
# lan 1 ip6 address 0 2001:db8:1111:4::1/64 infinity infinity c0
```



● 設定条件

[支社（Initiator)]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：支社-2001:db8:1111:2::66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- IKE（UDP:500 番ポート）のプライベートアドレス
  ：2001:db8:1111:1::66
  （インターネットプロバイダから割り当てられた IPv6 アドレス）
- ESP のプライベートアドレス　：2001:db8:1111:1::66
  （インターネットプロバイダから割り当てられた IPv6 アドレス）

[本社]

- ネットワーク名　：vpn-shi
- 接続先名　：shisya
- IPsec/IKE 区間　：2001:db8:1111:2::66-支社
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Aggressive Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 支社 ID/ID タイプ　：shisya（自装置名）/FQDN

- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは？

Aggressive Mode **の場合に、ネゴシエーションで使用する自装置を識別する** ID **の種別です。相手** VPN **装置の設定に合わせます。**

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。

支社（Initiator）を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ip6 use on
# remote 1 ip6 route 0 2001:db8:1111:4::/64 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel remote 2001:db8:1111:2::66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

本社（Responder）を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shi
# remote 0 ip route 0 192.168.1.0/24 1 0
# remote 0 ip6 use on
# remote 0 ip6 route 0 2001:db8:1111:3::/64 1
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 2001:db8:1111:2::66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any6 any6
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode aggressive
# remote 0 ap 0 ike name remote shisya
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

2.13.8 IPv4 over IPv4で1つのIKEセッションに複数のIPsecトンネル構成でのVPN（自動鍵交換）

適用機種　全機種

IPsec機能を使って複数のネットワークにそれぞれのIPsec SAを作成する環境を構築する場合を例に説明します（自動鍵交換の固定IPアドレスを使用した構成です）。

ここでは以下のコマンドにより、支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社（PPPoE常時接続)]

- ローカルネットワークIPアドレス　：192.168.1.1/24
- インターネットプロバイダから割り当てられた固定のIPアドレス　：202.168.1.66/24
- PPPoEユーザ認証ID　：userid（プロバイダから提示された内容）
- PPPoEユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用

[本社]

- ローカルネットワークIPアドレス1　：LAN0ポート使用
- ローカルネットワークIPアドレス2　：192.168.3.1/24
- インターネットプロバイダから割り当てられた固定のIPアドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートのIPアドレス　：202.168.2.65

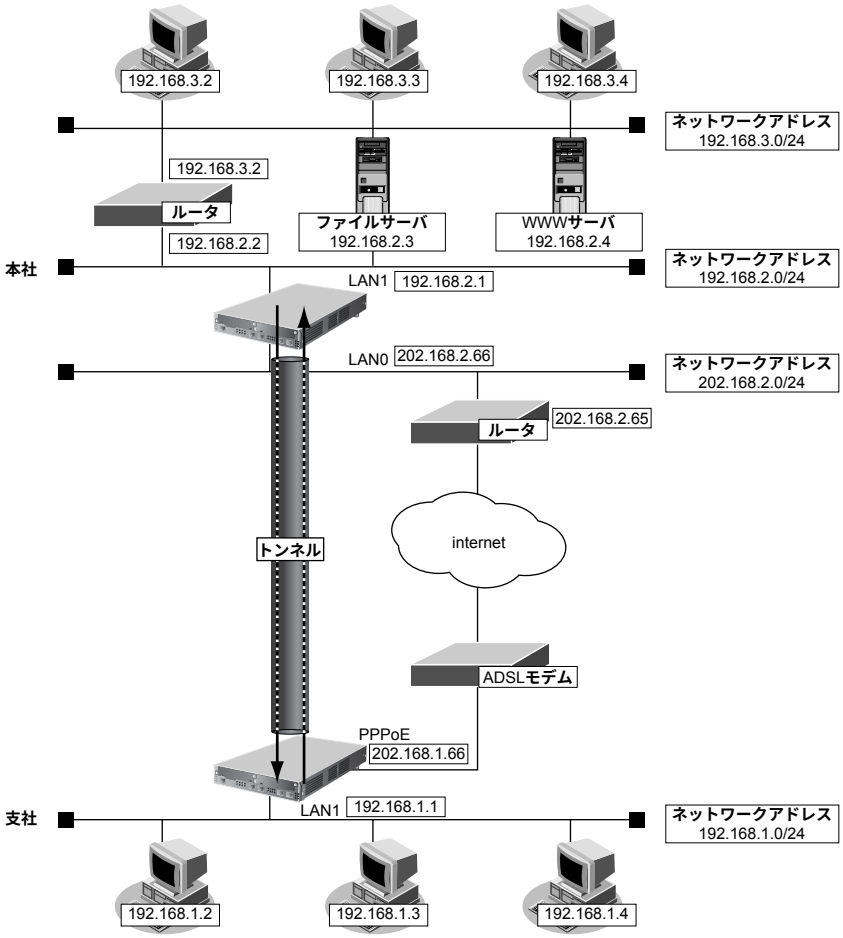
● 設定コマンド

[支社（PPPoE接続)]

```
# delete lan 0
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1
# remote 0 ip address local 202.168.1.66
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ip route 0 192.168.3.0/24 192.168.2.2 1
```



● 設定条件

[支社]

- IPsec/IKE 区間　：202.168.1.66 - 202.168.2.66
- IPsec 対象範囲（1）　：any - 192.168.2.0/24（マルチルーティングにも定義する）
- IPsec 対象範囲（2）　：any - 192.168.3.0/24

[本社]

- IPsec/IKE 区間　：202.168.2.66 - 202.168.1.66
- IPsec 対象範囲（1）　：192.168.2.0/24 - any（マルチルーティングにも定義する）
- IPsec 対象範囲（2）　：192.168.3.0/24 - any

[共通]

- 鍵交換モード　：Main Mode
- IPsec プトロコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec PFS 時の DH グループ　：なし
- IKE 共有鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方式　：shared（事前共有鍵方式）
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証（ハッシュ）アルゴリズム：hmac-md5
- IKE DH グループ　：modp768（グループ 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。

支社を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ip route 1 192.168.3.0/24 1 0
# remote 1 ap 0 name honten1
# remote 1 ap 0 multiroute pattern 0 use any any 192.168.2.0/24 any 0 any
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 192.168.2.0/24
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
# remote 1 ap 1 datalink type ipsec
# remote 1 ap 1 ipsec type ike
# remote 1 ap 1 ipsec ike protocol esp
# remote 1 ap 1 ipsec ike range any4 192.168.3.0/24
# remote 1 ap 1 ipsec ike encrypt des-cbc
# remote 1 ap 1 ipsec ike auth hmac-md5
# remote 1 ap 1 ike bind ap 0

設定終了
# save
# commit
```

本社を設定する

● コマンド

VPN を設定する
remote 0 name vpn-shi
remote 0 ip route 0 192.168.1.0/24 1 0
remote 0 ap 0 name shiten
remote 0 ap 0 multiroute pattern 0 use 192.168.2.0/24 any any any 0 any
remote 0 ap 0 datalink type ipsec
remote 0 ap 0 tunnel local 202.168.2.66
remote 0 ap 0 tunnel remote 202.168.1.66
remote 0 ap 0 ipsec type ike
remote 0 ap 0 ipsec ike protocol esp
remote 0 ap 0 ipsec ike range 192.168.2.0/24 any4
remote 0 ap 0 ipsec ike encrypt des-cbc
remote 0 ap 0 ipsec ike auth hmac-md5
remote 0 ap 0 ike bind self
remote 0 ap 0 ike mode main
remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
remote 0 ap 0 ike proposal encrypt des-cbc
remote 0 ap 1 datalink type ipsec
remote 0 ap 1 ipsec type ike
remote 0 ap 1 ipsec ike protocol esp
remote 0 ap 1 ipsec ike range 192.168.3.0/24 any4
remote 0 ap 1 ipsec ike encrypt des-cbc
remote 0 ap 1 ipsec ike auth hmac-md5
remote 0 ap 1 ike bind ap 0

設定終了
save
commit

2.13.9　IPsec 機能と他機能との併用

適用機種　全機種

IPsec 機能と他機能を併用する場合のいくつかの設定例を、以下に説明します。

ここでは、「1.14 複数の事業所 LAN を VPN（IPsec）で接続する」（P.46）の設定が行われていることを前提とします。

- IPsec 変換前のマルチ NAT ／ IP フィルタリング ／ TOS 値書き換え機能
- IPsec 変換前のシェーピング機能と帯域制御（WFQ）機能
- IPsec 変換前の MSS 書換え機能
- IPsec 変換前の MTU 分割機能
- 接続先監視機能
- IKE セッション監視機能
- 動的経路（RIP）機能

補足　以下の機能については、IPv6 アドレスで使用することはできません。
- IPsec 変換前のマルチ NAT 機能
- IKE セッション監視機能

IPsec 変換前のマルチ NAT ／ IP フィルタリング／ TOS 値書き換え機能との併用例

● 設定条件

[支社]

- NAT の使用　：マルチ NAT を使用する
  グローバルアドレス　：192.168.1.1
  アドレス個数　：1
  アドレス割当てタイマ　：5 分
- IP フィルタリング　：支社 - 本社間の telnet ／ ftp 通信以外遮断
- TOS 値書き換え　：ftp 通信を 0xa0 に変換

[本社]

- IP フィルタリング　：支社 - 本社間の telnet ／ ftp 通信以外遮断
- TOS 値書き換え　：ftp 通信を 0xa0 に変換

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。

支社を設定する

● コマンド

```
# remote 1 ip nat mode multi 192.168.1.1 1

# acl 0 ip 192.168.1.0/24 192.168.2.0/24 6 any
# acl 0 tcp any 21,23 yes
# acl 1 ip 192.168.2.0/24 192.168.1.0/24 6 any
# acl 1 tcp 21,23 any no
# acl 2 ip any any any any
# acl 3 ip 192.168.1.0/24 192.168.2.0/24 6 any
# acl 3 tcp any 20,21 yes

# remote 1 ip filter 0 pass acl 0 out
# remote 1 ip filter 1 pass acl 1 in
# remote 1 ip filter 2 reject acl 2 any
# remote 1 ip tos 0 acl 3 a0
```

本社を設定する

● コマンド

```
# acl 0 ip 192.168.1.0/24 192.168.2.0/24 6 any
# acl 0 tcp any 21,23 yes
# acl 1 ip 192.168.2.0/24 192.168.1.0/24 6 any
# acl 1 tcp 21,23 any no
# acl 2 ip any any any any
# acl 3 ip 192.168.2.0/24 192.168.1.0/24 6 any
# acl 3 tcp any 20,21 yes

# remote 0 ip filter 0 pass acl 0 in
# remote 0 ip filter 1 pass acl 1 out
# remote 0 ip filter 2 reject acl 2 any
# remote 0 ip tos 0 acl 3 a0
```

IPsec 変換前のシェーピング機能と帯域制御（WFQ）機能の併用例

● 設定条件

[本社]

- シェーピングレート　：2Mbps
- 帯域制御対象送信元 IP アドレス　：192.168.2.0/24
- 帯域制御対象送信元ポート番号　：すべて
- 帯域制御対象あて先 IP アドレス　：192.168.1.0/24
- 帯域制御対象あて先ポート番号　：すべて
- 帯域制御対象プロトコル　：TCP
- 帯域制御対象 TOS 値　：すべて
- 割り当て帯域　：最優先

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。

本社を設定する

● コマンド

```
# remote 0 shaping on 2m
# acl 0 ip 192.168.2.0/24 192.168.1.0/24 6 any
# remote 0 ip priority 0 acl 0 express
```

こんな事に気をつけて

IPsec 機能と帯域制御（WFQ）機能を併用する場合、IPsec 前のパケットに対して帯域制御を行うときには、IPsec 用の remote で設定します。この場合、IPsec 用の remote でシェーピングを行うか、または、実回線の remote で IPsec 後のパケットに対して帯域制御を設定する必要があります。

IPsec 変換前の MSS 書き換え機能との併用例

● 設定条件

[共通]

- MSS 書き換え値　：1414Byte

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。

支社を設定する

● コマンド

```
# remote 1 ip msschange 1414
```

本社を設定する

● コマンド

```
# remote 0 ip msschange 1414
```

IPsec変換前のMTU分割機能との併用例

● 設定条件

[共通]

- MTU長　：1460Byte

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。

支社を設定する

● コマンド

```
# remote 1 mtu 1460
```

本社を設定する

● コマンド

```
# remote 0 mtu 1460
```

接続先監視機能との併用例

● 設定条件

[支社]

- 送信元IPアドレス　：192.168.1.1
- あて先IPアドレス　：192.168.2.1
- タイムアウト時間　：5秒
- 正常時送信間隔　：10秒
- 異常時送信間隔　：1分

補足 監視対象装置は、本社側VPN装置を指定します。

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。

支社を設定する

● コマンド

```
# remote 1 ap 0 sessionwatch address 192.168.1.1 192.168.2.1
```

IKE セッション監視機能との併用例

● 設定条件

[支社]

- あて先 IP アドレス　：192.168.2.1
- タイムアウト時間　：5 秒
- 正常時送信間隔　：10 秒
- 異常時送信間隔　：1 分

補足 監視対象装置は、本社側 VPN 装置を指定します。

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。

支社を設定する

● コマンド

```
# remote 1 ap 0 ike sessionwatch 192.168.2.1 10s 1m 5s
```

こんな事に気をつけて

- **接続先監視／ IKE セッション監視のあて先 IP アドレスは、**remote ap ipsec ike range **コマンドで設定する** IPsec **対象パケット範囲に含まれる IP アドレスを指定してください。**
- **接続先監視／ IKE セッション監視のあて先 IP アドレスに、常時運転している** IPsec **対象の装置を指定してください。あて先 IP アドレスに相手 IKE サーバとは異なる装置を指定した場合、あて先 IP アドレスからの応答が受信できなくなります。その場合、相手 IKE サーバが生存していても** IPsec/IKE SA **は解放されます。そのため通信が不安定にあることがあります。**

動的経路（RIP）機能との併用例

● 設定条件

[共通]

- RIP 送信　：v1
- RIP 受信　：v1
- RIP 送信時加算メトリック値　：0

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。

支社を設定する

● コマンド

```
# delete remote 1 ip route
# remote 1 ip rip use v1 v1 0 off
```

本社を設定する

● コマンド

```
# delete remote 0 ip route
# remote 0 ip rip use v1 v1 0 off
```

2.13.10 IPv4 over IPv4で固定IPアドレスでバックアップ用に使用するVPN（自動鍵交換）

適用機種 ***Si-R220B,370,570***

専用線側の通信パスに障害が発生した場合にISDN回線を利用し、ISDN回線側ではIPsec機能を使って自動鍵交換でVPNを構築することによって通信をバックアップする場合の設定方法を説明します。

ここでは、以下のとおり支社と本社が専用線で接続されていることを前提とします。

● 前提条件

[支社]

- ローカルネットワークIPアドレス　：192.168.1.1/24
- 専用線使用スロット　：SLOT0
- 専用線回線速度　：128K
- 専用線自側IPアドレス　：201.168.1.1
- ネットワーク名　：honsya
- 接続先名　：honsya

[本社]

- ローカルネットワークIPアドレス　：192.168.2.1/24
- 専用線使用スロット　：SLOT0
- 専用線回線速度　：128K
- 専用線自側IPアドレス　：201.168.1.2
- ネットワーク名　：shisya
- 接続先名　：shisya

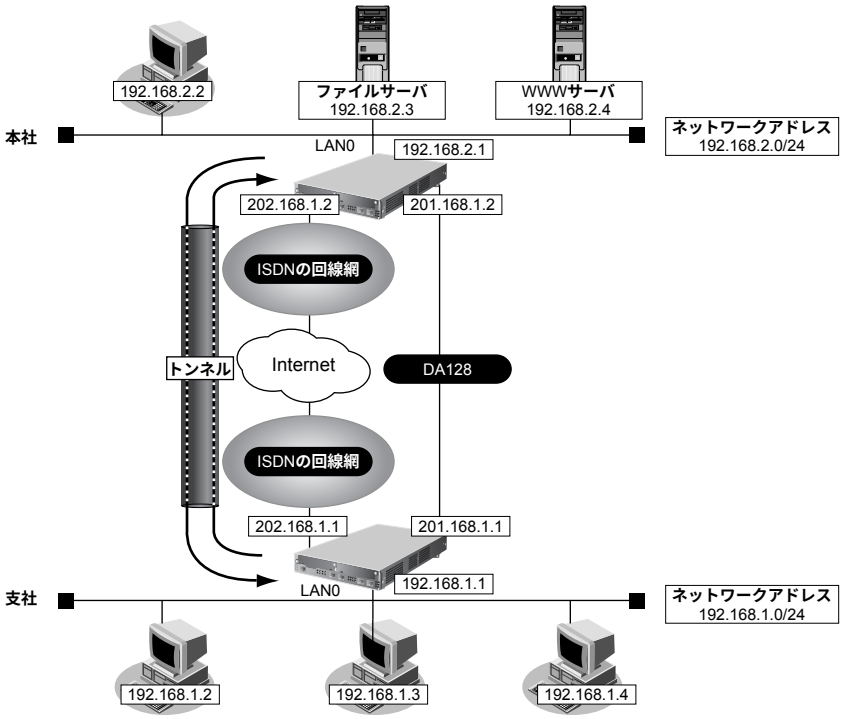
● 設定コマンド

[支社]

```
# wan 0 line hsd 128k
# wan 0 bind 0
# lan 0 ip address 192.168.1.1/24 3
# remote 0 name honsya
# remote 0 ip address local 201.168.1.1
# remote 0 ip route 0 default 1
# remote 0 ap 0 name honsya
# remote 0 ap 0 datalink bind wan 0
```

[本社]

```
# wan 0 line hsd 128k
# wan 0 bind 0
# lan 0 ip address 192.168.2.1/24 3
# remote 0 name shisya
# remote 0 ip address local 201.168.1.2
# remote 0 ip route 0 default 1
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink bind wan 0
```



● 設定条件

[支社]

- 接続先名　：vpn-hon

[バックアップ回線（ISDN）]

- ネットワーク名　：hon-back
- 接続先名　：hon-back
- ISDN 回線使用スロット　：SLOT1
- ISP 電話番号　：123-4567-891
- ユーザ認証 ID　：userid（プロバイダから提示された内容）
- ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- ISDN 自側 IP アドレス　：202.168.1.1
- ISDN 回線無通信監視　：5 分
- IPsec/IKE 区間　：202.168.1.1 - 202.168.1.2
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- 専用線（レギュラー回線）ダウン時動作　：ISDN 回線で IPsec/IKE を使用
- 接続先監視機能　：使用する

[本社]

- 接続先名　：vpn-shi

[バックアップ回線（ISDN）]

- ネットワーク名　：shi-back
- 接続先名　：shi-back
- ISDN 回線使用スロット　：SLOT1
- ISP 電話番号　：123-4567-890
- ユーザ認証 ID　：userid（プロバイダから提示された内容）
- ユーザ認証パスワード　：userpass（プロバイダから提示された内容）

- ISDN 自側 IP アドレス　：202.168.1.2
- 常時接続　：する
- IPsec/IKE 区間　：202.168.1.2 - 202.168.1.1
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- 専用線（レギュラー回線）ダウン時動作　：ISDN 回線で IPsec/IKE を使用
- 接続先監視機能　：使用する

[共通]

- 鍵交換タイプ　：Main Mode
- IPsec プトロコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

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。

支社を設定する

● コマンド

VPN を設定する
remote 0 ap 0 sessionwatch address 201.168.1.1 201.168.1.2
remote 0 ap 1 name vpn-hon
remote 0 ap 1 datalink type ipsec
remote 0 ap 1 tunnel local 202.168.1.1
remote 0 ap 1 tunnel remote 202.168.1.2
remote 0 ap 1 ipsec type ike
remote 0 ap 1 ipsec ike protocol esp
remote 0 ap 1 ipsec ike encrypt des-cbc
remote 0 ap 1 ipsec ike auth hmac-md5
remote 0 ap 1 ike mode main
remote 0 ap 1 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
remote 0 ap 1 ike proposal encrypt des-cbc

バックアップ回線（ISDN）を設定する
wan 1 line isdn
wan 1 bind 1
remote 1 name hon-back
remote 1 autodial enable
remote 1 ip address local 202.168.1.1
remote 1 ip route 0 202.168.1.2/32 1
remote 1 ap 0 name hon-back
remote 1 ap 0 datalink bind wan 1
remote 1 ap 0 dial 0 number 123-4567-891
remote 1 ap 0 idle 5m
remote 1 ap 0 ppp auth send userid userpass

設定終了
save

再起動
reset

本社を設定する

● コマンド

```
VPNを設定する
# remote 0 ap 0 sessionwatch address 201.168.1.2 201.168.1.1
# remote 0 ap 1 name vpn-shi
# remote 0 ap 1 datalink type ipsec
# remote 0 ap 1 tunnel local 202.168.1.2
# remote 0 ap 1 tunnel remote 202.168.1.1
# remote 0 ap 1 ipsec type ike
# remote 0 ap 1 ipsec ike protocol esp
# remote 0 ap 1 ipsec ike encrypt des-cbc
# remote 0 ap 1 ipsec ike auth hmac-md5
# remote 0 ap 1 ike mode main
# remote 0 ap 1 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 1 ike proposal encrypt des-cbc

バックアップ回線（ISDN）を設定する
# wan 1 line isdn
# wan 1 bind 1
# remote 1 name shi-back
# remote 1 autodial enable
# remote 1 ip address local 202.168.1.2
# remote 1 ip route 0 202.168.1.1/32 1
# remote 1 ap 0 name shi-back
# remote 1 ap 0 datalink bind wan 1
# remote 1 ap 0 dial 0 number 123-4567-890
# remote 1 ap 0 ppp auth send userid userpass
# remote 1 ap 0 keep connect

設定終了
# save

再起動
# reset
```

2.13.11 テンプレート着信機能（AAA 認証）を使用した固定 IP アドレスでの VPN

適用機種　全機種

IPsec 機能とテンプレート機能を使って、自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社（PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.1.66/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65

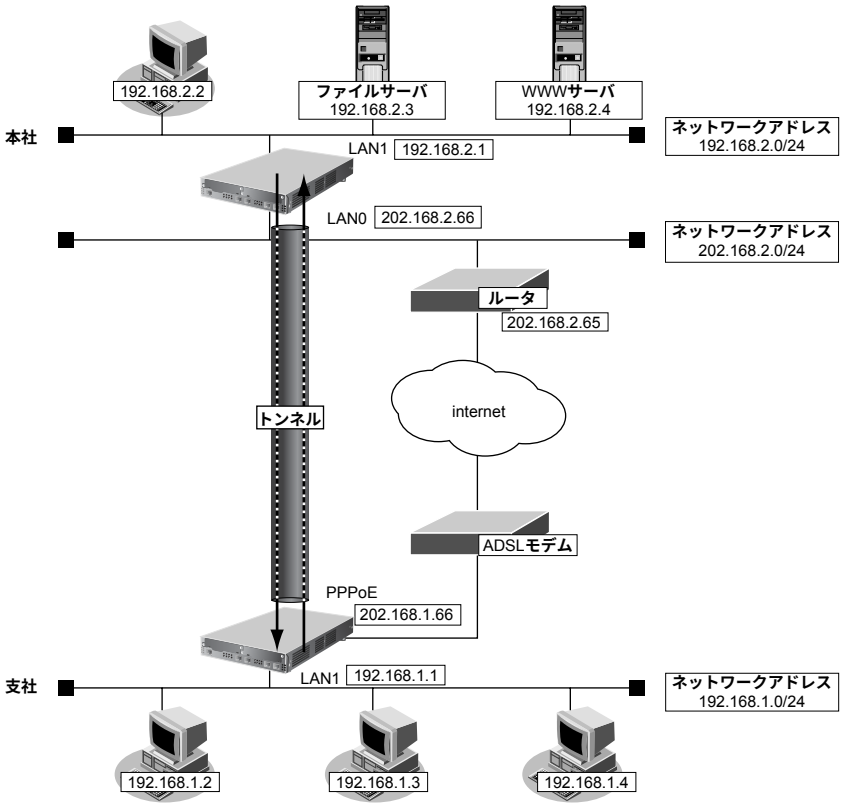
● 設定コマンド

[支社（PPPoE 常時接続)]

```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 1 ip address 192.168.2.1/24 3
```



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：202.168.1.66 － 202.168.2.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[本社]

- テンプレート名　：vpn-shi
- IPsec/IKE 区間　：202.168.2.66 － 202.168.1.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Main Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

こんな事に気をつけて

- テンプレート着信機能（AAA 認証）を使用した IPsec では、AAA 設定のユーザ ID とユーザ認証パスワードを同じに設定してください。
- ユーザ ID とユーザ認証パスワードは、テンプレート情報の IKE 情報の交換モードにより以下のように設定します。
  Main Mode の場合　：相手側 IPsec トンネルアドレス
  Aggressive Mode の場合 ：相手側の装置識別情報
- テンプレート着信側から IKE ネゴシエーションを行う場合、認証しないため、
  template ipsec ike newsa responder off 0 の設定を推奨します。

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

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。

支社を設定する（Initiator）

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 0

設定終了
# save
# reset
```

本社を設定する（Responder）

● コマンド

VPN（テンプレート）を設定する
template 0 name vpn-shi
template 0 combine use aaa
template 0 datalink type ipsec
template 0 interface pool 1 1
template 0 aaa 0
template 0 ipsec ike protocol esp
template 0 ipsec ike encrypt des-cbc
template 0 ipsec ike auth hmac-md5
template 0 ipsec ike pfs off
template 0 ipsec ike lifetime 8h
template 0 ipsec ike lifebyte 0
template 0 ipsec ike newsa initiator 90s 0
template 0 ipsec ike newsa responder off 0
template 0 ike mode main
template 0 ike proposal 0 encrypt des-cbc
template 0 ike proposal 0 hash hmac-md5
template 0 ike proposal 0 pfs modp768
template 0 ike proposal 0 lifetime 1d
template 0 ike retry 10s 3
template 0 ike release on
template 0 tunnel local 202.168.2.66

AAA 情報を設定する
aaa 0 name shisya
aaa 0 user 0 id 202.168.1.66
aaa 0 user 0 password 202.168.1.66
aaa 0 user 0 ipsec ike range any4 any4
aaa 0 user 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
aaa 0 user 0 ip route 0 192.168.1.0/24 1 1

設定終了
save
reset

2.13.12 テンプレート着信機能（AAA 認証）を使用した可変 IP アドレスでの VPN

適用機種　全機種

IPsec 機能とテンプレート機能を使って、自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社（PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65

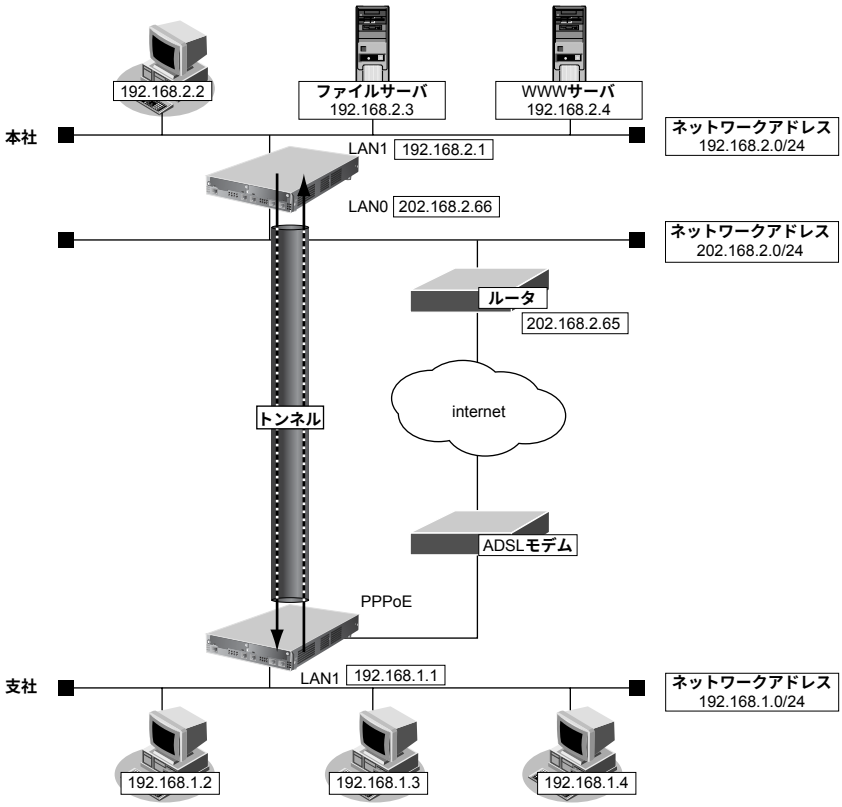
● 設定コマンド

[支社（PPPoE 常時接続)]

```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 1 ip address 192.168.2.1/24 3
```



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：支社 ー 202.168.2.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[本社]

- テンプレート名　：vpn-shi
- IPsec/IKE 区間　：202.168.2.66 ー 支社
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Aggressive Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 支社 ID ／ ID タイプ　：shisya（自装置名）／ FQDN
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

こんな事に気をつけて

- テンプレート着信機能（AAA 認証）を使用した IPsec では、AAA 設定のユーザ ID とユーザ認証パスワードを同じに設定してください。
- ユーザ ID とユーザ認証パスワードは、テンプレート情報の IKE 情報の交換モードにより以下のように設定します。
  Main Mode の場合　　：相手側 IPsec トンネルアドレス
  Aggressive Mode の場合 ：相手側の装置識別情報
- テンプレート着信側から IKE ネゴシエーションを行う場合、認証しないため、
  template ipsec ike newsa responder off 0 の設定を推奨します。

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは？

Aggressive Mode の場合に、ネゴシエーションで使用する自装置を識別する ID の種別です。相手 VPN 装置の設定に合わせます。

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。

支社を設定する（Initiator）

● コマンド

```
インターネットから IPsec/IKE パケットを受信するように設定する
 # remote 0 ip nat static 0 192.168.1.1 500 any 500 17
 # remote 0 ip nat static 1 192.168.1.1 any any any 50
 # remote 0 ip nat static default reject

VPN を設定する
 # remote 1 name vpn-hon
 # remote 1 ap 0 name honsya
 # remote 1 ap 0 datalink type ipsec
 # remote 1 ap 0 ipsec type ike
 # remote 1 ap 0 ipsec ike protocol esp
 # remote 1 ap 0 ipsec ike range any4 any4
 # remote 1 ap 0 ipsec ike encrypt des-cbc
 # remote 1 ap 0 ipsec ike auth hmac-md5
 # remote 1 ap 0 ipsec ike pfs off
 # remote 1 ap 0 ipsec ike lifetime 8h
 # remote 1 ap 0 ipsec ike lifebyte 0
 # remote 1 ap 0 ipsec ike newsa initiator 90s 0
 # remote 1 ap 0 ipsec ike newsa responder 30s 0
 # remote 1 ap 0 ike mode aggressive
 # remote 1 ap 0 ike bind self
 # remote 1 ap 0 ike idtype fqdn
 # remote 1 ap 0 ike name local shisya
 # remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
 # remote 1 ap 0 ike proposal 0 encrypt des-cbc
 # remote 1 ap 0 ike proposal 0 hash hmac-md5
 # remote 1 ap 0 ike proposal 0 pfs modp768
 # remote 1 ap 0 ike proposal 0 lifetime 1d
 # remote 1 ap 0 ike retry 10s 3
 # remote 1 ap 0 ike release on
 # remote 1 ap 0 ike initial forward
 # remote 1 ap 0 tunnel remote 202.168.2.66
 # remote 1 ip route 0 192.168.2.0/24 1 0

設定終了
 # save
 # reset
```

本社を設定する（Responder）

● コマンド

VPN（テンプレート）を設定する
```
# template 0 name vpn-hon
# template 0 combine use aaa
# template 0 datalink type ipsec
# template 0 interface pool 1 1
# template 0 aaa 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt des-cbc
# template 0 ipsec ike auth hmac-md5
# template 0 ipsec ike pfs off
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ipsec ike newsa initiator 90s 0
# template 0 ipsec ike newsa responder off 0
# template 0 ike mode aggressive
# template 0 ike idtype fqdn
# template 0 ike proposal 0 encrypt des-cbc
# template 0 ike proposal 0 hash hmac-md5
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 ike release on
# template 0 tunnel local 202.168.2.66
```

AAA 情報を設定する
```
# aaa 0 name shisya
# aaa 0 user 0 id shisya
# aaa 0 user 0 password shisya
# aaa 0 user 0 ipsec ike range any4 any4
# aaa 0 user 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# aaa 0 user 0 ip route 0 192.168.1.0/24 1 1
```

設定終了
```
# save
# reset
```

2.13.13 テンプレート着信機能（RADIUS 認証）を使用した固定 IP アドレスでの VPN

適用機種　全機種

IPsec 機能とテンプレート機能を使って、自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社（PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.1.66/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス　：202.168.2.65

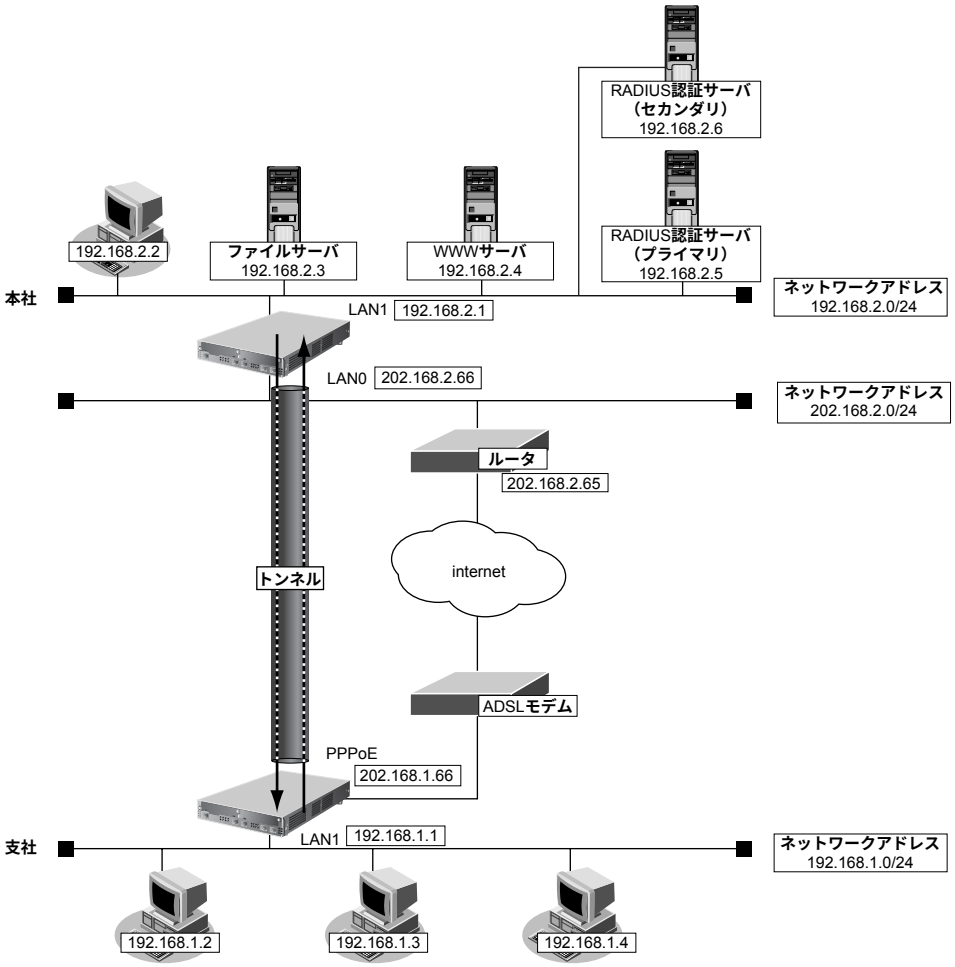
● 設定コマンド

[支社（PPPoE 常時接続)]

```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 1 ip address 192.168.2.1/24 3
```



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：202.168.1.66 － 202.168.2.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[本社]

- テンプレート名　：vpn-shi
- IPsec/IKE 区間　：202.168.2.66 － 202.168.1.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- RADIUS サービス　：クライアント機能
  ：認証、アカウンティング
- 自側認証 IP アドレス　：192.168.2.1
- 自側アカウンティング IP アドレス　：192.168.2.1
- 認証情報 1（プライマリ）
  共有鍵　：192.168.2.1
  サーバ IP アドレス　：192.168.2.5
  復旧待機時間　：30 分
  優先度　：0

- 認証情報２（セカンダリ）
  共有鍵　：192.168.2.1
  サーバ IP アドレス　：192.168.2.6
  復旧待機時間　：30 分
  優先度　：100
- アカウンティング情報１（プライマリ）
  共有鍵　：192.168.2.1
  サーバ IP アドレス　：192.168.2.5
  復旧待機時間　：30 分
  優先度　：0
- アカウンティング情報２（セカンダリ）
  共有鍵　：192.168.2.1
  サーバ IP アドレス　：192.168.2.6
  復旧待機時間　：30 分
  優先度　：100

[共通]

- 鍵交換タイプ　：Main Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

こんな事に気をつけて

- **テンプレート着信機能（RADIUS 認証）を使用した IPsec では、RADIUS 認証サーバ側のユーザ ID とユーザ認証パスワードを同じに設定してください。**
- **ユーザ ID とユーザ認証パスワードは、テンプレート情報の IKE 情報の交換モードにより以下のように設定します。**
  Main Mode の場合　：相手側 IPsec トンネルアドレス
  Aggressive Mode の場合　：相手側の装置識別情報
- **テンプレート着信側から IKE ネゴシエーションを行う場合、認証しないため、**
  template ipsec ike newsa responder off 0 の設定を推奨します。

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

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。

支社を設定する（Initiator）

● コマンド

```
VPNを設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 0

設定終了
# save
# reset
```

本社を設定する（Responder）

● コマンド

VPN（テンプレート）を設定する
template 0 name vpn-shi
template 0 combine use aaa
template 0 datalink type ipsec
template 0 interface pool 1 1
template 0 aaa 0
template 0 ipsec ike protocol esp
template 0 ipsec ike encrypt des-cbc
template 0 ipsec ike auth hmac-md5
template 0 ipsec ike pfs off
template 0 ipsec ike lifetime 8h
template 0 ipsec ike lifebyte 0
template 0 ipsec ike newsa initiator 90s 0
template 0 ipsec ike newsa responder off 0
template 0 ike mode main
template 0 ike proposal 0 encrypt des-cbc
template 0 ike proposal 0 hash hmac-md5
template 0 ike proposal 0 pfs modp768
template 0 ike proposal 0 lifetime 1d
template 0 ike retry 10s 3
template 0 ike release on
template 0 tunnel local 202.168.2.66

AAA 情報を設定する
aaa 0 name shisya

RADIUS クライアントに関する情報を設定する
aaa 0 radius service client both
aaa 0 radius auth source 192.168.2.1
aaa 0 radius accounting source 192.168.2.1
aaa 0 radius client server-info auth 0 secret 192.168.2.1
aaa 0 radius client server-info auth 0 address 192.168.2.5
aaa 0 radius client server-info auth 0 deadtime 30m
aaa 0 radius client server-info auth 0 priority 0
aaa 0 radius client server-info auth 1 secret 192.168.2.1
aaa 0 radius client server-info auth 1 address 192.168.2.6
aaa 0 radius client server-info auth 1 deadtime 30m
aaa 0 radius client server-info auth 1 priority 100
aaa 0 radius client server-info accounting 0 secret 192.168.2.1
aaa 0 radius client server-info accounting 0 address 192.168.2.5
aaa 0 radius client server-info accounting 0 deadtime 30m
aaa 0 radius client server-info accounting 0 priority 0
aaa 0 radius client server-info accounting 1 secret 192.168.2.1
aaa 0 radius client server-info accounting 1 address 192.168.2.6
aaa 0 radius client server-info accounting 1 deadtime 30m
aaa 0 radius client server-info accounting 1 priority 100

設定終了
save
reset

2.13.14 テンプレート着信機能（RADIUS 認証）を使用した可変 IP アドレスでの VPN

適用機種　全機種

IPsec 機能とテンプレート機能を使って、自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社（PPPoE 常時接続）]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65

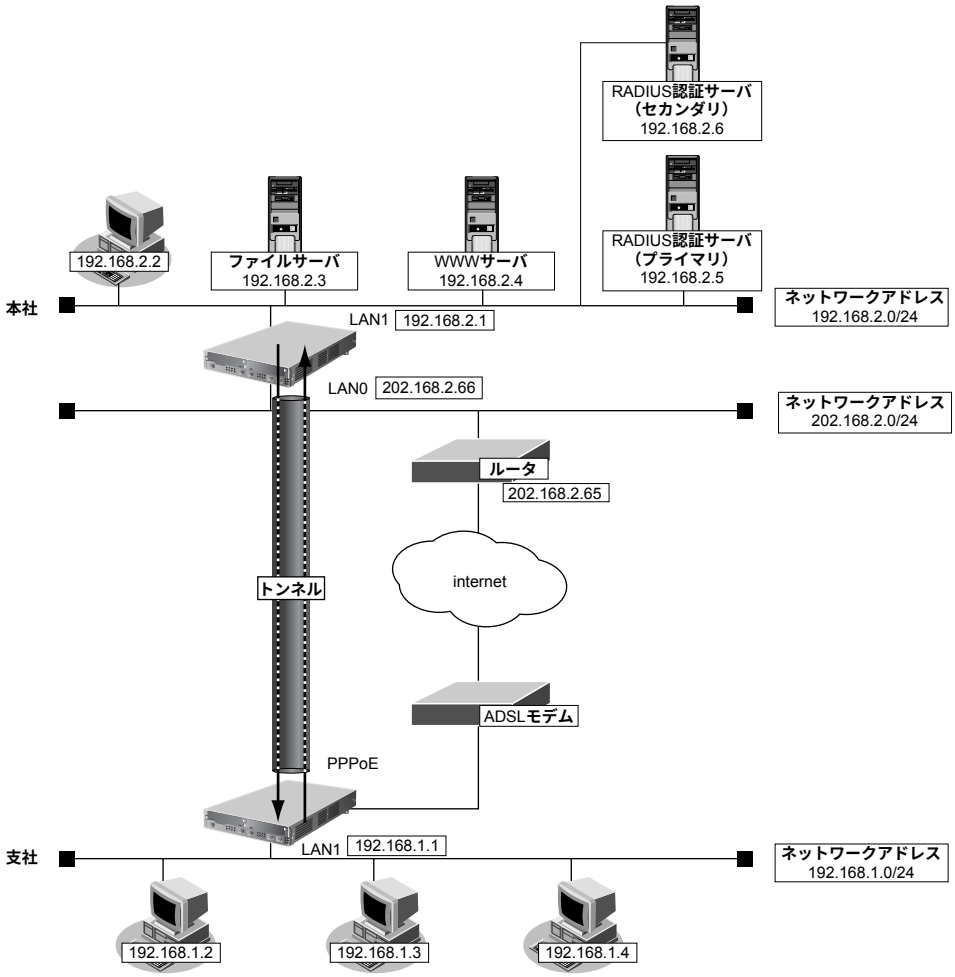
● 設定コマンド

[支社（PPPoE 常時接続）]

```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 1 ip address 192.168.2.1/24 3
```



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：支社 － 202.168.2.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[本社]

- テンプレート名　：vpn-shi
- IPsec/IKE 区間　：202.168.2.66 － 支社
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- RADIUS サービス　：クライアント機能
  ：認証、アカウンティング
- 自側認証 IP アドレス　：192.168.2.1
- 自側アカウンティング IP アドレス　：192.168.2.1
- 認証情報 1（プライマリ）
  共有鍵　：192.168.2.1
  サーバ IP アドレス　：192.168.2.5
  復旧待機時間　：30 分
  優先度　：0

- 認証情報２（セカンダリ）
  共有鍵　：192.168.2.1
  サーバ IP アドレス　：192.168.2.6
  復旧待機時間　：30 分
  優先度　：100
- アカウンティング情報１（プライマリ）
  共有鍵　：192.168.2.1
  サーバ IP アドレス　：192.168.2.5
  復旧待機時間　：30 分
  優先度　：0
- アカウンティング情報２（セカンダリ）
  共有鍵　：192.168.2.1
  サーバ IP アドレス　：192.168.2.6
  復旧待機時間　：30 分
  優先度　：100

[共通]

- 鍵交換タイプ　：Aggressive Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 支社 ID ／ ID タイプ　：shisya（自装置名）／ FQDN
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

こんな事に気をつけて

- **テンプレート着信機能（RADIUS 認証）を使用した IPsec では、RADIUS 認証サーバ側のユーザ ID とユーザ認証パスワードを同じに設定してください。**
- **ユーザ ID とユーザ認証パスワードは、テンプレート情報の IKE 情報の交換モードにより以下のように設定します。**
  Main Mode の場合　：相手側 IPsec トンネルアドレス
  Aggressive Mode の場合　：相手側の装置識別情報
- **テンプレート着信側から IKE ネゴシエーションを行う場合、認証しないため、**
  template ipsec ike newsa responder off 0 の設定を推奨します。

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは？

Aggressive Mode の場合に、ネゴシエーションで使用する自装置を識別する ID の種別です。相手 VPN 装置の設定に合わせます。

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。

支社を設定する（Initiator）

● コマンド

```
インターネットから IPsec/IKE パケットを受信するように設定する
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50
# remote 0 ip nat static default reject

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike idtype fqdn
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 0

設定終了
# save
# reset
```

本社を設定する（Responder）

● コマンド

VPN（テンプレート）を設定する
template 0 name vpn-hon
template 0 combine use aaa
template 0 datalink type ipsec
template 0 interface pool 1 1
template 0 aaa 0
template 0 ipsec ike protocol esp
template 0 ipsec ike encrypt des-cbc
template 0 ipsec ike auth hmac-md5
template 0 ipsec ike pfs off
template 0 ipsec ike lifetime 8h
template 0 ipsec ike lifebyte 0
template 0 ipsec ike newsa initiator 90s 0
template 0 ipsec ike newsa responder off 0
template 0 ike mode aggressive
template 0 ike idtype fqdn
template 0 ike proposal 0 encrypt des-cbc
template 0 ike proposal 0 hash hmac-md5
template 0 ike proposal 0 pfs modp768
template 0 ike proposal 0 lifetime 1d
template 0 ike retry 10s 3
template 0 ike release on
template 0 tunnel local 202.168.2.66

AAA 情報を設定する
aaa 0 name shisya

RADIUS クライアントに関する情報を設定する
aaa 0 radius service client both
aaa 0 radius auth source 192.168.2.1
aaa 0 radius accounting source 192.168.2.1
aaa 0 radius client server-info auth 0 secret 192.168.2.1
aaa 0 radius client server-info auth 0 address 192.168.2.5
aaa 0 radius client server-info auth 0 deadtime 30m
aaa 0 radius client server-info auth 0 priority 0
aaa 0 radius client server-info auth 1 secret 192.168.2.1
aaa 0 radius client server-info auth 1 address 192.168.2.6
aaa 0 radius client server-info auth 1 deadtime 30m
aaa 0 radius client server-info auth 1 priority 100
aaa 0 radius client server-info accounting 0 secret 192.168.2.1
aaa 0 radius client server-info accounting 0 address 192.168.2.5
aaa 0 radius client server-info accounting 0 deadtime 30m
aaa 0 radius client server-info accounting 0 priority 0
aaa 0 radius client server-info accounting 1 secret 192.168.2.1
aaa 0 radius client server-info accounting 1 address 192.168.2.6
aaa 0 radius client server-info accounting 1 deadtime 30m
aaa 0 radius client server-info accounting 1 priority 100

設定終了
save
reset

2.13.15 テンプレート着信機能（動的VPN）を使用した IPv4 over IPv4で固定IPアドレスでのVPN

適用機種　全機種

IPsec機能、動的VPN情報交換機能およびテンプレート機能を使って、自動鍵交換でVPNを構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社A（PPPoE常時接続）]

- ローカルネットワークIPv4アドレス　：192.168.1.1/24
- PPPoEユーザ認証ID　：userid1（プロバイダから提示された内容）
- PPPoEユーザ認証パスワード　：userpass1（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用
- NAT機能　：マルチNATを使用する
- ネットワーク名　：internet
- 接続先名　：ISP-1

[支社B（PPPoE常時接続）]

- ローカルネットワークIPv4アドレス　：192.168.2.1/24
- PPPoEユーザ認証ID　：userid2（プロバイダから提示された内容）
- PPPoEユーザ認証パスワード　：userpass2（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用
- NAT機能　：マルチNATを使用する
- ネットワーク名　：internet
- 接続先名　：ISP-1

[本社]

- ローカルネットワークIPv4アドレス　：192.168.0.1/24
- インターネットプロバイダから割り当てられた固定IPv4アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートのIPv4アドレス　：202.168.2.65

● 設定コマンド

[支社A（PPPoE常時接続）]

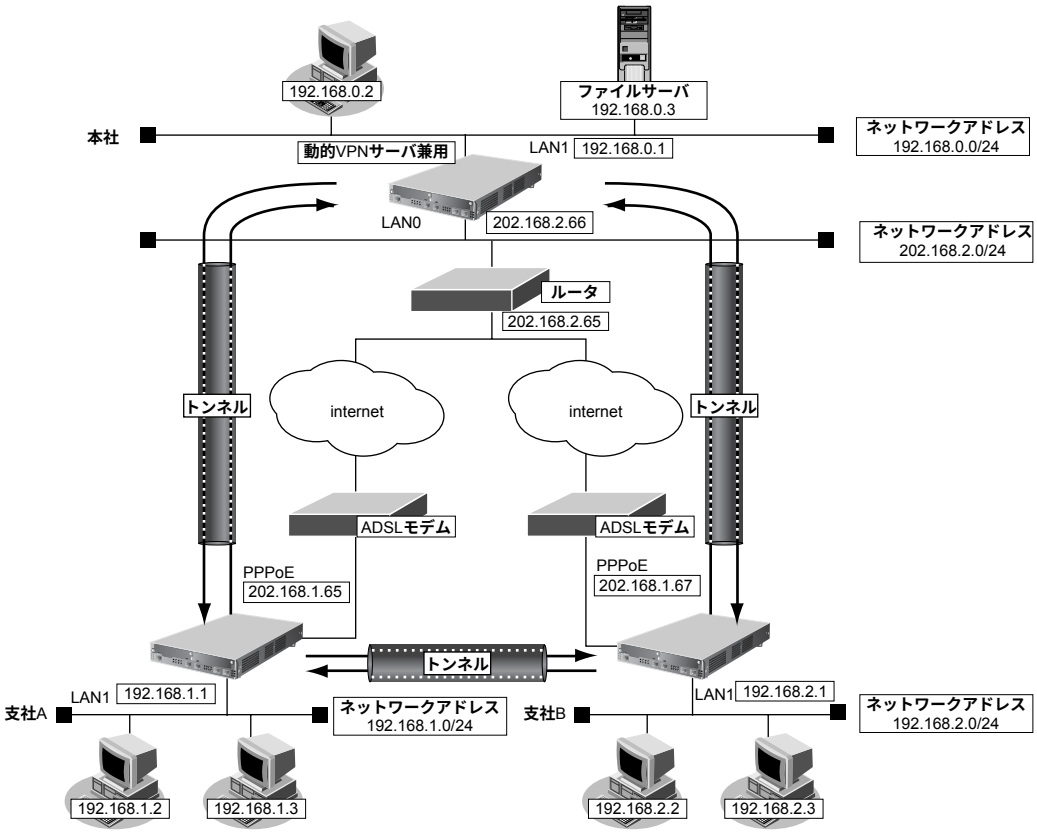
```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid1 userpass1
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

[支社 B（PPPoE 常時接続）]

```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.2.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid2 userpass2
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 1 ip address 192.168.0.1/24 3
```



● 設定条件（VPN 接続）

[支社 A（Initiator)]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：支社 A － 202.168.2.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- IKE（UDP：500 番ポート）のプライベートアドレス
  ：192.168.1.1
- ESP のプライベートアドレス　：192.168.1.1

- テンプレート名　：vpn-shiB
- IPsec/IKE 始点　：インターネットプロバイダから割り当てられた IPv4 アドレスを使用する
- 接続先監視アドレス　：192.168.1.1

[支社 B（Initiator)]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：支社 B ー 202.168.2.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- IKE（UDP：500 番ポート）のプライベートアドレス
  ：192.168.2.1
- ESP のプライベートアドレス　：192.168.2.1
- テンプレート名　：vpn-shiA
- IPsec/IKE 始点　:インターネットプロバイダから割り当てられた IPv4 アドレス を使用する
- 接続先監視アドレス　：192.168.2.1

[本社（Responder)]

- ネットワーク名　：vpn-shiA
- 接続先名　：shisyaA
- IPsec/IKE 区間　：202.168.2.66 ー 支社 A
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- ネットワーク名　：vpn-shiB
- 接続先名　：shisyaB
- IPsec/IKE 区間　：202.168.2.66 ー 支社 B
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通（本社 - 支社 A、B)]

- 鍵交換タイプ　：Aggressive Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 支社 A ID/ID タイプ　：shisyaA（自装置識別情報）/FQDN
- IKE 支社 B ID/ID タイプ　：shisyaB（自装置識別情報）/FQDN
- IKE 支社 A IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890
- IKE 支社 B IKE 認証鍵　：1234567890abcdefghijklmnopqrstuvwxyz
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

● 設定条件（動的VPN接続）

[支社A]

- クライアント情報　：0
- サーバ情報
  アドレス　：192.168.0.1
  ポート番号　：5070
  認証ID　：shisyaAid
  認証パスワード　：shisyaApass
- 有効期間　：1時間
- セッション更新間隔　：5分
- クライアントIPアドレス　：192.168.1.1
- ドメイン名　：example.com
- VPN通信
  利用インタフェース　：rmt0
- 動的VPNクライアントの優先度　：10
- 動的VPN IPv4経路情報の優先度　：1

[支社B]

- クライアント情報　：0
- サーバ情報
  アドレス　：192.168.0.1
  ポート番号　：5070
  認証ID　：shisyaBid
  認証パスワード　：shisyaBpass
- 有効期間　：1時間
- セッション更新間隔　：5分
- クライアントIPアドレス　：192.168.2.1
- ドメイン名　：example.com
- VPN通信
  利用インタフェース　：rmt0
- 動的VPNクライアントの優先度　：10
- 動的VPN IPv4経路情報の優先度　：1

[本社]

- サーバ機能　：使用する
  ドメイン名　：example.com
  認証　：行う
  AAAグループID　：0
- AAAユーザ情報（支社A認証情報）
  ユーザID　：shisyaAid
  認証パスワード　：shisyaApass
- AAAユーザ情報（支社B認証情報）
  ユーザID　：shisyaBid
  認証パスワード　：shisyaBpass

[共通（支社 A-支社 B)]

- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：aes-cbc-128
- IPsec 認証アルゴリズム　：hmac-sha1
- IPsec DH グループ　：modp768
- IKE 認証鍵　：ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：aes-cbc-128
- IKE 認証アルゴリズム　：hmac-sha1
- IKE DH グループ　：modp768

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは？

Aggressive Mode **の場合に、ネゴシエーションで使用する自装置を識別する** ID **の種別です。相手** VPN **装置の設定に合わせます。**

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。

支社 A を設定する（Initiator）

● コマンド

```
インターネットから IPsec/IKE パケットを受信するように設定する
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50
# remote 0 ip nat static default reject

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike name local shisyaA
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
```

```
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.0.0/24 1 0
# remote 1 ip route 1 192.168.2.0/24 1 2
# remote 1 ip dvpn 0 invite acl 0 24 0
# acl 0 ip 192.168.1.0/24 192.168.2.0/24 any any

動的VPN情報を定義する
# dvpn client 0 server 0 address 192.168.0.1 5070
# dvpn client 0 server 0 auth shisyaAid shisyaApass
# dvpn client 0 expire register 1h
# dvpn client 0 expire session 5m
# dvpn client 0 ua 192.168.1.1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 192.168.1.0/24 on
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip route distance 1

テンプレート情報を設定する
# template 0 name vpn-shiB
# template 0 mtu 1500
# template 0 idle 0d
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 tunnel local 192.168.1.1
# template 0 sessionwatch address 192.168.1.1

設定終了
# save
# reset
```

支社 B を設定する（Initiator）

● コマンド

インターネットから IPsec/IKE パケットを受信するように設定する
```
# remote 0 ip nat static 0 192.168.2.1 500 any 500 17
# remote 0 ip nat static 1 192.168.2.1 any any any 50
# remote 0 ip nat static default reject
```

VPN を設定する
```
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike name local shisyaB
# remote 1 ap 0 ike shared key text 1234567890abcdefghijklmnopqrstuvwxyz
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.0.0/24 1 0
# remote 1 ip route 1 192.168.1.0/24 1 2
# remote 1 ip dvpn 0 invite acl 0 24 0
# acl 0 ip 192.168.2.0/24 192.168.1.0/24 any any
```

動的 VPN 情報を設定する
```
# dvpn client 0 server 0 address 192.168.0.1 5070
# dvpn client 0 server 0 auth shisyaBid shisyaBpass
# dvpn client 0 expire register 1h
# dvpn client 0 expire session 5m
# dvpn client 0 ua 192.168.2.1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 192.168.2.0/24 on
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip route distance 1
```

テンプレート情報を設定する
```
# template 0 name vpn-shiA
# template 0 mtu 1500
# template 0 idle 0d
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
```

```
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 tunnel local 192.168.2.1
# template 0 sessionwatch address 192.168.2.1

設定終了
# save
# reset
```

本社を設定する（Responder）

● コマンド

```
VPN を設定する
# remote 0 name vpn-shiA
# remote 0 ap 0 name shisyaA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 any4
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ipsec ike pfs off
# remote 0 ap 0 ipsec ike lifetime 8h
# remote 0 ap 0 ipsec ike lifebyte 0
# remote 0 ap 0 ipsec ike newsa initiator 90s 0
# remote 0 ap 0 ipsec ike newsa responder 30s 0
# remote 0 ap 0 ike mode aggressive
# remote 0 ap 0 ike bind self
# remote 0 ap 0 ike name remote shisyaA
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal 0 encrypt des-cbc
# remote 0 ap 0 ike proposal 0 hash hmac-md5
# remote 0 ap 0 ike proposal 0 pfs modp768
# remote 0 ap 0 ike proposal 0 lifetime 1d
# remote 0 ap 0 ike retry 10s 3
# remote 0 ap 0 ike release on
# remote 0 ap 0 ike initial forward
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ip route 0 192.168.1.0/24 1 0
# remote 1 name vpn-shiB
# remote 1 ap 0 name shisyaB
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
```

```
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike name remote shisyaB
# remote 1 ap 0 ike shared key text 1234567890abcdefghijklmnopqrstuvwxyz
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 0
```

動的VPNサーバを設定する

```
# dvpn server use on
# dvpn server domain example.com
# dvpn server auth use on
# dvpn server auth aaa 0
# aaa name dvpnserver
# aaa user 0 id shisyaAid
# aaa user 0 password shisyaApass
# aaa user 1 id shisyaBid
# aaa user 1 password shisyaBpass
```

設定終了

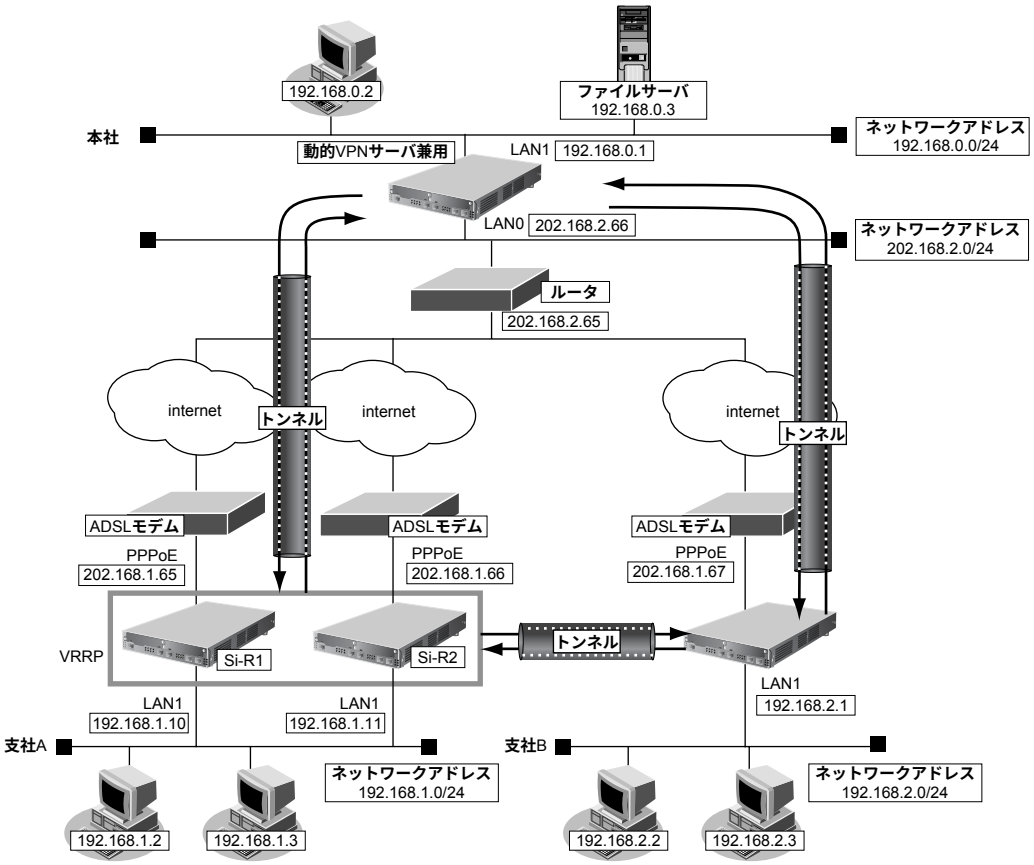
```
# save
# reset
```

2.13.16 テンプレート着信機能（動的VPN）を使用した IPv4 over IPv4で固定IPアドレスでのVPN（冗長構成）

適用機種　全機種

IPsec機能、動的VPN情報交換機能およびテンプレート機能を使って、自動鍵交換でVPNを冗長構成で構築する場合の設定方法を説明します。

ここでは「2.13.15 テンプレート着信機能（動的VPN）を使用したIPv4 over IPv4で固定IPアドレスでのVPN」（P.238）で説明したネットワーク構成で、支社と本社が動的VPNによって接続されていることを前提とします。ただし、支社AはVRRPによる冗長構成の設定を行います。



● 設定コマンド

[支社A（Si-R1）]

「2.13.15 テンプレート着信機能（動的VPN）を使用したIPv4 over IPv4で固定IPアドレスでのVPN」（P.238）で説明した支社Aの設定を事前に行います。

[支社A（Si-R2）]

「2.13.15 テンプレート着信機能（動的VPN）を使用したIPv4 over IPv4で固定IPアドレスでのVPN」（P.238）で説明した支社Aの設定を事前に行います。

● 設定条件（冗長構成）

[支社 A（Si-R1)]

- ローカルネットワーク IPv4 アドレス　：192.168.1.10/24
- VRRP 優先度　：254
- 動的 VPN クライアントの優先度　：1
- ノードダウントリガ　：202.168.2.66

[支社 A（Si-R2)]

- ローカルネットワーク IPv4 アドレス　：192.168.1.11/24
- VRRP 優先度　：100
- 動的 VPN クライアントの優先度　：2

[支社 A（共通)]

- VRRP 仮想 IP アドレス　：192.168.1.1/24
- VRRP グループ ID　：10
- OSPF エリア ID　：0.0.0.0

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。

支社 A を設定する（Si-R1）

● コマンド

```
# lan 1 ip address 192.168.1.10/24 3
# remote 0 ip nat static 0 192.168.1.10 500 any 500 17
# remote 0 ip nat static 1 192.168.1.10 any any any 50
# remote 1 ip route 1 192.168.2.0/24 1 200

VRRP を設定する
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 10 254 192.168.1.1
# lan 1 vrrp group 0 preempt off
# lan 1 vrrp group 0 trigger 0 node 202.168.2.66 any

OSPF を設定する
# lan 1 ip ospf use on 0
# routemanage ip redist ospf static on 20 type2
# ospf ip area 0 id 0.0.0.0

動的 VPN を設定する
# template 0 tunnel local 192.168.1.10
# template 0 sessionwatch address 192.168.1.10
# dvpn client 0 ua 192.168.1.10
# dvpn client priority 1

設定終了
# save
# reset
```

支社 A を設定する（Si-R2）

● コマンド

```
# lan 1 ip address 192.168.1.11/24 3
# remote 0 ip nat static 0 192.168.1.11 500 any 500 17
# remote 0 ip nat static 1 192.168.1.11 any any any 50
# remote 1 ip route 1 192.168.2.0/24 1 200

VRRP を設定する
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 10 100 192.168.1.1
# lan 1 vrrp group 0 preempt off

OSPF を設定する
# lan 1 ip ospf use on 0
# routemanage ip redist ospf static on 20 type2
# ospf ip area 0 id 0.0.0.0

動的 VPN を設定する
# template 0 tunnel local 192.168.1.11
# template 0 sessionwatch address 192.168.1.11
# dvpn client 0 ua 192.168.1.11
# dvpn client priority 2

設定終了
# save
# reset
```

本社を設定する

● コマンド

```
# remote 0 ip route 0 192.168.1.0/24 1 10
# remote 2 name vpn-shia
# remote 2 ap 0 name shisyaa
# remote 2 ap 0 datalink type ipsec
# remote 2 ap 0 ipsec type ike
# remote 2 ap 0 ipsec ike protocol esp
# remote 2 ap 0 ipsec ike encrypt des-cbc
# remote 2 ap 0 ipsec ike auth hmac-md5
# remote 2 ap 0 ike mode aggressive
# remote 2 ap 0 ike name remote shisyaa
# remote 2 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 2 ap 0 ike proposal 0 encrypt des-cbc
# remote 2 ap 0 tunnel local 202.168.2.66
# remote 2 ip route 0 192.168.1.0/24 1 254

設定終了
# save
# reset
```

2.13.17 テンプレート着信機能（動的VPN）を使用した IPv6 over IPv6で固定IPアドレスでのVPN

適用機種　全機種

IPsec機能、動的VPN情報交換機能およびテンプレート機能を使って、自動鍵交換でVPNを構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社A（PPPoE常時接続）]

- ローカルネットワークIPv4アドレス　：192.168.1.1/24
- ローカルネットワークIPv6アドレス　：2001:db8:1111:3::1/64
- インターネットプロバイダから割り当てられた固定IPv4アドレス　：202.168.1.66/24
- インターネットプロバイダから割り当てられた固定IPv6アドレス　：2001:db8:1111:1::66/64
- PPPoEユーザ認証ID　：userid1（プロバイダから提示された内容）
- PPPoEユーザ認証パスワード　：userpass1（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用

[支社B（PPPoE常時接続）]

- ローカルネットワークIPv4アドレス　：192.168.2.1/24
- ローカルネットワークIPv6アドレス　：2001:db8:1111:5::1/64
- インターネットプロバイダから割り当てられた固定IPv4アドレス　：202.168.1.67/24
- インターネットプロバイダから割り当てられた固定IPv6アドレス　：2001:db8:1111:1::67/64
- PPPoEユーザ認証ID　：userid2（プロバイダから提示された内容）
- PPPoEユーザ認証パスワード　：userpass2（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用

[本社]

- ローカルネットワークIPv4アドレス　：192.168.0.1/24
- ローカルネットワークIPv6アドレス　：2001:db8:1111:4::1/64
- インターネットプロバイダから割り当てられた固定IPv4アドレス　：202.168.2.66/24
- インターネットプロバイダから割り当てられた固定IPv6アドレス　：2001:db8:1111:2::66/64
- インターネットプロバイダから指定されたデフォルトルートのIPv4アドレス　：202.168.2.65
- インターネットプロバイダから指定されたデフォルトルートのIPv6アドレス　：2001:db8:1111:2::65

● 設定コマンド

[支社 A（PPPoE 常時接続）]

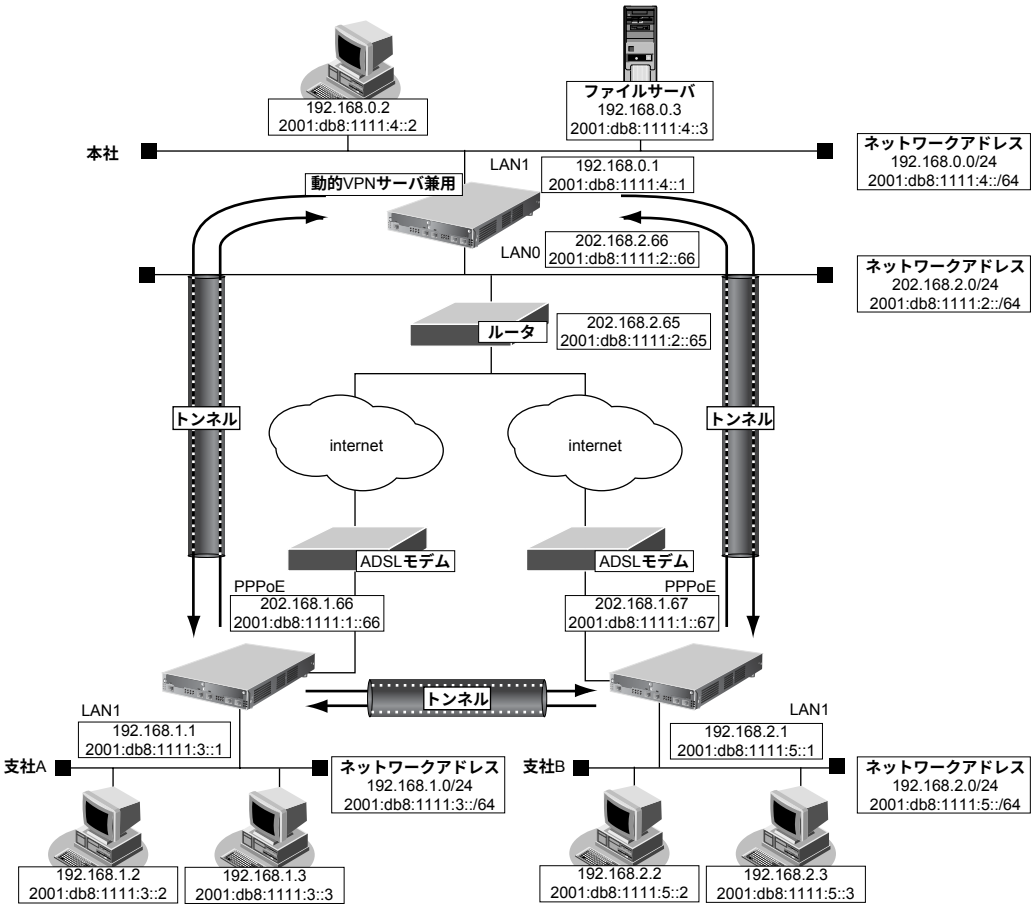
```
# delete lan
# lan 0 mode auto
# lan 0 ip6 use on
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip6 use on
# lan 1 ip6 address 0 2001:db8:1111:3::1/64 infinity infinity c0
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid1 userpass1
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
# remote 0 ip6 use on
# remote 0 ip6 address 0 2001:db8:1111:1::66/64 infinity infinity c0
# remote 0 ip6 route 0 default 1 0
```

[支社 B（PPPoE 常時接続）]

```
# delete lan
# lan 0 mode auto
# lan 0 ip6 use on
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ip6 use on
# lan 1 ip6 address 0 2001:db8:1111:5::1/64 infinity infinity c0
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid2 userpass2
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
# remote 0 ip6 use on
# remote 0 ip6 address 0 2001:db8:1111:1::67/64 infinity infinity c0
# remote 0 ip6 route 0 default 1 0
```

[本社]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 0 ip6 use on
# lan 0 ip6 address 0 2001:db8:1111:2::66/64 infinity infinity c0
# lan 0 ip6 route 0 default 2001:db8:1111:2::65 1 0
# lan 1 ip address 192.168.0.1/24 3
# lan 1 ip6 use on
# lan 1 ip6 address 0 2001:db8:1111:4::1/64 infinity infinity c0
```



● 設定条件（VPN 接続）

[支社 A]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：2001:db8:1111:1::66 － 2001:db8:1111:2::66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- テンプレート名　：vpn-shiB
- IPsec/IKE 始点　：インターネットプロバイダから割り当てられた固定 IPv6 アドレスを使用する
- 接続先監視アドレス　：2001:db8:1111:3::1

[支社 B]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：2001:db8:1111:1::67 － 2001:db8:1111:2::66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- テンプレート名　：vpn-shiA
- IPsec/IKE 始点　：インターネットプロバイダから割り当てられた固定 IPv6 アドレスを使用する
- 接続先監視アドレス　：2001:db8:1111:5::1

[本社]

- ネットワーク名　：vpn-shiA
- 接続先名　：shisyaA
- IPsec/IKE 区間　：2001:db8:1111:2::66 － 2001:db8:1111:1::66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- ネットワーク名　：vpn-shiB
- 接続先名　：shisyaB
- IPsec/IKE 区間　：2001:db8:1111:2::66 － 2001:db8:1111:1::67
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通（本社 - 支社 A、B)]

- 鍵交換タイプ　：Main Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 支社 A IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890
- IKE 支社 B IKE 認証鍵　：1234567890abcdefghijklmnopqrstuvwxyz
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

● 設定条件（動的 VPN 接続）

[支社 A]

- クライアント情報　：0
- サーバ情報
  アドレス　：2001:db8:1111:4::1
  ポート番号　：5070
  認証 ID　：shisyaAid
  認証パスワード　：shisyaApass
- 有効期間　：1 時間
- セッション更新間隔　：5 分
- クライアント IP アドレス　：2001:db8:1111:3::1
- ドメイン名　：example.com
- VPN 通信
  利用インタフェース　：rmt0
- 動的 VPN クライアントの優先度　：10
- 動的 VPN IPv6 経路情報の優先度　：1

[支社 B]

- クライアント情報　：0
- サーバ情報
  アドレス　：2001:db8:1111:4::1
  ポート番号　：5070
  認証 ID　：shisyaBid
  認証パスワード　：shisyaBpass
- 有効期間　：1 時間
- セッション更新間隔　：5 分
- クライアント IP アドレス　：2001:db8:1111:5::1
- ドメイン名　：example.com
- VPN 通信
  利用インタフェース　：rmt0
- 動的 VPN クライアントの優先度　：10
- 動的 VPN IPv6 経路情報の優先度　：1

[本社]

- サーバ機能　：使用する
  ドメイン名　：example.com
  認証　：行う
  AAA グループ ID　：0
- AAA ユーザ情報（支社 A 認証情報）
  ユーザ ID　：shisyaAid
  認証パスワード　：shisyaApass
- AAA ユーザ情報（支社 B 認証情報）
  ユーザ ID　：shisyaBid
  認証パスワード　：shisyaBpass

[共通（支社 A-支社 B）]

- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：aes-cbc-128
- IPsec 認証アルゴリズム　：hmac-sha1
- IPsec DH グループ　：modp768
- IKE 認証鍵　：ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：aes-cbc-128
- IKE 認証アルゴリズム　：hmac-sha1
- IKE DH グループ　：modp768

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

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。

支社 A を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel local 2001:db8:1111:1::66
# remote 1 ap 0 tunnel remote 2001:db8:1111:2::66
# remote 1 ip6 use on
# remote 1 ip6 route 0 2001:db8:1111:4::/64 1 0
# remote 1 ip6 route 1 2001:db8:1111:5::/64 1 2
# remote 1 ip6 dvpn 0 invite acl 0 64 0
# acl 0 ip6 2001:db8:1111:3::/64 2001:db8:1111:5::/64 any any

動的 VPN 情報を設定する
# dvpn client 0 server 0 address 2001:db8:1111:4::1 5070
# dvpn client 0 server 0 auth shisyaAid shisyaApass
# dvpn client 0 expire register 1h
# dvpn client 0 expire session 5m
# dvpn client 0 ua 2001:db8:1111:3::1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 2001:db8:1111:3::/64
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
```

```
# dvpn client 0 ip6 route distance 1

テンプレート情報を設定する
# template 0 name vpn-shiB
# template 0 mtu 1500
# template 0 idle 0d
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ip6 use on
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 tunnel local 2001:db8:1111:1::66
# template 0 sessionwatch address 2001:db8:1111:3::1

設定終了
# save
# reset
```

支社 B を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike shared key text 1234567890abcdefghijklmnopqrstuvwxyz
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel local 2001:db8:1111:1::67
# remote 1 ap 0 tunnel remote 2001:db8:1111:2::66
# remote 1 ip6 use on
```

```
# remote 1 ip6 route 0 2001:db8:1111:4::/64 1 0
# remote 1 ip6 route 1 2001:db8:1111:3::/64 1 2
# remote 1 ip6 dvpn 0 invite acl 0 64 0
# acl 0 ip6 2001:db8:1111:5::/64 2001:db8:1111:3::/64 any any

動的VPN情報を設定する
# dvpn client 0 server 0 address 2001:db8:1111:4::1 5070
# dvpn client 0 server 0 auth shisyaBid shisyaBpass
# dvpn client 0 expire register 1h
# dvpn client 0 expire session 5m
# dvpn client 0 ua 2001:db8:1111:5::1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 2001:db8:1111:5::/64
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip6 route distance 1

テンプレート情報を設定する
# template 0 name vpn-shiA
# template 0 mtu 1500
# template 0 idle 0d
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ip6 use on
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 tunnel local 2001:db8:1111:1::67
# template 0 sessionwatch address 2001:db8:1111:5::1

設定終了
# save
# reset
```

本社を設定する

● コマンド

```
VPNを設定する
# remote 0 name vpn-shiA
# remote 0 ap 0 name shisyaA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any6 any6
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ipsec ike pfs off
# remote 0 ap 0 ipsec ike lifetime 8h
# remote 0 ap 0 ipsec ike lifebyte 0
```

```
# remote 0 ap 0 ipsec ike newsa initiator 90s 0
# remote 0 ap 0 ipsec ike newsa responder 30s 0
# remote 0 ap 0 ike mode main
# remote 0 ap 0 ike bind self
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal 0 encrypt des-cbc
# remote 0 ap 0 ike proposal 0 hash hmac-md5
# remote 0 ap 0 ike proposal 0 pfs modp768
# remote 0 ap 0 ike proposal 0 lifetime 1d
# remote 0 ap 0 ike retry 10s 3
# remote 0 ap 0 ike release on
# remote 0 ap 0 ike initial forward
# remote 0 ap 0 tunnel local 2001:db8:1111:2::66
# remote 0 ap 0 tunnel remote 2001:db8:1111:1::66
# remote 0 ip6 use on
# remote 0 ip6 route 0 2001:db8:1111:3::/64 1 0
# remote 1 name vpn-shiB
# remote 1 ap 0 name shisyaB
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike shared key text 1234567890abcdefghijklmnopqrstuvwxyz
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel local 2001:db8:1111:2::66
# remote 1 ap 0 tunnel remote 2001:db8:1111:1::67
# remote 1 ip6 use on
# remote 1 ip6 route 0 2001:db8:1111:5::/64 1 0
```

動的VPNサーバを設定する

```
# dvpn server use on
# dvpn server domain example.com
# dvpn server auth use on
# dvpn server auth aaa 0
# aaa name dvpnserver
# aaa user 0 id shisyaAid
# aaa user 0 password shisyaApass
# aaa user 1 id shisyaBid
# aaa user 1 password shisyaBpass
```

設定終了

```
# save
# reset
```

2.13.18 NAT トラバーサルを使用した可変 IP アドレスでの VPN

適用機種　全機種

接続するたびに IP アドレスが変わる環境で NAT トラバーサルを使って、VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

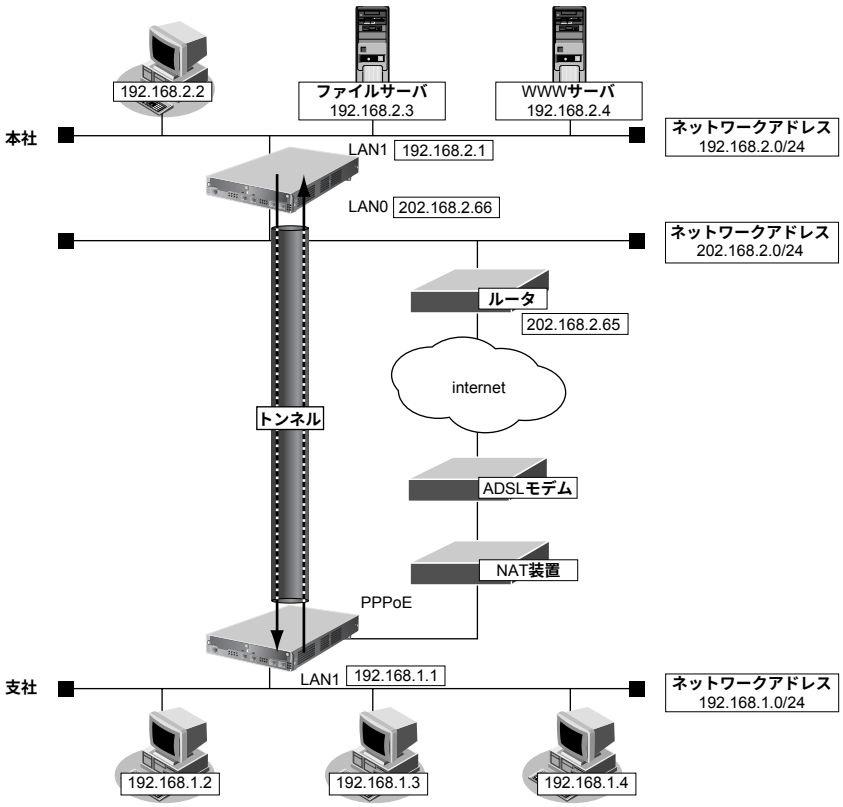
● 前提条件

[支社（PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：支社 － 202.168.2.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[本社]

- ネットワーク名　：vpn-shi
- 接続先名　：shisya
- IPsec/IKE 区間　：202.168.2.66 － 支社
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Aggressive Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 支社 ID ／ ID タイプ　：shisya（自装置名）／ FQDN
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768
- IKE NAT トラバーサル機能　：使用する

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは？

Aggressive Mode の場合に、ネゴシエーションで使用する自装置を識別する ID の種別です。相手 VPN 装置の設定に合わせます。

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。

支社を設定する（Initiator）

● コマンド

PPPoE を設定する
```
# delete lan 0
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
```

VPN を設定する
```
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
# remote 1 ap 0 ike nat-traversal use on
```

設定終了
```
# save
# commit
```

本社を設定する（Responder）

● コマンド

```
LAN を設定する
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 1 ip address 192.168.2.1/24 3

VPN を設定する
# remote 0 name vpn-shi
# remote 0 ip route 0 192.168.1.0/24 1 0
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 any4
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode aggressive
# remote 0 ap 0 ike name remote shisya
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 0 ap 0 ike nat-traversal use on

設定終了
# save
# commit
```

2.13.19 テンプレート着信機能（AAA 認証）および NAT トラバーサルを使用した可変 IP アドレスでの VPN

適用機種　全機種

IPsec 機能、テンプレート機能および NAT トラバーサルを使って、自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

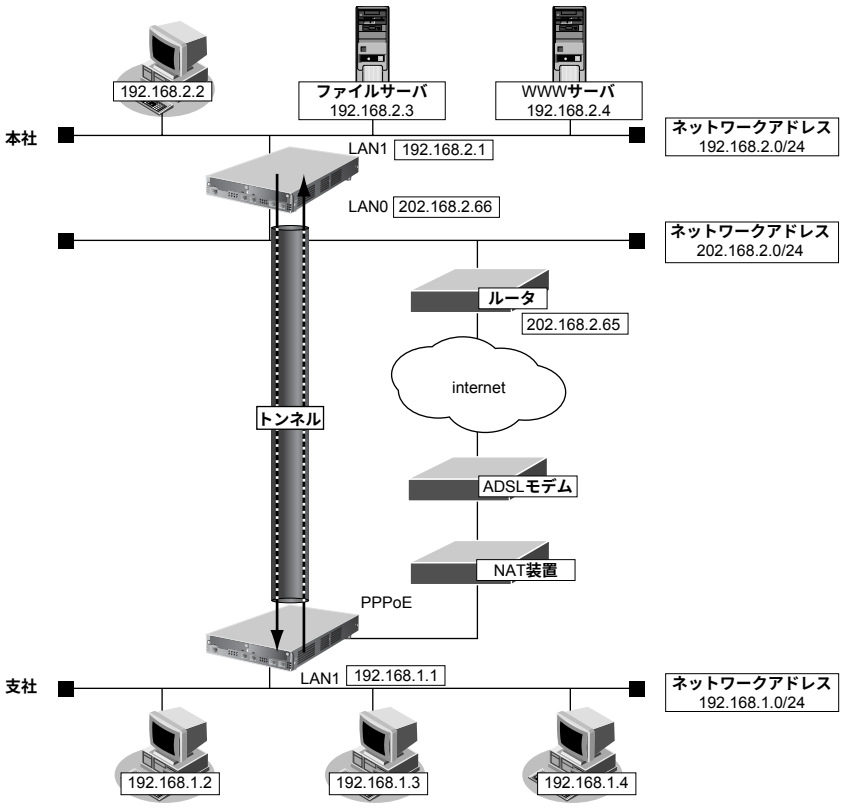
● 前提条件

[支社（PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：支社 － 202.168.2.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[本社]

- テンプレート名　：vpn-shi
- IPsec/IKE 区間　：202.168.2.66 － 支社
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Aggressive Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 支社 ID ／ ID タイプ　：shisya（自装置名）／ FQDN
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768
- IKE NAT トラバーサル機能　：使用する

こんな事に気をつけて

- **テンプレート着信機能（AAA 認証）を使用した IPsec では、AAA 設定のユーザ ID とユーザ認証パスワードを同じに設定してください。**
- **ユーザ ID とユーザ認証パスワードは、テンプレート情報の IKE 情報の交換モードにより以下のように設定します。**
  Main Mode の場合　：相手側 IPsec トンネルアドレス
  Aggressive Mode の場合　：相手側の装置識別情報

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは？

Aggressive Mode の場合に、ネゴシエーションで使用する自装置を識別する ID の種別です。相手 VPN 装置の設定に合わせます。

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。

支社を設定する（Initiator）

● コマンド

PPPoE を設定する
```
# delete lan 0
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
```

VPN を設定する
```
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
# remote 1 ap 0 ike nat-traversal use on
```

設定終了
```
# save
# commit
```

本社を設定する（Responder）

● コマンド

```
LANを設定する
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 1 ip address 192.168.2.1/24 3

VPN（テンプレート）を設定する
# template 0 name vpn-shi
# template 0 combine use aaa
# template 0 datalink type ipsec
# template 0 interface pool 1 1
# template 0 aaa 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt des-cbc
# template 0 ipsec ike auth hmac-md5
# template 0 ipsec ike pfs off
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ipsec ike newsa initiator 90s 0
# template 0 ipsec ike newsa responder off 0
# template 0 ike mode aggressive
# template 0 ike idtype fqdn
# template 0 ike proposal 0 encrypt des-cbc
# template 0 ike proposal 0 hash hmac-md5
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 ike release on
# template 0 ike nat-traversal use on
# template 0 tunnel local 202.168.2.66

AAA情報を設定する
# aaa 0 name vpn-shi
# aaa 0 user 0 id shisya
# aaa 0 user 0 password shisya
# aaa 0 user 0 ipsec ike range any4 any4
# aaa 0 user 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# aaa 0 user 0 ip route 0 192.168.1.0/24 1 1

設定終了
# save
# commit
```

2.13.20 接続先情報（動的VPN）を使用したIPv4 over IPv4で固定IPアドレスでのVPN

適用機種　全機種

IPsec機能、動的VPN情報交換機能、接続先およびテンプレート機能を使って、自動鍵交換でVPNを構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社および本社はPPPoEでインターネットに接続され、動的VPNサーバはグローバルアドレス空間の終端装置として本装置が接続されていることを前提とします。

● 前提条件

[本社（PPPoE常時接続)]

- ローカルネットワークIPv4アドレス　：192.168.0.1/24
- PPPoEユーザ認証ID　：userid0（プロバイダから提示された内容）
- PPPoEユーザ認証パスワード　：userpass0（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用
- NAT機能　：マルチNATを使用する
- ネットワーク名　：internet
- 接続先名　：ISP-1

[支社A（PPPoE常時接続)]

- ローカルネットワークIPv4アドレス　：192.168.1.1/24
- PPPoEユーザ認証ID　：userid1（プロバイダから提示された内容）
- PPPoEユーザ認証パスワード　：userpass1（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用
- NAT機能　：マルチNATを使用する
- ネットワーク名　：internet
- 接続先名　：ISP-1

[支社B（PPPoE常時接続)]

- ローカルネットワークIPv4アドレス　：192.168.2.1/24
- PPPoEユーザ認証ID　：userid2（プロバイダから提示された内容）
- PPPoEユーザ認証パスワード　：userpass2（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用
- NAT機能　：マルチNATを使用する
- ネットワーク名　：internet
- 接続先名　：ISP-1

[動的VPNサーバ]

- ローカルネットワークIPv4アドレス　：192.168.10.1/24
- インターネットプロバイダから割り当てられた固定IPv4アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートのIPv4アドレス　：202.168.2.65

● 設定コマンド

[本社（PPPoE 常時接続）]

```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.0.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid0 userpass0
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

[支社 A（PPPoE 常時接続）]

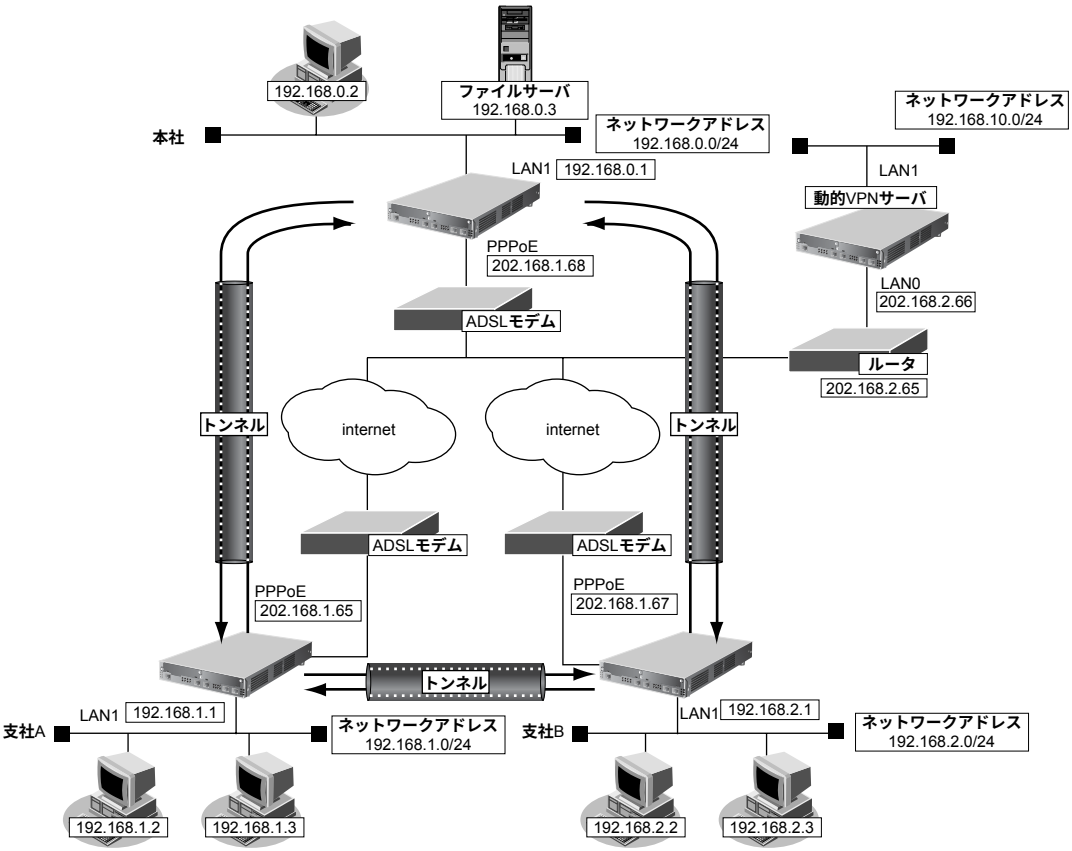
```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid1 userpass1
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

[支社 B（PPPoE 常時接続）]

```
# delete lan
# lan 0 mode auto
# lan 1 ip address 192.168.2.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid2 userpass2
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

[動的 VPN サーバ]

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 0
# lan 1 ip address 192.168.10.1/24 3
```



● 設定条件（動的VPN サーバ -本社、支社 A、B）

[本社（Initiator)]

- ネットワーク名　：vpn-srv
- 接続先名　：dvpn-srv
- IPsec/IKE 区間　：本社－ 202.168.2.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- IKE（UDP：500 番ポート）のプライベートアドレス
  ：192.168.0.1
- ESP のプライベートアドレス　：192.168.0.1

[支社 A（Initiator)]

- ネットワーク名　：vpn-srv
- 接続先名　：dvpn-srv
- IPsec/IKE 区間　：支社 A － 202.168.2.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- IKE（UDP：500 番ポート）のプライベートアドレス
  ：192.168.1.1
- ESP のプライベートアドレス　：192.168.1.1

[支社 B（Initiator)]

- ネットワーク名　：vpn-srv
- 接続先名　：dvpn-srv
- IPsec/IKE 区間　：支社 B － 202.168.2.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

- IKE（UDP：500番ポート）のプライベートアドレス
  ：192.168.2.1
- ESPのプライベートアドレス　：192.168.2.1

[動的VPNサーバ（Responder)]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE区間　：202.168.2.66 ー本社
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット
- ネットワーク名　：vpn-shiA
- 接続先名　：shisyaA
- IPsec/IKE区間　：202.168.2.66 ー支社A
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット
- ネットワーク名　：vpn-shiB
- 接続先名　：shisyaB
- IPsec/IKE区間　：202.168.2.66 ー支社B
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット

[共通（本社、支社A、B-動的VPNサーバ)]

- 鍵交換タイプ　：Aggressive Mode
- IPsecプロトコル　：esp
- IPsec暗号アルゴリズム　：des-cbc
- IPsec認証アルゴリズム　：hmac-md5
- IPsec DHグループ　：なし
- IKE本社 ID/IDタイプ　：honsya （自装置識別情報）/FQDN
- IKE支社A ID/IDタイプ　：shisyaA（自装置識別情報）/FQDN
- IKE支社B ID/IDタイプ　：shisyaB（自装置識別情報）/FQDN
- IKE本社 IKE認証鍵　：1234567890ABCDEFGHIJKLMNOPQRSTUVWXYZ
- IKE支社A IKE認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890
- IKE支社B IKE認証鍵　：1234567890abcdefghijklmnopqrstuvwxyz
- IKE認証方法　：shared
- IKE暗号アルゴリズム　：des-cbc
- IKE認証アルゴリズム　：hmac-md5
- IKE DHグループ　：modp768

● 設定条件（本社 - 支社A、B）

[本社]

- テンプレート名　：vpn-shi
- IKE（UDP：500番ポート）のプライベートアドレス
  ：192.168.0.1
- ESPのプライベートアドレス　：192.168.0.1
- テンプレート接続先監視アドレス　：192.168.0.1

[支社 A]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- テンプレート名　：vpn-shiB
- IKE（UDP：500 番ポート）のプライベートアドレス　：192.168.1.1
- ESP のプライベートアドレス　：192.168.1.1
- 接続先監視アドレス　：192.168.1.1-192.168.0.1
- テンプレート接続先監視アドレス　：192.168.1.1

[支社 B]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- テンプレート名　：vpn-shiA
- IKE（UDP：500 番ポート）のプライベートアドレス　：192.168.2.1
- ESP のプライベートアドレス　：192.168.2.1
- 接続先監視アドレス　：192.168.2.1-192.168.0.1
- テンプレート接続先監視アドレス　：192.168.2.1

● 設定条件（動的 VPN 接続）

[本社 - 支社 A/B 間の動的 VPN 共通設定]

- クライアント情報　：0
- サーバ情報
  アドレス　：192.168.10.1
  ポート番号　：5070
- 有効期間　：1 時間
- セッション更新間隔　：5 分
- ドメイン名　：example.com
- VPN 通信
  利用インタフェース　：rmt0
- 動的 VPN クライアントの優先度　：10
- 動的 VPN IPv4 経路情報の優先度　：1
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：aes-cbc-128
- IPsec 認証アルゴリズム　：hmac-sha1
- IPsecDH グループ　：modp768
- IKE 認証鍵　：ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：aes-cbc-128
- IKE 認証アルゴリズム　：hmac-sha1
- IKE DH グループ　：modp768

[本社の動的 VPN 設定]

- サーバ情報
  認証 ID　：honsyaid
  認証パスワード　：honsyapass
- クライアントの IP アドレス（本社）　：192.168.0.1
- ローカル ID　：honsya

[支社 A の動的 VPN 設定]

- サーバ情報
  認証 ID　：shisyaAid
  認証パスワード　：shisyaApass
- クライアントの IP アドレス（支社 A）　：192.168.1.1

[支社 B の動的 VPN 設定]

- サーバ情報
  認証 ID　：shisyaBid
  認証パスワード　：shisyaBpass
- クライアントの IP アドレス（支社 B）　：192.168.2.1

[動的 VPN サーバ設定]

- サーバ機能　：使用する
  ドメイン名　：example.com
  認証　：行う
  AAA グループ ID　：0
- AAA ユーザ情報（本社認証情報）
  ユーザ ID　：honsyaid
  認証パスワード　：honsyapass
- AAA ユーザ情報（支社 A 認証情報）
  ユーザ ID　：shisyaAid
  認証パスワード　：shisyaApass
- AAA ユーザ情報（支社 B 認証情報）
  ユーザ ID　：shisyaBid
  認証パスワード　：shisyaBpass

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。

本社を設定する

● コマンド

```
インターネットから IPsec/IKE パケットを受信するように設定する
# remote 0 ip nat static 0 192.168.0.1 500 any 500 17
# remote 0 ip nat static 1 192.168.0.1 any any any 50
# remote 0 ip nat static default reject

本社 - 動的 VPN サーバ間の VPN を設定する
# remote 1 name vpn-srv
# remote 1 ap 0 name dvpn-srv
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local honsya
# remote 1 ap 0 ike shared key text 1234567890ABCDEFGHIJKLMNOPQRSTUVWXYZ
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.10.0/24 1 0

本社 - 支社 A/B 間の動的 VPN を設定する
# remote 0 ip dvpn 0 invite acl 0 24 0
# remote 0 ip dvpn 1 invite acl 1 24 0
# acl 0 ip 192.168.0.0/24 192.168.1.0/24 any any
# acl 1 ip 192.168.0.0/24 192.168.2.0/24 any any
# template 0 name vpn-shi
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 tunnel local 192.168.0.1
# template 0 sessionwatch address 192.168.0.1
# dvpn client 0 server 0 address 192.168.10.1 5070
# dvpn client 0 server 0 auth honsyaid honsyapass
# dvpn client 0 ua 192.168.0.1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 192.168.0.0/24 on
# dvpn client 0 localid honsya
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip route distance 1

設定終了
# save
# reset
```

支社 A を設定する

● コマンド

```
インターネットから IPsec/IKE パケットを受信するように設定する
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50
# remote 0 ip nat static default reject

支社 A- 動的 VPN サーバ間の VPN を設定する
# remote 1 name vpn-srv
# remote 1 ap 0 name dvpn-srv
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisyaA
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.10.0/24 1 0

本社 - 支社 A 間の動的 VPN を設定する
# remote 2 name vpn-hon
# remote 2 ap 0 name honsya
# remote 2 ap 0 datalink type ipsec
# remote 2 ap 0 dvpn client 0
# remote 2 ap 0 dvpn remotenet 0 192.168.0.0/24 off
# remote 2 ap 0 dvpn remoteid honsya
# remote 2 ap 0 ipsec type dvpn
# remote 2 ap 0 ipsec ike protocol esp
# remote 2 ap 0 ipsec ike encrypt aes-cbc-128
# remote 2 ap 0 ipsec ike auth hmac-sha1
# remote 2 ap 0 ipsec ike pfs modp768
# remote 2 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# remote 2 ap 0 ike proposal 0 encrypt aes-cbc-128
# remote 2 ap 0 ike proposal 0 hash hmac-sha1
# remote 2 ap 0 ike proposal 0 pfs modp768
# remote 2 ap 0 tunnel local 192.168.1.1
# remote 2 ap 0 sessionwatch address 192.168.1.1 192.168.0.1
# remote 2 ip route 0 192.168.0.0/24 1 0
# remote 2 ip route 1 192.168.2.0/24 1 2

支店間の動的 VPN を設定する
# remote 2 ip dvpn 0 invite acl 0 24 0
# acl 0 ip 192.168.1.0/24 192.168.2.0/24 any any
# template 0 name vpn-shiB
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
```

```
# template 0 tunnel local 192.168.1.1
# template 0 sessionwatch address 192.168.1.1

動的VPN（共通部分）を設定する
# dvpn client 0 server 0 address 192.168.10.1 5070
# dvpn client 0 server 0 auth shisyaAid shisyaApass
# dvpn client 0 ua 192.168.1.1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 192.168.1.0/24 on
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip route distance 1

設定終了
# save
# reset
```

支社Bを設定する

● コマンド

```
インターネットからIPsec/IKEパケットを受信するように設定する
# remote 0 ip nat static 0 192.168.2.1 500 any 500 17
# remote 0 ip nat static 1 192.168.2.1 any any any 50
# remote 0 ip nat static default reject

支社A-動的VPNサーバ間のVPNを設定する
# remote 1 name vpn-srv
# remote 1 ap 0 name dvpn-srv
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisyaB
# remote 1 ap 0 ike shared key text 1234567890abcdefghijklmnopqrstuvwxyz
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.10.0/24 1 0

本社-支社B間の動的VPNを設定する
# remote 2 name vpn-hon
# remote 2 ap 0 name honsya
# remote 2 ap 0 datalink type ipsec
# remote 2 ap 0 dvpn client 0
# remote 2 ap 0 dvpn remotenet 0 192.168.0.0/24 off
# remote 2 ap 0 dvpn remoteid honsya
# remote 2 ap 0 ipsec type dvpn
# remote 2 ap 0 ipsec ike protocol esp
# remote 2 ap 0 ipsec ike encrypt aes-cbc-128
# remote 2 ap 0 ipsec ike auth hmac-sha1
# remote 2 ap 0 ipsec ike pfs modp768
# remote 2 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# remote 2 ap 0 ike proposal 0 encrypt aes-cbc-128
# remote 2 ap 0 ike proposal 0 hash hmac-sha1
# remote 2 ap 0 ike proposal 0 pfs modp768
# remote 2 ap 0 tunnel local 192.168.2.1
# remote 2 ap 0 sessionwatch address 192.168.2.1 192.168.0.1
```

```
# remote 2 ip route 0 192.168.0.0/24 1 0
# remote 2 ip route 1 192.168.1.0/24 1 2

支店間の動的VPNを設定する
# remote 2 ip dvpn 0 invite acl 0 24 0
# acl 0 ip 192.168.2.0/24 192.168.1.0/24 any any
# template 0 name vpn-shiA
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 tunnel local 192.168.2.1
# template 0 sessionwatch address 192.168.2.1

動的VPN（共通部分）を設定する
# dvpn client 0 server 0 address 192.168.10.1 5070
# dvpn client 0 server 0 auth shisyaBid shisyaBpass
# dvpn client 0 ua 192.168.2.1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 192.168.2.0/24 on
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip route distance 1

設定終了
# save
# reset
```

動的VPNサーバを設定する

● コマンド

```
VPNを設定する
# remote 0 name vpn-hon
# remote 0 ap 0 name honsya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode aggressive
# remote 0 ap 0 ike name remote honsya
# remote 0 ap 0 ike shared key text 1234567890ABCDEFGHIJKLMNOPQRSTUVWXYZ
# remote 0 ap 0 ike proposal 0 encrypt des-cbc
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ip route 0 192.168.0.0/24 1 0
# remote 1 name vpn-shi
# remote 1 ap 0 name shisyaA
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
```

```
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name remote shisyaA
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ip route 0 192.168.1.0/24 1 0
# remote 2 name vpn-shiB
# remote 2 ap 0 name shisyaB
# remote 2 ap 0 datalink type ipsec
# remote 2 ap 0 ipsec type ike
# remote 2 ap 0 ipsec ike protocol esp
# remote 2 ap 0 ipsec ike encrypt des-cbc
# remote 2 ap 0 ipsec ike auth hmac-md5
# remote 2 ap 0 ike mode aggressive
# remote 2 ap 0 ike name remote shisyaB
# remote 2 ap 0 ike shared key text 1234567890abcdefghijklmnopqrstuvwxyz
# remote 2 ap 0 ike proposal 0 encrypt des-cbc
# remote 2 ap 0 tunnel local 202.168.2.66
# remote 2 ip route 0 192.168.2.0/24 1 0

動的VPNサーバを設定する
# dvpn server use on
# dvpn server domain example.com
# dvpn server auth use on
# aaa 0 name dvpnserver
# aaa 0 user 0 id honsyaid
# aaa 0 user 0 password honsyapass
# aaa 0 user 1 id shisyaAid
# aaa 0 user 1 password shisyaApass
# aaa 0 user 2 id shisyaBid
# aaa 0 user 2 password shisyaBpass

設定終了
# save
# reset
```

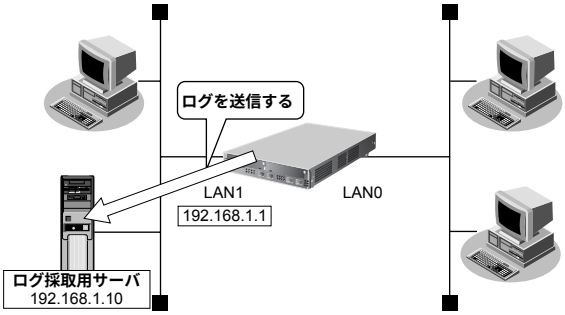
2.14 システムログを採取する

適用機種　全機種

本装置では、各種システムログ（回線の接続／切断など）をネットワーク上のシステムログサーバに送信することができます。また、セキュリティログとして以下のログを採取することができます。

- PPP（着信拒否）
- IP フィルタ（遮断したパケット）
- URL フィルタ（遮断したパケット）
- NAT（遮断したパケット、変換テーブル作成）
- DHCP（配布した IPv4 アドレス、IPv6 プレフィックス）
- IDS（検出されたパケット）
- MAC アドレス認証（不正端末の MAC 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
  - IP フィルタ
  - NAT
  - PPP
  - DHCP
  - Proxy DNS
  - IDS
  - MAC アドレス認証
- 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 192.168.1.10

システムログを設定する
# syslog pri error,warn,notice,info
# syslog security ipfilter,nat,ppp,dhcp,proxydns,ids,macauth

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。

2.15 マルチ NAT 機能（アドレス変換機能）を使う

適用機種　全機種

本装置のマルチ NAT 機能を使用すると、通信発生のたびにあいているグローバルアドレスを割り当てるので、限られた数のグローバルアドレスでそれ以上のパソコンを接続できます。
ここでは、静的 NAT を使って、サーバを公開する場合を例に説明します。静的 NAT は、特定のパソコンやアプリケーションに同じ IP アドレス、ポート番号を割り当てます。そのために Web を公開するような場合に適しています。

☛参照 Si-R シリーズ　機能説明書「2.14 マルチ NAT 機能」（P.71）

ヒント

◆ 同時に接続できる台数

機能	同時接続台数およびセッション数	備考
基本 NAT	グローバルアドレス数 セッション数制限なし	割り当て時間内は外部からの通信もできる 基本 NAT と静的 NAT で同一グローバルアドレスを使用しないでください
動的 NAT	Si-R180、260B は最大 1024 セッション、 Si-R220B、240 は最大 2000 セッション、 Si-R370 は最大 3000 セッション、 Si-R570 は最大 5000 セッションまで	外部からの通信はできない
静的 NAT	Si-R180、260B は最大 64 個、 Si-R220B、240 は最大 200 個、 Si-R370 は最大 300 個、 Si-R570 は最大 500 個まで割り当て可能	プライベートアドレスとポートをグローバルアドレスとポートに割り当てできる 割り当てたアドレスとポートに関しては外部からの通信もできる
あて先変換	Si-R180、260B は最大 64 個、 Si-R220B、240 は最大 200 個、 Si-R370 は最大 300 個、 Si-R570 は最大 500 個まで割り当て可能	グローバルアドレスをプライベートアドレスに割り当てできる

こんな事に気をつけて

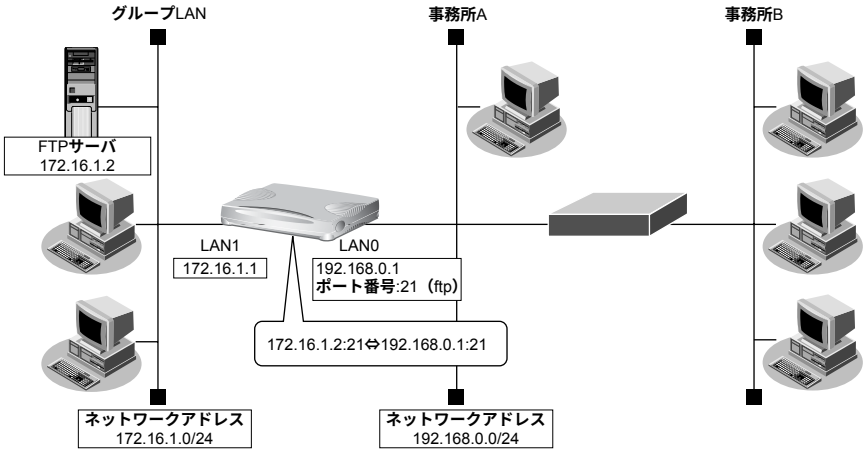
コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

☛参照 Si-R シリーズ　コマンドユーザーズガイド「1.7 コマンドで入力できる文字一覧」（P.26）

2.15.1　プライベートLAN 接続でサーバを公開する

適用機種　全機種

ここでは、静的NAT を使って、FTP サーバを公開する場合の設定方法を説明します。



● 設定条件

[事務所 A 側]

- LAN0 ポートを使用する
- 静的NAT を使用する

[グループ LAN 側]

- IP アドレス　：172.16.1.1
- ネットワークアドレス/ネットマスク　：172.16.1.0/24
- FTP サーバの IP アドレス　：172.16.1.2

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 IP アドレスを設定する
# lan 0 ip address 192.168.0.1/24 3
# lan 1 ip address 172.16.1.1/24 3

NAT 情報を設定する
# lan 0 ip nat mode multi any 1 5m
# lan 0 ip nat static 0 172.16.1.2 21 192.168.0.1 21 6

設定終了
# save
# commit
```

こんな事に気をつけて

NAT では、FTP や DNS が要求した相手からの応答かどうかをチェックします。相手サーバが NAT 機能を使用している場合など、要求先とは別のアドレスから応答する場合は、以下の設定を追加してください。

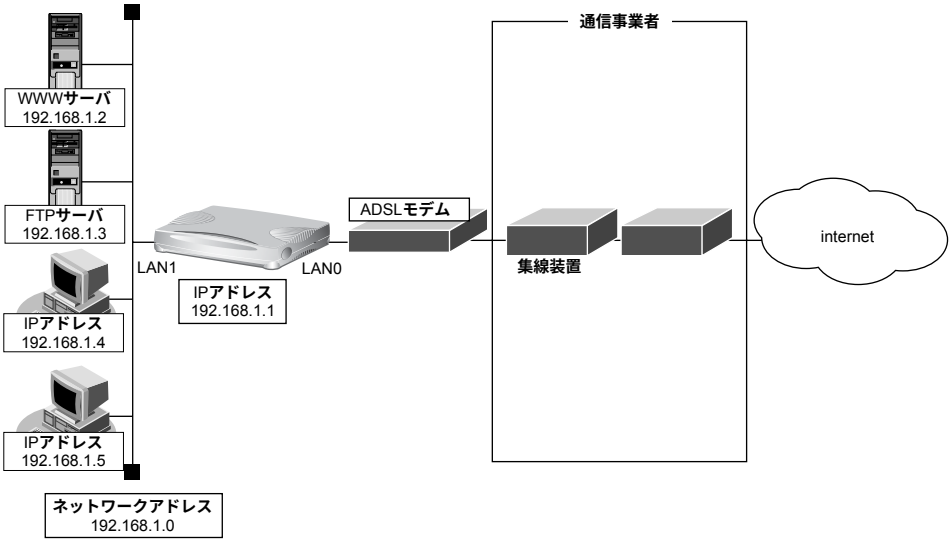
```
# lan 0 ip nat rule 0 ftp any 21 off
# lan 0 ip nat rule 1 dns global 53 off
```

2.15.2　PPPoE 接続でサーバを公開する

適用機種　全機種

PPPoE を使ってインターネットへ接続している場合の例です。

ここでは、PPPoE 接続時に静的 NAT を使ってサーバを公開する場合の設定方法を説明します。



● 設定条件

- 既存の LAN を使用する
- ユーザ認証 ID　：userid
- ユーザ認証パスワード　：userpass
- ネットワークアドレス/ネットマスク　：192.168.1.0/24
- ブロードキャストアドレス　：192.168.1.255

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

```
PPPoE でインターネットへ接続する環境を設定する
# delete lan 0
# lan 0 mode auto
# 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
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip route 0 default 1 0
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# proxydns domain 0 any * any to 0
# proxydns address 0 any to 0

NAT 情報を設定する
# remote 0 ip nat static 0 192.168.1.2 80 any 80 any
# remote 0 ip nat static 1 192.168.1.3 21 any 21 any

設定終了
# save

再起動
# reset
```

こんな事に気をつけて

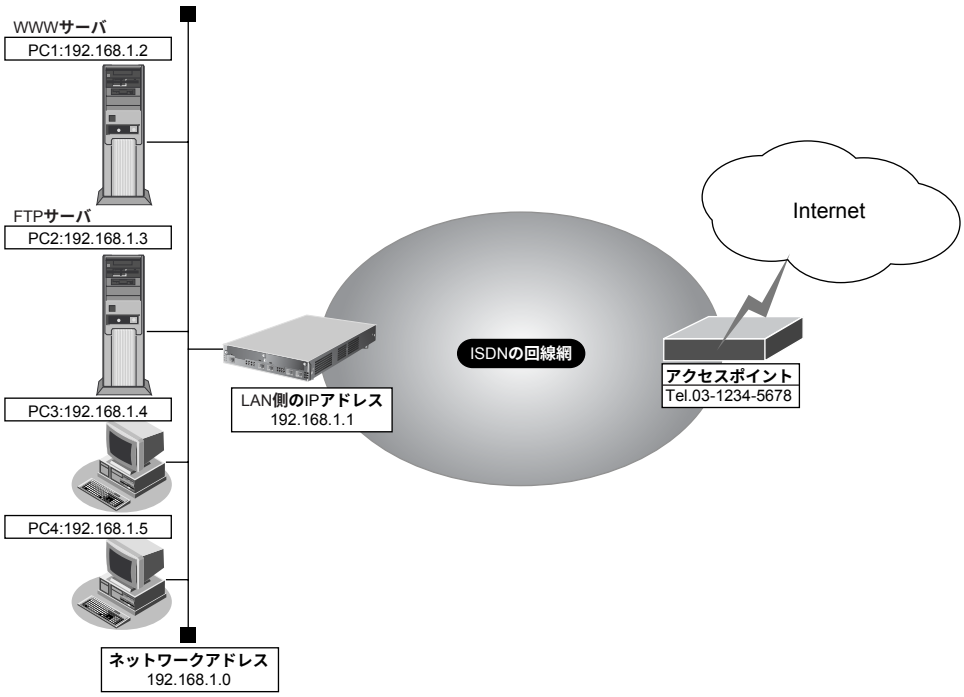
- ネットワーク型接続でマルチ NAT を使用する際、グローバルアドレスの設定が必須となります。なお、端末型接続では、接続時にグローバルアドレスが割り当てられるため、設定は不要です。
- 動的 NAT と静的 NAT が混在する場合、動的 NAT で使用する IP アドレスと静的 NAT で使用する IP アドレスは重複しないようにしてください。
- NAT では、FTP や DNS が要求した相手からの応答かどうかをチェックします。相手サーバが NAT 機能を使用している場合など、要求先とは別のアドレスから応答する場合は、以下の設定を追加してください。

```
# remote 0 ip nat rule 0 ftp any 21 off
# remote 0 ip nat rule 1 dns global 53 off
```

2.15.3　ネットワーク型接続でサーバを公開する

適用機種　***Si-R220B,370,570***

ここでは、静的 NAT を使ってサーバを公開する場合の設定方法を説明します。



● 設定条件

- slot0 に実装された BRI 拡張モジュール L2 または基本ボード上の ISDN ポート（Si-R220B の場合）で ISDN でインターネットに接続する
- ISDN に接続する
- ユーザ認証 ID　：userid
- ユーザ認証パスワード　：userpass
- ネットワーク型接続を行う
- 既存の LAN を使用する
- 割り当てネットワークアドレス　：10.10.10.96/29
- www に割り当てる IP アドレス　：10.10.10.98
- ftp に割り当てる IP アドレス　：10.10.10.99
- 動的 NAT で使用する IP アドレス　：10.10.10.100 ～ 102
- ネットワークアドレス/ネットマスク　：192.168.1.0/24
- ブロードキャストアドレス　：192.168.1.255

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

```
回線情報を設定する
# wan 0 bind 0
# wan 0 line isdn

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

接続先の情報を設定する
# remote 0 name internet
# remote 0 ip route 0 default 1
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind wan 0
# remote 0 ap 0 dial 0 number 03-1234-5678
# remote 0 ap 0 ppp auth send userid userpass

NAT 情報を設定する
# remote 0 ip nat mode multi 10.10.10.100 3 5m
# remote 0 ip nat static 0 192.168.1.2 80 10.10.10.98 80 any
# remote 0 ip nat static 1 192.168.1.3 21 10.10.10.99 21 any

設定終了
# save

再起動
# reset
```

こんな事に気をつけて

- NAT では、FTP や DNS が要求した相手からの応答かどうかをチェックします。相手サーバが NAT 機能を使用している場合など、要求先とは別のアドレスから応答する場合は、以下の設定を追加してください。

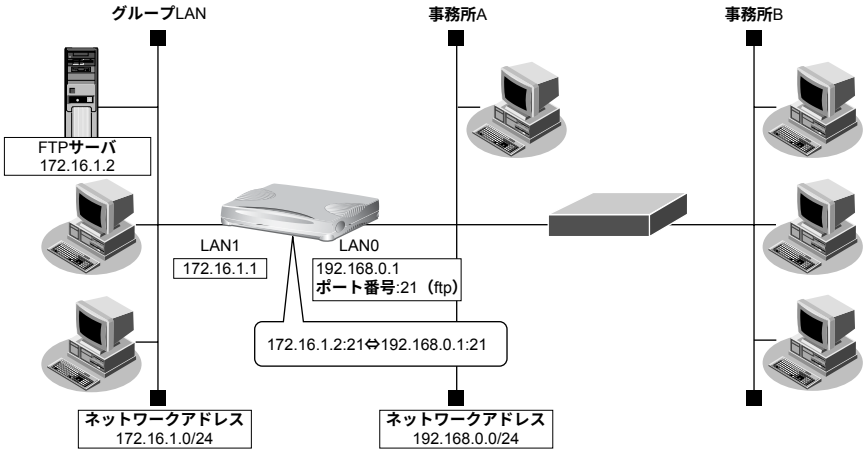
```
# remote 0 ip nat rule 0 ftp any 21 off
# remote 0 ip nat rule 1 dns global 53 off
```

- Si-R220B では、利用物理回線設定でスロット番号に“mb”を指定してください。

2.15.4 サーバ以外のアドレス変換をしないで、プライベートLAN接続でサーバを公開する

適用機種　全機種

ここでは、静的NATだけを使って、サーバ以外のアドレス変換をしないで、FTPサーバを公開する場合の設定方法を説明します。



● 設定条件

[事務所A側]

- LAN0ポートを使用する
- 静的NATだけを使用する

[グループLAN側]

- IPアドレス　：172.16.1.1
- ネットワークアドレス/ネットマスク　：172.16.1.0/24
- FTPサーバのIPアドレス　：172.16.1.2

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IPアドレスを設定する
# lan 0 ip address 192.168.0.1/24 3
# lan 1 ip address 172.16.1.1/24 3

NAT情報を設定する
# lan 0 ip nat mode multi any 1 5m
# lan 0 ip nat static 0 172.16.1.2 21 192.168.0.1 21 6

設定終了
# save
# commit
```

こんな事に気をつけて

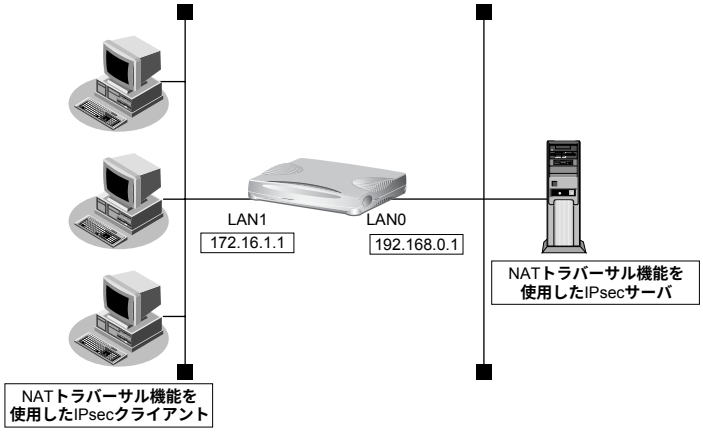
NATでは、FTPやDNSが要求した相手からの応答かどうかをチェックします。相手サーバがNAT機能を使用している場合など、要求先とは別のアドレスから応答する場合は、以下の設定を追加してください。

```
# lan 0 ip nat rule 0 ftp any 21 off
# lan 0 ip nat rule 1 dns global 53 off
```

2.15.5 複数の NAT トラバーサル機能を使用した IPsec クライアントを同じ IPsec サーバに接続する

適用機種　全機種

ここでは、静的 NAT を使って、複数の NAT トラバーサル機能を使用した IPsec クライアントを同じ IPsec サーバに接続する場合の設定方法を説明します。



● 設定条件

[IPsec サーバ側]

- LAN0 ポートを使用する
- マルチ NAT 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 172.16.1.1/24 3
```

NAT 情報を設定する
```
# lan 0 ip nat mode multi any 1 5m
# lan 0 ip nat wellknown 0 500 off
```

設定終了
```
# save
# commit
```

こんな事に気をつけて

NAT では、FTP や DNS が要求した相手からの応答かどうかをチェックします。相手サーバが NAT 機能を使用している場合など、要求先とは別のアドレスから応答する場合は、以下の設定を追加してください。

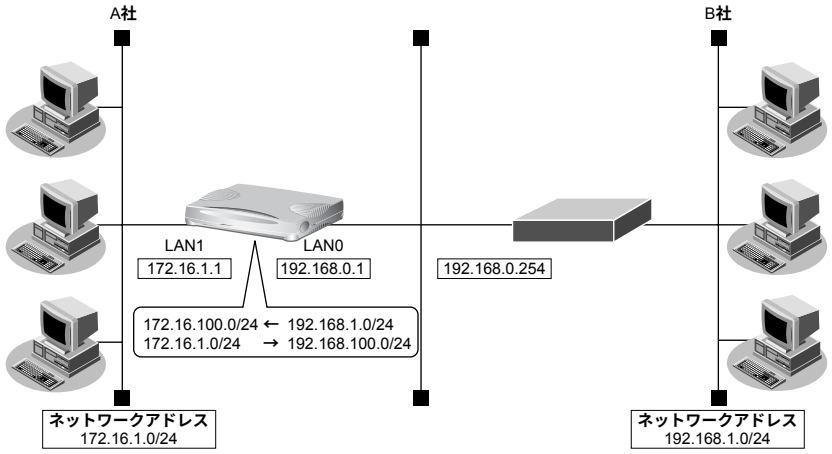
```
# lan 0 ip nat rule 0 ftp any 21 off
# lan 0 ip nat rule 1 dns global 53 off
```

2.15.6　NAT あて先変換で双方向のアドレスを変換する

適用機種　全機種

ここでは、NAT あて先変換を使って、双方向の IP アドレスを変換する場合の設定方法を説明します。

この機能を使用して異なるアドレス体系をもつ A 社と B 社を接続した場合、同じアドレス体系であるかのように見せることができます。



● 設定条件

[A 社]

- IP アドレス　：172.16.1.1
- ネットワークアドレス/ネットマスク　：172.16.1.0/24

[B 社]

- LAN0 ポートを使用する
- マルチ NAT を使用する
- NAT あて先変換を使用する

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 172.16.1.1/24 3

B 社 への経路を設定する
# lan 0 ip route 0 192.168.1.0/24 192.168.0.254

NAT 情報を設定する
# lan 0 ip nat mode multi any 1 5m
# lan 0 ip nat static 0 172.16.1.2 192.168.100.2-192.168.100.254
# lan 0 ip nat destination 0 172.16.100.2 192.168.1.2-192.168.1.254

設定終了
# save
# commit
```

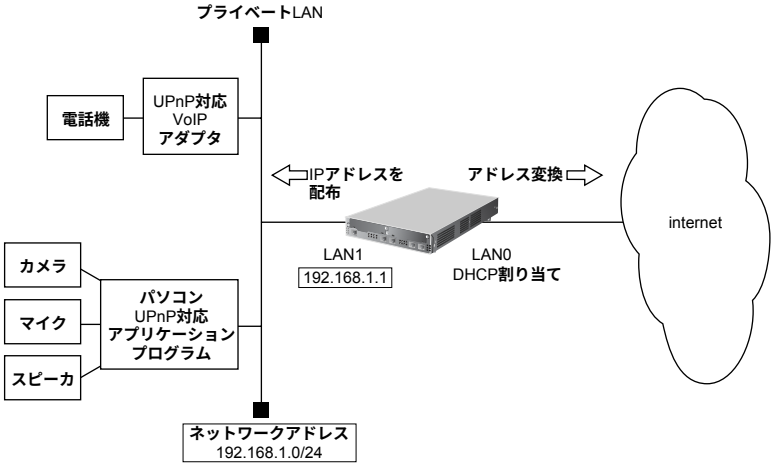
2.16 VoIP NAT トラバーサル機能を使う

適用機種　全機種

マルチ NAT 機能を使用すると動作しない VoIP アダプタが UPnP に対応している場合、本装置の VoIP NAT トラバーサル機能を使用することによって動作できるようになることがあります。同様に、UPnP に対応した装置やアプリケーションプログラムもマルチ NAT 機能を使用しても動作できるようになることがあります。

参照　Si-R シリーズ　機能説明書「2.15 VoIP NAT トラバーサル機能」（P.75）

ここでは、UPnP 対応 VoIP アダプタや UPnP 対応アプリケーションプログラムを使用する設定方法を説明します。



● 設定条件

[インターネット側 LAN]

- LAN0 ポートを使用する
- 転送レート　：自動認識
- IP アドレス　：DHCP サーバから自動的に取得
- マルチ NAT を使用する
  グローバルアドレス　：インターネットプロバイダから割り当てられた IP アドレスを使用する
  アドレス個数　：1
  アドレス割り当てタイマ　：5 分

[UPnP 対応装置（プライベート LAN）側]

- LAN1 ポートを使用する
- 転送レート　：自動認識
- IP アドレス　：192.168.1.1/24
- DHCP サーバ機能を使用する
  割り当て先頭アドレス　：192.168.1.2
  割り当てアドレス数　：253
  リース期間　：1 日
  デフォルトルータ広報　：192.168.1.1
  DNS サーバ広報　：192.168.1.1

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 Si-R シリーズ　コマンドユーザーズガイド「1.7 コマンドで入力できる文字一覧」（P.26）

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

インターネット側の LAN 情報を設定する
delete lan 0
lan 0 mode auto
lan 0 ip dhcp service client
lan 0 ip rip use off v1 0 off
lan 0 ip nat mode multi any 1

UPnP 対応装置側の LAN 情報を設定する
lan 1 mode auto
lan 1 ip address 192.168.1.1/24 3
lan 1 ip dhcp service server
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
lan 1 ip dhcp info dns 192.168.1.1
lan 1 ip rip use v1 v1 0 off

UPnP 機能を設定する
upnp use on

設定終了
save

再起動
reset

本装置の設定が終了したら、設定を有効にするためにパソコンのシステムを終了し、パソコンおよび本装置の電源を切断します。各装置を LAN ケーブルで正しく接続したあと、本装置、UPnP 対応装置やパソコンの順に電源を投入します。

2.17 TOS/Traffic Class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TOS/Traffic Class値を変更することにより、ポリシーベースネットワークのポリシに合わせることができます。

参照　Si-Rシリーズ　機能説明書「2.16 TOS/Traffic Class値書き換え機能」（P.78）

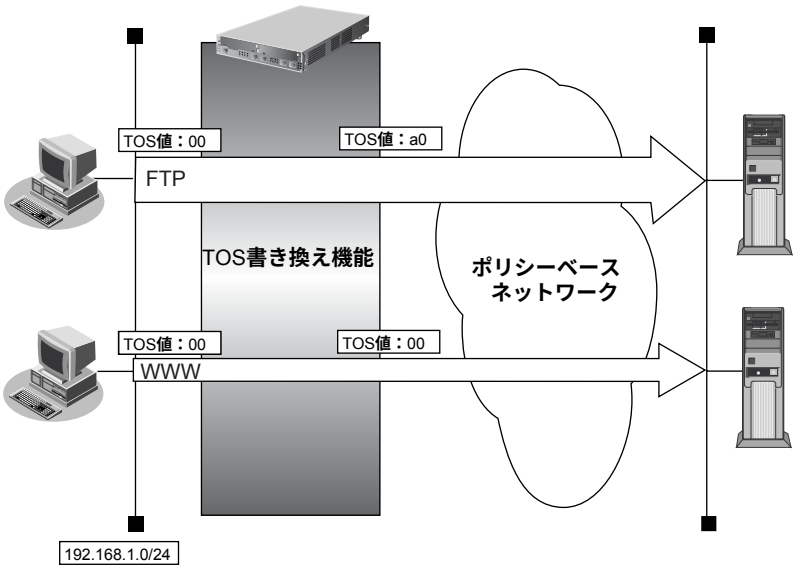
TOS/Traffic Class値書き換え機能の条件

本装置では、コマンドで以下の条件を指定することによって、ポリシーベースネットワークのポリシに合ったTOS/Traffic Class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IPv6パケットのTraffic Class値
- 新TOSまたはTraffic Class

ここではネットワークが以下のポリシをもつ場合の設定方法を説明します。

- FTP（TOS値a0）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
- TOS 値　：00
- 新 TOS 値　：a0

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 TOS 値を 00 から a0 に書き換える
# acl 0 ip 192.168.1.0/24 any 6 tos 0
# acl 0 tcp any 20,21 yes
# remote 0 ip tos 0 acl 0 a0

設定終了
# save
# commit
```

2.18 VLANプライオリティマッピング機能を使う

適用機種　全機種

VLAN プライオリティマッピング機能を使用して、レイヤ 2 スイッチなどで QoS 制御を行うことができます。

本装置から送信される VLAN パケットの VLAN のプライオリティ値を、IP パケットの TOS フィールドおよび IPv6 パケットのトラフィッククラスフィールドの値から設定します。

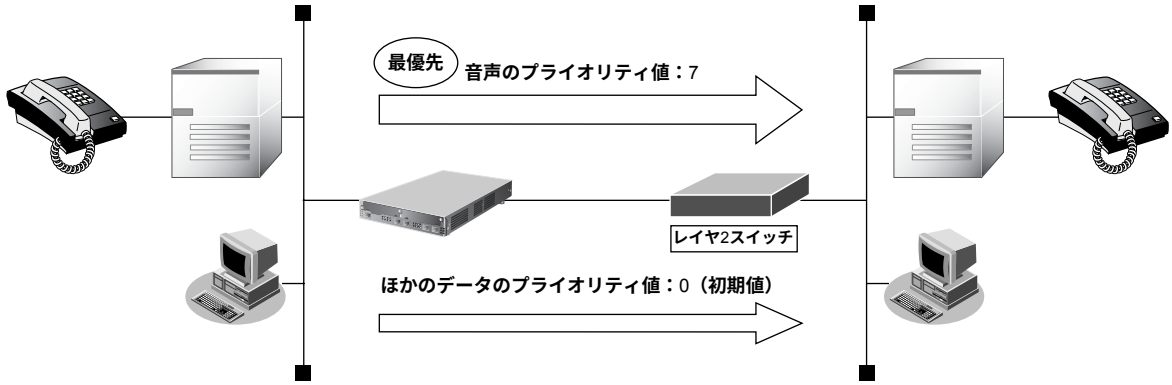
参照　Si-R シリーズ　機能説明書「2.17 VLAN プライオリティマッピング機能」（P.80）

本装置では、コマンドで以下の条件を指定することによって、VLAN のプライオリティフィールドを設定することができます。

- プロトコル
- TOS/Traffic Class
- プライオリティ

ここでは、本装置が以下の音声データを転送する場合の設定方法を説明します。

- 音声（IP で TOS 値が a0）を最優先とする（プライオリティ値が 7）
- その他は初期値（プライオリティ値が 0）



● 設定条件

- プロトコル　：IPv4
- TOS 値　：a0
- プライオリティ値　：7

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

```
TOS値a0のパケットのプライオリティ値を7に設定する
# lan 0 vlan tag primap 0 ip a0 7

設定終了
# save
# commit
```

2.19 シェーピング機能を使う

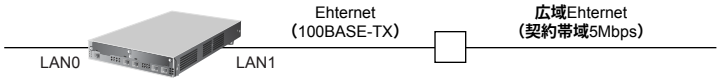
適用機種　全機種

シェーピング機能を使用すると、LAN および WAN 回線に送出するデータ量を制限することができます。

2.19.1 特定のインタフェースでシェーピング機能を使う

適用機種　全機種

ここでは、Ethernet 回線の送出するデータ量を制限する場合の設定方法を説明します。



● 設定条件

- 広域 Ethernet を利用する通信環境が設定済み
- 広域 Ethernet の契約帯域は 5Mbps

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。

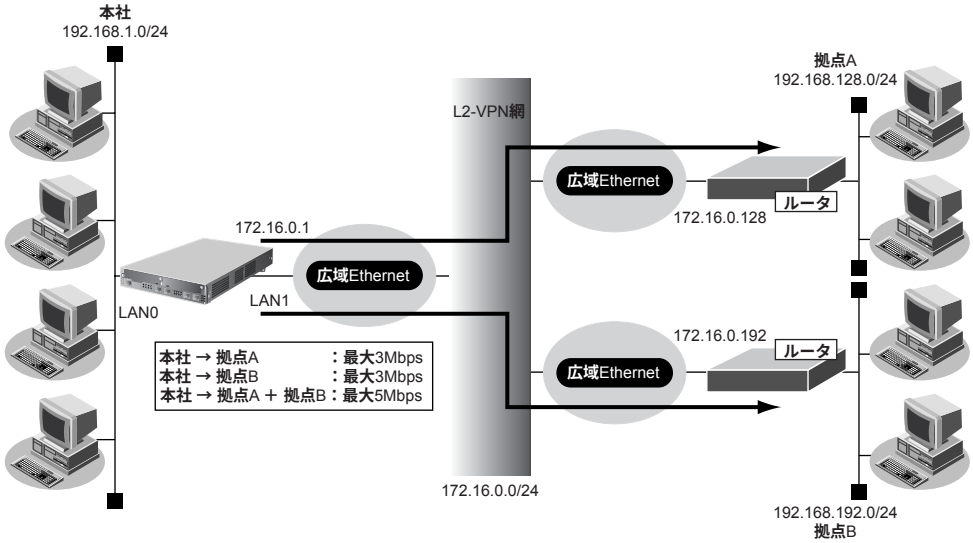
● コマンド

```
LAN1 の送出するデータ量を 5Mbps に制限する
# lan 1 shaping on 5m

設定終了
# save
# commit
```

2.19.2　送信先ごとにシェーピング機能を使う

適用機種　全機種

ここでは、各拠点に送出するデータ量を制限する場合の設定方法を説明します。



● 設定条件

- 広域 Ethernet をアクセスラインとする。L2-VPN 網を利用して本社と各拠点を接続する
- 本社から拠点 A への送信データは、最大 3Mbps に制限する
- 本社から拠点 B への送信データは、最大 3Mbps に制限する
- 本社から拠点 A と拠点 B への送信データの合計は、最大 5Mbps に制限する
- 本社の本装置は LAN ポートのアドレス設定ができた状態から設定を始める

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

```
シェーピング機能を設定する
# lan1 shaping on 5m

拠点Aの情報を設定する
# remote 0 name kyotenA
# remote 0 ip route 0 192.168.128.0/24 1 1
# remote 0 shaping on 3m
# remote 0 ap 0 name OV-A
# remote 0 ap 0 datalink type overlap
# remote 0 ap 0 overlap to lan 1
# remote 0 ap 0 overlap nexthop 172.16.0.128

拠点Bの情報を設定する
# remote 1 name kyotenB
# remote 1 ip route 0 192.168.192.0/24 1 1
# remote 1 shaping on 3m
# remote 1 ap 0 name OV-B
# remote 1 ap 0 datalink type overlap
# remote 1 ap 0 overlap to lan 1
# remote 1 ap 0 overlap nexthop 172.16.0.192

設定終了
# save
# commit
```

2.20 データ圧縮／ヘッダ圧縮機能を使う

適用機種　全機種

PPP を使った相手装置との接続時に、データ圧縮およびヘッダ圧縮機能によって回線の利用効率を高めることができます。

データ圧縮は、ISDN 接続、専用線接続、モデム接続、およびデータ通信カード接続をサポートしています。

データ圧縮およびヘッダ圧縮機能を利用する場合、接続する相手装置側でも同じ圧縮機能をサポートしている必要があります。以下に、サポートしている圧縮機能を示します。

- データ圧縮（Si-R220B、240、370、570）
  - LZS
- ヘッダ圧縮
  - VJ　：VJ ヘッダ圧縮（RFC1144 に準拠）の利用
  - IPHC　：IP ヘッダ圧縮（圧縮方法：RFC2507/RFC2508、ネゴシエーション方法：RFC2509 に準拠）の利用

ヘッダ圧縮の場合

ここでは、PPPoE 接続をネットワーク 0（remote 0）で定義している環境に対して、ヘッダ圧縮を行う場合の設定方法を説明します。

● 設定条件

- ネットワーク 0（remote 0）で PPPoE による通信環境が設定済み
- ヘッダ圧縮機能を使用する

上記の設定条件に従ってヘッダ圧縮を行う場合のコマンド例を示します。

● コマンド

```
ヘッダ圧縮機能を設定する
# remote 0 ppp ipcp vjcomp enable
# remote 0 ppp ipcp iphc enable

設定終了
# save
# commit
```

こんな事に気をつけて

ヘッダ圧縮機能は、シェーピングによって通信速度が低速の場合に効果があります。高速回線で使用した場合は、処理のオーバーヘッドによって回線の利用効率が低くなることがあります。

ISDN、専用線、モデム接続の場合

ここでは、ISDN 接続、専用線接続、およびモデム接続をネットワーク 0（remote 0）で定義している環境に対してデータ圧縮およびヘッダ圧縮を併用する場合の設定方法を説明します。

● 設定条件

- ネットワーク 0（remote 0）で ISDN による通信環境が設定済み
- データ圧縮機能を使用する
- ヘッダ圧縮機能を使用する

上記の設定条件に従ってデータ圧縮およびヘッダ圧縮を行う場合のコマンド例を示します。

● コマンド

```
データ圧縮機能を設定する
# remote 0 ppp compress on

ヘッダ圧縮機能を設定する
# remote 0 ppp ipcp vjcomp enable
# remote 0 ppp ipcp iphc enable

設定終了
# save
# commit
```

こんな事に気をつけて

MP と併用する場合は、受信順序制御機能を設定してください。

```
受信順序制御機能を設定する
# remote 0 ppp mp order on
```

2.21 帯域制御（WFQ）機能を使う

適用機種　全機種

本装置の帯域制御（WFQ）機能では、IP アドレスやポート番号の組み合わせで帯域を割り当てることによって、特定のデータを優先的に通すことができます。

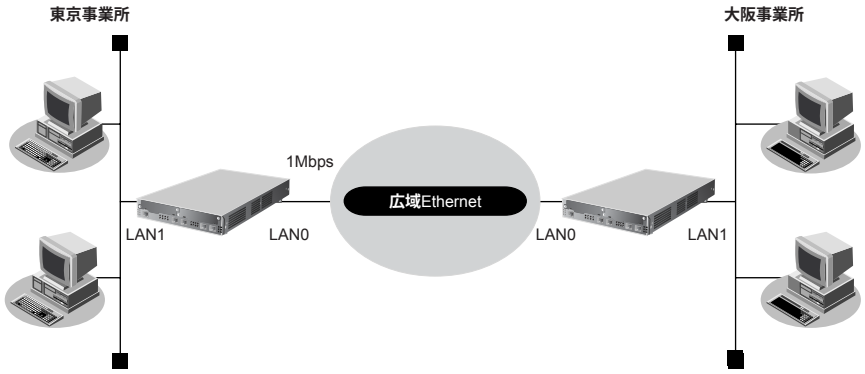
参照　Si-R シリーズ　機能説明書「2.19 帯域制御（WFQ）機能」（P.82）

帯域制御（WFQ）機能の条件

本装置では、以下の条件を指定することによって、優先的にデータを通すように帯域を割り当てることができます。

- プロトコル
- IP アドレス
- ポート番号
- IP パケットの TOS 値または IPv6 パケットの Traffic Class 値

ここでは、広域 Ethernet による拠点間の接続がすでに設定されている場合を例に帯域制御を利用する設定方法を説明します。



● 設定条件

- LAN0 インタフェースで広域 Ethernet を利用する通信環境が設定済み
- 広域 Ethernet の契約速度は 1Mbps
- 音声データ（TOS 値：a0）を最優先で透過させる

上記の設定条件に従って帯域制御する場合のコマンド例を示します。

東京事業所を設定する

● コマンド

```
シェーピングを設定する
# lan 0 shaping on 1m

帯域制御（WFQ）を設定する
# acl 0 ip any any any tos a0
# lan 0 ip priority acl 0 express

設定終了
# save
# commit
```

大阪事業所を設定する

● コマンド

```
シェーピングを設定する
# lan 0 shaping on 1m

帯域制御（WFQ）を設定する
# acl 0 ip any any any tos a0
# lan 0 ip priority acl 0 express

設定終了
# save
# commit
```

2.22 DHCP 機能を使う

適用機種　全機種

本装置の IPv4 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 クライアント機能
- DHCP リレーエージェント機能

参照　Si-R シリーズ　機能説明書「2.20.1 IPv4 DHCP 機能」（P.85）

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。**

本装置の IPv6 DHCP には、以下の機能があります。ここでは、IPv6 DHCP クライアント機能を使用する場合について説明しています。

- IPv6 DHCP サーバ機能
- IPv6 DHCP クライアント機能

参照　Si-R シリーズ　機能説明書「2.20.2 IPv6 DHCP 機能」（P.88）

2.22.1　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。

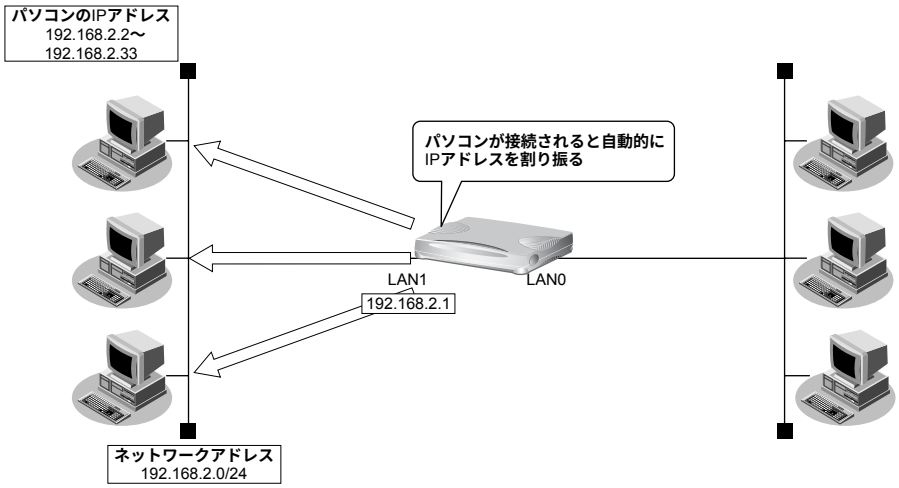
- IP アドレス
- ネットマスク
- リース期間
- デフォルトルータの IP アドレス
- DNS サーバの IP アドレス
- ドメイン名
- NTP サーバの IP アドレス
- TIME サーバの IP アドレス

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、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。



● 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
- デフォルトルータの IP アドレス　：192.168.2.1

- リース期間　：1 日
- DNS サーバの IP アドレス　：192.168.2.1
- 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

```
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
```

2.22.2 DHCP スタティック機能を使う

適用機種　全機種

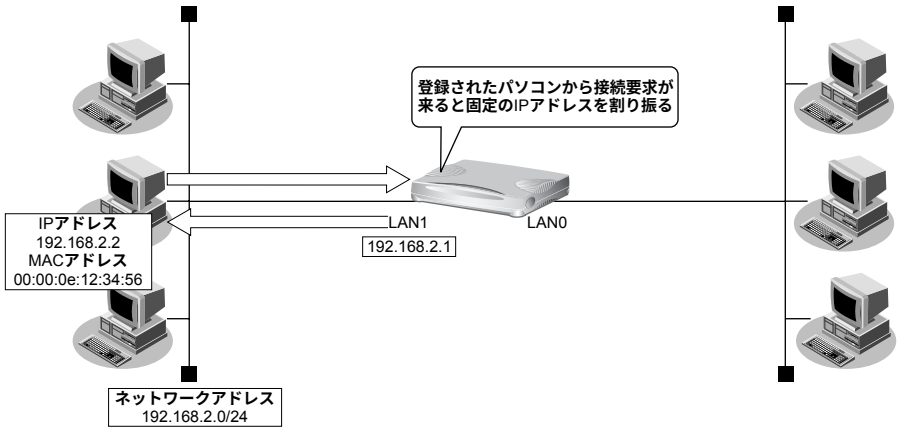
DHCP サーバは、使用していない IP アドレスを一定期間（またはパソコンが IP アドレスを返却するまで）割り当てます。不要になった IP アドレスは自動的に再利用されるため、パソコンの IP アドレスが変わることがあります。本装置では、IP アドレスと MAC アドレスを対応付けることによって、登録されたパソコンから DHCP 要求が発行されると、常に同じ IP アドレスを割り当てることができます。これを DHCP スタティック機能と言います。

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。

補足
- 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」、「マルチルーティング機能」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、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。

補足
- ホストデータベース情報は「リモートパワーオン機能」、「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 64 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

```
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
```

2.22.3 DHCP クライアント機能を使う

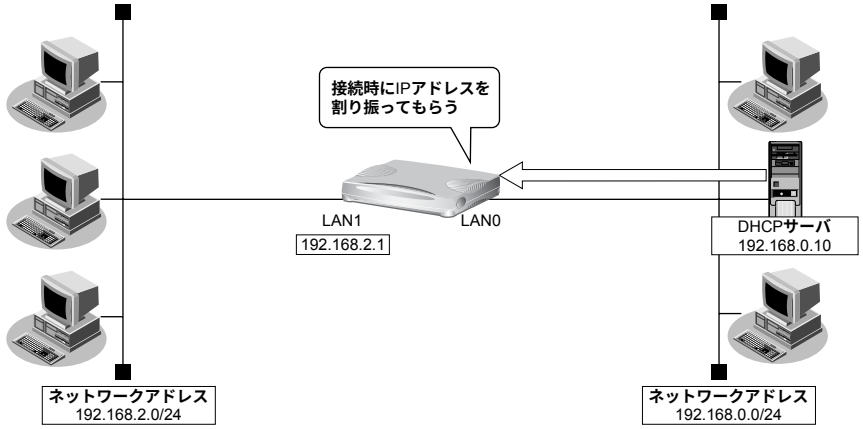
適用機種　全機種

DHCP クライアント機能は、DHCP サーバから IP アドレスなどの情報を取得する機能です。使用する場合は、DHCP サーバが動作している LAN に接続する必要があります。利用者は、IP アドレスを意識することなくネットワークを利用できます。

本装置の DHCP クライアント機能は、以下の情報を受け取って動作します。

- 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
- TIME サーバの IP アドレス
- NTP サーバの IP アドレス
- ドメイン名
- リース更新時間

ここでは、DHCP クライア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

- 本装置の IP アドレス　　：DHCP サーバから取得する

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

```
DHCP クライアント機能を設定する
# lan 0 ip dhcp service client

マルチ NAT 機能を設定する
# lan 0 ip nat mode multi any 1

LAN1 インタフェースを設定する
# lan 1 ip address 192.168.2.1/24 3

設定終了
# save
# commit
```

2.22.4　DHCP リレーエージェント機能を使う

適用機種　全機種

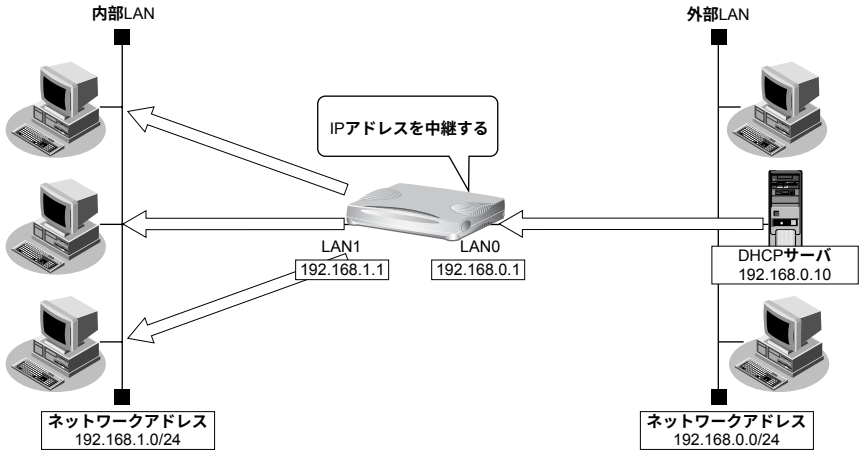
DHCPクライアントは、同じネットワーク上にあるサーバから、IPアドレスなどの情報を獲得することができます。

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。

LAN 接続の場合

適用機種　全機種



● 設定条件

[内部 LAN 側]

- 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

[外部 LAN 側]

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

補足　DHCP リレーエージェント機能を使用するときは、NAT 機能を使用できません。

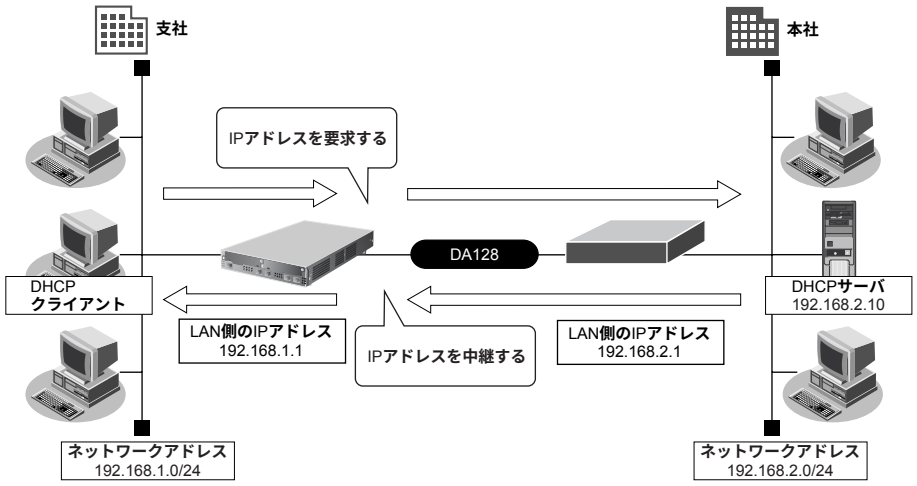
上記の設定条件に従って設定を行う場合のコマンド例を示します。

● 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
```

リモート接続の場合

適用機種　***Si-R220B,260B,370,570***



● 設定条件

- DHCPリレーエージェント機能を使用する
- 支社にDHCPクライアントが存在する
- 本社にDHCPサーバが存在する

[本社]

- ルータのIPアドレス　：192.168.2.1
- ネットワークアドレス/ネットマスク　：192.168.2.0/24
- DHCPサーバのIPアドレス　：192.168.2.10

[支社]

- 本装置の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

こんな事に気をつけて

Si-R220Bでは、利用物理回線設定でスロット番号に“mb”を指定してください。

ここでは、本社、支社のネットワークがすでに専用線接続されていることを前提としています。

☛ 参照 「1.10 事業所LANを専用線で接続する」（P.30）

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。

支社を設定する

● コマンド

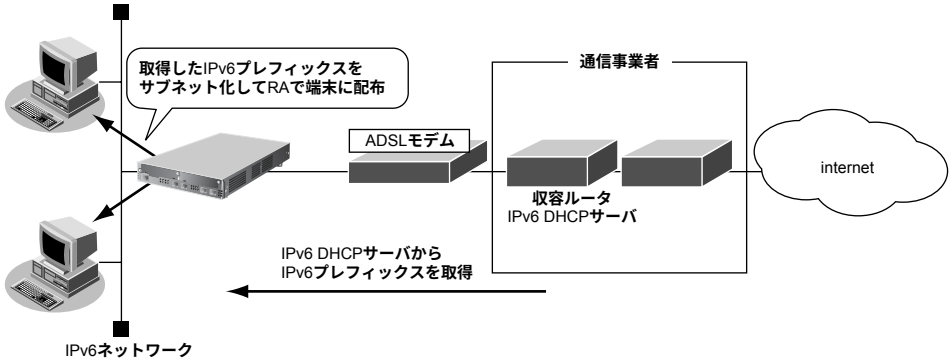
```
事務所 LAN を専用線で接続する
# wan 0 bind 0
# wan 0 line hsd 128k
# lan 0 ip address 192.168.1.1/24 3
# remote 0 name kaisya
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink bind wan 0
# remote 0 ip route 0 192.168.2.1/24 1
# save
# reset

DHCP リレーエージェント機能を設定する
# lan 0 ip dhcp service relay 192.168.2.10

設定終了
# save
# commit
```

2.22.5　IPv6 DHCP クライアント機能を使う

適用機種　全機種

IPv6 DHCP クライアント機能は、プロバイダの IPv6 DHCP サーバから IPv6 プレフィックスなどの情報を取得する機能です。この機能を利用すると、プロバイダから取得した IPv6 プレフィックスをサブネット化して、Router Advertisement Message（RA）で下流ネットワークに 64 ビットの IPv6 プレフィックスを配布することができます。

ここでは、PPPoE でインターネットに接続して、IPv6 DHCP クライア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

- PPPoE で使用する LAN ポート　：LAN0 ポート
- ユーザ認証 ID　：userid
- ユーザ認証パスワード　：userpass
- IPv6 DHCP サーバから取得する IPv6 プレフィックス長　：48 ビット
- IPv6 プレフィックスを配布する LAN ポート　：LAN1 ポート
- RA で配布する IPv6 プレフィックスのサブネット ID　：0001

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

```
ADSL モデムに接続するインタフェースを設定する
# delete lan 0
# lan 0 mode auto

接続先の情報を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 keep connect
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ip6 use on

IPv6 DHCP クライアントを設定する
# remote 0 ip6 dhcp service client

ProxyDNS を設定する
# proxydns domain 0 any * any on 0
# proxydns address 0 any on 0

LAN 情報を設定する
# lan 1 ip6 use on
# lan 1 ip6 address 0 dhcp@rmt0:1::/64 infinity infinity
# lan 1 ip6 ra mode send

設定終了
# save

再起動
# reset
```

2.23 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。

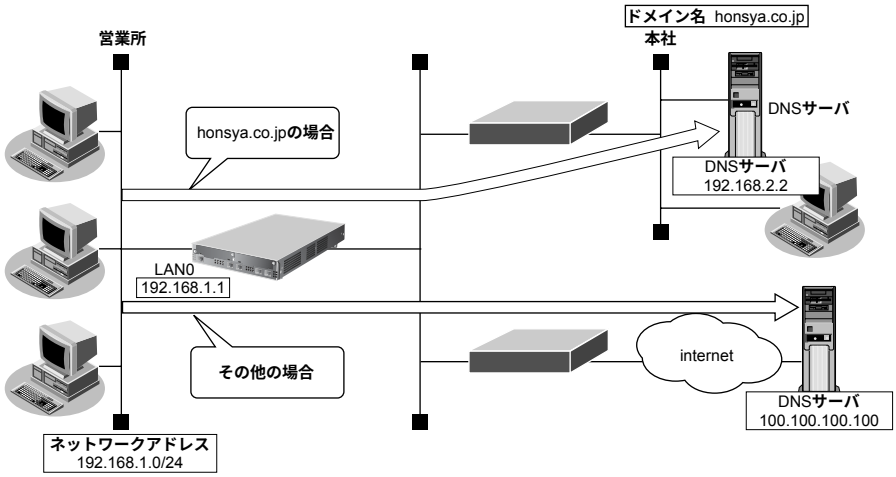
- DNS サーバの自動切り替え機能
- DNS サーバアドレスの自動取得機能
- DNS 問い合わせタイプフィルタ機能
- DNS サーバ機能

参照　Si-R シリーズ　機能説明書「2.21 DNS サーバ機能」（P.90）

2.23.1 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

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。

こんな事に気をつけて

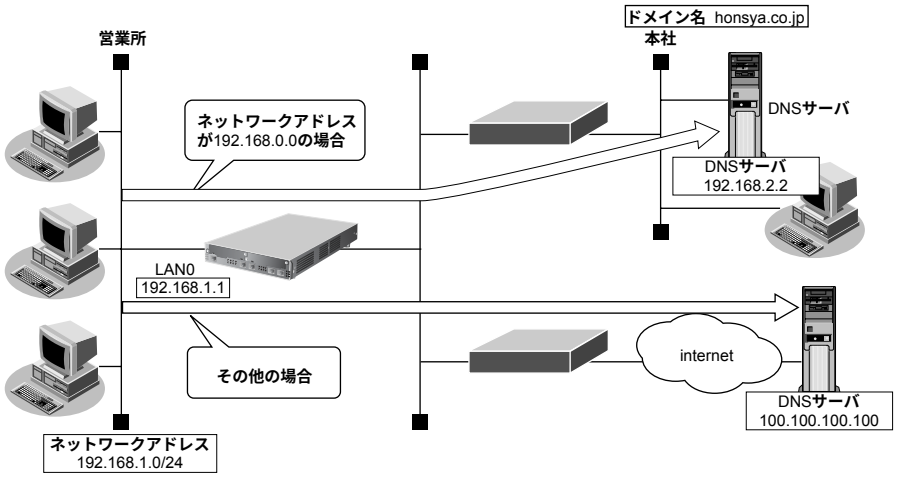
コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

☛ 参照 Si-R シリーズ　コマンドユーザーズガイド「1.7 コマンドで入力できる文字一覧」（P.26）

2.23.2　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
  使用する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
  使用する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 Si-R シリーズ　コマンドユーザーズガイド「1.7 コマンドで入力できる文字一覧」（P.26）

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。

2.23.3　DNS サーバアドレスの自動取得機能を使う

適用機種　全機種

この機能を利用すると、ProxyDNS が DNS サーバのアドレスを、回線接続時に接続先から自動的に取得します。そのため、DNS サーバのアドレスを、あらかじめ設定しておく必要はありません。

なお、この機能は、接続先が DNS サーバアドレスの配布機能（RFC1877）に対応している場合にだけ利用できます。

● 設定条件

- ドメイン名　：*
- 動作　：接続先の DNS サーバへ指定ネットワークを経由して問い合わせる

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　Si-R シリーズ　コマンドユーザーズガイド「1.7 コマンドで入力できる文字一覧」（P.26）

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 サーバアドレスの自動取得機能を設定する
# proxydns domain 0 any * any on 0 off

設定終了
# save
# commit
```

パソコン側の設定を行う

ここでは、Windows® 2000の場合を例に説明します。

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

ヒント

◆ 本装置の「DHCPサーバ機能」を使わない場合の設定は？

パソコン側の「DNS設定」で本装置のIPアドレスを指定すると、ProxyDNS機能だけ使用できます。また、本装置以外のDHCPサーバを使用している場合でも、DHCPサーバで広報するDNSサーバのIPアドレスとして本装置のIPアドレスを指定するとProxyDNS機能を使用できます。

◆ DNS解決したホストへのホスト経路を自動で作成する設定は？

以下のコマンドを設定することにより、DNS解決したホストへのホスト経路を自動で作成することができます。

```
# proxydns domain 0 any * any on 0 on
```

◆「接続先のDNSサーバへ問い合わせる」と「接続先のDNSサーバへ指定ネットワークを経由して問い合わせる」の違いは？

「接続先のDNSサーバへ問い合わせる」は、経路情報に従って、接続先から取得したDNSサーバへ問い合わせるのに対して、「接続先のDNSサーバへ指定ネットワークを経由して問い合わせる」は、経路情報を無視して指定ネットワークを経由して、接続先から取得したDNSサーバへ問い合わせます。

2.23.4　DNS サーバアドレスを DHCP サーバから取得して使う

適用機種　全機種

この機能を利用すると、ProxyDNS が DNS サーバのアドレスを、DHCP サーバから自動的に取得します。そのため、DNS サーバのアドレスを、あらかじめ設定しておく必要はありません。

なお、この機能は、DHCP サーバが DNS サーバのアドレスを広報している場合にだけ利用できます。

● 設定条件

- ドメイン名　：＊
- 動作　：lan0 の DNS サーバへ問い合わせる

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 Si-R シリーズ　コマンドユーザーズガイド「1.7 コマンドで入力できる文字一覧」（P.26）

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 サーバアドレスの自動取得機能を設定する
# proxydns domain 0 any * any dhcp lan0

設定終了
# save
# commit
```

パソコン側の設定を行う

ここでは、Windows® 2000の場合を例に説明します。

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

ヒント

◆ 本装置の「DHCPサーバ機能」を使わない場合の設定は？

パソコン側の「DNS設定」で本装置のIPアドレスを指定すると、ProxyDNS機能だけ使用できます。また、本装置以外のDHCPサーバを使用している場合でも、DHCPサーバで広報するDNSサーバのIPアドレスとして本装置のIPアドレスを指定するとProxyDNS機能を使用できます。

◆ DNS解決したホストへのホスト経路を自動で作成する設定は？

以下のコマンドを設定することにより、DNS解決したホストへのホスト経路を自動で作成することができます。

```
# proxydns domain 0 any * any on 0 on
```

◆「接続先のDNSサーバへ問い合わせる」と「接続先のDNSサーバへ指定ネットワークを経由して問い合わせる」の違いは？

「接続先のDNSサーバへ問い合わせる」は、経路情報に従って、接続先から取得したDNSサーバへ問い合わせるのに対して、「接続先のDNSサーバへ指定ネットワークを経由して問い合わせる」は、経路情報を無視して指定ネットワークを経由して、接続先から取得したDNSサーバへ問い合わせます。

2.23.5　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。たとえば、Windows® 2000 が送信する予期しない DNS パケットによって、自動発信する問題を回避するために、かんたん設定のかんたんフィルタを「使用する」に設定します。このとき、問い合わせタイプが SOA（6）と SRV（33）のパケットを破棄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

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 Si-R シリーズ　コマンドユーザーズガイド「1.7 コマンドで入力できる文字一覧」（P.26）

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

パソコン側の設定を行います。

設定方法は、「2.23.3 DNS サーバアドレスの自動取得機能を使う」（P.315）の「パソコン側の設定を行う」（P.316）を参照してください。

2.23.6　DNS サーバ機能を使う

適用機種　全機種

本装置のホストデータベースにホスト名と IP アドレスを登録します。登録したホストに対して DNS 要求があった場合は、ProxyDNS が DNS サーバの代わりに応答します。LAN 内の情報をホストデータベースにあらかじめ登録しておくと、LAN 内のホストの DNS 要求によって回線が接続されるといったトラブルを防止できます。

● 設定条件

- ホスト名　：host.com
- IPv4 アドレス　：192.168.1.2
- IPv6 アドレス　：2001:db8::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 Si-R シリーズ　コマンドユーザーズガイド「1.7 コマンドで入力できる文字一覧」（P.26）

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
# host 0 ip6 address 2001:db8::2

設定終了
# save
# commit
```

補足　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。

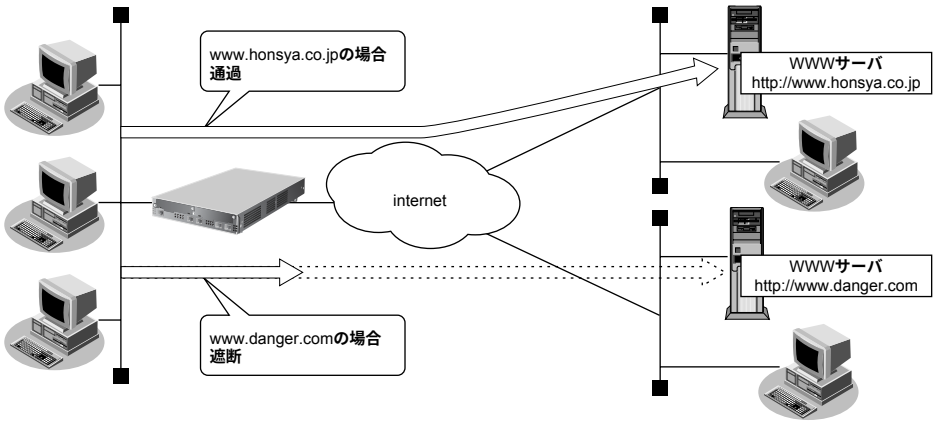
設定方法は、「2.23.3 DNS サーバアドレスの自動取得機能を使う」（P.315）の「パソコン側の設定を行う」（P.316）を参照してください。

2.24 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　Si-R シリーズ　機能説明書「2.21 DNS サーバ機能」（P.90）

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

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　Si-R シリーズ　コマンドユーザーズガイド「1.7 コマンドで入力できる文字一覧」（P.26）

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

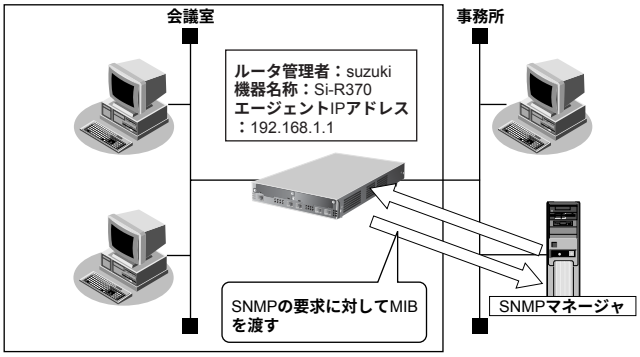
URL の情報を設定する
proxydns domain 0 any www.danger.com any reject
proxydns domain 1 any * any on 0

設定終了
save
commit

2.25 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、Si-R370 が SNMP マネージャに対して MIB 情報を通知する場合の設定方法を説明します。



参照 Si-R シリーズ　機能説明書「2.22 SNMP 機能」（P.92）

ヒント

◆ SNMP とは？

SNMP（Simple Network Management Protocol）は、ネットワーク管理用のプロトコルです。SNMP マネージャは、ネットワーク上の端末の稼動状態や障害状況を一元管理します。SNMP エージェントは、マネージャの要求に対して 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 trap という機能を用いて、エージェントからマネージャに対して非同期通知を行うことができます。エージェントは、エージェントが起動されたときに Trap を送信します。

参照 Si-R シリーズ　仕様一覧「3.1 標準 MIB 定義」（P.45）、「3.2 富士通拡張 MIB」（P.68）、「3.3 Trap 一覧」（P.71）

● 設定条件

- SNMP エージェント機能を使用する
- ルータ管理者　：suzuki
- 機器名称　：Si-R370
- 機器設置場所　：1 階（1F）
- エージェントアドレス　：192.168.1.1（自装置 IP アドレス）
- SNMP ホスト情報　：任意のホストを対象
  コミュニティ名　：public

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 エージェント機能を設定する
snmp agent contact suzuki
snmp agent sysname Si-R370
snmp agent location 1F
snmp agent address 192.168.1.1
snmp manager 0 0.0.0.0 public off disable
snmp service on

設定終了
save
commit

こんな事に気をつけて

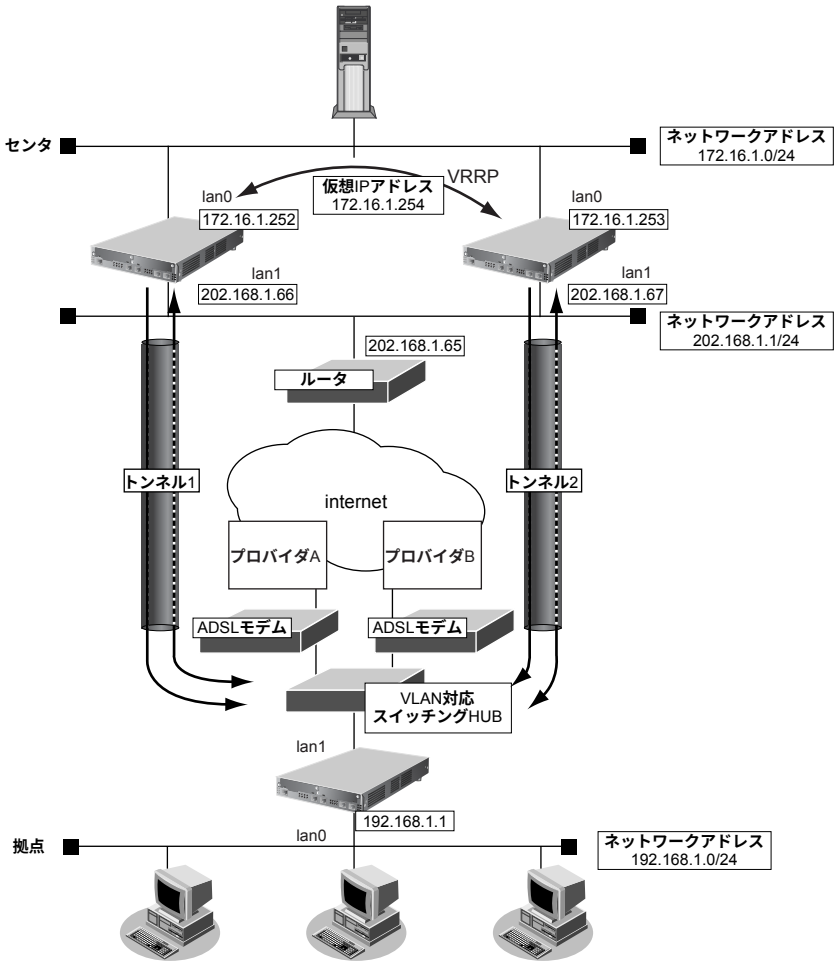
- エージェントアドレスには、本装置に設定されたどれかのインタフェースの IP アドレスを設定します。誤った IP アドレスを設定した場合は、SNMP マネージャとの通信ができなくなります。
- ATM 網によっては、物理リンクが確立してから通信ができるようになるまでに時間がかかるものがあります。装置起動時に、ATM 網の先の SNMP マネージャに送信した trap が、相手に正常に届かない場合があります。

2.26 ECMP 機能を使う

適用機種　全機種

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。

ADSL では、受信速度は高速ですが、送信速度はそれほど高速ではありません。この例では、ADSL を 2 本利用して負荷を分散することで、送信速度の向上をはかります。さらに、片方のトンネルに障害が発生した場合に、通信可能なトンネルを利用して通信のバックアップを実現します。



参照 Si-R シリーズ　機能説明書「2.23 ECMP 機能」（P.93）

● 設定条件

- 拠点では、センタへの通信は、トンネル 1 とトンネル 2 を利用して負荷分散して送信します。どちらかのトンネルで通信障害が発生した場合は、通信可能なトンネルだけを利用して送信します。
- センタでは、拠点への通信は、トンネル 1 だけを利用して送信します。トンネル 1 で通信障害が発生した場合は、トンネル 2 を利用して送信します。
- トンネル 1 の通信障害は、両端の本装置が接続先監視で検出します。
  この監視は、ISP A の通信障害およびセンタ側本装置（左）の故障を検出します。
- トンネル 2 の通信障害は、両端の本装置が接続先監視で検出します。
  この監視は、ISP B の通信障害およびセンタ側本装置（右）の故障を検出します。

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

[センタ側本装置（左）]

Si-R180 の場合は、まず以下のコマンドで LAN ポートを削除します。

```
LAN ポートを削除する
# delete lan
```

Si-R180 以外の機種の場合は、以下のコマンドから設定します。

```
LAN0 側を設定する
# lan 0 ip address 172.16.1.252/24 3
# lan 0 vrrp use on
# lan 0 vrrp group 0 id 10 254 172.16.1.254
# lan 0 vrrp group 0 trigger 0 ifdown rmt0

IPsec に関する ACL を設定する
# acl 0 ip 202.168.1.66/32 any 17 any
# acl 0 udp 500 500
# acl 1 ip 202.168.1.66/32 any 50 any

LAN1 側を設定する
# lan 1 ip address 202.168.1.66/24 3
# lan 1 ip route 0 default 202.168.1.65 1 0
# lan 1 ip filter 0 pass acl 0 reverse
# lan 1 ip filter 1 pass acl 1 reverse
# lan 1 ip filter default reject

トンネルを設定する
# remote 0 name RMTbyA
# remote 0 ip route 0 192.168.1.0/24 1 0
# remote 0 ip msschange 1360
# remote 0 mtu 1400
# remote 0 ap 0 name IPsecbyA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.1.66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 any4
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ipsec ike pfs modp768
# remote 0 ap 0 ike name remote RMTbyA
# remote 0 ap 0 ike shared key text 12345678-A
# remote 0 ap 0 ike proposal 0 encrypt des-cbc
# remote 0 ap 0 sessionwatch address 172.16.1.252 192.168.1.1
# remote 0 ap 0 sessionwatch interval 5s 1m 5s

設定終了
# save
# commit
```

[センタ側本装置（右）]

Si-R180 の場合は、まず以下のコマンドで LAN ポートを削除します。

```
LAN ポートを削除する
# delete lan
```

Si-R180 以外の機種の場合は、以下のコマンドから設定します。

```
LAN0 側を設定する
# lan 0 ip address 172.16.1.253/24 3
# lan 0 vrrp use on
# lan 0 vrrp group 0 id 10 100 172.16.1.254
# lan 0 vrrp group 0 trigger 0 ifdown rmt0

IPsec に関する ACL を設定する
# acl 0 ip 202.168.1.67/32 any 17 any
# acl 0 udp 500 500
# acl 1 ip 202.168.1.67/32 any 50 any

LAN1 側を設定する
# lan 1 ip address 202.168.1.67/24 3
# lan 1 ip route 0 default 202.168.1.65 1 0
# lan 1 ip filter 0 pass acl 0 reverse
# lan 1 ip filter 1 pass acl 1 reverse
# lan 1 ip filter default reject

トンネルを設定する
# remote 0 name RMTbyB
# remote 0 ip route 0 192.168.1.0/24 1 0
# remote 0 ip msschange 1360
# remote 0 mtu 1400
# remote 0 ap 0 name IPsecbyB
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.1.67
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 any4
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ipsec ike pfs modp768
# remote 0 ap 0 ike name remote RMTbyB
# remote 0 ap 0 ike shared key text 12345678-B
# remote 0 ap 0 ike proposal 0 encrypt des-cbc
# remote 0 ap 0 sessionwatch address 172.16.1.253 192.168.1.1
# remote 0 ap 0 sessionwatch interval 5s 1m 5s

設定終了
# save
# commit
```

[拠点側本装置]

Si-R180 の場合は、まず以下のコマンドで LAN ポートを削除します。

```
LAN ポートを削除する
# delete lan
```

Si-R180 以外の機種の場合は、以下のコマンドから設定します。

```
LAN のアドレスを設定する
# lan 0 ip address 192.168.1.1/24 3

PPPoE で利用する LAN を設定する
# lan 1 mode auto
# lan 2 vlan bind 1
# lan 2 vlan tag vid 10
# lan 3 vlan bind 1
# lan 3 vlan tag vid 20

IPsec に関する ACL を設定する
# acl 0 ip any 202.168.1.66/32 17 any
# acl 0 udp 500 500
# acl 1 ip any 202.168.1.66/32 50 any
# acl 2 ip any 202.168.1.67/32 17 any
# acl 2 udp 500 500
# acl 3 ip any 202.168.1.67/32 50 any

プロバイダ A を利用する PPPoE 接続を設定する
# remote 0 name INTER-A
# remote 0 ip route 0 202.168.1.66/32 1 0
# remote 0 ip filter 0 pass acl 0 reverse
# remote 0 ip filter 1 pass acl 1 reverse
# remote 0 ip filter default reject
# remote 0 ip msschange 1414
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-A
# remote 0 ap 0 datalink bind lan 2
# remote 0 ap 0 ppp auth send UIDtoA PASStoA
# remote 0 ap 0 keep connect
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50

プロバイダ B を利用する PPPoE 接続を設定する
# remote 1 name INTER-B
# remote 1 ip route 0 202.168.1.67/32 1 0
# remote 1 ip filter 0 pass acl 2 reverse
# remote 1 ip filter 1 pass acl 3 reverse
# remote 1 ip filter default reject
# remote 1 ip msschange 1414
# remote 1 mtu 1454
# remote 1 ap 0 name ISP-B
# remote 1 ap 0 datalink bind lan 3
# remote 1 ap 0 ppp auth send UIDtoB PASStoB
# remote 1 ap 0 keep connect
# remote 1 ip nat mode multi any 1 5m
# remote 1 ip nat static 0 192.168.1.1 500 any 500 17
# remote 1 ip nat static 1 192.168.1.1 any any any 50
```

センタ側本装置（左）とのトンネルを設定する
remote 2 name CENTER-A
remote 2 ip route 0 172.16.1.0/24 1 1
remote 2 ip msschange 1360
remote 2 mtu 1400
remote 2 ap 0 name IPsecbyA
remote 2 ap 0 datalink type ipsec
remote 2 ap 0 tunnel remote 202.168.1.66
remote 2 ap 0 ipsec type ike
remote 2 ap 0 ipsec ike protocol esp
remote 2 ap 0 ipsec ike range any4 any4
remote 2 ap 0 ipsec ike encrypt des-cbc
remote 2 ap 0 ipsec ike auth hmac-md5
remote 2 ap 0 ipsec ike pfs modp768
remote 2 ap 0 ike name local RMTbyA
remote 2 ap 0 ike shared key text 12345678-A
remote 2 ap 0 ike proposal 0 encrypt des-cbc
remote 2 ap 0 sessionwatch address 192.168.1.1 172.16.1.252
remote 2 ap 0 sessionwatch interval 5s 1m 5s

センタ側本装置（右）とのトンネルを設定する
remote 3 name CENTER-B
remote 3 ip route 0 172.16.1.0/24 1 1
remote 3 ip msschange 1360
remote 3 mtu 1400
remote 3 ap 0 name IPsecbyB
remote 3 ap 0 datalink type ipsec
remote 3 ap 0 tunnel remote 202.168.1.67
remote 3 ap 0 ipsec type ike
remote 3 ap 0 ipsec ike protocol esp
remote 3 ap 0 ipsec ike range any4 any4
remote 3 ap 0 ipsec ike encrypt des-cbc
remote 3 ap 0 ipsec ike auth hmac-md5
remote 3 ap 0 ipsec ike pfs modp768
remote 3 ap 0 ike name local RMTbyB
remote 3 ap 0 ike shared key text 12345678-B
remote 3 ap 0 ike proposal 0 encrypt des-cbc
remote 3 ap 0 sessionwatch address 192.168.1.1 172.16.1.253
remote 3 ap 0 sessionwatch interval 5s 1m 5s

ECMP を設定する
routemanage ip ecmp mode hash

設定終了
save
commit

2.27 VRRP 機能を使う

適用機種　全機種

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 Si-R シリーズ　機能説明書「2.24 VRRP 機能」（P.96）

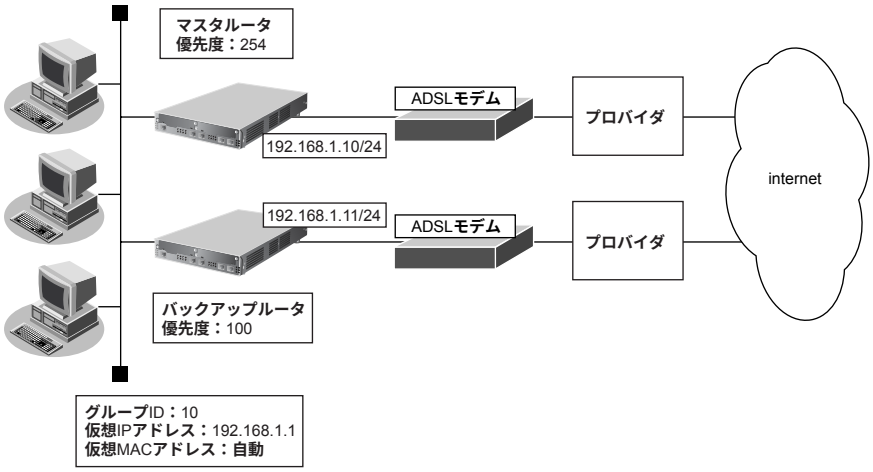
こんな事に気をつけて

- **本装置の電源の投入、マスタ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。**
- **ルータに設定する IP アドレスと仮想 IP アドレスには、異なる IP アドレスを設定することをお勧めします。同じ IP アドレスを設定した場合、その IP アドレスで装置にアクセスすることはできなくなります。同じにした場合、必ず、VRRP グループの VRRP ルータの優先度を “master” に設定してください（VRRP ルータの優先度として "master" を設定した場合、仮想 IP アドレスは設定できません）。**
- **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。**
  あて先 IP アドレス　：224.0.0.18
  プロトコル番号　：112

2.27.1　簡易ホットスタンバイ機能を使う

適用機種　全機種

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できます。2台のルータをPPPoEでインターネットに接続して、ホットスタンバイを構成する場合の設定方法を説明します。



● 設定条件

- 故障発生後の切り戻しは手動で行う
- マスタルータはWAN側経路をノードダウントリガによって監視する

[マスタルータ]

- PPPoEで使用するLANポート　：LAN0ポート
- 本装置のIPアドレス/ネットマスク　：192.168.1.10/24
- ユーザ認証ID　：userid
- ユーザ認証パスワード　：userpass
- 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]

- PPPoEで使用するLANポート　：LAN0ポート
- 本装置のIPアドレス/ネットマスク　：192.168.1.11/24
- ユーザ認証ID　：userid2
- ユーザ認証パスワード　：userpass2

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]

```
ADSL モデムに接続するインタフェースを設定する
# delete lan
# lan 0 ip address 0.0.0.0/0 3
# lan 0 mode auto

本装置の IP アドレスを設定する
# lan 1 ip address 192.168.1.10/24 3

接続先の情報を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass

VRRP を設定する（ノードダウントリガを使用する）
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 10 254 192.168.1.1
# 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

再起動
# reset
```

[バックアップルータの設定]

```
ADSL モデムに接続するインタフェースを設定する
# delete lan
# lan 0 ip address 0.0.0.0/0 3
# lan 0 mode auto

本装置の IP アドレスを設定する
# lan 1 ip address 192.168.1.11/24 3

接続先の情報を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid2 userpass2

VRRP を設定する
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 10 100 192.168.1.1
# lan 1 vrrp group 0 preempt on

設定終了
# save

再起動
# reset
```

上の設定例で、インタフェースダウントリガを使用して WAN 側（PPPoE）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

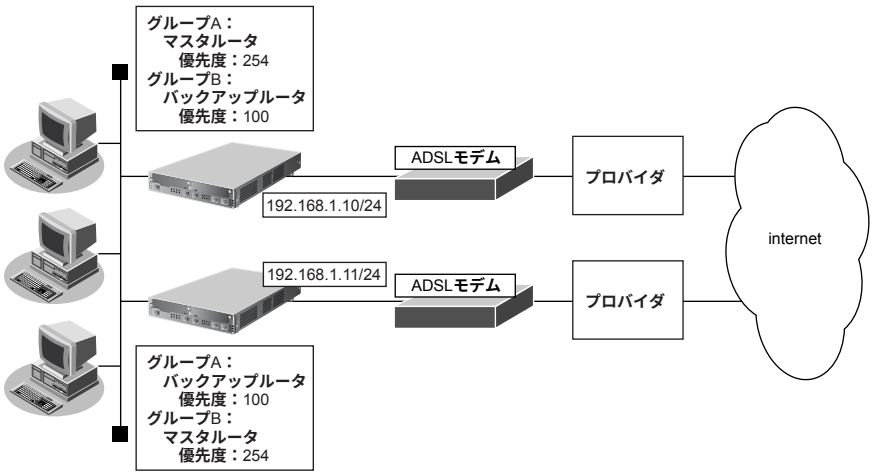
[マスタルータの設定]

```
# lan 1 vrrp 0 trigger 0 ifdown rmt0
```

2.27.2　クラスタリング機能を使う

適用機種　全機種

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。2 台のルータを PPPoE でインターネットに接続する場合の設定方法を説明します。



● 設定条件

- 故障発生後の切り戻しは手動で行う
- マスタルータは PPPoE 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

[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

[マスタルータ]

- PPPoE で使用する LAN ポート　：LAN0 ポート
- 本装置の IP アドレス/ネットマスク　：192.168.1.10/24
- ユーザ認証 ID　：userid
- ユーザ認証パスワード　：userpass

[バックアップルータ]

- PPPoE で使用する LAN ポート　：LAN0 ポート
- 本装置の IP アドレス/ネットマスク　：192.168.1.11/24
- ユーザ認証 ID　：userid2
- ユーザ認証パスワード　：userpass2

こんな事に気をつけて

クラスタリング機能を有効に利用するには、PC からのトラフィック量に応じて、PC 側で設定するデフォルトルートの定義を適切に分散する必要があります。

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

[マスタルータの設定]

```
ADSL モデムに接続するインタフェースを設定する
# delete lan
# lan 0 ip address 0.0.0.0/0 3
# lan 0 mode auto

本装置の IP アドレスを設定する
# lan 1 ip address 192.168.1.10/24 3

接続先の情報を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass

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 1 vrrp use on
# lan 1 vrrp group 0 id 10 254 192.168.1.1
# lan 1 vrrp group 0 preempt off
# lan 1 vrrp group 0 trigger 0 ifdown rmt0 254
# lan 1 vrrp group 1 id 11 100 192.168.1.2

設定終了
# save

再起動
# reset
```

[バックアップルータの設定]

```
ADSL モデムに接続するインタフェースを設定する
# delete lan
# lan 0 ip address 0.0.0.0/0 3
# lan 0 mode auto

本装置の IP アドレスを設定する
# lan 1 ip address 192.168.1.11/24 3

接続先の情報を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid2 userpass2

VRRP を設定する
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 10 100 192.168.1.1
# lan 1 vrrp group 1 id 11 254 192.168.1.2
# lan 1 vrrp group 1 preempt off
# lan 1 vrrp group 1 trigger 0 ifdown rmt0 254

設定終了
# save

再起動
# reset
```

2.28 ポリシールーティング機能を使う

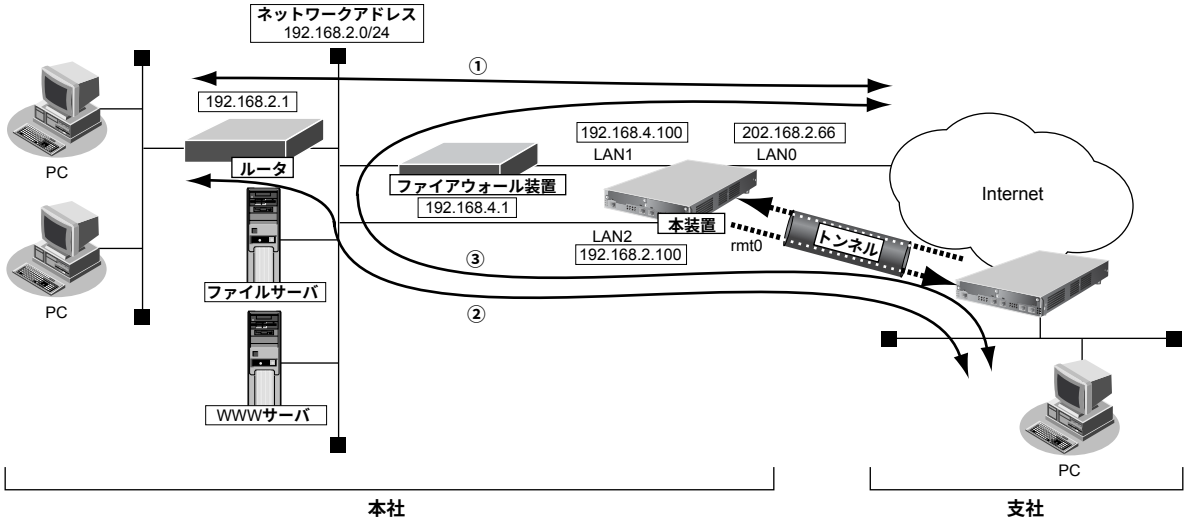
適用機種　全機種

本装置では、入力側でポリシールーティングを行う Ingress ポリシールーティングと、出力側でポリシールーティングを行うマルチルーティングの 2 つを設定することができます。

2.28.1 Ingress ポリシールーティング機能を使う

適用機種　全機種

Ingress ポリシールーティング機能とは、ルーティングによる経路情報の参照前に、入力パケットのあて先 IP アドレスだけではなく、送信元 IP アドレスやポート番号などの情報も利用して、設定した送出先へパケットを転送する機能です。この機能を利用することによって、受信インタフェースごとに経路情報に従わないパケット転送を行うことができます。ここでは、支社←→本社は本社ネットワークのファイアウォールを通さずに通信し、支社←→インターネットは本社ネットワークのファイアウォールを通して通信する場合の設定方法を説明します。



● 前提条件

- 本社←→インターネットの通信パス（①の通信パス）
  - 本社の本装置にインターネットへの通信が設定済み（lan 0）
- 支社←→本社の通信パス（②の通信パス）
  - 本社の本装置に IPsec を利用した VPN 通信が設定済み（remote 0 ap 0）

● 設定条件

- 支社←→インターネットの通信は、本社のファイアウォールを経由する（③の通信パス）
  - lan 0 インタフェースに、本装置あてパケット以外を lan1 の 192.168.4.1（ファイアウォール）に転送する Ingress ポリシールーティングを設定する
  - remote 0 インタフェースに、本装置あてパケット以外を lan2 の 192.168.2.1 に転送する Ingress ポリシールーティングを設定する

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。

● コマンド

```
本装置あて IPv4 パケットに一致する ACL 定義を設定する
# acl 0 ip any 202.168.2.66/32 any

すべての IPv4 パケットに一致する ACL 定義を設定する
# acl 1 ip any any any

本装置あてパケット以外を lan1 の 192.168.4.1 に転送するポリシーグループを設定する
# policy-group 0 pattern 0 unmatch acl 0
# policy-group 0 pattern 1 match acl 1
# policy-group 0 interface lan1
# policy-group 0 nexthop 192.168.4.1

本装置あてパケット以外を lan2 の 192.168.2.1 に転送するポリシーグループを設定する
# policy-group 1 pattern 0 unmatch acl 0
# policy-group 1 pattern 1 match acl 1
# policy-group 1 interface lan2
# policy-group 1 nexthop 192.168.2.1

lan 0 インタフェースに Ingress ポリシールーティングを設定する
# lan 0 ip in-policy 0 policy-group 0

remote 0 インタフェースに Ingress ポリシールーティングを設定する
# remote 0 ip in-policy 0 policy-group 1

設定終了
# save
# commit
```

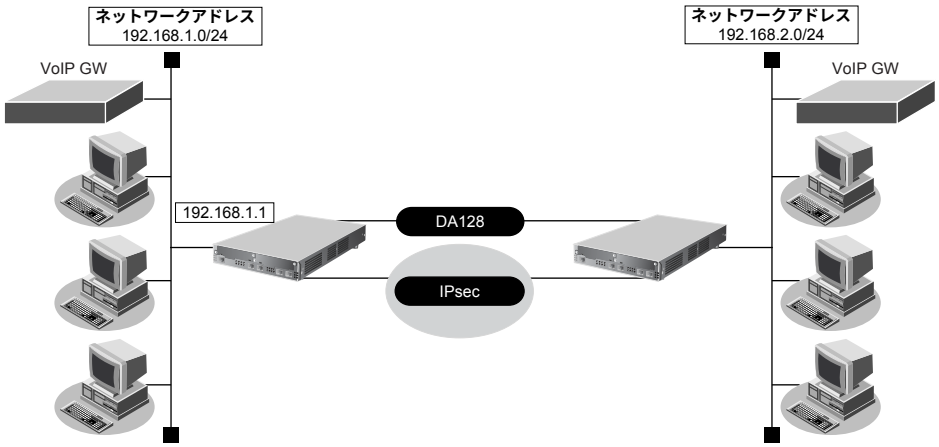
こんな事に気をつけて

Ingress ポリシールーティング機能は、パケット選択ルールに一致した場合、ブロードキャストパケットやマルチキャストパケット、本装置あてパケットも転送します。

2.28.2　マルチルーティング機能を使う

適用機種　全機種

マルチルーティング機能を使用すると、同じあて先ネットワークへの送信データを、別の通信パスを利用して送信することができます。



● 設定条件

- IPsec を利用した VPN 通信が設定済み（remote 0 ap 0）

参照 「2.13.1 IPv4 over IPv4 で固定 IP アドレスでの VPN（手動鍵交換）」（P.178）

- 新規に音声データ用の専用線（BRI:128Kbps）を追加する
- 通常、音声データ（TOS 値：a0）は専用線を利用する
- 通常、その他のデータは IP-VPN を利用する
- 専用線（音声用）がダウンした場合は、音声データも IP-VPN を使用する
- IP-VPN（データ用）がダウンした場合は、その他のデータも専用線を使用する

こんな事に気をつけて

Si-R220B では、利用物理回線設定でスロット番号に“mb”を指定してください。

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

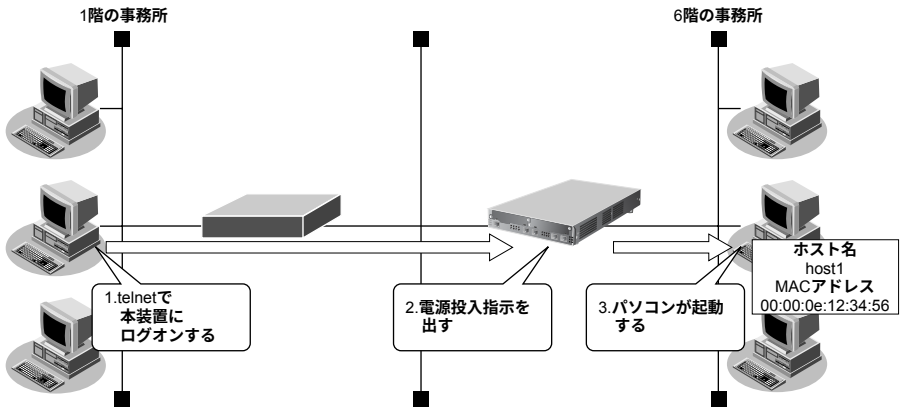
```
専用線を設定する
# wan 0 bind 0
# wan 0 line hsd 128k

通常は IP-VPN を音声データで使用しないように設定する
# remote 0 ap 0 multiroute pattern 0 backup any any any any 0 a0
# remote 0 ap 0 multiroute pattern 1 use any any any any 0 any

専用線の接続先を設定する
# remote 0 ap 1 name hsd
# remote 0 ap 1 datalink bind wan 0

設定終了
# save

再起動
# reset
```

2.29 遠隔地のパソコンを起動させる（リモートパワーオン機能）

適用機種　全機種

リモートパワーオン機能は、本装置につながっている離れた所にあるパソコンを、本装置からWakeup on LAN機能を使用して起動させることができます。

ここでは、1階の事務所のパソコンから6階の事務所のパソコンを起動する場合の設定方法を説明します。



● 設定条件

[本社側]

- 起動するパソコンのホスト名　：host1
- 起動するパソコンのMACアドレス　：00:00:0e:12:34:56

ヒント

◆ Wakeup on LAN機能とは？

AMD社が開発したネットワーク上の電源OFF状態のパソコンを遠隔操作で起動する機能です。起動はMagic Packetと呼ばれるパケットを送付して行います。なお、Wakeup on LAN機能はパソコンを起動するだけで電源OFFは行いません。

電源OFFする場合は、別途、電源制御用ソフトウェアが必要になります。

こんな事に気をつけて

- 本機能は、Wakeup on LANに対応したパソコンだけで利用できます。Wakeup on LAN対応機種については、パソコンのメーカーにお問い合わせください。
- 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 Si-Rシリーズ　コマンドユーザーズガイド「1.7 コマンドで入力できる文字一覧」（P.26）

補足 ホストデータベース情報は「リモートパワーオン機能」、「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。

2.29.1　リモートパワーオン情報を設定する

適用機種　全機種

● 設定コマンド

```
ホストデータベースへ登録する
# host 0 name host1
# host 0 mac 00:00:0e:12:34:56

設定終了
# save
# commit
```

2.29.2　リモートパワーオン機能を使う

適用機種　全機種

1. パソコン上の telnet クライアントから本装置にログオンします。
2. 本装置からコマンドによって、Wakeup on LAN 機能を使用します。

● コマンド

```
# rpon all
```

補足　パソコンが Magic Packet を受信してから起動が完了するまで、数十秒から数分かかります（お使いの機種や OS によって異なります）。

2.30 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には、以下のとおりです。

- スケジュール予約
  特定の動作とそれを行う時間をスケジュール予約情報として登録できます。スケジュール予約情報を登録しておくと、特定時間帯のデータの発着信を制限したり、定期的に課金情報をクリアしたりする作業を、本装置が自動的に行います。スケジュール予約情報は、最大 16 件まで登録できます。
- 電話番号変更予約（Si-R220B、240、370、570）
  指定した日時に構成定義情報の電話番号を一括して変更することができます。電話番号変更予約情報は、最大 4 件まで登録できます。電話番号は、予約情報 1 件に対して 4 つまで登録することができます。
- 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計を正しくセットしてください。

☛ 参照 Si-R シリーズ　コマンドユーザーズガイド「1.2 時計を設定する」（P.12）

2.30.1 スケジュールを予約する

適用機種　全機種

発信抑止を予約する

ここでは、毎日午後 11 時から午前 8 時までの発信を抑止する場合の設定方法を説明します。

● 設定条件

- 動作　：発信抑止
- 日／曜日　：毎日
- 開始時刻　：23:00
- 終了時刻　：08:00

上記の設定条件に従ってスケジュールを予約する場合のコマンド例を示します。

● コマンド

```
スケジュールを予約する
# schedule 0 in any 2300-0800 diallock

設定終了
# save
# commit
```

こんな事に気をつけて

回線接続中に、発信抑止または着信抑止が実行されても、回線は切断されません。

リモートパワーオンを予約する

ここでは、毎朝8時に特定のパソコンを起動する場合の設定方法を説明します。

● 設定条件

- 動作　：リモートパワーオン
- 予約時刻　：08:00
　：毎日

上記の設定条件に従ってリモートパワーオンを予約する場合のコマンド例を示します。

● コマンド

スケジュールを予約する
schedule 0 at any 0800 rpon all

設定終了
save
commit

こんな事に気をつけて

リモートパワーオン機能を利用する場合は、あらかじめ対象とするパソコンの情報を本装置のホストデータベース情報に登録しておく必要があります。スケジュール機能を使ってリモートパワーオンを行うと、host rpon コマンドで off が指定されていないすべてのパソコンが起動します。

☛ 参照 「2.29 遠隔地のパソコンを起動させる（リモートパワーオン機能）」（P.340）

2.30.2　電話番号変更を予約する

適用機種　*Si-R220B,240,370,570*

ここでは、2004年7月1日午前2時に電話番号を「06-123-4567」から「06-6123-4567」に変更する場合の設定方法を説明します。

● 設定条件

- 実行日時　：2004年7月1日　2時00分
- 電話番号変更前情報　：06-123-4567
- 電話番号変更後情報　：06-6123-4567

上記の設定条件に従って電話番号変更を予約する場合のコマンド例を示します。

● コマンド

```
電話番号変更を予約する
# dnconvinfo 0 date 0407010200
# dnconvinfo 0 dial 0 06-123-4567 06-6123-4567

設定終了
# save
# commit
```

こんな事に気をつけて

指定時刻になると自動的に本装置が再起動され、電話番号が更新されます。その際、データ通信中の場合は、回線が切断されます。

2.30.3　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、構成定義情報を内部に2つ持つことができます。

ここでは、2004年7月1日6時30分に構成定義情報を1から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　：2004年7月1日　6時30分
- 構成定義情報切り替え　：構成定義情報1→構成定義情報2

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 0407010630 reset config2

設定終了
# save
# commit
```

2.31 通信料金を節約する（課金制御機能）

適用機種　***Si-R220B,240,370,570***

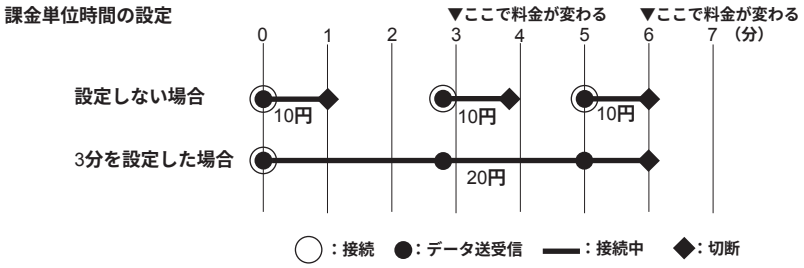
本装置は通信料金を節約するための機能をサポートしています。この機能は、通信料金のむだ、使い過ぎを防ぐことができます。
以下に、各機能について説明します。

● 課金単位時間

ISDN 回線やプロバイダの多くは、一定時間単位で料金を算定する従量課金制度を採用して料金を決めています。通信料金が 3 分 10 円で計算される場合、3 分の中で何度も切断／接続を繰り返すと、料金額はその回数× 10 円になります。

そこで課金単位時間（通信料金が計算されるときの単位時間）を設定し、無通信監視タイマ（初期値：60 秒）と連動することで、単位時間内は回線を切断させないようにします。無通信監視タイマとは、設定した時間を超えてアクセスがなければ自動的に切断するという機能です。

課金単位時間に 3 分間を指定した場合、以下のようになります。



● 課金制御機能（発信抑止／強制切断）

データ通信に費やした通信時間や通信料金が一定の値を超えた場合、接続を禁止したり、ログにアラームを出したりする課金制御機能（発信抑止）もあります。また、Si-R240 のデータ通信カード接続では、通信時間や送受信パケット数の累計が一定の値を超えた場合、接続中の回線を切断し、以降の手動および自動発信を禁止する課金制御機能（強制切断）もあります。無意識のうちに通信料金を使いすぎるのを防ぐことができます。

こんな事に気をつけて

- **設定前に本装置の内部時計を正しくセットしてください。**
- **課金制御機能（発信抑止）は、指定された料金を超えた場合に発信を制御する機能であり、運用中の回線を切断する機能ではありません。回線の接続中に指定された料金を超えても、回線を接続したままだと料金がかかり続けます。その結果、通信料金が指定した金額を超えてしまうのでご注意ください。**
- **モデムでは、回線の切断に時間がかかるため、課金単位を超えて切断される場合があります。**
- **通信料金による課金制御機能（発信抑止）は、ISDN 接続の場合のみ有効です。**

2.31.1　課金単位時間を設定する

適用機種　***Si-R220B,240,370,570***

ここでは、相手情報として remote0、接続先情報として ap0 がすでに登録済みであることを前提とします。

● 設定条件

- 無通信監視タイマ　：60 秒
- 課金単位時間
  昼間（08:00 ～ 19:00）　：180 秒
  夜間（19:00 ～ 23:00）　：180 秒
  深夜・早朝（23:00 ～ 08:00）　：240 秒

上記の設定条件に従って課金単位時間を設定する場合のコマンド例を示します。

● コマンド

```
課金単位時間を設定する
# remote 0 ap 0 idle 1m
# remote 0 ap 0 step 1800
# remote 0 ap 0 step2 1800
# remote 0 ap 0 step3 2400

設定終了
# save
# commit
```

2.31.2　課金制御機能（発信抑止）を設定する

適用機種　***Si-R220B,370,570***

ここでは、接続累計時間が 50 時間、または通信料金の合計が 10,000 円になると接続要求を抑止する場合の設定方法を示します。

● 設定条件

- 通信時間累計の上限時間　：50 時間
- 通信料金の上限金額　：10,000 円

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

```
課金制御機能を設定する
# wan 0 isdn limit time 50h yes
# wan 0 isdn limit charge 10000 yes

設定終了
# save
# commit
```

補足　「wan <number> isdn limit」「diallock」パラメタで「no」を指定した場合は、設定した通信時間累計の上限、または通信料金の上限を超えたときに、システムログ情報に警告通知を記録します。

こんな事に気をつけて

- **本書の表記で使われる通信料金とは、INS ネット 64 基本サービスの「料金情報通知」をもとに、本装置のソフトウェアが算出した値です。算出される値は、お客様の契約や回線利用状況によって異なりますので、請求金額とは必ずしも一致しません。**
  たとえば以下のような場合があります。
  - **INS テレホーダイサービス利用時**
  - **各種料金割り引きサービス利用時**
- **本装置の電源を切ると、課金情報（通信時間累計、通信料金累計など）はすべてクリアされます。**

2.32 ブリッジ／STP 機能を使う

適用機種　全機種

ここでは、ブリッジで FNA をつないで STP 機能を使用する場合、ブリッジグルーピング機能を使用する場合および IP トンネルでブリッジ通信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

- **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 Si-R シリーズ　コマンドユーザーズガイド「1.7 コマンドで入力できる文字一覧」（P.26）

- **STP 機能は、グループ 0 でだけ動作します。VLAN インタフェースでは、STP を使用できません。**
- **WAN インタフェースでブリッジを利用する場合は、1 つの相手情報（remote）に対して、1 つの接続先情報（ap）となるように設計してください。**
- **本装置では、ファームウェアの更新や SNMP での監視などの目的で IPv4 の IP アドレスを使用します。そのため、IPv4 の IP アドレスを設定しないで運用することはできません。IPv6 およびブリッジだけを使用しているネットワークで運用する場合でも、どれかの LAN インタフェースに必ず IPv4 の IP アドレスを設定してください。**
- **VLAN でバインドされたインタフェースでブリッジを行うことはできません。**
- **本装置のブリッジ MAC 学習は、異なる VLAN 上で同一の MAC アドレスを学習することはできません。本装置は、唯一装置がもつ学習テーブルを各 VLAN が共有する SVL（Shared VLAN Learning）と呼ばれる方式で学習を行っています。VLAN インタフェースでブリッジを行う場合は、異なる VLAN 上に同一の MAC アドレスを持つネットワークと接続しないでください。**
- **設定を間違えてループ構成を構成し、ブロードキャストストームが発生してコンソールなどが反応しなくなった場合は、ブリッジが有効な WAN や LAN のケーブルを抜くとブロードキャストストームが収まります。ブロードキャストストームが収まったところで設定を修正してください。**

2.32.1 ブリッジで FNA をつないで STP 機能を使う

適用機種　全機種

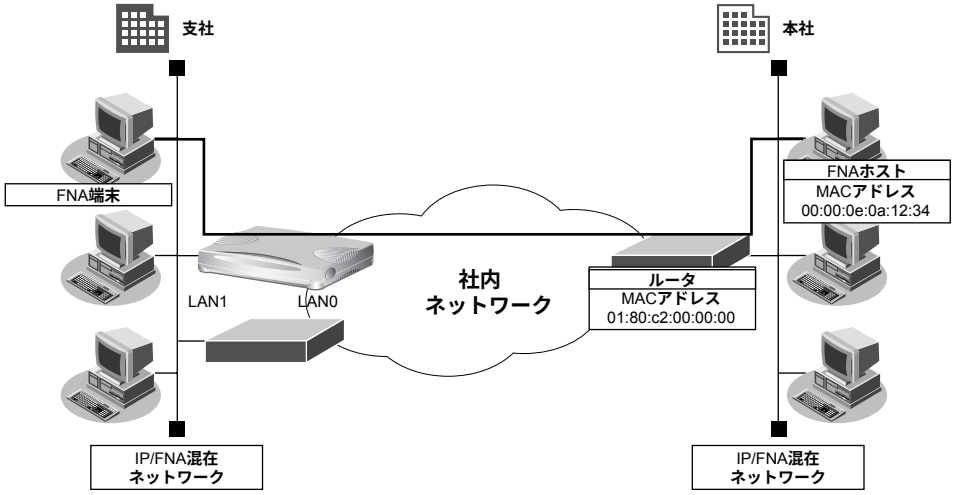
ブリッジ機能を使用すると、離れた LAN どうしを 1 つのサブネットワークとして使用することができます。また、STP 機能を使用すると、物理的にループしているネットワークでも、論理的にループしないようにすることができます。これによって、ネットワーク内のデータを円滑に流すことができます。

参照 Si-R シリーズ　機能説明書「2.25 ブリッジ機能」（P.101）

LAN 接続の場合

適用機種　全機種

ここでは、離れたLAN（FNA）をブリッジでつなぐ場合を例に説明します。



● 設定条件

- 本社へFNAのデータだけをブリッジする
- STP機能を使用する

こんな事に気をつけて

ブリッジ機能によりネットワークを接続する場合は、ブリッジ通信をするパケット以外をフィルタリングする設定にしてください。フィルタリングしないと不要なトラフィックが発生するだけでなく、IP通信できなくなる場合があります。

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。

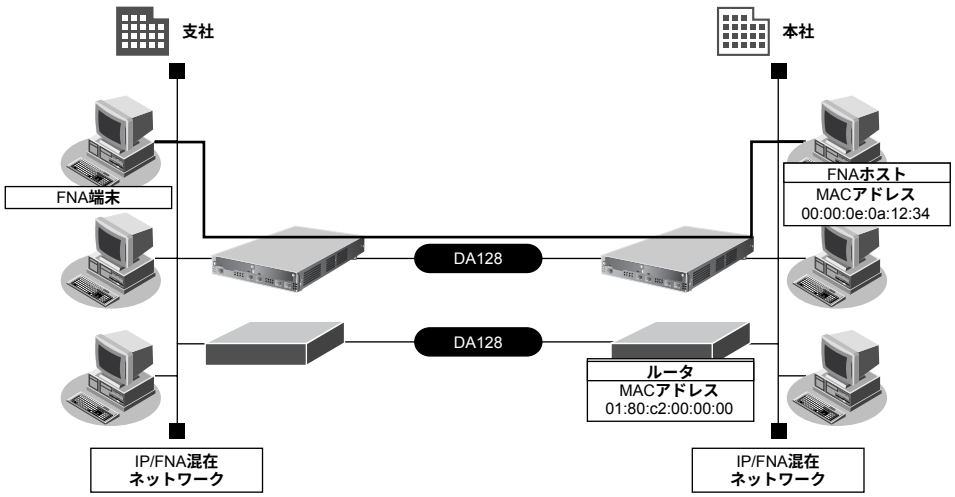
● コマンド

```
ブリッジ情報を設定する
# lan 0 bridge use on
# lan 0 bridge stp use on
# lan 1 bridge use on
# lan 1 bridge stp use on

フィルタリング情報でFNAを透過させる
# acl 0 mac any 00:00:0e:0a:12:34 llc 8080
# lan 0 bridge filter 0 pass acl 0 reverse

フィルタリング情報でSTPを透過させる
# acl 1 mac any 01:80:c0:00:00:00 llc 4242
# lan 0 bridge filter 1 pass acl 1 reverse

残りの通信をすべて遮断する
# acl 2 mac any any any
# lan 0 bridge filter 2 reject acl 2 any

設定終了
# save
# commit
```

リモート接続の場合

適用機種　***Si-R220B,260B,370,570***

ここでは、専用線をはさんで離れたLAN（FNA）をブリッジでつなぐ場合の設定方法を説明します。WANインタフェースの種類によって設定が異なりますので、使用するWANインタフェースに応じてWAN関連定義を行ってください。



● 設定条件

- SLOT0に実装されたBRI拡張モジュールL2または基本ボード上のISDNポート（Si-R220Bの場合）で専用線（128kbps）を使用する
- 本社へFNAのデータだけをブリッジする
- STP機能を使用する

こんな事に気をつけて

- **ブリッジ機能を使用すると定期的に発信するため、超過課金が発生します。ISDN回線やモデム接続でSTP機能を使用しないでください。**
- **Si-R220Bでは、利用物理回線設定でスロット番号に“mb”を指定してください。**

この例では、本社と支社がすでに専用線接続されていることを前提としています。

☛ 参照 「1.10 事業所LANを専用線で接続する」（P.30）

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

事業所 LAN を専用線で接続する
wan 0 bind 0
wan 0 line hsd 128k
lan 0 ip address 192.168.1.1/24 3
lan 0 ip dhcp service off
remote 0 name Siten1
remote 0 ip route 0 192.168.2.1/24 1
remote 0 ap 0 name shisya-1
remote 0 ap 0 datalink bind wan 0
save
reset

ブリッジ情報を設定する
lan 0 bridge use on
lan 0 bridge stp use on
remote 0 bridge use on
remote 0 bridge stp use on

フィルタリング情報で FNA を透過させる
acl 0 mac any 00:00:0e:0a:12:34 llc 8080
remote 0 bridge filter 0 pass acl 0 reverse

フィルタリング情報で STP を透過させる
acl 1 mac any 01:80:c0:00:00:00 llc 4242
remote 0 bridge filter 1 pass acl 1 reverse

残りの通信をすべて遮断する
acl 2 mac any any any
remote 0 bridge filter 2 reject acl 2 any

設定終了
save

再起動
reset

2.32.2　ブリッジグルーピング機能を使う

適用機種　全機種

ブリッジグルーピング機能とは、各インタフェースにグループ識別子を設定し、それぞれのインタフェースにグループを割り当てることによって、ブリッジ転送が、そのグループ内に閉じた形で行われるようにする機能です。グループを分けることで、ブリッジ通信を各グループに分離することができます。

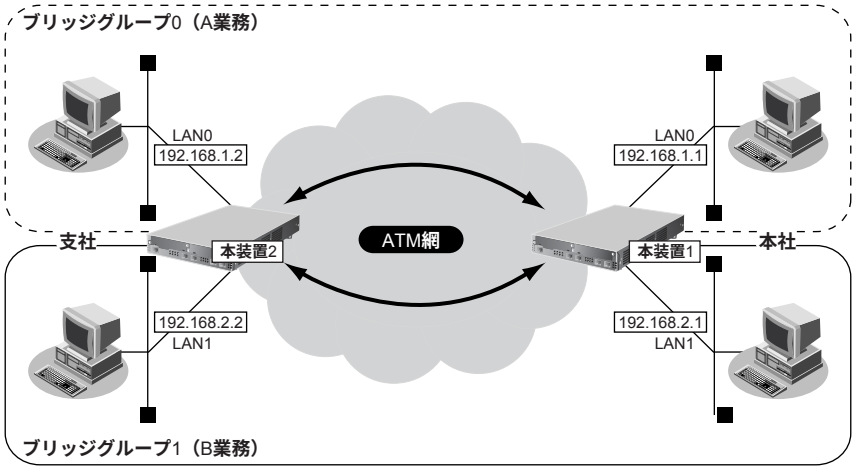
こんな事に気をつけて

- ブリッジ学習テーブル生存時間は、グループ 0 に設定した値がすべてのグループで使用されます。
- VLAN インタフェースをブリッジグループに含める場合は、1 つまたは複数のリモートインタフェースと VLAN インタフェースでだけグルーピングできます。
- IP フレームをブリッジする場合、そのブリッジグループに属するインタフェース上では、以下の機能を利用することができます。それ以外の機能は、IP フレームをブリッジするインタフェース上では利用できません。また、複数の LAN インタフェースを同じグループに含めて IP ブリッジをする場合は、同じグループ内で定義番号がもっとも小さい LAN インタフェースでだけ以下の機能を利用できます。
  - FTP（ファームアップデートなど）
  - telnet
  - Web ブラウザによる設定
  - syslog の送信
  - SNMP エージェント、Trap 送信
  - ダイナミックルーティング

  IP フレームをブリッジする場合に、転送ポリシを loose に設定したときだけ、ブリッジグループ外とブリッジ転送が行われます。また、ブリッジドメイン内は唯一の IP セグメントであることに注意してダイナミックルーティングを使用してください。
- STP はグループ 0 でだけ動作するため、グループ 0 以外のグループでは冗長リンクを持つなどループを構成するブリッジ構成は行わないでください。ブロードキャストストームが発生して通信できなくなります。また、グループ 0 でループを構成するブリッジ構成を行う場合は、必ず STP を有効にしてください。
- IP をブリッジする場合、WAN 側にはブリッジで中継されるフレームだけが転送され、直接 WAN 側に Ethernet フレームではない IP パケットを送受信することはできません。よって、IP をブリッジする運用形態では、IP に関するすべての設定は LAN インタフェース側で定義します。リモートインタフェースでは IP に関する設定は定義しないでください。
- WAN 経由で IP をブリッジし、ブリッジ転送を許す場合（転送ポリシが Loose）、たとえ WAN の先に存在するネットワークに対する経路であっても、すべての静的経路の設定は LAN インタフェース側で定義してください。ブリッジによって相手装置の LAN と本装置の LAN が WAN 経由で接続されているため、LAN 側に経路設定を定義すれば、問題なく WAN の先に存在するあて先ネットワークにブリッジで転送されて到達します。

ここでは、ブリッジグルーピング機能を使用して、本社と特定の支社との間で業務ごとに異なる通信を分離して実現する場合の設定方法を説明します。

本社の LAN0 と支社の LAN0 との間は A 業務関連だけを通信し、本社の LAN1 と支社の LAN1 との間は B 業務関連だけを通信します。互いの通信は IP も含めて完全に分離します。



● 前提条件

[本社、支社共通]

- slot0 に実装された ATM25M または ATM155M 拡張モジュール L2、または本装置に内蔵の ATM インタフェース（Si-R260B の場合）で ATM 網を使用する
- A 業務向けネットワーク名　：A-gyomu
- A 業務向け接続先名　：ATM-VC40
- A 業務向け VPI/VCI　：0/40
- A 業務向け VP 速度　：1Mbps
- B 業務向けネットワーク名　：B-gyomu
- B 業務向け接続先名　：ATM-VC41
- B 業務向け VPI/VCI　：0/41
- B 業務向け VP 速度　：1Mbps

[本社]

- LAN0 の IPv4 アドレス　：192.168.1.1/24
- LAN1 の IPv4 アドレス　：192.168.2.1/24

[支社]

- LAN0 の IPv4 アドレス　：192.168.1.2/24
- LAN1 の IPv4 アドレス　：192.168.2.2/24

● 設定条件

[本社、支社共通]

- ブリッジグループ数　：2 グループ（A 業務用と B 業務用）
- IPv4 の転送方式　：ブリッジで転送
- 転送ポリシ　：strict（完全に IPv4 通信を分離）

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（本社側）]

「WAN 関連定義を行う」は、WAN インタフェースの種類によって設定が異なります。ここでは ATM を例に示します。

```
ブリッジグループ 0 に属するインタフェースを設定する
# lan 0 bridge use on
# lan 0 ip address 192.168.1.1/24 3
# lan 0 bridge group 0
# remote 0 bridge use on
# remote 0 bridge group 0

ブリッジグループ 0 を設定する
# bridge 0 ip routing off
# bridge 0 ip policy strict

ブリッジグループ 1 に属するインタフェースのを設定する
# lan 1 bridge use on
# lan 1 ip address 192.168.2.1/24 3
# lan 1 bridge group 1
# remote 1 bridge use on
# remote 1 bridge group 1

ブリッジグループ 1 を設定する
# bridge 1 ip routing off
# bridge 1 ip policy strict

WAN 関連定義を行う
# wan 0 bind 0
# wan 0 line atm
# wan 0 atm vpi 0
# remote 0 name A-gyomu
# remote 0 ap 0 name ATM-VC40
# remote 0 ap 0 atm vci 40
# remote 0 ap 0 atm rate 1m
# remote 1 name B-gyomu
# remote 1 ap 0 name ATM-VC41
# remote 1 ap 0 atm vci 41
# remote 1 ap 0 atm rate 1m

設定終了
# save

再起動
# reset
```

[本装置 2（支社側)]

「WAN 関連定義を行う」は、WAN インタフェースの種類によって設定が異なります。ここでは ATM を例に示します。

```
ブリッジグループ 0 に属するインタフェースを設定する
# lan 0 bridge use on
# lan 0 ip address 192.168.1.2/24 3
# lan 0 bridge group 0
# remote 0 bridge use on
# remote 0 bridge group 0

ブリッジグループ 0 を設定する
# bridge 0 ip routing off
# bridge 0 ip policy strict

ブリッジグループ 1 に属するインタフェースを設定する
# lan 1 bridge use on
# lan 1 ip address 192.168.2.2/24 3
# lan 1 bridge group 1
# remote 1 bridge use on
# remote 1 bridge group 1

ブリッジグループ 1 を設定する
# bridge 1 ip routing off
# bridge 1 ip policy strict

WAN 関連定義を行う
# wan 0 bind 0
# wan 0 line atm
# wan 0 atm vpi 0
# remote 0 name A-gyomu
# remote 0 ap 0 name ATM-VC40
# remote 0 ap 0 atm vci 40
# remote 0 ap 0 atm rate 1m
# remote 1 name B-gyomu
# remote 1 ap 0 name ATM-VC41
# remote 1 ap 0 atm vci 41
# remote 1 ap 0 atm rate 1m

設定終了
# save

再起動
# reset
```

2.32.3 IP トンネルで事業所間をブリッジ接続する（Ethernet over IP ブリッジ）

適用機種　全機種

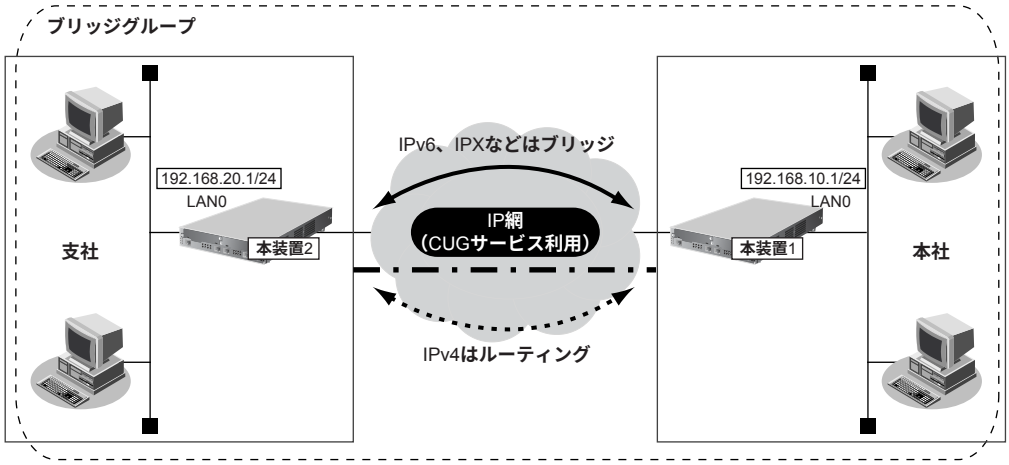
IP トンネル上でブリッジ機能を使用することにより、IP 通信だけが可能な網でも、拠点間でブリッジ通信を行うことができます。

こんな事に気をつけて

- ブリッジ学習テーブル生存時間は、グループ 0 に設定した値がすべてのグループで使用されます。
- VLAN インタフェースをブリッジグループに含める場合は、1 つまたは複数のリモートインタフェースと VLAN インタフェースでだけグルーピングできます。
- IP フレームをブリッジする場合、そのブリッジグループに属するインタフェース上では、以下の機能を利用することができます。それ以外の機能は、IP フレームをブリッジするインタフェース上では利用できません。また、複数の LAN インタフェースを同じグループに含めて IP ブリッジをする場合は、同じグループ内で定義番号がもっとも小さい LAN インタフェースでだけ以下の機能を利用できます。
  - FTP（ファームアップデートなど）
  - telnet
  - Web ブラウザによる設定
  - syslog の送信
  - SNMP エージェント、Trap 送信
  - ダイナミックルーティング

  IP フレームをブリッジする場合に、転送ポリシを loose に設定したときだけ、ブリッジグループ外とブリッジ転送が行われます。また、ブリッジドメイン内は唯一の IP セグメントであることに注意してダイナミックルーティングを使用してください。
- STP はグループ 0 でだけ動作するため、グループ 0 以外のグループでは冗長リンクを持つなどループを構成するブリッジ構成は行わないでください。ブロードキャストストームが発生して通信できなくなります。また、グループ 0 でループを構成するブリッジ構成を行う場合は、必ず STP を有効にしてください。
- IP をブリッジする場合、WAN 側にはブリッジで中継されるフレームだけが転送され、直接 WAN 側に Ethernet フレームではない IP パケットを送受信することはできません。よって、IP をブリッジする運用形態では、IP に関するすべての設定は LAN インタフェース側で定義します。リモートインタフェースでは IP に関する設定は定義しないでください。
- WAN 経由で IP をブリッジし、ブリッジ転送を許す場合（転送ポリシが Loose）、たとえ WAN の先に存在するネットワークに対する経路であっても、すべての静的経路の設定は LAN インタフェース側で定義してください。ブリッジによって相手装置の LAN と本装置の LAN が WAN 経由で接続されているため、LAN 側に経路設定を定義すれば、問題なく WAN の先に存在するあて先ネットワークにブリッジで転送されて到達します。
- Ethernet over IP ブリッジの接続先に対して接続先監視を行うことができません。接続先監視の設定は行わないでください。

ここでは、本社と特定の支社との間で、IP 網を経由し、IPv4 以外のフレームに対してブリッジ通信を行う場合の設定方法を説明します。



● 前提条件

- IP 網は、PPPoE 接続で LAN 型払い出しによりアドレス割り当てを行う CUG（Closed Users Group）サービスを利用する

[本社（PPPoE 常時接続)]

- 払い出される IPv4 アドレス（LAN0 ポートに設定）
  ：192.168.10.1/24
- PPPoE ユーザ認証 ID　：userid1@groupname
- PPPoE ユーザ認証パスワード　：userpass1
- PPPoE LAN ポート　：LAN1 ポート使用
- NAT 機能を使用しない
- 常時接続機能を使用する

[支社（PPPoE 常時接続)]

- 払い出される IPv4 アドレス（LAN0 ポートに設定）
  ：192.168.20.1/24
- PPPoE ユーザ認証 ID　：userid2@groupname
- PPPoE ユーザ認証パスワード　：userpass2
- PPPoE LAN ポート　：LAN1 ポート使用
- NAT 機能を使用しない
- 常時接続機能を使用する

● 設定条件

[本社]

- 自側エンドポイントアドレス　：192.168.10.1
- 相手側エンドポイントアドレス　：192.168.20.1

[支社]

- 自側エンドポイントアドレス　：192.168.20.1
- 相手側エンドポイントアドレス　：192.168.10.1

[本社、支社共通]

- ブリッジ対象インタフェース　：LAN0 ポートと IP トンネル
- IPv4 の転送方式　：ルーティングで転送
- IPv6 の転送方式　：ブリッジで転送

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（本社側）]

```
# delete lan

CUG サービスに接続する PPPoE の接続情報を設定する
# lan 1 mode auto
# remote 0 name CUG
# remote 0 mtu 1454
# remote 0 ap 0 name user1
# remote 0 ap 0 datalink bind lan 1
# remote 0 ap 0 ppp auth send userid1@groupname userpass1
# remote 0 ap 0 keep connect
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414

LAN0 の IP アドレスを設定する
# lan 0 ip address 192.168.10.1/24 3

IPv4 トンネルを設定する
# remote 1 name EtherIP
# remote 1 ap 0 name EtherIP
# remote 1 ap 0 datalink type ip
# remote 1 ap 0 tunnel local 192.168.10.1
# remote 1 ap 0 tunnel remote 192.168.20.1

ブリッジを行うインタフェースを設定する
# remote 1 bridge use on
# lan 0 bridge use on

ブリッジグループを設定する
# bridge 0 ip routing on
# bridge 0 ip6 routing off

設定終了
# save
# commit
```

[本装置 2（支社側）]

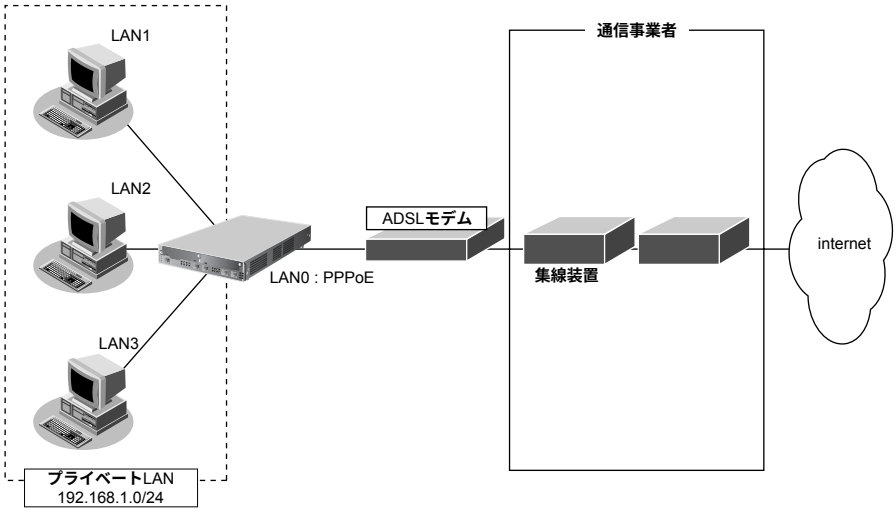
```
# delete lan

CUG サービスに接続する PPPoE の接続情報を設定する
# lan 1 mode auto
# remote 0 name CUG
# remote 0 mtu 1454
# remote 0 ap 0 name user2
# remote 0 ap 0 datalink bind lan 1
# remote 0 ap 0 ppp auth send userid2@groupname userpass2
# remote 0 ap 0 keep connect
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414

LAN0 の IP アドレスを設定する
# lan 0 ip address 192.168.20.1/24 3

IPv4 トンネルを設定する
# remote 1 name EtherIP
# remote 1 ap 0 name EtherIP
# remote 1 ap 0 datalink type ip
# remote 1 ap 0 tunnel local 192.168.20.1
# remote 1 ap 0 tunnel remote 192.168.10.1

ブリッジを行うインタフェースを設定する
# remote 1 bridge use on
# lan 0 bridge use on

ブリッジグループを設定する
# bridge 0 ip routing on
# bridge 0 ip6 routing off

設定終了
# save
# commit
```

2.33 複数の LAN ポートをスイッチング HUB のように使う

適用機種　*Si-R220B,260B,370,570*

ここでは、1 つの LAN ポートを PPPoE で使用し、残りの LAN ポートをスイッチング HUB のように設定してプライベート LAN を構築し、インターネットを利用する例を説明します。

まず、この機能を使用する前に Si-R シリーズ　機能説明書「2.25 ブリッジ機能」（P.101）を参照して、ブリッジグルーピングの機能と注意事項を理解してから設定してください。



こんな事に気をつけて

- **パソコンの LAN インタフェースと本装置の切り替えスイッチのない LAN ポートを接続する場合は、クロスケーブルを使って接続してください。**
- **IPv4 や IPv6 をブリッジする場合、IP 関連の定義は、ブリッジグループ内で定義番号がもっとも小さい LAN インタフェース（レイヤ 3 代表インタフェース）を設定してください。ブリッジグループ内では、レイヤ 3 代表インタフェースでだけ、レイヤ 3 の機能が有効になります。**
- **LAN ポートのリンク状態によって動作する機能（例：OSPF や VRRP など）は、これらの機能が定義されたレイヤ 3 代表インタフェースのリンク状態だけを監視して動作しています。レイヤ 3 代表インタェースが同期はずれを起こし、これ機能が代表インタフェースへの出力を止めた場合、同じグループ内のほかのポートからも、これの機能が出力するパケットが出なくなります。よって、リンク状態をみて動作する機能は、レイヤ 3 代表インタフェースの LAN ポートだけを使用してください。**

「1.7 インターネットへ PPPoE で接続する」（P.22）の設定が終了し、以下のとおりに設定されていることを前提とします。

☛ 参照　Si-R シリーズ　機能説明書「2.25 ブリッジ機能」（P.101）

● 前提条件

- プライベート LAN 側のネットワーク　：192.168.1.0/24
- レイヤ 3 代表インタフェース　：LAN1

● 設定条件

- LAN1、LAN2、LAN3 をグルーピングして、スイッチング HUB のように利用して、プライベート LAN 側に使用する
- IPv4 をブリッジ対象とする
- プライベート LAN 側のブリッジグループとインターネット側の間のルーティングを許可する

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

スイッチング HUB のように利用する LAN インタフェースを設定する
lan 1 bridge use on
lan 1 bridge group 0
lan 2 bridge use on
lan 2 bridge group 0
lan 3 bridge use on
lan 3 bridge group 0

ブリッジグループを設定する
bridge 0 ip routing off
bridge 0 ip policy loose
bridge 0 ip6 routing off
bridge 0 ip6 policy loose

設定終了
save

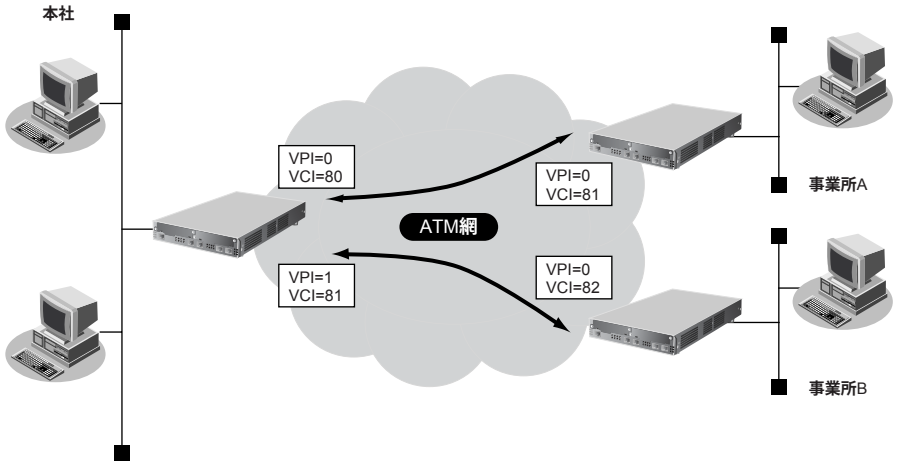
再起動
reset

2.34 ATM 網を使う

適用機種　*Si-R260B,370,570*

ここでは、ATM 網を利用して複数の事業所のネットワークを接続し、複数の VPC を使用する場合と VPC と VCC の同時シェーピングを使用する場合の設定方法を説明します。

2.34.1 事業所ごとに別の VPC を使用する



● 設定条件

[本社]

- slot0 に実装された ATM25M または ATM155M 拡張モジュール L2、または本装置に内蔵の ATM インタフェース（Si-R260B の場合）で ATM 網を使用する
- LAN 側の IP アドレス　：192.168.1.1/24（LAN0）
- 事業所 A 向けネットワーク名　：JigyoA
- 事業所 A 向け接続先名　：jigyo-a
- 事業所 A 向け VPI/VCI　：0/80
- 事業所 A 向け VP 速度　：6Mbps
- 事業所 B 向けネットワーク名　：JigyoB
- 事業所 B 向け接続先名　：jigyo-b
- 事業所 B 向け VPI/VCI　：1/81
- 事業所 B 向け VP 速度　：4Mbps

[事業所 A]

- slot0 に実装された ATM25M または ATM155M 拡張モジュール L2、または本装置に内蔵の ATM インタフェース（Si-R260B の場合）で ATM 網を使用する
- LAN 側の IP アドレス　：192.168.101.1/24（LAN0）
- ネットワーク名　：Honsya
- 接続先名　：honsya-1
- VPI/VCI　：0/81
- VP 速度　：6Mbps

[事業所 B]

- slot0 に実装された ATM25M または ATM155M 拡張モジュール L2、または本装置に内蔵の ATM インタフェース（Si-R260B の場合）で ATM 網を使用する
- LAN 側 IP アドレス　：192.168.102.1/24（LAN0）
- ネットワーク名　：Honsya
- 接続先名　：honsya-2
- VPI/VCI　：0/82
- VP 速度　：4Mbps

こんな事に気をつけて

使用する拡張モジュールによって、以下の点に注意して設定してください。Si-R260B の ATM25 インタフェースは ATM25 拡張モジュール L2 と同じです。

拡張モジュール	注意点
ATM25M ／ ATM155M 拡張モジュール L2	• VP ／ VC 速度を設定する場合は、64Kbps ～ 25Mbps の範囲で 8Kbps または 50Kbps 刻みで指定します。 • VP シェーピングを前提とした運用を本装置で行う場合は、以下のように設定してください。 - VPC が 1VPC の場合にだけ、VP シェーピングと VC シェーピングを同時に利用することができます。 - VP シェーピングを行う VPC と VP シェーピングを行わない VPC は、同一拡張モジュール内で同時に利用することはできません。 • 本装置で複数 VPC を使って ATM 網を利用する場合は、以下のように設定してください。 - 複数 VPC で VP シェーピングが必要となる場合は、1VPC あたり 1VCC となるようにネットワークを設計してください。このとき、16VPC まで利用することができます。 - VP 速度は設定しないでください。契約時の VP 速度は VC 速度として設定し、サービスタイプを CBR に設定してください。 • VP シェーピングを必要としない場合は、複数 VPC 上で複数 VC シェーピングを行うことができます。 • VP シェーピング時は、VC 速度（CBR、GFR+）、平均速度（SCR）および最低速度（UBR+）の総和が VP 速度を超えないようにように設定してください。 • VC シェーピング時は、VC 速度（CBR、GFR+）、平均速度（SCR）および最低速度（UBR+）の総和が 25Mbps を超えないようにように設定してください。
ATM25M 拡張モジュール H1	• VP ／ VC 速度を設定する場合は、以下の設定範囲で設定してください。 - 64Kbps ～ 25Mbps の範囲で 8Kbps または 50Kbps 刻みで指定します。 • VP シェーピングを前提とした運用を本装置で行う場合は、以下のように設定してください。 - VP 速度の総和を 25Mbps 以下に設定してください。 - 1-VPC での VP ／ VC シェーピング時以外で、サービスタイプ UBR+ は設定できません。複数 VPC での VP ／ VC シェーピング時は VBR を設定してください。 - サービスタイプが VBR の場合は、平均速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが CBR の場合は、VC 速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが UBR+ の場合は、最低速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが GFR+ の場合は、VC 速度の総和が VP 速度を超えないように設定してください。 - VP シェーピングを行う VPC と VP シェーピングを行わない VPC は、同一拡張モジュール内で同時に利用することはできません。

拡張モジュール	注意点
ATM155M 拡張モジュール H1	• VP ／ VC 速度を設定する場合は、以下の設定範囲で設定してください。 - VP 速度は、200Kbps ～ 50Mbps の範囲で 8Kbps または 50Kbps 刻みで指定できます。 - VC 速度は、64Kbps ～ 100Mbps の範囲で 8Kbps または 50Kbps 刻みで指定できます。 • VP シェーピングを前提とした運用を本装置で行う場合は、以下のように設定してください。 - VP 速度の総和を 50Mbps 以下に設定してください。 - 1-VPC での VP ／ VC シェーピング時以外ではサービスタイプ UBR+ は設定できません。複数 VPC での VP ／ VC シェーピング時は VBR を設定してください。 - サービスタイプが VBR の場合は、平均速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが CBR の場合は、VC 速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが UBR+ の場合は、最低速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが GFR+ の場合は、VC 速度の総和が VP 速度を超えないように設定してください。 - VPC 内の VC 速度の最高速度は 50Mbps になります。 - VP シェーピングを行う VPC と VP シェーピングを行わない VPC は、同一拡張モジュール内で同時に利用することはできません。 • DSU 接続する場合は、atm send clock コマンドで送信クロックの設定を recovery にしてください。 `atm <slot> send clock recovery`

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

[本社]

```
VPCの情報を設定する
# wan 0 bind 0
# wan 0 line atm
# wan 0 atm vpi 0
# wan 1 bind 0
# wan 1 line atm
# wan 1 atm vpi 1

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

事業所A向けの情報を設定する
# remote 0 name JigyoA
# remote 0 ap 0 name jigyo-a
# remote 0 ap 0 datalink bind wan 0
# remote 0 ap 0 atm vci 80
# remote 0 ap 0 atm rate 6m
# remote 0 ap 0 atm ast cbr
# remote 0 ip route 0 192.168.101.0/24 1

事業所B向けの情報を設定する
# remote 1 name JigyoB
# remote 1 ap 0 name jigyo-b
# remote 1 ap 0 datalink bind wan 1
# remote 1 ap 0 atm vci 81
# remote 1 ap 0 atm rate 4m
# remote 1 ap 0 atm ast cbr
# remote 1 ip route 0 192.168.102.0/24 1

設定終了
# save

再起動
# reset
```

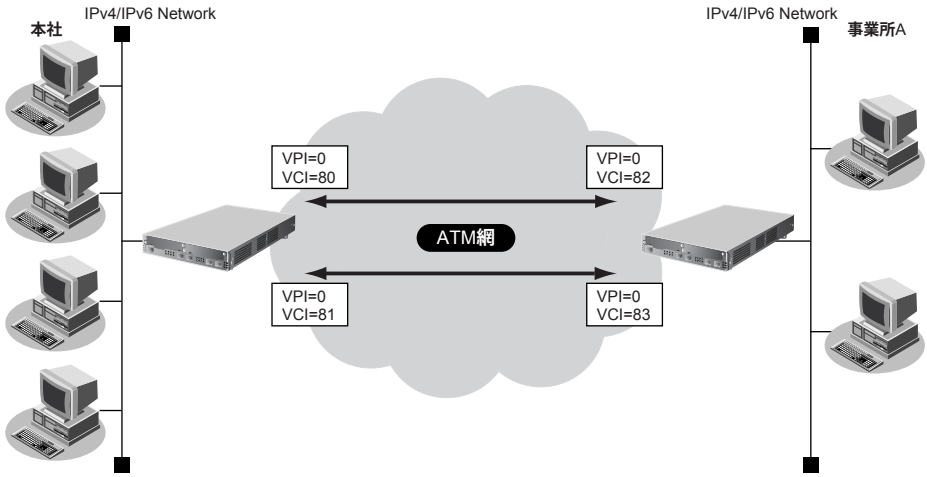
[事業所 A]

```
VPC の情報を設定する
# wan 0 bind 0
# wan 0 line atm
# wan 0 atm vpi 0

本装置の IP アドレスを設定する
# lan 0 ip address 192.168.101.1/24 3

本社向けの情報を設定する
# remote 0 name Honsya
# remote 0 ap 0 name honsya-1
# remote 0 ap 0 datalink bind wan 0
# remote 0 ap 0 atm vci 81
# remote 0 ap 0 atm rate 6m
# remote 0 ap 0 atm ast cbr
# remote 0 ip route 0 default 1

設定終了
# save

再起動
# reset
```

[事業所 B]

```
VPC の情報を設定する
# wan 0 bind 0
# wan 0 line atm
# wan 0 atm vpi 0

本装置の IP アドレスを設定する
# lan 0 ip address 192.168.102.1/24 3

本社向けの情報を設定する
# remote 0 name Honsya
# remote 0 ap 0 name honsya-1
# remote 0 ap 0 datalink bind wan 0
# remote 0 ap 0 atm vci 82
# remote 0 ap 0 atm rate 4m
# remote 0 ap 0 atm ast cbr
# remote 0 ip route 0 default 1

設定終了
# save

再起動
# reset
```

2.34.2　VPC と VCC の同時シェーピングを使用する



● 設定条件

[本社]

- slot0 に実装された ATM25M または ATM155M 拡張モジュール L2、または本装置に内蔵の ATM インタフェース（Si-R260B の場合）で ATM 網を使用する
- IPv4 アドレス　：192.168.1.1/24（LAN0）
- IPv4 通信向けネットワーク名　：JigyoA1
- IPv4 通信向け接続先名　：jigyoa-1
- IPv4 通信向け VPI/VCI　：0/80
- IPv6 アドレス　：2001:db8:1111:1000::/64（LAN0）
- IPv6 通信向けネットワーク名　：JigyoA2
- IPv6 通信向け接続先名　：jigyoa-2
- IPv6 通信向け VPI/VCI　：0/81
- VP 速度　：8Mbps
- IPv4 通信向けサービスタイプ　：VBR（VC 速度：6Mbps、平均速度：5Mbps）
- IPv6 通信向けサービスタイプ　：UBR+（VC 速度：5Mbps、最低速度：3Mbps）

[事業所 A]

- slot0 に実装された ATM25M または ATM155M 拡張モジュール L2、または本装置に内蔵の ATM インタフェース（Si-R260B の場合）で ATM 網を使用する
- IPv4 アドレス　：192.168.2.1/24（LAN0）
- IPv4 通信向けネットワーク名　：Honsya1
- IPv4 通信向け接続先名　：honsya-1
- IPv4 通信向け VPI/VCI　：0/82
- IPv6 アドレス　：2001:db8:1111:1001::/64（LAN0）
- IPv6 通信向けネットワーク名　：Honsya2
- IPv6 通信向け接続先名　：honsya-2
- IPv6 通信向け VPI/VCI　：0/83
- VP 速度　：8Mbps
- IPv4 通信向けサービスタイプ　：VBR（VC 速度：6Mbps、平均速度：5Mbps）
- IPv6 通信向けサービスタイプ　：UBR+（VC 速度：5Mbps、最低速度：3Mbps）

こんな事に気をつけて

使用する拡張モジュールによって、以下の点に注意して設定してください。Si-R260B の ATM25 インタフェースは ATM25 拡張モジュール L2 と同じです。

拡張モジュール	注意点
ATM25M ／ ATM155M 拡張モジュール L2	• VP ／ VC 速度を設定する場合は、64Kbps ～ 25Mbps の範囲で 8Kbps または 50Kbps 刻みで指定します。 • VP シェーピングを前提とした運用を本装置で行う場合は、以下のように設定してください。 - VPC が 1VPC の場合にだけ、VP シェーピングと VC シェーピングを同時に利用することができます。 - VP シェーピングを行う VPC と VP シェーピングを行わない VPC は、同一拡張モジュール内で同時に利用することはできません。 • 本装置で複数 VPC を使って ATM 網を利用する場合は、以下のように設定してください。 - 複数 VPC で VP シェーピングが必要となる場合は、1VPC あたり 1VCC となるようにネットワークを設計してください。このとき、16VPC まで利用することができます。 - VP 速度は設定しないでください。契約時の VP 速度は VC 速度として設定し、サービスタイプを CBR に設定してください。 • VP シェーピングを必要としない場合は、複数 VPC 上で複数 VC シェーピングを行うことができます。 • VP シェーピング時は、VC 速度（CBR、GFR+）、平均速度（SCR）および最低速度（UBR+）の総和が VP 速度を超えないようにように設定してください。 • VC シェーピング時は、VC 速度（CBR、GFR+）、平均速度（SCR）および最低速度（UBR+）の総和が 25Mbps を超えないようにように設定してください。
ATM25M 拡張モジュール H1	• VP ／ VC 速度を設定する場合は、以下の設定範囲で設定してください。 - 64Kbps ～ 25Mbps の範囲で 8Kbps または 50Kbps 刻みで指定します。 • VP シェーピングを前提とした運用を本装置で行う場合は、以下のように設定してください。 - VP 速度の総和を 25Mbps 以下に設定してください。 - 1-VPC での VP ／ VC シェーピング時以外で、サービスタイプ UBR+ は設定できません。複数 VPC での VP ／ VC シェーピング時は VBR を設定してください。 - サービスタイプが VBR の場合は、平均速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが CBR の場合は、VC 速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが UBR+ の場合は、最低速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが GFR+ の場合は、VC 速度の総和が VP 速度を超えないように設定してください。 - VP シェーピングを行う VPC と VP シェーピングを行わない VPC は、同一拡張モジュール内で同時に利用することはできません。

拡張モジュール	注意点
ATM155M 拡張モジュール H1	• VP ／ VC 速度を設定する場合は、以下の設定範囲で設定してください。 - VP 速度は、200Kbps ～ 50Mbps の範囲で 8Kbps または 50Kbps 刻みで指定できます。 - VC 速度は、64Kbps ～ 100Mbps の範囲で 8Kbps または 50Kbps 刻みで指定できます。 • VP シェーピングを前提とした運用を本装置で行う場合は、以下のように設定してください。 - VP 速度の総和を 50Mbps 以下に設定してください。 - 1-VPC での VP ／ VC シェーピング時以外ではサービスタイプ UBR+ は設定できません。複数 VPC での VP ／ VC シェーピング時は VBR を設定してください。 - サービスタイプが VBR の場合は、平均速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが CBR の場合は、VC 速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが UBR+ の場合は、最低速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが GFR+ の場合は、VC 速度の総和が VP 速度を超えないように設定してください。 - VPC 内の VC 速度の最高速度は 50Mbps になります。 - VP シェーピングを行う VPC と VP シェーピングを行わない VPC は、同一拡張モジュール内で同時に利用することはできません。 • DSU 接続する場合は、atm send clock コマンドで送信クロックの設定を recovery にしてください。 `atm <slot> send clock recovery`

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

[本社]

```
VPC を設定する
# wan 0 bind 0
# wan 0 line atm
# wan 0 atm vpi 0
# wan 0 atm rate 8m

LAN 情報を設定する
# lan 0 ip address 192.168.1.1/24 3
# lan 0 ip6 use on
# lan 0 ip6 address 0 2001:db8:1111:1000::/64 30d 7d
# lan 0 ip6 ra mode send

IPv4 の相手情報を設定する
# remote 0 name JigyoA-1
# remote 0 ap 0 name jigyoa-1
# remote 0 ap 0 datalink bind wan 0
# remote 0 ap 0 atm vci 80
# remote 0 ap 0 atm rate 6m
# remote 0 ap 0 atm ast vbr 5m 32
# remote 0 ip route 0 192.168.2.0/24 1

IPv6 の相手情報を設定する
# remote 1 name JigyoA-2
# remote 1 ap 0 name jigyoa-2
# remote 1 ap 0 datalink bind wan 0
# remote 1 ap 0 atm vci 81
# remote 1 ap 0 atm rate 5m
# remote 1 ap 0 atm ast ubrp 3m
# remote 1 ip6 use on
# remote 1 ip6 route 0 2001:db8:1111:1001::/64 1

設定終了
# save

再起動
# reset
```

[事業所 A]

VPC を設定する
wan 0 bind 0
wan 0 line atm
wan 0 atm vpi 0
wan 0 atm rate 8m

LAN 情報を設定する
lan 0 ip address 192.168.2.1/24 3
lan 0 ip6 use on
lan 0 ip6 address 0 2001:db8:1111:1001::/64 30d 7d
lan 0 ip6 ra mode send

IPv4 の相手情報を設定する
remote 0 name Honsya-1
remote 0 ap 0 name honsya-1
remote 0 ap 0 datalink bind wan 0
remote 0 ap 0 atm vci 82
remote 0 ap 0 atm rate 6m
remote 0 ap 0 atm ast vbr 5m 32
remote 0 ip route 0 192.168.1.0/24 1

IPv6 の相手情報を設定する
remote 1 name Honsya-2
remote 1 ap 0 name honsya-2
remote 1 ap 0 datalink bind wan 0
remote 1 ap 0 atm vci 83
remote 1 ap 0 atm rate 5m
remote 1 ap 0 atm ast ubrp 3m
remote 1 ip6 use on
remote 1 ip6 route 0 2001:db8:1111:1000::/64 1

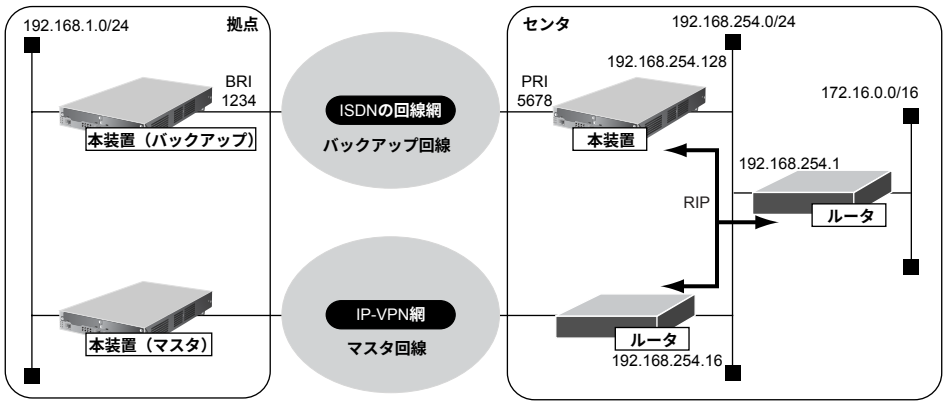
設定終了
save

再起動
reset

2.35 ISDN 接続を契機とした通信バックアップを使う

適用機種　***Si-R220B,370,570***

マスタ回線側で経路制御ができなくても、バックアップ回線である ISDN 回線の接続状態によって、通信をバックアップ側に切り替えることができます。



● 設定条件

- センタ側は、本装置以外の装置は設定が完了済み
- センタ側の 192.168.254.0/24 に接続されたそれぞれのルータは、本装置が広報する経路が選択されるように設定されている
- センタから拠点への発信は行わない
- 拠点側本装置は、ISDN 接続の設定以外は設定が完了済み

こんな事に気をつけて

Si-R220B では、利用物理回線設定でスロット番号に“mb”を指定してください。

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

[センタ側本装置]

```
ISDN回線（PRI）を設定する
# wan 0 bind 0
# wan 0 line isdn
# wan 0 isdn autodial disable

LANを設定する
# lan 0 ip address 192.168.254.128/24 3
# lan 0 ip rip use v2m v2 0 off

拠点への接続先を設定する
# remote 0 name kyoten
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ap 0 name kyoten
# remote 0 ap 0 dial 0 number 1234
# remote 0 ap 0 ppp auth receive kyoten kyotenpass

設定終了
# save

再起動
# reset
```

[拠点側本装置（バックアップ)]

```
センタへの接続先を設定する
# remote 0 name center
# remote 0 ip route 0 default 1 1
# remote 0 ap 0 name center
# remote 0 ap 0 dial 0 number 5678
# remote 0 ap 0 ppp auth send kyoten kyotenpass
# remote 0 ap 0 idle 1m send

設定終了
# save
# commit
```

2.36 外部のパソコンからPIAFS接続する

適用機種　*Si-R220B,370*

ここでは、PIAFS 対応の PHS を使用して外部のパソコンから本装置へ着信接続する例を説明します。接続先のパソコンの設定に関する説明は省略しています。

こんな事に気をつけて

- **本装置の PIAFS 接続は PIAFS 1.0/2.0/2.1 に対応します。**
- **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っ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　Si-R シリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.49）

- **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。**

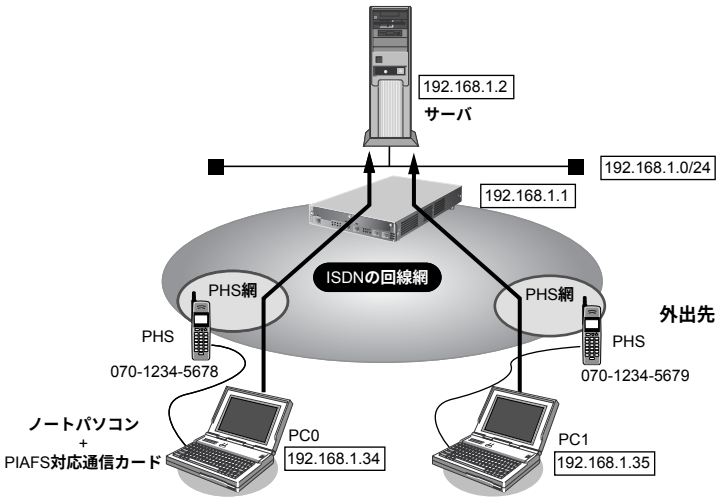
  ☛ 参照　Si-R シリーズ　コマンドユーザーズガイド「1.7 コマンドで入力できる文字一覧」（P.26）

ヒント

本装置の LAN 側のネットワークと同じネットワークアドレスを別ネットワークのパソコンに割り当てることによって、Proxy ARP が自動的に動作し、ISDN 回線経由で接続されたパソコンが LAN 上に存在するように扱えます。

◆ Proxy ARP とは

Ethernet 上で通信する場合、相手を識別するために MAC アドレスが使用されます。このとき、IP アドレスと MAC アドレスの対応付けを行う手段として ARP（Address Resolution Protocol）が使用されます。
ブロードキャストで ARP 要求を発行すると、LAN 上で自分の IP アドレスに関連する ARP 要求であると認識したパソコンは、自分の MAC アドレスを送り返します。
Proxy ARP とは、パソコンから送られてくる ARP 要求に対して、実際のパソコンの代わりに応答する機能です。



● 設定条件

- SLOT0 に装着した BRI 拡張モジュール L2（Si-R370）または ISDN U ポート（Si-R220B）を使用して ISDN 回線に接続する
- 本装置の LAN 側のネットワークアドレス/ネットマスク
  ：192.168.1.0/24

- 以下からの着信を許可する

  [PC0＜ノートパソコン＋ PHS ＞で外出先から接続]

  - 接続先ネットワーク名　：pc0
  - 接続先名　：phs0
  - 割り当てIPアドレス　：192.168.1.34
  - 電話番号　：070-1234-5678
  - 受諾認証ID　：mobileid
  - 受諾認証パスワード　：mobilepass

  [PC1＜ノートパソコン＋ PHS ＞で外出先から接続]

  - 接続先ネットワーク名　：pc1
  - 接続先名　：phs1
  - 割り当てIPアドレス　：192.168.1.35
  - 電話番号　：070-1234-5679
  - 受諾認証ID　：mobileid
  - 受諾認証パスワード　：mobilepass

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

```
BRI 拡張モジュール L2 を装着したスロット番号を設定する（Si-R370 の場合のみ）
# wan 0 bind 0

回線インタフェースとして ISDN を設定する
# wan 0 line isdn

LAN 情報を設定する
# lan 0 ip address 192.168.1.1/24 3

接続先情報（PC0）を設定する
# remote 0 name pc0
# remote 0 autodial disable
# remote 0 ap 0 name phs0
# remote 0 ap 0 ppp auth receive mobileid mobilepass
# remote 0 ap 0 dial 0 number 070-1234-5678
# remote 0 ip address local 192.168.1.1
# remote 0 ip address remote 192.168.1.34

接続先情報（PC1）を設定する
# remote 1 name pc1
# remote 1 autodial disable
# remote 1 ap 0 name phs1
# remote 1 ap 0 ppp auth receive mobileid mobilepass
# remote 1 ap 0 dial 0 number 070-1234-5679
# remote 1 ip address local 192.168.1.1
# remote 1 ip address remote 192.168.1.35

設定終了
# save

再起動
# reset
```

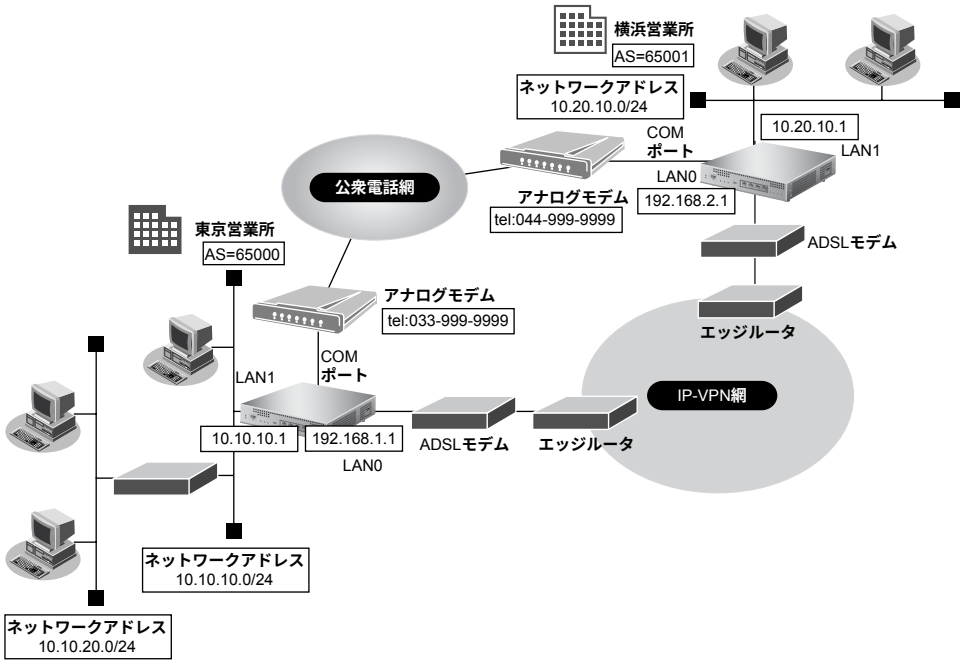
2.37 アナログモデムで通信バックアップをする

適用機種　*Si-R220B*

本装置の COM ポートに外付けのアナログモデムを接続することによって、アナログ回線を使用して通信することができます。

ここでは、営業所間を IP-VPN 網で接続し、IP-VPN 網側の通信が通信不能になった場合にアナログ回線側で通信バックアップする場合を例に説明します。

この例では、BGP 経路よって優先度の低いスタティックルートをバックアップ回線側に設定します。メインの IP-VPN 側が通信不能になって BGP セッションが切断され、相手拠点の BGP 経路が消えた際に、バックアップ回線側に定義したスタティックルートが有効になり、通信がバックアップ回線側に切り替わる方法を用います。



本装置に接続できるモデムの条件は、以下のとおりです。

- COM ポート側の通信速度が 9600/19200/38400/57600/115200/230400bps のどれかの速度で通信できる
- 工場出荷時の設定で、RS/CS 信号によるハードフロー制御が有効になっている
- 通信中に`+++`を COM ポートから受信することによってエスケープモードになる
- 以下の AT コマンドに対応している

カテゴリ	サポートコマンド
ソフトリセット	ATZ
リザルトコードを文字列にする	ATV1
エコーバックを抑止する	ATE0
CONNECT リザルトコードに DCE 速度を付加する	ATW2
切断	ATH
応答	ATA
コマンド送出時先行文字	AT
電話番号送出時先行文字	ATD
パルス	P
トーン	T

カテゴリ	サポートコマンド
ダイヤルトーン検知なし	X3
ダイヤルトーン検知あり	X4
スピーカを OFF にする	M0
発呼時だけスピーカを ON にする	M1
スピーカを ON にする	M2
スピーカをダイヤル終了からキャリア検出まで ON にする	M3
音量 LOW	L0
音量 Midium	L2
音量 High	L3

- 以下のリザルトコードを返す

カテゴリ	サポートコマンド
正常実行	OK
接続完了	CONNECT <回線速度>（※）
コマンドエラー	ERROR、+FCERROR、+FCON、+F4、FAX、DATA、VOICE
回線接続	NO CARRIER
ダイヤルトーン未検出	NO DIALTONE、NO DIAL TONE
話し中音検出	BUSY、PHONE IN USE、HAND SET IN USE
無音未検出	NO ANSWER
呼び出し検出	RING

※） 回線速度　:接続した回線速度
0-9 の数字文字列の場合だけ回線速度として扱います。
0-9 以外の文字が含まれる場合は、無視するため、回線速度を取得できません。

動作確認済みのアナログモデムは、以下のとおりです。

会社名	製品名
（株）アイ・オー・データ機器	DFML-560EL
（株）バッファロー	IGM-B56KS
オムロン（株）	ME5614E2

こんな事に気をつけて

- アナログモデムは、COM ポートに接続してください。コンソールポートは、コンソール専用ですので、モデム接続はできません。
- モデムの不揮発性メモリ（プロファイル）を工場出荷時設定にしてからモデムを接続してください。
- モデムでは、回線の切断に時間がかかるため、課金単位時間を超えて切断される場合があります。
- アナログモデム接続では、以下の機能は動作しません。
  - 電話番号による相手識別機能
  - コールバック機能
  - 金額による課金制御機能
  - 常時接続機能
  - 回線接続保持タイマ機能
  - シェーピング機能
- モデムで通信できるプロトコルは、IPv4、IPv6、ブリッジだけです。
- アナログモデムによる発信は従量課金が発生するため、モデム統計情報を監視して異常課金が発生していないか、こまめに確認してください。また、異常課金を防止する場合は、課金制御機能の接続時間制限を設定してください。
- アナログモデムでの通信速度は 56Kbps とみなして動作しますが、モデムの接続完了リザルトコードから速度を取得できた場合は取得した速度を採用して動作します。

ここでは、以下を参照して、IP-VPN 網接続が設定されていることを前提とします。

☛ 参照 「1.13 複数の事業所 LAN を IP-VPN 網を利用して接続する」（P38）

● 設定条件

- ADSL モデムを使用して IP-VPN 網と接続する

[東京営業所]

＜横浜営業所とモデムで接続する条件＞

- ネットワーク名　：backup
- 接続先名　：yokohama
- WAN の自側 IP アドレス　：172.17.1.1
- WAN の相手側 IP アドレス　：172.17.1.2
- 電話番号　：044-999-9999
- 無通信監視　：1 分
- ユーザ認証 ID とユーザ認証パスワード
  発信　：tokyo、tokyopass
  着信　：kawasaki、kawapass
- ダイヤル方式　：トーン
- バックアップ用のスタティックルート　：10.20.0.0/16（優先度 30）

[横浜営業所]

＜東京営業所とモデムで接続する条件＞

- ネットワーク名　：backup
- 接続先名　：tokyo
- WAN の自側 IP アドレス　：172.17.1.2
- WAN の相手側 IP アドレス　：172.17.1.1
- 電話番号　：033-999-9999
- 無通信監視　：1 分
- ユーザ認証 ID とユーザ認証パスワード
  発信　：kawasaki、kawapass
  着信　：tokyo、tokyopass
- ダイヤル方式　：トーン
- バックアップ用のスタティックルート　：10.10.0.0/16（優先度 30）

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。

東京営業所のバックアップ回線を設定する

● コマンド

```
接続先の情報を設定する
# remote 0 name backup
# remote 0 ap 0 name yokohama
# remote 0 ap 0 datalink bind serial 0
# remote 0 ap 0 dial 0 number 044-999-9999
# remote 0 ap 0 ppp auth send yokohama yokopass
# remote 0 ap 0 ppp auth receive tokyo tyokyopass
# remote 0 ap 0 idle 1m

シリアル情報を設定する
# serial 0 use on

着信デフォルト情報を設定する
# answer accept enable

BGP 経路より優先度の低いスタティックルートを設定する
# remote 0 ip route 0 10.20.0.0/16 1 30

設定終了
# save

再起動
# reset
```

横浜営業所のバックアップ回線を設定する

● コマンド

```
接続先の情報を設定する
# remote 0 name backup
# remote 0 ap 0 name tokyo
# remote 0 ap 0 datalink bind serial 0
# remote 0 ap 0 dial 0 number 033-999-9999
# remote 0 ap 0 ppp auth send tokyo tyokyopass
# remote 0 ap 0 ppp auth receive yokohama yokopass
# remote 0 ap 0 idle 1m

シリアル情報を設定する
# serial 0 use on

着信デフォルト情報を設定する
# answer accept enable

BGP 経路より優先度の低いスタティックルートを設定する
# remote 0 ip route 0 10.10.0.0/16 1 30

設定終了
# save

再起動
# reset
```

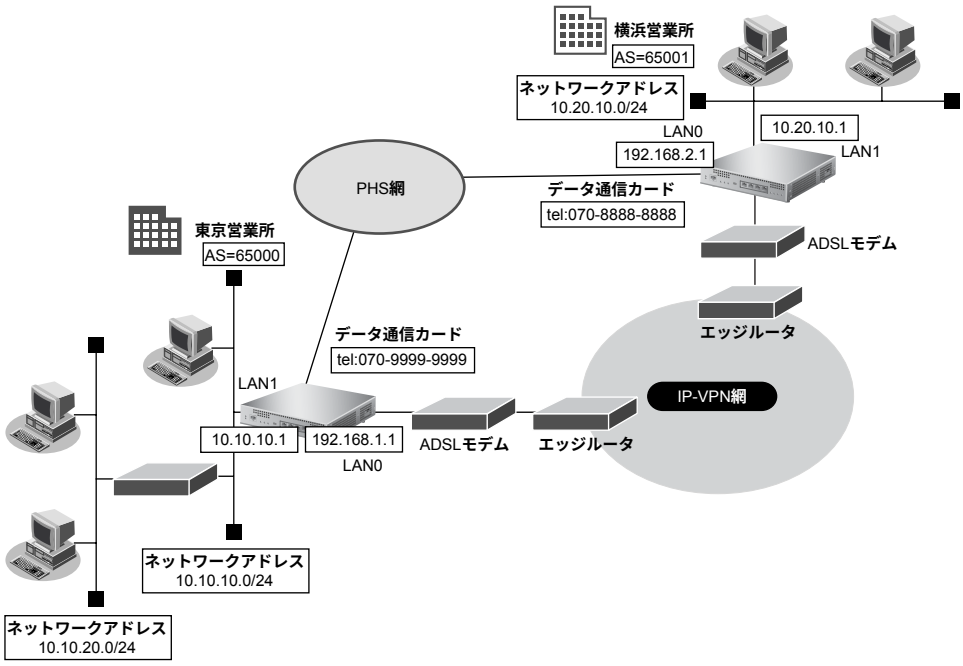
2.38 データ通信カードで通信バックアップをする

適用機種 ***Si-R240***

本装置の SLOT0 に PIAFS 着信対応のデータ通信カードを装着することによって、PHS 回線を使用して通信することができます。
ここでは、営業所間を IP-VPN 網で接続し、IP-VPN 網側の通信が通信不能になった場合にウィルコムの PHS 回線側で通信バックアップする場合を例に説明します。

参照 動作検証済みのデータ通信カード（富士通ホームページ）
http://fenics.fujitsu.com/products/sir/sir240/supportcard.html

この例では、BGP 経路よって優先度の低いスタティックルートをバックアップ回線側に設定します。メインの IP-VPN 側が通信不能になって BGP セッションが切断され、相手拠点の BGP 経路が消えた際に、バックアップ回線側に定義したスタティックルートが有効になり、通信がバックアップ回線側に切り替わる方法を用います。



こんな事に気をつけて

- **データ通信カードの不揮発性メモリ（プロファイル）を工場出荷時設定にしてからデータ通信カードを SLOT0 に装着してください。**
- **データ通信カードでは、回線の切断に時間がかかるため、課金単位時間を超えて切断される場合があります。**
- **データ通信カード接続では、以下の機能は動作しません。**
  - **電話番号による相手識別機能**
  - **コールバック機能**
  - **金額による課金制御機能**
  - **常時接続機能**
  - **回線接続保持タイマ機能**
  - **シェーピング機能**
- **データ通信カードで通信できるプロトコルは、IPv4、IPv6、ブリッジだけです。**
- **データ通信カードによる発信は従量課金が発生するため、データ通信カード統計情報を監視して異常課金が発生していないか、こまめに確認してください。また、異常課金を防止する場合は、課金制御機能や強制切断機能の接続時間制限を設定してください。**
- **データ通信カードの通信速度は 64Kbps とみなして動作します。**

ここでは、以下を参照して、IP-VPN 網接続が設定されていることを前提とします。

☛ 参照 「1.13 複数の事業所 LAN を IP-VPN 網を利用して接続する」（P38）

● 設定条件

- ADSL モデムを使用して IP-VPN 網と接続する

[東京営業所]

＜横浜営業所とデータ通信カードで接続する条件＞

- ネットワーク名　：backup
- 接続先名　：yokohama
- WAN の自側 IP アドレス　：172.17.1.1
- WAN の相手側 IP アドレス　：172.17.1.2
- 電話番号　：070-8888-8888
- 通信方式　：64kPIAFS（ベストエフォート）方式
- 無通信監視　：1 分
- ユーザ認証 ID とユーザ認証パスワード
  発信　：tokyo、tokyopass
  着信　：kawasaki、kawapass
- バックアップ用のスタティックルート　：10.20.0.0/16（優先度 30）

[横浜営業所]

＜東京営業所とデータ通信カードで接続する条件＞

- ネットワーク名　：backup
- 接続先名　：tokyo
- WAN の自側 IP アドレス　：172.17.1.2
- WAN の相手側 IP アドレス　：172.17.1.1
- 電話番号　：070-9999-9999
- 通信方式　：64kPIAFS（ベストエフォート）方式
- 無通信監視　：1 分
- ユーザ認証 ID とユーザ認証パスワード
  発信　：kawasaki、kawapass
  着信　：tokyo、tokyopass
- バックアップ用のスタティックルート　：10.10.0.0/16（優先度 30）

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。

東京営業所のバックアップ回線を設定する

● コマンド

```
接続先の情報を設定する
# remote 0 name backup
# remote 0 ap 0 name yokohama
# remote 0 ap 0 datalink bind wan 0
# remote 0 ap 0 dial 0 number 070-8888-8888##4
# remote 0 ap 0 ppp auth send yokohama yokopass
# remote 0 ap 0 ppp auth receive tokyo tyokyopass
# remote 0 ap 0 idle 1m

PIAFS 着信対応データ通信カードを装着したスロット番号（0 固定）を設定する
# wan 0 bind 0 0

回線インタフェースとしてデータ通信カードを設定する
# wan 0 line cardmodem

着信デフォルト情報を設定する
# answer accept enable

BGP 経路より優先度の低いスタティックルートを設定する
# remote 0 ip route 0 10.20.0.0/16 1 30

設定終了
# save

再起動
# reset
```

横浜営業所のバックアップ回線を設定する

● コマンド

```
接続先の情報を設定する
# remote 0 name backup
# remote 0 ap 0 name tokyo
# remote 0 ap 0 datalink bind wan 0
# remote 0 ap 0 dial 0 number 070-9999-9999##4
# remote 0 ap 0 ppp auth send tokyo tyokyopass
# remote 0 ap 0 ppp auth receive yokohama yokopass
# remote 0 ap 0 idle 1m

PIAFS 着信対応データ通信カードを装着したスロット番号（0 固定）を設定する
# wan 0 bind 0 0

回線インタフェースとしてデータ通信カードを設定する
# wan 0 line cardmodem

着信デフォルト情報を設定する
# answer accept enable

BGP 経路より優先度の低いスタティックルートを設定する
# remote 0 ip route 0 10.10.0.0/16 1 30

設定終了
# save

再起動
# reset
```

2.39 外部のパソコンから着信接続する（リモートアクセスサーバ）

適用機種 ***Si-R220B,370,570***

ISDN 回線を使用して、外部のパソコンから本装置に着信接続する場合、本装置をリモートアクセスサーバとして使用することができます。以下の環境の場合に、リモートアクセスを行うことができます。

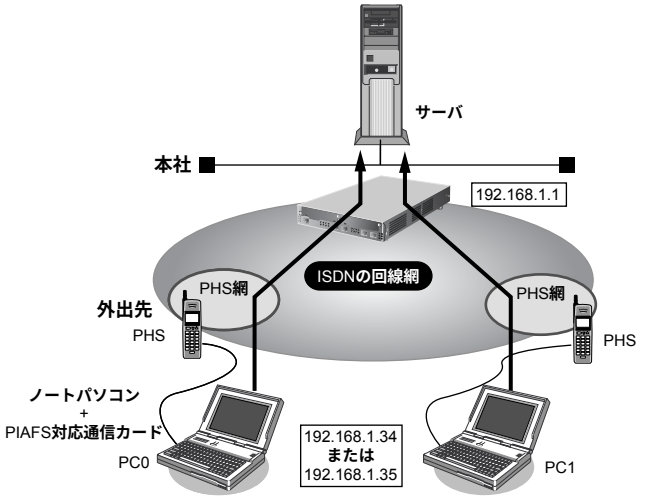
- デスクトップパソコン +TA →（ISDN）→本装置
- ノート型パソコン +ISDN カード →（ISDN）→本装置
- ノート型パソコン +PIAFS 通信カード +PHS →（PHS 網）→（ISDN）→本装置
- 本装置→（ISDN）→本装置

本装置では、テンプレート着信機能を使用した不特定着信と、AAA による認証（ローカル認証、RADIUS 認証）を組み合わせることで、リモートアクセスサーバを実現することができます。

参照 Si-R シリーズ　機能説明書「2.27 テンプレート着信機能」（P.128）

2.39.1 1 台の装置でリモートアクセスサーバを構成する

ここでは、ノートパソコンに PHS を繋いで外出先から本社のネットワークに接続する場合を例に説明します。



● 設定条件

- SLOT0 に装着した BRI 拡張モジュール L2（Si-R220B 以外）または ISDN U ポート（Si-R220B）を使用して ISDN 回線に接続する
- テンプレートで使用するインタフェース　：rmt30 から 2 個
- 以下からの着信を許可する

  [PC0 ＜ノートパソコン＋ PHS ＞で外出先から接続]

  - 受諾認証 ID　：mobile-a
  - 受諾認証パスワード　：mobilepass-a
  - PHS の電話番号は未登録

[PC1＜ノートパソコン＋ PHS ＞で外出先から接続]

- 受諾認証 ID　：mobile-b
- 受諾認証パスワード　：mobilepass-b
- PHS の電話番号は未登録

- 本社の LAN 側のネットワークアドレス/ネットマスク　：192.168.1.0/24
- 外部のパソコンに割り当てる IP アドレス　：192.168.1.34、192.168.1.35

こんな事に気をつけて

- テンプレート着信機能をサポートする回線は ISDN です（MP 接続はできません）。
- テンプレート着信で使用するインタフェースはテンプレート専用になります。テンプレート用に予約された rmt インタフェースには、remote 定義を設定しないでください。
  たとえば、rmt30 ～ 47 インタフェースをテンプレート用に予約した場合、remote 30 ～ 47 までの remote 定義を設定しないでください。
- テンプレート情報を定義する場合（IP フィルタリングなど）、定義数は「テンプレート情報で設定した定義数×テンプレートで使用する rmt インタフェース数」で計算されるため、それを含めて装置最大定義数の範囲に収まるように定義してください。装置最大定義数を超えたときは、資源不足により該当機能が動作しない場合があります。
- 接続先情報を設定する場合、テンプレート用のインタフェースの個数分は設定しないでください。
  たとえば、接続先定義を最大 48 定義可能な装置で、10 インタフェースをテンプレート用に使用する場合、接続先定義の定義数は 38 となります。
- テンプレート情報と AAA 情報のユーザ側の設定に同じ項目がある場合は、個人情報である AAA 情報が適用されます。AAA 情報の未登録の項目に対しては、テンプレート情報の設定値が適用されます。
- 発信者番号による識別（CLID 相手判定）を AAA 情報に設定していない場合は、発信者番号による相手判定は行いません（PPP のユーザ認証の結果だけで接続できるかどうかが決まります）。
- AAA 情報に同一ユーザ（パスワードも同一）が存在するときには、定義番号が小さい AAA ユーザ情報が優先されます。定義番号が大きいユーザ情報に発信者番号が一致する定義があり、定義番号が小さいユーザ情報に発信番号で識別を行わない定義がある場合も、定義番号の小さいユーザで着信が行われます。
- 共通 ID で複数の着信を行う場合は、AAA 情報のユーザ定義に、ID とパスワードだけを定義してください（個別情報を定義しないで、ID とパスワードだけのユーザ情報を定義すると共有 ID として扱われます）。

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。

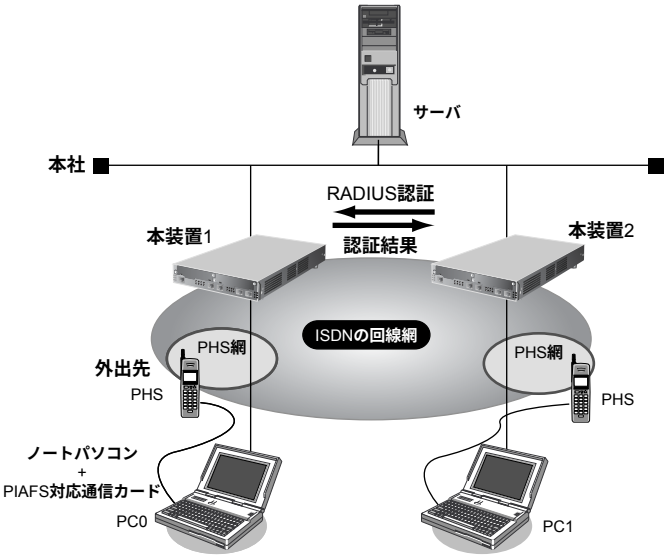
● コマンド

```
本社 LAN 側の IP アドレスを設定する
# lan 0 ip address 192.168.1.1/24 3

回線種別を設定する
# wan 0 bind 0（Si-R220B の場合は wan 0 bind mb 0）
# wan 0 line isdn

着信のためのテンプレートを設定する
# template 0 name mobile
# template 0 datalink bind wan 0
# template 0 interface pool 30 2
# template 0 ip address remote-pool 192.168.1.34 2
# template 0 aaa 0

認証情報を AAA のデータベースに設定する
# aaa 0 name mobile
# aaa 0 user 0 id mobile-a
# aaa 0 user 0 password mobilepass-a
# aaa 0 user 1 id mobile-b
# aaa 0 user 1 password mobilepass-b

設定終了
# save

再起動
# reset
```

2.39.2　複数台の装置でリモートアクセスサーバを構成する

RADIUS 機能を用いることで、アクセスユーザの情報を RADIUS サーバで一元管理し、複数のリモートアクセスサーバから同一のアクセスユーザ情報を利用できるようにすることができます。

ここでは、「2.39.1 1 台の装置でリモートアクセスサーバを構成する」（P.383）の構成から、さらにリモートアクセスサーバを増設し着信可能な回線数を増やす場合を例に説明します。



● 設定条件

[本装置 1]

- SLOT0 に装着した BRI 拡張モジュール L2（Si-R220B 以外）または ISDN U ポート（Si-R220B）を使用して ISDN 回線に接続する
- テンプレートで使用するインタフェース　：rmt30 から 2 個
- 以下からの着信を許可する

  [PC0 ＜ノートパソコン＋ PHS ＞で外出先から接続]

  - 受諾認証 ID　：mobile-a
  - 受諾認証パスワード　：mobilepass-a
  - PHS の電話番号は未登録

  [PC1 ＜ノートパソコン＋ PHS ＞で外出先から接続]

  - 受諾認証 ID　：mobile-b
  - 受諾認証パスワード　：mobilepass-b
  - PHS の電話番号は未登録
- 本社の LAN 側のネットワークアドレス/ネットマスク　：192.168.1.0/24
- 本社の LAN 側の IP アドレス　：192.168.1.1
- 外部のパソコンに割り当てる IP アドレス　：192.168.1.34、192.168.1.35
- 本装置に接続する RADIUS クライアントの IP アドレス　：192.168.1.2
- RADIUS 共有鍵　：rassharepass

[本装置 2]

- SLOT0 に装着した BRI 拡張モジュール L2（Si-R220B 以外）または ISDN U ポート（Si-R220B）を使用して ISDN 回線に接続する
- テンプレートで使用するインタフェース　：rmt30 から 2 個
- RADIUS サーバに問い合わせて着信を許可する
- 本社の LAN 側のネットワークアドレス / ネットマスク　：192.168.1.0/24
- 本社の LAN 側の IP アドレス　：192.168.1.2
- 外部のパソコンに割り当てる IP アドレス　：192.168.1.36、192.168.1.37
- 本装置が問い合わせる RADIUS サーバの IP アドレス　：192.168.1.1
- RADIUS 共有鍵　：rassharepass

こんな事に気をつけて

- **1 台の本装置上で、RADIUS サーバ機能と RADIUS クライアント機能を併用することはできません。**
- **1 台の本装置上で、RADIUS サーバ機能を複数設定することはできません。**
- **RADIUS プロトコルの制約で、同時に認証およびアカウンティングが行える数は 256 です。同時に 257 以上の認証とアカウンティングを行った場合は、両方とも失敗します。**
- **本装置の RADIUS 機能は 4096 バイトを超える RADIUS のパケットを扱えません。RADIUS サーバ機能を用いる場合は、経路情報を大量に設定すると（たとえば aaa user ip route だけの場合は約 130 個）この上限を超えてしまい、パケットが送出できず RADIUS クライアント側で認証が失敗します。**
- **AAA 情報の aaa user ip route、aaa user ip6 route で設定した distance 値は RADIUS サーバ機能では伝達することはできません。**
- **AAA 情報の aaa user ip address local で設定した自側 IP アドレスは RADIUS サーバ機能では伝達することはできません。**
- **RADIUS クライアント機能で受信した Framed-Route、Framed-IPv6-Route の情報は distance 値 100 の経路情報として扱われます。また、これらの経路情報を受け入れた結果、装置の経路数の上限を超えてしまう場合は回線は切断されます。**
- **RADIUS クライアント機能を定義しても、同じグループのユーザ情報は利用されます。AAA グループに RADIUS クライアント機能（aaa radius）とユーザ情報（aaa user）の両方を定義した場合、まず RADIUS で認証が行われます。RADIUS での認証が成功した場合はのユーザ情報は利用されませんが、RADIUS で認証に失敗した場合は、次にユーザ情報で認証を行います。**

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

[本装置 1]

```
本社 LAN 側の IP アドレスを設定する
# lan 0 ip address 192.168.1.1/24 3

回線種別を設定する
# wan 0 bind 0（Si-R220B の場合は wan 0 bind mb 0）
# wan 0 line isdn

着信のためのテンプレートを設定する
# template 0 name mobile
# template 0 datalink bind wan 0
# template 0 interface pool 30 2
# template 0 ip address remote-pool 192.168.1.34 2
# template 0 aaa 0

認証情報を AAA のデータベースに設定する
# aaa 0 name mobile
# aaa 0 user 0 id mobile-a
# aaa 0 user 0 password mobilepass-a
# aaa 0 user 1 id mobile-b
# aaa 0 user 1 password mobilepass-b

認証情報を本装置 2 からも利用するため RADIUS サーバを設定する
# aaa 0 radius service server both
# aaa 0 radius server client-info 0 address 192.168.1.2
# aaa 0 radius server client-info 0 secret rassharepass

設定終了
# save

再起動
# reset
```

[本装置 2]

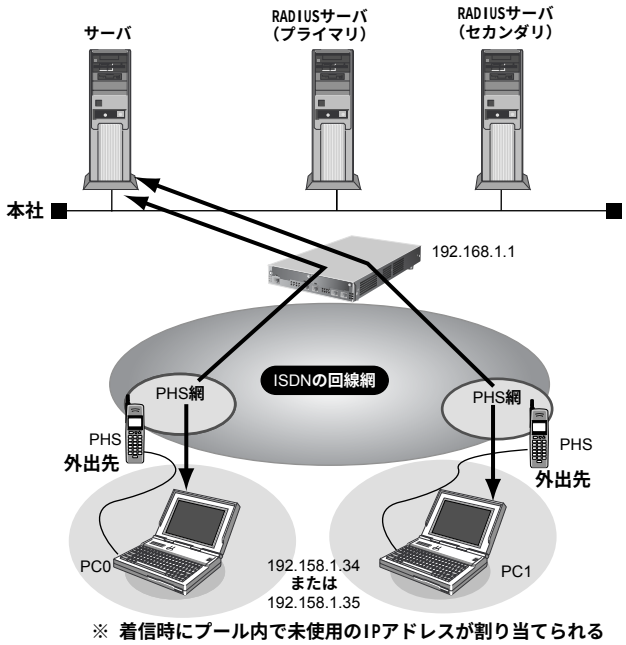
```
本社 LAN 側の IP アドレスを設定する
# lan 0 ip address 192.168.1.2/24 3

回線種別を設定する
# wan 0 bind 0（Si-R220B の場合は wan 0 bind mb 0）
# wan 0 line isdn

着信のためのテンプレートを設定する
# template 0 name mobile
# template 0 datalink bind wan 0
# template 0 interface pool 30 2
# template 0 ip address remote-pool 192.168.1.36 2
# template 0 aaa 0

認証情報を本装置 1 から利用するため RADIUS クライアントを設定する
# aaa 0 radius service client both
# aaa 0 radius client server-info auth 0 address 192.168.1.1
# aaa 0 radius client server-info auth 0 secret rassharepass
# aaa 0 radius client server-info accounting 0 address 192.168.1.1
# aaa 0 radius client server-info accounting 0 secret rassharepass

設定終了
# save

再起動
# reset
```

2.39.3　リモートアクセスサーバが使用するRADIUSサーバを多重化する

適用機種　*Si-R220B, 370, 570*

RADIUS 機能を用いて、複数台のRADIUS サーバを使用することで、RADIUS サーバの信頼性を向上させることができます。

ここでは、「2.39.1 1台の装置でリモートアクセスサーバを構成する」（P.383）の構成から、RADIUS サーバを増設する場合を例に説明します。



● 設定条件

- SLOT0 に装着したBRI 拡張モジュールL2（Si-R220B 以外）またはISDN U ポート（Si-R220B）を使用してISDN 回線に接続する
- テンプレートで使用するインタフェース　：rmt30 から 2 個
- 本社のLAN 側のネットワークアドレス/ネットマスク　：192.168.1.0/24
- 本社のLAN 側のIP アドレス　：192.168.1.1
- RADIUS 認証サーバ（プライマリ）のIP アドレス　: 192.168.1.2
- RADIUS 認証サーバ（プライマリ）の共有鍵　: rassharepass
- RADIUS 認証サーバ（セカンダリ）のIP アドレス　: 192.168.1.3
- RADIUS 認証サーバ（セカンダリ）の共有鍵　: rassharepass
- RADIUS アカウンティングサーバ（プライマリ）のIP アドレス : 192.168.1.2
- RADIUS アカウンティングサーバ（プライマリ）の共有鍵　: rassharepass
- RADIUS アカウンティングサーバ（セカンダリ）のIP アドレス : 192.168.1.3
- RADIUS アカウンティングサーバ（セカンダリ）の共有鍵　: rassharepass

[RADIUS サーバに登録する情報（プライマリ、セカンダリ共通)]

- PC0（ノートパソコン +PHS）で外出先から接続
  - 認証ユーザ ID　：mobile-a
  - 認証ユーザパスワード　：mobilepass-a
- PC1（ノートパソコン +PHS）で外出先から接続
  - 認証ユーザ ID　：mobile-b
  - 認証ユーザパスワード　：mobilepass-b

こんな事に気をつけて

- **テンプレート着信で使用するインタフェースはテンプレート専用になりますので、範囲に含まれる rmt インタフェースには remote 定義を設定しないでください。**
  例：rmt30 から rmt47 をテンプレートで予約した場合、remote 30 から remote 47 までの remote 定義に対して設定しないでください。
- **テンプレート情報内で設定されている定義の中で、RADIUS サーバのユーザ側にも同じ項目の定義が存在する場合は、RADIUS サーバでの設定値が適用されます。**
  RADIUS サーバで未登録の項目に対しては、テンプレート情報の設定値が適用されます。

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

```
本社 LAN 側の IP アドレスを設定する
# lan 0 ip address 192.168.1.1/24 3

回線種別を設定する
# wan 0 bind 0 （Si-R220 の場合は wan 0 bind mb 0）
# wan 0 line isdn

着信のためのテンプレートを設定する
# template 0 name mobile
# template 0 datalink bind wan 0
# template 0 interface pool 30 2
# template 0 ip address remote pool 192.168.1.34 2
# template 0 aaa 0

RADIUS クライアントに関する情報を設定する
# aaa 0 radius service client both
# aaa 0 radius client server-info auth 0 secret rassharepass
# aaa 0 radius client server-info auth 0 address 192.168.1.2
# aaa 0 radius client server-info auth 0 deadtime 30m
# aaa 0 radius client server-info auth 0 priority 0
# aaa 0 radius client server-info auth 1 secret rassharepass
# aaa 0 radius client server-info auth 1 address 192.168.1.3
# aaa 0 radius client server-info auth 1 deadtime 30m
# aaa 0 radius client server-info auth 1 priority 100
# aaa 0 radius client server-info accounting 0 secret rassharepass
# aaa 0 radius client server-info accounting 0 address 192.168.1.2
# aaa 0 radius client server-info accounting 0 deadtime 30m
# aaa 0 radius client server-info accounting 0 priority 0
# aaa 0 radius client server-info accounting 1 secret rassharepass
# aaa 0 radius client server-info accounting 1 address 192.168.1.3
# aaa 0 radius client server-info accounting 1 deadtime 30m
# aaa 0 radius client server-info accounting 1 priority 100

設定終了
# save

再起動
# reset
```

2.40 スイッチポートを使う

適用機種 ***Si-R180***

本装置ではLAN1 側のポートをスイッチングHUB として使用するか、従来の単独ポートとして使用するかを構成定義により選択できます。また、スイッチングHUB として使用する場合はVLAN 機能を併用することでスイッチポート（SW1~4）を独立ポートとして使用することもできます。

本装置のスイッチポートでは以下のような形態が利用できます。

- スイッチポートをHUB として使用する
  以下の2 つの方法で使用できます。
  - VLAN ヘッダを含む場合は、一致するVLAN ID のみ転送を行う
    VLAN を使用しない場合、またはVLAN を使用する場合でVLAN ID に応じた転送を行うときに選択します。

    ☛ 参照 「2.40.1 スイッチポートをHUB として使用する」（P.392）

  - VLAN ヘッダに依存しないで、MAC アドレスのみでスイッチポート間の転送を行う
    VLAN を使用していてVLAN ヘッダごと転送する場合、またはブリッジ機能をVLAN タグ転送モードで使用する場合に選択します。

    ☛ 参照 「2.40.2 VLAN 透過モードを使用する」（P.394）

- スイッチポートを独立した4 ポートとして使用する
  スイッチポートをすべて別のインタフェースとして使用する場合に選択します。

  ☛ 参照 「2.40.3 スイッチポートを独立ポートとして使用する」（P.397）

- スイッチポートを独立した2 ポートずつに分割して使用する
  スイッチポートをすべて別のインタフェースとして使用する場合に選択します。

  ☛ 参照 「2.40.4 スイッチポートを分割して使用する」（P.399）

こんな事に気をつけて

- **本装置のスイッチポートのMTU は1532 バイトです。EoMPLS などのトンネルプロトコルを利用する場合はMTU をスイッチポートのMTU サイズ以下になるように設定するか、スイッチポートを無効にし、使用するパケットの最大長の転送が可能な外付けのスイッチを使用してください。**
- **スイッチポートを使用しかつVLAN 透過モードを使用しない場合は、LAN 定義をVLAN として定義します。そのため、VLAN を使用した場合と同じ注意事項が適用されます。スイッチポートを使用する前に必ず「VLAN 機能」に関する記述を確認してください。**

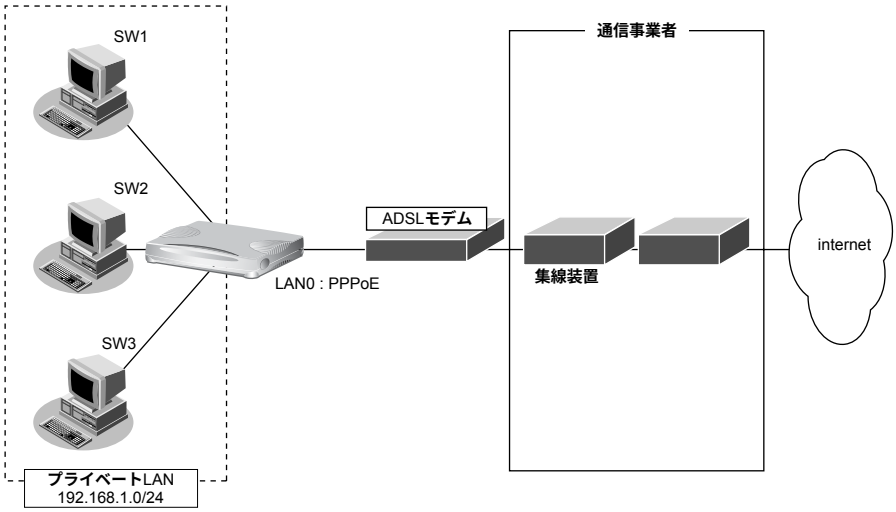
  ☛ 参照 「2.11 VLAN 機能を使う」（P.145）

2.40.1　スイッチポートを HUB として使用する

適用機種　*Si-R180*

接続するスイッチポートを HUB としてインターネットに接続する場合の設定方法を説明します。

参照 「1.7 インターネットへ PPPoE で接続する」（P.22）



● 設定条件

[通信事業者側]

- ユーザ認証 ID　：userid（プロバイダから提示された内容）
- ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- LAN0 ポートを使用する

[プライベート LAN 側]

- LAN1 側をスイッチポートとして使用する
- ローカルネットワークでは VLAN は使用しない
- ローカルネットワークでは DHCP サーバを使用し、パソコンに割り当てるアドレスは 192.168.1.2 から 64 個用意する
- 本装置の 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

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

```
ADSL モデムに接続するインタフェースを設定する
# delete lan 0
# lan 0 mode auto

スイッチポートを設定する
# switch 0 use on

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

LAN1 をスイッチポートにバインドする
# lan 1 vlan bind switch 0

DHCP サーバを設定する
# 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
# lan 1 ip dhcp service server
# lan 1 ip nat mode off

接続先の情報を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 autodial enable
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip route 0 default 1
# remote 0 ip rip use off off 0 off
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid userpass

ProxyDNS を設定する
# proxydns domain 0 any * any to 0
# proxydns address 0 any to 0

設定終了
# save

再起動
# reset
```

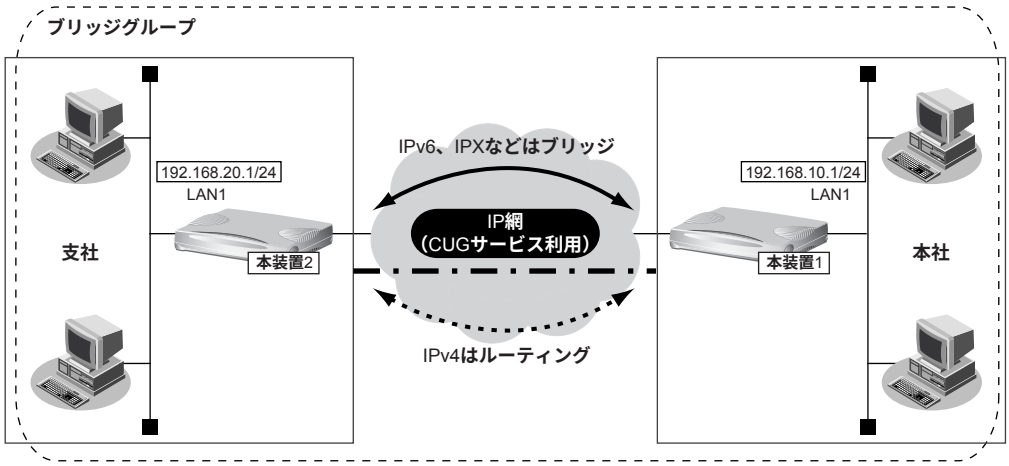
こんな事に気をつけて

- 本装置では VLAN ID の設定を省略した場合、VLAN ID として 1 が設定されたものとして動作します。
- 設定されたタグなし VLAN ID と同じ VLAN タグが付加されたパケットは、タグなし VLAN からパケットを受信したものとして処理されます。タグなし VLAN ID とネットワークで使用しているタグ付き VLAN ID が一致しないよう VLAN ID を設定してください。詳細については、「Si-R シリーズ　コマンドリファレンス」を参照してください。

2.40.2　VLAN 透過モードを使用する

VLAN 透過モードを使用すると、VLAN を使用しているネットワークで VLAN ヘッダも含めてスイッチングすることができます。

VLAN 透過モードを使用する場合の設定方法を説明します。



● 前提条件

- IP 網は、PPPoE 接続で LAN 型払い出しによりアドレス割り当てを行う CUG（Closed Users Group）サービスを利用する

[本社（PPPoE 常時接続)]

- 払い出される IPv4 アドレス（LAN1 ポートに設定）　：192.168.10.1/24
- PPPoE ユーザ認証 ID　：userid1@groupname
- PPPoE ユーザ認証パスワード　：userpass1
- PPPoE LAN ポート　：LAN0 ポート使用
- NAT 機能を使用しない
- 常時接続機能を使用する

[支社（PPPoE 常時接続)]

- 払い出される IPv4 アドレス（LAN1 ポートに設定）　：192.168.20.1/24
- PPPoE ユーザ認証 ID　：userid2@groupname
- PPPoE ユーザ認証パスワード　：userpass2
- PPPoE LAN ポート　：LAN0 ポート使用
- NAT 機能を使用しない
- 常時接続機能を使用する

● 設定条件

[本社]

- 自側エンドポイントアドレス　：192.168.10.1
- 相手側エンドポイントアドレス　：192.168.20.1

[支社]

- 自側エンドポイントアドレス　：192.168.20.1
- 相手側エンドポイントアドレス　：192.168.10.1

[本社、支社共通]

- ブリッジ対象インタフェース　：LAN0 ポートと IP トンネル
- IPv4 の転送方式　：ルーティングで転送
- IPv6 の転送方式　：ブリッジで転送
- VLAN タグを転送する

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（本社側）]

```
# delete lan
# delete switch

スイッチポートを設定する
# switch 0 use on
# switch 0 tag transparent enable

CUG サービスに接続する PPPoE の接続情報を設定する
# lan 0 mode auto
# remote 0 name CUG
# remote 0 mtu 1454
# remote 0 ap 0 name user1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid1@groupname userpass1
# remote 0 ap 0 keep connect
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414

LAN1 の IP アドレスを設定する
# lan 1 ip address 192.168.10.1/24 3

LAN1 をスイッチポートにバインドする
# lan 1 bind switch 0

IPv4 トンネルを設定する
# remote 1 name EtherIP
# remote 1 ap 0 name EtherIP
# remote 1 ap 0 datalink type ip
# remote 1 ap 0 tunnel local 192.168.10.1
# remote 1 ap 0 tunnel remote 192.168.20.1

ブリッジを行うインタフェースを設定する
# remote 1 bridge use on
# lan 1 bridge use on

ブリッジグループを設定する
# bridge 0 ip routing on
# bridge 0 ip6 routing off

設定終了
# save
# reset
```

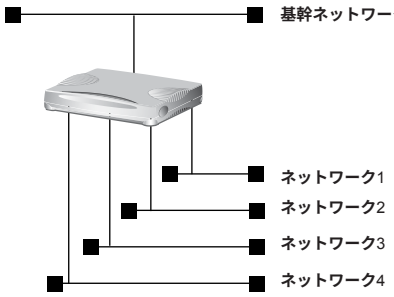
[本装置 2（支社側）]

```
# delete lan
# delete switch

スイッチポートを設定する
# switch 0 use on
# switch 0 tag transparent enable

CUG サービスに接続する PPPoE の接続情報を設定する
# lan 0 mode auto
# remote 0 name CUG
# remote 0 mtu 1454
# remote 0 ap 0 name user2
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid2@groupname userpass2
# remote 0 ap 0 keep connect
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip route 0 default 1 0
# remote 0 ip msschange 1414

LAN1 の IP アドレスを設定する
# lan 1 ip address 192.168.20.1/24 3

IPv4 トンネルを設定する
# remote 1 name EtherIP
# remote 1 ap 0 name EtherIP
# remote 1 ap 0 datalink type ip
# remote 1 ap 0 tunnel local 192.168.20.1
# remote 1 ap 0 tunnel remote 192.168.10.1

LAN1 をスイッチポートにバインドする
# lan 1 bind switch 0

ブリッジを行うインタフェースを設定する
# remote 1 bridge use on
# lan 1 bridge use on

ブリッジグループを設定する
# bridge 0 ip routing on
# bridge 0 ip6 routing off

設定終了
# save
# reset
```

2.40.3 スイッチポートを独立ポートとして使用する

適用機種 ***Si-R180***

スイッチポートをそれぞれ独立したLANポートとして使用する場合の設定方法を説明します。



● 設定条件

[基幹ネットワーク側]

- 本装置のIPアドレス　：10.200.100.1
- 本装置のネットワークアドレス/ネットマスク　：10.200.100.0/24
- ルーティング制御としてRIP（Version2）を使う
- DNSサーバ　：10.200.100.10

[ネットワーク1～4側]

- 本装置のIPアドレスは以下のとおり
  ネットワーク1　：192.168.1.1
  ネットワーク2　：192.168.2.1
  ネットワーク3　：192.168.3.1
  ネットワーク4　：192.168.4.1
- 本装置のネットワークアドレスおよびネットマスクは以下のとおり
  ネットワーク1　：192.168.1.0/24
  ネットワーク2　：192.168.2.0/24
  ネットワーク3　：192.168.3.0/24
  ネットワーク4　：192.168.4.0/24
- ネットワーク1～4ではVLANタグは使用しない
- ネットワーク1～4に対して、タグなしVLAN IDとしてそれぞれ10～13を割り当てる
- ネットワーク1～4ではDHCPサーバ機能を使用する
- ネットワーク1～4はそれぞれSW1～SW4ポートを使用する

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。

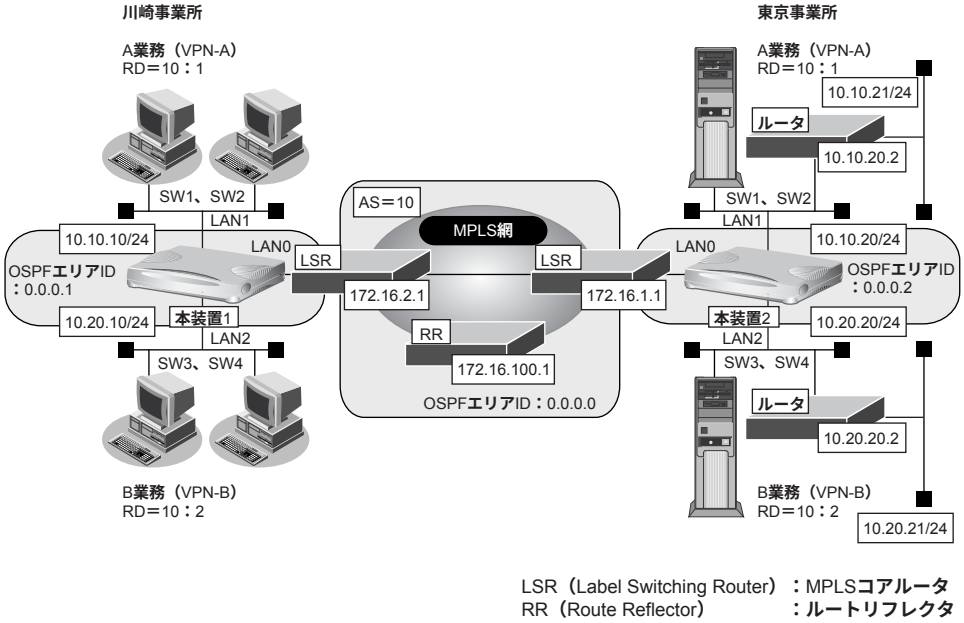
● コマンド

```
# delete lan
# delete switch

スイッチポートを設定する
# switch 0 use on
# switch 0 port 1 vlan untag 10
# switch 0 port 2 vlan untag 11
# switch 0 port 3 vlan untag 12
# switch 0 port 4 vlan untag 13

基幹ネットワーク側を設定する
# lan 0 ip address 10.200.100.1/24 3
# lan 0 ip rip use v2m v2 0 off

ネットワーク 1 を設定する
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip dhcp info dns 10.200.100.10
# 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
# lan 1 ip dhcp service server
# lan 1 vlan tag vid 10
# lan 1 vlan bind switch 0

ネットワーク 2 を設定する
# lan 2 ip address 192.168.2.1/24 3
# lan 2 ip dhcp info dns 10.200.100.10
# lan 2 ip dhcp info address 192.168.2.2/24 253
# lan 2 ip dhcp info time 1d
# lan 2 ip dhcp info gateway 192.168.2.1
# lan 2 ip dhcp service server
# lan 2 vlan tag vid 11
# lan 2 vlan bind switch 0

ネットワーク 3 を設定する
# lan 3 ip address 192.168.3.1/24 3
# lan 3 ip dhcp info dns 10.200.100.10
# lan 3 ip dhcp info address 192.168.3.2/24 253
# lan 3 ip dhcp info time 1d
# lan 3 ip dhcp info gateway 192.168.3.1
# lan 3 ip dhcp service server
# lan 3 vlan tag vid 12
# lan 3 vlan bind switch 0

ネットワーク 4 を設定する
# lan 4 ip address 192.168.4.1/24 3
# lan 4 ip dhcp info dns 10.200.100.10
# lan 4 ip dhcp info address 192.168.4.2/24 253
# lan 4 ip dhcp info time 1d
# lan 4 ip dhcp info gateway 192.168.4.1
# lan 4 ip dhcp service server
# lan 4 vlan tag vid 13
# lan 4 vlan bind switch 0

設定終了
# save
# reset
```

2.40.4 スイッチポートを分割して使用する

適用機種 ***Si-R180***

4つのスイッチポートを2ポートずつに分割して使用する場合の設定方法を説明します。



● 設定条件

- MPLS網の使用条件
  BGP AS番号　：10
  RRのIPアドレス　：172.16.100.1
  MPLS網で使用するIPv4ネットワーク　：OSPF
  　：バックボーンエリア
- VPN-Aの使用条件
  ルート識別子　：10:1
  使用するネットワーク　：10.10.10/24 川崎事業所
  　：10.10.20/24 東京事業所
  　：10.10.21/24 東京事業所
- VPN-Bの使用条件
  ルート識別子　：10:2
  使用するネットワーク　：10.20.10/24 川崎事業所
  　：10.20.20/24 東京事業所
  　：10.20.21/24 東京事業所

[本装置1]

- スイッチポートを事業所内ネットワークの接続ポートとして使用する
- 川崎事業所のネットワークではVLANタグを使用しない
- スイッチポートの2ポートずつを異なるネットワークとし、VLAN ID、LAN定義およびネットワークアドレスを以下のように対応付ける
  - SW1、SW2ポート
    VLAN ID：2　LAN定義：LAN1　ネットワークアドレス：10.10.10.0/24
  - SW3、SW4ポート
    VLAN ID：3　LAN定義：LAN2　ネットワークアドレス：10.20.10.0/24

- LAN0 の IP アドレス　：172.16.2.2
- LAN1 の IP アドレス　：10.10.10.1
- LAN2 の IP アドレス　：10.20.10.1
- LAN0 ～ 2 では、NAT 機能および DHCP クライアント機能は使用しない
- ループバックインタフェースの IP アドレス　：10.1.1.1
- ループバックインタフェースでのルーティングプロトコル　：OSPF
- ループバックインタフェースでの OSPF エリア ID　：0.0.0.1
- LAN0 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 で使用する VPN　：VPN-A
- LAN2 で使用する VPN　：VPN-B

[本装置 2]

- スイッチポートを事業所内ネットワークの接続ポートとして使用する
- 川崎事業所のネットワークでは VLAN タグを使用しない
- スイッチポートの 2 ポートずつを異なるネットワークとし、VLAN ID、LAN 定義およびネットワークアドレスを以下のように対応付ける
  - SW1、SW2 ポート
    VLAN ID：2　LAN 定義：LAN1　ネットワークアドレス：10.10.20.0/24
  - SW3、SW4 ポート
    VLAN ID：3　LAN 定義：LAN2　ネットワークアドレス：10.20.20.0/24
- LAN0 の IP アドレス　：172.16.1.2
- LAN1 の IP アドレス　：10.10.20.1
- LAN2 の IP アドレス　：10.20.20.1
- LAN0 ～ 2 では、NAT 機能および DHCP サーバ／クライアント機能は使用しない
- ループバックインタフェースの IP アドレス　：10.2.1.1
- ループバックインタフェースでのルーティングプロトコル　：OSPF
- ループバックインタフェースでの OSPF エリア ID　：0.0.0.2
- LAN0 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 で使用する VPN　：VPN-A
- LAN1 で使用する BGP/MPLS VPN スタティック経路情報
  あて先 IP アドレス　：10.10.21.0/24
  中継ルータアドレス　：10.10.20.2
- LAN2 で使用する VPN　：VPN-B
- LAN2 で使用する BGP/MPLS VPN スタティック経路情報
  あて先 IP アドレス　：10.20.21.0/24
- 中継ルータアドレス　：10.20.20.2

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]

```
# delete switch
# delete lan

スイッチを設定する
# switch 0 use on
# switch 0 port 1 vlan untag 2
# switch 0 port 2 vlan untag 2
# switch 0 port 3 vlan untag 3
# switch 0 port 4 vlan untag 3

LAN0～2のアドレスを設定する
# lan 0 ip address 172.16.2.2/16 3
# lan 1 ip address 10.10.10.1/24 3
# lan 2 ip address 10.20.10.1/24 3

LAN1およびLAN2とスイッチポートをバインドする
# lan 1 vlan tag vid 2
# lan 1 vlan bind switch 0
# lan 2 vlan tag vid 3
# lan 2 vlan bind switch 0

ループバックインタフェースを設定する
# loopback ip address 0 10.1.1.1

MPLS網との接続情報を設定する
# lan 0 mpls use on
# mpls ldp router-id 10.1.1.1
# mpls ldp ip transport 10.1.1.1
# lan 0 ip ospf use on 0
# ospf ip area 0 id 0.0.0.1
# loopback ip ospf use on 0

RRとの接続情報を設定する
# bgp as 10
# bgp id 10.1.1.1
# bgp neighbor 0 address 172.16.100.1
# bgp neighbor 0 as 10
# bgp neighbor 0 family vpnv4
# bgp neighbor 0 source 10.1.1.1

VPN-A情報としてVRF0情報を設定する
# bgp vrf 0 rd 10 1
# routemanage ip redist bgp vrf 0 connected on

VPN-B情報としてVRF1情報を設定する
# bgp vrf 1 rd 10 2
# routemanage ip redist bgp vrf 1 connected on

LAN1にVPN-A（VRF0）を設定する
# lan 1 ip vrf use on 0

LAN2にVPN-B（VRF1）を設定する
# lan 2 ip vrf use on 1

設定終了
# save
# reset
```

[本装置 2]

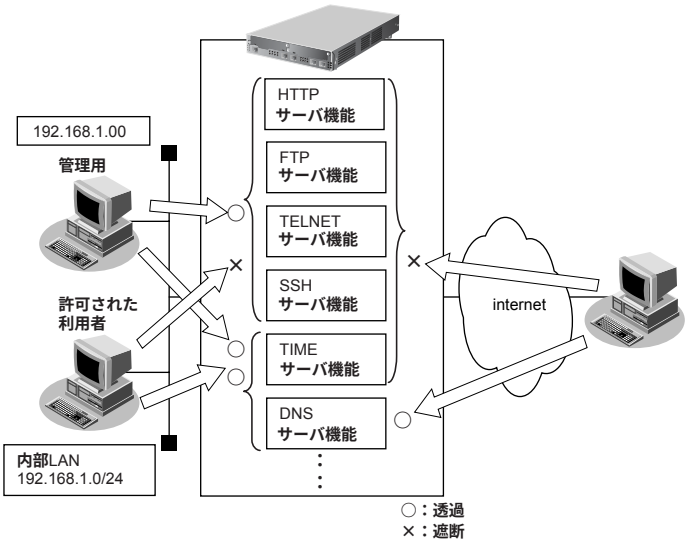
```
# delete switch
# delete lan

スイッチを設定する
# switch 0 use on
# switch 0 port 1 vlan untag 2
# switch 0 port 2 vlan untag 2
# switch 0 port 3 vlan untag 3
# switch 0 port 4 vlan untag 3

LAN0～2のアドレスを設定する
# lan 0 ip address 172.16.1.2/16 3
# lan 1 ip address 10.10.20.1/24 3
# lan 2 ip address 10.20.20.1/24 3

LAN1およびLAN2とスイッチポートをバインドする
# lan 1 vlan tag vid 2
# lan 1 vlan bind switch 0
# lan 2 vlan tag vid 3
# lan 2 vlan bind switch 0

ループバックインタフェースを設定する
# loopback ip address 0 10.2.1.1

MPLS網との接続情報を設定する
# lan 0 mpls use on
# mpls ldp router-id 10.2.1.1
# mpls ldp ip transport 10.2.1.1
# lan 0 ip ospf use on 0
# ospf ip area 0 id 0.0.0.2
# loopback ip ospf use on 0

RRとの接続情報を設定する
# bgp as 10
# bgp id 10.2.1.1
# bgp neighbor 0 address 172.16.100.1
# bgp neighbor 0 as 10
# bgp neighbor 0 family vpnv4
# bgp neighbor 0 source 10.2.1.1

VPN-A情報としてVRF0情報を設定する
# bgp vrf 0 rd 10 1
# routemanage ip redist bgp vrf 0 static on
# routemanage ip redist bgp vrf 0 connected on

VPN-B情報としてVRF1情報を設定する
# bgp vrf 1 rd 10 2
# routemanage ip redist bgp vrf 1 static on
# routemanage ip redist bgp vrf 1 connected on

LAN1にVPN-A（VRF0）を設定する
# lan 1 ip vrf use on 0
# lan 1 ip vrf route 0 10.10.21.0/24 10.10.20.2

LAN2にVPN-B（VRF1）を設定する
# lan 2 ip vrf use on 1
# lan 2 ip vrf route 0 10.20.21.0/24 10.20.20.2

設定終了
# save
# reset
```

2.41 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）からのみ HTTP/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）からのみ TIME サーバ機能へのアクセスを許可する。
- その他のサーバ機能は制限しない。

こんな事に気をつけて

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

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

● コマンド

```
制限するサーバ機能に対し、デフォルトのアクセスを遮断する
# serverinfo http filter default reject
# 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 http filter 0 accept acl 0
# 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
```

索引

O

P

R

S

T

U

V

W

あ

え

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

つ

て

と

に

ね

は

ふ

へ

ほ

ま

む

め

ゆ

り

れ

Si-R シリーズ　コマンド設定事例集

P3NK-2182-01Z0

発行日　　2006年9月

発行責任　　富士通株式会社