MR1000

取扱説明書

コマンド設定事例集

OMRON

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。

2005年1月初版
2005年3月第2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。

Microsoft® Windows® 2000 Server Network operating system、またはMicrosoft® Windows® 2000 Professional operating systemは、Windows® 2000と表記します。

フレッツは、NTT東日本・NTT西日本のサービス名であり、登録商標です。

フレッツ・ADSLは、NTT東日本・NTT西日本の登録商標です。

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。

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。

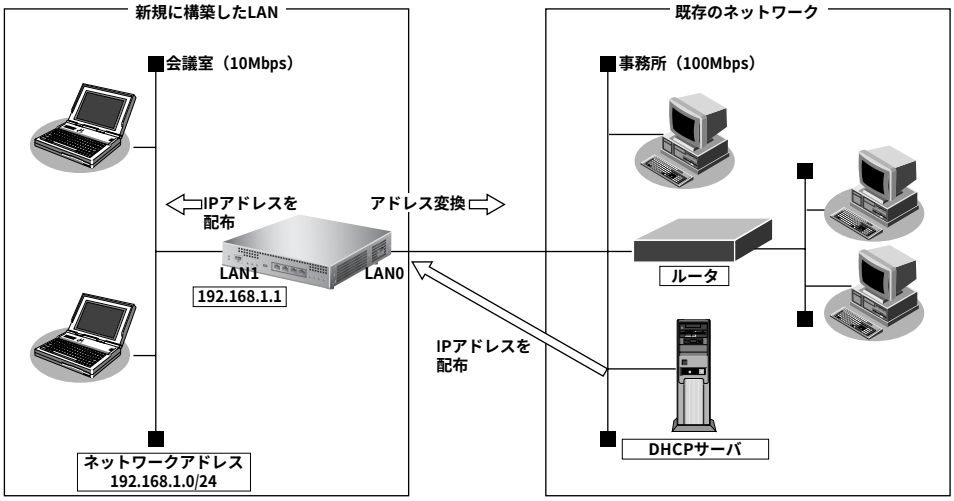
1.1　プライベートLANを構築する

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　MR1000　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.42）



● 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 MR1000　コマンドユーザーズガイド「1.4 コマンドで入力できる文字一覧」（P.18）

- **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
# enable
```

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.220）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　CATV インターネットに接続する

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。

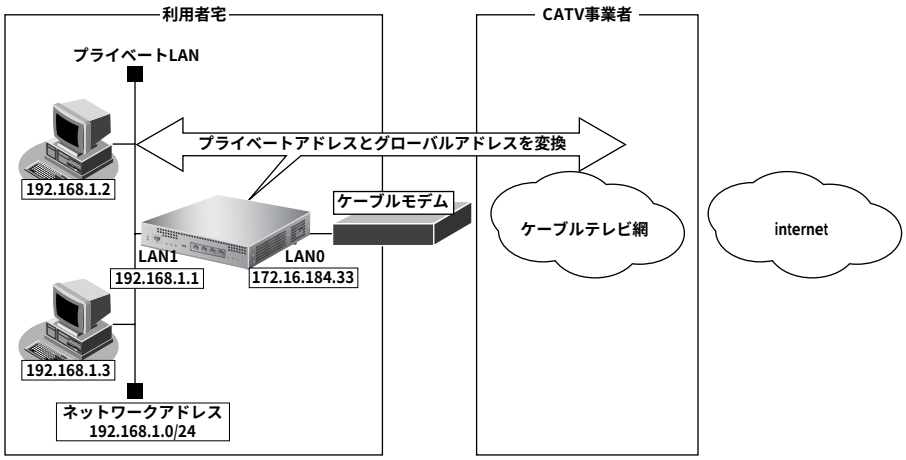
本装置を使った CATV インターネット接続は、CATV 事業者が提供するインターネット接続サービスをプライベート LAN 上の複数のパソコンから利用するための接続形態です。本装置と CATV 事業者が提供するケーブルモデムを接続することで、プライベート LAN 上のパソコンからインターネット接続サービスを利用できます。

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　MR1000　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.42）



● 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。**

● 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
```

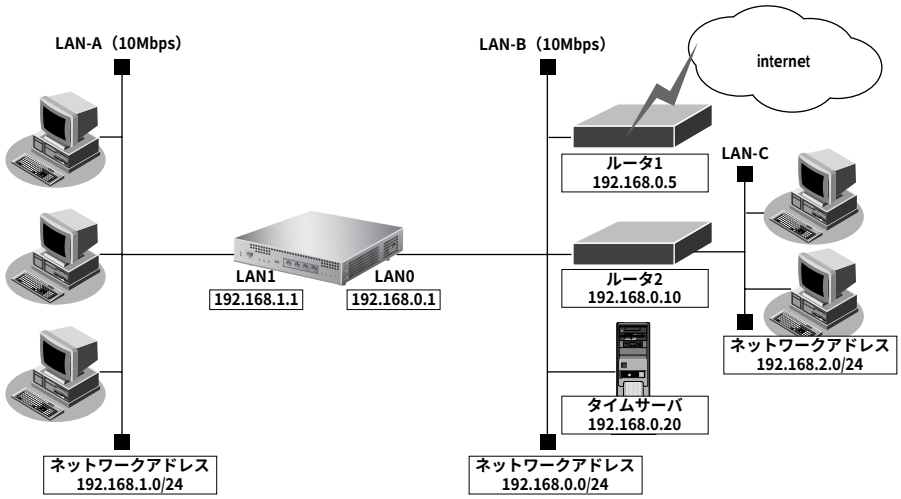
1.3　LAN をネットワーク間接続する

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　MR1000　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.42）



● 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付するプロトコルです。SNTP（Simple Network Time Protocol、RFC1361、RFC1769）は NTP（Network Time Protocol）のサブセットで、パソコンなど末端のクライアントマシンの時刻を同期させるのに適しています。

こんな事に気をつけて

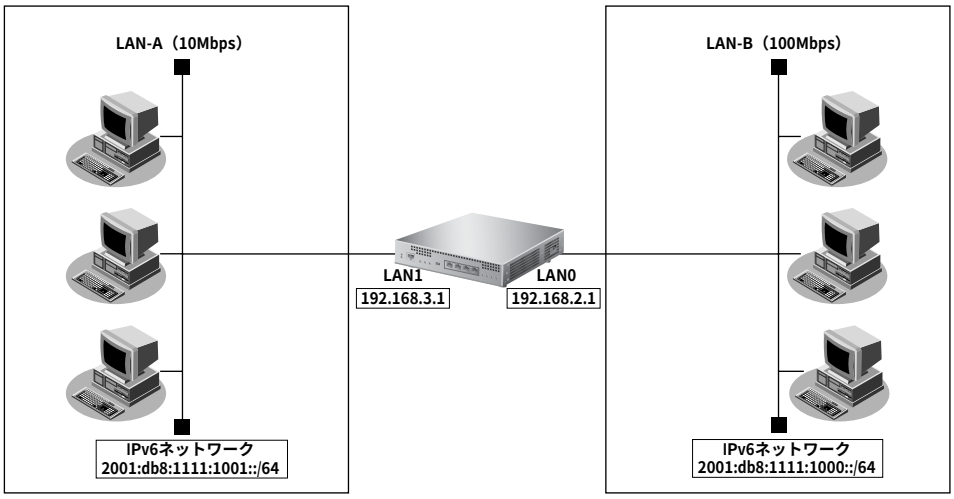
本装置の IP アドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。

● コマンド

```
LAN0 情報の設定
# 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 情報の設定
# 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

自動時刻の設定
# time auto server 192.168.0.20 time
# time auto interval start

設定終了
# save
# enable
```

1.4　IPv4のネットワークにIPv6ネットワークを追加する

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

● 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
# enable
```

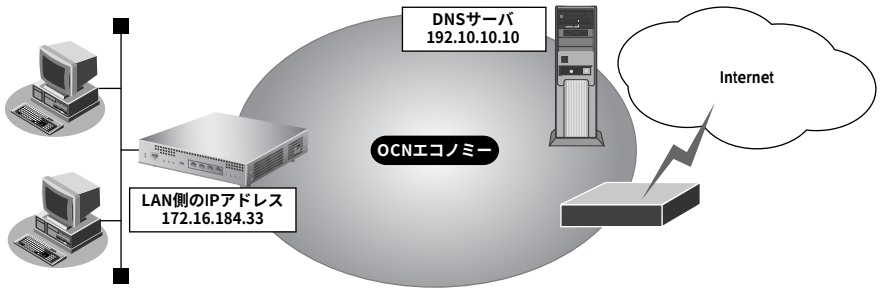
1.5　インターネットへ専用線で接続する

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　MR1000　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.42）



● 設定条件

- ISDN ポートで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　MR1000　コマンドユーザーズガイド「1.4 コマンドで入力できる文字一覧」（P.18）

- **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

回線情報を設定する
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

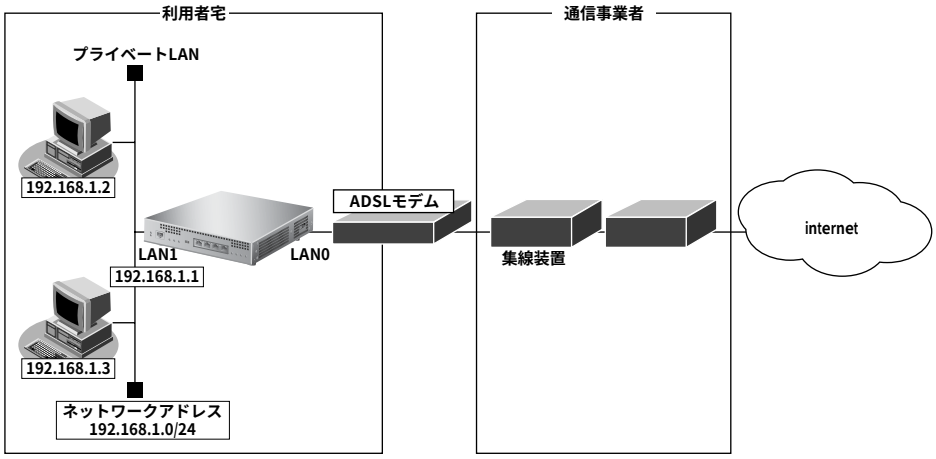
1.6　インターネットへ PPPoE で接続する

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　MR1000　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.42）



● 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　MR1000　コマンドユーザーズガイド「1.4 コマンドで入力できる文字一覧」（P.18）

- **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

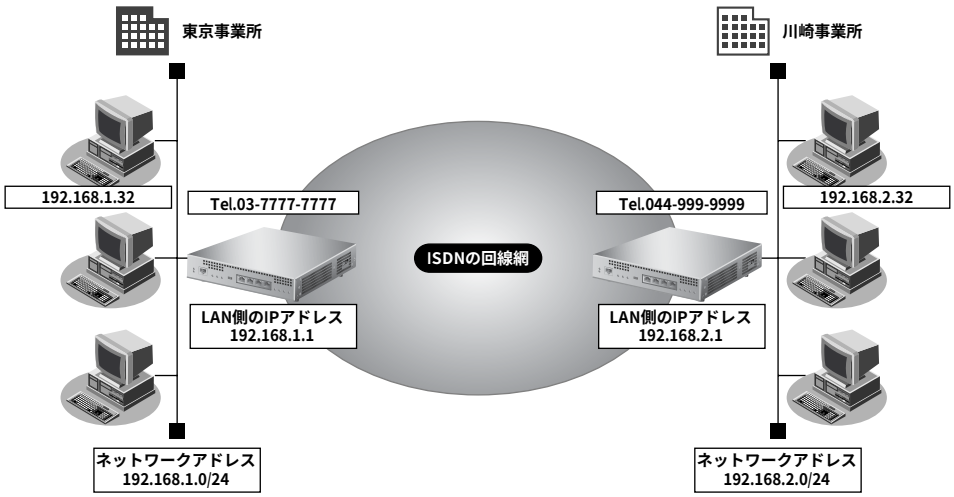
1.7　事業所LANをISDNで接続する

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　MR1000　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.42）



● 設定条件

- ISDNポートで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。

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 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 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
```

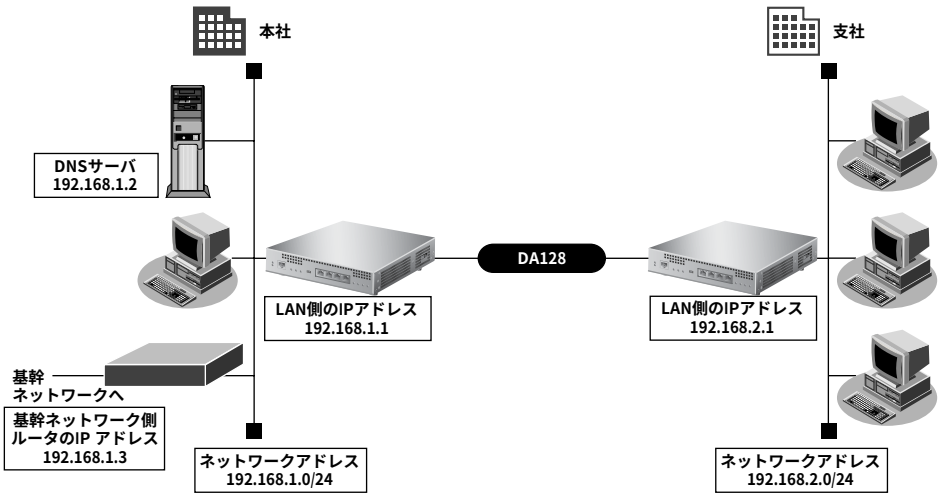
1.8　事業所 LAN を専用線で接続する

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　MR1000　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.42）



● 設定条件

- ISDN ポートで専用線（BRI：128Mbps）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 MR1000　コマンドユーザーズガイド「1.4 コマンドで入力できる文字一覧」（P.18）

- **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 line hsd 128k

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 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 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

「1.5 インターネットへ専用線で接続する」（P.15）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。

1.9　複数の事業所 LAN をフレームリレーで接続する

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。

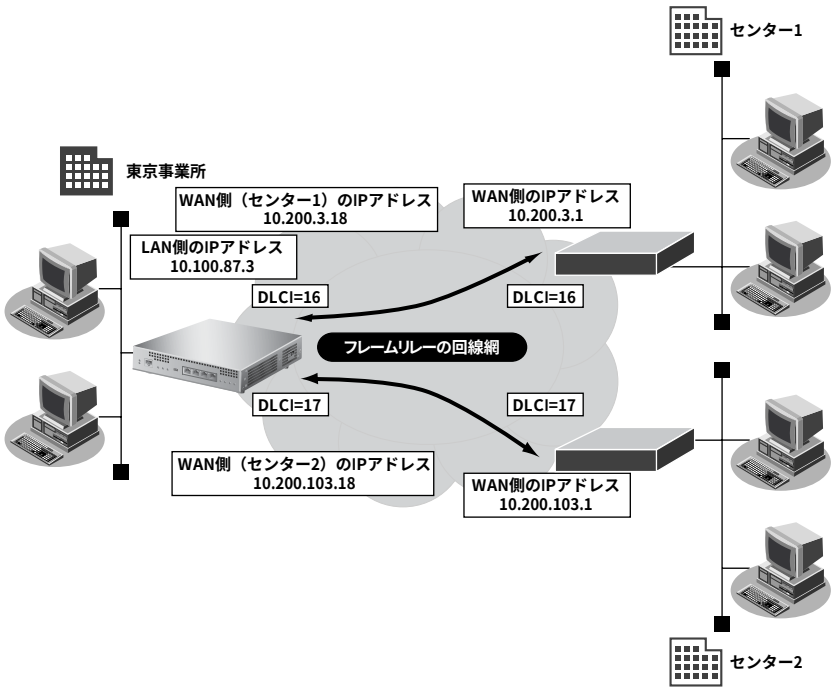
フレームリレーを利用すると複数の事業所の LAN と接続できるため、データを高速に転送することができます。

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　MR1000　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.42）



● 設定条件

- ISDN ポートでフレームリレー（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。

● コマンド

回線情報を設定する
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

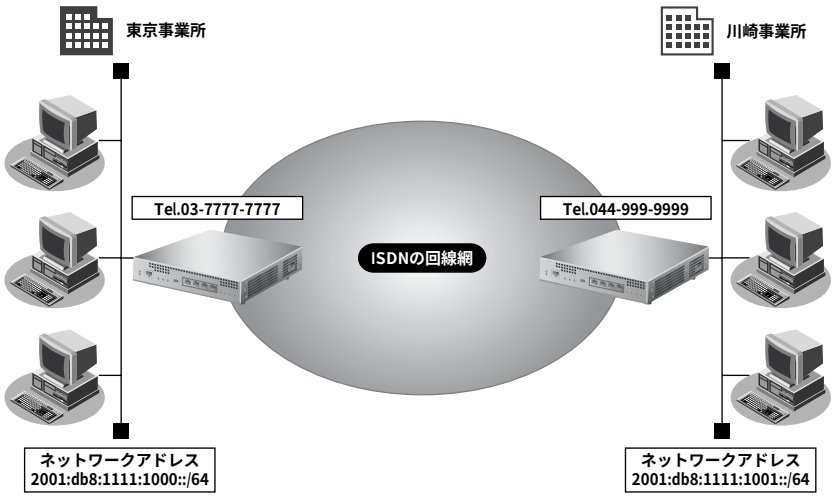
1.10　IPv6の事業所LANをISDNで接続する

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　MR1000　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.42）



● 設定条件

- ISDNポートで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 MR1000　コマンドユーザーズガイド「1.4 コマンドで入力できる文字一覧」（P.18）

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 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 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

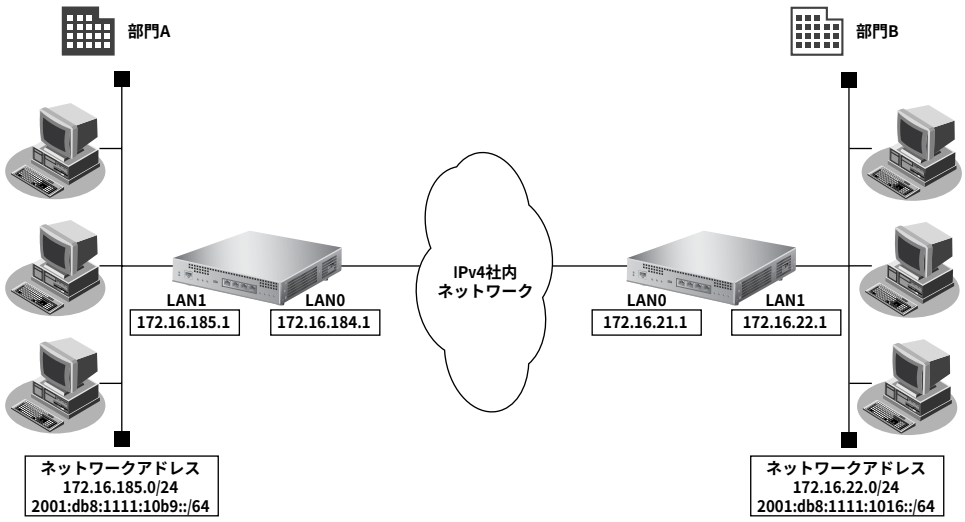
接続先の情報を設定する
remote 0 name kaisya
remote 0 ap 0 name tokyo
remote 0 ap 0 datalink bind wan 0
remote 0 ap 0 dial 0 number 03-7777-7777
remote 0 ap 0 dial 0 speed 64K
remote 0 ap 0 ppp auth type any
remote 0 ap 0 ppp auth send kawasaki kawapass
remote 0 ap 0 ppp auth receive tokyo tokyopass
remote 0 ap 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

1.11　IPv6 の事業所 LAN を IPv6 トンネルで接続する

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]

- ダイナミック経路を使用する
- 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]

- ダイナミック経路を使用する
- 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　MR1000　コマンドユーザーズガイド「1.4 コマンドで入力できる文字一覧」（P.18）

- **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。**

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
# 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 ip 6 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に本装置（NAT未使用）を利用する場合は、相手側の本装置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

1.12　複数の事業所LANをIP-VPN網を利用して接続する

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　MR1000　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.42）

- **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。**

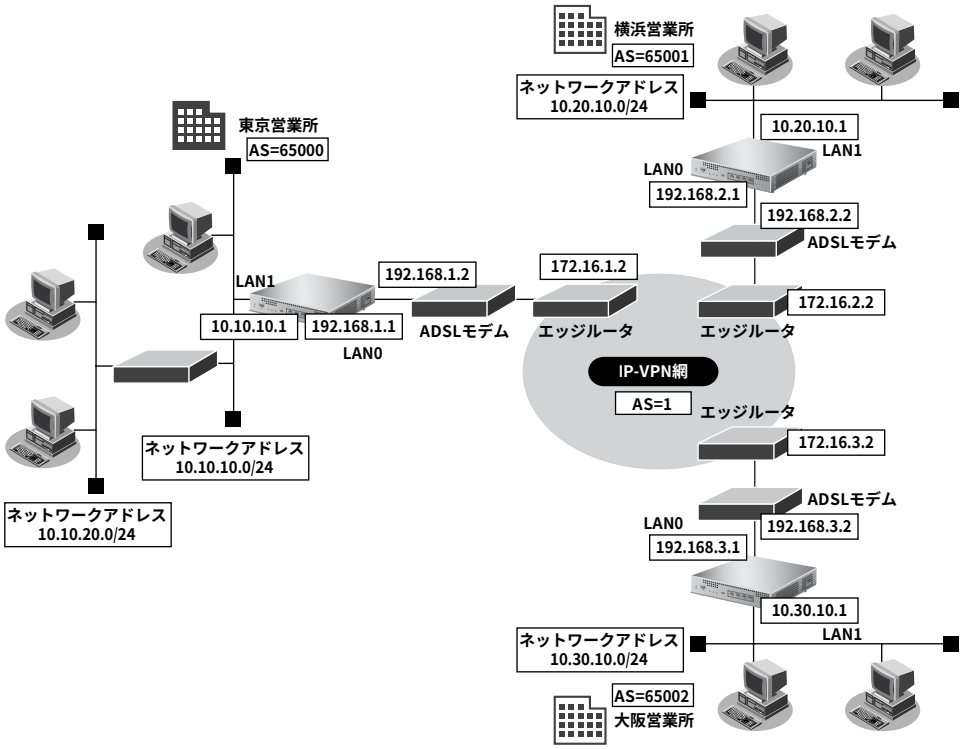
  ☛ 参照　MR1000　コマンドユーザーズガイド「1.4 コマンドで入力できる文字一覧」（P.18）

- **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 の認証機能はサポートしていません。**
- **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　MR1000　仕様一覧「2.3 システム最大値一覧」（P.19）

- **BGP 集約経路を設定した場合、設定した集約経路アドレス／アドレスマスクよりも長いサブネットマスクの経路は受信しません。**
- **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enable 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。**

1.12.1　ADSL モデムを使用して IP-VPN 網と接続する



● 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

東京営業所を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip address 192.168.1.1/24 3
# lan 0 ip nat mode off
# lan 0 ip dhcp service off
# 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

再起動
# reset
```

横浜営業所を設定する

● コマンド

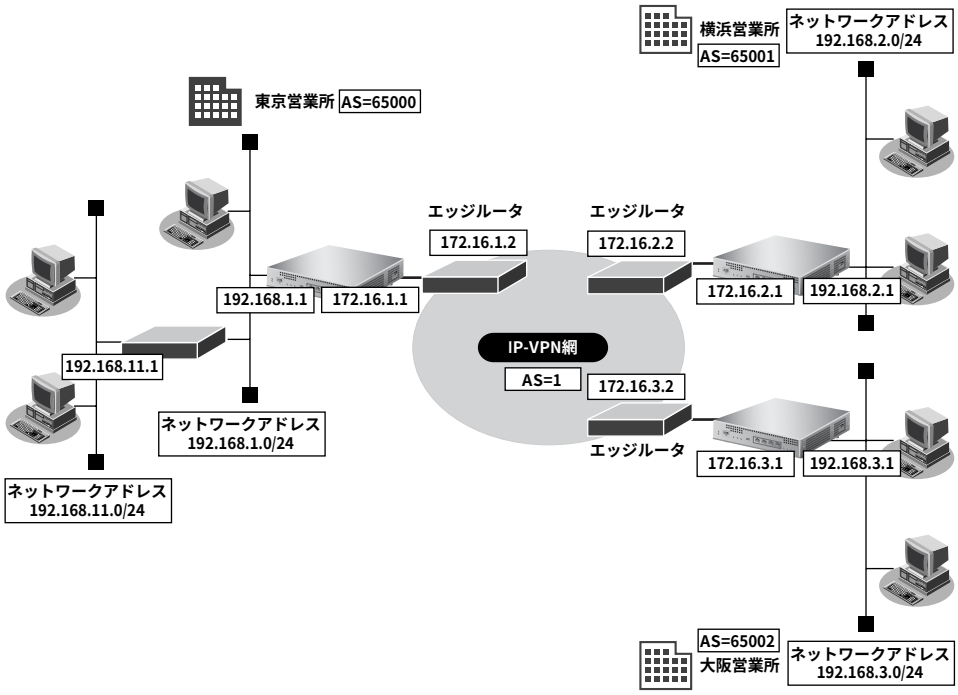
```
LAN 情報を設定する
# lan 0 ip address 192.168.2.1/24 3
# lan 0 ip nat mode off
# lan 0 ip dhcp service off
# lan 0 ip route 0 172.16.2.0/24  192.168.2.2 1
# lan 1 ip address 10.20.10.1/24 3

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

再起動
# reset
```

大阪営業所を設定する

● コマンド

```
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

再起動
# reset
```

1.12.2　高速ディジタル専用線を使用してIP-VPN網と接続する



● 設定条件

- ISDN ポート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

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 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

再起動
# reset
```

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 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

再起動
# reset
```

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 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

再起動
# reset
```

⚠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。**

1.13　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

● 設定コマンド

[支社A（PPPoE常時接続)]

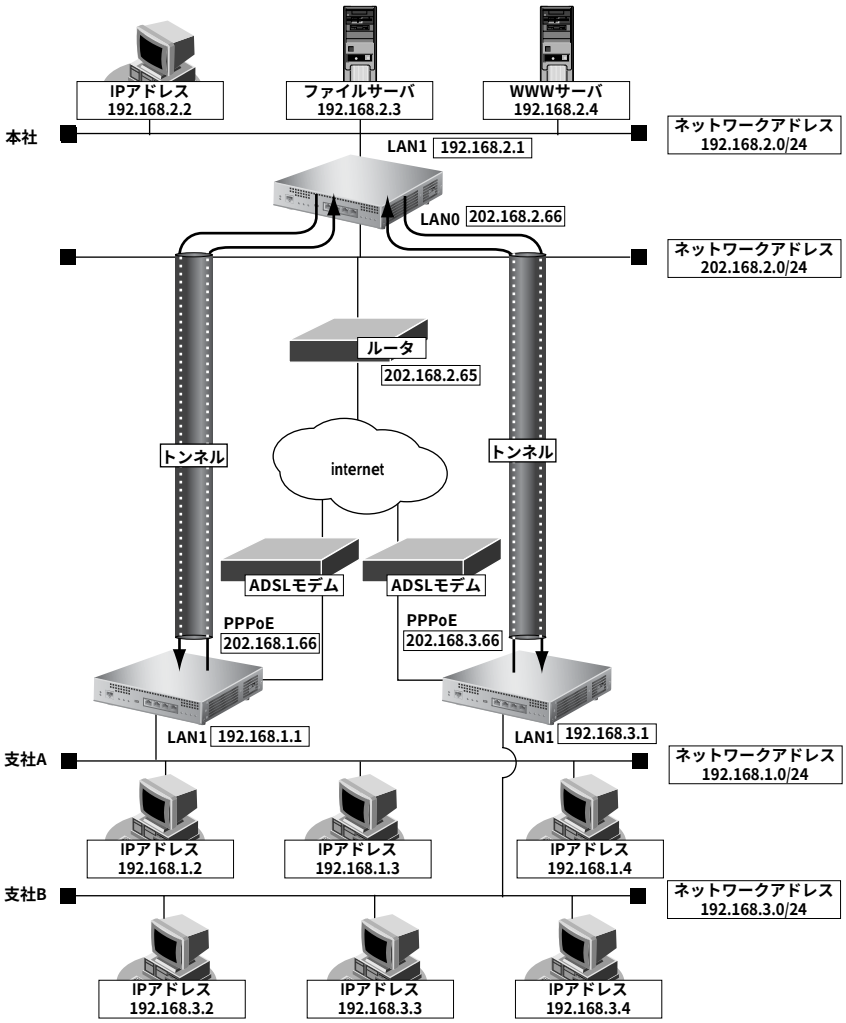
```
# delete lan 0
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid1 userpass1
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.1.66
# 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-l192.168.1.0/24
- 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-l192.168.3.0/24

[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
# enable
```

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
# enable
```

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
# enable
```

1.14　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

● 設定コマンド

[支社A（PPPoE常時接続）]

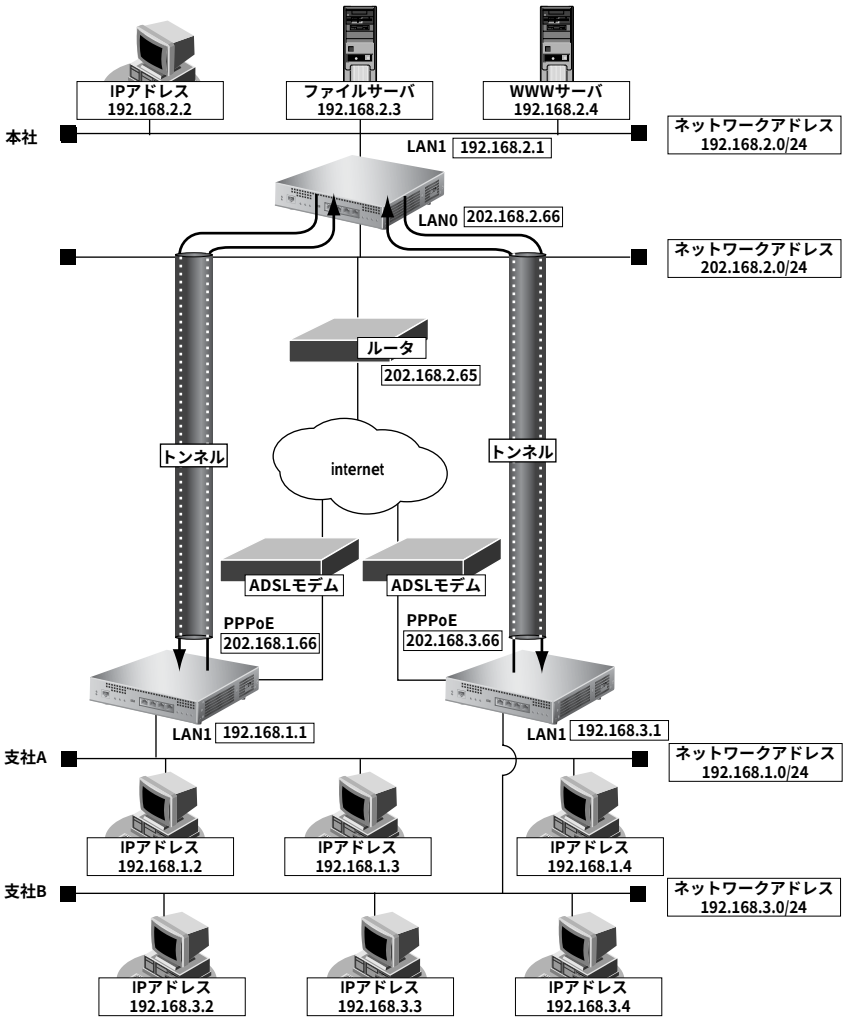
```
# delete lan 0
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send userid1 userpass1
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.1.66
# 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　：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-l192.168.1.0/24
- 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-l192.168.3.0/24

[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 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 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
# enable
```

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 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 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
# enable
```

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
# enable
```

1.15　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

● 設定コマンド

[支社A（PPPoE接続)]

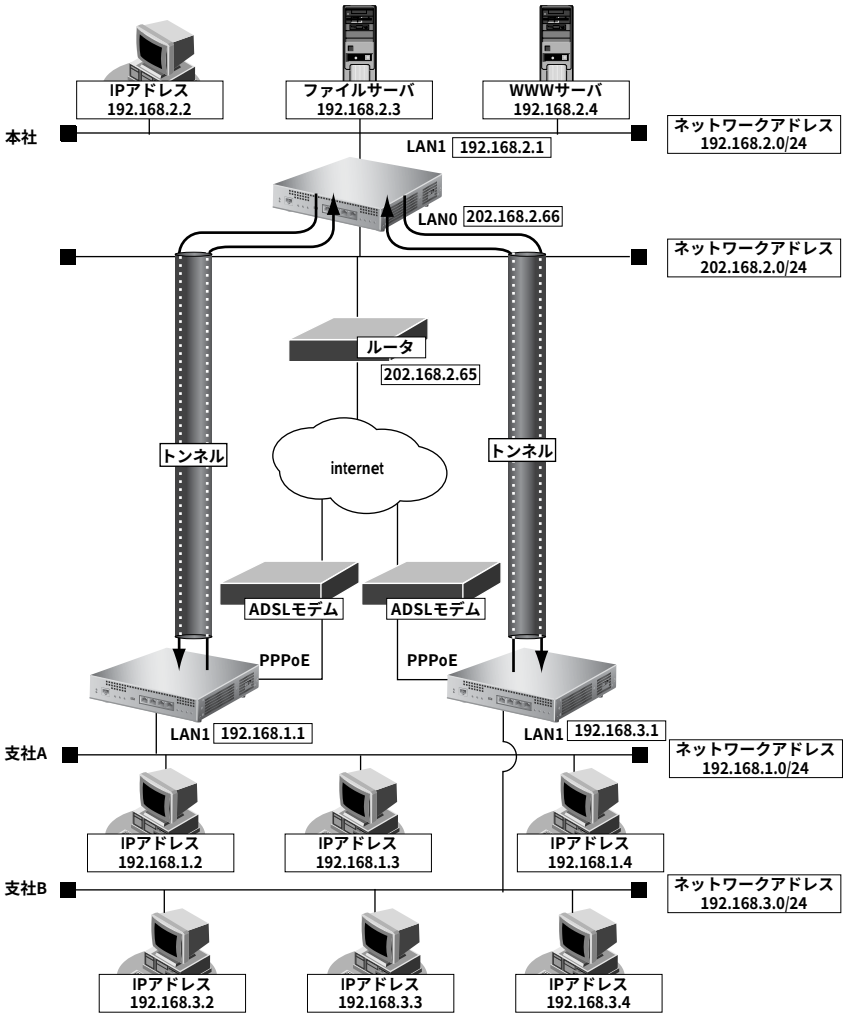
```
# delete lan 0
# lan 0 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 0
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp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

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
# enable
```

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
# enable
```

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）

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
- フィルタリング条件（IPアドレス／アドレスマスク）
- 方向
- 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、フィルタリング条件の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

フィルタリング条件　：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

フィルタリング条件　：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。

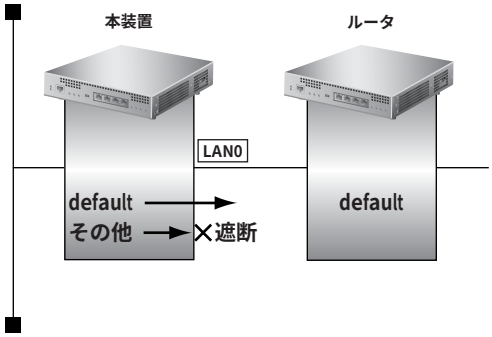
- 特定の経路情報の送信を禁止する
- 特定の経路情報の受信を禁止する

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

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。

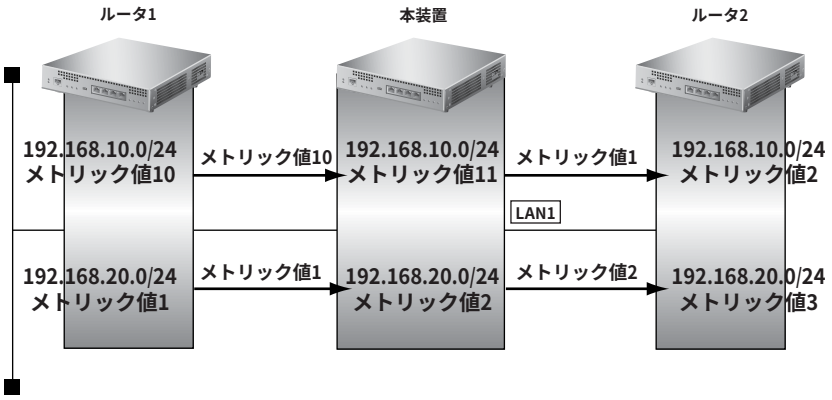
● コマンド

```
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
# enable
```

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

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

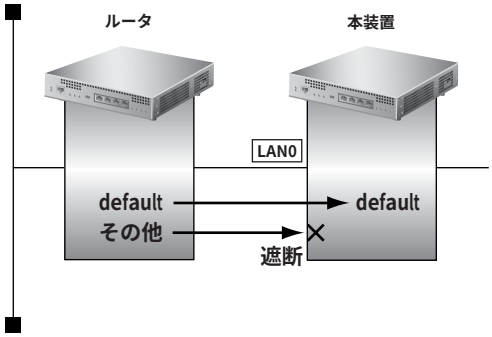
```
192.168.10.0/24 をメトリック値1で送信する
# lan 1 ip rip filter 0 act pass out
# lan 1 ip rip filter 0 route 192.168.10.0/24
# lan 1 ip rip filter 0 set metric 1

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
残りの経路情報は、すべて送信する
# lan 1 ip rip filter 1 act pass out
# lan 1 ip rip filter 1 route any

設定終了
# save
# enable
```

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

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

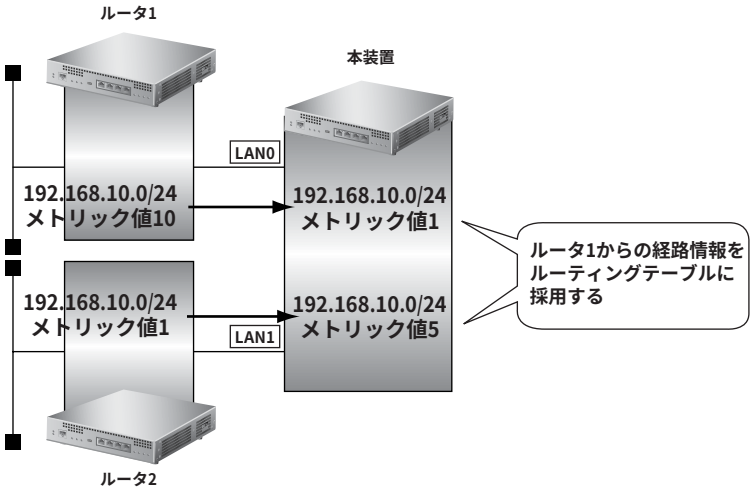
上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● 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
# enable
```

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

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

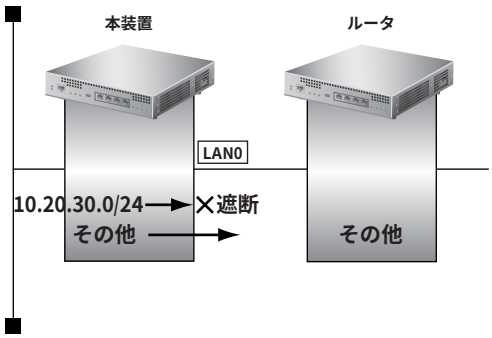
```
LAN0から192.168.10.0/24を受信した場合、メトリック値1で受信する
# lan 0 ip rip filter 0 act pass in
# lan 0 ip rip filter 0 route 192.168.10.0/24
# lan 0 ip rip filter 0 set metric 1

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
# enable
```

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

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

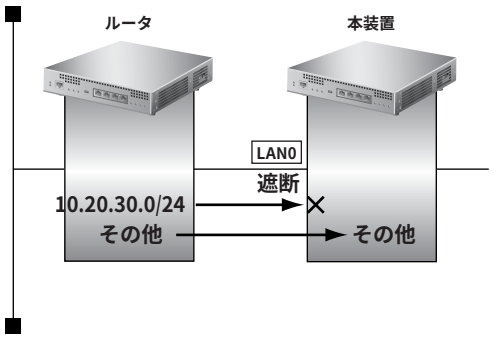
上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● 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
# enable
```

2.1.6　特定の経路情報の受信を禁止する

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
# enable
```

2.2 RIPの経路を制御する（IPv6）

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
- フィルタリング条件（プレフィックス／プレフィックス長）
- 方向
- 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。

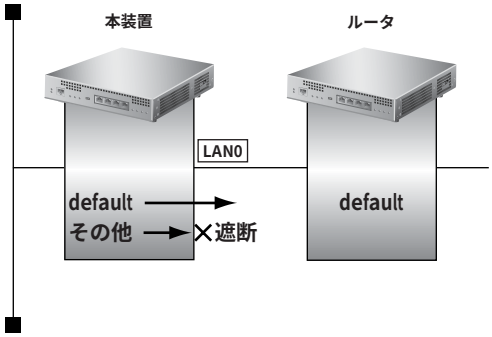
- 特定の経路情報の送信を禁止する
- 特定の経路情報の受信を禁止する

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

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。

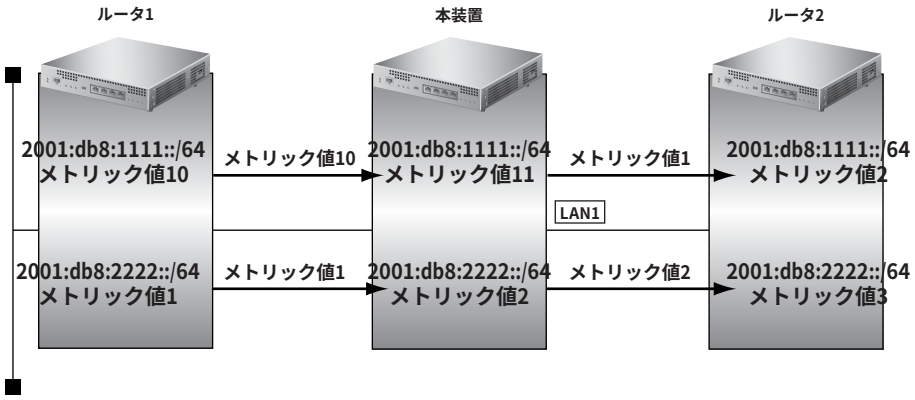
● コマンド

```
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
# enable
```

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

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

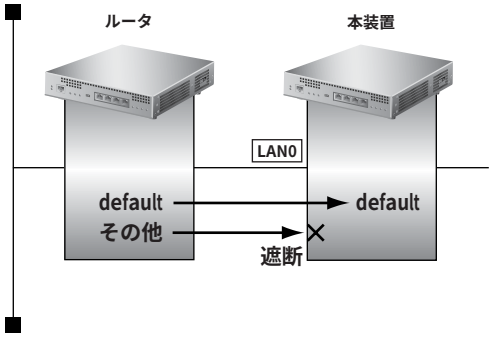
```
2001:db8:1111::/64 をメトリック値 1 で送信する
# lan 1 ip6 rip filter 0 act pass out
# lan 1 ip6 rip filter 0 route 2001:db8:1111::/64
# lan 1 ip6 rip filter 0 set metric 1

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
残りの経路情報は、すべて送信する
# lan 1 ip6 rip filter 1 act pass out
# lan 1 ip6 rip filter 1 route any

設定終了
# save
# enable
```

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

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

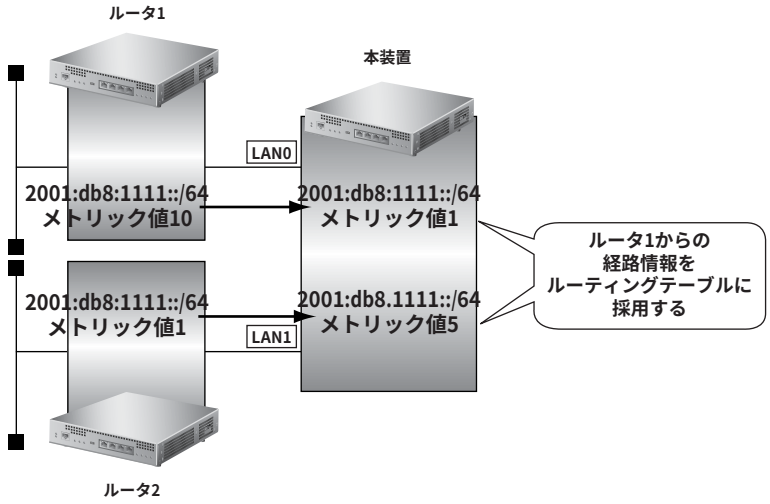
上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● 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
# enable
```

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

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

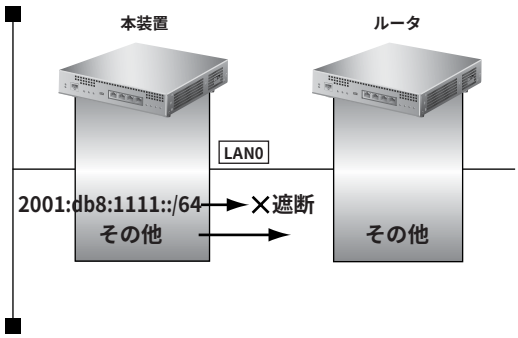
```
LAN0から2001:db8:1111::/64を受信した場合、メトリック値1で受信する
# lan 0 ip6 rip filter 0 act pass in
# lan 0 ip6 rip filter 0 route 2001:db8:1111::/64
# lan 0 ip6 rip filter 0 set metric 1

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
# enable
```

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

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

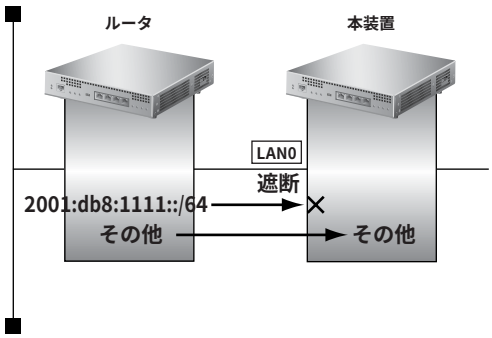
上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● 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
# enable
```

2.2.6　特定の経路情報の受信を禁止する

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
# enable
```

2.3　OSPFv2を使用したネットワークを構築する（IPv4）

ここでは、OSPFv2を使用したダイナミック経路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。

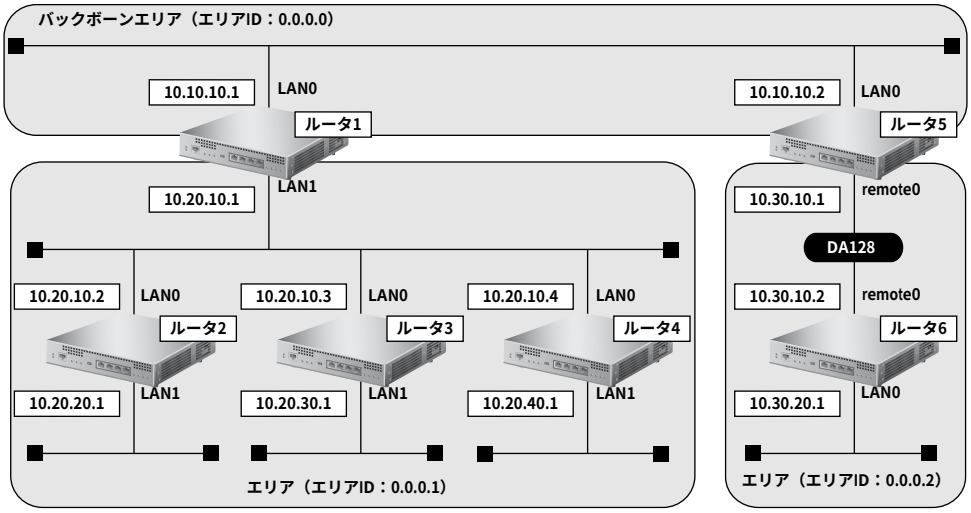
エリア境界ルータでは、エリア内の経路情報を集約して広報することができます。

参照　MR1000　機能説明書「2.5 OSPF機能」（P.33）

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、enable/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enable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。

項目	条件
インタフェース数	（30000÷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、ISDNポート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

再起動
# reset
```

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

再起動
# reset
```

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

再起動
# reset
```

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

再起動
# reset
```

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

再起動
# reset
```

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

再起動
# reset
```

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

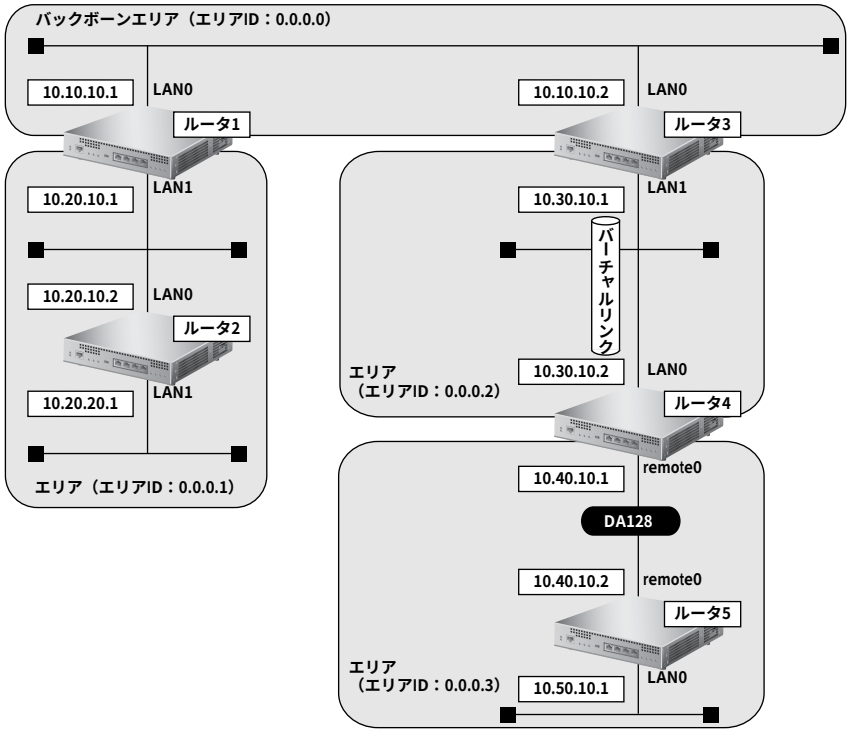
OSPF機能を使用する場合、定期的にパケットを送信します。このため、定額制でない回線を使用している場合は、超過課金の原因となることがあります。このような環境では、OSPF機能は使用しないでください。

2.3.1　バーチャルリンクを使う

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、ISDNポート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

再起動
# reset
```

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

再起動
# reset
```

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

再起動
# reset
```

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

再起動
# reset
```

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

再起動
# reset
```

2.3.2　スタブエリアを使う

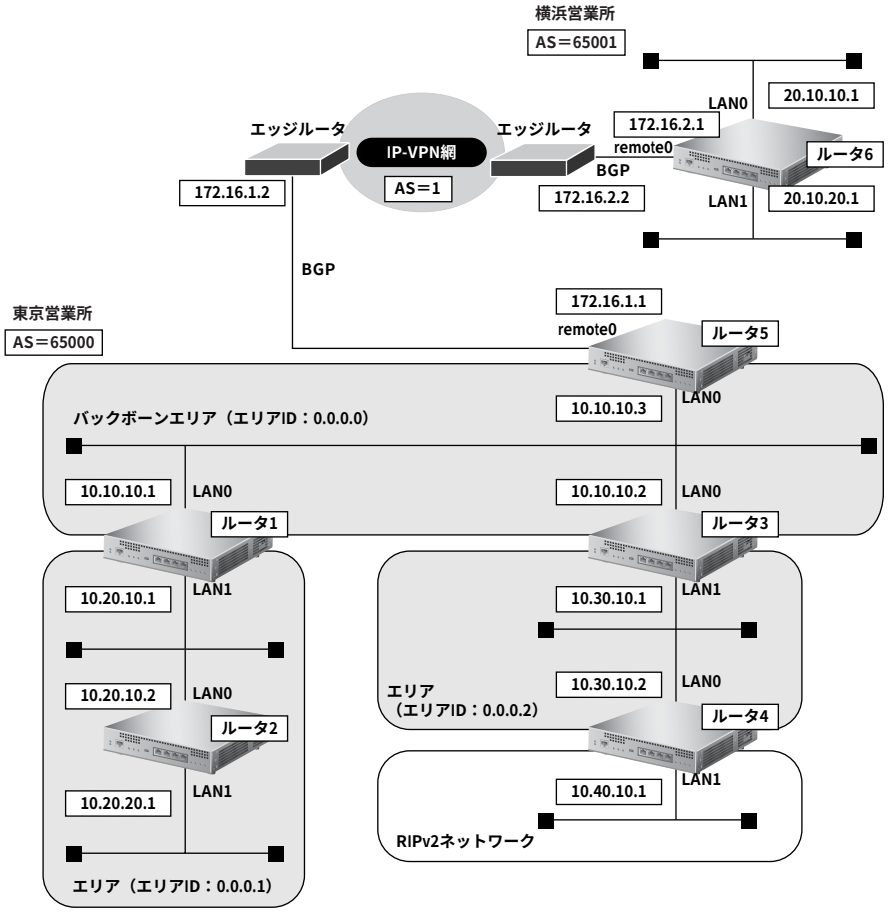
OSPF以外のルーティングプロトコルを使用したネットワークとの接続の設定について説明します。

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、ISDNポート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

再起動
# reset
```

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

再起動
# reset
```

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

再起動
# reset
```

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

再起動
# reset
```

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

再起動
# reset
```

ルータ6を設定する

● コマンド

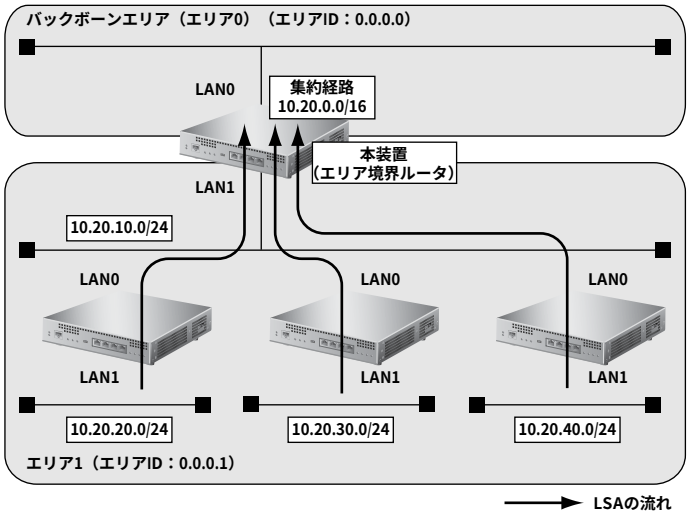
```
BGP情報を設定する
# bgp as 65001
# bgp neighbor 0 address 172.16.2.2
# bgp neighbor 0 as 1
# bgp network igp on
# bgp network route 0 20.10.10.0/24
# bgp network route 1 20.10.20.0/24

設定終了
# save

再起動
# reset
```

2.4 OSPFの経路を制御する（IPv4）

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

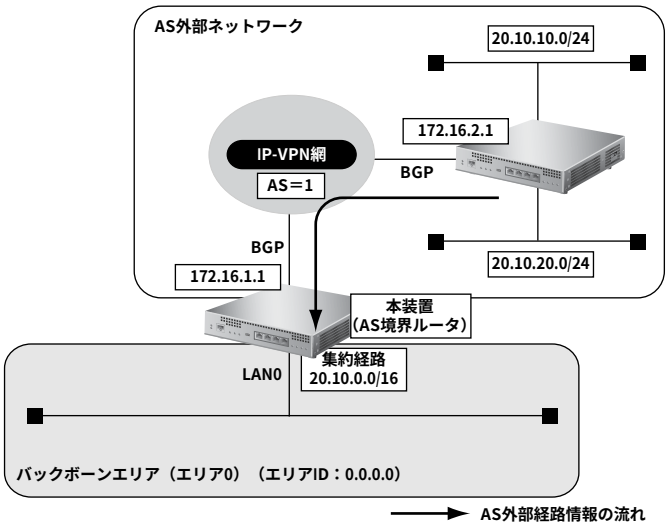
上記の経路情報に従って設定する場合のコマンド例を示します。

● 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
# enable
```

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

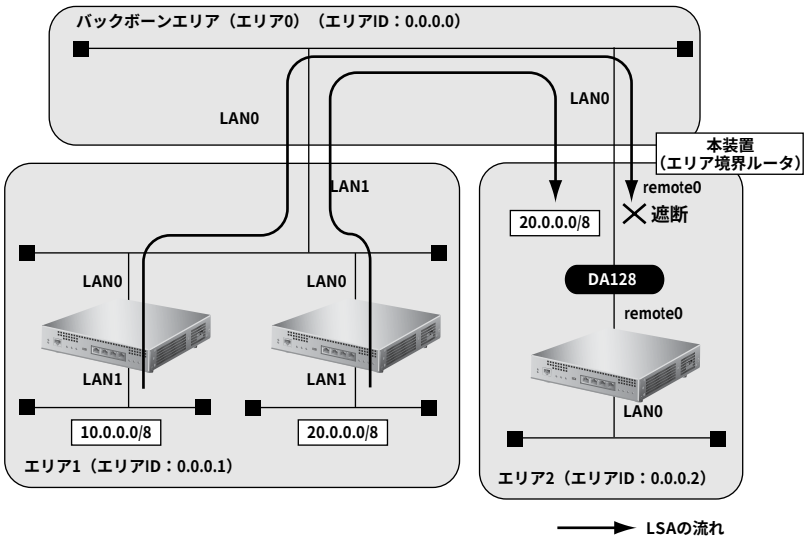
上記の経路情報に従って設定する場合のコマンド例を示します。

● 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
# enable
```

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
# enable
```

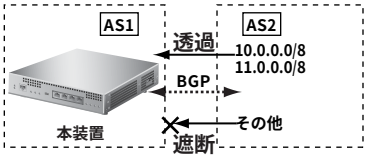
2.5　BGPの経路を制御する（IPv4）

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　MR1000　機能説明書「2.4 BGP4機能」（P.30）

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

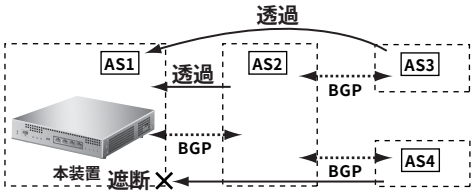
上記の経路情報に従って設定する場合のコマンド例を示します。

● 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
# enable
```

2.5.2　特定のASからの経路情報の受信を遮断する

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

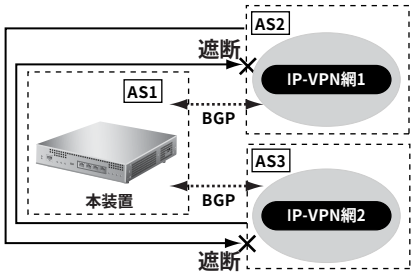
上記の経路情報に従って設定する場合のコマンド例を示します。

● 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
# enable
```

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

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

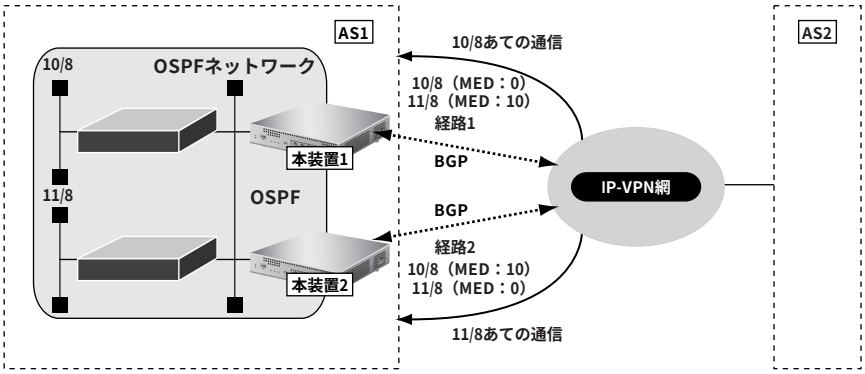
IP-VPN網1への送信を遮断する
```
# bgp neighbor 0 filter 0 act reject out
# bgp neighbor 0 filter 0 as 3
# bgp neighbor 0 filter 1 act pass out
# bgp neighbor 0 filter 1 route any
```

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
# enable
```

2.5.4　冗長構成の通信経路を使用する

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ネットワーク内での経路変更は 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
# enable
```

[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
# enable
```

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 enable 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

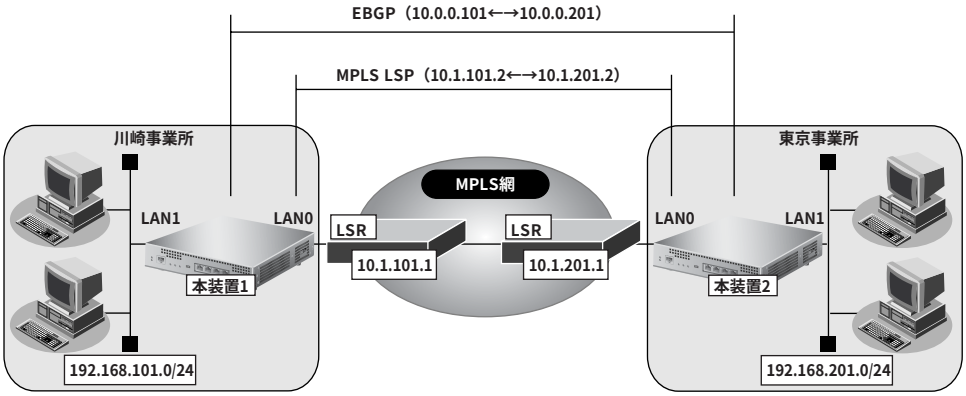
本装置ではMPLSのLSP（label Switching Path：トンネルラベルスイッチングパス）をトンネルとしてインタフェースに対応させるため、シェーピングや帯域制御などの機能をLSPごとに使用することができます（MPLS LSPトンネル）。

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、ダイナミック経路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、ダイナミック経路（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、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、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

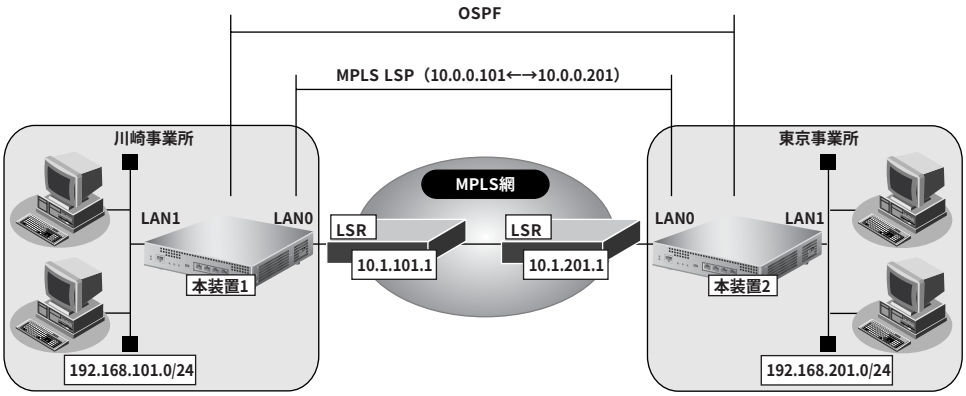
[本装置1]

```
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
# enable
```

[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
# enable
```

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、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、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　：10.0.0.101
- MPLSトンネルの相手側IPアドレス　：10.0.0.201

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 5m on

MPLSトンネルでセッション監視を行う
# remote 0 ap 0 sessionwatch 10.0.0.101 10.0.0.201 1s 1m 5s 1s 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
# enable
```

[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 5m on

MPLS トンネルでセッション監視を行う
remote 0 ap 0 sessionwatch 10.0.0.201 10.0.0.101 1s 1m 5s 1s 1

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
enable

2.7 MPLSを使用したレイヤ2VPN（EoMPLS）を構築する

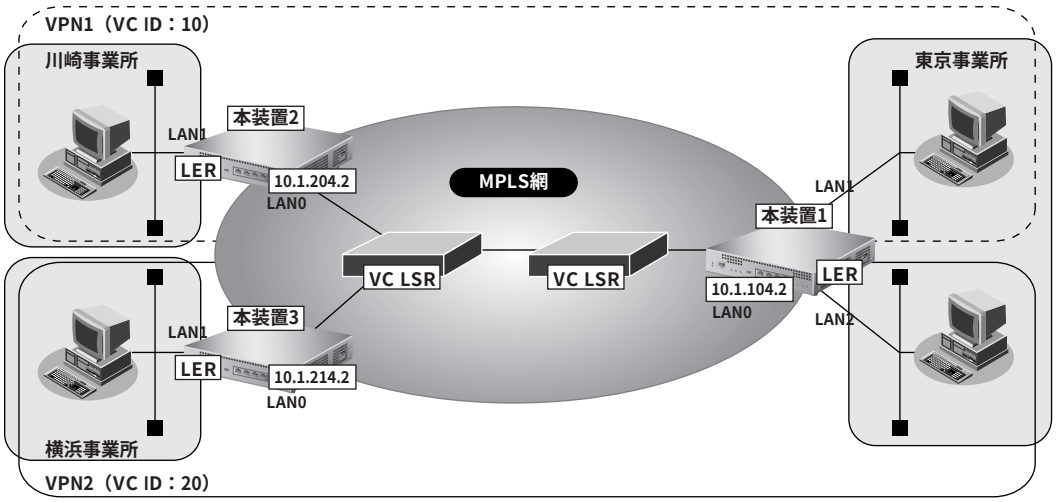
本装置では、MPLS網を経由することによって、公衆ネットワーク上に仮想的なプライベートネットワーク（閉域網）を構築することができ、遠隔地のネットワークを同じオフィス内のネットワークと同じように利用することができます。また、少ない設備で、業務単位で隔離したネットワークを実現することができます。

☛参照 MR1000　機能説明書「2.7.1 MPLSを使用したレイヤ2VPN（EoMPLS）」（P.39）

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
# enable
```

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
# enable
```

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
# enable
```

⚠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

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 MR1000　機能説明書「2.7.2 MPLSを使用したレイヤ3VPN（BGP/MPLS VPN）」（P.41）

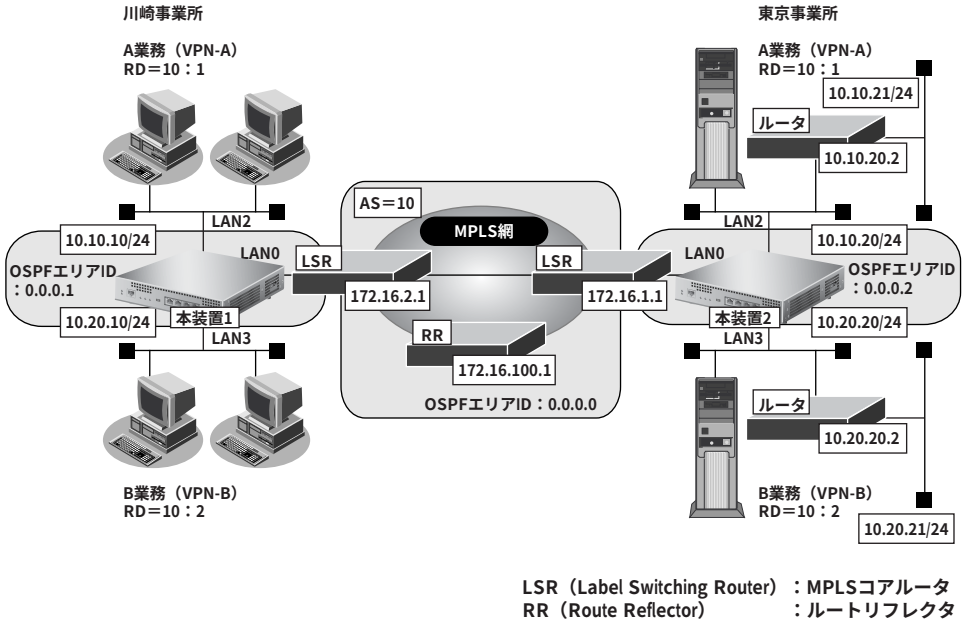
ここでは、MPLSを使用したVPNネットワークを構築する場合の設定方法を説明します。

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



● 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

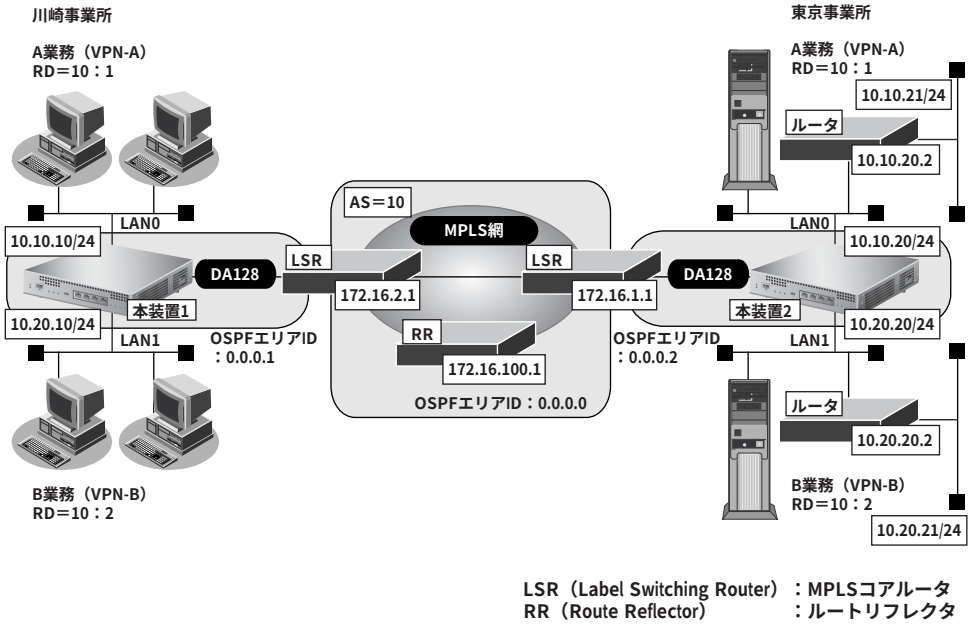
```
ループバックインタフェースを設定する
# loopback ip address 0 10.1.1.1

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
# enable
```

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
# enable
```

2.8.2　MPLS網と専用線を使用して接続する



● 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
# enable
```

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
# enable
```

こんな事に気をつけて

サポートインタフェースは BRI（ISDN、HSD）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

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2本束ねることによって、最大128Kbpsで通信できます。また、BAP/BACP機能を利用すると動的にチャネル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　MR1000　機能説明書「2.8 マルチリンク機能」（P.44）

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
- チャネルの使用率90％以上が60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10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

```
マルチリンク機能の利用を設定する
# remote 0 ap 0 ppp mp 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

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 60s
# remote 0 ppp mp traffic decrease 40 10s

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

設定終了
# save
# enable
```

2.10　マルチキャスト機能を使う

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

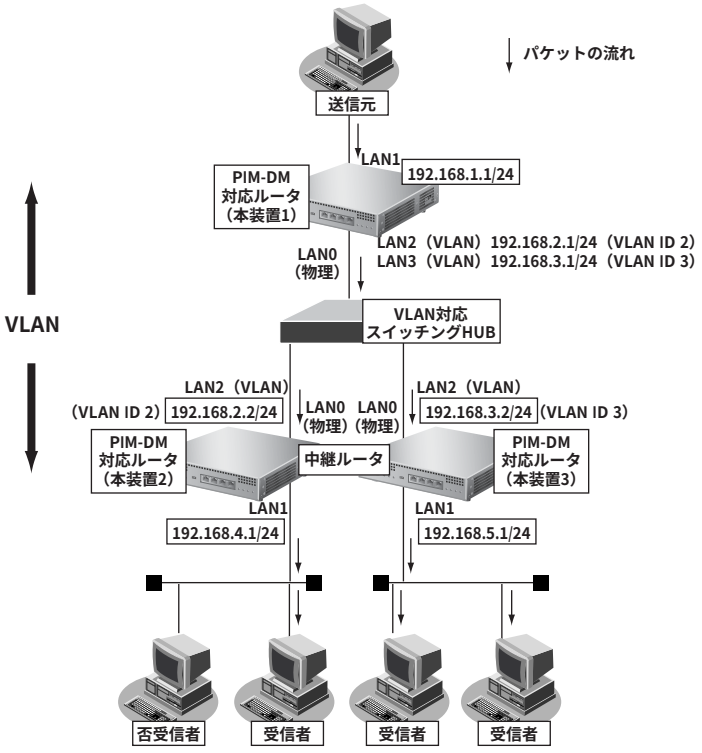
☛参照　MR1000　機能説明書「2.9 マルチキャスト機能」（P.45）

2.10.1　マルチキャスト機能（PIM-DM）を使う

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経路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
- ユニキャストの経路テーブルの作成に 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
- ユニキャストの経路テーブルの作成に 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
- ユニキャストの経路テーブルの作成に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
# enable
```

[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
# enable
```

[本装置3]

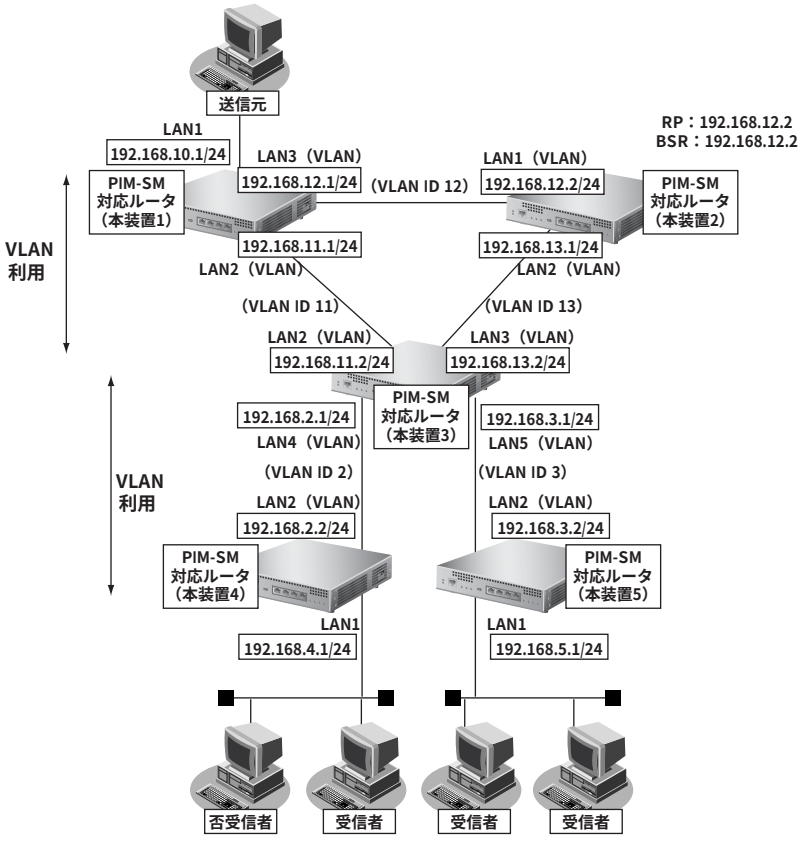
```
LAN0 ポートを削除する
# delete lan 0

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
# enable
```

2.10.2　マルチキャスト機能（PIM-SM）を使う

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経路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
  ユニキャストの経路テーブルの作成に 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
# enable
```

[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
# enable
```

[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
# enable
```

[本装置4]

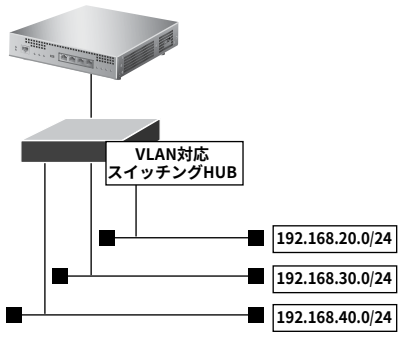
```
LAN0 ポートを削除する
# delete lan 0

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
# enable
```

[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
# enable
```

2.11　VLAN機能を使う

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 MR1000　機能説明書「2.10 VLAN機能」（P.48）

● 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
```

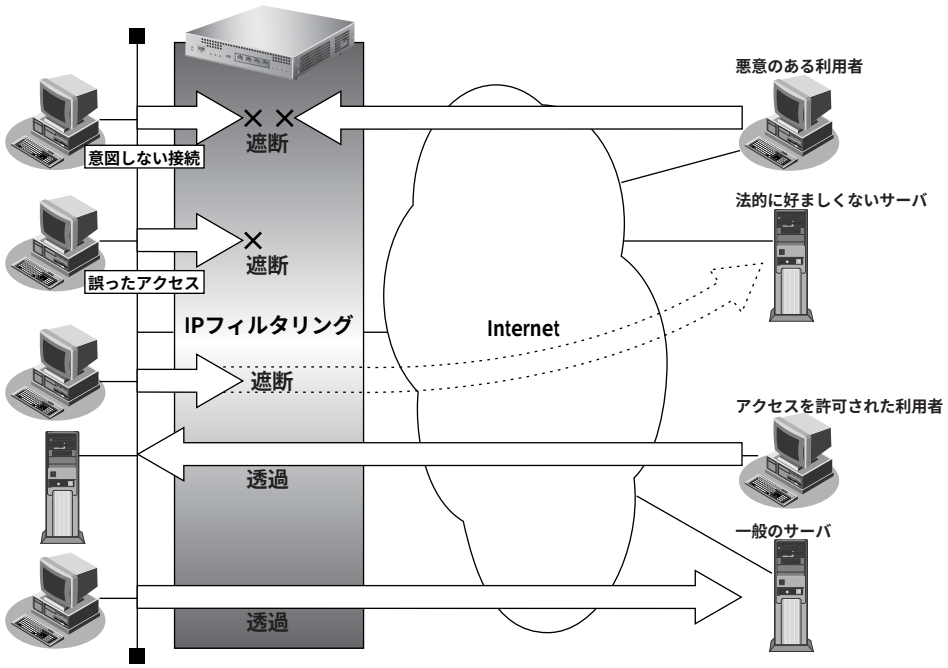
こんな事に気をつけて

- 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、帯域制御（WFQ）、ホットスタンバイ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、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 enable 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

参照　MR1000　機能説明書「2.11 IP フィルタリング機能」（P.49）

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。

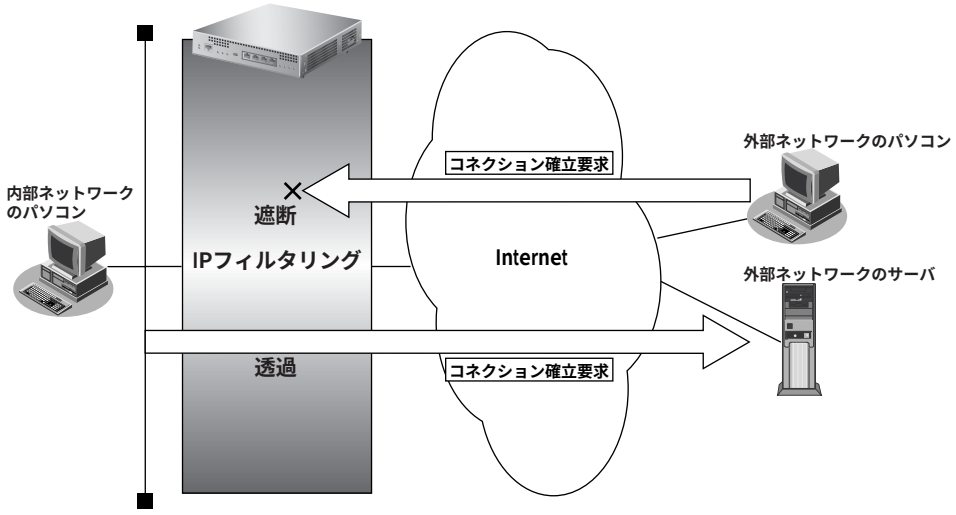
制御フラグ		TCP パケットの内容
SYN	ACK	
1	0	コネクションの確立要求
1	1	確立後の承認応答
0	1	確認応答、通常のデータ

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

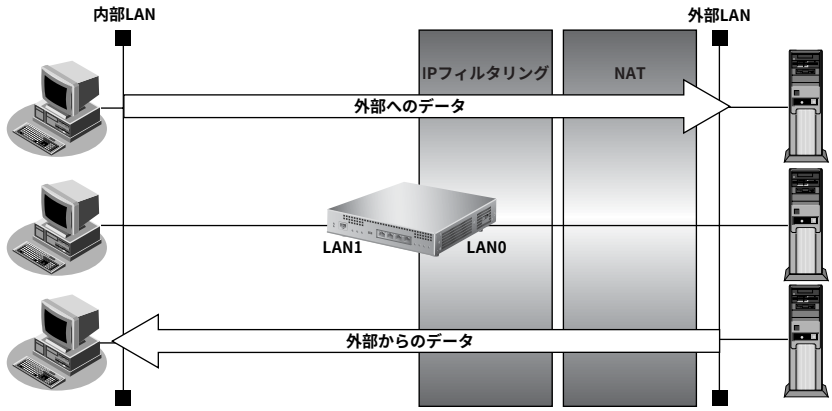
補足 IPフィルタリング機能とNAT機能を併用する場合、回線切断時にNAT機能の情報が消えてしまうため、回線切断後に再度接続しても、サーバからの応答が正しくアドレス変換されず、IPフィルタリング機能によってパケットは破棄されてしまいます。

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

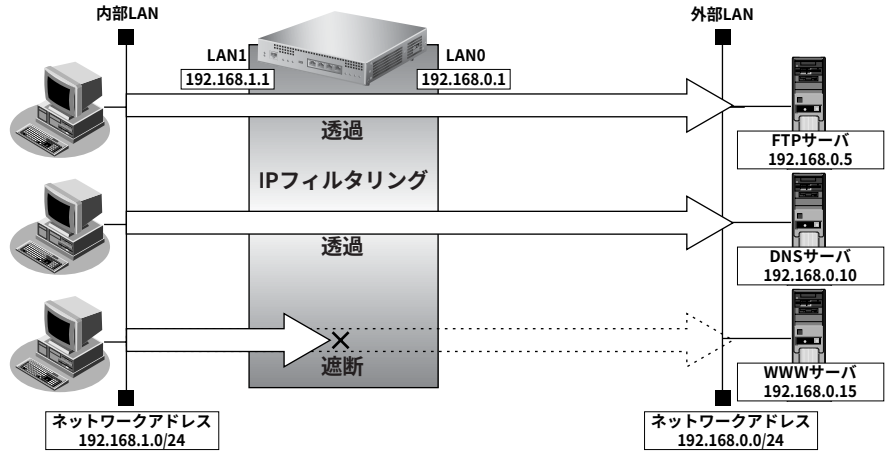
- **IP フィルタリングで WWW（ポート番号 80）でのアクセスを制限する設定を行った場合、外部の WWW ブラウザから設定ができなくなる場合があります。**
- **IP フィルタリングで DHCP（ポート番号 67、68）でのアクセスを制限する設定を行った場合、DHCP 機能が使用できなくなる場合があります。**
- **IP フィルタリング条件が複数存在する場合、それぞれの条件に優先順位がつき、数値の小さいものから優先的に採用されます。設定内容によっては通信できなくなる場合がありますので、優先順位を意識して設定してください。PPPoE の場合は、remote 側にフィルタをかけるようにしてください。**
- **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

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。

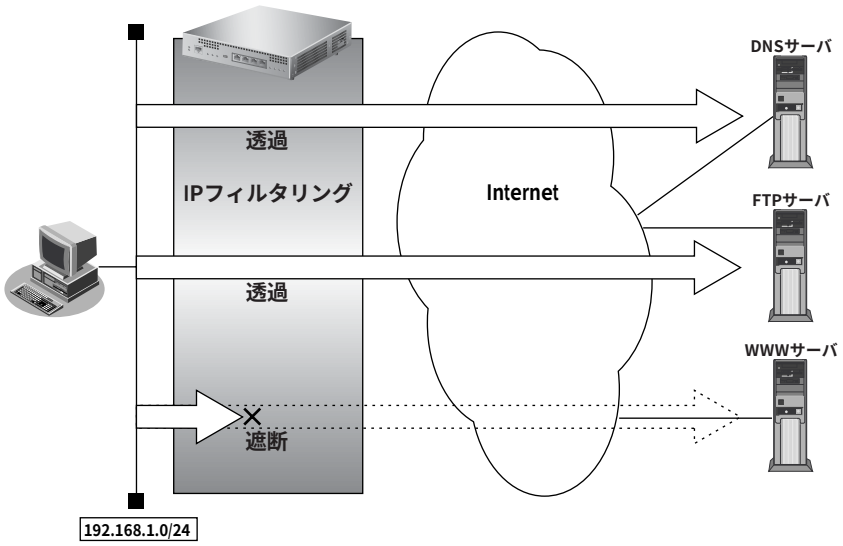
● コマンド

```
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
# lan 0 ip filter 0 pass 192.168.1.0/24 any any 21 6 yes any any

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

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

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

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

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

設定終了
# save
# enable
```

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

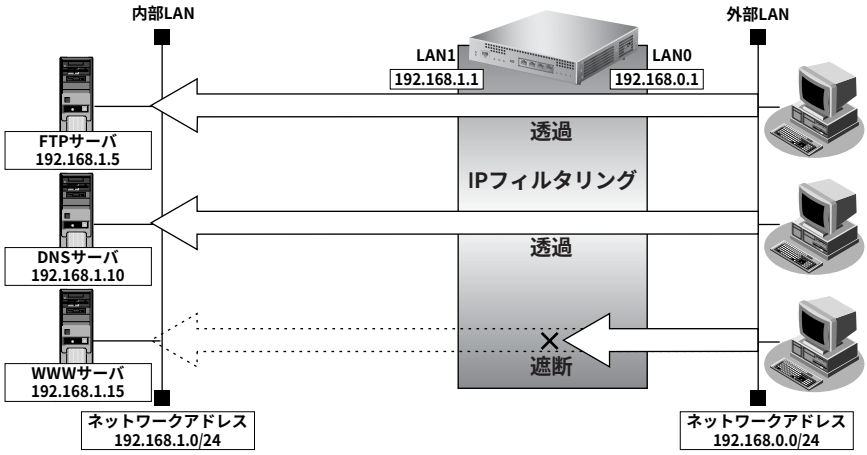
```
任意のFTPサーバのポート21へのTCPパケットを透過させる
# remote 0 ip filter 0 pass 192.168.1.0/24 any any 21 6 yes any any

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

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

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

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

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

設定終了
# save
# enable
```

2.12.2　外部から特定サーバへのアクセスだけ許可する

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

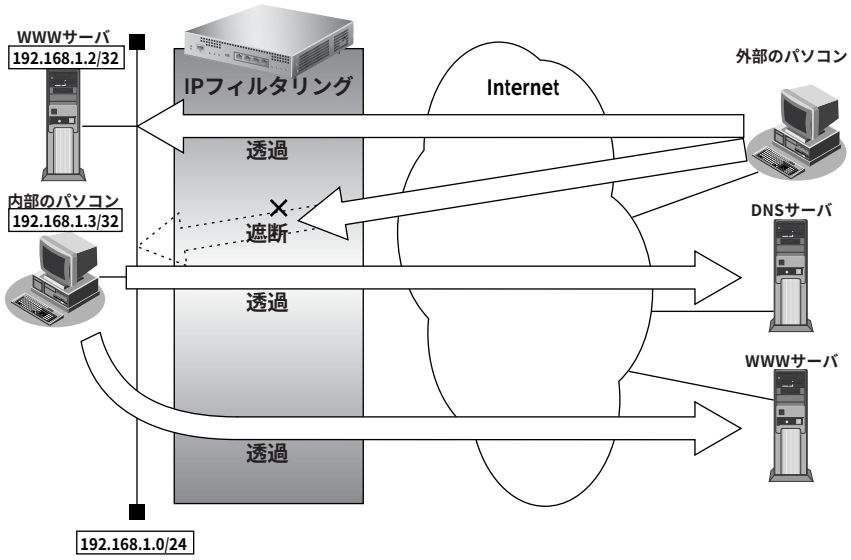
上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

● 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
# lan 0 ip filter 0 pass 192.168.0.0/24 any 192.168.1.5/32 21 6 yes any any

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

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

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

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

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

設定終了
# save
# enable
```

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

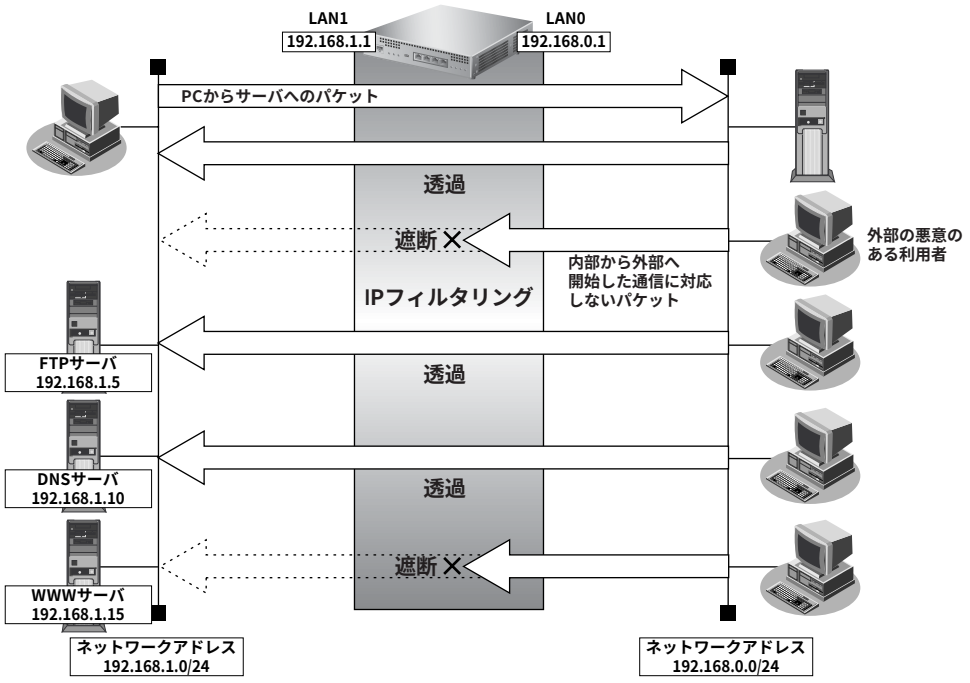
```
LAN上のホストのポート80へのパケットを透過させる
# remote 0 ip filter 0 pass any any 192.168.1.2/32 80 6 yes any any

LAN上のホストからの応答パケットを透過させる
# remote 0 ip filter 1 pass 192.168.1.2/32 80 any any 6 yes any 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
# remote 0 ip filter 2 pass 192.168.1.3/32 any any 80 6 yes any any

任意のWWWサーバからの応答パケットを透過させる
# remote 0 ip filter 3 pass any 80 192.168.1.3/32 any 6 yes any any

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

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

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

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

設定終了
# save
# enable
```

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

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

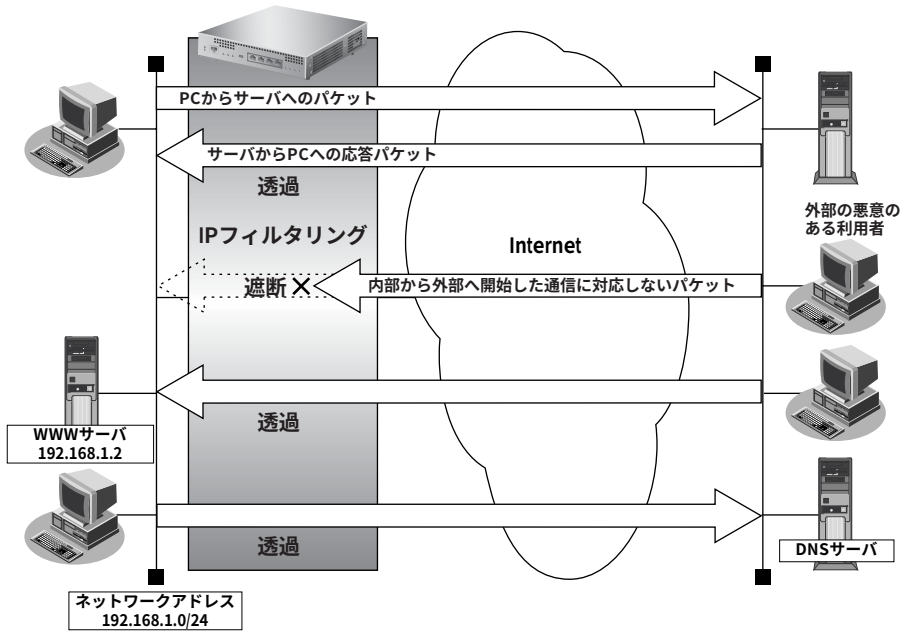
上記のフィルタリングルールに従って設定する場合のコマンド例を示します。

● 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
# lan 0 ip filter 0 pass 192.168.0.0/24 any 192.168.1.5/32 21 6 yes any any

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

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

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

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

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
# enable
```

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

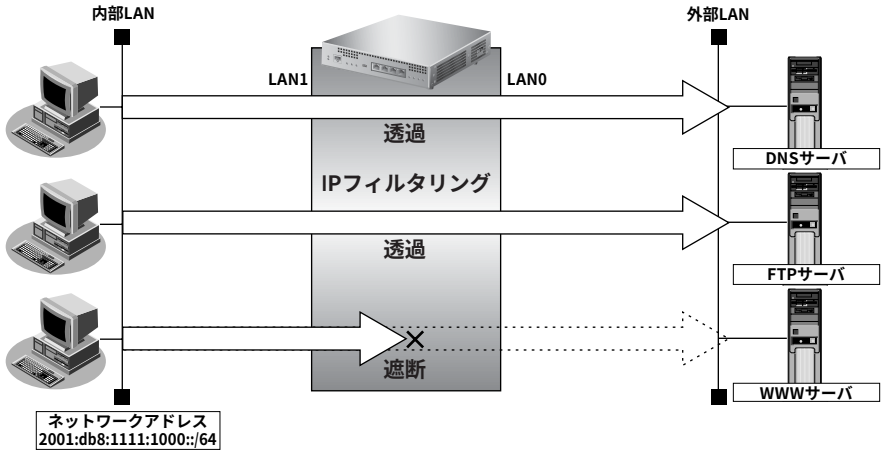
```
LAN上のホストのポート80へのパケットを透過させる
# remote 0 ip filter 0 pass any any 192.168.1.2/32 80 6 yes any any

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

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

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
# enable
```

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）

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。

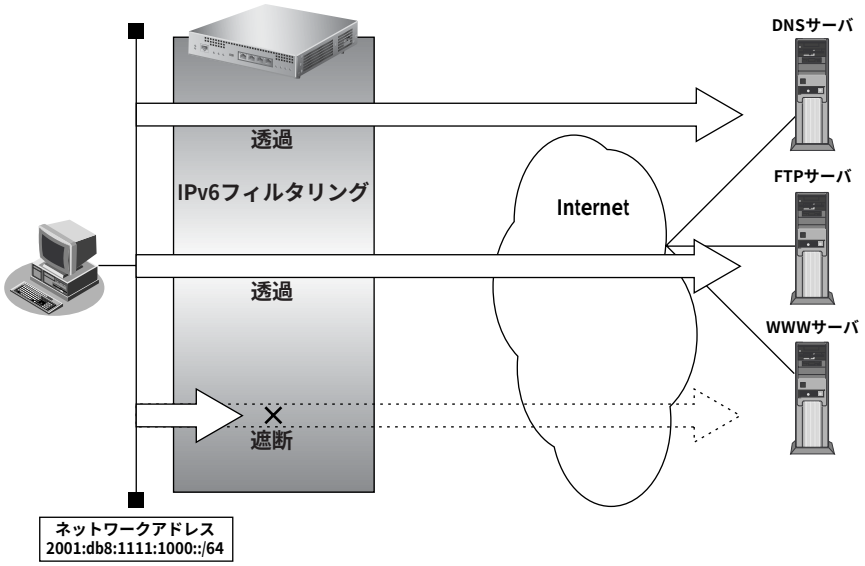
● コマンド

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

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

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

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

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

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

設定終了
# save
# enable
```

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。

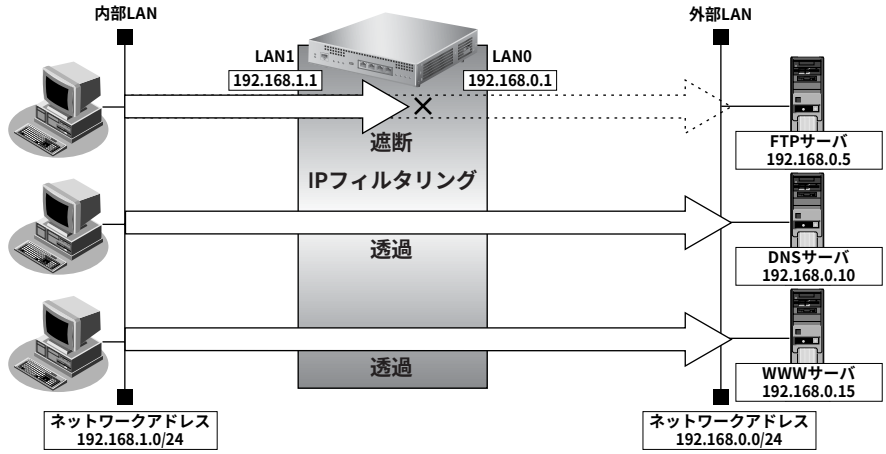
● コマンド

```
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
# remote 0 ip6 filter 0 pass 2001:db8:1111:1000::/64 any any 21 6 yes any any any any

FTPサーバからの応答パケットを透過させる
# remote 0 ip6 filter 1 pass any 21 2001:db8:1111:1000::/64 any 6 yes any any any any

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

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

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

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

設定終了
# save
# enable
```

2.12.5　外部の特定サーバへのアクセスだけを禁止する

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

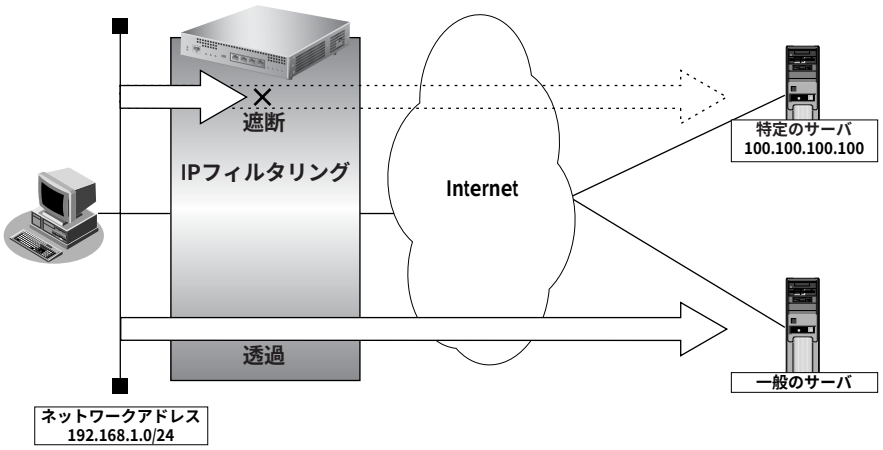
上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

● コマンド

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

設定終了
# save
# enable
```

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

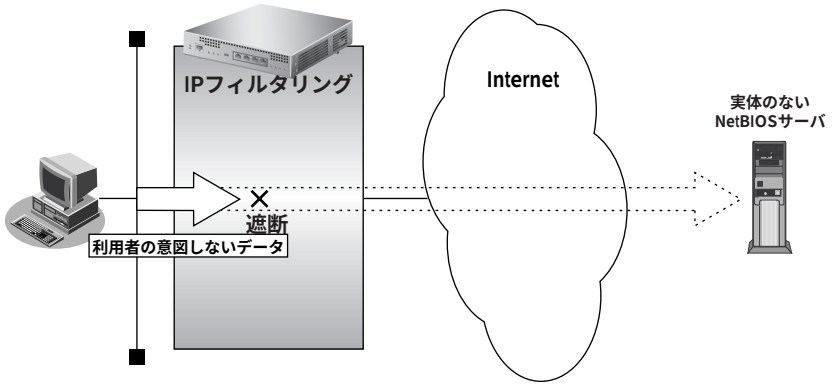
アドレス100.100.100.100へのすべてのパケットを遮断する
remote 0 ip filter 0 reject 192.168.1.0/24 any 100.100.100.100/32 any 0 yes any any

設定終了
save
enable

2.12.6　利用者が意図しない発信を防ぐ

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。

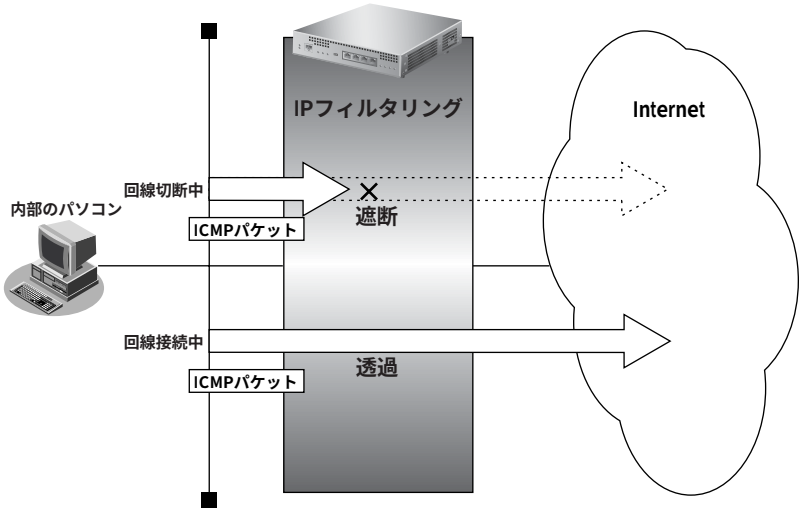
● コマンド

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

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

設定終了
# save
# enable
```

2.12.7　回線が接続しているときだけ許可する

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。

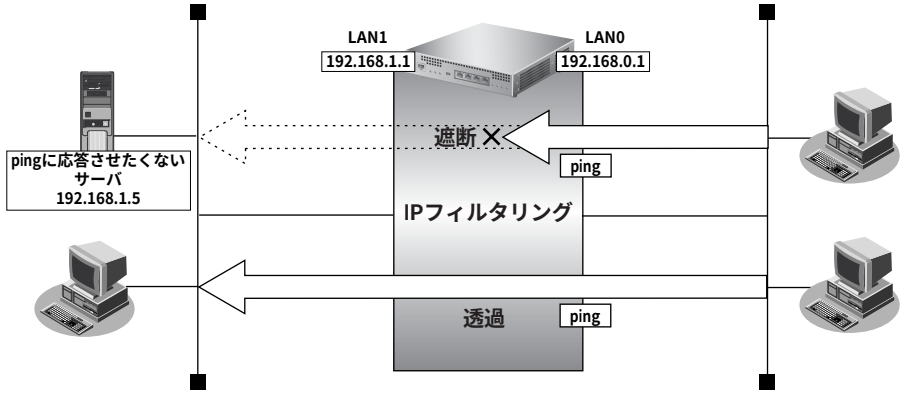
● コマンド

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

設定終了
# save
# enable
```

2.12.8　外部から特定サーバへのpingだけを禁止する

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

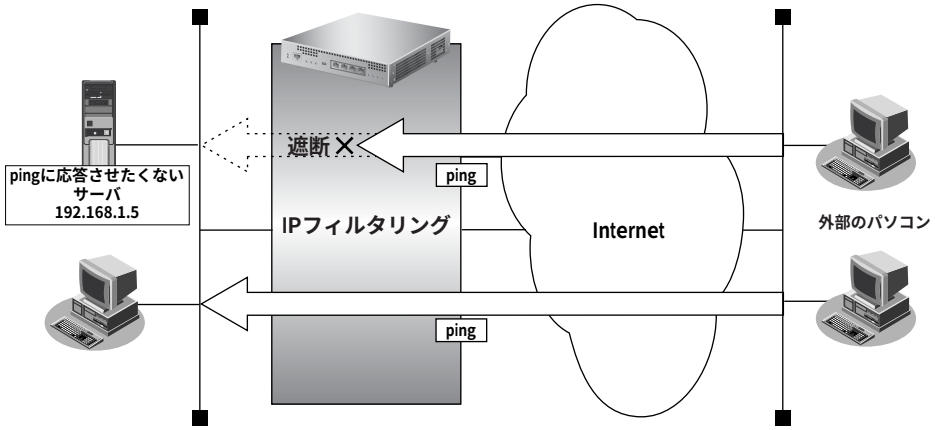
アドレス192.168.1.5/32へのICMP TYPE 8のICMPパケットを遮断する
lan 0 ip filter 0 reject any any 192.168.1.5/32 any 1 yes any any 8 any

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

設定終了
save
enable

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
remote 0 ip filter 0 reject any any 192.168.1.5/32 any 1 yes any any 8 any

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

設定終了
save
enable

2.13　IPsec機能を使う

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。

☛参照　MR1000　機能説明書「2.13 IPsec機能」（P.58）

こんな事に気をつけて

- **IPsec機能は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機能では、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機能と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機能とマルチ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。**
- **AES暗号アルゴリズムは、128ビット鍵長だけをサポートしています。他機種と接続する際には、128ビット鍵長を選択してください。**

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
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、と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IPアドレスおよびグローバルIPアドレスには、202.16.1.66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　何も設定しない ポート番号　500 ・プロトコル　UDP

利用形態	設定内容
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　何も設定しない 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）

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

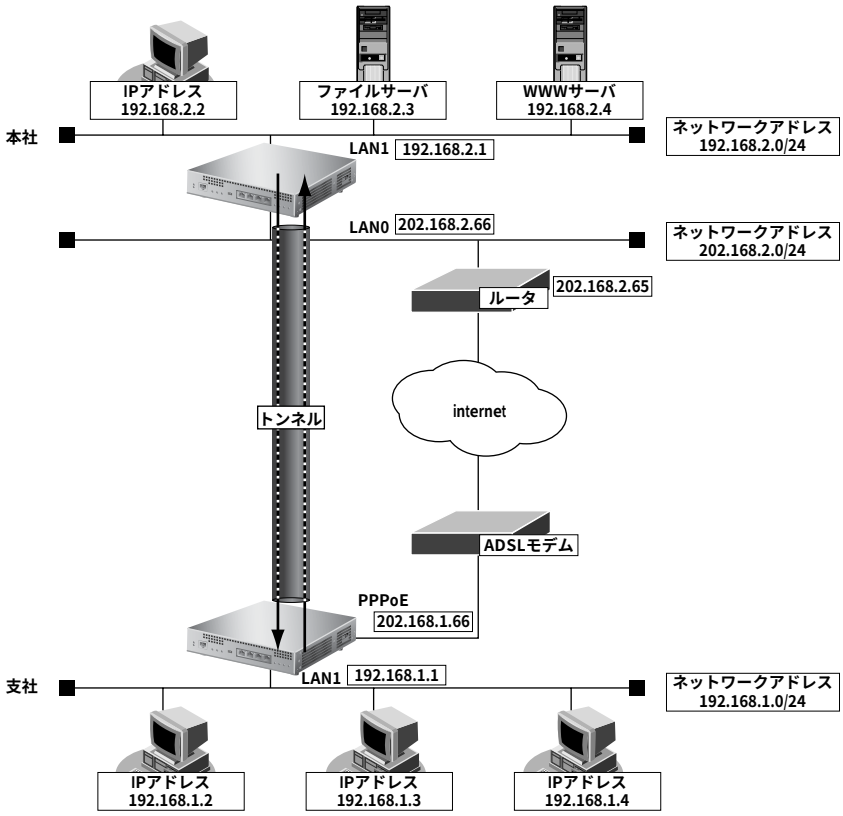
● 設定コマンド

[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
# enable
```

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
# enable
```

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

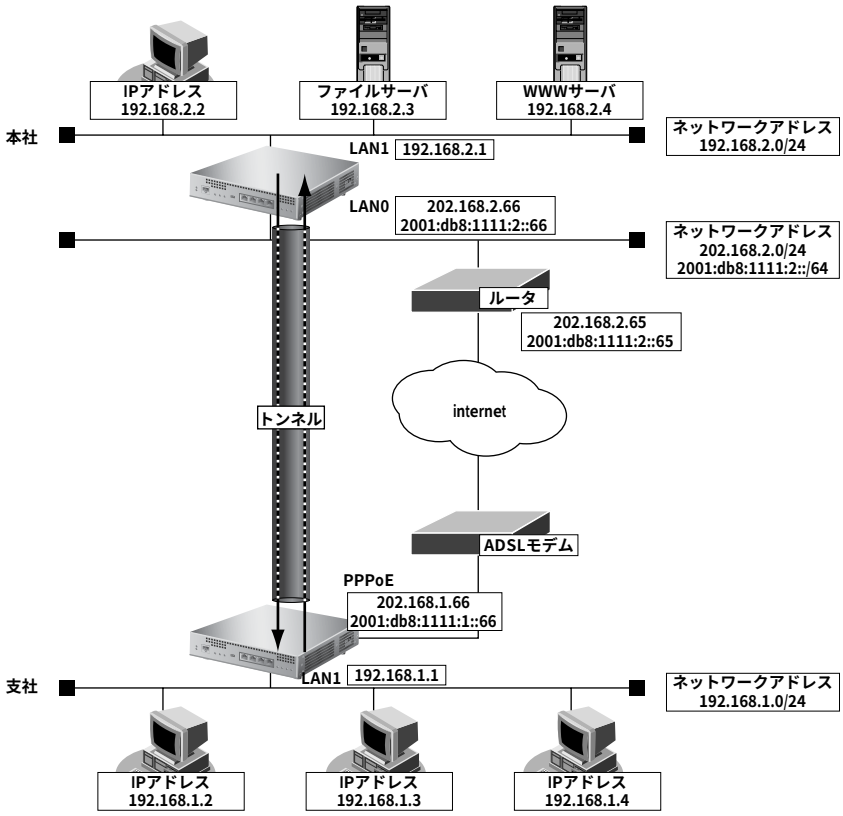
● 設定コマンド

[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
# enable
```

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
# enable
```

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

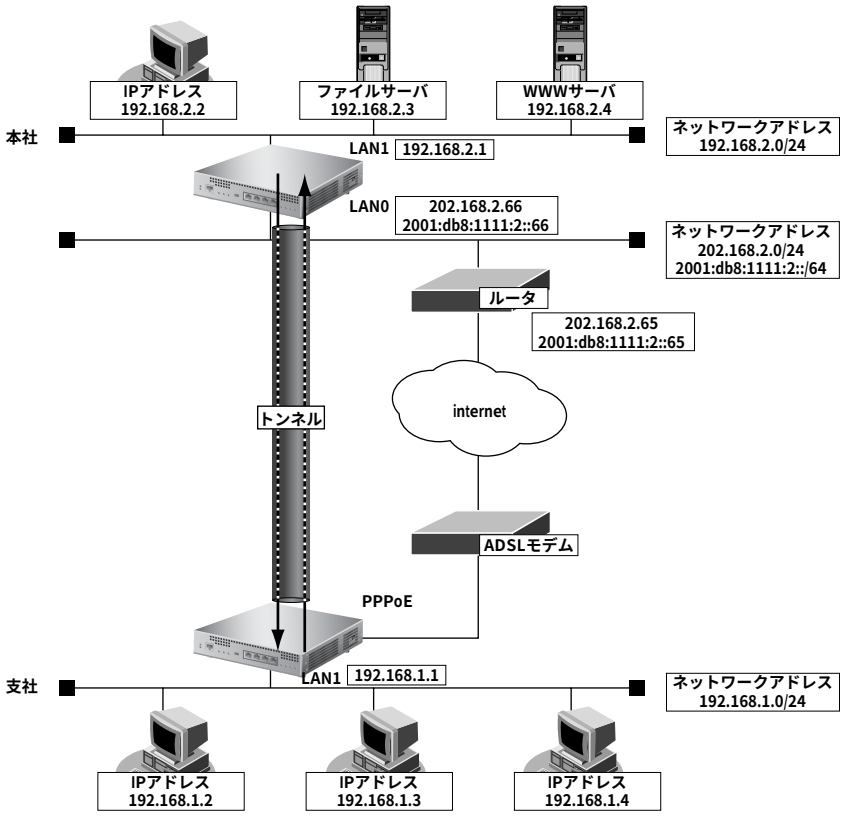
● 設定コマンド

[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
# enable
```

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
# enable
```

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

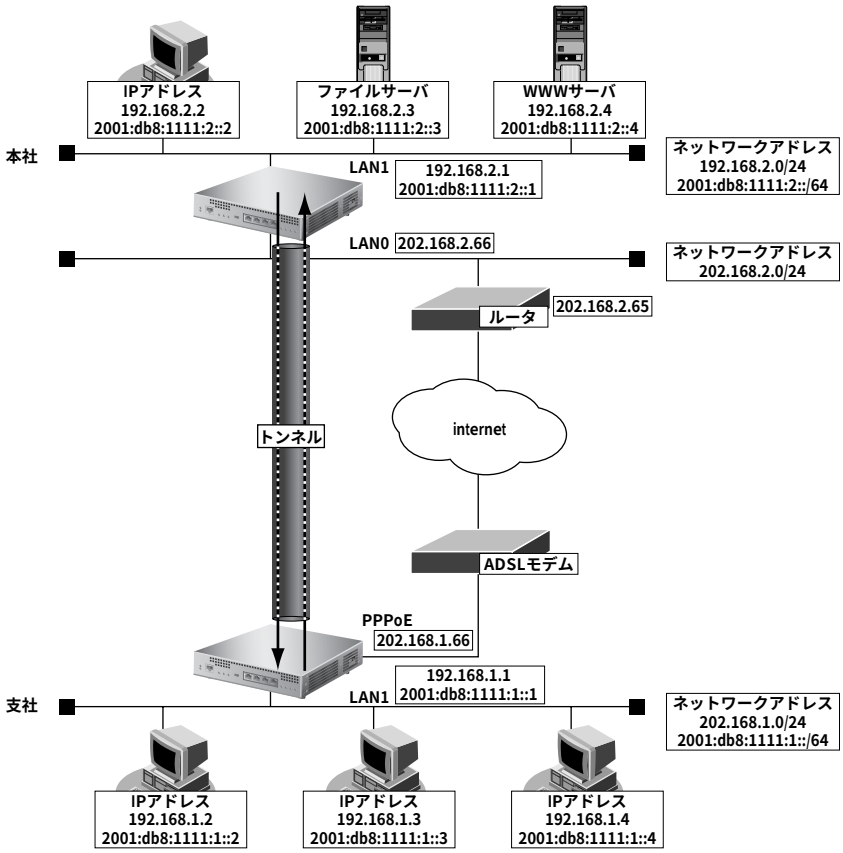
● 設定コマンド

[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 ip route 0 192.168.2.0/24 1 0
# 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
# enable
```

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:db8:1111:1::/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
# enable
```

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

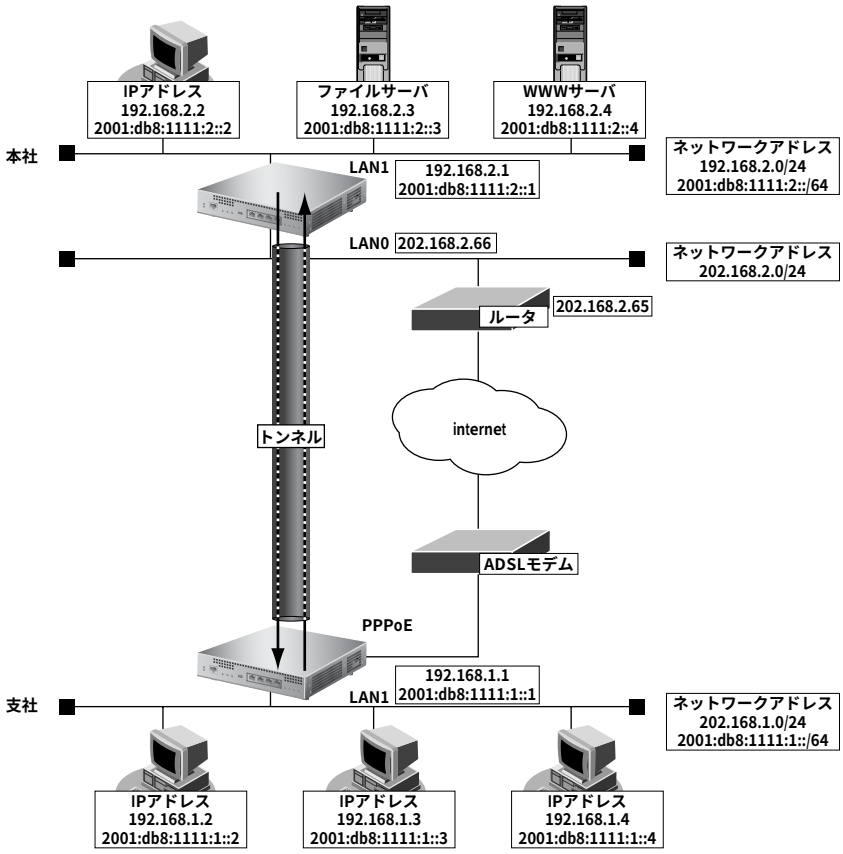
● 設定コマンド

[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 ip route 0 192.168.2.0/24 1 0
# 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
# enable
```

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:db8:1111:1::/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
# enable
```

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

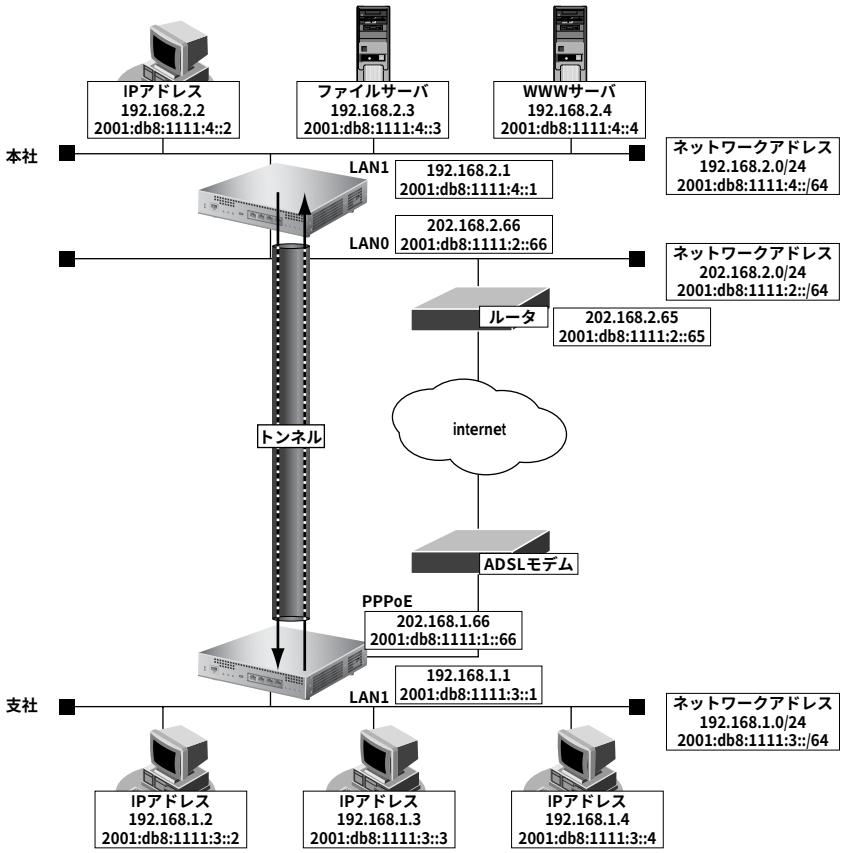
● 設定コマンド

[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
# enable
```

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::0/64 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
# enable
```

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

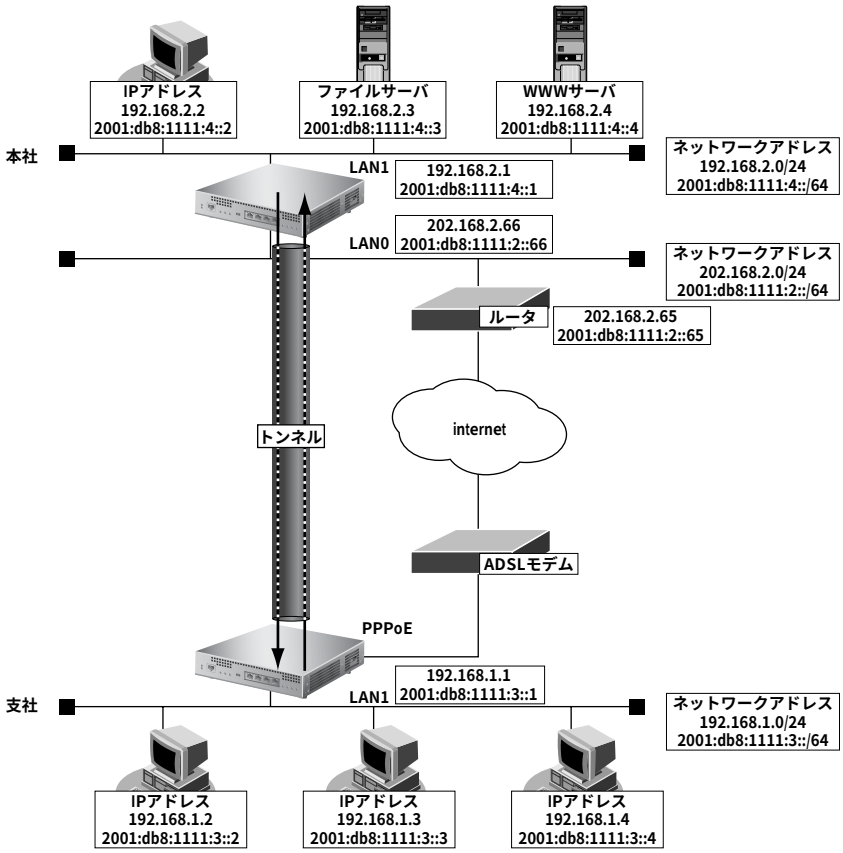
● 設定コマンド

[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
# enable
```

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
# enable
```

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）

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、支店は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

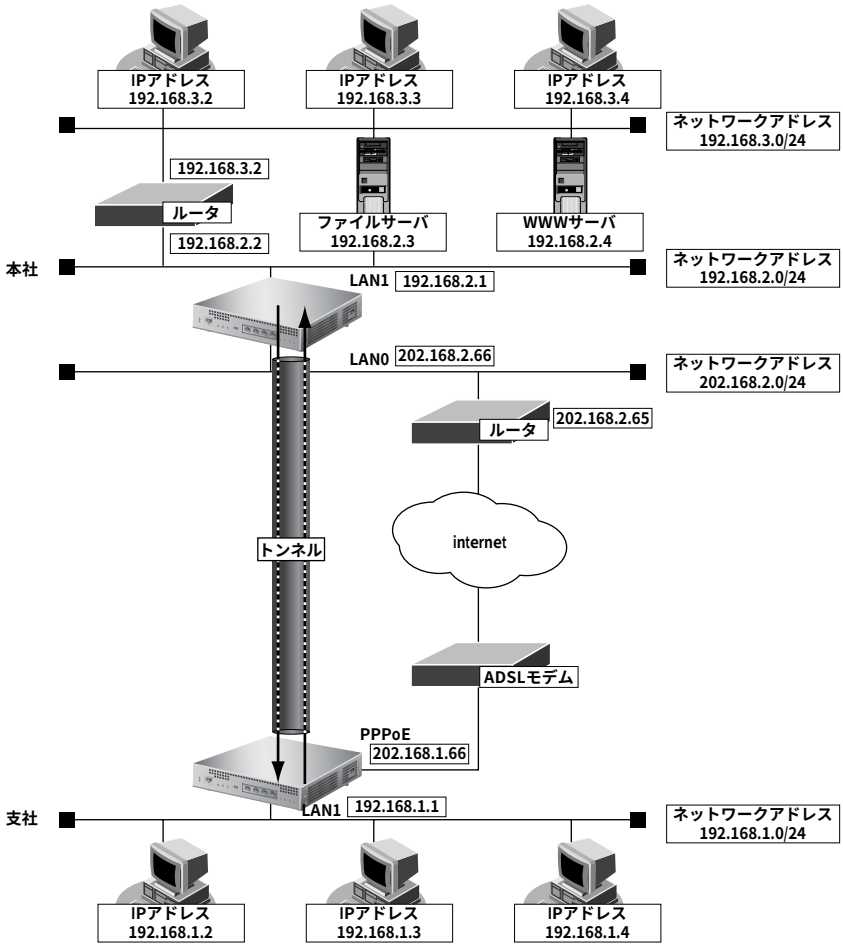
● 設定コマンド

[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
# enable
```

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
enable

2.13.9　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、以下に説明します。

ここでは、「IPv4 over IPv4で固定IPアドレスでのVPN（自動鍵交換）」または「IPv4 over IPv4で可変IPアドレスでのVPN（自動鍵交換）」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
# remote 1 ip filter 0 pass 192.168.1.0/24 any 192.168.2.0/24 21,23 6 yes any any
# remote 1 ip filter 1 pass 192.168.2.0/24 21,23 192.168.1.0/24 any 6 no any any
# remote 1 ip filter 2 reject any any any any 0 yes any any
# remote 1 ip tos 0 any any 192.168.2.0/24 20,21 6 any a0
```

本社を設定する

● コマンド

```
# remote 0 ip filter 0 pass 192.168.1.0/24 any 192.168.2.0/24 21,23 6 yes any any
# remote 0 ip filter 1 pass 192.168.2.0/24 21,23 192.168.1.0/24 any 6 no any any
# remote 0 ip filter 2 reject any any any any 0 yes any any
# remote 0 ip tos 0 192.168.2.0/24 20,21 192.168.1.0/24 20,21 6 any 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
# remote 0 ip priority 0 192.168.2.0/24 any 192.168.1.0/24 any 6 any 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 192.168.1.1 192.168.2.1 10s 1m 5s
```

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

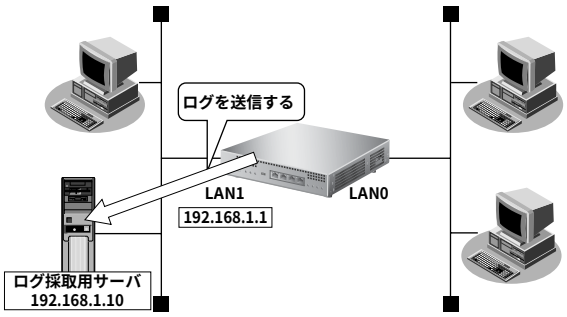
```
# delete remote 1 ip route
# remote 0 ip rip use v1 v1 0 off
```

2.14　システムログを採取する

本装置では、各種システムログ（回線の接続／切断など）をネットワーク上のシステムログサーバに送信することができます。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）

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
- 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

設定終了
# save
# enable
```

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。

☛参照 MR1000　コマンドユーザーズガイド「2.1.12 システムログを確認する」（P.41）

2.15　マルチNAT機能（アドレス変換機能）を使う

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　MR1000　機能説明書「2.14 マルチNAT機能」（P.63）

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IP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IPアドレスを使用しないでください
動的NAT	最大1024セッションまで	外部からの通信はできない
静的NAT	最大64個まで割り当て可能	プライベートIPアドレスとポートをグローバルIP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

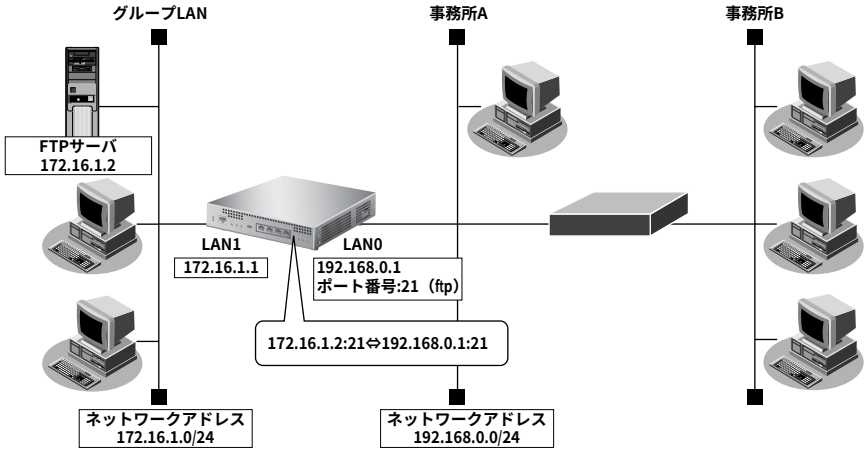
こんな事に気をつけて

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　MR1000　コマンドユーザーズガイド「1.4 コマンドで入力できる文字一覧」（P.18）

2.15.1　プライベートLAN接続でサーバを公開する

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
# enable
```

こんな事に気をつけて

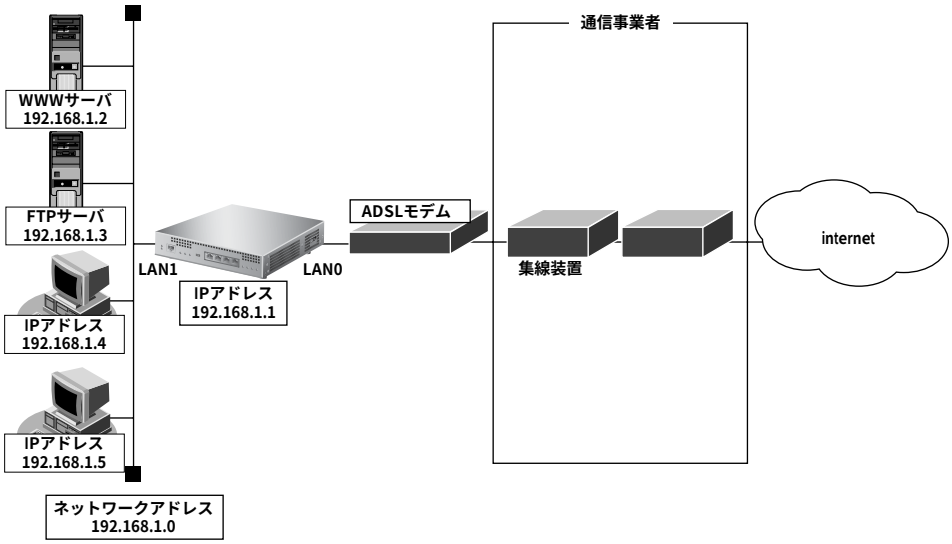
NATでは、FTPやDNSが要求した相手からの応答かどうかをチェックします。相手サーバがNAT機能を使用している場合など、要求先とは別のアドレスから応答する場合は、以下の設定を追加してください。

```
# 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

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
# enable
```

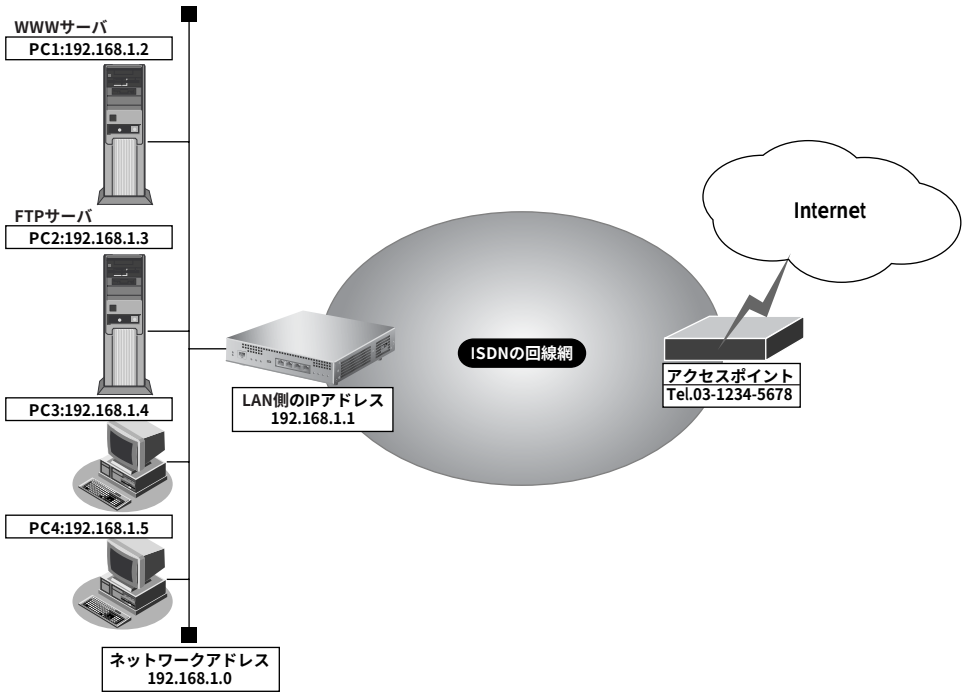
こんな事に気をつけて

- 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

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

- ISDNポートで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 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
```

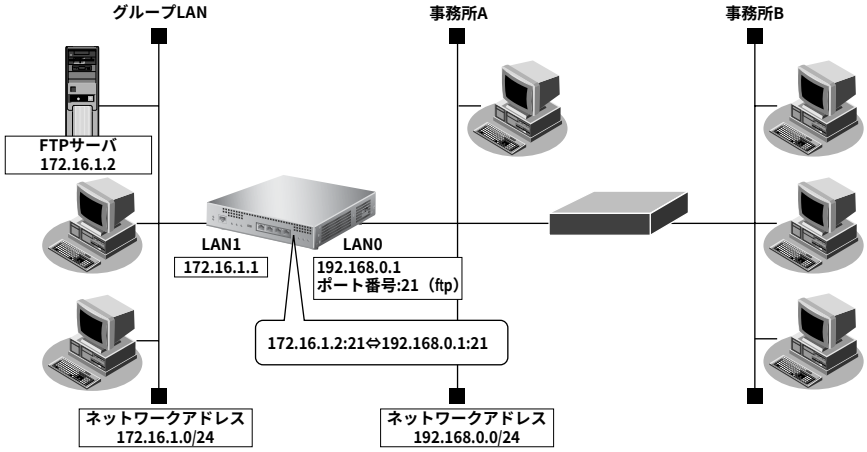
こんな事に気をつけて

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
```

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

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
# enable
```

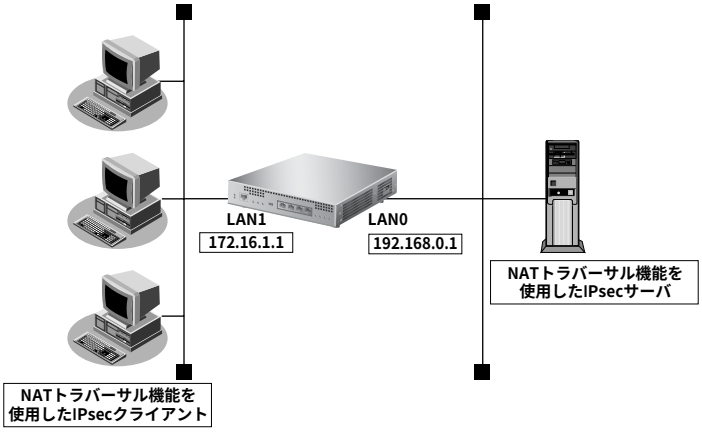
こんな事に気をつけて

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

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
# enable
```

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。

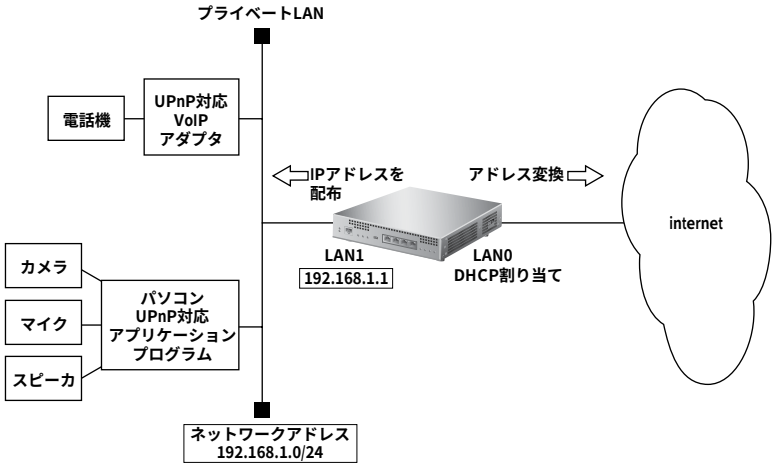
```
# lan 0 ip nat rule 0 ftp any 21 off
# lan 0 ip nat rule 1 dns global 53 off
```

2.16　VoIP NAT トラバーサル機能を使う

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　MR1000　機能説明書「2.15 VoIP NAT トラバーサル機能」（P.66）

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 MR1000　コマンドユーザーズガイド「1.4 コマンドで入力できる文字一覧」（P.18）

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
# enable
```

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

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　MR1000　機能説明書「2.16 TOS/Traffic Class 値書き換え機能」（P.69）

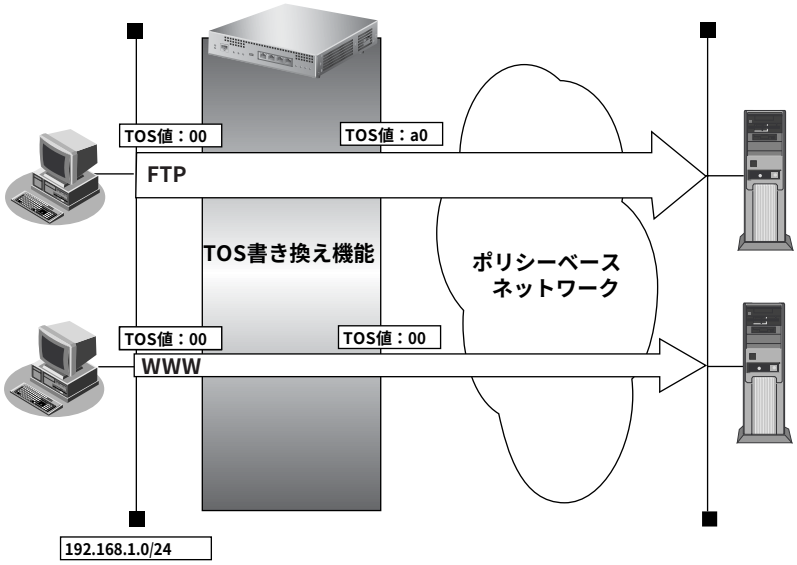
TOS/Traffic Class値書き換え機能の条件

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
# remote 0 ip tos 0 192.168.1.0/24 any any 20,21 6 0 a0

設定終了
# save
# enable
```

2.18　VLANプライオリティマッピング機能を使う

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。

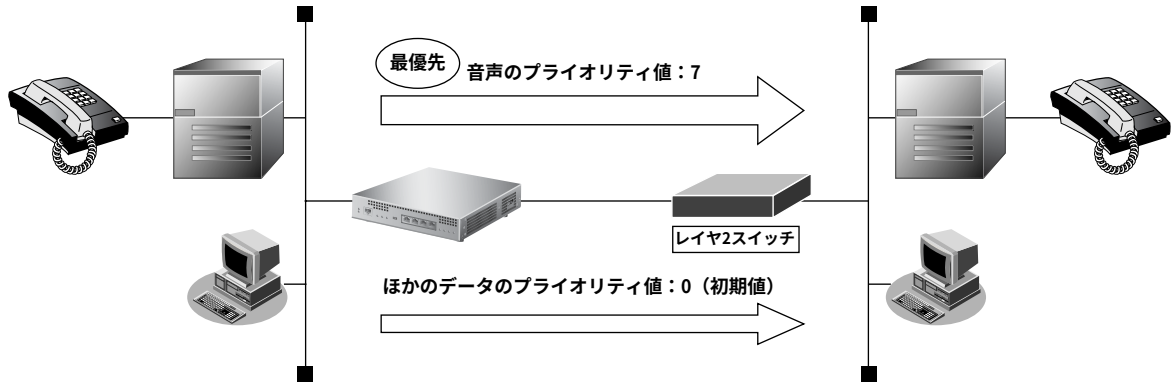
☛参照　MR1000　機能説明書「2.17 VLANプライオリティマッピング機能」（P.71）

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　：IP
- 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

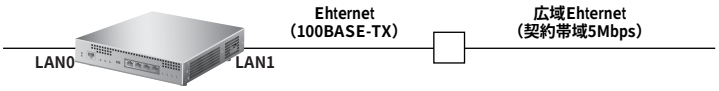
```
TOS値a0のパケットのプライオリティ値を7に設定する
# lan 0 vlan tag primap 0 ip a0 7

設定終了
# save
# enable
```

2.19　シェーピング機能を使う

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

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

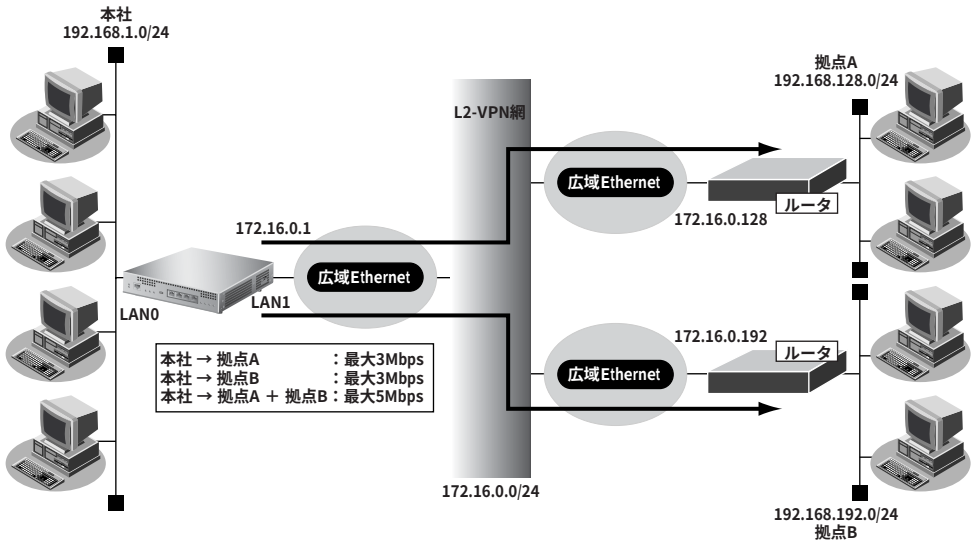
上記の設定条件に従って設定を行う場合のコマンド例を示します。

● 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
# enable
```

2.19.2　送信先ごとにシェーピング機能を使う

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
# enable
```

2.20　データ圧縮／ヘッダ圧縮機能を使う

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、およびモデム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
  - 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
# enable
```

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
# enable
```

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

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。

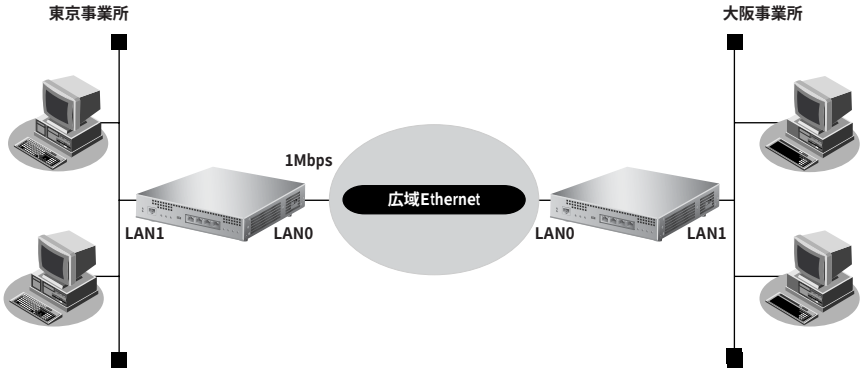
参照　MR1000　機能説明書「2.19 帯域制御（WFQ）機能」（P.73）

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
# lan 0 ip priority 0 any any any any any a0 express

設定終了
# save
# enable
```

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
# lan 0 ip priority 0 any any any any any a0 express

設定終了
# save
# enable
```

2.22　DHCP機能を使う

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　MR1000　機能説明書「2.20.1 IPv4 DHCP機能」（P.76）

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　MR1000　機能説明書「2.20.2 IPv6 DHCP機能」（P.78）

2.22.1　DHCPサーバ機能を使う

DHCPサーバ機能は、ネットワークに接続されているパソコンに対してIPアドレスの自動割り当てを行う機能です。

管理者はパソコンが増えるたびにIPアドレスが重複しないように設定する必要があります。

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

本装置のDHCPサーバ機能は、以下の情報を広報することができます。

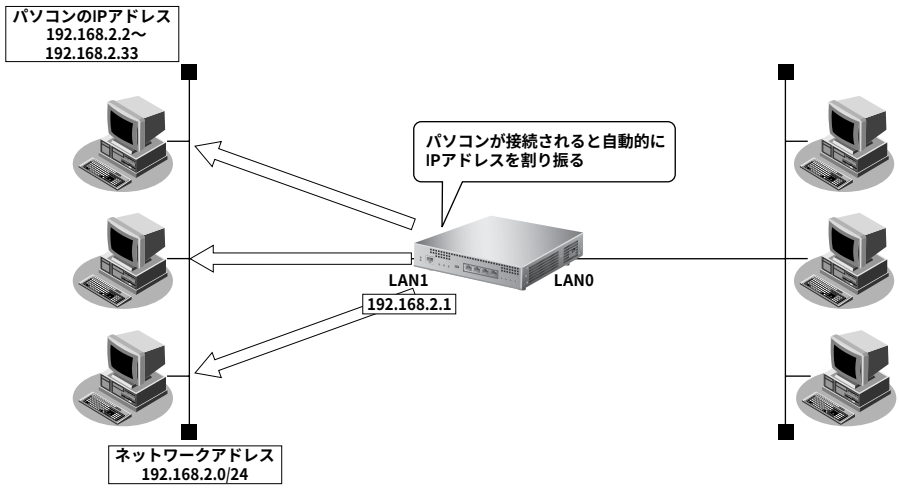
- IPアドレス
- ネットマスク
- リース期間
- デフォルトルータのIPアドレス
- DNSサーバのIPアドレス
- ドメイン名

こんな事に気をつけて

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

ここでは、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
- 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
# enable
```

2.22.2 DHCPスタティック機能を使う

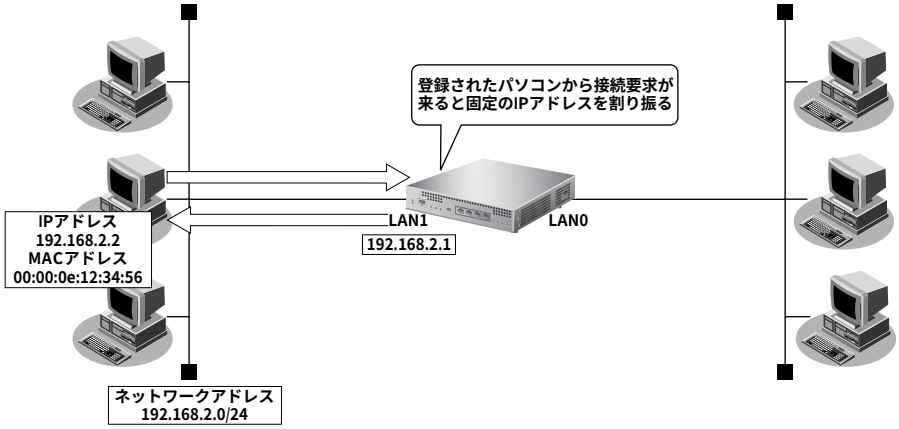
DHCPサーバは、使用していないIPアドレスを一定期間（またはパソコンがIPアドレスを返却するまで）割り当てます。不要になったIPアドレスは自動的に再利用されるため、パソコンのIPアドレスが変わることがあります。本装置では、IPアドレスとMACアドレスを対応付けることによって、登録されたパソコンからDHCP要求が発行されると、常に同じIPアドレスを割り当てることができます。これをDHCPスタティック機能と言います。

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
# enable
```

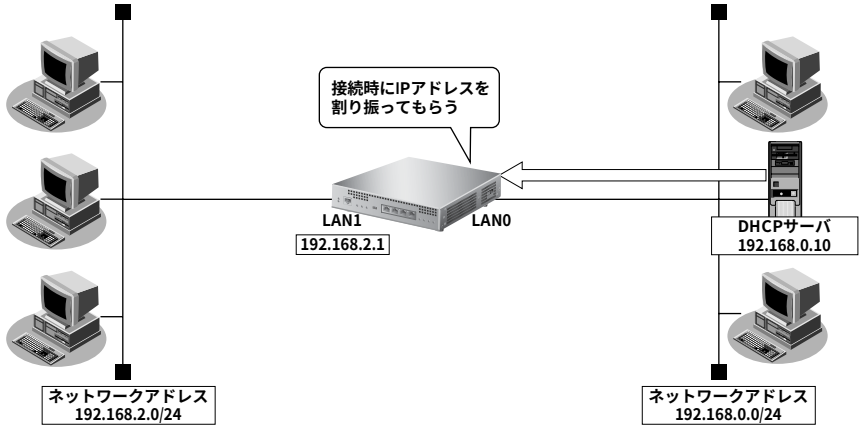
2.22.3　DHCP クライアント機能を使う

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

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
# enable
```

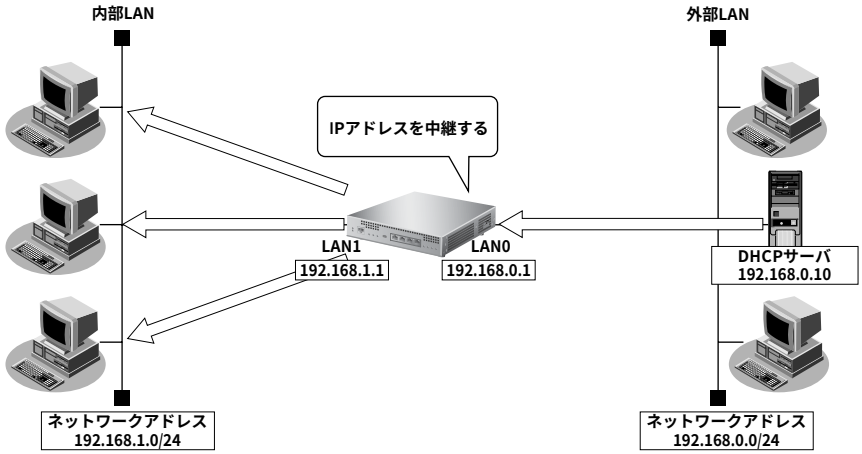
2.22.4　DHCPリレーエージェント機能を使う

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



● 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

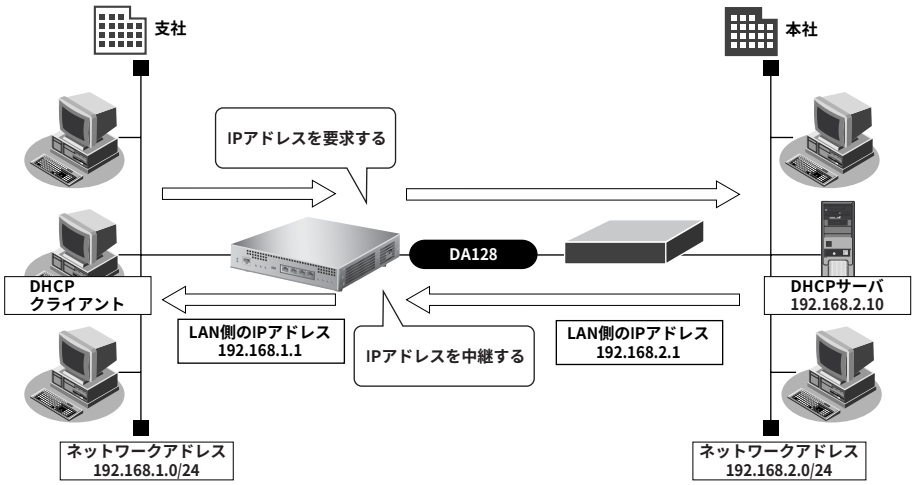
補足 DHCPリレーエージェント機能を使用するときは、NAT機能を使用できません。

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
# enable
```

リモート接続の場合



● 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 「1.8 事業所LANを専用線で接続する」（P.21）

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

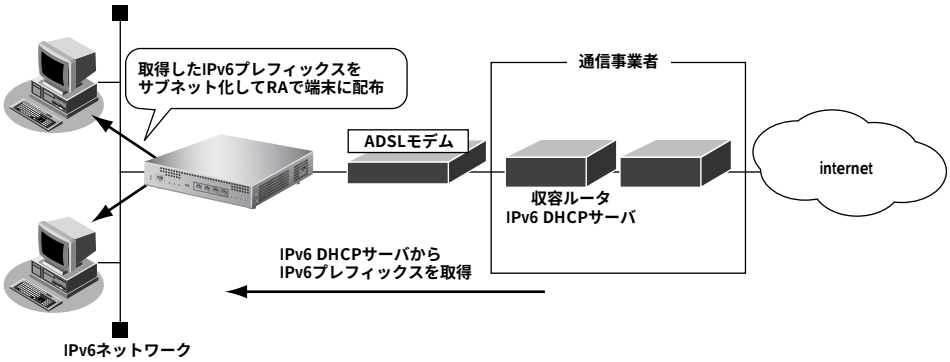
● コマンド

```
事務所 LAN を専用線で接続する
# wan 0 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
# enable
```

2.22.5　IPv6 DHCP クライアント機能を使う

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）

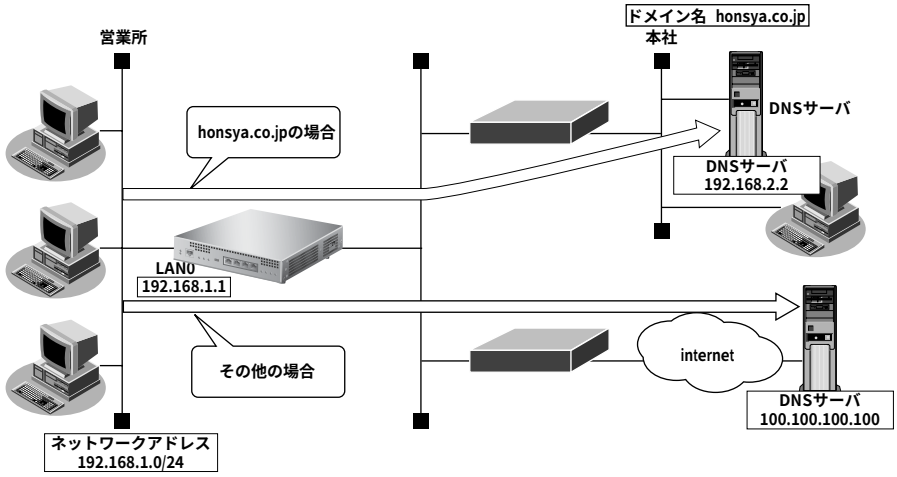
本装置のProxyDNSには、以下の機能があります。

- 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　MR1000　機能説明書「2.21 DNSサーバ機能」（P.80）

2.23.1　DNSサーバの自動切り替え機能（順引き）を使う

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
# enable
```

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。

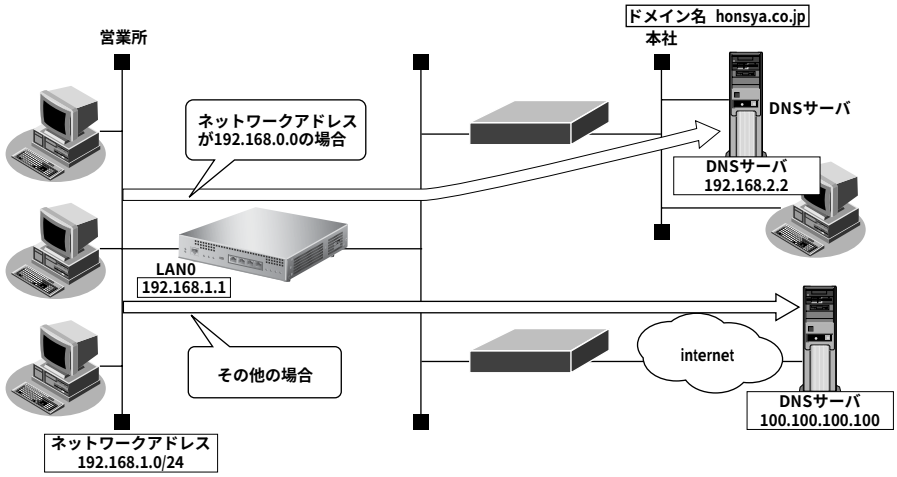
こんな事に気をつけて

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 MR1000　コマンドユーザーズガイド「1.4 コマンドで入力できる文字一覧」（P.18）

2.23.2　DNSサーバの自動切り替え機能（逆引き）を使う

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　MR1000　コマンドユーザーズガイド「1.4 コマンドで入力できる文字一覧」（P.18）

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
# enable
```

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

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 MR1000　コマンドユーザーズガイド「1.4 コマンドで入力できる文字一覧」（P.18）

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
# enable
```

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問い合わせタイプフィルタ機能を使う

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 MR1000　コマンドユーザーズガイド「1.4 コマンドで入力できる文字一覧」（P.18）

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
# enable
```

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、「DNSサーバアドレスの自動取得機能」の「パソコン側の設定を行う」（P.232）を参照してください。

2.23.5　DNS サーバ機能を使う

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 MR1000　コマンドユーザーズガイド「1.4 コマンドで入力できる文字一覧」（P.18）

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
# enable
```

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

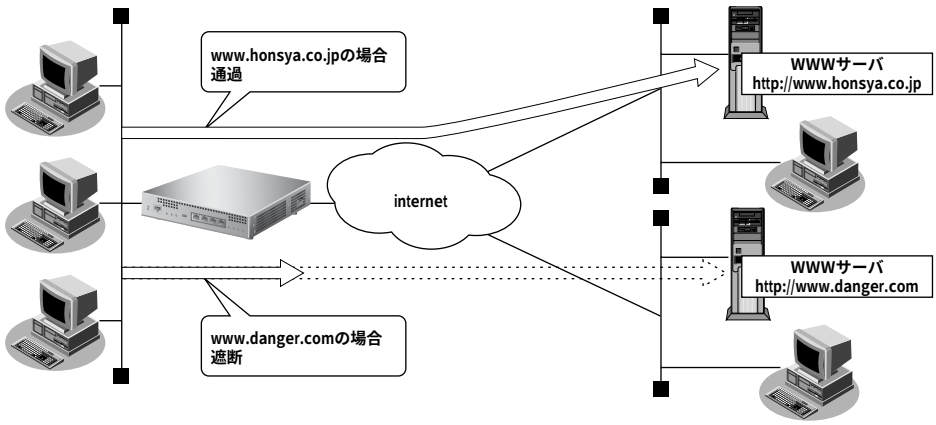
パソコン側の設定を行います。

設定方法は、「DNSサーバアドレスの自動取得機能」の「パソコン側の設定を行う」（P.232）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）

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 MR1000　機能説明書「2.21 DNSサーバ機能」（P.80）

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 MR1000　コマンドユーザーズガイド「1.4 コマンドで入力できる文字一覧」（P.18）

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。

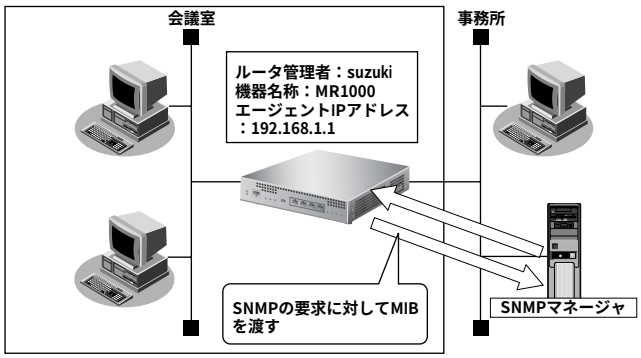
上記の設定条件に従って設定を行う場合のコマンド例を示します。

● 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
# enable
```

2.25　SNMPエージェント機能を使う

本装置は、SNMP（Simple Network Management Protocol）エージェント機能をサポートしています。
本装置が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 MR1000　機能説明書「2.22 SNMP機能」（P.82）

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 MR1000　仕様一覧「3.1 標準MIB定義」（P.23）、「3.2 Trap一覧」（P.35）

● 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　：MR1000
- 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ホスト名　：publicとする（任意のホストを対象とする）

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
SNMP エージェント機能を設定する
# snmp agent contact suzuki
# snmp agent sysname MR1000
# 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
# enable
```

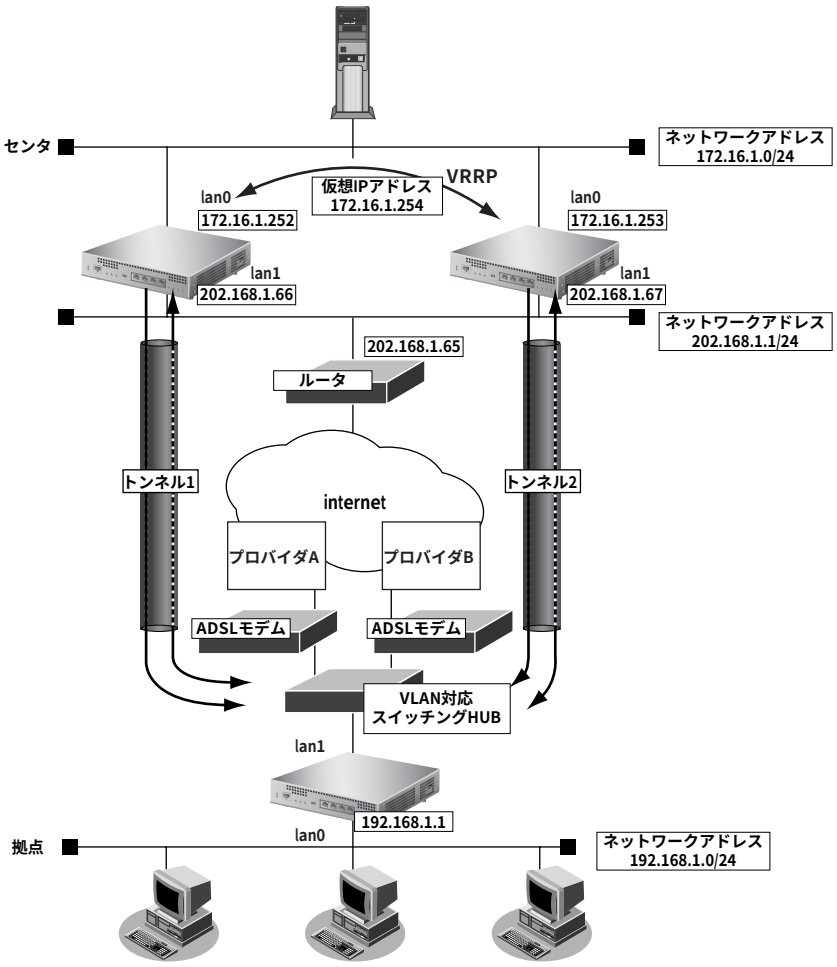
こんな事に気をつけて

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。

2.26　ECMP機能を使う

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　MR1000　機能説明書「2.23 ECMP機能」（P.83）

● 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）]

```
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

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 any 500 202.168.1.66/32 500 17 yes
# lan 1 ip filter 1 pass 202.168.1.66/32 500 any 500 17 yes
# lan 1 ip filter 2 pass any any 202.168.1.66/32 any 50 yes
# lan 1 ip filter 3 pass 202.168.1.66/32 any any any 50 yes
# lan 1 ip filter 4 reject any any any any 0 yes

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 172.16.1.252 192.168.1.1 5s 1m 5s

設定終了
# save
# enable
```

[センタ側本装置（右）]

```
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

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 any 500 202.168.1.67/32 500 17 yes
# lan 1 ip filter 1 pass 202.168.1.67/32 500 any 500 17 yes
# lan 1 ip filter 2 pass any any 202.168.1.67/32 any 50 yes
# lan 1 ip filter 3 pass 202.168.1.67/32 any any any 50 yes
# lan 1 ip filter 4 reject any any any any 0 yes

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 172.16.1.253 192.168.1.1 5s 1m 5s

設定終了
# save
# enable
```

[拠点側本装置]

```
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

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 any 500 202.168.1.66/32 500 17 yes
# remote 0 ip filter 1 pass 202.168.1.66/32 500 any 500 17 yes
# remote 0 ip filter 2 pass any any 202.168.1.66/32 any 50 yes
# remote 0 ip filter 3 pass 202.168.1.66/32 any any any 50 yes
# remote 0 ip filter 4 reject any any any any 0 yes
# 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 any 500 202.168.1.67/32 500 17 yes
# remote 1 ip filter 1 pass 202.168.1.67/32 500 any 500 17 yes
# remote 1 ip filter 2 pass any any 202.168.1.67/32 any 50 yes
# remote 1 ip filter 3 pass 202.168.1.67/32 any any any 50 yes
# remote 1 ip filter 4 reject any any any any 0 yes
# 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 192.168.1.1 172.16.1.252 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 192.168.1.1 172.16.1.253 5s 1m 5s

ECMPを設定する
# routemanage ip ecmp mode hash

設定終了
# save
# enable
```

2.27　VRRP機能を使う

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。

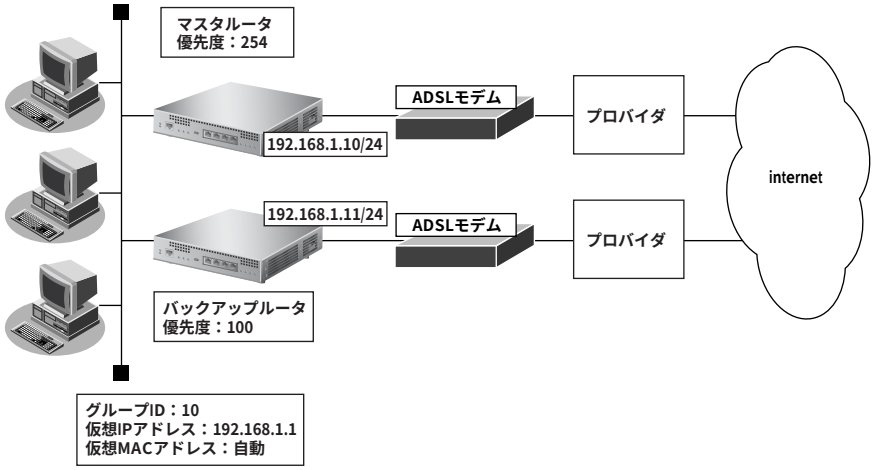
☛参照　MR1000　機能説明書「2.24 VRRP機能」（P.86）

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、vrrpctl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

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。

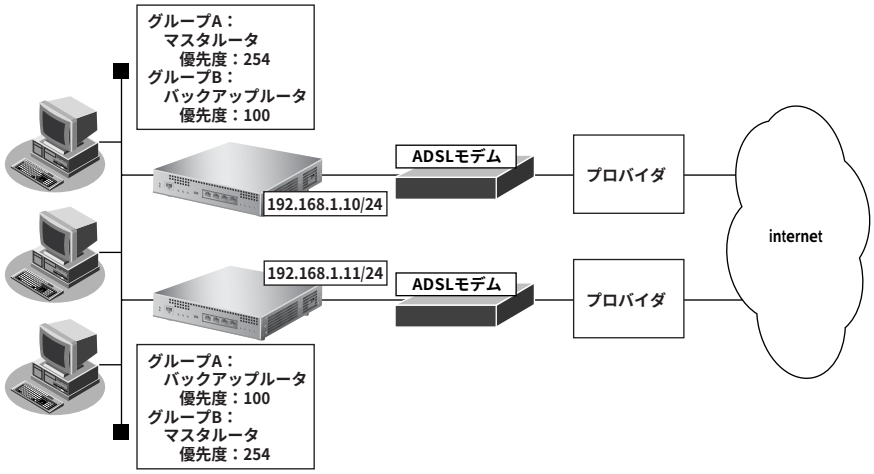
● コマンド

[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

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

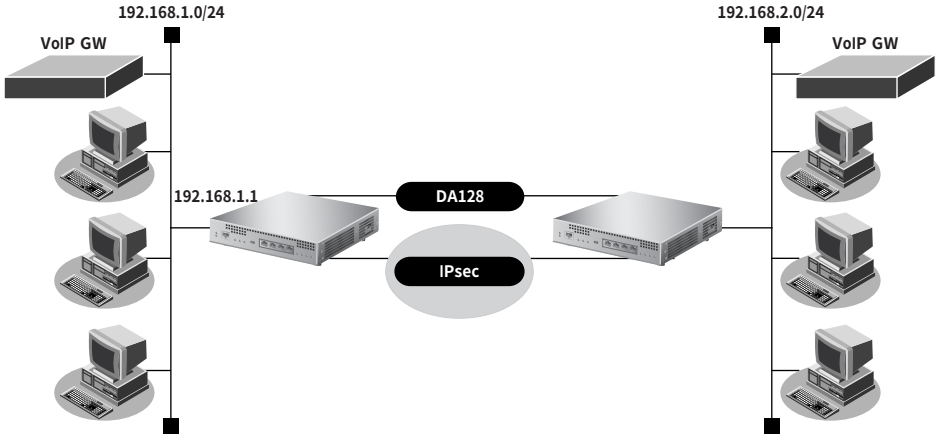
VRRP を設定する
lan 1 vrrp use on
lan 1 vrrp group 0 id 10 100 192.168.1.1
lan 1 vrrp group 1 id 11 254 192.168.1.2
lan 1 vrrp group 1 preempt off
lan 1 vrrp group 1 trigger 0 ifdown rmt0 254

設定終了
save

再起動
reset

2.28　マルチルーティング機能を使う

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.161）

- 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

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 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

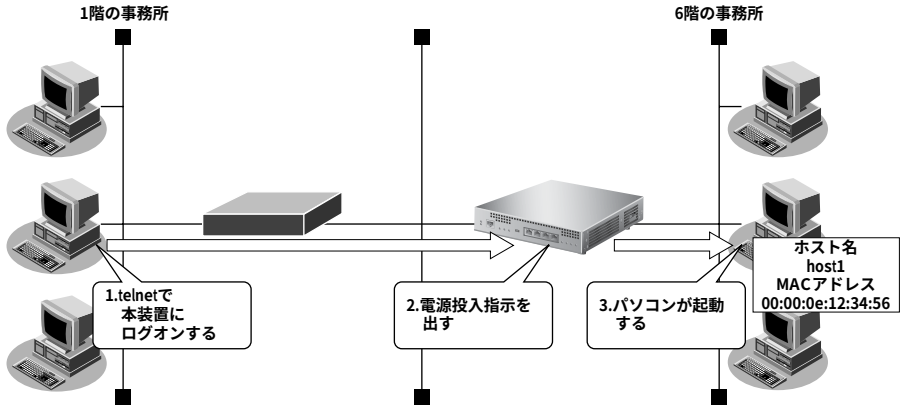
設定終了
save

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）

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 MR1000　コマンドユーザーズガイド「1.4 コマンドで入力できる文字一覧」(P.18)

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

● 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
# enable
```

2.29.2　リモートパワーオン機能を使う

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

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
  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　MR1000　コマンドユーザーズガイド「1.1 時計を設定する」（P.7）

2.30.1　スケジュールを予約する

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
# enable
```

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
# enable
```

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.252）

2.30.2　電話番号変更を予約する

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
# enable
```

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

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
# enable
```

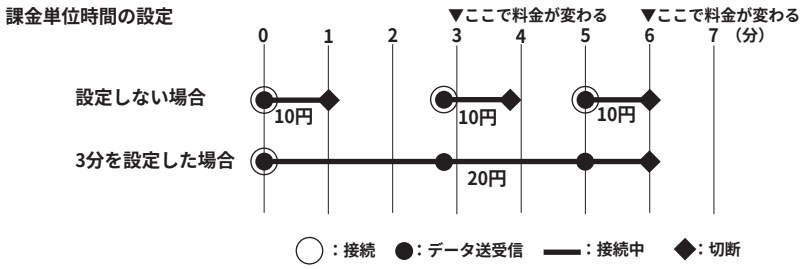
2.31　通信料金を節約する（課金制御機能）

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。

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。



また、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機能（課金制御機能）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。**

☛参照　MR1000　コマンドユーザーズガイド「2.1.8 課金情報で運用状況を確認する」（P.34）

2.31.1　課金単位時間を設定する

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
# enable
```

2.31.2　課金制御機能を設定する

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
# enable
```

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

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 MR1000　コマンドユーザーズガイド「1.4 コマンドで入力できる文字一覧」（P.18）

- **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。**

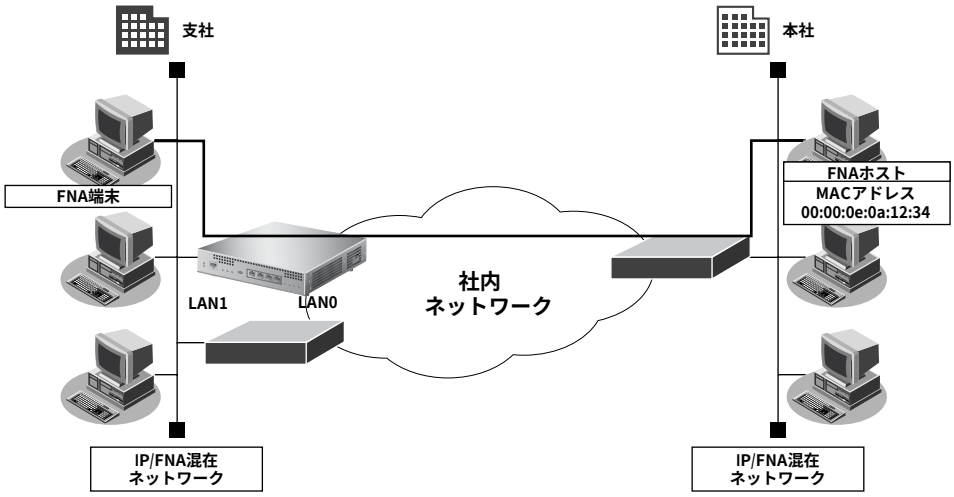
2.32.1　ブリッジでFNAをつないでSTP機能を使う

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 MR1000　機能説明書「2.25 ブリッジ機能」（P.91）

LAN接続の場合

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。

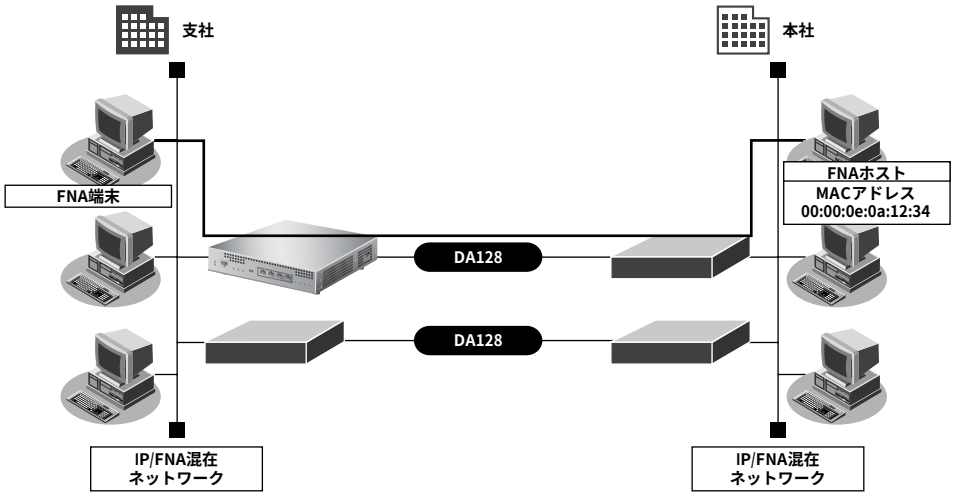
上記の設定条件に従って設定を行う場合のコマンド例を示します。

● 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（支社→本社）させる
# lan 0 bridge filter 0 pass any 00:00:0e:0a:12:34 llc 8080

フィルタリング情報でFNAを透過（本社→支社）させる
# lan 0 bridge filter 1 pass 00:00:0e:0a:12:34 any llc 8080

フィルタリング情報でSTPを透過させる
# lan 0 bridge filter 2 pass any 01:80:c0:00:00:00 llc 4242

残りの通信をすべて遮断する
# lan 0 bridge filter 3 reject any any any

設定終了
# save
# enable
```

リモート接続の場合

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

- ISDNポートで専用線（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。

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 「1.8 事業所LANを専用線で接続する」（P.21）

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 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（支社→本社）
# remote 0 bridge filter 0 pass any 00:00:0e:0a:12:34 llc 8080

フィルタリング情報で FNA を透過させる（本社→支社）
# remote 0 bridge filter 1 pass 00:00:0e:0a:12:34 any llc 8080

フィルタリング情報で STP を透過させる
# remote 0 bridge filter 2 pass any 01:80:c0:00:00:00 llc 4242

残りの通信をすべて遮断する
# remote 0 bridge filter 3 reject any any 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

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。

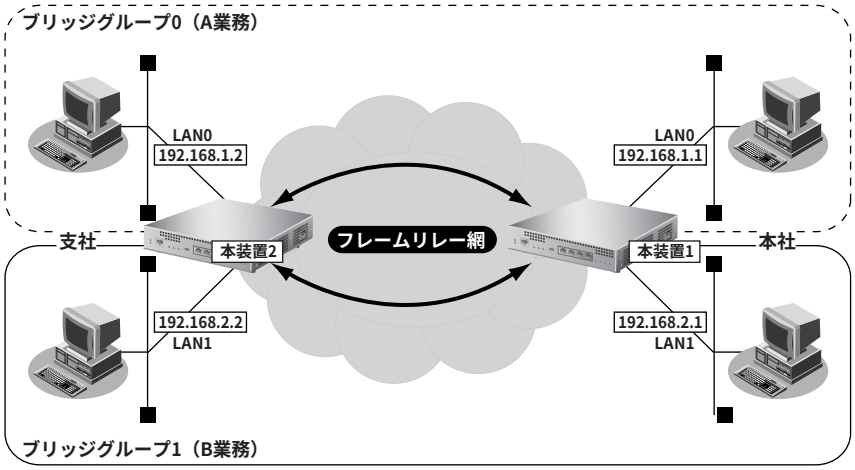
こんな事に気をつけて

- 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
  - ダイナミック経路

  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経路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]

- フレームリレー網を使用する
- A業務向けネットワーク名　：A-gyomu
- A業務向け接続先名　：FR-16
- A業務向けDLCI　：16
- A業務向けCIR　：64Kbps
- B業務向けネットワーク名　：B-gyomu
- B業務向け接続先名　：FR-17
- B業務向けDLCI　：17
- B業務向けCIR　：64Kbps

[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。ここではフレームリレーを例に示します。

```
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 line fr 128k
# remote 0 name A-gyomu
# remote 0 ap 0 name FR-16
# remote 0 ap 0 fr dlci 16
# remote 0 ap 0 fr cir 64
# remote 1 name B-gyomu
# remote 1 ap 0 name FR-17
# remote 1 ap 0 fr dlci 17
# remote 1 ap 0 fr cir 64

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。ここではフレームリレーを例に示します。

```
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 line fr 128k
# remote 0 name A-gyomu
# remote 0 ap 0 name FR-16
# remote 0 ap 0 fr dlci 16
# remote 0 ap 0 fr cir 64
# remote 1 name B-gyomu
# remote 1 ap 0 name FR-17
# remote 1 ap 0 fr dlci 17
# remote 1 ap 0 fr cir 64

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）

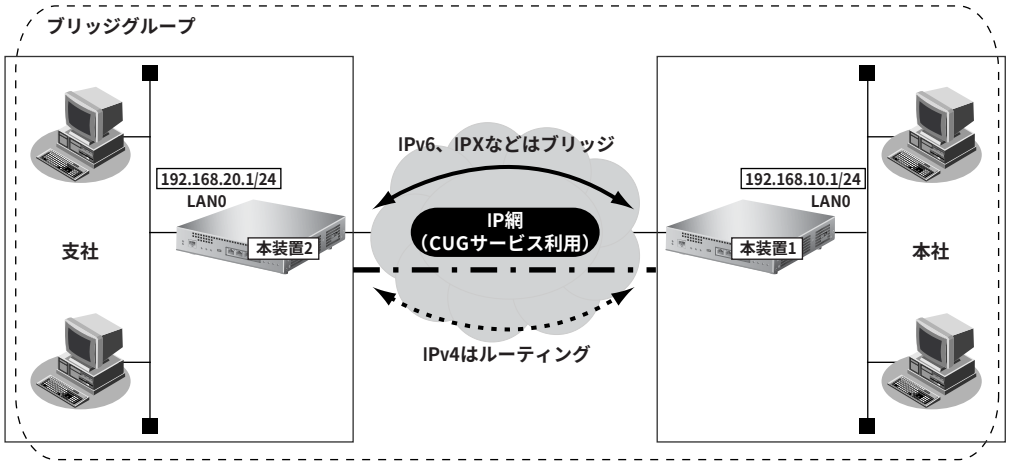
IPトンネル上でブリッジ機能を使用することにより、IP通信だけが可能な網でも、拠点間でブリッジ通信を行うことができます。

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
  - ダイナミック経路

  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経路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
# enable
```

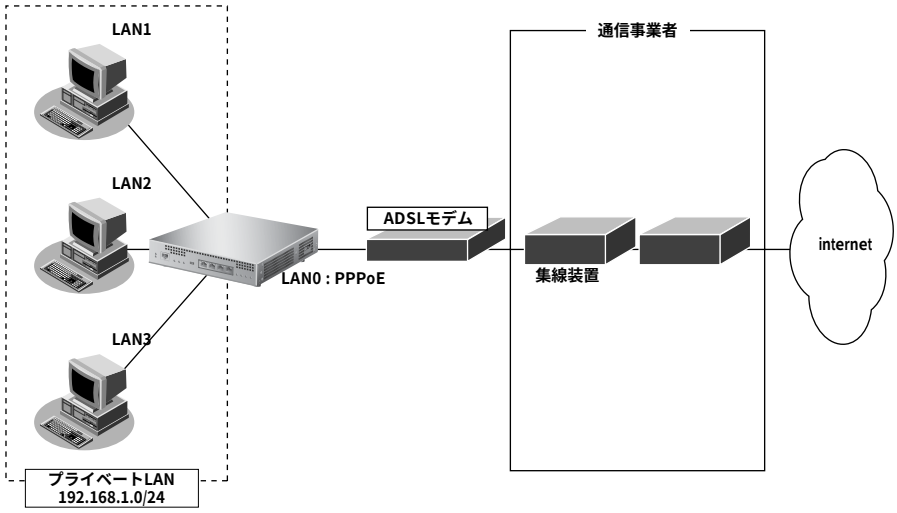
[本装置2（支社側）]

```
# 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
# enable
```

2.33　複数のLANポートをスイッチングHUBのように使う

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MR1000　機能説明書「2.25 ブリッジ機能」（P.91）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。**

「1.6 インターネットへPPPoEで接続する」（P.17）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　MR1000　機能説明書「2.25 ブリッジ機能」（P.91）

● 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経路を許可する

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

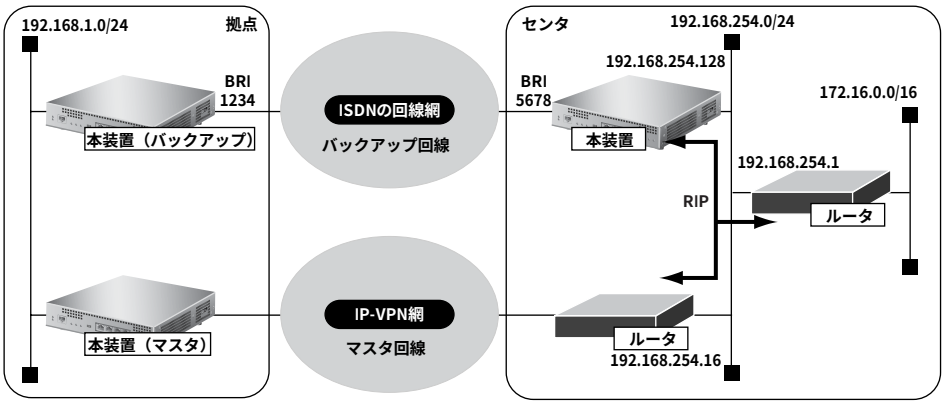
ブリッジグループを設定する
bridge 0 ip routing off
bridge 0 ip policy loose
bridge 0 ip6 routing off
bridge 0 ip6 policy loose

設定終了
save

再起動
reset

2.34　ISDN接続を契機とした通信バックアップを使う

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

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（BRI）を設定する
# 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
enable

2.35　外部のパソコンからPIAFS接続する

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　MR1000　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.42）

- **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。**

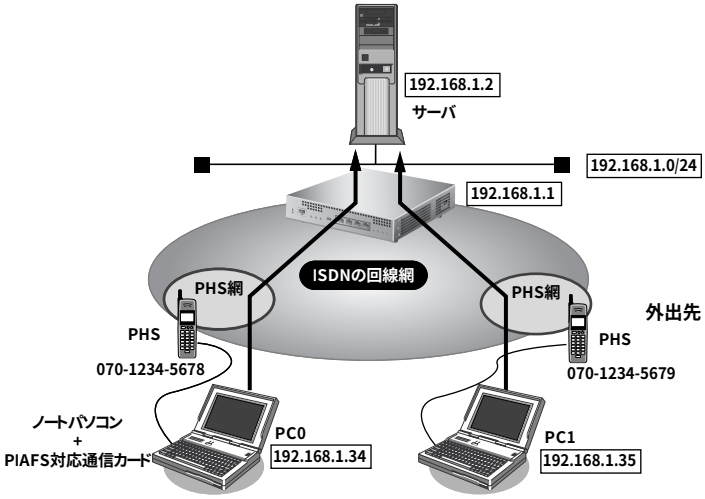
☛参照　MR1000　コマンドユーザーズガイド「1.4 コマンドで入力できる文字一覧」（P.18）

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

- ISDN Uポートを使用して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

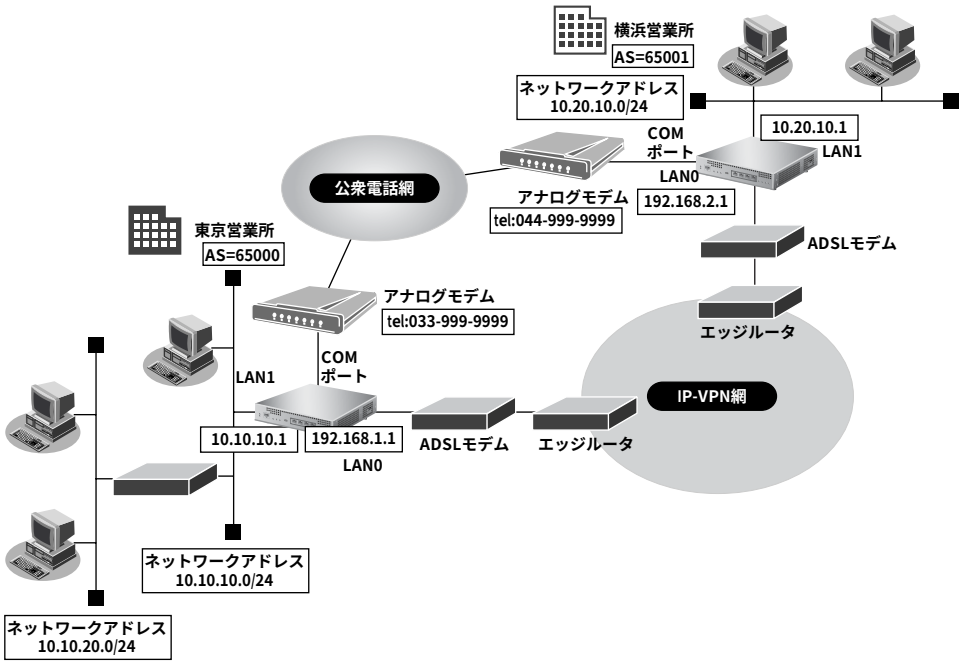
```
回線インタフェースとして ISDN を設定する
# wan 0 line isdn

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
```

2.36　アナログモデムで通信バックアップをする

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
ダイヤルトーン検知なし	X3
ダイヤルトーン検知あり	X4

カテゴリ	サポートコマンド
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
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 「1.12 複数の事業所 LAN を IP-VPN 網を利用して接続する」（P.33）

● 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
```

2.37 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）

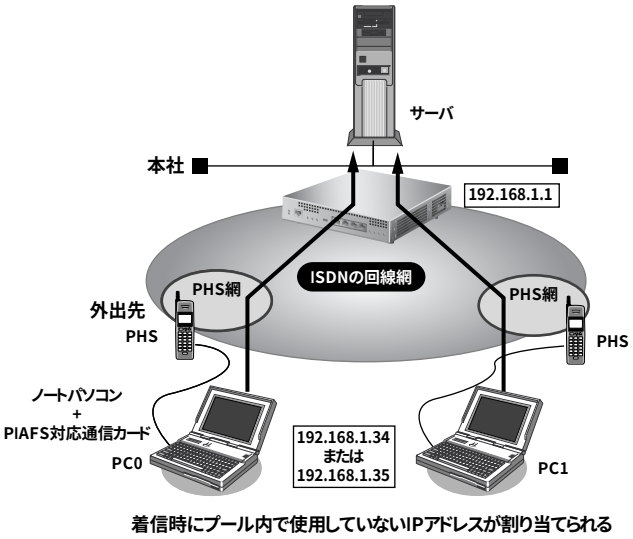
ISDN回線を使用して、外部のパソコンから本装置に着信接続する場合、本装置をリモートアクセスサーバとして使用することができます。以下の環境の場合に、リモートアクセスを行うことができます。

- 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による認証を組み合わせることで、リモートアクセスサーバを実現させることができます。

☛参照 MR1000　機能説明書「2.27 テンプレート着信機能」（P.117）

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

- ISDN Uポートを使用して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 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
```

索引

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

MR1000　コマンド設定事例集

発行日　　2005年3月

第2版　　K1N-D-04167B

発行責任　　オムロン株式会社

Printed in Japan