YAMAHA

ISDN

Network Equipment

設定例集

Rev.6.03, Rev.7.00, Rev.7.01
Rev.8.01, Rev.8.02, Rev.8.03
Rev.9.00, Rev.10.00, Rev.10.01 対応

はじめに

この設定例集では、ヤマハルーターのハードウェアインストール終了後の設定を、簡潔に説明します。
設定や操作コマンドの詳細についてはコマンドリファレンスを参照してください。

マニュアルのご案内

ご注意

●電波妨害について

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

●高調波について

JIS C 61000-3-2 適合品

JIS C-61000-3-2 適合品とは、日本工業規格「電磁両立性－第 3-2 部：限度値－高調波電流発生限度値（1 相当たりの入力電流が 20A 以下の機器）」に基づき、商用電力系統の高調波環境目標レベルに適合して設計・製造した製品です。

●輸出について

本製品は「外国為替及び外国貿易法」で定められた規制対象貨物 (および技術) に該当するため、輸出または国外への持ち出しには、同法および関連法令の定めるところに従い、日本国政府の許可を得る必要があります。

●通信料金について

本機をダイヤルアップルーターとしてご使用になる場合には、自動発信の機能をよくご理解の上ご使用ください。本機をコンピュータや LAN に接続した場合、本機はコンピュータや LAN 上を流れるデータの宛先を監視し、本体に設定された内容に従って自動的に回線への発信を行います。そのため、**設定間違い、回線切断忘れ、ソフトウェアが定期送信パケットを発信していたなどの場合には予想外の回線使用料やプロバイダ接続料金がかかる場合があります。**次のようなケースでは、通信履歴や課金額を時々調べて、意図しない発信が無いか、また課金額が適当であるかどうかにご注意ください。

- ○ 本機を使い始めた時
- ○ 本機の設定を変更した
- ○ プロバイダなどへの接続方式や通信速度（MP, PIAFS など）を変更したり、通信会社が提供する通信サービスの利用形態を変更した
- ○ コンピュータに新しいソフトウェアをインストールした
- ○ ネットワークに新しいコンピュータやネットワーク機器、周辺機器などを接続した
- ○ 本機のファームウェアをアップデートした
- ○ その他、いつもと違う操作を行ったり、通信速度の反応に違いを感じたなど

略称について

・本書では、RTX3000、RTX2000、RTX1500、RTX1100、RTX1000、RT300i、RT250i、RT107e、RT105、SRT100、RTX1200シリーズの総称を、ヤマハルーターと記述しています。
・本書では、Microsoft® Windows® を Windows、INS ネット 64/1500 のことを ISDN と記述しています。

商標について

目次

1.　コマンドの使い方

ヤマハルーターに直接コマンドを１つ１つ送って機能を設定したり操作したりする方法と、必要なコマンド一式を記述したファイルを送信して設定する方法の２種類をサポートしています。LANインタフェースが使用できない場合は、CONSOLE または SERIAL ポートを使ってコマンドを実行し、復旧などの必要な操作を行うができます。

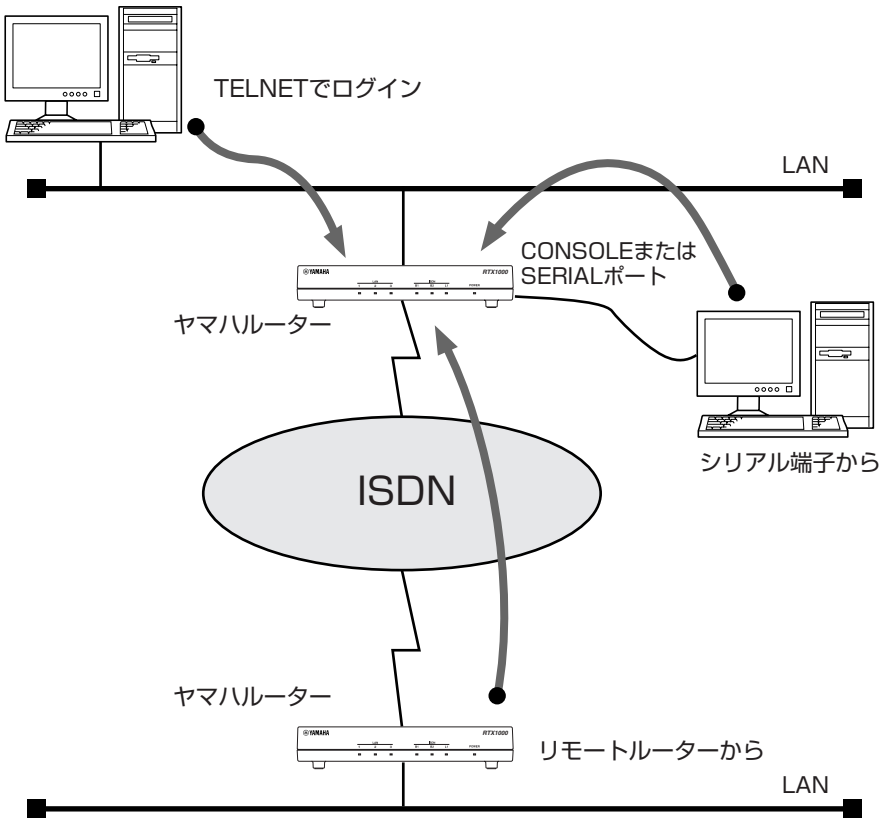
対話的に設定する手段をコンソールと呼び、コマンドを１つ１つ実行して設定や操作を行うことができます。必要なコマンド一式を記述したファイルを設定ファイル（Config）と呼び、TFTPによりヤマハルーターにアクセスできる環境から設定ファイルを送信したり受信することが可能です。

1.1　コンソールについて

ヤマハルーターに各種の設定を行うためには、本体の SERIAL(CONSOLE) コネクタに端末を接続する方法と、LAN 上のホストから TELNET でログインする方法、回線を介して別のヤマハルーターからログインする方法の３つがあります。

ヤマハルーターへのアクセス方法
ヤマハルーター本体の SERIAL(CONSOLE) コネクタに接続した端末からアクセス
LAN 上のホストから TELNET でログイン
ISDN 回線を介して別のヤマハルーターからログイン

ヤマハルーターへは、それぞれに対して 1 ユーザがアクセスすることができます。その中で管理ユーザになれるのは同時には 1 ユーザだけです。例えば、シリアル端末でアクセスしているユーザが管理ユーザとして設定を行っている場合には、別のユーザが一般ユーザとしてアクセスすることはできても管理ユーザになって設定を行うことはできません。



ご購入直後は、IP アドレス等のネットワークの設定が全くなされていません。初期設定を行うためには次の表の方法があります。

RARP サーバ	設定済ヤマハルーター	初期設定のためのアクセス方法
ある	ある	シリアル端末、イーサネット上のホスト、遠隔地のルーター
ある	ない	シリアル端末、イーサネット上のホスト
ない	ある	シリアル端末、遠隔地のルーター
ない	ない	シリアル端末

1.2　ヘルプ機能

ヤマハルーターでは、コンソールの使用方法を表示する機能と、コマンドの完全名称を忘れた場合やコマンドのパラメータの詳細が不明な場合に役立つ 2 つのヘルプ機能をサポートしています。
ヘルプ機能で提供するのはあくまで簡略な情報に過ぎませんから、コマンドの詳細な説明や注意事項、設定例などは、別冊の取扱説明書やコマンドリファレンスを参照するようにしてください。

1.2.1　コンソールの使用概要の表示 (help コマンドの実行)

コンソールの使用方法の概要が知りたい場合には、**help** コマンドを使用します。

```
> help
```

1.2.2　コマンド名称一覧の表示

コンソールにコマンド名称とその簡単な説明の一覧を表示させることができます。この場合には **show command** コマンドを使用します。
これにより類似したコマンドの差異を知ることができます。

```
> show command
```

1.3　コンソールによる設定手順

1.3.1　設定の開始から終了

CONSOLE または SERIAL ポートから設定を行う場合は、まずヤマハルーターの CONSOLE または SERIAL ポートとパソコンをクロスタイプのシリアルケーブルで接続します。シリアルケーブルの両端のコネクタはパソコンに適合したタイプをご使用ください。パソコンではターミナルソフトを使います。Windows をお使いの場合は OS に付属の『ハイパーターミナル』などのソフトウェアを使用します。MacOS X をお使いの場合は、OS に付属の『ターミナル』アプリケーションを使用します。

TELNET で設定を行う場合は、パソコンでは TELNET アプリケーションを使います。Windows をお使いの場合は OS に付属の『TELNET』ソフトウェアを使用します。MacOS X をお使いの場合は、OS に付属の『ターミナル』アプリケーションで telnet コマンドを実行します。

コンソールコマンドの具体的な内容については、別冊のコマンドリファレンスをご覧ください。

コンソールコマンドは、コマンドの動作をよく理解した上でお使いください。設定後に意図した動作をするかどうか、必ずご確認ください。

コンソールに表示される文字セットは初期値ではシフト JIS です。これは、**console character** コマンドを使用して端末の文字表示の能力に応じて選択できます。いずれの場合でもコマンドの入力文字は ASCII で共通であることに注意してください。

設定手順のおおまかな流れは次のようになります。

1. 一般ユーザとしてログインした後、**administrator** コマンドで管理ユーザとしてアクセスします。この時管理パスワードが設定してあれば、管理パスワードの入力が必要です。
2. 回線を接続していない相手の相手先情報を変更する場合には、**pp disable** コマンドを実行してから相手先情報の内容を変更してください。回線が接続されている場合には、**disconnect** コマンドでまず回線を手動切断しておきます。

3. 相手先情報の内容を各種コマンドを使用して変更します。ネットワーク形態に応じた設定の例は、第 2 章以降を参照してください。
4. **pp enable** コマンドを実行します。
5. **save** コマンドを実行して、不揮発性メモリに設定内容を保存します。

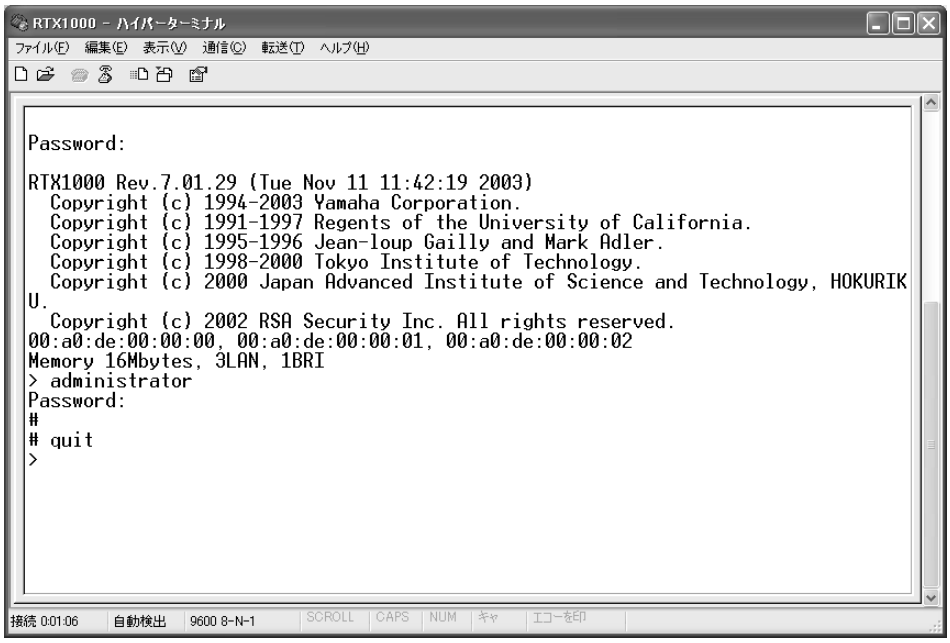
MEMO

Ctrl キーを押しながらS キーを押すと、コンソール出力を一時停止します。この状態でキーを押しても画面上は無反応に見えますが、キー入力は処理されます。コンソール出力を再開するには Crtl キーを押しながら Q キーを押します。

ヤマハルーターの電源を ON にすると、ルーターの出すメッセージが SERIAL(CONSOLE) コネクタに接続されたコンソールに表示されます。システムが起動して準備が整うと通常ログイン待ちの状態になります。
また、TELNET でログインしても同様な表示が現れます。

```
Password:
```

ログインを完了するとコマンド待ちの状態になり、各種コマンドが実行できます。
以下の例は、RTX1000 にハイパーターミナルを使ってログインした場合の表示です。



セキュリティの観点から、コンソールにキー入力が一定時間無い時には、自動的に 300 秒 (デフォルト値) でログアウトするように設定されています。この時間は **login timer** コマンドを使用して変更することができます。

新たに管理ユーザになって設定コマンドを実行すると、その内容はすぐに動作に反映されますが、**save** コマンドを実行しないと不揮発性メモリに書き込まれません。

注意

ご購入直後の起動や **cold start** 後にはログインパスワードも管理パスワードも設定されていません。ヤマハルーターのセキュリティ上、ログインパスワードと管理パスワードの設定をお勧めします。

MEMO

ヤマハルーターのご購入直後の起動でコンソールから各種の設定が行える状態になりますが、実際にパケットを配送する動作は行いません。

MEMO

セキュリティの設定や、詳細な各種パラメータなどの付加的な設定に関しては、個々のネットワークの運営方針などに基づいて行ってください。これらの詳細については、取扱説明書およびコマンドリファレンスを参照してください。

1.3.2　設定をデフォルトに戻す方法

設定をデフォルトに戻すコマンドには **cold start** コマンドがあります。このコマンドはすべてを工場出荷直後の設定に戻します。

cold start コマンドに際しては以下の点に注意してください。

- **cold start** コマンド実行には管理パスワードが必要です。
- 実行した直後にすべての通信が切断されます。
- デフォルト値が存在する設定はすべてデフォルトに変更されます。
- フィルタの定義や登録されたアドレスは消去されます。
- **save** コマンド無しで不揮発性メモリの内容が書き換えられますから、元に戻すことができなくなります。

各種コマンドの具体的なデフォルト値についてはコマンドリファレンスを参照してください。

2.　IP 設定例

本章では、IP ネットワークの基本的な接続形態を実現するための設定方法について、具体例をいくつかあげて説明します。セキュリティの設定や、詳細な各種パラメータなどの付加的な設定に関しては、個々のネットワークの運営方針などに基づいて行ってください。
なお、IPX の設定例は第 3 章を、ブリッジの設定例は第 4 章を参照してください。
この章で説明するネットワーク接続の形態は、次のようになります。

1. ISDN 回線で LAN を接続 (PP 側はスタティックルーティング)
2. ISDN 回線で LAN を MP 接続 (PP 側はスタティックルーティング)
3. ISDN 回線で LAN を接続 (PP 側は RIP2 を使用)
4. 128kbit/s ディジタル専用線で LAN を接続 (PP 側はスタティックルーティング、Un-numbered)
5. 128kbit/s ディジタル専用線で LAN を接続 (PP 側はスタティックルーティング、Numbered)
6. 128kbit/s ディジタル専用線で LAN を接続 (PP 側は RIP2 を使用)
7. ISDN 回線で 3 地点を接続
8. デフォルトルートを利用して接続
9. フリーダイヤルで接続
10. コールバックにより ISDN 回線を接続
11. Proxy ARP を使用して遠隔地の LAN を同一セグメントに見せる (ホストルート)
12. Proxy ARP を使用して遠隔地の LAN を同一セグメントに見せる
13. 端末型機器（TA、ISDN ボード等）との接続
14. 端末型機器（TA、ISDN ボード等）との接続 (相手は不特定)
15. IP マスカレード 機能による端末型ダイヤルアップ IP 接続
16. ISDN 回線で代表番号を使って LAN を接続
17. ISDN 回線と専用線を MP で接続
18. 専用線を ISDN 回線でバックアップ
19. ISDN3 回線で 5 対地の LAN を接続
20. ISDN4 回線ずつを MP で接続
21. ISDN 回線と専用線で 20ヶ所の LAN を接続 (RT300i)
22. 専用線によるプロバイダネットワーク型接続を ISDN によるプロバイダ端末型接続でバックアップ

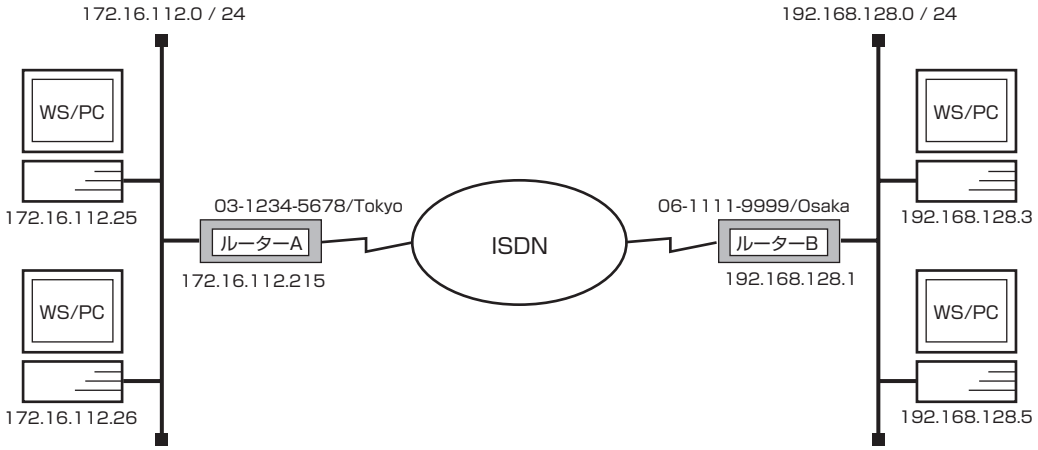
以下の説明では、それぞれのネットワークの接続形態例に対して構成図、手順、解説の順に行います。

MEMO

ヤマハリモートルーターを接続する LAN 上のパーソナルコンピュータやワークステーションに **default gateway** を設定する必要のある場合には、**ip *interface* address** コマンドで設定したヤマハリモートルーターの **LAN** 側の **IP** アドレスを設定します。

2.1　ISDN 回線で LAN を接続 (PP 側はスタティックルーティング)

[構成図]



[ルーター A の設定手順]

```
# isdn local address bri1 03-1234-5678/Tokyo
# ip lan1 address 172.16.112.215/24
# ip route 192.168.128.0/24 gateway pp 1
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 06-1111-9999/Osaka
pp1# pp enable 1
pp1# save
```

[ルーター B の設定手順]

```
# isdn local address bri1 06-1111-9999/Osaka
# ip lan1 address 192.168.128.1/24
# ip route 172.16.112.0/24 gateway pp 1
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 03-1234-5678/Tokyo
pp1# pp enable 1
pp1# save
```

[解説]

ネットワーク 172.16.112.0 とネットワーク 192.168.128.0 を ISDN 回線で接続するための設定を説明します。

相手のネットワークへの経路情報はコマンドで設定する (スタティックルーティング) ことでそれぞれのルーターに与えます。

ルーター A, ルーター B の設定手順は全く同じで、ISDN 番号や IP アドレスなどのコマンドのパラメータだけが異なります。

1. **isdn local address** コマンドを使用して、ISDN 番号を設定します 。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **ip route** コマンドを使用して、 接続先のネットワークへの経路情報を設定します。

4. **pp select** コマンドを使用して、相手先情報番号を選択します。

5. **pp bind** コマンドを使用して、選択した相手先番号に BRI ポートをバインドします。

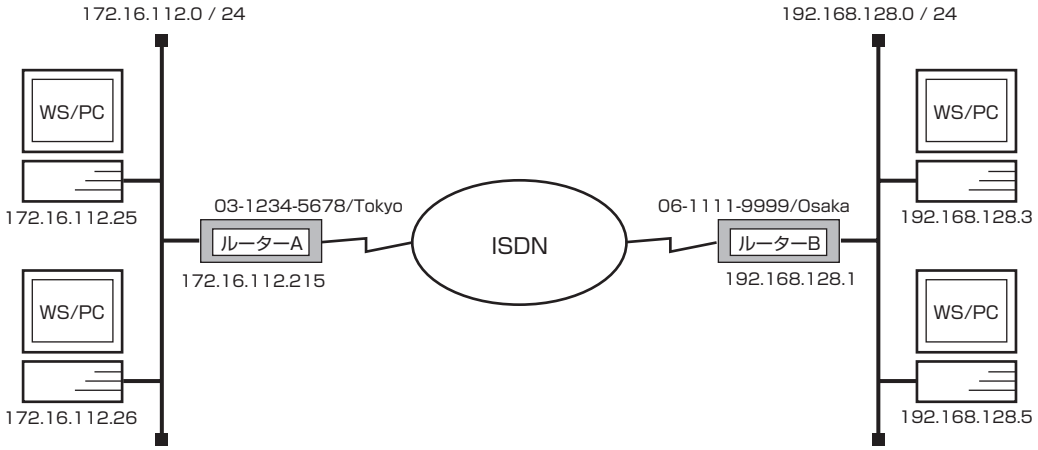
6. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、 サブアドレスを同時に設定する場合には、“/” に続けて入力します。

7. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、 実際にこのインタフェースをパケットが通過できるようになります。

8. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

2.2　ISDN 回線で LAN を MP 接続 (PP 側はスタティックルーティング)

[構成図]



[ルーター A の設定手順]

```
# isdn local address bri1 03-1234-5678/Tokyo
# ip lan1 address 172.16.112.215/24
# ip route 192.168.128.0/24 gateway pp 1
# pp select 1
pp1# pp bind bri1
pp1# ppp mp use on
pp1# isdn remote address call 06-1111-9999/Osaka
pp1# pp enable 1
pp1# save
```

[ルーター B の設定手順]

```
# isdn local address bri1 06-1111-9999/Osaka
# ip lan1 address 192.168.128.1/24
# ip route 172.16.112.0/24 gateway pp 1
# pp select 1
pp1# pp bind bri1
pp1# ppp mp use on
pp1# isdn remote address call 03-1234-5678/Tokyo
pp1# pp enable 1
pp1# save
```

[解説]

ネットワーク 172.16.112.0 とネットワーク 192.168.128.0 を ISDN 回線で MP で接続するための設定を説明します。

相手のネットワークへの経路情報はコマンドで設定する (スタティックルーティング) ことでそれぞれのルーターに与えます。

ルーター A, ルーター B の設定手順は全く同じで、ISDN 番号や IP アドレスなどのコマンドのパラメータだけが異なります。

1. **isdn local address** コマンドを使用して、ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **ip route** コマンドを使用して、 接続先のネットワークへの経路情報を設定します。

4. **pp select** コマンドを使用して、相手先情報番号を選択します。

5. **pp bind** コマンドを使用して、選択した相手先番号に BRI ポートをバインドします。

6. **ppp mp use** コマンドを使用して、MP 通信するように設定します。

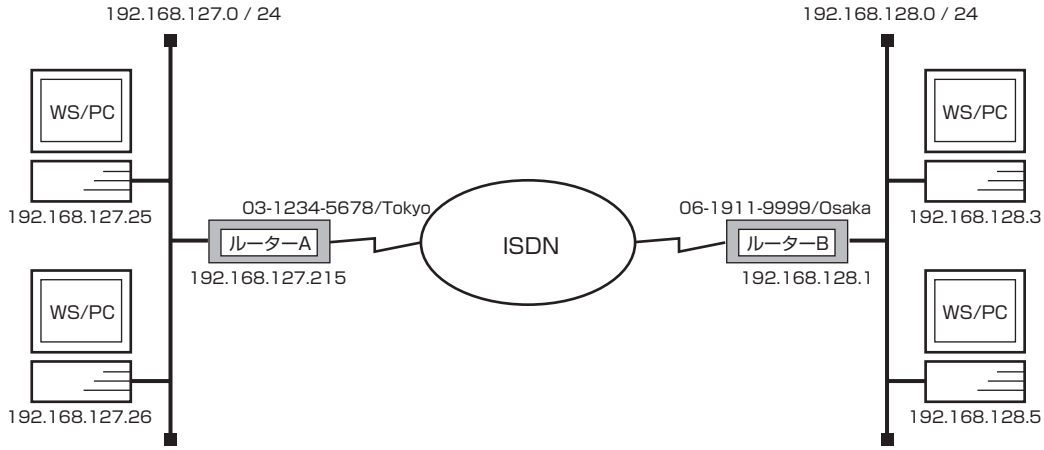
7. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、 サブアドレスを同時に設定する場合には、“/” に続けて入力します。

8. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、 実際にこのインタフェースをパケットが通過できるようになります。

9. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

2.3　ISDN 回線で LAN を接続 (PP 側は RIP2 を使用)

[構成図]



[ルーター A の設定手順]

```
# isdn local address bri1 03-1234-5678/Tokyo
# ip lan1 address 192.168.127.215/24
# rip use on
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 06-1111-9999/Osaka
pp1# ip pp rip send on version 2
pp1# ip pp rip hold routing on
pp1# pp enable 1
pp1# save
```

[ルーター B の設定手順]

```
# isdn local address bri1 06-1111-9999/Osaka
# ip lan1 address 192.168.128.1/24
# rip use on
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 03-1234-5678/Tokyo
pp1# ip pp rip send on version 2
pp1# ip pp rip hold routing on
pp1# pp enable 1
pp1# save
pp1# connect 1
pp1# disconnect 1
```

[解説]
ネットワーク 192.168.127.0 とネットワーク 192.168.128.0 を ISDN 回線で接続するための設定を説明します。

相手のネットワークへのルーティングはルーター同士の通信 (RIP2) で行います。
このためには、どちらかのルーターから一旦手動で回線を接続して経路情報を得る必要があります。(ルーター B の設定手順を参照)

■ルーター A
1. **isdn local address** コマンドを使用して、ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **rip use** コマンドを使用して、**rip** を有効にします。

4. **pp select** コマンドを使用して、相手先情報番号を選択します。

5. **pp bind** コマンドを使用して、選択した相手先番号に BRI ポートをバインドします。

6. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

7. **ip pp rip send** コマンドを使用して、回線側に RIP2 を流すように設定します。

8. **ip pp rip hold routing** コマンドを使用して、回線接続時に得られた RIP 情報を、回線切断後も保存するように設定します。

9. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

10. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

■ルーター B
1. **isdn local address** コマンドを使用して、ISDN 番号を設定します 。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **rip use** コマンドを使用して、**rip** を有効にします。

4. **pp select** コマンドを使用して、相手先情報番号を選択します。

5. **pp bind** コマンドを使用して、選択した相手先番号に BRI ポートをバインドします。

6. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

7. **ip pp rip send** コマンドを使用して、回線側に RIP2 を流すように設定します。

8. **ip pp rip hold routing** コマンドを使用して、回線接続時に得られた RIP 情報を、回線接続後も保存するように設定します。

9. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

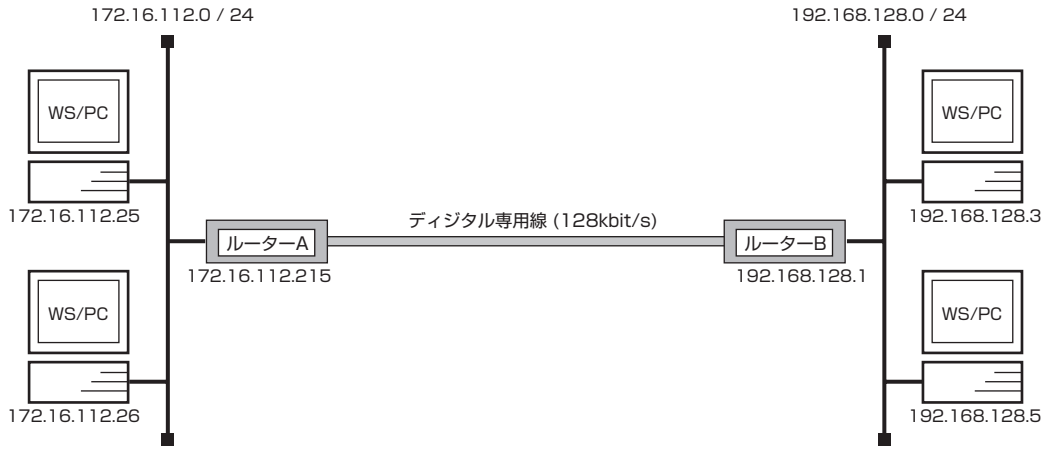
10. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

11. **connect** コマンドを使用して、手動でルーター A に接続し、RIP 情報を取得します。この時、ルーター A は正しく設定されている必要があります。

12. **disconnect** コマンドを使用して、回線を手動切断します。

2.4　128kbit/s ディジタル専用線で LAN を接続 (PP 側はスタティックルーティング、Un-numbered)

[構成図]



[ルーター A の設定手順]

```
# line type bri1 l128
# ip lan1 address 172.16.112.215/24
# ip route 192.168.128.0/24 gateway pp 1
# pp select 1
pp1# pp bind bri1
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

[ルーター B の設定手順]

```
# line type bri1 l128
# ip lan1 address 192.168.128.1/24
# ip route 172.16.112.0/24 gateway pp 1
# pp select 1
pp1# pp bind bri1
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

[解説]
ネットワーク 172.16.112.0 とネットワーク 192.168.128.0 を 128kbit/s のディジタル専用線で接続するための設定を説明します。

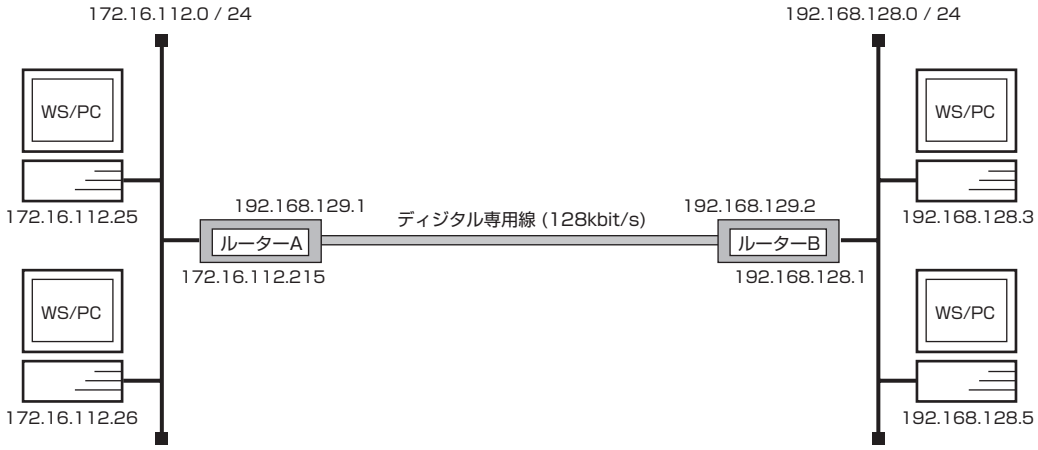
相手のネットワークへの経路情報はコマンドで設定する (スタティックルーティング) ことでそれぞれのルーターに与えます。
なお、通常は PP 側に IP アドレスを設定する必要はありません。これを Unnumbered といいます。相手側のルーターが IP アドレスを必要とする場合にだけ設定してください。

ルーター A, ルーター B の設定手順は全く同じで、ISDN 番号や IP アドレスなどのコマンドのパラメータだけが異なります。

1. **line type** コマンドを使用して、回線種別を 128kbit/s ディジタル専用線に指定します。
2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。
3. **ip route** コマンドを使用して、 接続先のネットワークへの経路情報を設定します。
4. **pp select** コマンドを使用して、相手先情報番号を選択します。
5. **pp bind** コマンドを使用して、選択した相手先番号に BRI ポートをバインドします。
6. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。
7. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。
8. **interface reset** コマンドを使用して、回線のハードウェアを切替えます。この後、実際にパケットが流れるようになります。

2.5　128kbit/s ディジタル専用線で LAN を接続 (PP 側はスタティックルーティング、Numbered)

[構成図]



[ルーター A の設定手順]

```
# line type bri1 l128
# ip lan1 address 172.16.112.215/24
# ip route 192.168.128.0/24 gateway pp 1
# pp select 1
pp1# pp bind bri1
pp1# ip pp address 192.168.129.1/24
pp1# ip pp remote address 192.168.129.2
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

[ルーター B の設定手順]

```
# line type bri1 l128
# ip lan1 address 192.168.128.1/24
# ip route 172.16.112.0/24 gateway pp 1
# pp select 1
# pp bind bri1
pp1# ip pp address 192.168.129.2/24
pp1# ip pp remote address 192.168.129.1
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

[解説]

ネットワーク 172.16.112.0 とネットワーク 192.168.128.0 を 128kbit/s のディジタル専用線で接続するための設定を説明します。

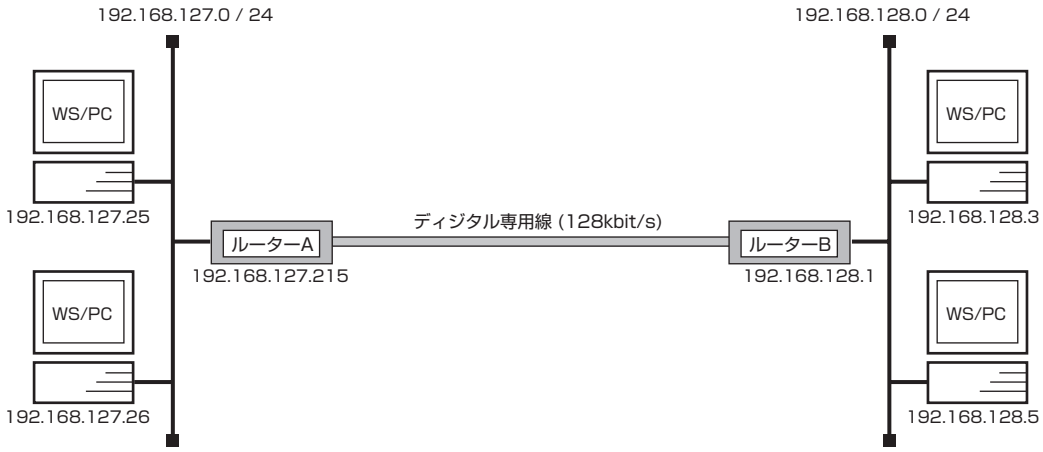
相手のネットワークへの経路情報はコマンドで設定する (スタティックルーティング) ことでそれぞれのルーターに与えます。
構成図で示す例では、 相手側のルーターが IP アドレスを必要とするものとして設定しています。これを Numbered といいます。
なお、通常は PP 側に IP アドレスを設定する必要はありません。

ルーター A, ルーター B の設定手順は全く同じで、IP アドレスなどのコマンドのパラメータだけが異なります。

1. **line type** コマンドを使用して、回線種別を 128kbit/s ディジタル専用線に指定します 。
2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。
3. **ip route** コマンドを使用して、 接続先のネットワークへの経路情報を設定します。
4. **pp select** コマンドを使用して、相手先情報番号を選択します。
5. **pp bind** コマンドを使用して、選択した相手先番号に BRI ポートをバインドします。
6. **ip pp address** コマンドを使用して、選択した PP 側のローカル IP アドレスとネットマスクを設定します。
7. **ip pp remote address** コマンドを使用して、選択した PP 側のリモート IP アドレスを設定します。
8. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。
9. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。
10. **interface reset** コマンドを使用して、回線のハードウェアを切替えます。この後、実際にパケットが流れるようになります。

2.6　128kbit/s ディジタル専用線で LAN を接続 (PP 側は RIP2 を使用)

[構成図]



[ルーター A の設定手順]

```
# line type bri1 l128
# ip lan1 address 192.168.127.215/24
# rip use on
# pp select 1
pp1# pp bind bri1
pp1# ip pp rip send on version 2
pp1# ip pp rip connect send interval
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

[ルーター B の設定手順]

```
# pp line l128
# line type bri1
# ip lan1 address 192.168.128.1/24
# rip use on
# pp select 1
pp1# pp bind bri1
pp1# ip pp rip send on version 2
pp1# ip pp rip connect send interval
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

[解説]
ネットワーク 192.168.127.0 とネットワーク 192.168.128.0 を 128kbit/s のディジタル専用線で接続するための設定を説明します。

相手のネットワークへのルーティングはルーター同士の通信 (RIP2) で行います。

ルーター A, ルーター B の設定手順は全く同じで、IP アドレスなどのコマンドのパラメータだけが異なります。

1. **line type** コマンドを使用して、回線種別を 128kbit/s ディジタル専用線に指定します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **rip use** コマンドを使用して、**rip** を有効にします。

4. **pp select** コマンドを使用して、相手先情報番号を選択します。

5. **pp bind** コマンドを使用して、選択した相手先番号に BRI ポートをバインドします。

6. **ip pp rip send** コマンドを使用して、回線側に RIP2 を流すように設定します。

7. **ip pp rip connect send** コマンドを使用して、回線接続時の RIP の送出を一定の時間間隔で行うようにします。この時間間隔は **ip pp rip connect interval** コマンドで設定します。デフォルト値は 30 秒です。

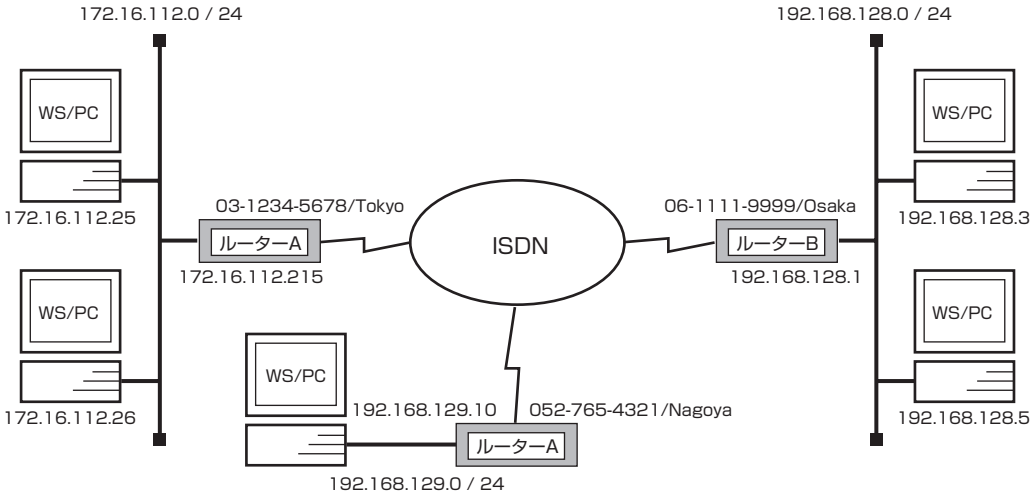
8. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

9. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

10. **interface reset** コマンドを使用して、回線種別の変更されたポートをリセットします。この後、実際にパケットが流れるようになります。

2.7　ISDN 回線で 3 地点を接続

[構成図]



[ルーター A の設定手順]

```
# isdn local address bri1 03-1234-5678/Tokyo
# ip lan1 address 172.16.112.215/24
# ip route 192.168.128.0/24 gateway pp 2
# ip route 192.168.129.0/24 gateway pp 3
# pp select 2
pp2# pp bind bri1
pp2# isdn remote address call 06-1111-9999/Osaka
pp2# pp enable 2
pp2# pp select 3
pp3# pp bind bri1
pp3# isdn remote address call 052-765-4321/Nagoya
pp3# pp enable 3
pp3# save
```

[ルーター B の設定手順]

```
# isdn local address bri1 06-1111-9999/Osaka
# ip lan1 address 192.168.128.1/24
# ip route 172.16.112.0/24 gateway pp 1
# ip route 192.168.129.0/24 gateway pp 3
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 03-1234-5678/Tokyo
pp1# pp enable 1
pp1# pp select 3
pp3# pp bind bri1
pp3# isdn remote address call 052-765-4321/Nagoya
pp3# pp enable 3
pp3# save
```

[ルーター C の設定手順]

```
# isdn local address bri1 052-765-4321/Nagoya
# ip lan1 address 192.168.129.10/24
# ip route 172.16.112.0/24 gateway pp 1
# ip route 192.168.128.0/24 gateway pp 2
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 03-1234-5678/Tokyo
pp1# pp enable 1
pp1# pp select 2
pp2# pp bind bri1
pp2# isdn remote address call 06-1111-9999/Osaka
pp2# pp enable 2
pp2# save
```

[解説]

ネットワーク 172.16.112.0 とネットワーク 192.168.128.0 、更にネットワーク 192.168.129.0 を ISDN 回線で接続するための設定を説明します。

相手のネットワークへの経路情報はコマンドで設定する (スタティックルーティング) ことでそれぞれのルーターに与えます。1 台のルーターには、その他の 2 地点のルーターそれぞれに対する設定を行います。

ルーター A, ルーター B, ルーター C の設定手順は全く同じで、ISDN 番号や IP アドレスなどのコマンドのパラメータだけが異なります。

1. **isdn local address** コマンドを使用して、ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **ip route** コマンドを使用して、 接続先のネットワークへの経路を設定します。

4. **pp select** コマンドを使用して、相手先情報番号を選択します。

5. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

6. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、 サブアドレスを同時に設定する場合には、“/” に続けて入力します。

7. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

8. **pp select** コマンドを使用して、相手先情報番号を選択します。

9. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

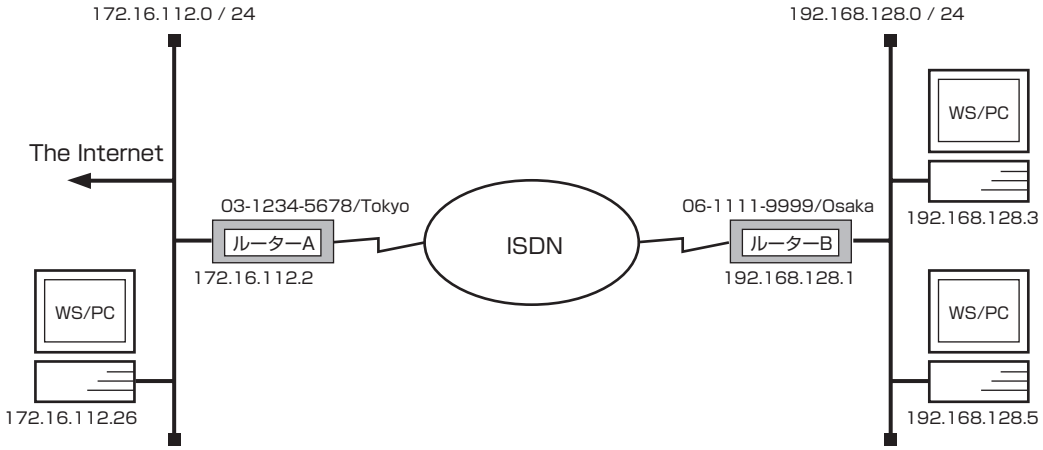
10. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、 サブアドレスを同時に設定する場合には、“/” に続けて入力します。

11. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

12. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

2.8　デフォルトルートを利用して接続

[構成図]



[手順]

```
# isdn local address bri1 06-1111-9999/Osaka
# ip lan1 address 192.168.128.1/24
# ip route default gateway pp 1
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 03-1234-5678/Tokyo
pp1# pp enable 1
pp1# save
```

[解説]

ネットワーク 192.168.128.0 をネットワーク 172.16.112.0 へ ISDN 回線によりデフォルトルート機能を使用して接続するための設定を説明します。

インターネットとの通信を具体的なアドレス情報を設定することで行うのではなく、デフォルトルートで行います。ここでは、デフォルトルートで指定したネットワーク上のルーターが、インターネットへのルーティングを行えることが前提になっています。

1. **isdn local address** コマンドを使用して、ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、"/" に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **ip route** コマンドを使用して、デフォルトルートを設定します。この場合、192.168.128.0/24 宛て以外のパケットはすべて ISDN 番号が 03-1234-5678/Tokyo のルーターへ送られます。

4. **pp select** コマンドを使用して、相手先情報番号を選択します。

5. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

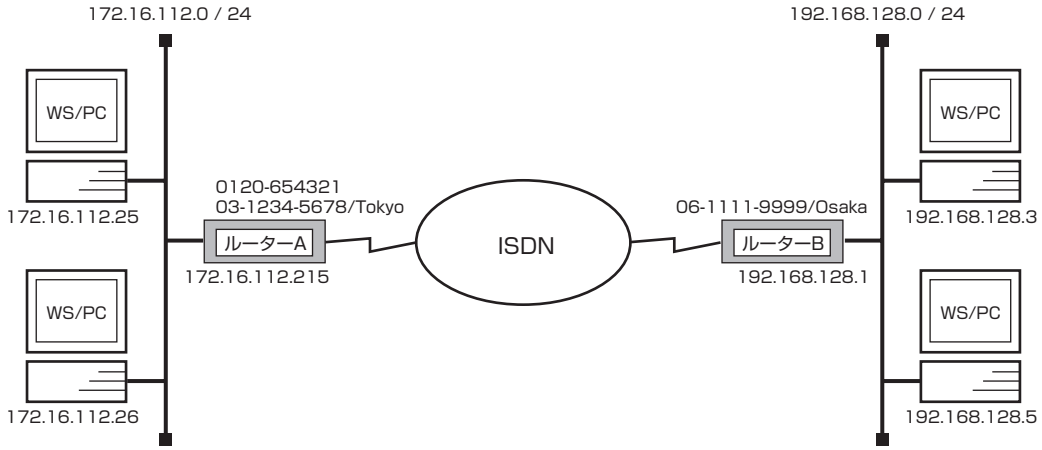
6. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、"/" に続けて入力します。

7. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

8. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

2.9　フリーダイヤルで接続

［構成図］



［ルーター A の設定手順］

```
# isdn local address bri1 03-1234-5678/Tokyo
# ip lan1 address 172.16.112.215/24
# ip route 192.168.128.0/24 gateway pp 1
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 06-1111-9999/Osaka
pp1# pp enable 1
pp1# save
```

［ルーター B の設定手順］

```
# isdn local address 06-1111-9999/Osaka
# ip lan1 address 192.168.128.1
# ip route 172.16.112.0/24 gateway pp 2
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 0120-654321/Tokyo 03-1234-5678/Tokyo
pp1# pp enable 1
pp1# save
```

［解説］
ネットワーク 172.16.112.0 と、ネットワーク 192.168.128.0 を ISDN 回線で接続します。
192.168.128.0 から 172.168.112.0 へはフリーダイヤルで接続します。

フリーダイヤルを設定している回線側のルーター A からも発信することがある状況とします。
この場合、ルーター B からルーター A へ発信する時はフリーダイヤルの番号を使用しますが、ルーター A からルーター B に発信する時の発番号には、ルーター A の契約者回線番号が使われます。従って、ルーター B では、ルーター A に発信する番号 (フリーダイヤルの番号) とルーター A の契約者回線番号の 2 つの番号を設定しなければなりません。

相手のネットワークへの経路情報はコマンドで設定する (スタティックルーティング) ことでそれぞれのルーターに与えます。

■ルーター A
1. **isdn local address** コマンドを使用して、ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、"/" に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **ip route** コマンドを使用して、接続先のネットワークへの経路を設定します。

4. **pp select** コマンドを使用して、相手先情報番号を選択します。

5. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

6. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

7. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

8. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

■ルーター B
1. **isdn local address** コマンドを使用して、ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **ip route** コマンドを使用して、接続先のネットワークへの経路を設定します。

4. **pp select** コマンドを使用して、相手先情報番号を選択します。

5. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

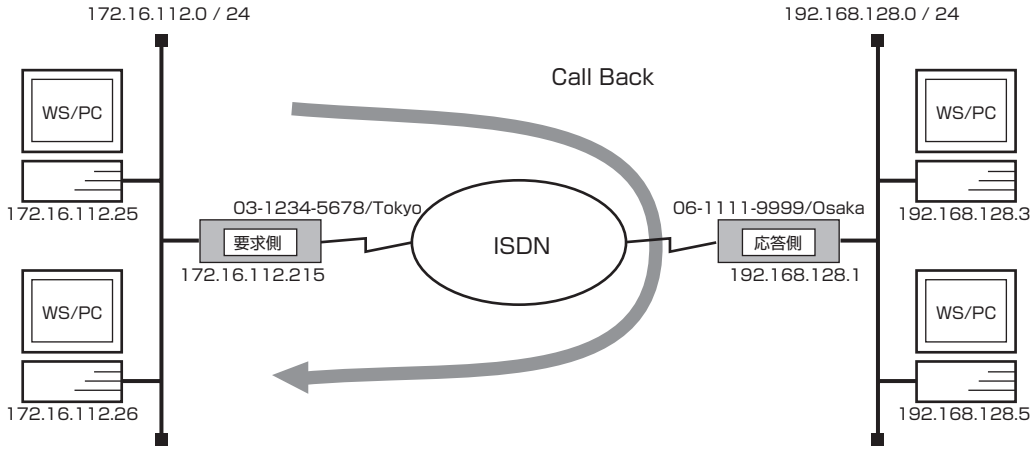
6. **isdn remote address** コマンドを使用して、ルーター A への発信用の番号 (フリーダイヤルの 0120-654321) と着信用の番号 (03-1234-5678/Tokyo) を設定します。

7. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

8. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

2.10 コールバックにより ISDN 回線を接続

［構成図］



［コールバックを要求するルーターの設定手順］

```
# isdn local address bri1 03-1234-5678/Tokyo
# ip lan1 address 172.16.112.215/24
# ip route 192.168.128.0/24 gateway pp 1
# pp select 1
pp1# pp bind bri1
pp1# isdn callback request on
pp1# isdn remote address call 06-1111-9999/Osaka
pp1# pp enable 1
pp1# save
```

［コールバックするルーターの設定手順］

```
# isdn local address bri1 06-1111-9999/Osaka
# ip lan1 address 192.168.128.1/24
# ip route 172.16.112.0/24 gateway pp 1
# pp select 1
pp1# pp bind bri1
pp1# isdn callback permit on
pp1# isdn remote address call 03-1234-5678/Tokyo
pp1# pp enable 1
pp1# save
```

［解説］

ネットワーク 172.16.112.0 とネットワーク 192.168.128.0 をコールバックにより接続するための設定を説明します。

相手のネットワークへの経路情報はコマンドで設定する (スタティックルーティング) ことでそれぞれのルーターに与えます。

コールバック機能は、接続したいヤマハリモートルーターに対してこちらへ発信してもらうように要求する機能です。コールバック機能を使用することにより、ISDN 回線の通信費を相手側のヤマハリモートルーター (発信側) に負担するようにできます。

コールバックを要求するルーターと、コールバックに応答するルーターでは設定コマンドが異なることに注意してください。

■コールバックを要求する側（要求側）

1. **isdn local address** コマンドを使用して、ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/”に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **ip route** コマンドを使用して、接続先のネットワークへの経路を設定します。

4. **pp select** コマンドを使用して、相手先情報番号を選択します。

5. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

6. **isdn callback request** コマンドを使用して、接続時にはコールバック要求を出すように設定します。

7. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、"/" に続けて入力します。

8. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

9. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

■コールバックする側（応答側）

1. **isdn local address** コマンドを使用して、ISDN 番号を設定します 。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/”に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **ip route** コマンドを使用して、接続先のネットワークへの経路を設定します。

4. **pp select** コマンドを使用して、相手先情報番号を選択します。

5. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

6. **isdn callback permit** コマンドを使用して、 コールバック要求を受信したらコールバックに応答するように設定します。

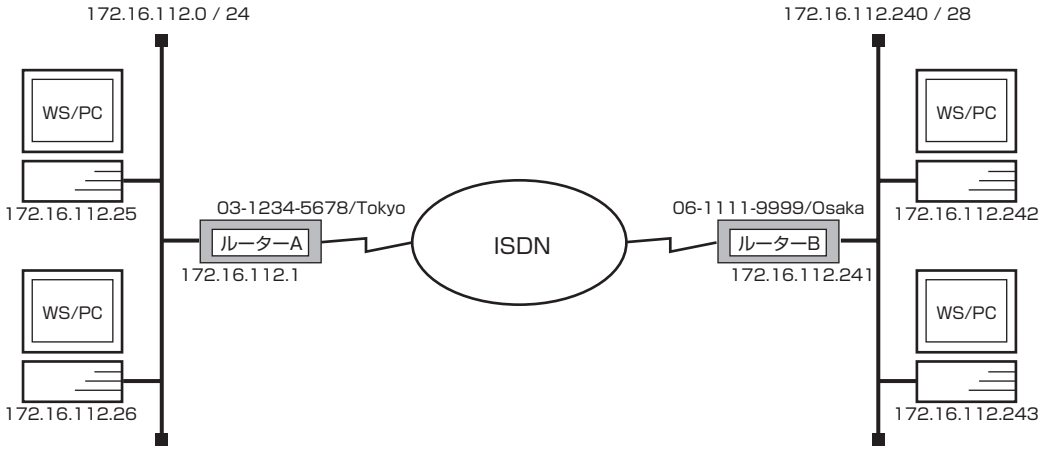
7. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、"/" に続けて入力します。

8. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

9. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

2.11 Proxy ARP を使用して遠隔地の LAN を同一セグメントに見せる (ホストルート)

[構成図]



[ルーター A の設定手順]

```
# isdn local address bri1 03-1234-5678/Tokyo
# ip lan1 address 172.16.112.1/24
# ip route 172.16.112.241 gateway pp 1
# ip route 172.16.112.242 gateway pp 1
# ip route 172.16.112.243 gateway pp 1
# ip lan1 proxyarp on
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 06-1111-9999/Osaka
pp1# pp enable 1
pp1# save
```

[ルーター B の設定手順]

```
# isdn local address 06-1111-9999/Osaka
# ip lan1 address 172.16.112.241/28
# ip route default gateway pp 1
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 03-1234-5678/Tokyo
pp1# pp enable 1
pp1# save
```

[解説]

ネットワーク 172.16.112.0 と、その一部分の IP アドレスを持つネットワークを Proxy ARP を使用して接続するための設定を説明します。

構成図における IP アドレスの割り当ては次の表のような関係になります。

IP アドレス	割り当て
172.16.112.0	ネットワーク
172.16.112.1	ルーター A
172.16.112.2 : 172.16.112.239	ホスト (238 台分)
172.16.112.240 : 172.16.112.254	ルーター B の ネットワーク
172.16.112.255	ブロードキャスト

IP アドレス	割り当て
172.16.112.240	ネットワーク
172.16.112.241	ルーター B
172.16.112.242 : 172.16.112.254	ホスト (13 台分)
172.16.112.255	ブロードキャスト

ルーター A は Proxy ARP を使用して、ルーター B の LAN との通信を行います。ルーター B の LAN 上のホストからのパケットはデフォルトルートを設定してルーター A に向けておきます。

■ルーター A

1. **isdn local address** コマンドを使用して、ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/”に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **ip lan1 proxyarp** コマンドを使用して、LAN 側に Proxy ARP を返すように設定します。

4. **ip route** コマンドを使用して、接続先のネットワークへの経路を設定します。
通常のネットルートではなくホストルートである点に注意してください。ip route 172.16.112.240/28 gateway pp 1 と設定すると、172.16.112.255 というブロードキャストパケットまでルーター B に流れることになります。

5. **pp select** コマンドを使用して、相手先情報番号を選択します。

6. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

7. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/”に続けて入力します。

8. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

9. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

■ルーター B

1. **isdn local address** コマンドを使用して、ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/”に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **ip route** コマンドを使用して、接続先のネットワークへの経路を設定します。他への経路がないので、デフォルトルートを使います。

4. **pp select** コマンドを使用して、相手先情報番号を選択します。

5. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

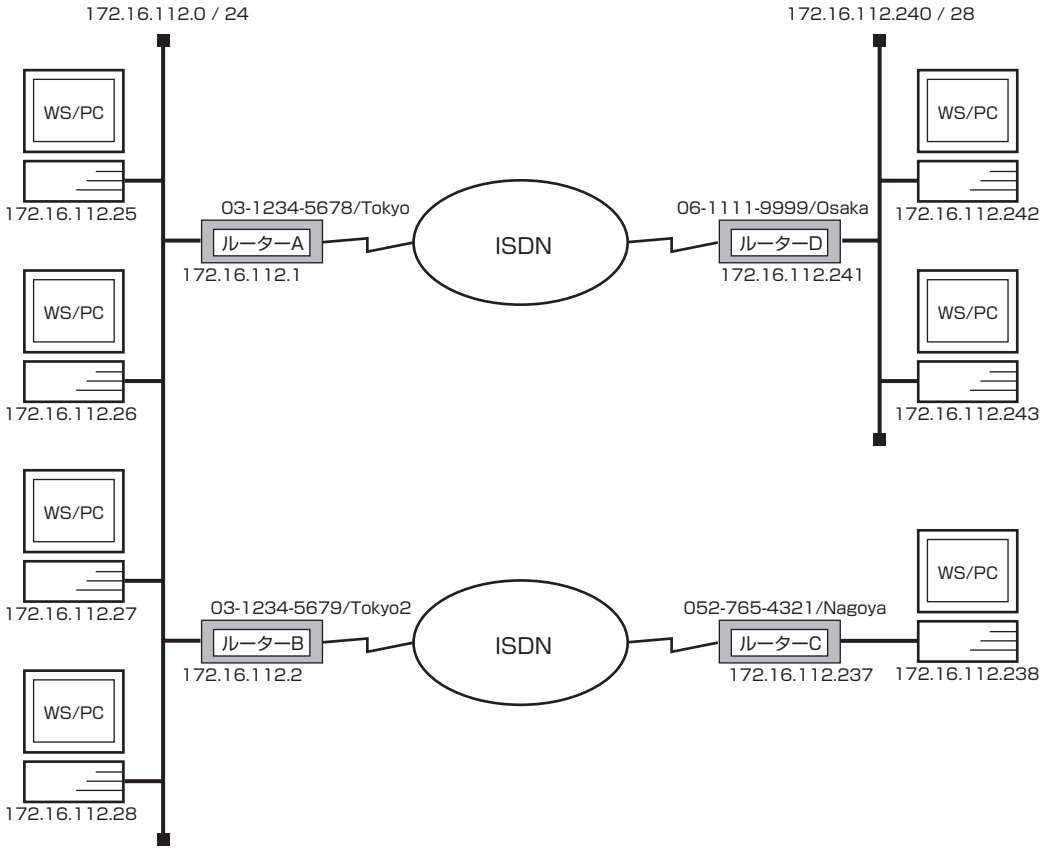
6. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、"/" に続けて入力します。

7. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

8. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

2.12 Proxy ARP を使用して遠隔地の LAN を同一セグメントに見せる

[構成図]



[ルーター A の設定手順]

```
# isdn local address bri1 03-1234-5679/Tokyo
# ip lan1 address 172.16.112.1/24
# ip route 172.16.112.241 gateway pp 1
# ip route 172.16.112.242 gateway pp 1
# ip route 172.16.112.243 gateway pp 1
.
（ホストの数だけ同様に経路を設定します）
.
# ip route 172.16.112.254 gateway pp 2
# ip lan1 proxyarp on
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 06-1111-9999/Osaka
pp1# pp enable 1
pp1# save
```

[ルーター B の設定手順]

```
# isdn local address 03-1234-5679/Tokyo2
# ip lan1 address 172.16.112.2/24
# ip route 172.16.112.237 gateway pp 1
# Ip route 172.16.112.238 gateway pp 1
# ip lan1 proxyarp on
# pp select 1
pp1# isdn remote address call 052-765-4321/Nagoya
pp1# pp bind bri1
pp1# pp enable 1
pp1# save
```

[ルーター C の設定手順]

```
# isdn local address bri1 052-765-4321/Nagoya
# ip lan1 address 172.16.112.237/30
# ip route default gateway pp 1
# pp select 1
# pp bind bri1
pp1# isdn remote address call 03-1234-5679/Tokyo2
pp1# pp enable 1
pp1# save
```

[ルーター D の設定手順]

```
# isdn local address 06-1111-9999/Osaka
# ip lan1 address 172.16.112.241/28
# ip route default gateway pp 1
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 03-1234-5678/Tokyo
pp1# pp enable 1
pp1# save
```

[解説]

ネットワーク 172.16.112.0 と、その一部分の IP アドレスを持つネットワークを Proxy ARP を使用して接続するための設定を説明します。

構成図における IP アドレスの割り当ては以下の表のような関係になります。

IP アドレス	割り当て
172.16.112.0	ネットワーク
172.16.112.1	ルーター A
172.16.112.2	ルーター B
172.16.112.3 : 172.16.112.235	ホスト (233 台分)
172.16.112.236 : 172.16.112.239	ルーター C の ネットワーク
172.16.112.240 : 172.16.112.254	ルーター D の ネットワーク
172.16.112.255	ブロードキャスト

IP アドレス	割り当て
172.16.112.236	ネットワーク
172.16.112.237	ルーター C
172.16.112.238	ホスト (1 台分)
172.16.112.239	ブロードキャスト

IP アドレス	割り当て
172.16.112.240	ネットワーク
172.16.112.241	ルーター D
172.16.112.242 : 172.16.112.254	ホスト (13 台分)
172.16.112.255	ブロードキャスト

ルーター A とルーター B は Proxy ARP を使用して、それぞれルーター D とルーター C の LAN との通信を行います。ルーター C とルーター D の LAN 上のホストからのパケットはデフォルトルートを設定してそれぞれルーター B 、ルーター A に向けておきます。
なお、ルーター C のネットワークには表の中に示したように 1 台のホストが接続でき、ルーター D のネットワークには 13 台のホストだけが接続できます。

■ルーター A およびルーター B

1. **isdn local address** コマンドを使用して、ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **ip lan1 proxyarp** コマンドを使用して、LAN 側に Proxy ARP を返すように設定します。

4. **ip route** コマンドを使用して、相手側ルーターが接続しているネットワークへのスタティックルーティング情報を設定します。通常のネットルートではなくホストルートである点に注意してください。例えば、ルーター A において ip route 172.16.112.240/28 gateway pp 1 のようにネットルートに設定すると、172.16.112.255 というブロードキャストパケットまでルーター D に流れることになります。

5. **pp select** コマンドを使用して、相手先情報番号を選択します。

6. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

7. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

8. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

9. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

■ルーター C およびルーター D

1. **isdn local address** コマンドを使用して、ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/”に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **ip route** コマンドを使用して、相手側ルーターが接続しているネットワーク へのデフォルトルートを設定します。

4. **pp select** コマンドを使用して、相手先情報番号を選択します。

5. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

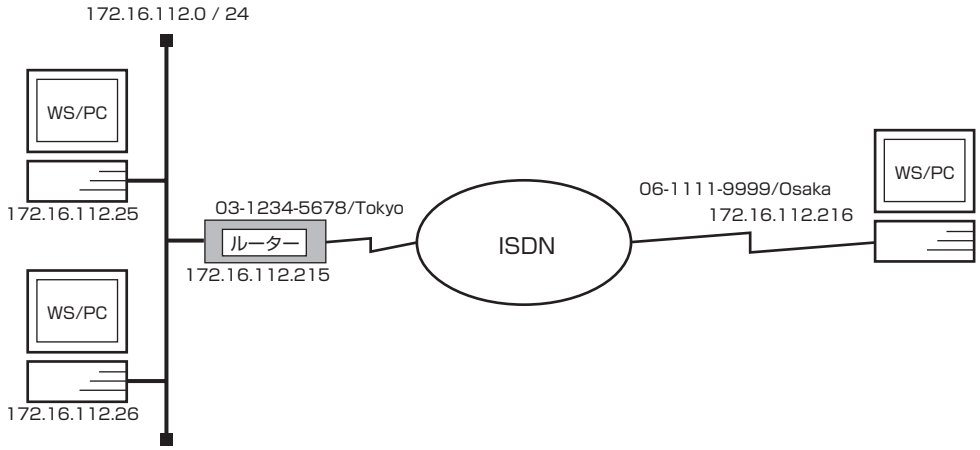
6. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/”に続けて入力します。

7. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

8. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

2.13 端末型機器（TA、ISDN ボード等）との接続

［構成図］



［手順］

```
# isdn local address bri1 03-1234-5678/Tokyo
# ip lan1 address 172.16.112.215/24
# ip lan1 proxyarp on
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 06-1111-9999/Osaka
pp1# ip pp remote address 172.16.112.216
pp1# pp enable 1
pp1# save
```

［解説］

ネットワーク 172.16.112.0 と、端末型機器（TA、ISDN ボード等）などを搭載したパーソナルコンピュータやワークステーションを ISDN 回線で接続するための設定を説明します。

PP 側に IP アドレスを設定していますので、コマンドによる経路情報の設定は必要ありません。
なお、ルーターの方から PPP により、相手のパーソナルコンピュータやワークステーションの IP アドレスを割り当てますので、相手側では IP アドレスを設定する必要はありません。もし、相手側の IP アドレスを相手側にて設定するような場合には **ip pp remote address** コマンドでその IP アドレスを設定してください。

1. **isdn local address** コマンドを使用して、ISDN 番号を設定します 。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **ip lan1 proxyarp** コマンドを使用して、LAN 側に Proxy ARP を返すように設定します。

4. **pp select** コマンドを使用して、相手先情報番号を選択します。

5. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

6. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、"/" に続けて入力します。

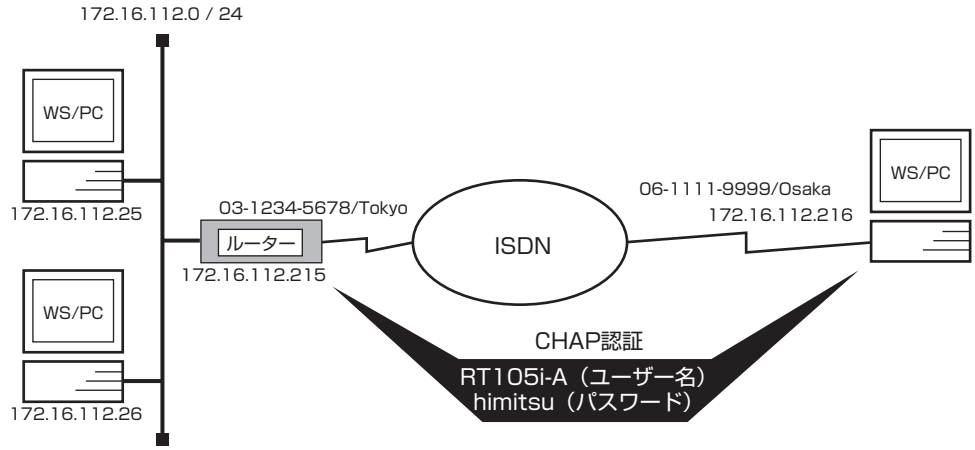
7. **ip pp remote address** コマンドを使用して、選択した PP 側のリモート IP アドレスを設定します。パーソナルコンピュータやワークステーションの方で設定されていればその IP アドレスを設定します。

8. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

9. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

2.14 端末型機器（TA、ISDN ボード等）との接続 (相手は不特定)

[構成図]



[ルーターの設定手順]

```
# isdn local address bri1 03-1234-5678/Tokyo
# ip lan1 address 172.16.112.215/24
# ip lan1 proxyarp on
# pp select anonymous
anonymous# pp bind bri1
anonymous# ip pp remote address pool 172.16.112.216 172.16.112.217
anonymous# pp auth request chap
anonymous# pp auth username RT105i-A himitsu
anonymous# pp enable anonymous
anonymous# save
```

[解説]

ネットワーク 172.16.112.0 と、端末型機器（TA、ISDN ボード等）などを搭載したパーソナルコンピュータやワークステーションに anonymous 扱いで ISDN 回線で接続するための設定を説明します。

PP 側に IP アドレスを設定していますので、コマンドによる経路情報の設定は必要ありません。
なお、ヤマハリモートルーターの方から PPP により、相手のパーソナルコンピュータやワークステーションの IP アドレスを割り当てますので、相手側では IP アドレスを設定する必要はありません。
不特定の相手と接続するので、セキュリティを考慮して CHAP 認証を行います。例として、相手側でのユーザ ID は“RT105i-A”、パスワードは“himitsu”としています。

1. **isdn local address** コマンドを使用して、ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/”に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **ip lan1 proxyarp** コマンドを使用して、LAN 側に Proxy ARP を返すように設定します。

4. **pp select** コマンドを使用して、相手先情報番号を選択します。

5. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

6. **ip pp remote address pool** コマンドを使用して、anonymous に対するリモート IP アドレスを設定します。

7. **pp auth request** コマンドを使用して、PPP の認証として CHAP を使用するように設定します。

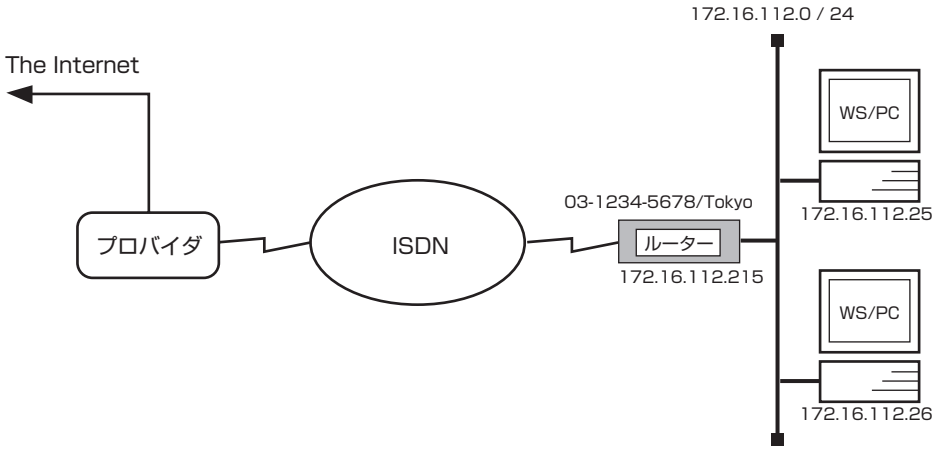
8. **pp auth username** コマンドを使用して、CHAP のユーザ名とパスワードを設定します。

9. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

10. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

2.15 IP マスカレード 機能による端末型ダイヤルアップ IP 接続

[構成図]



[手順]

```
# isdn local address bri1 03-1234-5678/Tokyo
# ip lan1 address 172.16.112.215/24
# ip route default gateway pp 1
# nat descriptor type 1 masquerade
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 06-1111-9999/Osaka
pp1# pp auth accept pap chap
pp1# pp auth myname RT105i-A himitsu
pp1# ppp ipcp ipaddress on
pp1# ip pp nat descriptor 1
pp1# pp enable 1
pp1# save
```

[解説]

ネットワーク 172.16.112.0 を、端末型ダイヤルアップ IP 接続でインターネット接続するための設定を説明します。

相手の商用プロバイダとの IP アドレスは、IPCP によるネゴシエーションをするように設定しておきます。
接続時の認証は PAP 、CHAP のどちらの認証でも受け付けるようにします。例として、相手側でのユーザ ID は“RT105i-A”、パスワードは“himitsu”としています。

また、IP マスカレード 機能を使用することにより、こちら側のプライベートアドレス空間の IP アドレスを変更することなく複数台の端末がインターネット接続できるようにします。

プロバイダ側に設置するルーターの設定例は 2.13 あるいは 2.14 のようになりますが、それに加えてデフォルトルートの設定が必要です。
例えばプロバイダ側の LAN 上にデフォルトゲートウェイがあり、その IP アドレスが 172.16.112.129 である場合には、ip route default gateway 172.16.112.129 という設定が、プロバイダ側に設置するルーターの設定に必要となります。

1. **isdn local address** コマンドを使用して、ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/”に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **ip route** コマンドを使用して、相手側ルーターが接続しているネットワークへのデフォルトルートを設定します。

4. **nat descriptor type** コマンドを使用して、NAT 変換のタイプを masquerade に指定します。

5. **pp select** コマンドを使用して、相手先情報番号を選択します。

6. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

7. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/”に続けて入力します。

8. **pp auth accept** コマンドを使用して、PPP の認証として PAP または CHAP を使用するように設定します。

9. **pp auth myname** コマンドを使用して、PAP または CHAP のユーザ名とパスワードを設定します。

10. **ppp ipcp ipaddress** コマンドを使用して、相手側の回線インタフェースの IP アドレスを取得できるようにします。

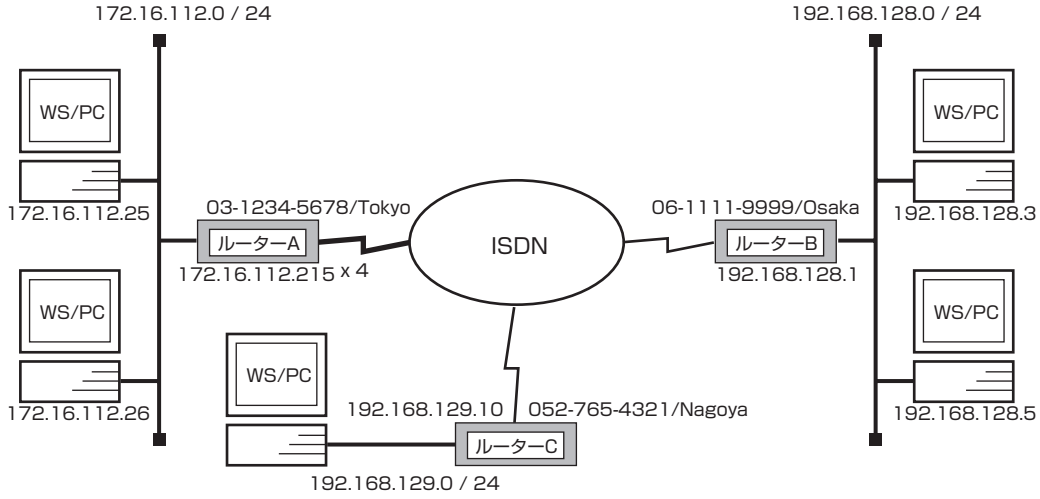
11. **ip pp nat descriptor** コマンドを使用して、4. で設定した NAT 変換を pp1 に適用します。

12. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

13. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

2.16 ISDN回線で代表番号を使って LAN を接続

［構成図］



[ルーター A の設定手順]

```
# isdn local address bri2.1 0312345678/Tokyo
# isdn local address bri2.2 0312345678/Tokyo
# isdn local address bri2.3 0312345678/Tokyo
# isdn local address bri2.4 0312345678/Tokyo
# ip lan1 address 172.16.112.215/24
# pp select anonymous
anonymous# pp bind bri2.1 bri2.2 bri2.3 bri2.4
anonymous# pp auth request chap-pap
anonymous# pp auth username Nagoya naisyo 0527654321/Nagoya
anonymous# pp auth username Osaka himitsu 0611119999/Osaka
anonymous# ip route 192.168.129.0/24 gateway pp anonymous name=Nagoya
anonymous# ip route 192.168.128.0/24 gateway pp anonymous name=Osaka
anonymous# pp enable anonymous
anonymous# save
```

[ルーター B の設定手順]

```
# isdn local address bri1 0611119999/Osaka
# ip lan1 address 192.168.128.1/24
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 0312345678/Tokyo
pp1# pp auth accept pap chap
pp1# pp auth myname Osaka himitsu
pp1# ip route 172.16.112.0/24 gateway pp 1
pp1# pp enable 1
pp1# save
```

[ルーター C の設定手順]

```
# isdn local address bri1 0527654321/Nagoya
# ip lan1 address 192.168.129.10/24
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 0312345678/Tokyo
pp1# pp auth accept pap chap
pp1# pp auth myname Nagoya naisyo
pp1# ip route 172.16.112.0/24 gateway pp 1
pp1# pp enable 1
pp1# save
```

[解説]

センタ側に複数 BRI モデル を設置し、ISDN 回線 4 回線で代表番号を組み、遠隔地のヤマハリモートルーターと BRI モデル により LAN を接続するための設定を説明します。

■ルーター A

1. **isdn local address** コマンドを使用して、接続した BRI 番号と ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/”に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **pp select** コマンドを使用して、相手先情報番号を選択します。

4. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。この設定例の場合、ISDN 4 回線が代表番号を組んでいますので、この 4 つの BRI ポートをバインドします。

5. **pp auth request** コマンドを使用して、要求する PPP の認証タイプを設定します。

6. **pp auth myname** コマンドを使用して、自分の名前とそのパスワードを設定します。

7. **pp auth username** コマンドを使用して、接続するネットワークの名前とそのパスワード、ISDN 番号を設定します。

8. **ip route** コマンドを使用して、名前によるルーティング情報を設定します。
これにより、**pp auth username** コマンドで設定した名前と ISDN 番号、ネットワークアドレスが相互に関係付けられます。

9. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

10. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

■ルーター B

1. **isdn local address** コマンドを使用して、ISDN 番号を設定します 。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/”に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **pp select** コマンドを使用して、相手先情報番号を選択します。

4. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

5. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/”に続けて入力します。

6. **pp auth accept** コマンドを使用して、受け入れる PPP の認証タイプを設定します。

7. **pp auth myname** コマンドを使用して、自分の名前とそのパスワードを設定します。

8. **ip route** コマンドを使用して、名前によるルーティング情報を設定します。

9. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

10. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

■ルーター C

1. **isdn local address** コマンドを使用して、ISDN 番号を設定します (モデルによっては **bri local address** コマンドになります) 。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **pp select** コマンドを使用して、相手先情報番号を選択します。

4. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

5. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

6. **pp auth accept** コマンドを使用して、受け入れる PPP の認証タイプを設定します。

7. **pp auth myname** コマンドを使用して、自分の名前とそのパスワードを設定します。

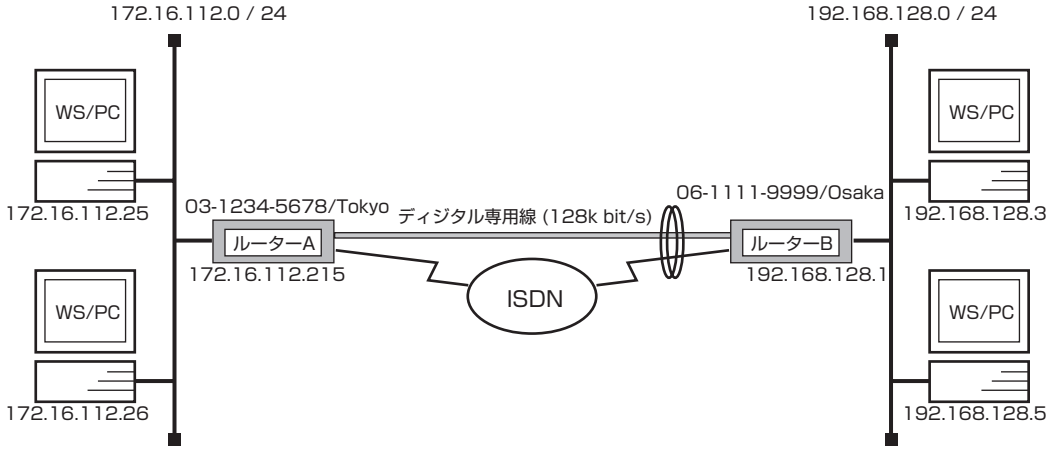
8. **ip route** コマンドを使用して、名前によるルーティング情報を設定します。

9. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

10. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

2.17 ISDN 回線と専用線を MP で接続

[構成図]



[ルーター A の設定手順]

```
# isdn local address bri2.1 0312345678/Tokyo
# line type bri3.1 l128
# isdn terminator bri3.1 on
# ip lan1 address 172.16.112.215/24
# pp select 1
pp1# pp bind bri2.1 bri3.1
pp1# ppp mp use on
pp1# ppp mp maxlink 3
pp1# isdn remote address call 0611119999/Osaka
pp1# ip route 192.168.128.0/24 gateway pp 1
pp1# pp keepalive use lcp-echo
pp1# pp enable 1
pp1# save
pp1# interface reset pp 1
```

[ルーター B の設定手順]

```
# isdn local address bri2.1 0611119999/Osaka
# line type bri3.1 l128
# isdn terminator bri3.1 on
# ip lan1 address 192.168.128.1/24
# pp select 1
pp1# pp bind bri2.1 bri3.1
pp1# ppp mp use on
pp1# ppp mp maxlink 3
pp1# isdn remote address call 0312345678/Tokyo
pp1# ip route 172.16.112.0/24 gateway pp 1
pp1# pp keepalive use lcp-echo
pp1# pp enable 1
pp1# save
pp1# interface reset pp 1
```

[解説]
ネットワーク 172.16.112.0 とネットワーク 192.168.128.0 を 128kbit/s のディジタル専用線と ISDN 回線の MP で接続するための設定を説明します。

ディジタル専用線のトラフィックに応じて、ISDN 回線を接続 / 切断します。ISDN 回線と接続するかどうかの閾値は **ppp mp load threshold** コマンドの設定で決まります。デフォルトでは、この例の場合、ディジタル専用線の負荷が 70% を越えた時に ISDN 回線を接続し、負荷が 30% を 2 回下回った時に切断されることになります。

2 台の複数 BRI モデルの設定手順は全く同じで、ISDN 番号や IP アドレスなどのコマンドのパラメータだけが異なります。

1. **isdn local address** コマンドを使用して、接続した BRI 番号と ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、"/" に続けて入力します。

2. **line type** コマンドを使用して、回線種別を 128kbit/s ディジタル専用線に指定します。

3. 終端抵抗無しのローゼットや DSU に直結する場合は、**isdn terminator** コマンドを使用して終端抵抗を on にします。そうでない場合にはこのコマンドは不要です。

4. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

5. **pp select** コマンドを使用して、相手先情報番号を選択します。

6. **ppp mp use** コマンドを使用して、MP を使用できるように設定します。

7. **ppp mp maxlink** コマンドを使用して、MP の最大リンク数を設定します。
この設定の場合、専用線と ISDN の 2B チャネルの合計 3 本のリンクを MP でコントロールすることになります。

8. **pp bind** コマンドを使用して、選択されている相手先情報番号と BRI 番号をバインドします。

9. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、"/" に続けて入力します。

10. **ip route** コマンドを使用して、相手側ルーターが接続している LAN へのスタティックルーティング情報を設定します。

11. **pp keepalive use** コマンドを使用して、専用線キープアライブを使用するように設定します。

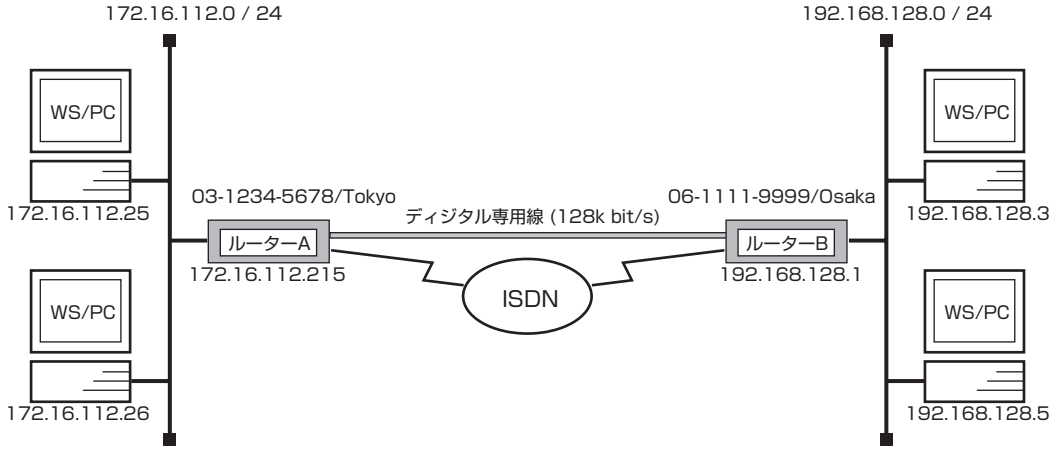
12. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

13. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

14. 回線種別がデフォルトと異なるので、リセットしてハードウェアを切替えます。**restart** コマンドによる装置全体の再起動でもかまいません。MP を使用しているインタフェースに関しては **interface reset** *interface* コマンドではなく **interface reset pp** コマンドを使用します。

2.18 専用線を ISDN 回線でバックアップ

[構成図]



[ルーター A の設定手順]

```
# isdn local address bri2.1 0312345678/Tokyo
# line type bri3.1 l128
# isdn terminator bri3.1 on
# ip lan1 address 172.16.112.215/24
# pp select 1
pp1# pp bind bri3.1
pp1# ip route 192.168.128.0/24 gateway pp 1
pp1# pp keepalive use lcp-echo
pp1# leased backup 2
pp1# pp enable 1
pp1# pp select 2
pp2# pp bind bri2.1
pp2# isdn remote address call 0611119999/Osaka
pp2# isdn call block time 15
pp2# pp enable 2
pp2# save
pp2# interface reset bri3.1
```

[ルーター B の設定手順]

```
# isdn local address bri2.1 0611119999/Osaka
# line type bri3.1 l128
# isdn terminator bri3.1 on
# ip lan1 address 192.168.128.1/24
# pp select 1
pp1# pp bind bri3.1
pp1# ip route 172.16.112.0/24 gateway pp 1
pp1# pp keepalive use lcp-echo
pp1# leased backup 2
pp1# pp enable 1
pp1# pp select 2
pp2# pp bind bri2.1
pp2# isdn remote address call 0312345678/Tokyo
pp2# isdn call block time 15
pp2# pp enable 2
pp2# save
pp2# interface reset bri3.1
```

[解説]

ネットワーク 172.16.112.0 とネットワーク 192.168.128.0 を 128kbit/s のディジタル専用線で接続し、この専用線がダウンした時は ISDN 回線でバックアップするための設定を説明します。

2 台の複数 BRI モデルの設定手順は全く同じで、ISDN 番号や IP アドレスなどのコマンドのパラメータだけが異なります。

1. **isdn local address** コマンドを使用して、接続した BRI 番号と ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、"/" に続けて入力します。

2. **line type** コマンドを使用して、回線種別を 128kbit/s ディジタル専用線に指定します。

3. 終端抵抗無しのローゼットや DSU に直結する場合は、**isdn terminator** コマンドを使用して終端抵抗を on にします。そうでない場合にはこのコマンドは不要です。

4. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

5. **pp select** コマンドを使用して、相手先情報番号を選択します。

6. **pp bind** コマンドを使用して、選択されている相手先情報番号と BRI 番号をバインドします。

7. **ip route** コマンドを使用して、相手側ルーターが接続している LAN へのスタティックルーティング情報を設定します。

8. **pp keepalive use** コマンドを使用して、専用線キープアライブを使用するように設定します。

9. **leased backup** コマンドを使用して、バックアップする際の相手先情報番号を指定します。

10. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

11. **pp select** コマンドを使用して、相手先情報番号を選択します。

12. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

13. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、"/" に続けて入力します。

14. **isdn call block time** コマンドを使用して、ISDN 回線への再発信抑制タイマを設定します。
このコマンドは必須ではありませんが、専用線ダウンの検出タイミングが双方のルーターで異なった場合に起こる無駄な発信を抑えられる場合があります。

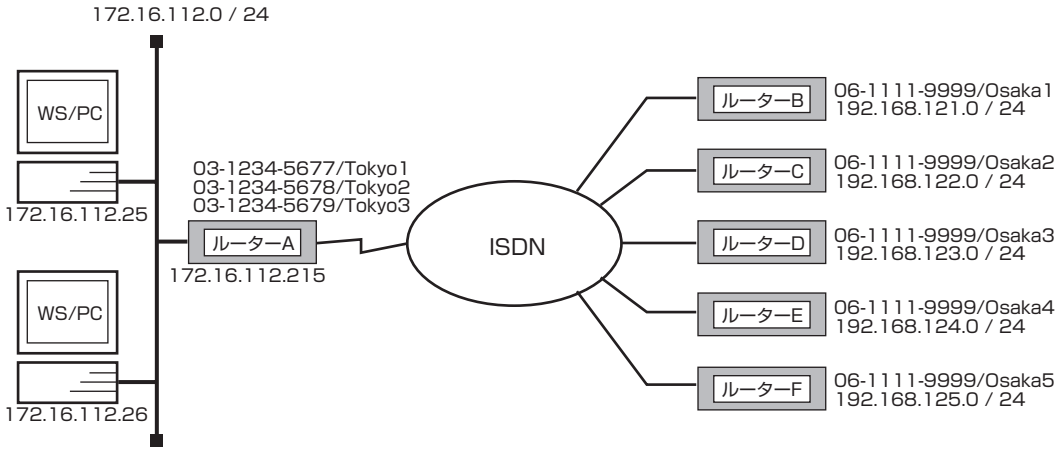
15. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

16. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

17. **interface reset** コマンドを使って回線種別の変更されたポートをリセットします。個々のポートをリセットする代わり **restart** コマンドを使って、ルーターを再起動させても回線種別は切り替わります。

2.19 ISDN3 回線で 5 対地の LAN を接続

[構成図]



[設定手順]

```
# isdn local address bri2.1 0312345677/Tokyo1
# isdn local address bri2.2 0312345678/Tokyo2
# isdn local address bri2.3 0312345679/Tokyo3
# ip lan1 address 172.16.112.215/24
# ip route 192.168.121.0/24 gateway pp 1
# ip route 192.168.122.0/24 gateway pp 2
# ip route 192.168.123.0/24 gateway pp 3
# ip route 192.168.124.0/24 gateway pp 4
# ip route 192.168.125.0/24 gateway pp 5
# pp select 1
pp1# pp bind bri2.1
pp1# isdn remote address call 0611119999/Osaka1
pp1# pp enable 1
pp1# pp select 2
pp2# pp bind bri2.1
pp2# isdn remote address call 0611118888/Osaka2
pp2# pp enable 2
pp2# pp select 3
pp3# pp bind bri2.2
pp3# isdn remote address call 0611117777/Osaka3
pp3# pp enable 3
pp3# pp select 4
pp4# pp bind bri2.2
pp4# isdn remote address call 0611116666/Osaka4
pp4# pp enable 4
pp4# pp select 5
pp5# pp bind bri2.3
pp5# isdn remote address call 0611115555/Osaka5
pp5# pp enable 5
pp5# save
```

[解説]

センタ側にルーターを設置し、遠隔地の 5 地点のヤマハリモートルーターの LAN を接続するための設定を説明します。
5 地点と同時に通信することが必要でない場合には、必ずしも ISDN 回線は 3 回線必要ではありません。その場合、3 地点以上の PP で同一の BRI 番号がバインドされることになります。

なお、ヤマハリモートルーター側の設定については、本章前半を参考にしてください。

1. **isdn local address** コマンドを使用して、接続した BRI 番号と ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、"/" に続けて入力します。
   この設定の場合、各ヤマハリモートルーター毎に B チャネル 1 本を割り当てますので、最低 5 本の B チャネルを確保するための 3 回線が必要となります。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **pp select** コマンドを使用して、相手先情報番号を選択します。

4. **pp bind** コマンドを使用して、選択されている相手先情報番号と BRI 番号をバインドします。
   この設定の場合、各ヤマハリモートルーター毎に B チャネル 1 本を割り当てますので、各 BRI ポートは 1 ～ 2 地点でバインドされます。

5. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、"/" に続けて入力します。
   * センタ側から発信しない場合には、**isdn call permit off**　を入力した上で、**isdn remote address arrive** を用います。

6. **ip route** コマンドを使用して、相手側ヤマハリモートルーターが接続している LAN へのスタティックルーティング情報を設定します。

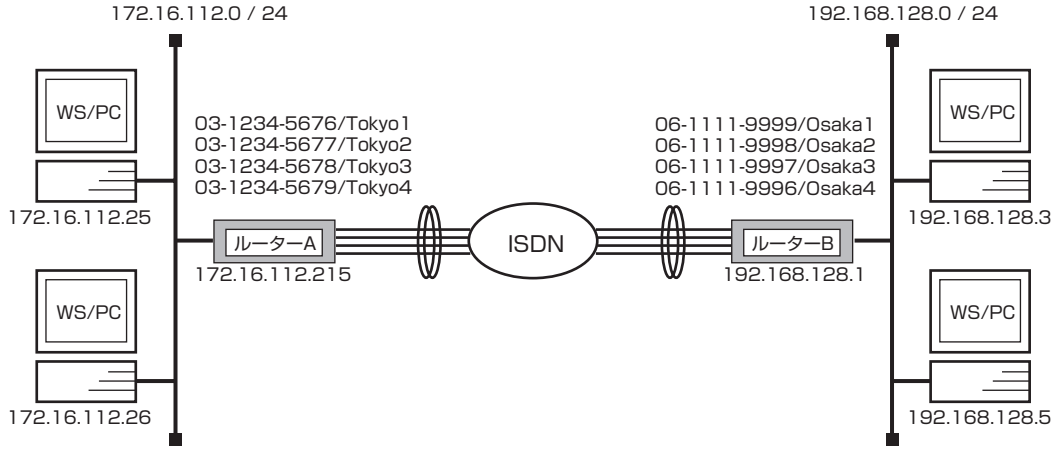
7. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

8. 他の 4 地点についても同様に設定します。

9. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

2.20 ISDN4 回線ずつを MP で接続

[構成図]



[ルーター A の設定手順]

```
# isdn local address bri2.1 0312345676/Tokyo1
# isdn local address bri2.2 0312345677/Tokyo2
# isdn local address bri2.3 0312345678/Tokyo3
# isdn local address bri2.4 0312345679/Tokyo4
# ip lan1 address 172.16.112.215/24
# pp select 1
pp1# pp bind bri2.1 bri2.2 bri2.3 bri2.4
pp1# ppp mp use on
pp1# ppp mp maxlink 8
pp1# isdn remote address call 0611119999/Osaka1 0611119998/Osaka2
     0611119997/Osaka3 0611119996/Osaka4
pp1# ip route 192.168.128.0/24 gateway pp 1
pp1# pp enable 1
pp1# save
```

[ルーター B の設定手順]

```
# isdn local address bri2.1 0611119999/Osaka1
# isdn local address bri2.2 0611119998/Osaka2
# isdn local address bri2.3 0611119997/Osaka3
# isdn local address bri2.4 0611119996/Osaka4
# ip lan1 address 192.168.128.1/24
# pp select 1
pp1# pp bind bri2.1 bri2.2 bri2.3 bri2.4
pp1# ppp mp use on
pp1# ppp mp maxlink 8
pp1# isdn remote address call 0312345676/Tokyo1 0312345677/Tokyo2
     0312345678/Tokyo3 0312345679/Tokyo4
pp1# ip route 172.16.112.0/24 gateway pp 1
pp1# pp enable 1
pp1# save
```

[解説]

ネットワーク 172.16.112.0 とネットワーク 192.168.128.0 を 4 回線 (最大 B チャネル 8 本) の MP で接続するための設定を説明します。

トラフィックに応じて、2 本目以降の ISDN 回線が接続されたり切断されたりします。接続するかどうかの閾値は **ppp mp load threshold** コマンドの設定で決まります。デフォルトでは、この例の場合、1 本目の回線の 1 本目の B チャネルの負荷が 70% を超えた時に 2 本目の B チャネルが接続し、さらにそれらでの負荷が 70% を超えると 2 本目の回線が接続します。このように、最大 4 本の回線で B チャネル 8 本での接続まで可能とします。負荷が 30% を 2 回下回る毎に、チャネルおよび回線は逆の順で切断されていくことになります。

2 台の複数 BRI モデルの設定手順は全く同じで、ISDN 番号や IP アドレスなどのコマンドのパラメータだけが異なります。

1. **isdn local address** コマンドを使用して、接続した BRI 番号と ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。
   この設定の場合、B チャネルが 8 本、回線にして 4 本が必要となります。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **pp select** コマンドを使用して、相手先情報番号を選択します。

4. **ppp mp use** コマンドを使用して、MP を使用できるように設定します。

5. **ppp mp maxlink** コマンドを使用して、MP の最大リンク数を設定します。この設定の場合、B チャネル 8 本のリンクを MP でコントロールすることになります。

6. **pp bind** コマンドを使用して、選択されている相手先情報番号と BRI 番号をバインドします。

7. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

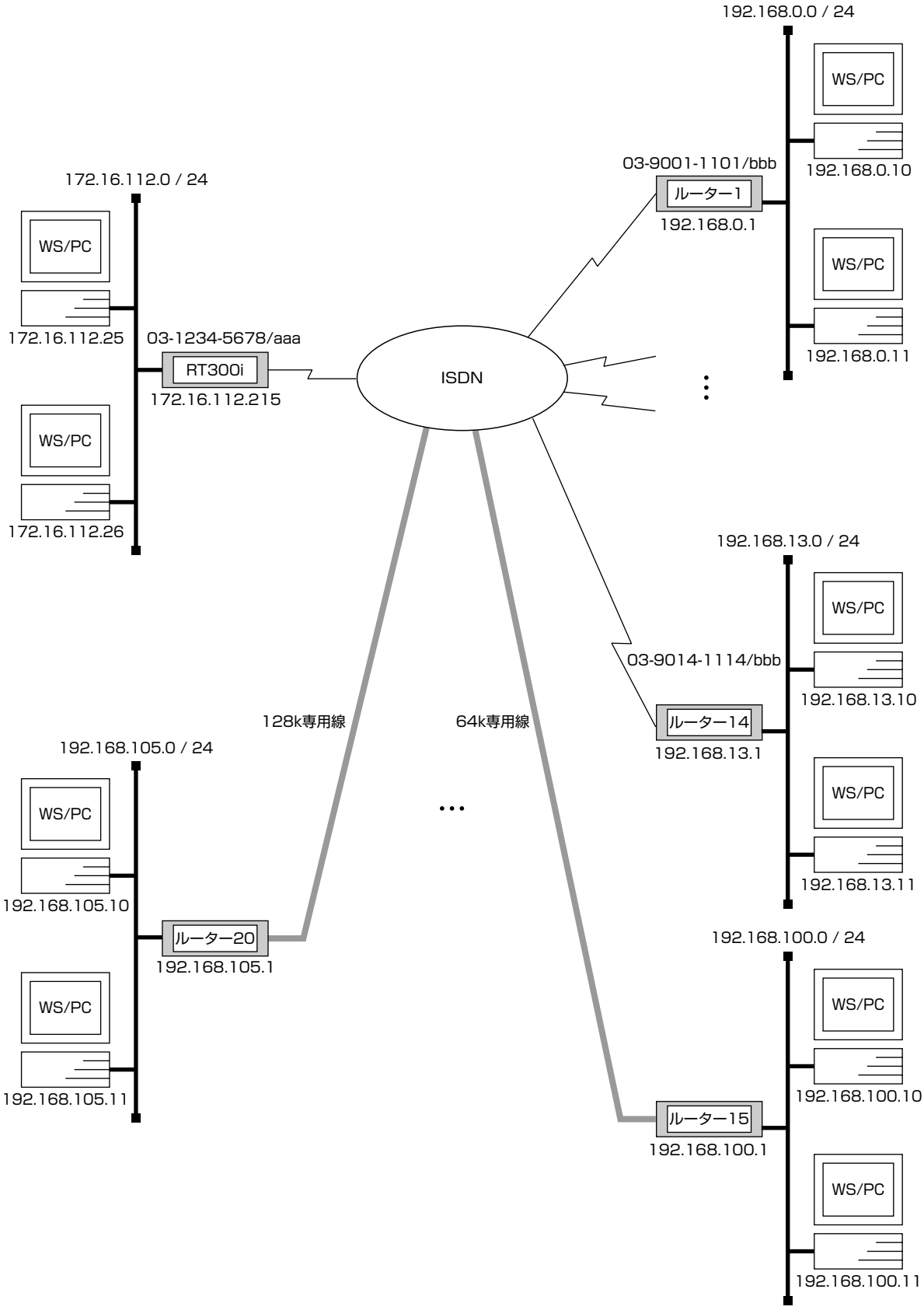
8. **ip route** コマンドを使用して、相手側ヤマハリモートルーターが接続している LAN へのスタティックルーティング情報を設定します。

9. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

10. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

2.21 ISDN 回線と専用線で 20ヶ所の LAN を接続 (RT300i)

［構成図］



[構成例]

ルーター	ネットワークアドレス	回線種別	ISDN 番号	ISDN サブアドレス
RT300i	172.16.112.0/24	ISDN/ 64k 専用線 / 128k 専用線	03-1234-5678	aaa
ルーター 1	192.168.0.0/24	ISDN	03-9001-1101	bbb
ルーター 2	192.168.1.0/24	ISDN	03-9002-1102	bbb
ルーター 3	192.168.2.0/24	ISDN	03-9003-1103	bbb
ルーター 4	192.168.3.0/24	ISDN	03-9004-1104	bbb
ルーター 5	192.168.4.0/24	ISDN	03-9005-1105	bbb
ルーター 6	192.168.5.0/24	ISDN	03-9006-1106	bbb
ルーター 7	192.168.6.0/24	ISDN	03-9007-1107	bbb
ルーター 8	192.168.7.0/24	ISDN	03-9008-1108	bbb
ルーター 9	192.168.8.0/24	ISDN	03-9009-1109	bbb
ルーター 10	192.168.9.0/24	ISDN	03-9010-1110	bbb
ルーター 11	192.168.10.0/24	ISDN	03-9011-1111	bbb
ルーター 12	192.168.11.0/24	ISDN	03-9012-1112	bbb
ルーター 13	192.168.12.0/24	ISDN	03-9013-1113	bbb
ルーター 14	192.168.13.0/24	ISDN	03-9014-1114	bbb
ルーター 15	192.168.100.0/24	64k 専用線		
ルーター 16	192.168.101.0/24	64k 専用線		
ルーター 17	192.168.102.0/24	64k 専用線		
ルーター 18	192.168.103.0/24	64k 専用線		
ルーター 19	192.168.104.0/24	128k 専用線		
ルーター 20	192.168.105.0/24	128k 専用線		

[ルーターの設定手順]

```
# line type bri2.8 l64
# line type bri3.1 l64
# line type bri3.2 l64
# line type bri3.3 l64
# line type bri3.4 l128
# line type bri3.5 l128
# isdn local address bri2.1 03-1234-5678/aaa
# isdn local address bri2.2 03-1234-5678/aaa
# isdn local address bri2.3 03-1234-5678/aaa
# isdn local address bri2.4 03-1234-5678/aaa
# isdn local address bri2.5 03-1234-5678/aaa
# isdn local address bri2.6 03-1234-5678/aaa
# isdn local address bri2.7 03-1234-5678/aaa
# ip lan1 address 172.16.112.215/24
# rip use on
# ip route 192.168.0.0/24 gateway pp 1
# ip route 192.168.1.0/24 gateway pp 2
# ip route 192.168.2.0/24 gateway pp 3
# ip route 192.168.3.0/24 gateway pp 4
# ip route 192.168.4.0/24 gateway pp 5
# ip route 192.168.5.0/24 gateway pp 6
# ip route 192.168.6.0/24 gateway pp 7
# ip route 192.168.7.0/24 gateway pp 8
# ip route 192.168.8.0/24 gateway pp 9
# ip route 192.168.9.0/24 gateway pp 10
# ip route 192.168.10.0/24 gateway pp 11
# ip route 192.168.11.0/24 gateway pp 12
# ip route 192.168.12.0/24 gateway pp 13
# ip route 192.168.13.0/24 gateway pp 14
```

```
# ip route 192.168.100.0/24 gateway pp 15
# ip route 192.168.101.0/24 gateway pp 16
# ip route 192.168.102.0/24 gateway pp 17
# ip route 192.168.103.0/24 gateway pp 18
# ip route 192.168.104.0/24 gateway pp 19
# ip route 192.168.105.0/24 gateway pp 20
# pp select 1
pp1# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp1# isdn remote address call 03-9001-1101/bbb
pp1# pp enable 1
pp1# pp select 2
pp2# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp2# isdn remote address call 03-9002-1102/bbb
pp2# pp enable 2
pp2# pp select 3
pp3# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp3# isdn remote address call 03-9003-1103/bbb
pp3# pp enable 3
pp3# pp select 4
pp4# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp4# isdn remote address call 03-9004-1104/bbb
pp4# pp enable 4
pp4# pp select 5
pp5# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp5# isdn remote address call 03-9005-1105/bbb
pp5# pp enable 5
pp5# pp select 6
pp6# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp6# isdn remote address call 03-9006-1106/bbb
pp6# pp enable 6
pp6# pp select 7
pp7# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp7# isdn remote address call 03-9007-1107/bbb
pp7# pp enable 7
pp7# pp select 8
pp8# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp8# isdn remote address call 03-9008-1108/bbb
pp8# pp enable 8
pp8# pp select 9
pp9# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp9# isdn remote address call 03-9009-1109/bbb
pp9# pp enable 9
pp9# pp select 10
pp10# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp10# isdn remote address call 03-9010-1110/bbb
pp10# pp enable 10
pp10# pp select 11
pp11# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp11# isdn remote address call 03-9011-1111/bbb
pp11# pp enable 11
pp11# pp select 12
pp12# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp12# isdn remote address call 03-9012-1112/bbb
pp12# pp enable 12
pp12# pp select 13
```

```
pp13# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp13# isdn remote address call 03-9013-1113/bbb
pp13# pp enable 13
pp13# pp select 14
pp14# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp14# isdn remote address call 03-9014-1114/bbb
pp14# pp enable 14
pp14# pp select 15
pp15# pp bind bri2.8
pp15# pp enable 15
pp15# pp select 16
pp16# pp bind bri3.1
pp16# pp enable 16
pp16# pp select 17
pp17# pp bind bri3.2
pp17# pp enable 17
pp17# pp select 18
pp18# pp bind bri3.3
pp18# pp enable 18
pp18# pp select 19
pp19# pp bind bri3.4
pp19# pp enable 19
pp19# pp select 20
pp20# pp bind bri3.5
pp20# pp enable 20
pp20# save
pp20# interface reset bri2.8
pp20# interface reset bri3.1
pp20# interface reset bri3.2
pp20# interface reset bri3.3
pp20# interface reset bri3.4
pp20# interface reset bri3.5
```

[解説]

ルーターの設置されている LAN と 14ヵ所の LAN を ISDN 回線、6ヵ所の LAN を専用線で接続します。RT300i 側の ISDN 番号は代表番号を用います。

RT300i の拡張スロット 1 に装着された BRI 拡張モジュール (YBA-8BRI-ST) の 1 から 7 ポートは ISDN 回線、8 ポート目は 64k 専用線、拡張スロット 2 に装着された BRI 拡張モジュール (YBA-8BRI-ST) の 1、2、3 ポートは 64k 専用線、4、5 ポートは 128k 専用線を用います。

拡張スロット 2 に装着された BRI 拡張モジュールの残り 3 ポートは使用しません。

LAN 側の経路情報には rip を用い、回線側の経路情報はコマンドで設定します。(スタティックルーティング)

1. **line type** コマンドを使って回線種別を設定します。設定していないポートはデフォルトの isdn のままです。

2. **isdn local address** コマンドを使って本機の ISDN 番号を設定します。ISDN 番号には代表番号を用いていますので、すべての BRI に同じ番号を設定しています。aaa はサブアドレスです。

3. **ip lan1 address** コマンドを使って LAN 側の IP アドレスとネットマスクを設定します。

4. **rip use** コマンドを使って rip を有効にします。

5. **ip route** コマンドを使って接続先の LAN への経路情報を設定します。

6. **pp select** コマンドを使って相手先情報番号を選択します。

7. **pp bind** コマンドを使って選択した相手先情報番号に BRI ポートをバインドします。

8. **isdn remote address** コマンドを使って選択した相手先の ISDN 番号を設定します。相手先のサブアドレスはすべて bbb です。専用線の場合にはこのコマンドは不要です。

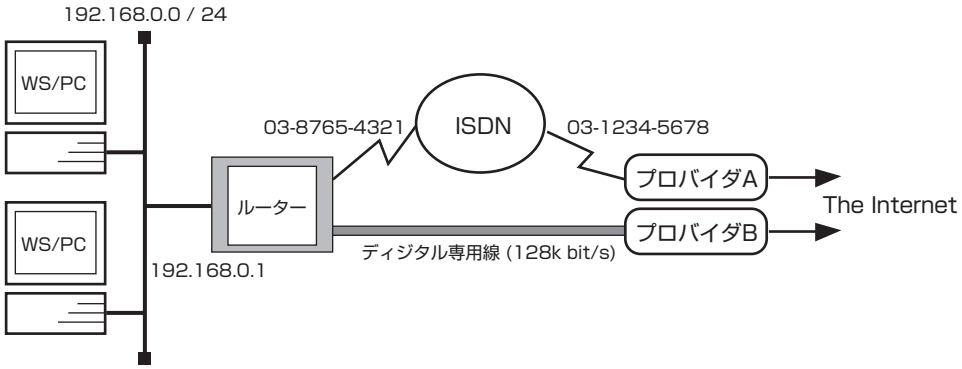
9. **pp enable** コマンドを使って PP 側のインタフェースを有効にします。このコマンドの実行直後にインタフェースは有効になります。

10. **save** コマンドを使って設定を内蔵の不揮発性メモリに書き込みます。

11. **interface reset** コマンドを使って回線種別の変更されたポートをリセットします。個々のポートをリセットする代わり **restart** コマンドを使って、ルーターを再起動させても回線種別は切り替わります。

2.22 専用線によるプロバイダネットワーク型接続を ISDN によるプロバイダ端末型接続でバックアップ

[構成図]



[設定手順]

```
# line type bri1 l128
# isdn local address bri2 0387654321
# ip lan1 address 192.168.0.1/24
# nat descriptor type 1 nat
# nat descriptor address outer 1 172.16.112.177-172.16.112.182
# nat descriptor type 2 masquerade
# pp select 1
pp1# pp bind bri1
pp1# pp backup pp 2
pp1# pp keepalive use lcp-echo
pp1# ip pp nat descriptor 1
pp1# ip route default gateway pp 1
pp1# pp enable 1
pp1# pp select 2
pp2# pp bind bri2
pp2# isdn remote address call 0312345678
pp2# pp auth accept chap
pp2# pp auth myname name pass
pp2# ppp ipcp ipaddress on
pp2# ppp ipcp msext on
pp2# ip pp nat descriptor 2
pp2# pp enable 2
pp2# save
```

[解説]

プロバイダ接続のバックアップを行います。専用線接続が何らかの原因で切れた場合に ISDN でプロバイダに接続します。プロバイダへの接続は専用線の場合がネットワーク型接続で NAT を使用し、ISDN の場合は端末型接続で IP マスカレードを使用します。

1. # line type bri1 l128
   # isdn local address bri2 0387654321
   各回線の情報を設定します。

2. # ip lan1 address 192.168.0.1/24
   LAN 側のアドレスを設定します。

3. # nat descriptor type 1 nat
   # nat descriptor address outer 1 172.16.112.177-172.16.112.182
   専用線接続時に使用する NAT を定義します。

4. # nat descriptor type 2 masquerade
   ISDN で接続する場合に使用する IP マスカレードを定義します。

5. # pp select 1
   pp1# pp bind bri1
   pp1# pp backup pp 2
   バックアップの pp を設定します。

6. pp1# pp keepalive use lcp-echo
   キープアライブによる切断検知を行うための設定です。専用線の場合には pp always-on コマンドは使用できません。

7. pp1# ip pp nat descriptor 1
   NAT を定義した NAT ディスクリプタを pp1 に適用します。

8. pp1# ip route default gateway pp 1
   pp1# pp enable 1
   デフォルト経路を設定します。バックアップに切り替わると経路情報もバックアップ先に引き継がれますので、バックアップ先に対して経路設定は不要です。

9. pp1# pp select 2
   pp2# pp bind bri2
   pp2# isdn remote address call 0312345678
   pp2# pp auth accept chap
   pp2# pp auth myname name pass
   pp2# ppp ipcp ipaddress on
   pp2# ppp ipcp msext on
   pp2# ip pp nat descriptor 2
   pp2# pp enable 2
   pp2# save
   pp2 に対して ISDN 経由のプロバイダ接続設定を行います。IP マスカレード機能を定義した NAT ディスクリプタを pp2 に適用します。バックアップ回線に切り替わった時にはこちらの NAT/ マスカレードテーブルが使われます。

3. IPX 設定例

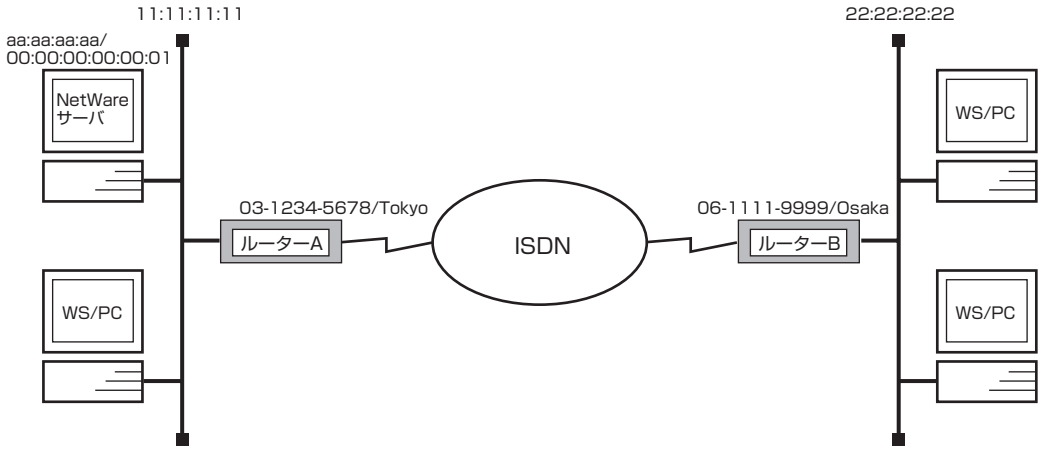
本章では、IPX ネットワークの基本的な接続形態を実現するための設定方法について、具体例を用いて説明します。セキュリティの設定や、詳細な各種パラメータなどの付加的な設定に関しては、個々のネットワークの運営方針などに基づいて行ってください。
本章で説明するネットワーク接続の形態は、次のようになります。

1. ISDN 回線で LAN を接続 (PP 側はスタティックルーティング)
2. ISDN 回線で LAN を接続 (双方にサーバがある場合)
3. 64kbit/s ディジタル専用線で LAN を接続 (PP 側はダイナミックルーティング)

以下の説明では、それぞれのネットワークの接続形態例に対して構成図、手順、解説の順に行います。

3.1　ISDN 回線で LAN を接続 (PP 側はスタティックルーティング)

[構成図]



[ルーター A の設定手順]

```
# ipx routing on
# isdn local address bri1 03-1234-5678/Tokyo
# ipx lan1 network 11:11:11:11
# pp select 1
pp1# pp bind bri1
pp1# ipx pp routing on
pp1# isdn remote address call 06-1111-9999/Osaka
pp1# ipx pp route 22:22:22:22 2
pp1# pp enable 1
pp1# save
```

[ルーター B の設定手順]

```
# ipx routing on
# isdn local address bri1 06-1111-9999/Osaka
# ipx lan1 network 22:22:22:22
# ipx sap add file SERVER aa:aa:aa:aa 00:00:00:00:00:01 ncp 3
# pp select 1
pp1# pp bind bri1
pp1# ipx pp routing on
pp1# isdn remote address call 03-1234-5678/Tokyo
pp1# ipx pp route 11:11:11:11 2
pp1# ipx pp route aa:aa:aa:aa 3
pp1# pp enable 1
pp1# save
```

[解説]

■ルーター A

1. **ipx routing** コマンドを使用して、IPX パケットのルーティングを可能にします。

2. **isdn local address** コマンドを使用して、ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

3. **ipx lan1 network** コマンドを使用して、LAN 側の IPX ネットワーク番号を設定します。

4. **pp select** コマンドを使用して、相手先情報番号を選択します。

5. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

6. **ipx pp routing** コマンドを使用して、PP 側へのルーティングを可能にします。

7. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

8. **ipx pp route** コマンドを使用して、相手側ヤマハリモートルーターが接続しているネットワーク への経路情報を設定します。

9. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

10. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

MEMO

ipx lan1 network コマンドで設定するLAN 側の IPX ネットワーク番号は、LAN 上のNetWare サーバにより決定されています。
NetWare サーバは SYSTEM ディレクトリ中の AUTOEXEC.NCF ファイルにある bind コマンドによりネットワークカードと IPX プロトコルをバインドしますが、そこで与える net パラメータが IPX ネットワーク番号のことです。

■ルーター B

1. **ipx routing** コマンドを使用して、IPX パケットのルーティングを可能にします。

2. **isdn local address** コマンドを使用して、ISDN 番号を設定します 。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

3. **ipx lan1 network** コマンドを使用して、LAN 側の IPX ネットワーク番号を設定します。

4. **ipx sap** コマンドを使用して、 NetWare サーバの SAP テーブル情報を設定します。

5. **pp select** コマンドを使用して、相手先情報番号を選択します。

6. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

7. **ipx pp routing** コマンドを使用して、PP 側へのルーティングを可能にします。

8. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

9. **ipx pp route** コマンドを使用して、相手側ヤマハリモートルーターが接続している LAN への経路情報を設定します。

10. **ipx pp route** コマンドを使用して、相手側ヤマハリモートルーターが接続している LAN 上のサーバへの経路情報を設定します。

11. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

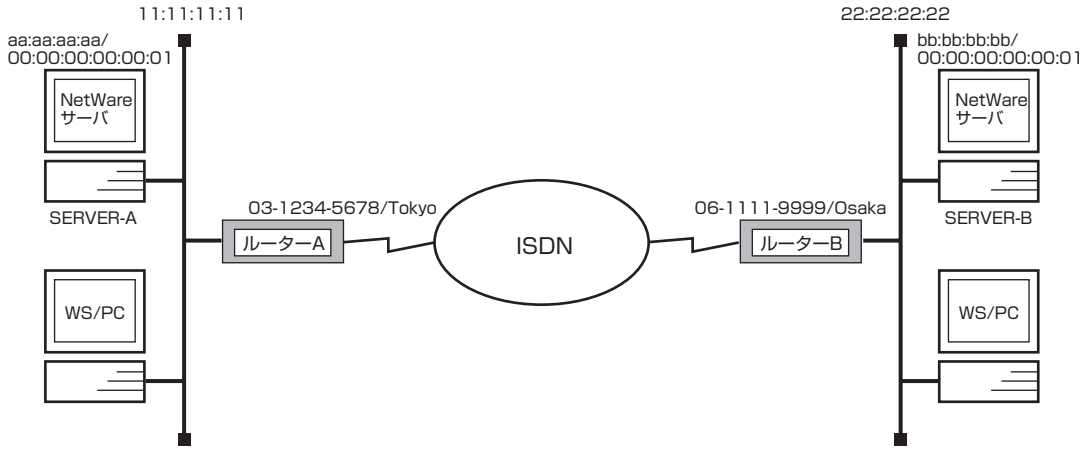
12. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

MEMO

ipx sap コマンドで設定する NetWare サーバの内部 IPX ネットワーク番号は、NetWare サーバの SYSTEM ディレクトリ中の AUTOEXEC.NCF ファイルにある **ipx internalnet** コマンドで設定されています。NetWare サーバの内部 IPX ノード番号は通常 **00:00:00:00:00:01** です。
また、ルーター A とは異なり、ルーター B 側には LAN 上に NetWare サーバがないので、**ipx lan1 network** コマンドで設定する LAN 側の IPX ネットワーク番号は他と重複しない範囲で自由に設定できます。

3.2　ISDN 回線で LAN を接続 (双方にサーバがある場合)

[構成図]



[ルーター A の設定手順]

```
# ipx routing on
# isdn local address bri1 03-1234-5678/Tokyo
# ipx lan1 network 11:11:11:11
# ipx sap file SERVER-B bb:bb:bb:bb: 00:00:00:00:00:01 ncp 3
# pp select 1
pp1# pp bind bri1
pp1# ipx pp routing on
pp1# isdn remote address call 06-1111-9999/Osaka
pp1# ipx pp route 22:22:22:22 2
pp1# ipx pp route bb:bb:bb:bb 3
pp1# pp enable 1
pp1# save
```

[ルーター B の設定手順]

```
# ipx routing on
# isdn local address bri1 06-1111-9999/Osaka
# ipx lan1 network 22:22:22:22
# ipx sap file SERVER-A aa:aa:aa:aa 00:00:00:00:00:01 ncp 3
# pp select 1
pp1# pp bind bri1
pp1# ipx pp routing on
pp1# isdn remote address call 03-1234-5678/Tokyo
pp1# ipx pp route 11:11:11:11 2
pp1# ipx pp route aa:aa:aa:aa 3
pp1# pp enable 1
pp1# save
```

［解説］

1. **ipx routing** コマンドを使用して、IPX パケットのルーティングを可能にします。

2. **isdn local address** コマンドを使用して、ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/”に続けて入力します。

3. **ipx lan1 network** コマンドを使用して、LAN 側の IPX ネットワーク番号を設定します。

4. **ipx sap** コマンドを使用して、NetWare サーバの SAP テーブル情報を設定します。

5. **pp select** コマンドを使用して、相手先情報番号を選択します。

6. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

7. **ipx pp routing** コマンドを使用して、PP 側へのルーティングを可能にします。

8. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/”に続けて入力します。

9. **ipx pp route** コマンドを使用して、相手側ヤマハリモートルーターが接続している LAN への経路情報を設定します。

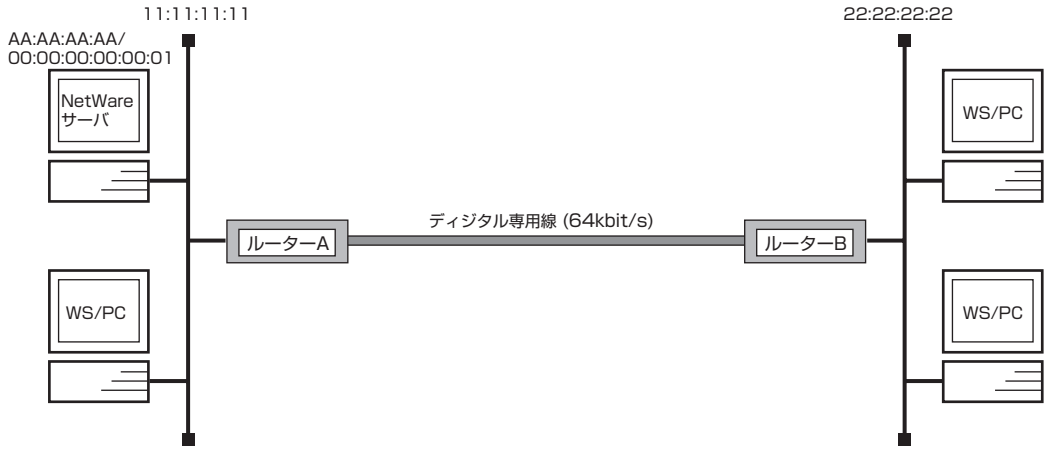
10. **ipx pp route** コマンドを使用して、相手側ヤマハリモートルーターが接続している LAN 上のサーバへの経路情報を設定します。

11. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

12. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

3.3　64kbit/s ディジタル専用線で LAN を接続 (PP 側はダイナミックルーティング)

[構成図]



[ルーター A の設定手順]

```
# line type bri1 l64
# ipx routing on
# ipx lan1 network 11:11:11:11
# pp select 1
pp1# pp bind bri1
pp1# ipx pp routing on
pp1# ipx pp ripsap connect send interval
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

[ルーター B の設定手順]

```
# line type bri1 l64
# ipx routing on
# ipx lan1 network 22:22:22:22
# pp select 1
pp1# pp bind bri1
pp1# ipx pp routing on
pp1# ipx pp ripsap connect send interval
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

［解説］

ルーター A にも B にもスタティックな経路情報を持たせずに RIP で通信を行います。

1. **line type** コマンドを使用して、回線種別を 64kbit/s ディジタル専用線に指定します。
2. **ipx routing** コマンドを使用して、IPX パケットのルーティングを可能にします。
3. **ipx lan1 network** コマンドを使用して、LAN 側の IPX ネットワーク番号を設定します。
4. **pp select** コマンドを使用して、相手先情報番号を選択します。
5. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。
6. **ipx pp routing** コマンドを使用して、PP 側へのルーティングを可能にします。
7. **ipx pp ripsap connect send** コマンドを使用して、回線接続時の RIP/SAP の送出を **ipx pp ripsap connect interval** コマンドで設定されている時間間隔で行うように設定します。
8. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。
9. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。
10. **interface reset** コマンドを使用して、回線のハードウェアを切替えます。この後、実際にパケットが流れるようになります。

4. ブリッジ設定例

本章では、ブリッジによる基本的な設定方法について、具体例を用いて説明します。セキュリティの設定や、詳細な各種パラメータなどの付加的な設定に関しては、個々のネットワークの運営方針などに基づいて行ってください。

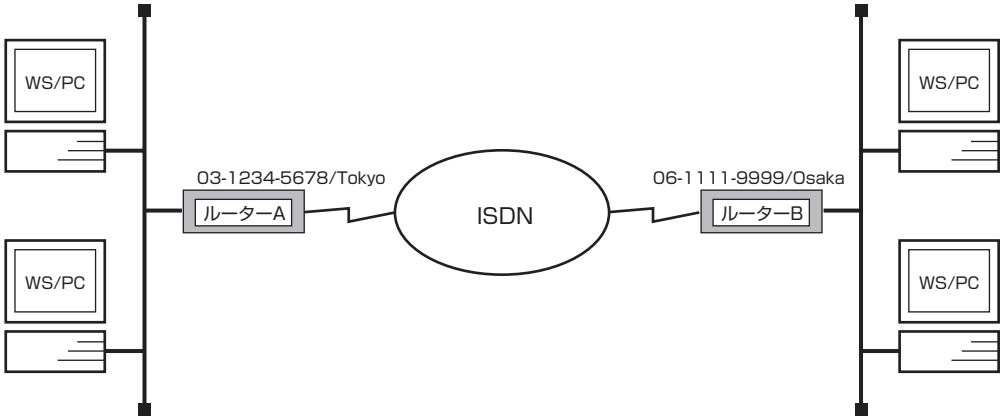
本章で説明するネットワーク接続の形態は、次のようになります。

1. ISDN 回線で LAN をブリッジ接続
2. 64kbit/s ディジタル専用線で LAN をブリッジ接続

以下の説明は、それぞれのネットワークの接続形態例に対して構成図、手順、解説の順に行います。

4.1　ISDN 回線で LAN をブリッジ接続

［構成図］



［ルーター A の設定手順］

```
# bridge use on
# isdn local address bri1 03-1234-5678/Tokyo
# bridge group lan1 1
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 06-1111-9999/Osaka
pp1# pp enable 1
pp1# save
```

［ルーター B の設定手順］

```
# bridge use on
# isdn local address bri1 06-1111-9999/Osaka
# bridge group lan1 1
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 03-1234-5678/Tokyo
pp1# pp enable 1
pp1# save
```

[解説]
ネットワーク同士を ISDN 回線でブリッジ接続するための設定を説明します。

この例では、IP パケットはブリッジングの対象とはなりません。IP パケットも同時にブリッジする場合には、**save** コマンド実行前に **ip routing off** コマンドを実行します。

2 台のルーターの設定手順は全く同じで、ISDN 番号を設定するコマンドのパラメータだけが異なります。

1. **bridge use** コマンドを使用して、ブリッジングを可能にします。

2. **isdn local address** コマンドを使用して、ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

3. **bridge group** コマンドを使用して、ブリッジするインタフェースを指定します。

4. **pp select** コマンドを使用して、相手先情報番号を選択します。

5. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

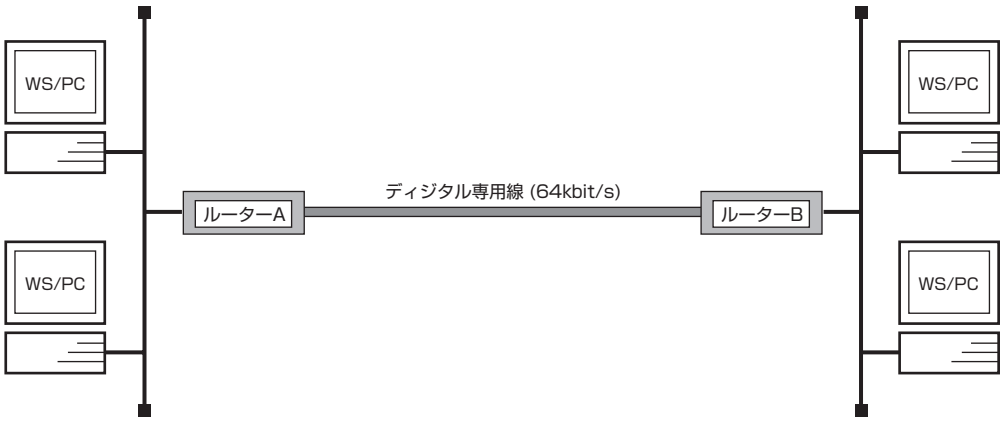
6. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

7. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

8. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

4.2　64kbit/s ディジタル専用線で LAN をブリッジ接続

[構成図]



[設定手順]

```
# line type bri1 l64
# bridge use on
# bridge group lan1 1
# pp select 1
pp1# pp bind bri1
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

[解説]

64kbit/s ディジタル専用線で結ばれたネットワーク同士をブリッジで接続するための設定を説明します。

この例では、IP パケットはブリッジングの対象とはなりません。IP パケットも同時にブリッジする場合には、**save** コマンド実行前に **ip routing off** コマンドを実行します。

2 台のルーターの設定手順は全く同じになります。

1. **line type** コマンドを使用して、回線種別を 64kbit/s ディジタル専用線に指定します 。
2. **bridge use** コマンドを使用して、ブリッジングを可能にします。
3. **bridge group** コマンドを使用して、ブリッジするインタフェースを指定します。
4. **pp select** コマンドを使用して、相手先情報番号を選択します。
5. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。
6. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。
7. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。
8. **interface reset** コマンドを使用して回線のハードウェアを切替えます。この後、実際にパケットが流れるようになります。

5. IP フィルタリング設定例

本章では、ネットワークのセキュリティ対策である IP パケットのフィルタリングの設定方法について、具体例を用いて説明します。

本章では次のようなフィルタリングの例を説明します。

1. 特定のネットワーク発のパケットだけを送信する
2. 特定のネットワーク着のパケットを送信しない
3. 特定のネットワーク発のパケットだけを受信する
4. 特定のネットワーク着のパケットを受信しない
5. Established のみ通信可能にする
6. SNMP のみ通信可能にする
7. 両方向で TELNET のみ通信可能にする
8. 外部からの PING コマンドを拒否する
9. 片方からの FTP のみ通信可能にする
10. RIP 使用時に特定のルーティング情報を通さない
11. インターネット接続し、外部からのアクセスを制限する (バリアセグメントあり)
12. インターネット接続し、外部からのアクセスを制限する (バリアセグメントなし)

以下の説明では、それぞれのフィルタリングに対して条件、手順、解説の順に行います。

5.1　特定のネットワーク発のパケットだけを送信する

[条件]

相手先情報番号が 1 の相手に対して、始点のネットワークアドレスが 192.168.128.0/24 となっているパケットだけを PP 側に送信する。

[設定手順]

```
# pp select 1
pp1# ip filter 1 pass 192.168.128.0/24 *
pp1# ip pp secure filter out 1
pp1# save
```

[解説]

1. **pp select** コマンドを使用して、相手先情報番号を選択します。

2. **ip filter** コマンドを使用してフィルタを定義します。
   始点 IP アドレスは 192.168.128.0/24 のみで、終点 IP アドレスは任意なので“*****”を指定します。

3. **ip pp secure filter** コマンドを使用して、相手先情報番号 1 の相手に対してフィルタをかけます。PP 側への出口でフィルタをかけるので“**out**”を指定します。

4. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

5.2　特定のネットワーク着のパケットを送信しない

[条件]

相手先情報番号が 1 の相手に対して、終点のネットワークアドレスが 192.168.128.0/24 となっているパケットを PP 側に送信しない。

[設定手順]

```
# pp select 1
pp1# ip filter 1 reject * 192.168.128.0/24
pp1# ip filter 2 pass * *
pp1# ip pp secure filter out 1 2
pp1# save
```

[解説]

1. **pp select** コマンドを使用して、相手先情報番号を選択します。

2. **ip filter** コマンドを使用してフィルタを定義します。
   始点 IP アドレスは任意なので“**`*`**”を指定し、終点 IP アドレスは 192.168.128.0/24 を指定します。“**`reject`**”のフィルタを定義する場合、条件に合わないその他のパケットもすべて捨てられるので、その他はすべて通すというフィルタの定義も必要です。

3. **ip pp secure filter** コマンドを使用して、相手先情報番号 1 の相手に対してフィルタをかけます。PP 側の出口でフィルタをかけるので“**`out`**”を指定します。また、フィルタは 1, 2 の順番でかけるように指定します。

4. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

5.3　特定のネットワーク発のパケットだけを受信する

[条件]

相手先情報番号が 1 の相手に対して、始点のネットワークアドレスが 192.168.128.0/24 となっているパケットだけを PP 側で受信する。

[設定手順]

```
# pp select 1
pp1# ip filter 1 pass 192.168.128.0/24 *
pp1# ip pp secure filter in 1
pp1# save
```

[解説]

1. **pp select** コマンドを使用して、相手先情報番号を選択します。

2. **ip filter** コマンドを使用してフィルタを定義します。
   始点 IP アドレスは 192.168.128.0/24 のみで、終点 IP アドレスは任意なので“*****”を指定します。

3. **ip pp secure filter** コマンドを使用して、相手先情報番号 1 の相手に対してフィルタをかけます。PP 側への入口でフィルタをかけるので“**in**”を指定します。

4. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

5.4　特定のネットワーク着のパケットを受信しない

[条件]

相手先情報番号が 1 の相手に対して、終点のネットワークアドレスが 192.168.128.0/24 となっているパケットを PP 側で受信しない。

[設定手順]

```
# pp select 1
pp1# ip filter 1 reject * 192.168.128.0/24
pp1# ip filter 2 pass * *
pp1# ip pp secure filter in 1 2
pp1# save
```

[解説]

1. **pp select** コマンドを使用して、相手先情報番号を選択します。

2. **ip filter** コマンドを使用してフィルタを定義します。
   始点 IP アドレスは任意なので“**`*`**”を指定し、終点 IP アドレスは 192.168.128.0/24 を指定します。“**`reject`**”のフィルタを定義する場合、条件に合わないその他のパケットもすべて捨てられるので、その他はすべて通すというフィルタの定義も必要です。

3. **ip pp secure filter** コマンドを使用して、相手先情報番号 1 の相手に対してフィルタをかけます。PP 側の入口でフィルタをかけるので“**`in`**”を指定します。また、フィルタは 1, 2 の順番でかけるように指定します。

4. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

5.5　Established のみ通信可能にする

[条件]

相手先情報番号が 1 の相手に対して、Established を利用して、PP 側からのアクセスはすべて拒否するが LAN 側からの TCP のアクセスはすべて許可する。

[設定手順]

```
# pp select 1
pp1# ip filter 1 pass * * established
pp1# ip filter 2 pass * * tcp ftpdata *
pp1# ip pp secure filter in 1 2
pp1# save
```

[解説]

1. **pp select** コマンドを使用して、相手先情報番号を選択します。

2. **ip filter** コマンドを使用してフィルタを定義します。
   始点、終点 IP アドレスは任意なので“**`*`**”を指定します。プロトコルパラメータの部分には“**`established`**”を指定します。“**`established`**”を指定すると、TCP 以外のプロトコルはすべて当てはまらないことになります。
   また、始点ポート番号が“**`ftpdata`**”のセッションに関しては PP 側からのアクセスを許可します。これは LAN 側から外に向けて FTP を実行した時のデータ転送のために用いられるからです。

3. **ip pp secure filter** コマンドを使用して、相手先情報番号 1 の相手に対してフィルタをかけます。PP 側の入口でフィルタをかけるので“**`in`**”を指定します。また、フィルタは 1, 2 の順番でかけるように指定します。

4. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

5.6　SNMP のみ通信可能にする

[条件]

相手先情報番号が 1 の相手に対して、SNMP プロトコルのパケットだけを双方向に通信可能にする。

[設定手順]

```
# pp select 1
pp1# ip filter 1 pass * * udp snmp *
pp1# ip filter 2 pass * * udp * snmp
pp1# ip pp secure filter in 1 2
pp1# ip pp secure filter out 1 2
pp1# save
```

[解説]

1. **pp select** コマンドを使用して、相手先情報番号を選択します。

2. **ip filter** コマンドを使用してフィルタを定義します。
   始点、終点 IP アドレスは任意なので“*****”を指定します。プロトコルパラメータの部分には UDP プロトコル、ポートパラメータの部分には“**snmp** ”を指定します。ポートは双方向で指定する必要があるので、始点ポートに対するフィルタと終点ポートに対するフィルタが必要です。

3. **ip pp secure filter** コマンドを使用して、相手先情報番号 1 の相手に対してフィルタをかけます。PP 側の送信受信とも可能にしますから、それぞれに対してフィルタをかけます。

4. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

5.7　両方向で TELNET のみ通信可能にする

[条件]
相手先情報番号が 1 の相手に対して、TELNET プロトコルのパケットだけを双方向に通信可能にする。

[設定手順]

```
# pp select 1
pp1# ip filter 1 pass * * tcp telnet *
pp1# ip filter 2 pass * * tcp * telnet
pp1# ip pp secure filter in 1 2
pp1# ip pp secure filter out 1 2
pp1# save
```

[解説]

1. **pp select** コマンドを使用して、相手先情報番号を選択します。

2. **ip filter** コマンドを使用してフィルタを定義します。
   始点、終点 IP アドレスは任意なので“**`*`**”を指定します。プロトコルパラメータの部分には TCP プロトコル、ポートパラメータの部分には“**`telnet`** ”を指定します。ポートは双方向で指定する必要があるので、始点ポートに対するフィルタと終点ポートに対するフィルタが必要です。

3. **ip pp secure filter** コマンドを使用して、相手先情報番号 1 の相手に対してフィルタをかけます。PP 側の送信受信とも可能にしますから、それぞれに対してフィルタをかけます。

4. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

5.8　外部からの PING コマンドを拒否する

[条件]

相手先情報番号が 1 の相手に対して、PP 側からのすべての ICMP プロトコルのパケットを拒否する。

[設定手順]

```
# pp select 1
pp1# ip filter 1 reject * * icmp
pp1# ip filter 2 pass * *
pp1# ip pp secure filter in 1 2
pp1# save
```

[解説]

1. **pp select** コマンドを使用して、相手先情報番号を選択します。

2. **ip filter** コマンドを使用してフィルタを定義します。
   始点、終点 IP アドレスは任意なので“**`*`**”を指定します。プロトコルパラメータの部分には“**`icmp`** ”プロトコルを指定します。“**`reject`** ”のフィルタを定義する場合、条件に合わないその他のパケットもすべて捨てられるので、その他はすべて通すというフィルタの定義も必要です。

3. **ip pp secure filter** コマンドを使用して、相手先情報番号 1 の相手に対してフィルタをかけます。PP 側の入口でフィルタをかけるので“**`in`**”を指定します。また、フィルタは 1, 2 の順番でかけるように指定します。

4. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

5.9　片方からの FTP のみ通信可能にする

[条件]

相手先情報番号が 1 の相手方向への FTP プロトコルのみ通信可能にする。

[設定手順]

```
# pp select 1
pp1# ip filter 1 pass * * tcp * ftp
pp1# ip filter 2 pass * * tcp ftp *
pp1# ip pp secure filter out 1
pp1# ip pp secure filter in 2
pp1# save
```

[解説]

1. **pp select** コマンドを使用して、相手先情報番号を選択します。

2. **ip filter** コマンドを使用してフィルタを定義します。
   始点、終点 IP アドレスは任意なので“**`*`**”を指定します。プロトコルパラメータの部分には TCP プロトコル、ポートパラメータの部分には“**`ftp`**”を指定します。ポートは始点ポートに対するフィルタと、終点ポートに対するフィルタを用意しておきます。

3. **ip pp secure filter** コマンドを使用して、相手先情報番号 1 の相手に対してフィルタをかけます。PP 側への送信時には、終点ポートが FTP のものを通すようにするので“**`out`**”を指定します。PP 側からの受信時には、始点ポートが FTP のものを通すようにするので“**`in`**”を指定します。

4. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

5.10 RIP 使用時に特定のルーティング情報を通さない

[条件]

相手先情報番号が 1 の相手に対して RIP を使用する場合、ネットワークアドレスが 192.168.128.0/24 に関するルーティング情報だけを PP 側へ流さない。

[設定手順]

```
# pp select 1
pp1# ip filter 1 reject 192.168.128.* *
pp1# ip filter 2 pass * *
pp1# ip pp rip filter out 1 2
pp1# save
```

[解説]

1. **pp select** コマンドを使用して、相手先情報番号を選択します。

2. **ip filter** コマンドを使用してフィルタを定義します。
   始点 IP アドレスは 192.168.128.* を指定し、終点 IP アドレスは任意なので“**`*`**”を指定します。“**`reject`**”のフィルタを定義する場合、条件に合わないその他のパケットもすべて捨てられるので、その他はすべて通すというフィルタの定義も必要です。

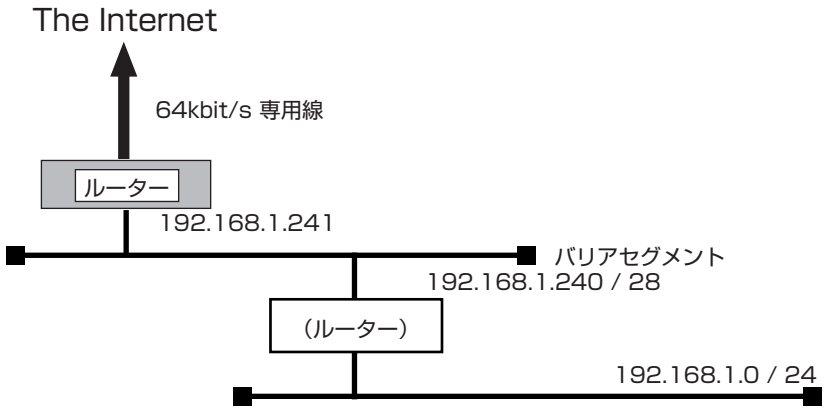
3. **ip pp rip filter** コマンドを使用して、相手先情報番号 1 の相手に対して RIP 情報のフィルタをかけます。PP 側の出口でフィルタをかけるので“**`out`**”を指定します。また、フィルタは 1, 2 の順番でかけるように指定します。

4. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

5.11 インターネット接続し、外部からのアクセスを制限する (バリアセグメントあり)

[条件]

以下の図のように 192.168.1.0/24 のネットワークがバリアセグメント 192.168.1.240/28 を介して専用線経由でインターネット接続する。



更に次のような条件を仮定します。

・外からのパケットはバリアセグメント 192.168.1.240/28 までしか到達できない
・外へのパケットは制限なく出ていける
・セキュリティ関係の設定はすべてヤマハリモートルーターで行い、バリアセグメントとサイト内を結ぶルーターには特にセキュリティに関する設定は行わない

[設定手順]

```
# line type bri1 l64
# ip lan1 address 192.168.1.241/28
# ip route default gateway pp 1
# ip filter 10 reject 192.168.1.0/24 * * * *
# ip filter 11 pass * 192.168.1.0/24 icmp * *
# ip filter 12 pass * 192.168.1.0/24 established **
# ip filter 13 pass * 192.168.1.0/24 tcp * ident
# ip filter 14 pass * 192.168.1.0/24 tcp ftpdata *
# ip filter 15 pass * 192.168.1.0/24 udp domain *
# ip filter 16 pass * 192.168.1.240/28 tcp,udp * telnet,smtp, gopher,finger,www,nntp,ntp,
    33434-33500
# ip filter source-route on
# ip filter directed-broadcast on
# pp select 1
pp1# pp bind bri1
pp1# ip pp secure filter in 10 11 12 13 14 15 16
pp1# pp enable 1
pp1# syslog host 192.168.1.242
pp1# syslog notice on
pp1# save
pp1# interface reset bri1
```

[解説]

1. **line type** コマンドを使用して、回線種別を 64kbit/s ディジタル専用線に指定します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **ip route** コマンドを使用して、外部へ送信するパケットをデフォルトルートにより専用線に向けます。

4. **ip filter** コマンドを使用してフィルタを定義します。
   まず、フィルタの 10 番で、始点 IP アドレスに 192.168.1.* を持つものを排除します。
   次に、フィルタの 11 番から 15 番までで、外部からサイト内部まで通すサービスに対するフィルタを定義します。次に、フィルタの 16 番で、外部からバリアセグメントまで通すサービスに対するフィルタを定義します。デスティネーションポート番号の 33434-33500 は traceroute です。

5. **ip filter source-route** コマンドを使用して、Source-route オプション付き IP パケットをフィルタアウトするように設定します。

6. **ip filter directed-broadcast** コマンドを使用して、終点 IP アドレスが Directed-Broadcast アドレス宛になっている IP パケットをフィルタアウトするように設定します。

7. **pp select** コマンドを使用して、相手先情報番号を選択します。

8. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

9. **ip pp secure filter** コマンドを使用して、PP 側の入口でフィルタをかけるので "**in**" を指定します。

10. **syslog host** コマンドを使用して、フィルタアウトしたパケットの SYSLOG を受けとるホストを設定します。

11. **syslog notice** コマンドを使用して、フィルタアウトしたパケットを SYSLOG で報告するようにします。

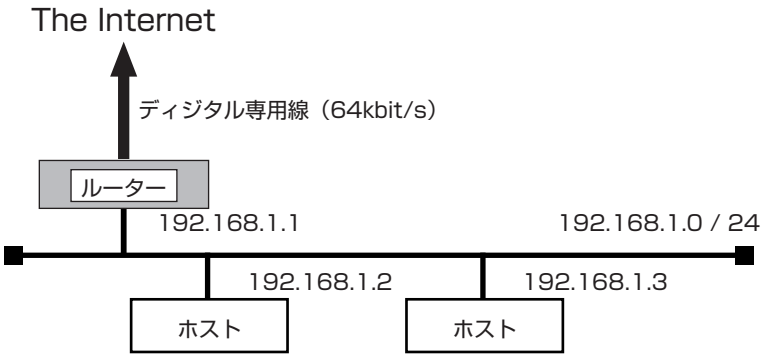
12. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

13. **interface reset** コマンドを使用して、回線のハードウェアを切替えます。この後、実際にパケットが流れるようになります。

5.12 インターネット接続し、外部からのアクセスを制限する (バリアセグメントなし)

[条件]

以下の図のように 192.168.1.0/24 のネットワークがバリアセグメントなしで専用線経由でインターネット接続する。



更に次のような条件を仮定します。

・外からのパケットは 192.168.1.2 だけにしか到達できない
・外へのパケットは制限なく出ていける
・セキュリティ関係の設定はすべてヤマハリモートルーターで行う

[設定手順]

```
# line type bri1 l64
# ip lan1 address 192.168.1.1/24
# ip route default gateway pp 1
# ip filter 10 reject 192.168.1.0/24 * * * *
# ip filter 11 pass * 192.168.1.0/24 icmp * *
# ip filter 12 pass * 192.168.1.0/24 established **
# ip filter 13 pass * 192.168.1.0/24 tcp * ident
# ip filter 14 pass * 192.168.1.0/24 tcp ftpdata *
# ip filter 15 pass * 192.168.1.0/24 udp domain *
# ip filter 16 pass * 192.168.1.2 tcp,udp * smtp,gopher,finger,www,nntp,ntp,33434-33500
# ip filter source-route on
# ip filter directed-broadcast on
# pp select 1
pp1# pp bind bri1
pp1# ip pp secure filter in 10 11 12 13 14 15 16
pp1# pp enable 1
pp1# syslog host 192.168.1.3
pp1# syslog notice on
pp1# save
pp1# interface reset bri1
```

[解説]

1. **line type** コマンドを使用して、回線種別を 64kbit/s ディジタル専用線に指定します 。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **ip route** コマンドを使用して、外部へ送信するパケットをデフォルトルートにより専用線に向けます。

4. **ip filter** コマンドを使用してフィルタを定義します。
   まず、フィルタの 10 番で、始点 IP アドレスに 192.168.1.* を持つものを排除します。次に、フィルタの 11 番から 15 番までで、外部からサイト内部まで通すサービスに対するフィルタを定義します。次に、フィルタの 16 番で、外部から通すサービスに対するフィルタを定義します。デスティネーションポート番号の 33434-33500 は traceroute です。

5. **ip filter source-route** コマンドを使用して、Source-route オプション付き IP パケットをフィルタアウトするように設定します。

6. **ip filter directed-broadcast** コマンドを使用して、終点 IP アドレスが Directed-Broadcast アドレス宛になっている IP パケットをフィルタアウトするように設定します。

7. **pp select** コマンドを使用して、相手先情報番号を選択します。

8. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

9. **ip pp secure filter** コマンドを使用して、PP 側の入口でフィルタをかけるので "**in**" を指定します。

10. **syslog host** コマンドを使用して、フィルタアウトしたパケットの SYSLOG を受けとるホストを設定します。

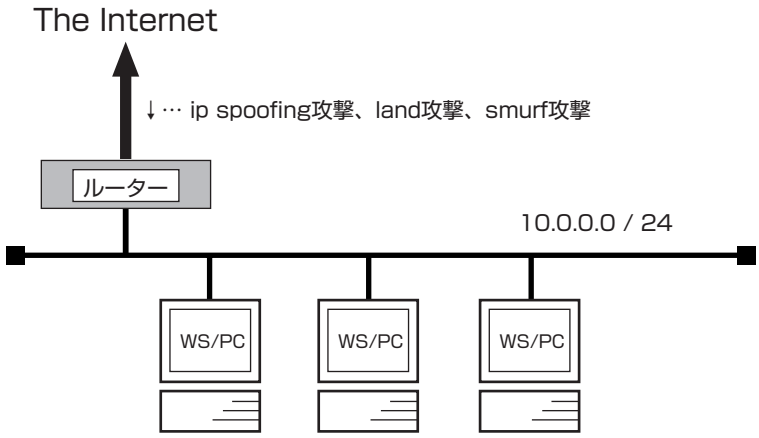
11. **syslog notice** コマンドを使用して、フィルタアウトしたパケットを SYSLOG で報告するようにします。

12. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

13. **interface reset** コマンドを使用して回線のハードウェアを切替えます。この後、実際にパケットが流れるようになります。

5.13 ip spoofing 攻撃、land 攻撃、smurf 攻撃に対処する

[条件]
以下の図のように 10.0.0.0/24 のネットワーク機器を守るための IP パケットフィルタリングである。
ip spoofing 攻撃、land 攻撃、smurf 攻撃の三つすべてに対する防御機能を兼ねる。



[設定手順]

```
# pp select 1
pp1# ip filter 60 reject 10.0.0.0/24 * * * *
pp1# ip filter 100 pass * 10.0.0.0/24 * * *
pp1# ip pp secure filter in 60 100
pp1# save
```

[解説]
ip spoofing 攻撃 (Source Address Spoofing) とは、始点となる IP アドレスを偽造し、あたかも、ネットワーク内部の通信であるかのように見せかけてくるものです。
プロバイダ接続などでは、内部で使用しているネットワーク (の IP アドレス) が外に存在している筈はありませんので、IP パケットフィルタリングで落とします。

land 攻撃とは、基本的に発側 IP アドレスと着側 IP アドレスが同じパケットを投げつけてくるものです。そのようなパケットを IP パケットフィルタリングで落とします。

smurf 攻撃とは、IP ブロードキャストアドレスに送りつけられる偽造した ICMP echo Request パケットを使用した、連続したサービス妨害攻撃です。
「ネットワークアドレス + オール 0…network address」と「ネットワークアドレス + オール 1…directed broadcast address」のパケットを IP パケットフィルタリングで落とします。
ip filter directed-broadcast コマンドを以下のように設定しても同様に smurf 攻撃を防御できます。

```
#ip filter directed-broadcast on
```

6. 動的フィルタリング

動的フィルタでは、パケットを監視し必要に応じて動的にパケットを通したり遮断したりすることができます。
例えば特定のクライアント - サーバ間の通信パケットのみを通過させることを考えた場合、一般的に静的フィルタでは、クライアント - サーバ間の双方向のパケットの流れに対して、それらを通すための通過フィルタを固定的に設定しておく必要があります。この場合、クライアント - サーバ間の通信がない状態でも、その通過フィルタ条件に合致するパケットは通過できることになります。
一方、動的フィルタでこれを設定した場合には、クライアントからサーバへの要求パケットを検出した時点で、その通信で使われるパケットを通すための双方向の通過フィルタが動的に生成されます。またコネクションの終了などを検知することでそれらの通過フィルタは無効となりますので、クライアント - サーバ間の通信がない状態では、一切のパケットは遮断されることになります。
なおここで、他のパケットを遮断するためには、動的フィルタと同時に静的フィルタを併用する必要があることに注意が必要です。

例えば pp out に動的フィルタを適用した場合、逆方向 (pp in) のパケットに対する通過フィルタが動的に生成されますが、それ以外のパケットを遮断するためには静的フィルタ設定

```
ip filter 100 reject * * * * *
ip pp secure filter in 100
```

が必要です。

また同一位置に静的フィルタと動的フィルタを併用する場合には、以下のような動作となります。
静的フィルタのみを設定した場合

```
ip pp secure filter out 1
```

パケットはフィルタ 1 と比較・適用され、合致しないものは遮断されます。
静的フィルタと動的フィルタを併用した場合

```
ip pp secure filter out 1 dynamic 10
```

各パケットはまず静的フィルタ 1 と比較され、通過か遮断かが決定されます。通過するパケットだけがさらに動的フィルタ 10 と比較されます。静的フィルタ 1 で通過したパケットはすべて、動的フィルタと合致しないパケットも含めて通過することになります。
ここで例えば、同時に逆方向に

```
ip pp secure filter in dynamic 20
```

の設定があり、この動的フィルタ 20 の働きで pp out に通過フィルタが動的に生成されていた場合には、各パケットは上記静的フィルタ 1 との比較に先立ってその自動生成されたフィルタと比較され、合致するようであればその時点で通過が決定し、静的フィルタで遮断されることはありません。
動的フィルタのみを設定した場合

```
ip pp secure filter out dynamic 10
```

各パケットは動的フィルタ 10 と比較・適用され、合致しないものも含めてすべてのパケットが通過します。

なお動的フィルタを設定した場合には、静的フィルタと比較して処理の負荷は高くなります。

6.1　PP 側へは特定ネットワーク発の TCP/UDP パケットだけを許可し、PP 側からはその応答パケットを許可する

[設定手順]

```
# ip filter dynamic 1 192.168.0.0/24 * ftp
# ip filter dynamic 2 192.168.0.0/24 * tftp
# ip filter dynamic 3 192.168.0.0/24 * tcp
# ip filter dynamic 4 192.168.0.0/24 * udp
# ip filter 1 pass 192.168.0.0/24 * tcp,udp
# ip filter 100 reject * * * * *
# pp select 1
pp1# ip pp secure filter in 100
pp1# ip pp secure filter out 1 dynamic 1 2 3 4
```

[解説]

1. # ip filter dynamic 1 192.168.0.0/24 * ftp
   # ip filter dynamic 2 192.168.0.0/24 * tftp
   # ip filter dynamic 3 192.168.0.0/24 * tcp
   # ip filter dynamic 4 192.168.0.0/24 * udp
   TCP/UDP に関して、動的フィルタを定義します。FTP と TFTP では逆方向のパケットを判断して通過させる必要があるため、このように別途指定します。送信元 IP アドレスを指定し、特定ネットワーク発のパケットだけを対象とします。

2. # ip filter 1 pass 192.168.0.0/24 * tcp,udp
   PP 側へ送信するパケットを限定するためのフィルタを定義します。

3. # ip filter 100 reject * * * * *
   動的に生成されるフィルタに合致するパケット以外を遮断するためのフィルタを定義します。

4. # pp select 1
   pp1# ip pp secure filter in 100
   PP 側からのパケットは、基本的にはすべて遮断します。PP 側から受信する必要のあるパケットのための通過フィルタは、pp out に適用される動的フィルタにより動的に生成されます。

5. pp1# ip pp secure filter out 1 dynamic 1 2 3 4
   PP 側へ送信されるパケットに関してフィルタを適用します。静的フィルタ 1 に合致しないパケットはすべて遮断されます。また動的フィルタの適用順として、FTP は TCP より先に指定する必要があり、TFTP は UDP より先に指定する必要があります。

6.2　PP 側へは内部の特定ネットワークからのすべてのパケットの送信を許可する。外部の DNS/ メールサーバは特定する

PP 側からは、内部から要求された通信の応答パケットの他、内部の DNS/HTTP/ メールサーバに外部から確立されるコネクションのパケット、および ICMP パケットを通す。

DNS サーバ　　172.16.128.2
メールサーバ　　172.16.128.3
PP への送信を許可する内部の特定ネットワーク　　192.168.0.0/24
内部 DNS サーバ　192.168.0.2
内部 HTTP サーバ　192.168.0.3
内部メールサーバ　192.168.0.3

[設定手順]

```
# ip filter dynamic 1 * 172.16.128.2 domain
# ip filter 1 pass * * tcp * smtp,pop3
# ip filter 2 pass * * tcp * ident
# ip filter dynamic 2 192.168.0.0/24 172.16.128.3 filter 1 in 2
# ip filter dynamic 3 192.168.0.0/24 * www
# ip filter dynamic 4 192.168.0.0/24 * ftp
# ip filter dynamic 5 192.168.0.0/24 * telnet
# ip filter dynamic 10 192.168.0.0/24 * tcp syslog=off
# ip filter dynamic 11 192.168.0.0/24 * udp syslog=off
# ip filter 3 pass * 192.168.0.0/24 icmp * *
# ip filter dynamic 20 * 192.168.0.2 domain
# ip filter dynamic 21 * 192.168.0.3 www
# ip filter 4 pass * 192.168.0.2 tcp * domain
# ip filter 5 pass * 192.168.0.3 tcp * www
# ip filter 6 pass * 192.168.0.3 tcp * smtp,pop3
# ip filter 7 pass * * tcp * ident
# ip filter dynamic 22 * 192.168.0.3 filter 6 in 7
# pp select 1
pp1# ip pp secure filter in 3 4 5 6 dynamic 20 21 22
pp1# ip pp secure filter out dynamic 1 2 3 4 5 10 11
```

[解説]

1. # ip filter dynamic 1 * 172.16.128.2 domain
   外部の特定 DNS サーバに対する動的フィルタを定義します。プロトコルとして tcp/udp ではなくアプリケーション名を指定しているのは、動的フィルタのアプリケーション固有な処理まで行うためです。

2. # ip filter 1 pass * * tcp * smtp,pop3
   # ip filter 2 pass * * tcp * ident
   # ip filter dynamic 2 192.168.0.0/24 172.16.128.3 filter 1 in 2
   外部の特定メールサーバに対する動的フィルタを定義します。送信元 IP アドレスを指定し、内部の特定ネットワーク発のパケットのみを対象とします。フィルタ 1 に合致するパケットを検出したら、その逆方向においてフィルタ 2 に合致するパケットを一定時間通過させます。この逆方向の通過フィルタは、デフォルト状態ではデータが流れなくなってから 3600 秒間保持されます。
   TCP の ident は、一種の認証です。メールの通信を行う際、メールサーバ側から ident によりユーザ情報確認が行われる場合があります。
   このように、**ip filter dynamic** コマンドでは、**ip filter** コマンドの定義を利用することもできますが、その場合はアプリケーション固有な処理は行われません。
   侵入検知の目的などで smtp, pop3 固有の処理を行わせたい場合には、例えば
   ip filter dynamic 1 192.168.0.0/24 172.16.128.3 smtp　　(client → server)
   ip filter dynamic 2 192.168.0.0/24 172.16.128.3 pop3　　(client → server)
   ip filter 1 pass 172.16.128.3 192.168.0.0/24 tcp * ident
   ip filter dynamic 20 172.16.128.3 192.168.0.0/24 filter 1　　(server → client)
   pp select 1
   ip pp secure filter in 1 dynamic 20
   ip pp secure filter out dynamic 1 2
   のように設定する必要があります。

pp in に静的フィルタ 1 を適用しているのは、この静的フィルタ 1 に合致するパケット以外のパケットを遮断するためです。SMTP/POP3 で必要なパケットは、動的フィルタ 1,2 の働きで pp in に通過フィルタが自動生成されますので、通過できることになります。

3. # ip filter dynamic 3 192.168.0.0/24 * www
   # ip filter dynamic 4 192.168.0.0/24 * ftp
   # ip filter dynamic 5 192.168.0.0/24 * telnet
   DNS サーバに対する動的フィルタの設定同様、動的フィルタのアプリケーション固有な処理まで行う目的で、プロトコルとして単に tcp/udp と指定するのではなくアプリケーション名を指定しています。送信元 IP アドレスを指定し、内部の特定ネットワーク発のパケットのみを対象とします。

4. # ip filter dynamic 10 192.168.0.0/24 * tcp syslog=off
   # ip filter dynamic 11 192.168.0.0/24 * udp syslog=off
   その他の TCP/UDP パケットのための動的フィルタを定義します。syslog=off とし、TCP/UDP パケットに関する動的フィルタのログ出力を行わないよう設定します。また送信元 IP アドレスを指定し、内部の特定ネットワーク発のパケットのみを対象とします。

5. # ip filter 3 pass * 192.168.0.0/24 icmp * *
   ICMP パケットを通過させるためのフィルタを定義します。

6. # ip filter dynamic 20 * 192.168.0.2 domain
   # ip filter dynamic 21 * 192.168.0.3 www
   内部の DNS/HTTP サーバへの、外部からのアクセスに対する動的フィルタを定義します。

7. # ip filter 4 pass * 192.168.0.2 tcp * domain
   # ip filter 5 pass * 192.168.0.3 tcp * www
   内部の DNS/HTTP サーバへの、外部からのアクセスに対する静的フィルタを定義します。静的フィルタで遮断されると動的フィルタが適用されませんので、このように通過フィルタを定義して適用する必要があります。

8. # ip filter 6 pass * 192.168.0.3 tcp * smtp,pop3
   # ip filter 7 pass * * tcp * ident
   # ip filter dynamic 22 * 192.168.0.3 filter 6 in 7
   内部のメールサーバへの、外部からのアクセスに対する動的フィルタと静的フィルタを定義します。この動的フィルタは上記動的フィルタ 2 と逆方向の設定となり、pp in 側に適用されることになります。侵入検知の目的などで smtp, pop3 固有の処理を行わせたい場合には、例えば
   ip filter dynamic 20 * 192.168.0.3 smtp (client → server)
   ip filter dynamic 21 * 192.168.0.3 pop3 (client → server)
   ip filter 1 pass * 192.168.0.3 tcp * smtp,pop3
   ip filter 2 pass * * tcp * ident
   ip filter dynamic 1 192.168.0.3 * filter 2 (server → client)
   pp select 1
   ip pp secure filter in 1 dynamic 20 21
   ip pp secure filter out dynamic 1
   のように設定する必要があります。

9. # pp select 1
   pp1# ip pp secure filter in 3 4 5 6 dynamic 20 21 22
   PP 側から受信するパケットに関して動的フィルタを適用します。動的フィルタを適用することで、コネクションの管理などを行うことになります。

10. pp1# ip pp secure filter out dynamic 1 2 3 4 5 10 11
    PP 側へ送信されるパケットに関して動的フィルタを適用します。適用順として、フィルタ 10,11 はアプリケーション指定のフィルタよりも後に指定する必要があります。

6.3 PP 側へはすべてのパケットを送信、 PP 側からは外部のサーバに対して内部から確立される制御コネクションのパケットと、それに続く 2 本のデータコネクションのパケットを通す

トリガーとなる制御コネクションは TCP の 6000 番宛である。2 本のデータコネクションのうち 1 本は制御コネクションと同じ方向で内部からサーバに向けて確立され、UDP の 7001 番宛である。もう 1 本のデータコネクションは逆に外部 (サーバ側) から確立され、UDP の 7002 番宛である。

外部のサーバ　　172.16.128.128

[設定手順]

```
# ip filter 1 pass * * tcp * 6000
# ip filter 2 pass * * udp * 7001
# ip filter 3 pass * * udp * 7002
# ip filter dynamic 1 * 172.16.128.128 filter 1 in 3 out 2
# ip filter 100 reject * * * * *
# pp select 1
pp1# ip pp secure filter in 100
pp1# ip pp secure filter out dynamic 1
```

[解説]

1. # ip filter 1 pass * * tcp * 6000
   # ip filter 2 pass * * udp * 7001
   # ip filter 3 pass * * udp * 7002
   # ip filter dynamic 1 * 172.16.128.128 filter 1 in 3 out 2
   フィルタ 1 に合致する外部の特定サーバ宛のパケットを検出した後、同方向で同ホスト間のフィルタ 2 に合致するパケットと、逆方向で同ホスト間のフィルタ 3 に合致するパケットを、一定時間通過させます。この通過フィルタは、デフォルト状態ではデータが流れなくなってから 30 秒間保持されます。

2. # ip filter 100 reject * * * * *
   動的に生成されるフィルタに合致するパケット以外を遮断するためのフィルタを定義します。

3. # pp select 1
   pp1# ip pp secure filter in 100
   PP 側からのパケットは、基本的にはすべて遮断します。
   PP 側から受信する必要のあるパケットのための通過フィルタは、pp out に適用される動的フィルタにより動的に生成されます。

4. pp1# ip pp secure filter out dynamic 1
   PP 側へ送信されるパケットに関して動的フィルタを適用します。

6.4　インターネット接続し、外部からのアクセスを制限する (バリアセグメントあり)

[設定手順]

```
# line type bri1 l128
# ip lan1 address 192.168.1.241/28
# ip filter 1 reject 192.168.1.0/24 * * * *
# ip filter 2 pass * * icmp * *
# ip filter dynamic 20 * 192.168.1.240/28 telnet
# ip filter dynamic 21 * 192.168.1.240/28 smtp
# ip filter dynamic 22 * 192.168.1.240/28 www
# ip filter dynamic 30 * 192.168.1.240/28 tcp
# ip filter dynamic 31 * 192.168.1.240/28 udp
# ip filter 3 reject * 192.168.1.240/28 established * telnet,smtp,gopher,finger,www,nntp,ntp
# ip filter 4 pass * 192.168.1.240/28 tcp,udp * telnet,smtp,gopher,finger,www,nntp,ntp,33434-33500
# ip filter dynamic 1 * * domain
# ip filter dynamic 2 * * www
# ip filter dynamic 3 * * ftp
# ip filter 5 pass * * tcp * smtp,pop3
# ip filter 6 pass * * tcp * ident
# ip filter dynamic 4 * * filter 5 in 6
# ip filter dynamic 10 * * tcp
# ip filter dynamic 11 * * udp
# ip filter source-route on
# ip filter directed-broadcast on
# pp select 1
pp1# pp bind bri1
pp1# ip pp secure filter in 1 2 3 4 dynamic 20 21 22 30 31
pp1# ip pp secure filter out dynamic 1 2 3 4 10 11
pp1# pp enable 1
pp1# pp select none
# ip route default gateway pp 1
# syslog host 192.168.1.242
# syslog notice on
# save
# interface reset bri1
```

[解説]

1. # line type bri1 l128
   回線種別を設定します。この設定はインタフェースリセットあるいは装置の再起動を行った後に有効になります。

2. # ip lan1 address 192.168.1.241/28
   # ip filter 1 reject 192.168.1.0/24 * * * *
   始点アドレスに 192.168.1.0/24 を持つものを遮断するためのフィルタを定義します。

3. # ip filter 2 pass * * icmp * *
   ICMP パケットを通過させるためのフィルタを定義します。

4. # ip filter dynamic 20 * 192.168.1.240/28 telnet
   # ip filter dynamic 21 * 192.168.1.240/28 smtp
   # ip filter dynamic 22 * 192.168.1.240/28 www
   # ip filter dynamic 30 * 192.168.1.240/28 tcp
   # ip filter dynamic 31 * 192.168.1.240/28 udp
   # ip filter 3 reject * 192.168.1.240/28 established * telnet,smtp,gopher, finger,www,nntp,ntp
   # ip filter 4 pass * 192.168.1.240/28 tcp,udp * telnet,smtp,gopher, finger,www,nntp,ntp,33434-33500
   バリアセグメント上で外部に提供するサービスを許可するフィルタを定義します。ポート 33434-33500 は traceroute で使用されます。動的フィルタの定義でプロトコルとして tcp/udp ではなくアプリケーション名を指定しているものに関しては、動的フィルタのアプリケーション固有の処理を行うことができます。

5. # ip filter dynamic 1 * * domain
   # ip filter dynamic 2 * * www
   # ip filter dynamic 3 * * ftp
   外部の各サーバに対する動的フィルタを定義します。
   プロトコルとして tcp/udp ではなくアプリケーション名を指定しているのは、動的フィルタのアプリケーション固有な処理まで行うためです。

6. # ip filter 5 pass * * tcp * smtp,pop3
   # ip filter 6 pass * * tcp * ident
   # ip filter dynamic 4 * * filter 5 in 6
   外部のメールサーバに対する動的フィルタを定義します。フィルタ 5 に合致するパケットを検出したら、その逆方向においてフィルタ 6 に合致するパケットを一定時間通過させます。この逆方向の通過フィルタは、デフォルト状態ではデータが流れなくなってから 3600 秒間保持されます。
   TCP の ident は、一種の認証です。メールの通信を行う際、メールサーバ側から ident によりユーザ情報確認が行われる場合があります。
   このように、**ip filter dynamic** コマンドでは、**ip filter** コマンドの定義を利用することもできますが、その場合はアプリケーション固有な処理は行われません。
   侵入検知の目的などで smtp, pop3 固有の処理を行わせたい場合には、例えば
   ip filter dynamic 1 * * smtp (client → server)
   ip filter dynamic 2 * * pop3 (client → server)
   ip filter 1 pass * * tcp * ident
   ip filter dynamic 20 * * filter 1 (server → client)
   pp select 1
   ip pp secure filter in 1 dynamic 20
   ip pp secure filter out dynamic 1 2
   のように設定する必要があります。
   pp in に静的フィルタ 1 を適用しているのは、この静的フィルタ 1 に合致するパケット以外のパケットを遮断するためです。SMTP/POP3 で必要なパケットは、動的フィルタ 1,2 の働きで pp in に通過フィルタが自動生成されますので、通過できることになります。
   # ip filter dynamic 10 * * tcp
   # ip filter dynamic 11 * * udp
   その他の TCP/UDP パケットのためのフィルタを定義します。
   # ip filter source-route on
   source-route オプション付き IP パケットを遮断するための設定です。source-route オプションは、フィルタリングをくぐり抜けるなどのアタックの道具にされる可能性があるために遮断します。

7. # ip filter directed-broadcast on
   Directed Broadcast アドレス宛の IP パケットを遮断するための設定です。smurf attack に対して有効です。

8. # pp select 1
   pp1# pp bind bri1
   pp1# ip pp secure filter in 1 2 3 4 dynamic 20 21 22 30 31
   PP 側から受信するパケットに対してフィルタを適用します。適用順として、フィルタ 30,31 はアプリケーション指定のフィルタよりも後に指定する必要があります。

9. pp1# ip pp secure filter out dynamic 1 2 3 4 10 11
   PP 側へ送信されるパケットに関して動的フィルタを適用します。適用順として、フィルタ 10,11 はアプリケーション指定のフィルタよりも後に指定する必要があります。また静的フィルタが適用されていませんので、pp インタフェースの送信方向に関しては すべてのパケットが通過します。

10. pp1# pp enable 1
    pp1# pp select none
    # ip route default gateway pp 1
    # syslog host 192.168.1.242
    # syslog notice on
    # save
    # interface reset bri1
    回線種別が設定変更前と異なるのでインタフェースをリセットします。**restart** コマンドによる装置全体の再起動でもかまいません。

6.5　インターネット接続し、外部からのアクセスを制限する (バリアセグメントなし)

[設定手順]

```
# line type bri1 l128
# ip lan1 address 192.168.1.1/24
# ip filter 1 reject 192.168.1.0/24 * * * *
# ip filter 2 pass * * icmp * *
# ip filter dynamic 20 * 192.168.1.2 telnet
# ip filter dynamic 21 * 192.168.1.2 smtp
# ip filter dynamic 22 * 192.168.1.2 www
# ip filter dynamic 30 * 192.168.1.2 tcp
# ip filter dynamic 31 * 192.168.1.2 udp
# ip filter 3 reject * 192.168.1.2 established * telnet,smtp,gopher,
    finger,www,nntp,ntp
# ip filter 4 pass * 192.168.1.2 tcp,udp * telnet,smtp,gopher,
    finger,www,nntp,ntp,33434-33500
# ip filter dynamic 1 * * domain
# ip filter dynamic 2 * * www
# ip filter dynamic 3 * * ftp
# ip filter 5 pass * * tcp * smtp,pop3
# ip filter 6 pass * * tcp * ident
# ip filter dynamic 4 * * filter 5 in 6
# ip filter dynamic 10 * * tcp
# ip filter dynamic 11 * * udp
# ip filter source-route on
# ip filter directed-broadcast on
# pp select 1
pp1# pp bind bri1
pp1# ip pp secure filter in 1 2 3 4 dynamic 20 21 22 30 31
pp1# ip pp secure filter out dynamic 1 2 3 4 10 11
pp1# pp enable 1
pp1# pp select none
# ip route default gateway pp 1
# syslog host 192.168.1.3
# syslog notice on
# save
# interface reset bri1
```

[解説]

1. # line type bri1 l128
   回線種別を設定します。この設定はインタフェースリセットあるいは装置の再起動を行った後に有効になります。

2. # ip lan1 address 192.168.1.1/24
   # ip filter 1 reject 192.168.1.0/24 * * * *
   始点アドレスに 192.168.1.0/24 を持つものを遮断するための定義です。

3. # ip filter 2 pass * * icmp * *
   ICMP パケットの通過を許可するための定義です。

4. # ip filter dynamic 20 * 192.168.1.2 telnet
   # ip filter dynamic 21 * 192.168.1.2 smtp
   # ip filter dynamic 22 * 192.168.1.2 www
   # ip filter dynamic 30 * 192.168.1.2 tcp
   # ip filter dynamic 31 * 192.168.1.2 udp
   # ip filter 3 reject * 192.168.1.2established * telnet,smtp,gopher,finger,www,nntp,ntp
   # ip filter 4 pass * 192.168.1.2 tcp,udp * telnet,smtp,gopher,finger,www,nntp,ntp,33434-33500

特定サーバ 192.168.1.2 が外部に提供するサービスを許可するための定義です。ポート 33434-33500 は traceroute で使用されます。動的フィルタの定義でプロトコルとして tcp/udp ではなくアプリケーション名を指定しているものに関しては、動的フィルタのアプリケーション固有の処理を行うことができます。

5. # ip filter dynamic 1 * * domain
   # ip filter dynamic 2 * * www
   # ip filter dynamic 3 * * ftp
   外部の各サーバに対する動的フィルタを定義します。
   プロトコルとして tcp/udp ではなくアプリケーション名を指定しているのは、動的フィルタのアプリケーション固有の処理まで行うためです。

6. # ip filter 5 pass * * tcp * smtp,pop3
   # ip filter 6 pass * * tcp * ident
   # ip filter dynamic 4 * * filter 5 in 6
   外部のメールサーバに対する動的フィルタを定義します。フィルタ 5 に合致するパケットを検出したら、その逆方向においてフィルタ 6 に合致するパケットを一定時間通過させます。この逆方向の通過フィルタは、デフォルト状態ではデータが流れなくなってから 3600 秒間保持されます。TCP の ident は、一種の認証です。メールの通信を行う際、メールサーバ側から ident によりユーザ情報確認が行われる場合があります。
   このように、**ip filter dynamic** コマンドでは、**ip filter** コマンドの定義を利用することもできますが、その場合はアプリケーション固有な処理は行われません。
   侵入検知の目的などで smtp, pop3 固有の処理を行わせたい場合には、例えば
   ip filter dynamic 1 * * smtp (client → server)
   ip filter dynamic 2 * * pop3 (client → server)
   ip filter 1 pass * * tcp * ident
   ip filter dynamic 20 * * filter 1 (server → client)
   pp select 1
   ip pp secure filter in 1 dynamic 20
   ip pp secure filter out dynamic 1 2
   のように設定する必要があります。
   pp in に静的フィルタ 1 を適用しているのは、この静的フィルタ 1 に合致するパケット以外のパケットを遮断するためです。SMTP/POP3 で必要なパケットは、動的フィルタ 1,2 の働きで pp in に通過フィルタが自動生成されますので、通過できることになります。
   # ip filter dynamic 10 * * tcp
   # ip filter dynamic 11 * * udp
   その他の TCP/UDP パケットのための動的フィルタを定義します。

7. # ip filter source-route on
   source-route オプション付き IP パケットを遮断するための設定です。source-route オプションは、フィルタリングをくぐり抜けるなどのアタックの道具にされる可能性があるために遮断します。

8. # ip filter directed-broadcast on
   Directed Broadcast アドレス宛になっている IP パケットを遮断するための設定です。smurf attack に対して有効です。

9. # pp select 1
   pp1# pp bind bri1
   pp1# ip pp secure filter in 1 2 3 4 dynamic 20 21 22 30 31
   PP 側から受信するパケットに対してフィルタを適用します。適用順として、フィルタ 30,31 はアプリケーション指定のフィルタよりも後に指定する必要があります。

10. pp1# ip pp secure filter out dynamic 1 2 3 4 10 11
    PP 側へ送信されるパケットに関して動的フィルタを適用します。適用順として、フィルタ 10,11 はアプリケーション指定のフィルタよりも後に指定する必要があります。
    また静的フィルタが適用されていませんので、pp インタフェースの送信方向に関してはすべてのパケットが通過します。

11. pp1# pp enable 1
    pp1# pp select none
    # ip route default gateway pp 1
    # syslog host 192.168.1.3
    # syslog notice on
    # save
    # interface reset bri1
    回線種別が設定変更前と異なるのでインタフェースをリセットします。**restart** コマンドによる装置全体の再起動でもかまいません。

7. 動的フィルタリングその 2 （不正アクセス検知）

通過するパケットを、不正なパケットの持つパターンと比較することで、侵入や攻撃を検出し、ユーザに通知することができます。パケット単位の処理の他、コネクションの状態に基づく検査や、ポートスキャンのような状態管理の必要な検査も実施します。ただし、侵入に該当するか否かを正確に判定することは難しく、完全な検知は不可能であることに注意してください。
動的フィルタで管理している情報を利用して動作するため、動的フィルタと併用することで、最大限の効果を発揮します。例えば、SMTP に対する動的フィルタが設定されていれば、その情報に基づいて、SMTP に関する侵入を検知します。逆に、動的フィルタが設定されていなければ、SMTP に関する侵入を検知しません。

一方、IP ヘッダや ICMP のように、動的フィルタでは扱えないパケットについては、動的フィルタの設定の有無に関わらず動作します。また、TCP や UDP についても、基本的には動的フィルタを定義しなくても機能します。

7.1 PP インタフェースの内向きのトラフィックで侵入や攻撃を検知する

[設定手順]

```
# pp select 1
pp1# ip pp intrusion detection in on
```

[解説]
pp インタフェースから入ってくるパケットを対象に不正なアクセスを検知します。検知した場合、デフォルトではログに記録するだけで不正なパケットの破棄は行いません。

7.2 PP インタフェースの内向きのトラフィックで侵入や攻撃を検知し、かつ不正パケットは破棄する

[設定手順]

```
# pp select 1
pp1# ip pp intrusion detection in on reject=on
```

[解説]
reject の指定で不正パケットを破棄するよう設定します。

7.3 PP インタフェースの内向きのトラフィックで、FTP/SMTP に関する侵入や攻撃まで含めて検知する

[設定手順]

```
# ip filter dynamic 1 * * ftp
# ip filter dynamic 2 * * smtp
# pp select 1
pp1# ip pp secure filter in dynamic 1 2
pp1# ip pp intrusion detection in on
```

[解説]
FTP/SMTP に関する検知は動的フィルタを設定しなければ働かないため、このように併用します。すべてのパケットはフィルタとの合致に関わりなく通過します。

8.　ポリシーフィルタ設定例

Rev.10 以降のファームウェアではそれ以前の動的フィルタの機能に替わりポリシーフィルタの機能が実装されています。
ポリシーフィルタは従来のファームウェアの動的フィルタに相当しており、Stateful Inspection 方式のフィルタリングを実現するものです。すなわち、パケットの単位ではなく、コネクションの単位で、通過と破棄を指定することができます。たとえば、「SMTP のコネクションを通す」とか「TELNET のコネクションを破棄する」というような制御が可能です。
コネクションを指定するために、下記の項目を設定します。

・受信インターフェース
・送信インターフェース
・始点アドレス
・終点アドレス
・サービス

サービスとは、多くの場合、アプリケーションに対応しており、たとえば、TELNET、SMTP、POP、FTP、WWW などの値を取るものです。

動作としては、通過と破棄のいずれかを設定できます。例えば、

```
#ip policy filter 10 reject-log lan2 lan1 * * telnet
#ip policy filter 11 pass-nolog lan1 lan2 * * ping
```

の例では、

・LAN2 から LAN1 へ抜ける TELNET を破棄する
・LAN1 から LAN2 へ抜ける ping を許可する

という 2 つのルールを定義しています。ヤマハルーターでは、このように条件と動作を組み合わせたルールをポリシーと呼んでいます。

ポリシーの動作としては、次の 4 種類があります。

動作	説明
pass	パケットを通します。TCP と UDP と ping については、Stateful Inspection 方式で通し、それ以外のパケットについては、そのまま通します。
static-pass	Stateful Inspection 方式を使わずにパケットを通します。
reject	パケットを破棄します。
restrict	パケットを送信しようとするインターフェースが up しており、パケットを送信できる状態になっているならば通し、そうでなければパケットを破棄します。パケットを通すときには、TCP と UDP と ping については、Stateful Inspection 方式で通し、それ以外のパケットについては、そのまま通します。

インターフェースやアドレスやサービスを表現するときには、グループという概念を使うことができます。グループは複数の値をまとめて扱うときに使うもので、例えば以下のように設定すると、複数のインターフェースをまとめた「Private」という名前のインターフェースグループや、smtp と pop3 をまとめて「Mail」という名前のサービスグループを作ることができます。

```
#ip policy interface group 1 name=Private local lan1
#ip policy service group 1 name=Mail smtp pop3
```

ポリシーを順に並べたものをポリシーセットと呼びます。ヤマハルーターでは複数のポリシーセットを定義でき、そのうちの 1 つを選んで使用します。例えば、普段は「通常設定」という名前のポリシーセットを使っておき、何か問題が発生したら、「緊急設定」という名前のポリシーセットに切り替えるという使い方をします。

ポリシーを階層的に並べることもできます。これは、条件を絞り込んで例外的なポリシーを追加するときに便利です。ポリシーを階層的に書く場合、下位のポリシーは、上位のポリシーの条件を引き継ぎます。つまり、下位のポリシーの条件は、上位のポリシーの条件を絞り込むことになります。ポリシーの階層は最大で 4 階層まで定義できます。

GUI での設定方法やより詳しい情報については、ヤマハホームページをご参照ください。

8.1 PP 側へは特定ネットワーク発の TCP/UDP パケットだけを許可し、PP 側からはその応答パケットを許可する

内部の特定ネットワーク　192.168.0.0/24

[設定手順]

```
#ip policy filter 10 pass-log local * * * *
#ip policy filter 11 static-pass-log * lan1 * * *
#ip policy filter 20 reject-nolog lan1 * * * *
#ip policy filter 21 static-pass-nolog * local * * *
#ip policy filter 22 pass-nolog * pp1 192.168.0.0/24 * tcp
#ip policy filter 23 pass-nolog * pp1 192.168.0.0/24 * udp
#ip policy filter 30 reject-nolog * * * * *

#ip policy filter set 1 10 [11] 20 [21 22 23] 30
#ip policy filter set enable 1
#save
```

[解説]

1. #ip policy filter 10 pass-log local * * * *
   ルーター発のパケットを通過させるポリシーフィルタを定義します。
   キーワード「local」は、ルーター自身を表します。

2. #ip policy filter 11 static-pass-log * lan1 * * *
   フィルタ 10 の例外的条件として，内部ネットワーク（LAN1）宛のパケットを Stateful Inspection 方式を使用しないで通過させます。
   ポリシーフィルタの Stateful Inspection 方式では、フローを用いてコネクションを管理しますが、ヤマハルーターではポリシーフィルタを処理するフローの最大値が決まっています。
   内部ネットワーク内の通信を Stateful Inspection 方式で処理すると、過度のトラヒックが流れた場合にルーター自身にアクセスできなくなる可能性があります。
   そこで、Stateful Inspection 方式を使用しないで通過させるためのキーワード「static-pass-nolog」を指定する必要があります。

3. #ip policy filter 20 reject-nolog lan1 * * * *
   受信インターフェースが lan1 のパケットを遮断するポリシーフィルタを定義します。

4. #ip policy filter 21 static-pass-nolog * local * * *
   フィルタ 20 の例外的条件として、受信インターフェースが lan1 のパケットのうち、送信インターフェースが local のパケットについて、Stateful Inspection 方式を用いないで通過させるためのポリシーフィルタを定義します。

5. #ip policy filter 22 pass-nolog * pp1 192.168.0.0/24 * tcp
   #ip policy filter 23 pass-nolog * pp1 192.168.0.0/24 * udp
   フィルタ 20 の例外的条件として、PP 側への TCP/UDP パケットを通過させるポリシーフィルタを定義します。
   送信元 IP アドレスを特定のネットワークに限定し、特定ネットワーク発のパケットのみを PP 側へと通過させます。

6. #ip policy filter 30 reject-nolog * * * * *
   ここまでのフィルタの判定条件に一致しなかったパケットを遮断するためのポリシーフィルタを定義します。

7. #ip policy filter set 1 10 [11] 20 [21 22 23] 30
   ポリシーセットを定義します。
   このようにフィルタを並べた場合には、新しいコネクションが発生するたびに先頭から順にフィルタと一致するか否かを評価します。

   また、ヤマハルーターではポリシーフィルタを階層的に並べることによって、上位フィルタの例外的条件を定義し、下位フィルタの条件を絞り込むことができますが、その階層構成をここで定義します。
   階層構成の親子関係は「[」と「]」記号を用いて表現し、「[」は 1 つ下の階層へ移動、「]」は 1 つ上の階層へ移動することを意味します。
   ポリシーセットを階層構成で定義した場合、下位のフィルタが上位のフィルタの条件を引き継ぐことを意味します。

例えば、フィルタ番号のならびが 「1 [2]」という表現は、フィルタ 2 が上位フィルタ 1 の判定条件を引き継ぐということを表しており、言い替えればフィルタ 1 の例外的条件としてフィルタ 2 を定義するということができます。

8. #ip policy filter set enable 1
定義したフィルタを適用するため、ポリシーセットを有効にします。

9. #save
設定を不揮発性メモリに保存します.

8.2 PP 側へは内部の特定ネットワークから、特定サービスのパケットのみ通過を許可する

PP 側からは、内部から要求された通信の応答パケットのみを通過させ、それ以外の PP 側から確立されるコネクションは遮断する。
＃外部の特定の DNS/ メールサーバへのアクセスを許可する。

内部の特定ネットワーク	192.168.0.0/24
PP 側へパケットを通過させるサービス	HTTP/ メール /DNS
DNS サーバ	172.16.128.2
メールサーバ	172.16.128.3

[設定手順]

```
#ip policy interface group 1 name=Private local lan1
#ip policy service group 1 name=Mail pop3 smtp

#ip policy filter 10 pass-nolog local * * * *
#ip policy filter 11 static-pass-nolog * lan1 * * *
#ip policy filter 100 reject-nolog lan1 * * * *
#ip policy filter 110 static-pass-nolog * 1 * * *
#ip policy filter 120 reject-nolog * * 192.168.0.0/24 * *
#ip policy filter 121 pass-log * * * 172.16.128.2 dns
#ip policy filter 122 pass-log * * * * www
#ip policy filter 123 pass-log * * * 172.16.128.3 1
#ip policy filter 200 reject-nolog * * * * *

#ip policy filter set 1 name="Internet Access" 10 [11] 100 [110 120 [121 122 123]] 200
#ip policy filter set enable 1
#save
```

[解説]

1. #ip policy interface group 1 name=Private local lan1
   ポリシーフィルタでは、送信 / 受信に使用されるインターフェースをまとめてインターフェースグループを定義することができます。
   キーワード「local」はルーター自身、キーワード「lan1」は内部ネットワークに用いる LAN1 インターフェースを意味します。

2. #ip policy service group 1 name=Mail pop3 smtp
   ポリシーフィルタでは、複数のサービス名をまとめてサービスグループを定義することができます。
   ここではメールサーバへのアクセスを制御するために、pop3、smtp のプロトコルに関するフィルタを定義する必要がありますが、サービスグループとして一つの識別子を定義することで、ポリシーフィルタの定義自体を簡略化することができます。

3. #ip policy filter 10 pass-nolog local * * * *
   #ip policy filter 11 static-pass-nolog * lan1 * * *
   ルーター発のパケットを Stateful Inspection 方式を用いて通過させ、その例外的条件として lan1 宛のパケットは Stateful Inspection 方式を使用しないで通過させるためのポリシーフィルタを定義します。

4. #ip policy filter 100 reject-nolog lan1 * * * *
   内部ネットワークからの通信を遮断するためのポリシーフィルタを定義します。
   このフィルタでは受信インターフェースが lan1 のパケットを遮断します。

5. #ip policy filter 110 static-pass-nolog * 1 * * *
   フィルタ 100 の例外的条件として、内部ネットワークから、ルーター宛、または内部ネットワーク宛のパケットを、Stateful Inspection 方式を使用しないで通過させるためのポリシーフィルタを定義します。

6. #ip policy filter 120 reject-nolog * * 192.168.0.0/24 * *
   フィルタ 100 の例外的条件として、内部の特定ネットワーク発のパケットを遮断するためのポリシーフィルタを定義します。

7. #ip policy filter 121 pass-log * * * 172.16.128.2 dns
   #ip policy filter 122 pass-log * * * * www
   #ip policy filter 123 pass-log * * * 172.16.128.3 1
   フィルタ 120 の例外的条件として、受信インターフェースが lan1 で送信元アドレスが 192.168.0.0/24 のネットワーク発のパケットのうち、特定のサーバまたは特定のサービスへ通過させるポリシーフィルタを定義します。
   フィルタ 121 では、外部の特定の DNS サーバに対するパケットを通過させ、記録します。
   フィルタ 122 では、外部の不特定の WWW サーバに対するパケットを通過させ、記録します。
   ここでキーワード「www」は http（80 番ポート）と https（441 番ポート）の両方を含みます。
   フィルタ 123 では、外部の特定のメールサーバに対するパケットを通過させ、記録します。サービス名には、キーワードではなく、先に定義したサービスグループ "Mail" をサービスグループ番号で指定します。

8. #ip policy filter 200 reject-nolog * * * * *
   これまでのポリシーフィルタの判定条件に一致しなかったパケットをすべて遮断するための、ポリシーフィルタを定義します。

9. #ip policy filter set 1 name="Internet Access" 10 [11] 100 [110 120 [121 122 123]] 200
   ポリシーセットを定義します。
   先に定義したポリシーフィルタの親子関係を基に、階層構成を作成します。

10. #ip policy filter set enable 1
    定義したフィルタを適用するため、ポリシーセットを有効にします。

11. #save
    設定を不揮発性メモリに保存します.

8.3 内部ネットワークから外部への通信を、特定のサービス宛、特定のネットワーク発に制限する不要なパケットを入力遮断フィルタで破棄する

内部ネットワーク側（LAN1）からの DNS アクセスを許可する。
外部の特定の NTP サーバへのアクセスを許可する。
内部の特定ネットワークから PP 側へは、HTTP ／メールサーバへのアクセスのみを許可する。
PP 側からは、内部から要求された通信の応答パケットの他、HTTP ／ FTP サーバに外部から確立されるコネクションのパケットを通過させる。
WAN 側から受信した不要なパケットを入力遮断フィルタで破棄する。

内部の特定ネットワーク	192.168.0.0/24 192.168.1.0/24
内部の HTTP/FTP サーバ	192.168.0.5
外部の NTP サーバ	172.16.0.1

[設定手順]

```
#ip inbound filter 1 reject-nolog * * tcp,udp * 135
#ip inbound filter 2 reject-nolog * * tcp,udp 135 *
#ip inbound filter 3 reject-nolog * * tcp,udp * netbios_ns-netbios_ssn
#ip inbound filter 4 reject-nolog * * tcp,udp netbios_ns-netbios_ssn *
#ip inbound filter 5 reject-nolog * * tcp,udp * 445
#ip inbound filter 6 reject-nolog * * tcp,udp 445 *
#ip inbound filter 7 pass-nolog * * * * *

#pp select 1
pp1#ip pp inbound filter list 1 2 3 4 5 6 7
pp1#pp select none

#ip policy interface group 1 name=Private local lan1
#ip policy address group 1 name=Private 192.168.0.0/24 192.168.1.0/24
#ip policy service group 1 name="Mail" pop3 smtp
#ip policy service group 2 name="HTTP Access" www ftp

#ip policy filter 100 pass-nolog local * * * *
#ip policy filter 110 static-pass-nolog * lan1 * * *
#ip policy filter 200 reject-nolog lan1 * * * *
#ip policy filter 210 static-pass-nolog * 1 * * *
#ip policy filter 211 static-pass-log * * * * http
#ip policy filter 220 pass-nolog * * * * dns
#ip policy filter 230 pass-nolog * * * 172.16.0.1 ntp
#ip policy filter 240 reject-nolog * pp1 1 * *
#ip policy filter 241 pass-log * * * * 1
#ip policy filter 242 pass-log * * * * 2
#ip policy filter 300 reject-nolog pp1 * * * *
#ip policy filter 310 reject-nolog * lan1 * * *
#ip policy filter 311 pass-log * * * 192.168.0.5 2
#ip policy filter 400 reject-nolog * * * * *

#ip policy filter set 1 name="Internet Access" 100 [110] 200 [210 [211] 220 230 240 [241 242]] 300 [310 [311]] 400
#ip policy filter set enable 1
#save
```

[解説]

1. #ip inbound filter 1 reject-nolog * * tcp,udp * 135
   #ip inbound filter 2 reject-nolog * * tcp,udp 135 *
   #ip inbound filter 3 reject-nolog * * tcp,udp * netbios_ns-netbios_ssn
   #ip inbound filter 4 reject-nolog * * tcp,udp netbios_ns-netbios_ssn *
   #ip inbound filter 5 reject-nolog * * tcp,udp * 445
   #ip inbound filter 6 reject-nolog * * tcp,udp 445 *
   不要なサービスへのアクセスをあらかじめ遮断するために、入力遮断フィルタを定義します。
   ヤマハルーターでは、NAT 処理やルーティング処理、ポリシーフィルタの処理に先だって、受信したパケットを入力遮断フィルタで処理します。
   そのため、評価条件としてコネクションを監視する必要のないアクセスに対しては入力遮断フィルタを用いることで、ルーターの処理の早い段階でパケットを遮断することができます。
   ここでは、不要なサービスへのパケットをルーターで通過させないように、入力遮断フィルタを定義します。

2. #ip inbound filter 7 pass-nolog * * * * *
   それ以外のパケットを通過させる入力遮断フィルタを定義します。
   ここで通過したパケットは、NAT 処理、ルーティングの後にポリシーフィルタで評価されます。

3. #pp select 1
   pp1#ip pp inbound filter list 1 2 3 4 5 6 7
   pp1#pp select none
   入力遮断フィルタを選択した PP インターフェースに適用します。

4. #ip policy interface group 1 name=Private local lan1
   ルーター自身（local）及び内部ネットワークインターフェース（lan1）をまとめてインターフェースグループを定義します。

5. #ip policy address group 1 name=Private 192.168.0.0/24 192.168.1.0/24
   ポリシーフィルタでは、インターフェースグループやサービスグループと同じように送信元 / 宛先に使用されるアドレスをまとめて、アドレスグループを定義することができます。
   ここでは、内部ネットワークとして利用するふたつのネットワークアドレスをまとめてアドレスグループを定義しています。

6. #ip policy service group 1 name="Mail" pop3 smtp
   #ip policy service group 2 name="HTTP Access" www ftp
   ポリシーフィルタで制御するサービスをまとめて、サービスグループを定義することができます。
   メールサービスに関するフィルタを作成するために、pop3、smtp をまとめてひとつのサービスグループを定義しています。
   また、HTTP アクセスを制御するために www、ftp サービスをまとめてひとつのサービスグループを定義しています。

7. #ip policy filter 100 pass-nolog local * * * *
   #ip policy filter 110 static-pass-nolog * lan1 * * *
   ルーター発のパケットを Stateful Inspection 方式を用いて通過させ、その例外的条件として lan1 宛のパケットは Stateful Inspection 方式を使用しないで通過させるためのポリシーフィルタを定義します。

8. #ip policy filter 200 reject-nolog lan1 * * * *
   内部ネットワークからの通信を遮断するためのポリシーフィルタを定義します。

9. #ip policy filter 210 static-pass-nolog * 1 * * *
   #ip policy filter 211 static-pass-log * * * * http
   フィルタ 200 の例外条件として、送信インターフェースが local、または lan1 のパケットを Stateful Inspection 方式を使わずに通過させるためのポリシーフィルタを定義します。送信インターフェースには、インターフェースグループ 1 を指定します。
   続いて、フィルタ 210 の条件に一致するパケットのうち、http に関するパケットを記録するためのポリシーフィルタを定義します。

10. #ip policy filter 220 pass-nolog * * * * dns
    フィルタ 200 の例外条件として、dns サービスを利用するためのパケットを通過させるポリシーフィルタを定義します。

11. #ip policy filter 230 pass-nolog * * * 172.16.0.1 ntp
フィルタ 200 の例外条件として、ntp のパケットを通過させるポリシーフィルタを定義します。外部の ntp サーバは特定のものだけを許可します。

12. #ip policy filter 240 reject-nolog * pp1 1 * *
#ip policy filter 241 pass-log * * * * 1
#ip policy filter 242 pass-log * * * * 2
フィルタ 200 の条件を絞り込むために、内部の特定ネットワークから PP 側へのパケットを遮断するポリシーフィルタを定義します。
PP 側へのパケットは基本的に遮断しますが、メールサービスと HTTP アクセスに関するパケットを通過させるために、フィルタ 241、242 のフィルタを定義します。
サービス名には、先に定義したサービスグループの "Mail"、"HTTP Access" を指定します。
また、通過するパケットを記録するために pass-log を指定します。

13. #ip policy filter 300 reject-nolog pp1 * * * *
#ip policy filter 310 reject-nolog * lan1 * * *
#ip policy filter 311 pass-log * * * 192.168.0.5 2
PP 側からのアクセスを遮断するためのポリシーフィルタ 300 を定義します。
受信インターフェース PP1 から送信インターフェース lan1 へのパケットは基本的に遮断しますが、外部からの 192.168.0.5 への HTTP アクセスはパケットを通過させます。

14. #ip policy filter 400 reject-nolog * * * * *
それまでのフィルタの判定条件に一致しないすべてのパケットを遮断するためのポリシーフィルタを定義します。

15. #ip policy filter set 1 name="Internet Access" 100 [110] 200 [210 [211] 220 230 240 [241 242]] 300 [310 [311]] 400
#ip policy filter set enable 1
ポリシーセットを定義します。
定義したポリシーフィルタを、正しい階層構成でフィルタセットとして定義する必要があります。
また、ポリシーフィルタを動作させるために、作成したフィルタセットを有効にします。

16. #save
設定を不揮発性メモリに保存します.

9. PAP/CHAP の設定

本章では、PAP/CHAP によるセキュリティの設定を解説します。
PPP の認証プロトコルである、**PAP**(Password Authentication Protocol) と **CHAP**(Challenge Handshake Authentication Protocol) により、PP 側との通信にセキュリティをかけることができます。特定の相手先に対して PAP と CHAP の両方を併用することはできません。

PAP の場合と CHAP の場合の設定方法を以下に示した順に説明します。

1. どちらか一方で PAP を用いる場合
2. 両側で PAP を用いる場合
3. どちらか一方で CHAP を用いる場合
4. 両側で CHAP を用いる場合

9.1 どちらか一方で PAP を用いる場合

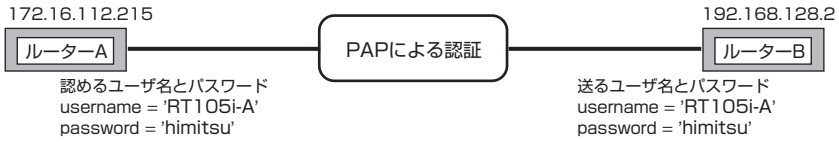
[認証の設定条件]

・ルーター A が認証するなら PAP だけである

・ルーター A が認めるルーター B のユーザ名は 'RT105i-A' であり、かつそのパスワードは 'himitsu' である

・ルーター B は PAP 認証を認める

・ルーター B がルーター A に送るユーザ名は 'RT105i-A' であり、かつそのパスワードは 'himitsu' である



[ルーター A (認証する側) の設定手順]

```
# pp select 1
pp1# pp auth request pap
pp1# pp auth username RT105i-A himitsu
pp1# pp enable 1
pp1# save
```

[ルーター B (認証される側) の設定手順]

```
# pp select 1
pp1# pp auth accept pap
pp1# pp auth myname RT105i-A himitsu
pp1# pp enable 1
pp1# save
```

9.2　両側で PAP を用いる場合

片側で PAP を用いる場合と同様にして、両側とも以下のように設定します。

[手順]

```
# pp select 1
pp1# pp auth request pap
pp1# pp auth accept pap
pp1# pp auth myname RT105i-A himitsu
pp1# pp auth username RT105i-A himitsu
pp1# pp enable 1
pp1# save
```

9.3　どちらか一方で CHAP を用いる場合

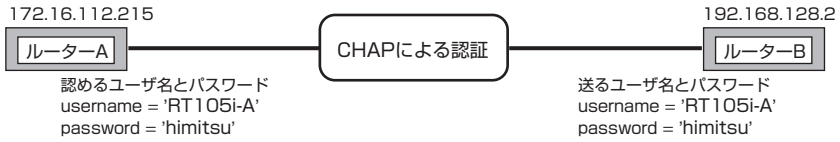
[認証の設定条件]

・ルーター A が認証するなら CHAP だけである

・ルーター A が認めるルーター B のユーザ名は 'RT105i-A' であり、かつそのパスワードは 'himitsu' である

・ルーター B は CHAP 認証を認める

・ルーター B がルーター A に送るユーザ名は 'RT105i-A' であり、かつそのパスワードは 'himitsu' である



[ルーター A (認証する側) の設定手順]

```
# pp select 1
pp1# pp auth request chap
pp1# pp auth username RT105i-A himitsu
pp1# pp enable 1
pp1# save
```

[ルーター B (認証される側) の設定手順]

```
# pp select 1
pp1# pp auth accept chap
pp1# pp auth myname RT105i-A himitsu
pp1# pp enable 1
pp1# save
```

9.4 両側で CHAP を用いる場合

片側で CHAP を用いる場合と同様にして、両側とも以下のように設定します。

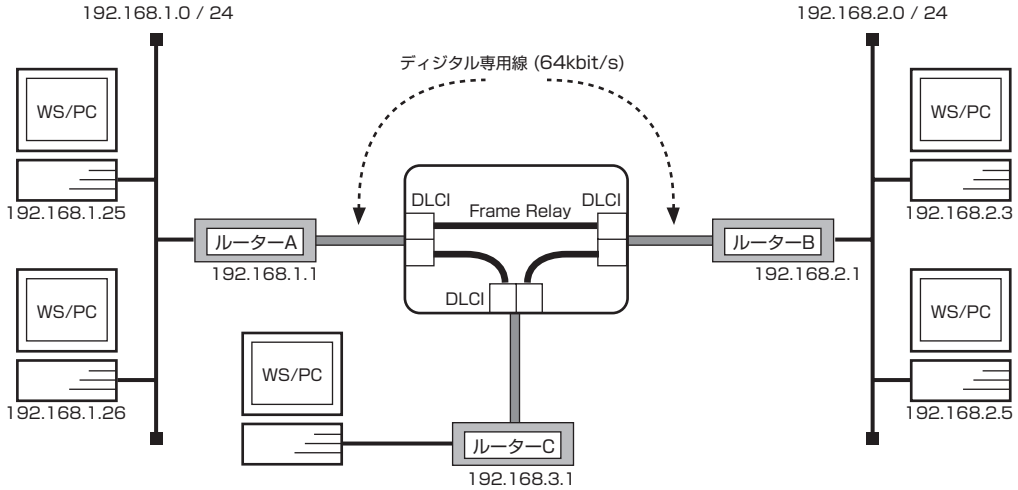
[認証の設定手順]

```
# pp select 1
pp1# pp auth request chap
pp1# pp auth accept chap
pp1# pp auth myname RT105i-A himitsu
pp1# pp auth username RT105i-A himitsu
pp1# pp enable 1
pp1# save
```

10. フレームリレー設定例

10.1 フレームリレーで LAN を接続 (IP、unnumbered、RIP2)

[構成図]



[ルーター A の設定手順]

```
# line type bri1 l64
# ip lan1 address 192.168.1.1/24
# rip use on
# pp select 1
pp1# pp bind bri1
pp1# pp encapsulation fr
pp1# ip pp rip send on version 2
pp1# ip pp rip connect send interval
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

[ルーター B の設定手順]

```
# line type bri1 l64
# ip lan1 address 192.168.2.1/24
# rip use on
# pp select 1
pp1# pp bind bri1
pp1# pp encapsulation fr
pp1# ip pp rip send on version 2
pp1# ip pp rip connect send interval
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

[ルーター C の設定手順]

```
# line type bri1 l64
# ip lan1 address 192.168.3.1/24
# rip use on
# pp select 1
pp1# pp bind bri1
pp1# pp encapsulation fr
pp1# ip pp rip send on version 2
pp1# ip pp rip connect send interval
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

[解説]

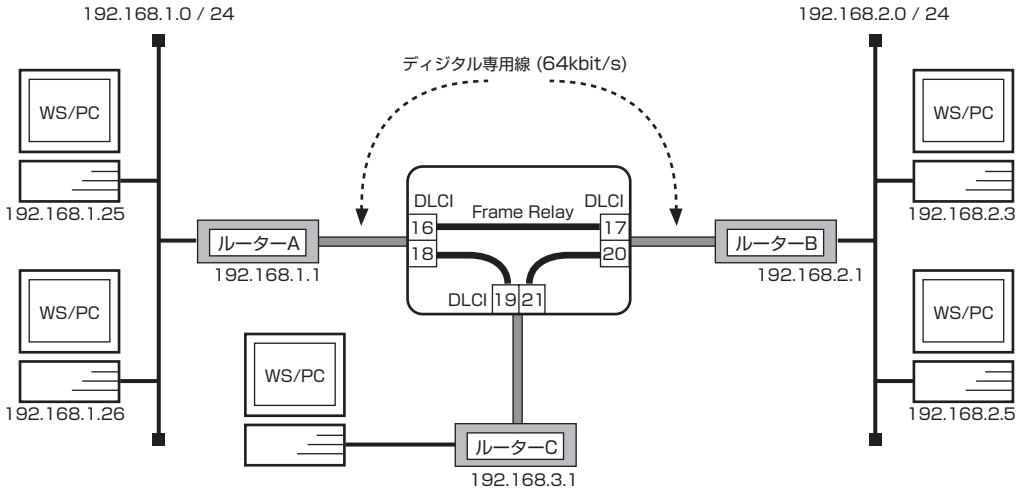
ネットワーク 192.168.1.0 とネットワーク 192.168.2.0 、ネットワーク 192.168.3.0 を 64kbit/s のディジタル専用線をアクセス回線とするフレームリレーで接続するための設定を説明します。

相手のネットワークへのルーティングはルーター同士の通信 (ダイナミックルーティング) で行います。
なお、通常は PP 側に IP アドレスを設定する必要はありません。これを Unnumbered といいます。相手側のルーターが IP アドレスを必要とする場合にだけ設定してください。
ディジタル専用線で LAN を接続する場合の設定と異なる事項は、カプセル化の種類をフレームリレー (**fr**) に指定する点です。

1. **line type** コマンドを使用して、回線種別を 64kbit/s ディジタル専用線に指定します。
2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。
3. **rip use** コマンドを使用して、rip を有効にします。
4. **pp select** コマンドを使用して、相手先情報番号を選択します。
5. **pp encapsulation** コマンドを使用して、PP 側のカプセル化の種類としてフレームリレーを設定します。
6. **ip pp rip send** コマンドを使用して、回線側に RIP2 を流すようにします。
7. **ip pp rip connect send** コマンドを使用して、回線接続時の RIP の送出を **ip pp rip connect interval** コマンドで設定されている時間間隔で行うように設定します。この時間間隔はデフォルトでは 30 秒です。
8. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。
9. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。
10. **interface reset** コマンドを使用して、回線のハードウェアを切り替えます。

10.2 フレームリレーで LAN を接続 (IP 、unnumbered, スタティックルーティング)

[構成図]



[ルーター A の設定手順]

```
# line type bri1 l64
# ip lan1 address 192.168.1.1/24
# ip route 192.168.2.0/24 gateway pp 1 dlci=16
# ip route 192.168.3.0/24 gateway pp 1 dlci=18
# pp select 1
pp1# pp bind bri1
pp1# pp encapsulation fr
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

[ルーター B の設定手順]

```
# line type bri1 l64
# ip lan1 address 192.168.2.1/24
# ip route 192.168.1.0/24 gateway pp 1 dlci=17
# ip route 192.168.3.0/24 gateway pp 1 dlci=20
# pp select 1
pp1# pp bind bri1
pp1# pp encapsulation fr
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

[ルーター C の設定手順]

```
# line type bri1 l64
# ip lan1 address 192.168.3.1/24
# ip route 192.168.1.0/24 gateway pp 1 dlci=19
# ip route 192.168.2.0/24 gateway pp 1 dlci=21
# pp select 1
pp1# pp bind bri1
pp1# pp encapsulation fr
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

[解説]

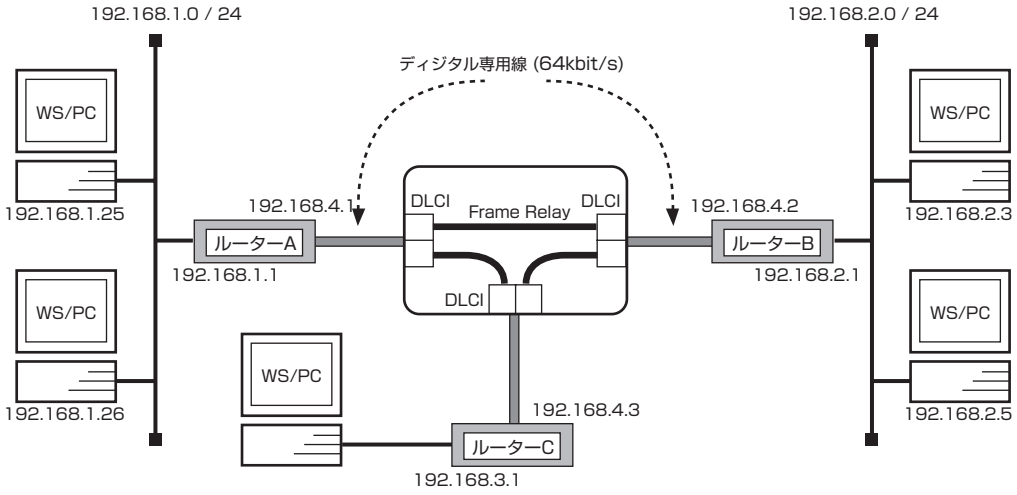
ネットワーク 192.168.1.0 とネットワーク 192.168.2.0 、ネットワーク 192.168.3.0 を 64kbit/s のディジタル専用線をアクセス回線とするフレームリレーで接続するための設定を説明します。

相手のネットワークへの経路情報はコマンドで設定する (スタティックルーティング) ことでそれぞれのルーターに与えます。相手のネットワークへのルーティングは、**ip route** コマンドにより、DLCI 値と IP アドレスを結び付けることで行います。
この設定例の場合、DLCI が分かっているので PP 側の IP アドレスを設定しなくてもルーティングが可能になります。

1. **line type** コマンドを使用して、回線種別を 64kbit/s ディジタル専用線に指定します。
2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。
3. **ip route** コマンドを使用して、相手側ルーターが接続しているネットワークへのスタティックな経路情報を設定します。
4. **pp select** コマンドを使用して、相手先情報番号を選択します。
5. **pp bind** コマンドを使用して、選択されている相手先情報番号と BRI 番号をバインドします。
6. **pp encapsulation** コマンドを使用して、PP 側のカプセル化の種類としてフレームリレーを設定します。
7. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。
8. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。
9. **interface reset** コマンドを使用して、回線のハードウェアを切り替えます。

10.3 フレームリレーで LAN を接続 (IP、numbered、RIP2)

[構成図]



[ルーター A の設定手順]

```
# line type bri1 l64
# ip lan1 address 192.168.1.1/24
# rip use on
# pp select 1
pp1# pp bind bri1
pp1# pp encapsulation fr
pp1# ip pp address 192.168.4.1/24
pp1# ip pp rip send on version 2
pp1# ip pp rip connect send interval
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

[ルーター B の設定手順]

```
# line type bri1 l64
# ip lan1 address 192.168.2.1/24
# rip use on
# pp select 1
pp1# pp bind bri1
pp1# pp encapsulation fr
pp1# ip pp address 192.168.4.2/24
pp1# ip pp rip send on version 2
pp1# ip pp rip connect send interval
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

[ルーター C の設定手順]

```
# line type bri1 l64
# ip lan1 address 192.168.3.1/24
# rip use on
# pp select 1
pp1# pp bind bri1
pp1# pp encapsulation fr
pp1# ip pp address 192.168.4.3/24
pp1# ip pp rip send on version 2
pp1# ip pp rip connect send interval
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

[解説]

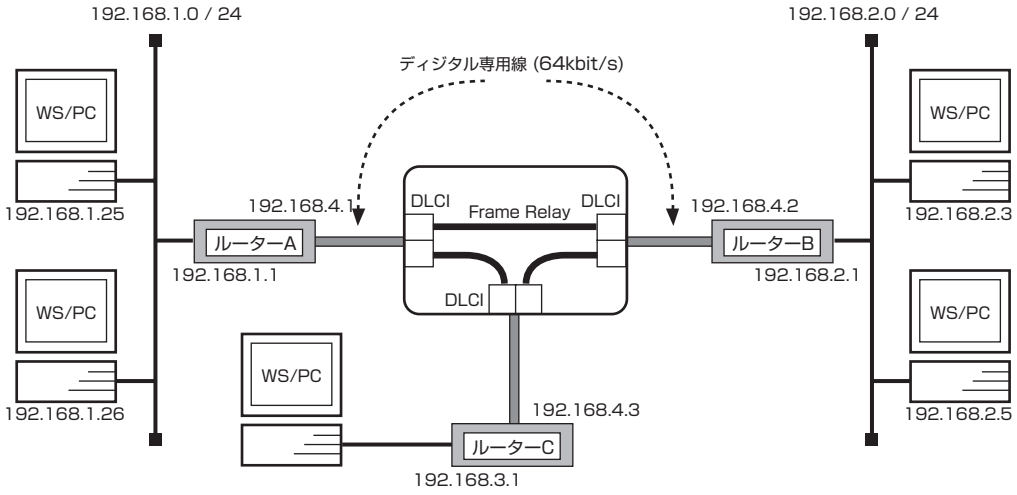
ネットワーク 192.168.1.0 とネットワーク 192.168.2.0 、ネットワーク 192.168.3.0 を 64kbit/s のディジタル専用線をアクセス回線とするフレームリレーで接続するための設定を説明します。

相手のネットワークへのルーティングはルーター同士の通信 (RIP2) で行います。
ディジタル専用線で LAN を接続する場合の設定と異なる事項は、カプセル化の種類をフレームリレー (**fr**) に指定する点です。

1. **line type** コマンドを使用して、回線種別を 64kbit/s ディジタル専用線に指定します。
2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。
3. **rip use** コマンドを使用して、rip を有効にします。
4. **pp select** コマンドを使用して、相手先情報番号を選択します。
5. **pp bind** コマンドを使用して、選択されている相手先情報番号と BRI 番号をバインドします。
6. **pp encapsulation** コマンドを使用して、PP 側のカプセル化の種類としてフレームリレーを設定します。
7. **ip pp address** コマンドを使用して、選択した PP 側のローカル IP アドレスとネットマスクを設定します。
8. **ip pp rip send** コマンドを使用して、回線側に RIP2 を流すように設定します。
9. **ip pp rip connect send** コマンドを使用して、回線接続時の RIP の送出を **ip pp rip connect interval** コマンドで設定されている時間間隔で行うように設定します。この時間間隔はデフォルトでは 30 秒です。
10. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。
11. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。
12. **interface reset** コマンドを使用して、回線のハードウェアを切り替えます。

10.4 フレームリレーで LAN を接続 (IP、numbered、スタティックルーティング)

[構成図]



[ルーター A の設定手順]

```
# line type bri1 l64
# ip lan1 address 192.168.1.1/24
# ip route 192.168.2.0/24 gateway 192.168.4.2
# ip route 192.168.3.0/24 gateway 192.168.4.3
# pp select 1
pp1# pp bind bri 1
pp1# pp encapsulation fr
pp1# ip pp address 192.168.4.1/24
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

[ルーター B の設定手順]

```
# line type bri1 l64
# ip lan1 address 192.168.2.1/24
# ip route 192.168.1.0 gateway 192.168.4.1
# ip route 192.168.3.0 gateway 192.168.4.3
# pp select 1
pp1# pp bind bri1
pp1# pp encapsulation fr
pp1# ip pp address 192.168.4.2/24
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

[ルーター C の設定手順]

```
# line type bri1 l64
# ip lan1 address 192.168.3.1/24
# ip route 192.168.1.0/24. gateway 192.168.4.1
# ip route 192.168.2.0/24. gateway 192.168.4.2
# pp select 1
pp1# pp bind bri1
pp1# pp encapsulation fr
pp1# ip pp address 192.168.4.3/24
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

[解説]

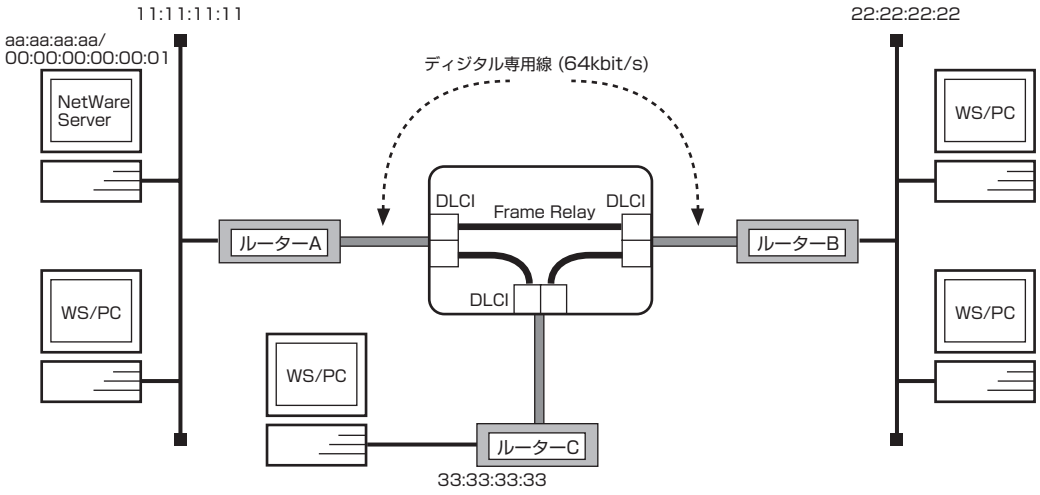
ネットワーク 192.168.1.0 とネットワーク 192.168.2.0 、ネットワーク 192.168.3.0 を 64kbit/s のディジタル専用線をアクセス回線とするフレームリレーで接続するための設定を説明します。

相手のネットワークへの経路情報はコマンドで設定する (スタティックルーティング) ことでそれぞれのルーターに与えます。このスタティックルーティングを設定するコマンド (**ip route**) において、gateway に指定されたアドレスは、InARP によって自動的に取得されます。InARP 機能を使用するか否かを設定する **fr inarp** コマンドのデフォルトは「使用する」ですので、上記設定手順に **fr inarp** コマンドは記述されていません。

1. **line type** コマンドを使用して、回線種別を 64kbit/s ディジタル専用線に指定します。
2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。
3. **ip route** コマンドを使用して、相手側ルーターが接続しているネットワーク へのスタティックな経路情報を設定します。
4. **pp select** コマンドを使用して、相手先情報番号を選択します。
5. **pp bind** コマンドを使用して、選択されている相手先情報番号と BRI 番号をバインドします。
6. **pp encapsulation** コマンドを使用して、PP 側のカプセル化の種類としてフレームリレーを設定します。
7. **ip pp address** コマンドを使用して、選択した PP のローカル IP アドレスとネットマスクを設定します。
8. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。
9. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。
10. **interface reset** コマンドを使用して、回線のハードウェアを切り替えます。

10.5 フレームリレーで LAN を接続 (IPX 、ダイナミックルーティング)

[構成図]



[ルーター A の設定手順]

```
# ipx routing on
# line type bri1 l64
# ipx lan1 network 11:11:11:11
# pp select 1
pp1# pp bind bri1
pp1# pp encapsulation fr
pp1# ipx pp routing on
pp1# ipx pp ripsap connect send interval
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

[ルーター B の設定手順]

```
# ipx routing on
# line type bri1 l64
# ipx lan1 network 22:22:22:22
# pp select 1
# pp bind bri1
pp1# pp encapsulation fr
pp1# ipx pp routing on
pp1# ipx pp ripsap connect send interval
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

[ルーター C の設定手順]

```
# ipx routing on
# line type bri1 l64
# ipx lan1 network 33:33:33:33
# pp select 1
pp1# pp bind bri1
pp1# pp encapsulation fr
pp1# ipx pp routing on
pp1# ipx pp ripsap connect send interval
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

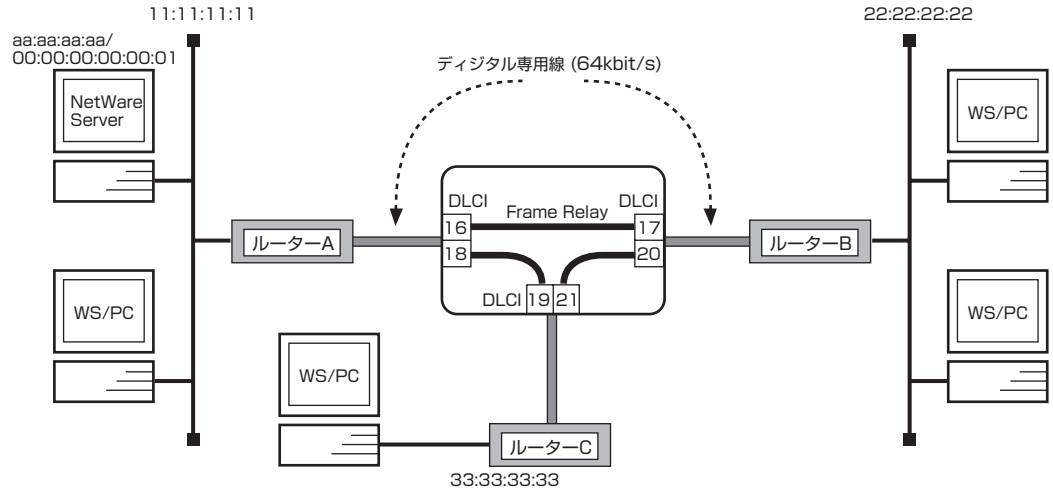
[解説]

ディジタル専用線で LAN を接続する場合の設定と異なる事項は、カプセル化の種類をフレームリレー (**fr**) に指定する点です。

1. **ipx routing** コマンドを使用して、IPX パケットのルーティングを可能にします。
2. **line type** コマンドを使用して、回線種別を 64kbit/s ディジタル専用線に指定します。
3. **ipx lan1 network** コマンドを使用して、LAN 側の IPX ネットワーク番号を設定します。
4. **pp select** コマンドを使用して、相手先情報番号を選択します。
5. **pp bind** コマンドを使用して、選択されている相手先情報番号と BRI 番号をバインドします。
6. **pp encapsulation** コマンドを使用して、PP 側のカプセル化の種類としてフレームリレーを設定します。
7. **ipx pp routing** コマンドを使用して、PP 側へのルーティングを可能にします。
8. **ipx pp ripsap connect send** コマンドを使用して、回線接続時の RIP/SAP の送出を **ipx pp ripsap connect interval** コマンドで設定されている時間間隔で行うように設定します。この時間間隔はデフォルトでは 60 秒です。
9. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。
10. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。
11. **interface reset** コマンドを使用して、回線のハードウェアを切り替えます。

10.6 フレームリレーで LAN を接続 (IPX 、スタティックルーティング)

[構成図]



[ルーター A の設定手順]

```
# ipx routing on
# line type bri1 l64
# ipx lan1 network 11:11:11:11
# pp select 1
pp1# pp bind bri1
pp1# pp encapsulation fr
pp1# ipx pp routing on
pp1# ipx pp route 22:22:22:22 dlci=16 1
pp1# ipx pp route 33:33:33:33 dlci=18 1
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

[ルーター B の設定手順]

```
# ipx routing on
# line type bri1 l64
# ipx lan1 network 22:22:22:22
# ipx sap file SERVER aa:aa:aa:aa 00:00:00:00:00:01 ncp 2
# pp select 1
# pp bind bri1
pp1# pp encapsulation fr
pp1# ipx pp routing on
pp1# ipx pp route 11:11:11:11 dlci=17 1
pp1# ipx pp route aa:aa:aa:aa dlci=17 2
pp1# ipx pp route 33:33:33:33 dlci=20 1
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

[ルーター C の設定手順]

```
# ipx routing on
# line type bri1 l64
# ipx lan1 network 33:33:33:33
# ipx sap file SERVER aa:aa:aa:aa 00:00:00:00:00:01 ncp 2
# pp select 1
# pp bind bri1
pp1# pp encapsulation fr
pp1# ipx pp routing on
pp1# ipx pp route 11:11:11:11 dlci=19 1
pp1# ipx pp route aa:aa:aa:aa dlci=19 2
pp1# ipx pp route 22:22:22:22 dlci=21 1
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

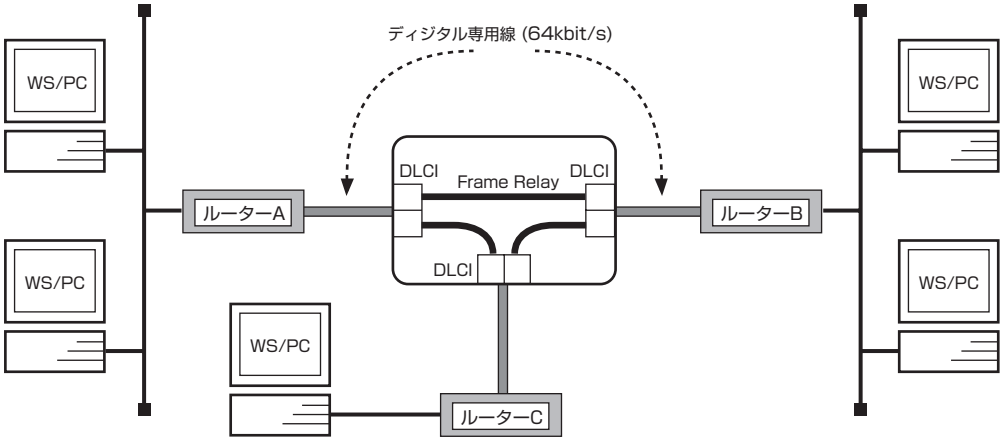
[解説]

ディジタル専用線で LAN を接続する場合の設定と異なる事項は、カプセル化の種類をフレームリレー (**fr**) に指定する点です。

1. **ipx routing** コマンドを使用して、IPX パケットのルーティングを可能にします。
2. **line type** コマンドを使用して、回線種別を 64kbit/s ディジタル専用線に指定します。
3. **ipx lan1 network** コマンドを使用して、LAN 側の IPX ネットワーク番号を設定します。
4. **pp select** コマンドを使用して、相手先情報番号を選択します。
5. **pp bind** コマンドを使用して、選択されている相手先情報番号と BRI 番号をバインドします。
6. **pp encapsulation** コマンドを使用して、PP 側のカプセル化の種類としてフレームリレーを設定します。
7. **ipx pp routing** コマンドを使用して、PP 側へのルーティングを可能にします。
8. **ipx pp route** コマンドを使用して、相手側ヤマハリモートルーターが接続しているネットワークへの経路情報を設定します。
9. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。
10. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。
11. **interface reset** コマンドを使用して、回線のハードウェアを切り替えます。

10.7 フレームリレーで LAN をブリッジ接続

[構成図]



[ルーター A, ルーター B, ルーター C の設定手順]

```
# line type bri1 l64
# bridge use on
# bridge group lan1 1
# pp select 1
pp1# pp bind bri1
pp1# pp encapsulation fr
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

[解説]

ネットワーク同士を 64kbit/s のディジタル専用線をアクセス回線とするフレームリレーでブリッジ接続するための設定を説明します。

この例では、IP パケットはブリッジングの対象とはなりません。IP パケットも同時にブリッジする場合には、**save** コマンド実行前に **ip routing off** を実行します。
ディジタル専用線で LAN を接続する場合の設定と異なる事項は、カプセル化の種類をフレームリレー (**fr**) に指定する点です。

1. **line type** コマンドを使用して、回線種別を 64kbit/s ディジタル専用線に指定します。
2. **bridge use** コマンドを使用して、ブリッジングを可能にします。
3. **bridge group** コマンドを使用して、ブリッジするインタフェースを指定します。
4. **pp select** コマンドを使用して、相手先情報番号を選択します。
5. **pp bind** コマンドを使用して、選択されている相手先情報番号と BRI 番号をバインドします。
6. **pp encapsulation** コマンドを使用して、PP 側のカプセル化の種類としてフレームリレーを設定します。
7. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。
8. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。
9. **interface reset** コマンドを使用して、回線のハードウェアを切り替えます。

11. DHCP 機能設定例

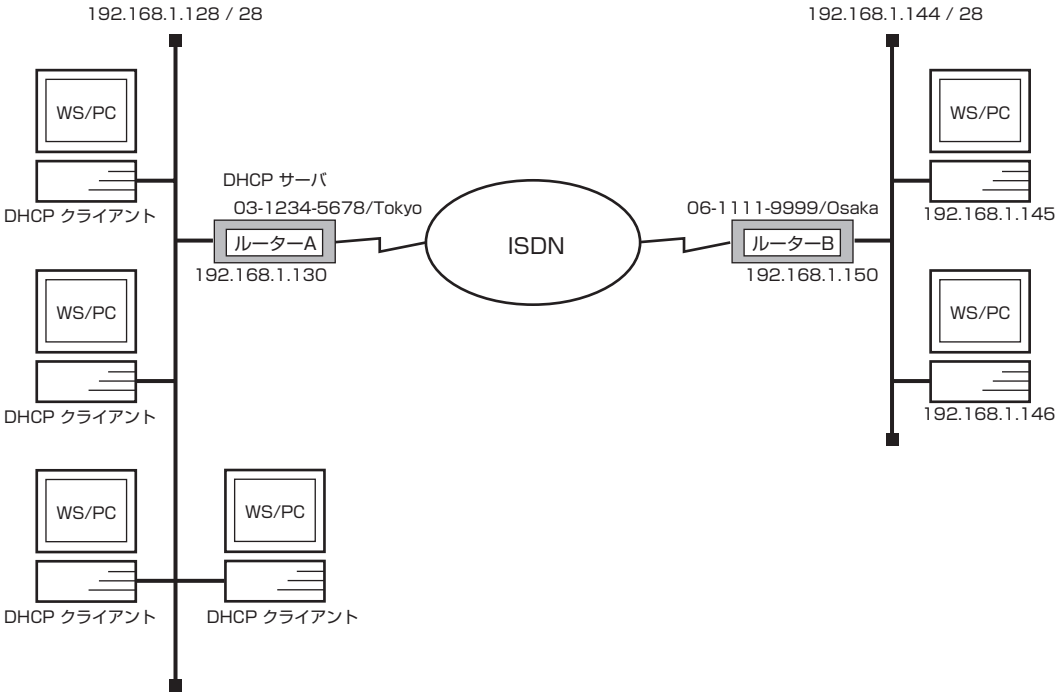
本章で説明するネットワーク接続の形態は、次のようになります。

1. ローカルネットワークでのみ DHCP サーバ機能を利用
2. 2 つのネットワークで DHCP 機能を利用
3. DHCP サーバからの WAN 側アドレスの取得（IP マスカレード使用）
4. DHCP サーバからの PP リモート側アドレスの取得

以下の説明では、それぞれのネットワークの接続形態例に対して構成図、手順、解説の順に行います。

11.1 ローカルネットワークでのみ DHCP サーバ機能を利用

[構成図]



[ルーター A の設定手順]

```
# isdn local address bri1 03-1234-5678/Tokyo
# ip lan1 address 192.168.1.130/28
# ip route 192.168.1.144/28 gateway pp 1
# dhcp scope 1 192.168.1.129-192.168.1.142/28 except 192.168.1.130
# dhcp service server
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 06-1111-9999/Osaka
pp1# pp enable 1
pp1# save
```

[ルーター B の設定手順]

```
# isdn local address bri1 06-1111-9999/Osaka
# ip lan1 address 192.168.1.150/28
# ip route 192.168.1.128/28 gateway pp 1
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 03-1234-5678/Tokyo
pp1# pp enable 1
pp1# save
```

[解説]
ルーター A を DHCP サーバとし、ネットワーク 192.168.1.128 に接続された DHCP クライアントに動的に IP アドレスを割り当てるための設定を説明します。
ISDN 回線で接続されるネットワーク 192.168.1.144 は DHCP の動作に関係しないため、ルーター B 側では DHCP に関する設定は必要ありません。

IP アドレス	割り当て
192.168.1.128	LAN 側のネットワーク
192.168.1.129	DHCP クライアント (1 台)
192.168.1.130	DHCP サーバルーターの LAN インタフェース
192.168.1.131 : 192.168.1.142	DHCP クライアント (12 台分)
192.168.1.143	LAN のブロードキャスト

■ルーター A
1. **isdn local address** コマンドを使用して、接続した BRI 番号と ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、"/" に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **ip route** コマンドを使用して、相手側ルーターが接続しているネットワークへのスタティックな経路情報を設定します。

4. **dhcp scope** コマンドを使用して、DHCP スコープを定義します。
この設定の場合、**gateway** キーワードによるパラメータ設定を省略しているので、ゲートウェイアドレスとしてはルーターの IP アドレスが DHCP クライアントへ通知されます。また、**expire, maxexpire** キーワードによるパラメータ設定を省略しているので IP アドレスのリース期間はデフォルト値の 72 時間になります。

5. **dhcp service** コマンドを使用して、DHCP サーバとして機能するように設定します。

6. **pp select** コマンドを使用して、相手先情報番号を選択します。

7. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

8. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、"/" に続けて入力します。

9. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

10. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

■ルーター B
1. **isdn local address** コマンドを使用して、ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、"/" に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **ip route** コマンドを使用して、相手側ルーターが接続しているネットワークへのスタティックな経路情報を設定します。

4. **pp select** コマンドを使用して、相手先情報番号を選択します。

5. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

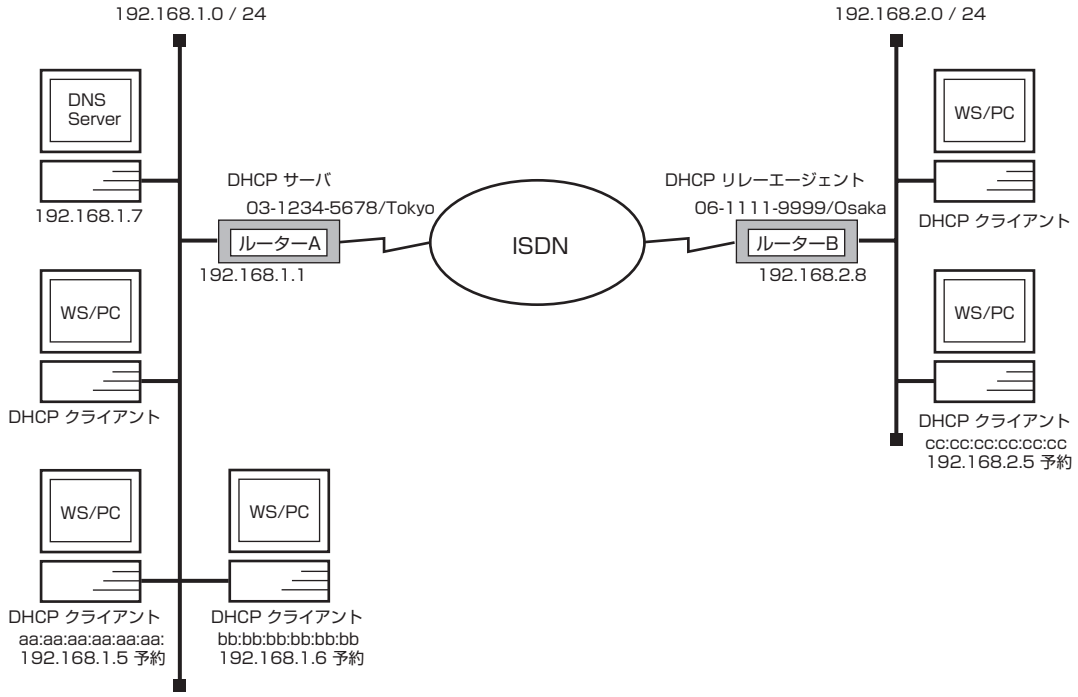
6. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、"/" に続けて入力します。

7. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

8. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

11.2 2つのネットワークで DHCP 機能を利用

［構成図］



［ルーター A の設定手順］

```
# isdn local address bri1 03-1234-5678/Tokyo
# ip lan1 address 192.168.1.1/24
# ip route 192.168.2.0/24 gateway pp 1
# dhcp scope 1 192.168.1.2-192.168.1.64/24 except 192.168.1.7
# dhcp scope 2 192.168.2.1-192.168.2.32/24 except 192.168.2.8 gateway 192.168.2.8
# dhcp scope bind 1 192.168.1.5 aa:aa:aa:aa:aa:aa
# dhcp scope bind 1 192.168.1.6. ethernet bb:bb:bb:bb:bb:bb
# dhcp scope bind 2 192.168.2.5. ethernet cc:cc:cc:cc:cc:cc
# dns server 192.168.1.7
# dhcp service server
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 06-1111-9999/Osaka
pp1# pp enable 1
pp1# save
```

[ルーター B の設定手順]

```
# isdn local address bri1 06-1111-9999/Osaka
# ip lan1 address 192.168.2.8/24
# ip route 192.168.1.0/24 gateway pp 1
# dhcp relay server 192.168.1.1
# dhcp service relay
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 03-1234-5678/Tokyo
pp1# pp enable 1
pp1# save
```

[解説]

ルーター A を DHCP サーバとし、ネットワーク 192.168.1.0 とネットワーク 192.168.2.0 に接続された DHCP クライアントに動的および固定的に IP アドレスを割り当てるための設定を説明します。
ISDN 回線で接続されるネットワーク 192.168.2.0 のルーター B は DHCP リレーエージェントとして機能する必要があります。また、ネットワーク上の DNS サーバ等の IP アドレスへの割当を行わないように DHCP スコープから必ず除外します。

IP アドレス	割り当て	スコープ
192.168.1.0	LAN 側のネットワーク	−
192.168.1.1	DHCP サーバルーターの LAN インタフェース	−
192.168.1.2 : 192.168.1.6	DHCP クライアント (5 台分)	1
192.168.1.7	DNS サーバ	−
192.168.1.8 : 192.168.1.64	DHCP クライアント (57 台分)	1
192.168.1.65 : 192.168.1.254	ホスト (190 台分)	−
192.168.1.255	LAN のブロードキャスト	−
192.168.2.0	LAN 側のネットワーク	−
192.168.2.1 : 192.168.2.7	DHCP クライアント (7 台分)	2
192.168.2.8	DHCP リレーエージェントルーターの LAN インタフェース	−
192.168.2.9 : 192.168.2.32	DHCP クライアント (24 台分)	2
192.168.2.33 : 192.168.2.254	ホスト (222 台分)	−
192.168.2.255	LAN のブロードキャスト	−

■ルーター A

1. **isdn local address** コマンドを使用して、接続した BRI 番号と ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/”に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **ip route** コマンドを使用して、相手側ルーターが接続しているネットワーク へのスタティックな経路情報を設定します。

4. **dhcp scope** コマンドを使用して、DHCP スコープを定義します。
スコープ 1 の設定の場合、DHCP サーバとなるルーターと同じネットワークであり、**gateway** キーワードによるパラメータ設定を省略しているので、ゲートウェイアドレスとしてはルーターの IP アドレスが DHCP クライアントへ通知されます。また、**expire, maxexpire** キーワードによるパラメータ設定を省略しているので IP アドレスのリース期間はデフォルト値の 72 時間になります。

5. **dhcp scope bind** コマンドを使用して、DHCP 予約アドレスを設定します。

6. **dns server** コマンドを使用して、DNS サーバの IP アドレスを設定します。

7. **dhcp service** コマンドを使用して、DHCP サーバとして機能するように設定します。

8. **pp select** コマンドを使用して、相手先情報番号を選択します。

9. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

10. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/”に続けて入力します。

11. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

12. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

■ルーター B

1. **isdn local address** コマンドを使用して、ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/”に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **ip route** コマンドを使用して、相手側ルーターが接続しているネットワーク へのスタティックな経路情報を設定します。

4. **dhcp relay server** コマンドを使用して、DHCP サーバの IP アドレスを設定します。

5. **dhcp service** コマンドを使用して、DHCP リレーエージェントとして機能するように設定します。

6. **pp select** コマンドを使用して、相手先情報番号を選択します。

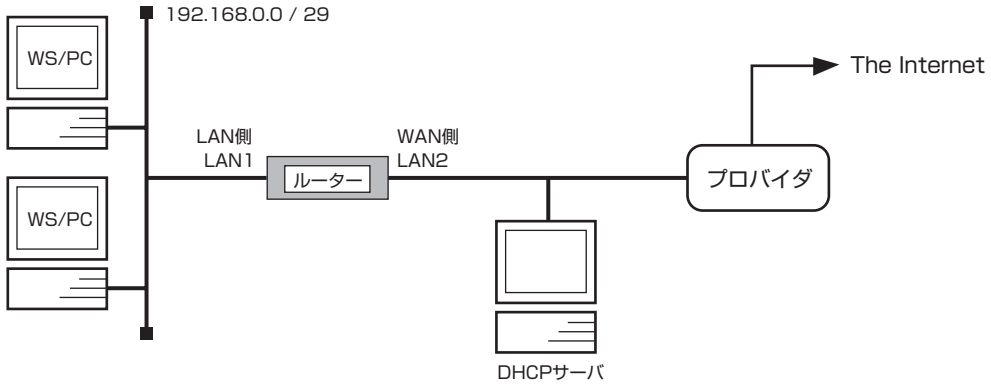
7. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/”に続けて入力します。

8. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

9. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

11.3 DHCP サーバからの WAN 側アドレスの取得（IP マスカレード使用）

[構成図]



[設定手順]

```
# ip lan1 address 192.168.0.1/24
# ip lan2 address dhcp
# nat descriptor type 1 masquerade
# nat descriptor address outer 1 primary
# ip lan2 nat descriptor 1
# ip route default gateway dhcp lan2
# save
```

[解説]

LAN1 側にプライベートアドレスのネットワークを構築し、LAN2 側で DHCP で得られるグローバルアドレスを使った IP マスカレードにより、LAN1 側からインターネットに接続します。CATV 事業者のインターネット接続で使用される場合がある形態です。

1. # ip lan1 address 192.168.0.1/24
   LAN1 側にはプライベートアドレスネットワークを構築します。

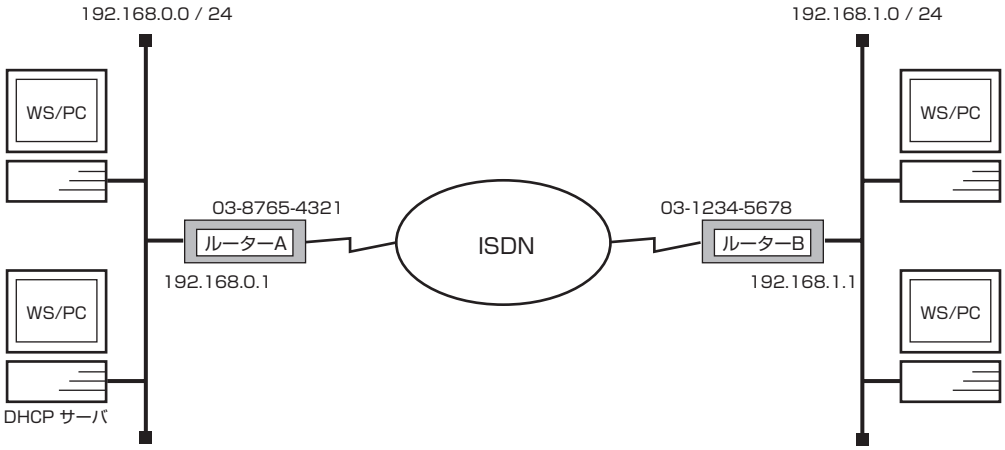
2. # ip lan2 address dhcp
   LAN2 側では DHCP サーバから取得するアドレスを使用します。DHCP サーバへのアドレスの要求はコマンド入力時や起動時になされます。アドレス取得に失敗した場合は ip lan2 dhcp retry コマンドの設定に従って取得を試みます。

3. # nat descriptor type 1 masquerade
   # nat descriptor address outer 1 primary
   # ip lan2 nat descriptor 1
   LAN2 に対して IP マスカレードを適用します。外側アドレスはプライマリアドレスとして指定し、DHCP で得られるアドレスを使用します。

4. # ip route default gateway dhcp lan2
   # save
   必要に応じて経路情報を設定します。この例の場合、デフォルトルートを DHCP で得られるゲートウェイに向けています。

11.4 DHCP サーバからの PP リモート側アドレスの取得

[構成図]



[ルーター A の設定手順]

```
# isdn local address bri1 0387654321
# ip lan1 address 192.168.0.1/24
# ip lan1 proxyarp on
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 0312345678
pp1# ip pp remote address dhcpc lan1
pp1# pp enable 1
pp1# save
```

[ルーター B の設定手順]

```
# isdn local address bri1 0312345678
# ip lan1 address 192.168.1.1/24
# ip route default gateway pp 1
# nat descriptor type 1 masquerade
# pp select 1
pp1# pp bind bri1
pp1# ip pp nat descriptor 1
pp1# isdn remote address call 0387654321
pp1# ppp ipcp ipaddress on
pp1# pp enable 1
pp1# save
```

[解説]

ルーター B がルーター A に ISDN で接続する時に IPCP で得るアドレスを、ルーター A が LAN 側にある DHCP サーバから得ます。

1.
```
# isdn local address bri1 0387654321
# ip lan1 address 192.168.0.1/24
# ip lan1 proxyarp on
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 0312345678
```
回線接続に必要な情報を設定します。

2. pp1# ip pp remote address dhcpc lan1
   pp1# pp enable 1
   ルーター A 側では pp 側のリモートアドレスを LAN1 にある DHCP サーバから得ます。DHCP サーバへのアドレスの要求はコマンド入力時や起動時になされます。アドレス取得に失敗した場合は ip lan1 dhcp retry コマンドの設定に従って取得を試みます。

3. # isdn local address bri1 0312345678
   # ip lan1 address 192.168.1.1/24
   # ip route default gateway pp 1
   # nat descriptor type 1 masquerade
   # pp select 1
   pp1# pp bind bri1
   pp1# ip pp nat descriptor 1
   pp1# isdn remote address call 0387654321
   pp1# ppp ipcp ipaddress on
   pp1# pp enable 1
   pp1# save
   ルーター B 側では接続時に IPCP でアドレスを得るよう設定します。またこの例では、得られた IP アドレスを IP マスカレードで使用します。詳しい設定内容は、IP マスカレード機能による端末型ダイヤルアップ接続の設定例などを参考にしてください。

12. PRI 設定例

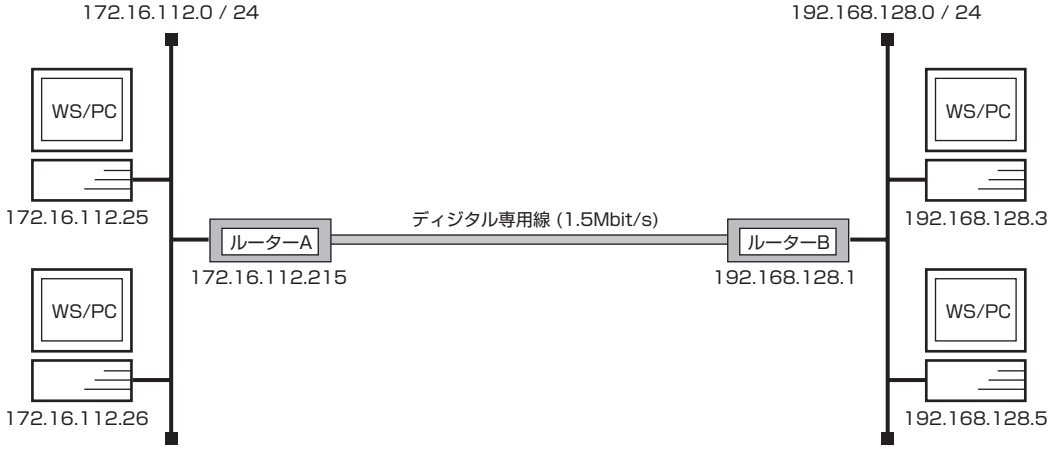
本章では、PRI(一次群速度インタフェース) の設定方法について説明します。セキュリティの設定や、詳細な各種パラメータなどの付加的な設定に関しては、個々のネットワークの運営方針などに基づいて行ってください。
本章で説明するネットワーク接続の形態は、次のようになります。

1. 1.5Mbit/s ディジタル専用線で LAN を接続
2. 専用線を ISDN 回線でバックアップ
3. PRI モジュールを用いたダイヤルアップ接続 (RADIUS による認証）(RT300i)

以下の説明では、それぞれのネットワークの接続形態例に対して構成図、手順、解説の順に行います。
構成図説明するネットワークの構成を図示します。
手順設定すべきルーターの設定手順だけをコンソール入力のイメージで表します。設定操作画面の例は、管理ユーザとしてアクセスを開始した直後からになっています。

12.1 1.5Mbit/s ディジタル専用線で LAN を接続

[構成図]



[ルーター A の設定手順]

```
# pri leased channel 1/1 1 24
# ip lan1 address 172.16.112.215/24
# pp select 1
pp1# pp bind pri1/1
pp1# ip route 192.168.128.0/24 gateway pp 1
pp1# pp enable 1
pp1# save
```

[ルーター B の設定手順]

```
# pri leased channel 1/1 1 24
# ip lan1 address 192.168.128.1/24
# pp select 1
pp1# pp bind pri1/1
pp1# ip route 172.16.112.0/24 gateway pp 1
pp1# pp enable 1
pp1# save
```

[解説]

ネットワーク 172.16.112.0 とネットワーク 192.168.128.0 を 1.5Mbit/s のディジタル専用線で接続するための設定を説明します。

相手のネットワークへの経路情報はコマンドで設定する（スタティックルーティング）ことでそれぞれのルーターに与えます。
なお、通常は PP 側に IP アドレスを設定する必要はありません。これを Unnumbered といいます。相手側のルーターが IP アドレスを必要とする場合にだけ設定してください。
2 台のヤマハリモートルーターの設定手順は全く同じで、IP アドレスなどのコマンドのパラメータだけが異なります。

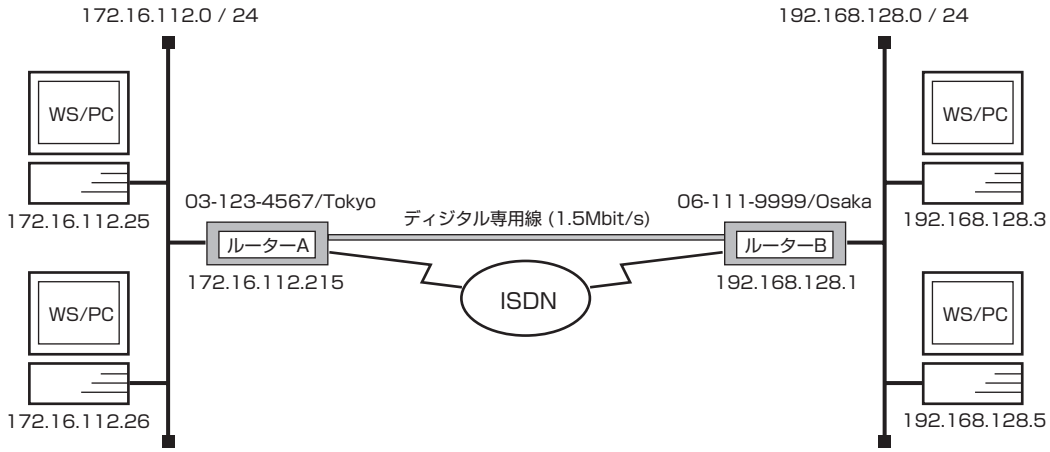
1. **pri leased channel** コマンドを使用して、PRI の情報チャネルとタイムスロットを設定します。
2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。
3. **pp select** コマンドを使用して、相手先情報番号を選択します。
4. **pp bind pri** コマンドを使用して、選択した相手先情報番号と PRI 情報チャネルをバインドします。
5. **ip route** コマンドを使用して、相手側ヤマハリモートルーターが接続している LAN へのスタティックルーティング情報を設定します。

6. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

7. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

12.2 専用線を ISDN 回線でバックアップ

[構成図]



[ルーター A の設定手順]

```
# pri leased channel 1/1 1 24
# isdn local address bri1 0312345678/Tokyo
# ip lan1 address 172.16.112.215/24
# pp select 1
pp1# pp bind pri1/1
pp1# ip route 192.168.128.0/24 gateway pp 1
pp1# pp keepalive use lcp-echo
pp1# leased backup 2
pp1# pp enable 1
pp1# pp select 2
pp2# pp bind bri1
pp2# isdn remote address call 0611119999/Osaka
pp2# isdn call block time 15
pp2# pp enable 2
pp2# save
```

[ルーター B の設定手順]

```
# pri leased channel 1/1 1 24
# isdn local address bri1 0611119999/Osaka
# ip lan1 address 192.168.128.1/24
# pp select 1
pp1# pp bind pri1/1
pp1# ip route 172.16.112.0/24 gateway pp 1
pp1# pp keepalive use lcp-echo
pp1# leased backup 2
pp1# pp enable 1
pp1# pp select 2
pp2# pp bind bri1
pp2# isdn remote address call 0312345678/Tokyo
pp2# isdn call block time 15
pp2# pp enable 2
pp2# save
```

[解説]
ネットワーク 172.16.112.0 とネットワーク 192.168.128.0 を 1.5Mbit/s のディジタル専用線で接続し、この専用線がダウンした時は ISDN 回線でバックアップするための設定を説明します。

2 台のヤマハリモートルーターの設定手順は全く同じで、ISDN 番号や IP アドレスなどのコマンドのパラメータだけが異なります。

1. **pri leased channel** コマンドを使用して、PRI の情報チャネルとタイムスロットを設定します。

2. **isdn local address** コマンドを使用して、接続した BRI 番号と ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

3. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

4. **pp select** コマンドを使用して、相手先情報番号を選択します。

5. **pp bind pri** コマンドを使用して、選択した相手先情報番号と PRI 情報チャネルをバインドします。

6. **ip route** コマンドを使用して、相手側ヤマハリモートルーターが接続している LAN へのスタティックルーティング情報を設定します。

7. **pp keepalive use** コマンドを使用して、専用線キープアライブを使用するように設定します。

8. **leased backup** コマンドを使用して、バックアップする際の相手先情報番号を指定します。

9. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

10. **pp select** コマンドを使用して、相手先情報番号を選択します。

11. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

12. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

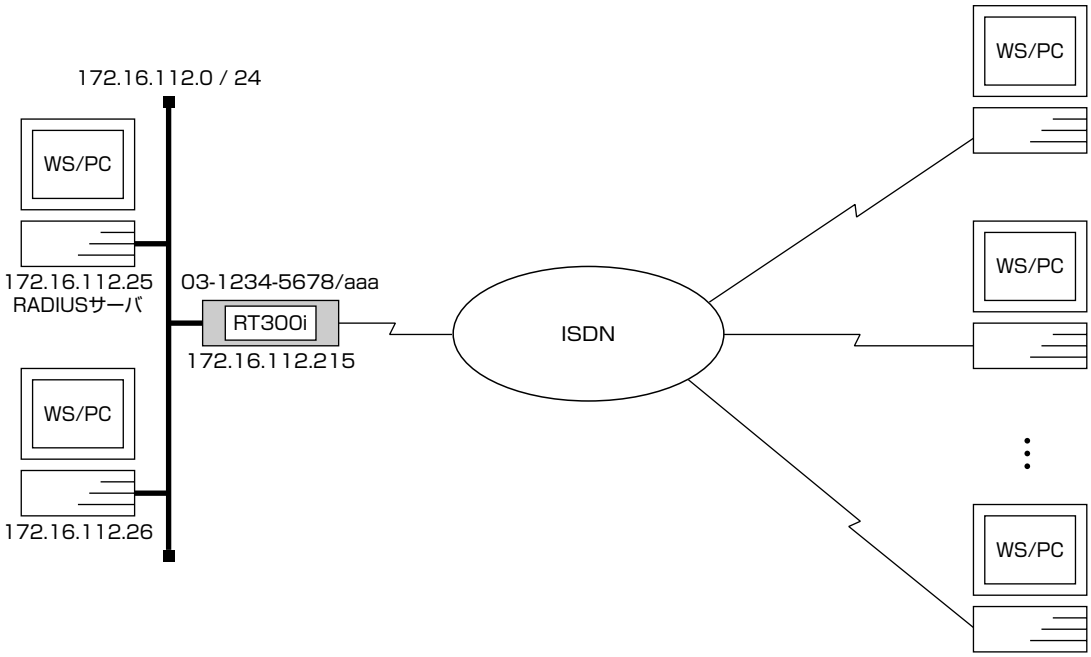
13. **isdn call block time** コマンドを使用して、ISDN 回線への再発信抑制タイマを設定します。
このコマンドは必須ではありませんが、専用線ダウンの検出タイミングが双方のルーターで異なった場合に起こる無駄な発信を抑えられる場合があります。

14. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

15. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

12.3 PRI モジュールを用いたダイヤルアップ接続 (RADIUS による認証) (RT300i)

[構成図]



[設定手順]

```
# line type pri1 isdn
# isdn local address pri1 03-1234-5678/aaa
# ip lan1 address 172.16.112.215/24
# radius auth on
# radius server 172.16.112.25
# radius secret himitsu
# pp select anonymous
anonymous# pp bind pri1
anonymous# pp auth request chap
anonymous# pp enable anonymous
anonymous# save
anonymous# interface reset pri1
```

[解説]

RT300i の拡張スロット 1 に装着した多重化対応の PRI 拡張モジュール (YBA-1PRI-M) と INS ネット 1500 を用いて、不特定の TA や PHS 端末などからのダイヤルアップ接続を受けます。

ユーザの認証、端末側の IP アドレスの管理などは RADIUS サーバで行います。

1. **line type** コマンドを使って **pri1** の回線種別を **isdn** に設定します。
2. **isdn local address** コマンドを使って本機の ISDN 番号を設定します。**aaa** はサブアドレスです。
3. **ip lan1 address** コマンドを使って LAN 側の IP アドレスとネットマスクを設定します。
4. **radius auth** コマンドを使って anonymous のユーザの情報を RADIUS サーバに問い合わせるようにします。
5. **radius server** コマンドを使って RADIUS サーバの IP アドレスを指定します。
6. **radius secret** コマンドを使って RADIUS シークレットを設定します。
7. **pp select** コマンドを使って相手先に anonymous を選択します。

8. **pp bind** コマンドを使って選択した相手先情報番号に PRI ポートをバインドします。

9. **pp auth request** コマンドを使って PPP の認証に CHAP を使用するように設定します。

10. **pp enable** コマンドを使って PP 側のインタフェースを有効にします。このコマンドの実行直後にインタフェースは有効になります。

11. **save** コマンドを使って設定を内蔵の不揮発性メモリに書き込みます。

12. **interface reset** コマンドを使って回線種別の変更されたポートをリセットします。**restart** コマンドを使って、ルーターを再起動させても回線種別は切り替わります。

13. IPsec 機能設定例

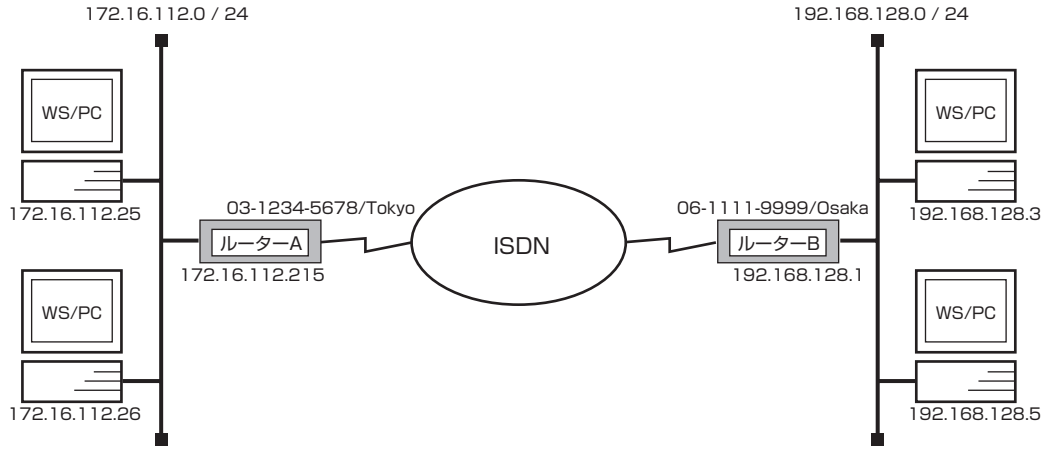
本章で説明するネットワーク接続の形態は、次のようになります。

1. トンネルモードを利用して LAN を接続
2. トランスポートモードの利用
3. ダイヤルアップ VPN

以下の説明では、それぞれのネットワークの接続形態例に対して構成図、手順、解説の順に行います。

13.1 トンネルモードを利用して LAN を接続

［構成図］



［ルーター A の設定手順］

```
# isdn local address bri1 03-1234-5678/Tokyo
# ip lan1 address 172.16.112.215/24
# ip route 192.168.128.1 gateway pp 1
# ip route 192.168.128.0/24 gateway tunnel 1
# ipsec ike pre-shared-key 1 text himitsu
# ipsec ike remote address 1 192.168.128.1
# ipsec sa policy 101 1 esp des-cbc md5-hmac
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 06-1111-9999/Osaka
pp1# pp enable 1
pp1# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel enable 1
tunnel1# ipsec auto refresh on
tunnel1# save
```

[ルーター B の設定手順]

```
# isdn local address bri1 06-1111-9999/Osaka
# ip lan1 address 192.168.128.1/24
# ip route 172.16.112.215 gateway pp 1
# ip route 172.16.112.0/24 gateway tunnel 1
# ipsec ike pre-shared-key 1 text himitsu
# ipsec ike remote address 1 172.16.112.215
# ipsec sa policy 101 1 esp des-cbc md5-hmac
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 03-1234-5678/Tokyo
pp1# pp enable 1
pp1# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel enable 1
tunnel1# ipsec auto refresh on
tunnel1# save
```

[解説]

ネットワーク 172.16.128.0 とネットワーク 192.168.128.0 を ISDN 回線で接続し、回線上を流れる双方向の IP パケットを IPsec で暗号化するための設定を説明します。
セキュリティ・ゲートウェイへの鍵交換のためのパケットまでトンネルしないように、セキュリティ・ゲートウェイの IP アドレスだけホストルートにより指定している点に注意してください。

■ルーター A

1. **isdn local address** コマンドを使用して、接続した BRI 番号と ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/”に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **ip route** コマンドを使用して、相手側のセキュリティ・ゲートウェイへのスタティックな経路情報を設定します。

4. **ip route** コマンドを使用して、相手側のセキュリティ・ゲートウェイが接続しているネットワークへのスタティックなトンネル経路情報を設定します。

5. **ipsec ike pre-shared-key** コマンドを使用して、相手側のセキュリティ・ゲートウェイに対する事前共有鍵を設定します。

6. **ipsec ike remote address** コマンドを使用して、鍵交換要求を受け付けるセキュリティ・ゲートウェイを設定します。

7. **ipsec sa policy** コマンドを使用して、相手側のセキュリティ・ゲートウェイに対する SA のポリシーを設定します。

8. **pp select** コマンドを使用して、相手先情報番号を選択します。

9. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

10. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/”に続けて入力します。

11. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

12. **tunnel select** コマンドを使用して、トンネルインタフェース番号を選択します。

13. **ipsec tunnel** コマンドを使用して、使用する SA のポリシーを設定します。

14. **tunnel enable** コマンドを使用して、トンネルインタフェースを有効にします。

15. **ipsec auto refresh** コマンドを使用して、SA を自動更新するように設定します。このコマンドを実行した直後に、新しい SA が生成されます。

16. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

■ルーター B

1. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/”に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **ip route** コマンドを使用して、相手側のセキュリティ・ゲートウェイへのスタティックな経路情報を設定します。

4. **ip route** コマンドを使用して、相手側のセキュリティ・ゲートウェイが接続しているネットワークへのスタティックなトンネル経路情報を設定します。

5. **ipsec ike pre-shared-key** コマンドを使用して、相手側のセキュリティ・ゲートウェイに対する事前共有鍵を設定します。

6. **ipsec ike remote address** コマンドを使用して、鍵交換要求を受け付けるセキュリティ・ゲートウェイを設定します。

7. **ipsec sa policy** コマンドを使用して、相手側のセキュリティ・ゲートウェイに対する SA のポリシーを設定します。

8. **pp select** コマンドを使用して、相手先情報番号を選択します。

9. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

10. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/”に続けて入力します。

11. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

12. **tunnel select** コマンドを使用して、トンネルインタフェース番号を選択します。

13. **ipsec tunnel** コマンドを使用して、使用する SA のポリシーを設定します。

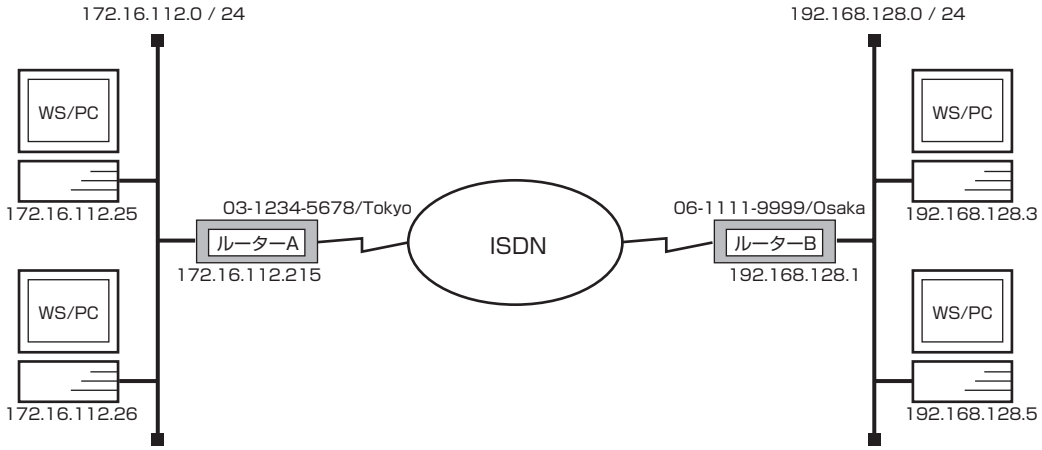
14. **tunnel enable** コマンドを使用して、トンネルインタフェースを有効にします。

15. **ipsec auto refresh** コマンドを使用して、SA を自動更新するように設定します。このコマンドを実行した直後に、新しい SA が生成されます。

16. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

13.2 トランスポートモードの利用

［構成図］



［ルーター A の設定手順］

```
# isdn local address bri1 03-1234-5678/Tokyo
# ip lan1 address 172.16.112.215/24
# ip route 192.168.128.0/24 gateway pp 1
# ipsec ike pre-shared-key 1 text himitsu
# ipsec ike remote address 1 192.168.128.1
# ipsec sa policy 102 1 esp des-cbc sha-hmac
# ipsec transport 1 102 tcp * telnet
# ipsec transport 2 102 tcp telnet *
# security class 1 on on
#pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 06-1111-9999/Osaka
pp1# pp enable 1
pp1# ipsec auto refresh on
pp1# save
```

[ルーター B の設定手順]

```
# isdn local address bri1 06-1111-9999/Osaka
# ip lan1 address 192.168.128.1/24
# ip route 172.16.112.0/24 gateway pp 1
# ipsec ike pre-shared-key 1 text himitsu
# ipsec ike remote address 1 172.16.112.215
# ipsec sa policy 102 1 esp des-cbc sha-hmac
# ipsec transport 1 102 tcp * telnet
# ipsec transport 2 102 tcp telnet *
# security class 1 on on
# pp select 1
pp1# isdn remote address call 03-1234-5678/Tokyo
pp1# pp enable 1
pp1# ipsec auto refresh on
pp1# save
```

[解説]

IP アドレス 172.16.112.215 のルーター A と IP アドレス 192.168.128.1 のルーター B が双方向で TELNET で通信する時に、IPsec によるトランスポートモードで暗号化を行うための設定を説明します。
これらのセキュリティ・ゲートウェイの IP アドレスを除く、その他のホストへのルーティングは暗号化しないものと仮定しています。

■ルーター A

1. **isdn local address** コマンドを使用して、接続した BRI 番号と ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/”に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **ip route** コマンドを使用して、相手側のセキュリティ・ゲートウェイが接続しているネットワーク へのスタティックな経路情報を設定します。

4. **ipsec ike pre-shared-key** コマンドを使用して、相手側のセキュリティ・ゲートウェイに対する事前共有鍵を設定します。

5. **ipsec ike remote address** コマンドを使用して、鍵交換要求を受け付けるセキュリティ・ゲートウェイを設定します。

6. **ipsec sa policy** コマンドを使用して、相手側のセキュリティ・ゲートウェイに対する SA のポリシーを設定します。

7. **ipsec transport** コマンドを使用して、 トランスポートモードを定義します。

8. **security class** コマンドを使用して、TELNET を使用可能に設定します。

9. **pp select** コマンドを使用して、相手先情報番号を選択します。

10. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

11. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/”に続けて入力します。

12. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

13. **ipsec auto refresh** コマンドを使用して、SA を自動更新するように設定します。このコマンドを実行した直後に、新しい SA が生成されます。

14. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

■ルーター B

1. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

2. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。

3. **ip route** コマンドを使用して、相手側のセキュリティ・ゲートウェイが接続しているネットワークへのスタティックな経路情報を設定します。

4. **ipsec ike pre-shared-key** コマンドを使用して、相手側のセキュリティ・ゲートウェイに対する事前共有鍵を設定します。

5. **ipsec ike remote address** コマンドを使用して、鍵交換要求を受け付けるセキュリティ・ゲートウェイを設定します。

6. **ipsec sa policy** コマンドを使用して、相手側のセキュリティ・ゲートウェイに対する SA のポリシーを設定します。

7. **ipsec transport** コマンドを使用して、トランスポートモードを定義します。

8. **security class** コマンドを使用して、TELNET を使用可能に設定します。

9. **pp select** コマンドを使用して、相手先情報番号を選択します。

10. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。

11. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

12. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

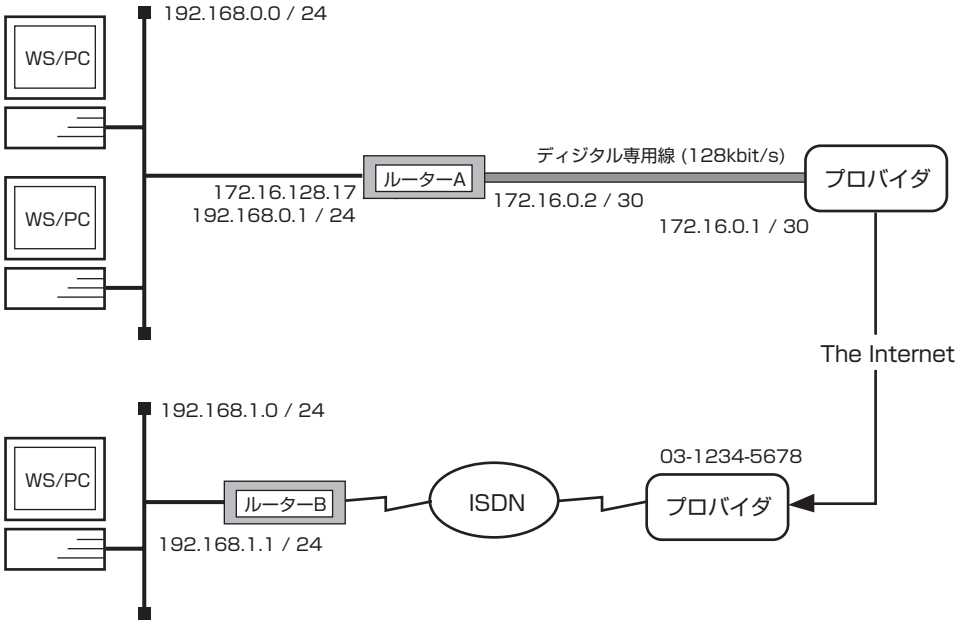
13. **ipsec auto refresh** コマンドを使用して、SA を自動更新するように設定します。このコマンドを実行した直後に、新しい SA が生成されます。

14. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

13.3 ダイヤルアップ VPN

片側が IP アドレスの変化するダイヤルアップ環境の場合でも、VPN を構築することが可能です。相手先識別子として IP アドレスではなく名前を用います。またこの場合、鍵交換は常にダイヤルアップ側から行われることになります。

[構成図]



[ルーター A 側]

・プロバイダと専用線接続
・プロバイダから割り当てられた IP アドレス範囲：172.16.128.16/28
・ルーター A の LAN 側 IP アドレス：172.16.128.17/28
・ルーター A の回線側 IP アドレス ：172.16.0.2/30
・ルーター A の回線対向側 IP アドレス：172.16.0.1/30
・ルーター B の LAN とは VPN で通信、その他は NAT 使用
・LAN 側ネットワークアドレス：192.168.0.0/24

[ルーター B 側]

・プロバイダにダイヤルアップ接続
・接続時にグローバルアドレス取得
・ルーター A の LAN とは VPN で通信、その他は IP マスカレードを使ってインターネットに接続
・LAN 側ネットワークアドレス：192.168.1.0/24

[ルーター A の設定手順]

```
# line type bri1 l128
# ip lan1 address 172.16.128.17/28
# ip lan1 secondary address 192.168.0.1/24
# nat descriptor type 1 nat-masquerade
# nat descriptor address outer 1 172.16.128.18-172.16.128.30
# nat descriptor address inner 1 192.168.0.1-192.168.0.254
# pp select 1
pp1# pp bind bri1
pp1# ip pp nat descriptor 1
pp1# ip pp address 172.16.0.2/30
pp1# ip pp remote address 172.16.0.1
pp1# ip route default gateway pp 1
pp1# pp enable 1
pp1# pp select none
# ipsec ike pre-shared-key 1 text secret
# ipsec ike remote address 1 any
# ipsec ike remote name 1 routerB
# ipsec sa policy 101 1 esp des-cbc md5-hmac
# tunnel select 1
tunnel1# ip route 192.168.1.0/24 gateway tunnel 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel enable 1
tunnel1# ipsec auto refresh on
tunnel1# tunnel select none
# save
# interface reset bri1
```

[ルーター B の設定手順]

```
# ip lan1 address 192.168.1.1/24
# nat descriptor type 1 masquerade
# nat descriptor masquerade static 1 1 192.168.1.1 udp 500
# nat descriptor masquerade static 1 2 192.168.1.1 esp *
# pp select 1
pp1# pp bind bri1
pp1# ip pp nat descriptor 1
pp1# isdn remote address call 0312345678
pp1# pp auth accept chap
pp1# pp auth myname userB passB
pp1# ppp ipcp ipaddress on
pp1# ip route default gateway pp 1
pp1# pp enable 1
pp1# pp select none
# ipsec ike local address 1 192.168.1.1
# ipsec ike local name 1 routerB
# ipsec ike remote address 1 172.16.0.2
# ipsec ike pre-shared-key 1 text secret
# ipsec sa policy 101 1 esp des-cbc md5-hmac
# tunnel select 1
tunnel1# ip route 192.168.0.0/24 gateway tunnel 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel enable 1
tunnel1# ipsec auto refresh on
tunnel1# tunnel select none
# save
```

[解説]

■ルーター A

1. # line type bri1 l128
   回線種別を設定します。この設定はインタフェースリセット
   あるいは装置の再起動を行った後に有効になります。

2. # ip lan1 address 172.16.128.17/28
   # ip lan1 secondary address 192.168.0.1/24
   回線側から RT に直接グローバルアドレスでアクセスする目的でプライマリアドレスにはグローバルアドレスを設定します。
   またプロバイダから与えられたグローバルアドレス数が LAN 側のホスト数に対して少ないため、セカンダリアドレスで別ネットワークを設定し、NAT でグローバルアドレスに変換します。

3. # nat descriptor type 1 nat-masquerade
   # nat descriptor address outer 1 172.16.128.18-172.16.128.30
   # nat descriptor address inner 1 192.168.0.1-192.168.0.254
   # pp select 1
   pp1# pp bind bri1
   pp1# ip pp nat descriptor 1
   回線側に適用する NAT ディスクリプタを設定します。外側アドレスにはプロバイダから与えられたグローバルアドレスを、内側アドレスには LAN 側のセカンダリネットワークアドレスを設定します。

4. pp1# ip pp address 172.16.0.2/30
   pp1# ip pp remote address 172.16.0.1
   プロバイダ側のルーターと接続するために必要であれば、回線側の IP アドレスの設定を行います。Unnumbered で接続する場合にはこの設定は不要となり、相手ルーター B での設定は ipsec ike remote address 172.16.128.17 となります。

5. pp1# ip route default gateway pp 1
   pp1# pp enable 1
   pp1# pp select none
   回線側にデフォルト経路を設定します。これは VPN 以外の相手と通信するための経路になります。

6. # ipsec ike pre-shared-key 1 text secret
   # ipsec ike remote address 1 any
   # ipsec ike remote name 1 routerB
   # ipsec sa policy 101 1 esp des-cbc md5-hmac
   IPsec の定義を設定します。pre-shared-key は相手側と同じものを設定する必要があります。相手側がダイヤルアップの都度異なる IP アドレスでアクセスしてくるため、IP アドレスは any と設定し、名前を設定します。この名前で相手側セキュリティゲートウェイが識別されることになります。暗号化を行い、アルゴリズムに des-cbc を、かつ認証に md5-hmac を用います。

7. # tunnel select 1
   tunnel1# ip route 192.168.1.0/24 gateway tunnel 1
   tunnel1# ipsec tunnel 101
   tunnel1# tunnel enable 1
   tunnel1# ipsec auto refresh on
   tunnel1# tunnel select none
   相手側 LAN との通信に IPsec を用いるため、その経路をトンネルルートに設定します。また IPsec 定義の適用と自動鍵交換を行うよう設定します。

8. # save
   # interface reset bri1
   回線種別がデフォルトと異なるのでインタフェースをリセットします。restart コマンドによる装置全体の再起動でもかまいません。

■ルーター B

1. # ip lan1 address 192.168.1.1/24
   LAN 側をプライベートアドレスネットワークとします。

2. # nat descriptor type 1 masquerade
   # nat descriptor masquerade static 1 1 192.168.1.1 udp 500
   # nat descriptor masquerade static 1 2 192.168.1.1 esp *
   # pp select 1
   pp1# pp bind bri1
   pp1# ip pp nat descriptor 1
   回線側に IP マスカレードを適用します。鍵交換に必要なポート udp 500 はセキュリティゲートウェイである RT 自身に静的に結び付けます。また外側から内側に対する通信があるときには、静的 IP マスカレードを使って ESP を通す必要があります。

3. pp1# isdn remote address call 0312345678
   pp1# pp auth accept chap
   pp1# pp auth myname userB passB
   pp1# ppp ipcp ipaddress on
   pp1# ip route default gateway pp 1
   pp1# pp enable 1
   pp1# pp select none
   プロバイダに接続するための情報を設定します。また回線側にデフォルト経路を設定します。これは VPN 以外の相手と通信するための経路になります。

4. # ipsec ike local address 1 192.168.1.1
   # ipsec ike local name 1 routerB
   # ipsec ike remote address 1 172.16.0.2
   # ipsec ike pre-shared-key 1 text secret
   # ipsec sa policy 101 1 esp des-cbc md5-hmac
   IPsec の定義を設定します。pre-shared-key は相手側と同じものを設定する必要があります。相手側セキュリティゲートウェイの IP アドレスと、相手側が自側を識別するための名前を設定します。暗号化を行い、アルゴリズムに des-cbc を、かつ認証に md5-hmac を用います。

5. # tunnel select 1
   tunnel1# ip route 192.168.0.0/24 gateway tunnel 1
   tunnel1# ipsec tunnel 101
   tunnel1# tunnel enable 1
   tunnel1# ipsec auto refresh on
   tunnel1# tunnel select none
   # save
   相手側 LAN との通信に IPsec を用いるため、その経路をトンネルルートに設定します。また IPsec 定義の適用と自動鍵交換を行うよう設定します。

14. ローカルルーター機能設定例

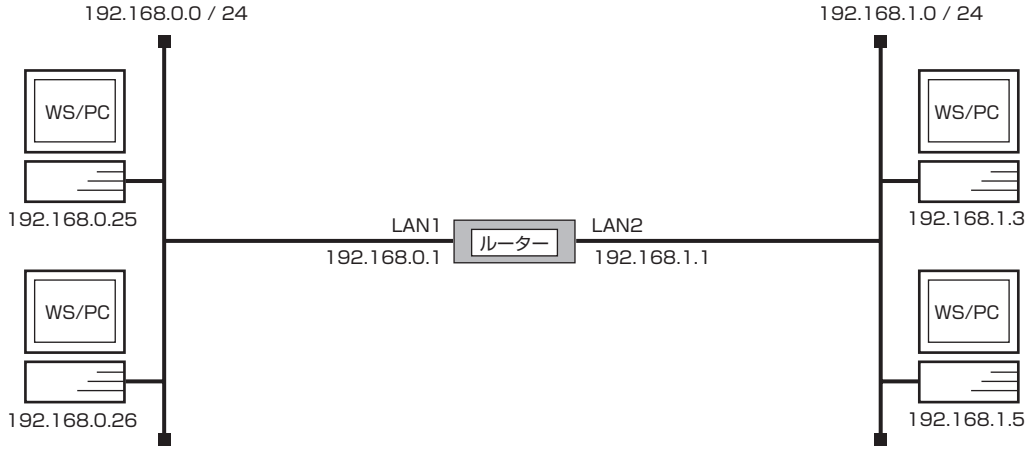
本章では、ローカルルーター機能の設定方法について、具体例をいくつかあげて説明します。セキュリティの設定や、詳細な各種パラメータなどの付加的な設定に関しては、個々のネットワークの運営方針などに基づいて行ってください。
本章で説明するネットワーク接続の形態は、次のようになります。

1. 2 つの LAN をローカルルーティング (TCP/IP のみ)
2. 2 つの LAN をローカルルーティング (IPX のみ)
3. 2 つの LAN をブリッジング
4. 2 つの LAN とプロバイダを 128kbit/s ディジタル専用線で接続
5. 3 つの LAN と遠隔地の LAN を 1.5Mbit/s ディジタル専用線で接続（RT300i）
6. 同一 LAN 内の相互通信を遮断し、ブロードキャストドメインを分離 (RT105e)

以下の説明では、それぞれのネットワークの接続形態例に対して構成図、 手順、解説の順に行います。

14.1 2 つの LAN をローカルルーティング (TCP/IP のみ)

[構成図]



[手順]

```
# ip lan1 address 192.168.0.1/24
# ip lan2 address 192.168.1.1/24
# save
```

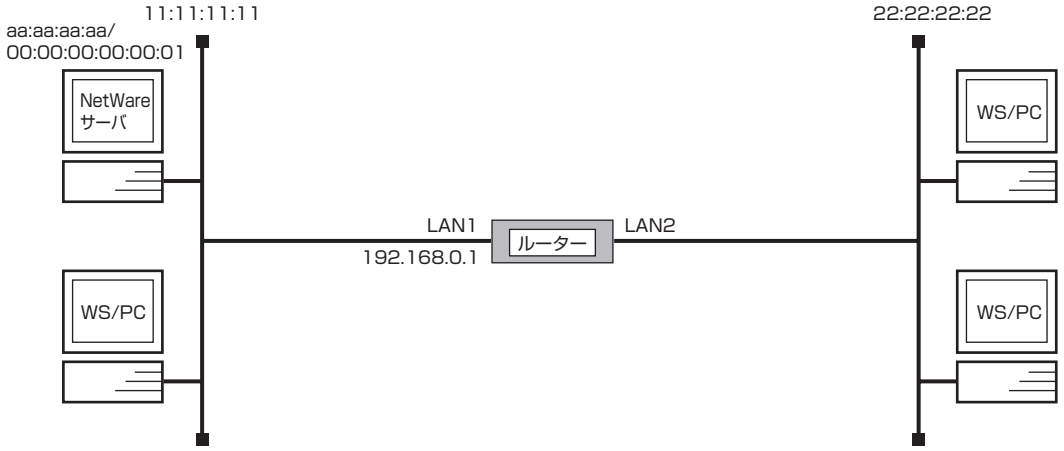
[解説]

ネットワーク 192.168.0.0 とネットワーク 192.168.1.0 をローカルルーティングするための設定を説明します。

1. **ip lan1 address** コマンドを使用して、LAN1 インタフェースの IP アドレスとネットマスクを設定します。
2. **ip lan2 address** コマンドを使用して、LAN2 インタフェースの IP アドレスとネットマスクを設定します。
3. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

14.2 2 つの LAN をローカルルーティング (IPX のみ)

[構成図]



[手順]

```
# ip routing off
# ip lan1 address 192.168.0.1/24
# ipx routing on
# ipx lan1 network 11:11:11:11
# ipx lan2 network 22:22:22:22
# save
```

[解説]

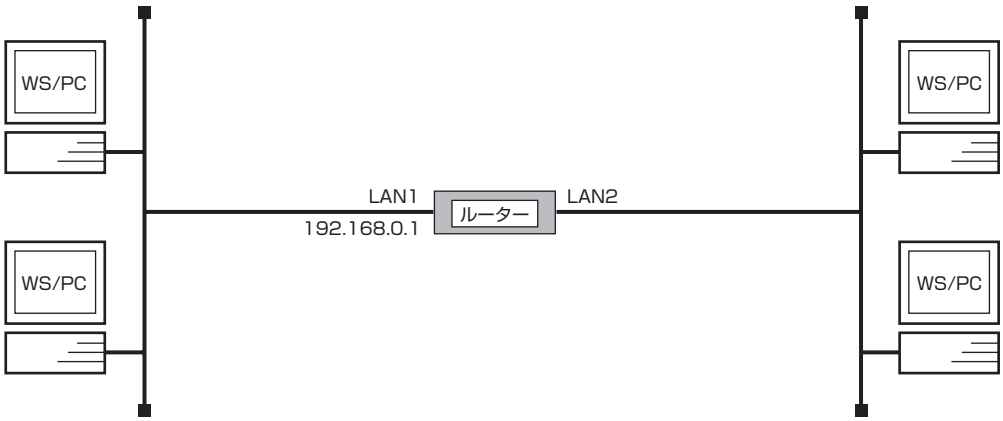
IPX ネットワーク同士をローカルルーティングするための設定を説明します。

LAN1 インタフェースの IP アドレスの設定は必須ではありませんが、プログラムのリビジョンアップや TELNET での設定を将来行うことを考慮して設定しておく方がよいでしょう。

1. **ip routing** コマンドを使用して、IP パケットをルーティングしないように設定します。
2. **ip lan1 address** コマンドを使用して、LAN1 インタフェースの IP アドレスとネットマスクを設定します。
3. **ipx routing** コマンドを使用して、IPX パケットをルーティングするように設定します。
4. **ipx lan1 address** コマンドを使用して、LAN1 インタフェースの IPX ネットワーク番号を設定します。
5. **ipx lan2 address** コマンドを使用して、LAN2 インタフェースの IPX ネットワーク番号を設定します。
6. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

14.3 2 つの LAN をブリッジング

［構成図］



［手順］

```
# ip routing off
# ip lan1 address 192.168.0.1/24
# bridge use on
# bridge group lan1 lan2
# save
```

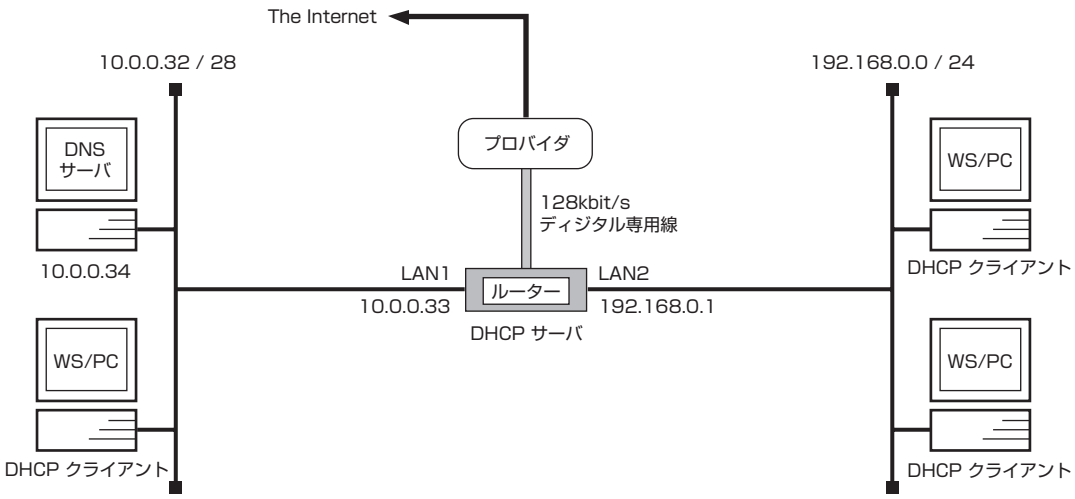
［解説］
ネットワーク同士をローカルブリッジ接続するための設定を説明します。

LAN1 インタフェースの IP アドレスの設定は必須ではありませんが、プログラムのリビジョンアップや TELNET での設定を将来行うことを考慮して設定しておく方がよいでしょう。

1. **ip routing** コマンドを使用して、IP パケットをルーティングしないように設定します。
2. **ip lan1 address** コマンドを使用して、LAN1 インタフェースの IP アドレスとネットマスクを設定します。
3. **bridge use** コマンドを使用して、ブリッジするように設定します。
4. **bridge group** コマンドを使用して、ブリッジするインタフェースを設定します。
5. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

14.4 2 つの LAN とプロバイダを 128kbit/s ディジタル専用線で接続

[構成図]



[設定手順]

```
# line type bri1 l128
# ip lan1 address 10.0.0.33/28
# ip lan2 address 192.168.0.1/24
# dns server 10.0.0.34
# dns domain rtpro.yamaha.co.jp
# dhcp scope 1 10.0.0.35-10.0.0.45/28
# dhcp scope 2 192.168.0.2-192.168.0.254/24
# dhcp service server
# pp select 1
pp1# pp bind bri1
pp1# ip route default gateway pp 1
pp1# nat descriptor type 1 masquerade
pp1# nat descriptor address outer 1 10.0.0.46
pp1# nat descriptor address inner 1 192.168.0.1-192.168.0.254
pp1# ip pp nat descriptor 1
pp1# pp enable 1
pp1# save
pp1# interface reset bri1
```

[解説]

ネットワーク 10.0.0.32 とネットワーク 192.168.0.0 を別々のセグメントに割り当て、プロバイダと 128kbit/s ディジタル専用線で接続するための設定を説明します。

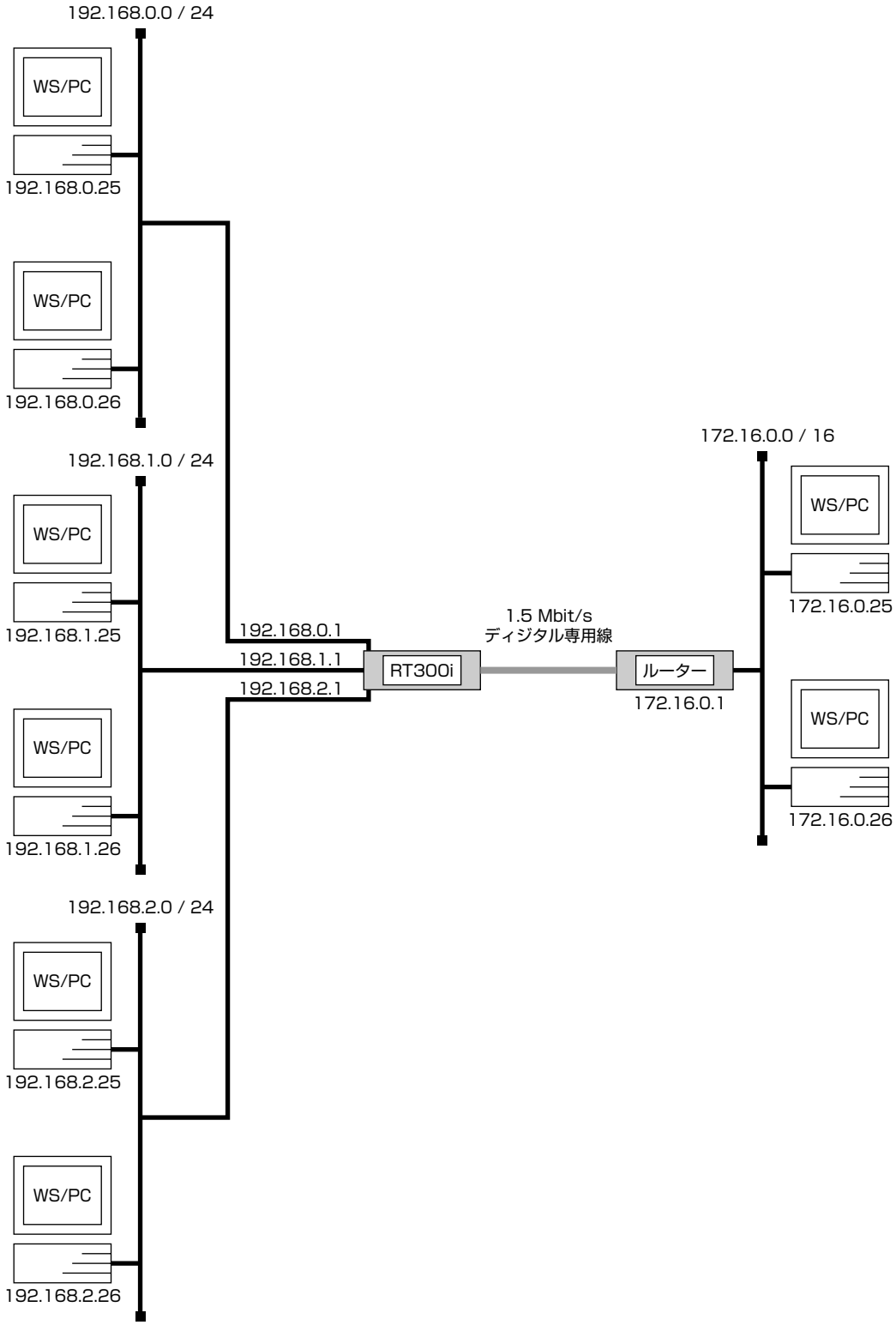
LAN1 インタフェースは 16 個のグローバル IP アドレス、LAN2 インタフェースは 256 個のプライベート IP アドレスの割り当てを仮定します。ルーターは DHCP クライアントのために DHCP サーバとして動作するように設定しています。プライベート IP アドレス側からは NAT を使用してインターネットへ接続しますが、このためのグローバル IP アドレスを節約するために IP マスカレード 機能を使用しています。
更に、静的 IP マスカレード エントリの設定を行わないためにグローバル IP アドレス空間からのアクセスができないため、LAN1 インタフェースのセグメントがバリアセグメントのように見えます。

IP アドレス	割り当て	DHCP スコープ番号
10.0.0.32	LAN1 のネットワーク	−
10.0.0.33	ルーターの LAN1 インタフェース	−
10.0.0.34	DNS サーバ	−
10.0.0.35 : 10.0.0.45	DHCP クライアント (11 台)	1
10.0.0.46	LAN2 のための NAT 用グローバル IP アドレス	−
10.0.0.47	LAN1 のブロードキャスト	−
192.168.0.0	LAN2 のネットワーク	−
192.168.0.1	ルーターの LAN2 インタフェース	−
192.168.0.2 : 192.168.0.254	DHCP クライアント (253 台)	2
192.168.0.255	LAN2 のブロードキャスト	−

1. **line type** コマンドを使用して、回線種別を 128kbit/s ディジタル専用線に指定します。
2. **ip lan1 address** コマンドを使用して、LAN1 インタフェースの IP アドレスとネットマスクを設定します。
3. **ip lan2 address** コマンドを使用して、LAN2 インタフェースの IP アドレスとネットマスクを設定します。
4. **dns server** コマンドを使用して、DNS サーバの IP アドレスを設定します。
5. **dns domain** コマンドを使用して、DNS で使用するドメイン名を設定します。
6. **dhcp scope** コマンドを使用して、DHCP スコープを定義します。
7. **dhcp service** コマンドを使用して、DHCP サーバとして機能するように設定します。
8. **pp select** コマンドを使用して、相手先情報番号を選択します。
9. **pp bind** コマンドを使用して、選択した相手先情報番号と BRI ポートをバインドします。
10. **ip route** コマンドを使用して、プロバイダ側へのデフォルトルートを設定します。
11. **nat descriptor type** コマンドを使用して、NAT の識別番号とそのタイプを設定します。
12. **nat descriptor address outer** コマンドを使用して、NAT で使用する外側の IP アドレスを設定します。
13 **nat descriptor address inner** コマンドを使用して、NAT で使用する内側の IP アドレスを設定します。
14 **ip pp nat descriptor** コマンドを使用して、PP インタフェースに適用する NAT 識別番号を設定します。
15. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。
16. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。
17. 回線種別がデフォルトと異なるので、**interface reset bri1** コマンドを使用してインタフェースをリセットしてハードウェアを切替えます。**restart** コマンドによる装置全体の再起動でもかまいません。

14.5 3つのLANと遠隔地のLANを1.5Mbit/sディジタル専用線で接続（RT300i）

[構成図]



[設定手順]

```
# pri leased channel 1/1 1 24
# ip lan1 address 192.168.0.1/24
# ip lan2 address 192.168.1.1/24
# ip lan3 address 192.168.2.1/24
# ip route 172.16.0.0/16  gateway pp 1
# pp select 1
pp1# pp bind pri1/1
pp1# pp enable 1
pp1# save
pp1# interface reset pri1
```

[解説]

2 枚の LAN 拡張モジュール (YBA-1ETH-TX) と PRI 拡張モジュール (YBA-1PRI-N) を装着し、3 つのローカルセグメントと遠隔地の LAN を接続します。

1. **pri leased channel** コマンドを使って PRI の情報チャネルとタイムスロットを設定します。

2. **ip lan1 address** コマンド、**ip lan2 address** コマンド、**ip lan3 address** コマンドを使って、メインボード、本機の拡張スロットに装着されたモジュール上の LAN の IP アドレスを設定します。

3. **ip route** コマンドを使って遠隔地の LAN への経路情報を設定します。

4. **pp select** コマンドを使って相手先情報番号を選択します。

5. **pp bind** コマンドを使って選択した相手先情報番号に PRI 情報チャネルをバインドします。

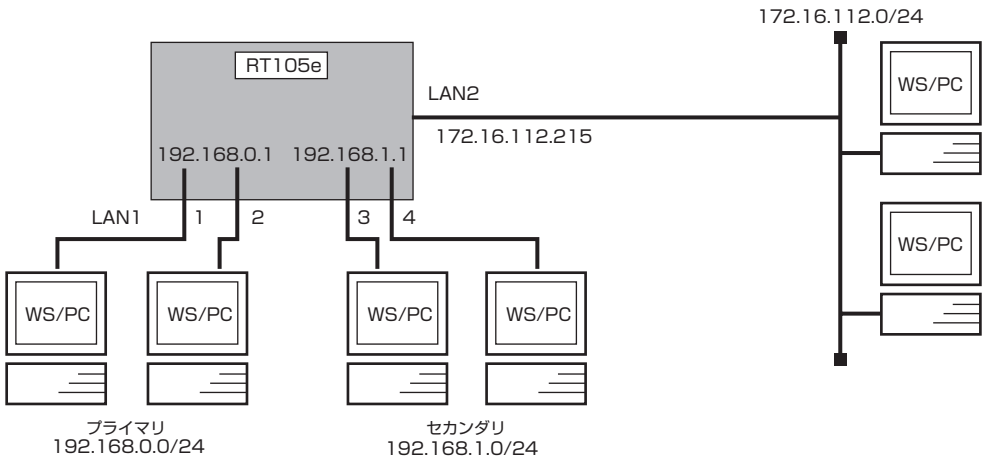
6. **pp enable** コマンドを使って PP 側のインタフェースを有効にします。

7. **save** コマンドを使って設定を内蔵の不揮発性メモリに書き込みます。

8. **interface reset** コマンドを使って PRI の情報チャネルとタイムスロットの設定を有効にします。**restart** コマンドを使って、ルーターを再起動させても PRI の情報チャネルとタイムスロットの設定は有効になります。

14.6 同一 LAN 内の相互通信を遮断し、ブロードキャストドメインを分離 (RT105e)

[構成図]



[設定手順]

```
# lan type lan1 port-based-ks8995e primary 1 2
# ip lan1 address 192.168.0.1/24
# ip lan1 secondary address 192.168.1.1/24
# ip lan2 address 172.16.112.215/24
# save
```

[解説]

LAN1 のポート 1,2 がプライマリアドレスネットワークに、ポート 3,4 がセカンダリアドレスネットワークに属します。LAN1 側でブロードキャストドメインが分けられます。

プライマリ / セカンダリ間の相互通信のパケットは必ず RT のルーティング処理を経由することになります。フィルタや NAT 処理も可能です。

LAN1 の両ネットワークから LAN2 へのアクセスが可能です。
LAN1 に対する RT 自身からのブロードキャストパケットは LAN1 全ポートに送出されます。
RIP はプライマリアドレスネットワークにしか使用できません。

1. # lan type lan1 port-based-ks8995e primary 1 2
   LAN1 にセカンダリセグメント機能を設定します。ポート 1 と 2 がプライマリネットワークに、残りのポートはセカンダリネットワークに属することになります。

2. # ip lan1 address 192.168.0.1/24
   # ip lan1 secondary address 192.168.1.1/24
   # ip lan2 address 172.16.112.215/24
   # save
   それぞれのネットワークに適用する IP アドレスを設定します。

15. NAT ディスクリプタ設定例

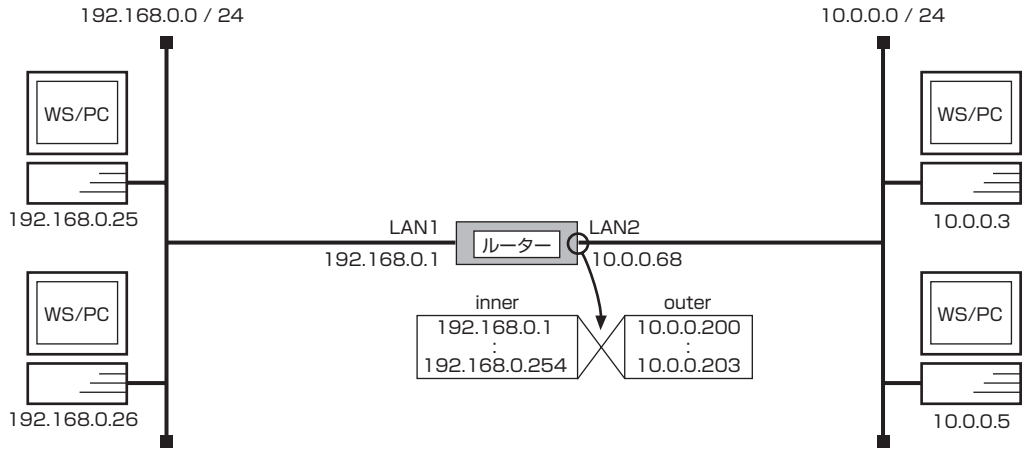
本章では、NAT ディスクリプタ機能の設定方法について、具体例をいくつかあげて説明します。セキュリティの設定や、詳細な各種パラメータなどの付加的な設定に関しては、個々のネットワークの運営方針などに基づいて行ってください。
本章で説明するネットワーク接続の形態は、次のようになります。

1. 動的 NAT で 2 つの LAN を接続
2. 静的 NAT で 2 つの LAN を接続
3. IP マスカレード で 2 つの LAN を接続
4. 動的 NAT と動的 IP マスカレード の併用
5. IP マスカレードでプライマリ - セカンダリ間を接続
6. 特定ポートをサーバ公開用セグメントとして使用 (RT105e)

以下の説明では、それぞれのネットワークの接続形態例に対して構成図、手順、解説の順に行います。

15.1 動的 NAT で 2 つの LAN を接続

[構成図]



[手順]

```
# ip lan1 address 192.168.0.1/24
# ip lan2 address 10.0.0.68/24
# ip lan2 nat descriptor 1
# nat descriptor type 1 nat
# nat descriptor address outer 1 10.0.0.200-10.0.0.203
# nat descriptor address inner 1 192.168.0.1-192.168.0.254
# dhcp service server
# dhcp scope 1 192.168.0.2-192.168.0.254/24
# save
```

[解説]

プライベートなネットワーク 192.168.0.0 とグローバルなネットワーク 10.0.0.0 を動的な NAT を用いて接続するための設定を説明します。

この例では、LAN2 インタフェースに接続されたグローバルアドレス空間の 4 つの IP アドレスと、LAN1 インタフェースに接続されたプライベートアドレス空間のすべての IP アドレスを、NAT により動的に変換します。NAT の変換は LAN2 インタフェースの出口方向へかけられるので、プライベートからグローバルの方向へ同時に最大 4 つのホストが自由にアクセスすることができます。

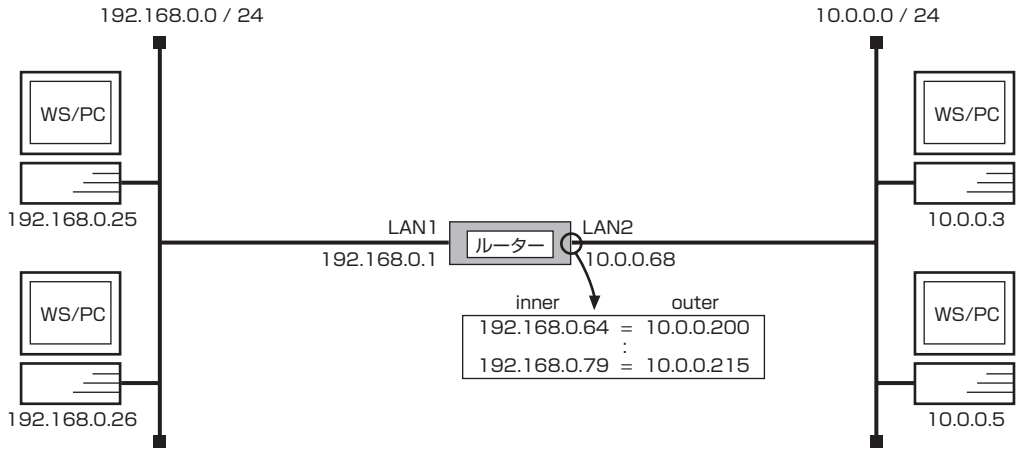
IP アドレス	割り当て	DHCP スコープ番号
192.168.0.0	LAN1 のネットワーク	−
192.168.0.1	ルーターの LAN1 インタフェース	−
192.168.0.2 : 192.168.0.254	DHCP クライアント (253 台)	1
192.168.0.255	LAN1 のブロードキャスト	−
10.0.0.0	LAN2 のネットワーク	−
10.0.0.68	ルーターの LAN2 インタフェース	−
10.0.0.255	LAN2 のブロードキャスト	−

1. **ip lan1 address** コマンドを使用して、LAN1 インタフェースの IP アドレスとネットマスクを設定します。
2. **ip lan2 address** コマンドを使用して、LAN2 インタフェースの IP アドレスとネットマスクを設定します。
3. **ip lan2 nat descriptor** コマンドを使用して、LAN2 インタフェースに適用する NAT 識別番号を設定します。
4. **nat descriptor type** コマンドを使用して、NAT の識別番号とそのタイプを設定します。

5. **nat descriptor address outer** コマンドを使用して、NAT で使用する外側の IP アドレスを設定します。
6. **nat descriptor address inner** コマンドを使用して、NAT で使用する内側の IP アドレスを設定します。
7. **dhcp service** コマンドを使用して、DHCP サーバとして機能するように設定します。
8. **dhcp scope** コマンドを使用して、DHCP スコープを定義します。
9. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

15.2 静的 NAT で 2 つの LAN を接続

[構成図]



[手順]

```
# ip lan1 address 192.168.0.1/24
# ip lan2 address 10.0.0.68/24
# ip lan2 nat descriptor 1
# nat descriptor type 1 nat
# nat descriptor address outer 1 10.0.0.200
# nat descriptor address inner 1 192.168.0.64
# nat descriptor static 1 1 10.0.0.200=192.168.0.64 16
# dhcp service server
# dhcp scope 1 192.168.0.2-192.168.0.254/24
# save
```

[解説]

プライベートなネットワーク 192.168.0.0 とグローバルなネットワーク 10.0.0.0 を静的な NAT を用いて接続するための設定を説明します。

この例では、LAN2 インタフェースに接続されたグローバルアドレス空間の連続する 16 個の IP アドレスと、LAN1 インタフェースに接続されたプライベートアドレス空間の連続する 16 個の IP アドレスを結び付けています。

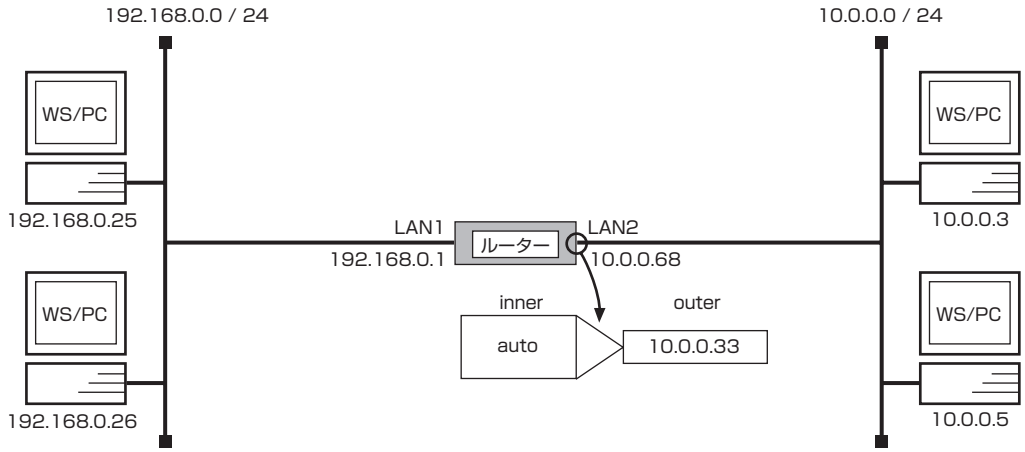
静的な NAT 変換で設定された IP アドレスに対しては、グローバル空間とプライベート空間のどちらからもアクセスを開始することが可能です。

IP アドレス	割り当て	DHCP スコープ番号
192.168.0.0	LAN1 のネットワーク	−
192.168.0.1	ルーターの LAN1 インタフェース	−
192.168.0.2 : 192.168.0.63	DHCP クライアント (62 台)	1
192.168.0.64 : 192.168.0.79	DHCP クライアント、かつ 静的 NAT エントリ (16 台)	1
192.168.0.80 : 192.168.0.254	DHCP クライアント (175 台)	1
192.168.0.255	LAN1 のブロードキャスト	−
10.0.0.0	LAN2 のネットワーク	−
10.0.0.68	ルーターの LAN2 インタフェース	−
10.0.0.200 : 10.0.0.215	静的 NAT エントリ (16 台)	−
10.0.0.255	LAN2 のブロードキャスト	−

1. **ip lan1 address** コマンドを使用して、LAN1 インタフェースの IP アドレスとネットマスクを設定します。
2. **ip lan2 address** コマンドを使用して、LAN2 インタフェースの IP アドレスとネットマスクを設定します。
3. **ip lan2 nat descriptor** コマンドを使用して、LAN2 インタフェースに適用する NAT 識別番号を設定します。
4. **nat descriptor type** コマンドを使用して、NAT の識別番号とそのタイプを設定します。
5. **nat descriptor address outer** コマンドを使用して、NAT で使用する外側の IP アドレスを設定します。
6. **nat descriptor address inner** コマンドを使用して、NAT で使用する内側の IP アドレスを設定します。
7. **nat descriptor static** コマンドを使用して、静的 NAT で使用する IP アドレスを設定します。
8. **dhcp service** コマンドを使用して、DHCP サーバとして機能するように設定します。
9. **dhcp scope** コマンドを使用して、DHCP スコープを定義します。
10. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

15.3 IP マスカレード で 2 つの LAN を接続

［構成図］



［手順］

```
# ip lan1 address 192.168.0.1/24
# ip lan2 address 10.0.0.68/24
# ip lan2 nat descriptor 1
# nat descriptor type 1 masquerade
# nat descriptor address outer 1 10.0.0.33
# dhcp service server
# dhcp scope 1 192.168.0.2-192.168.0.254/24
# save
```

［解説］

プライベートなネットワーク 192.168.0.0 とグローバルなネットワーク 10.0.0.0 を IP マスカレード を用いて接続するための設定を説明します。

この例では、LAN2 インタフェースに接続されたグローバルアドレス空間の 1 つの IP アドレスと、LAN1 インタフェースに接続されたプライベートアドレス空間の IP アドレスを、IP マスカレード により動的に変換します。

IP マスカレード 変換は LAN2 インタフェースの出口方向へかけられるので、プライベートからグローバルの方向へ複数のホストが自由にアクセスすることができます。

IP アドレス	割り当て	DHCP スコープ番号
192.168.0.0	LAN1 のネットワーク	−
192.168.0.1	ルーターの LAN1 インタフェース	−
192.168.0.2 : 192.168.0.254	DHCP クライアント (253 台)	1
192.168.0.255	LAN1 のブロードキャスト	−
10.0.0.0	LAN2 のネットワーク	−
10.0.0.68	ルーターの LAN2 インタフェース	−
10.0.0.255	LAN2 のブロードキャスト	−

1. **ip lan1 address** コマンドを使用して、LAN1 インタフェースの IP アドレスとネットマスクを設定します。
2. **ip lan2 address** コマンドを使用して、LAN2 インタフェースの IP アドレスとネットマスクを設定します。
3. **ip lan2 nat descriptor** コマンドを使用して、LAN2 インタフェースに適用する NAT 識別番号を設定します。
4. **nat descriptor type** コマンドを使用して、NAT の識別番号とそのタイプを設定します。
5. **nat descriptor address outer** コマンドを使用して、NAT で使用する外側の IP アドレスを設定します。

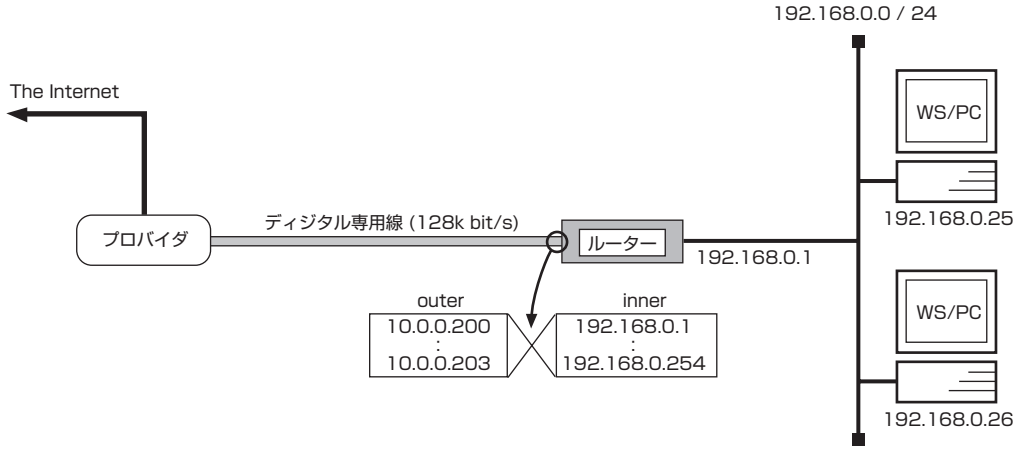
6. **dhcp service** コマンドを使用して、DHCP サーバとして機能するように設定します。

7. **dhcp scope** コマンドを使用して、DHCP スコープを定義します。

8. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

15.4 動的 NAT と動的 IP マスカレード の併用

[構成図]



[設定手順]

```
# line type bri1 l128
# ip lan1 address 192.168.0.1/24
# nat descriptor type 1 nat-masquerade
# nat descriptor address outer 1 10.0.0.200-10.0.0.203
# nat descriptor address inner 1 192.168.0.1-192.168.0.254
# pp select 1
pp1# pp bind bri1
pp1# ip route default gateway pp 1
pp1# ip pp nat descriptor 1
pp1# pp enable 1
pp1# pp select none
# dhcp service server
# dhcp scope 1 192.168.0.2-192.168.0.254/24
# save
# interface reset bri1
```

[解説]

ネットワーク型プロバイダ接続でプライベートなネットワーク 192.168.0.0 を NAT と IP マスカレード を用いて接続するための設定を説明します。

この例では、プロバイダ側のグローバルアドレス空間の 4 つの IP アドレスと、LAN インタフェースに接続されたプライベートアドレス空間の IP アドレスを、動的な NAT と IP マスカレード により動的に変換します。動的な NAT 変換では 3 個目までの IP アドレスを動的に変換し、4 番目以降は IP マスカレード で対応します。

IP アドレス	割り当て	DHCP スコープ番号
192.168.0.0	LAN のネットワーク	−
192.168.0.1	ルーターの LAN インタフェース	−
192.168.0.2 : 192.168.0.254	DHCP クライアント (253 台)	1
192.168.0.255	LAN のブロードキャスト	−

1. **line type** コマンドを使用して、回線種別を 128kbit/s ディジタル専用線に指定します。

2. **ip lan1 address** コマンドを使用して、LAN インタフェースの IP アドレスとネットマスクを設定します。

3. **nat descriptor type** コマンドを使用して、NAT の識別番号とそのタイプを設定します。

4. **nat descriptor address outer** コマンドを使用して、NAT で使用する外側の IP アドレスを設定します。

5. **nat descriptor address inner** コマンドを使用して、NAT で使用する内側の IP アドレスを設定します。

6. **pp select** コマンドを使用して、相手先情報番号を選択します。

7. **ip route** コマンドを使用して、デフォルトルートを設定します。この場合、LAN 上のホスト以外のパケットはすべてプロバイダ側へ送られます。

8. **ip pp nat descriptor** コマンドを使用して、PP インタフェースに適用する NAT 識別番号を設定します。

9. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

10. **dhcp service** コマンドを使用して、DHCP サーバとして機能するように設定します。

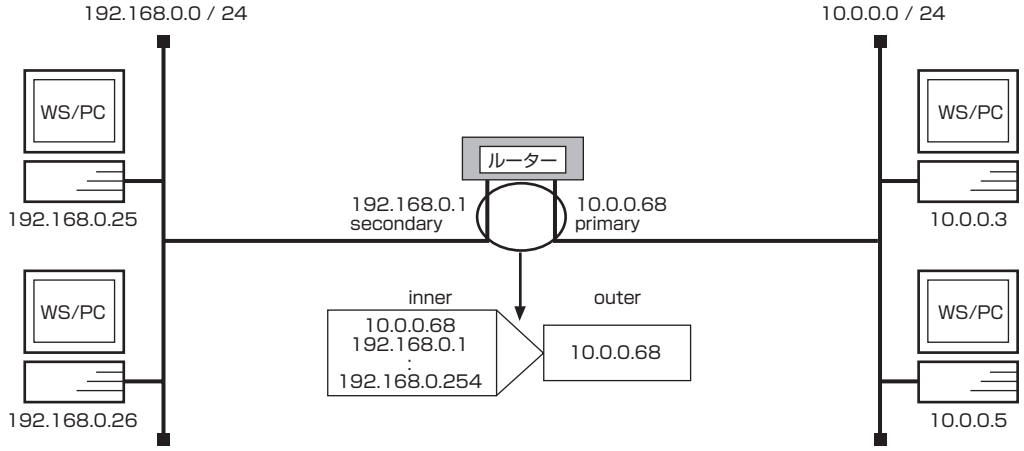
11. **dhcp scope** コマンドを使用して、DHCP スコープを定義します。

12. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

13. **interface reset** コマンドを使って回線種別の変更されたポートをリセットします。個々のポートをリセットする代わり **restart** コマンドを使って、ルーターを再起動させても回線種別は切り替わります。

15.5 IP マスカレードでプライマリ - セカンダリ間を接続

[構成図]



[設定手順]

```
# ip lan1 address 10.0.0.68/24
# ip lan1 secondary address 192.168.0.1/24
# ip lan1 nat descriptor 1
# nat descriptor type 1 masquerade
# nat descriptor address outer 1 primary
# nat descriptor address inner 1 10.0.0.68 192.168.0.2-192.168.0.254
# save
```

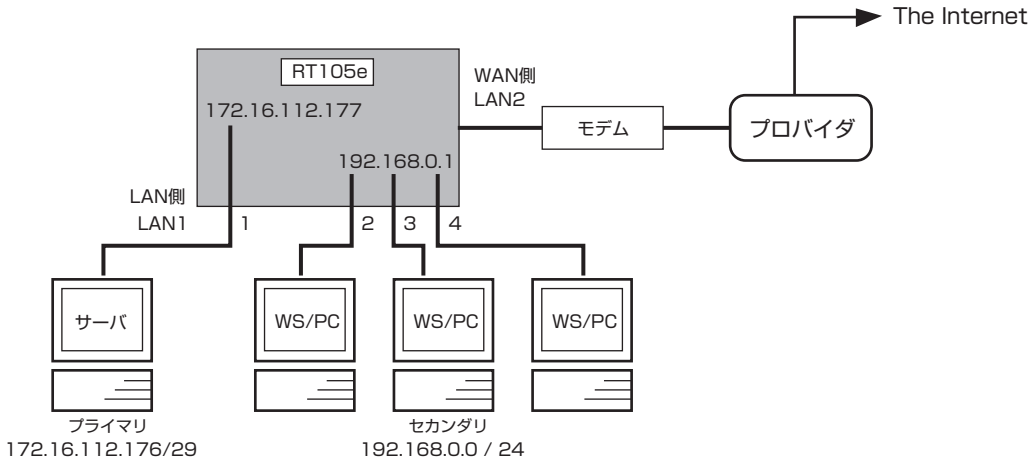
[解説]

プライマリのグローバルネットワークと、セカンダリのプライベートなネットワーク 192.168.0.0 を IP マスカレードを用いて接続するための設定を説明します。
この例では、プライマリのグローバルアドレス空間の 1 つの IP アドレスと、セカンダリのプライベートアドレス空間の IP アドレスを、IP マスカレードにより動的に変換します。

1. **ip lan1 address** コマンドを使用して、LAN インタフェースの IP アドレスとネットマスクを設定します。
2. **ip lan1 secondary address** コマンドを使用して、LAN インタフェースのセカンダリ IP アドレスとネットマスクを設定します。
3. **ip lan1 nat descriptor** コマンドを使用して、LAN インタフェースに適用する NAT 識別番号を設定します。
4. **nat descriptor type** コマンドを使用して、NAT の識別番号とそのタイプを設定します。
5. **nat descriptor address outer** コマンドを使用して、NAT で使用する外側の IP アドレスを設定します。
6. **nat descriptor address inner** コマンドを使用して、NAT で使用する内側の IP アドレスを設定します。
7. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

15.6 特定ポートをサーバ公開用セグメントとして使用 (RT105e)（グローバルアドレス 8 個で NAT 使用）

[構成図]



[設定手順]

```
# lan type lan1 port-based-ks8995e primary 1 secondary 2 3 4
# ip lan1 address 172.16.112.177/29
# ip lan1 secondary address 192.168.0.1/24
# nat descriptor type 1 masquerade
# nat descriptor address outer 1 172.16.112.182
# nat descriptor address inner 1 192.168.0.2-192.168.0.254
# ip lan2 nat descriptor 1
# save
```

[解説]

公開サーバにはひとつのグローバル IP アドレスを割り当てます。セカンダリセグメント機能を利用して公開サーバ用のネットワークを独立させます。LAN1 側でブロードキャストドメインが分けられます。LAN2 側には適宜 WAN 接続の設定が必要です (PPPoE 接続設定例等参照)。

プライマリ / セカンダリ間の相互通信のパケットは必ず RT のルーティング処理を経由することになります。フィルタや NAT 処理も可能です。

LAN1 の両ネットワークから LAN2 経由 WAN へのアクセスが可能です。LAN1 に対する RT 自身からのブロードキャストパケットは LAN1 全ポートに送出されます。

RIP はプライマリアドレスネットワークにしか使用できません。

1. # lan type lan1 port-based-ks8995e primary 1 secondary 2 3 4
   LAN1 のポート 1 を公開サーバ用のプライマリネットワーク、他のポートをセカンダリネットワークとします。

   プライマリネットワークには 172.16.112.176/29 のネットワークアドレスを持つサーバ群 (IP マスカレードで使用する 172.16.112.182 は除く) を接続し、セカンダリネットワークには 192.168.0.0/24 のネットワークアドレスを持つホストを接続します。

2. # ip lan1 address 172.16.112.177/29
   # ip lan1 secondary address 192.168.0.1/24
   それぞれのネットワークに適用する IP アドレスを設定します。

3. # nat descriptor type 1 masquerade
   # nat descriptor address outer 1 172.16.112.182
   # nat descriptor address inner 1 192.168.0.2-192.168.0.254
   LAN1 からの WAN アクセスのために IP マスカレードを定義します。
   セカンダリネットワークのホストだけを対象します。

4. # ip lan2 nat descriptor 1
   # save
   IP マスカレード機能を定義した NAT ディスクリプタを LAN2 に適用します。
   PPPoE で WAN に接続する場合には、このコマンドの代わりに PPPoE の設定を行った pp に対して
   # ip pp nat descriptor 1
   を設定します。

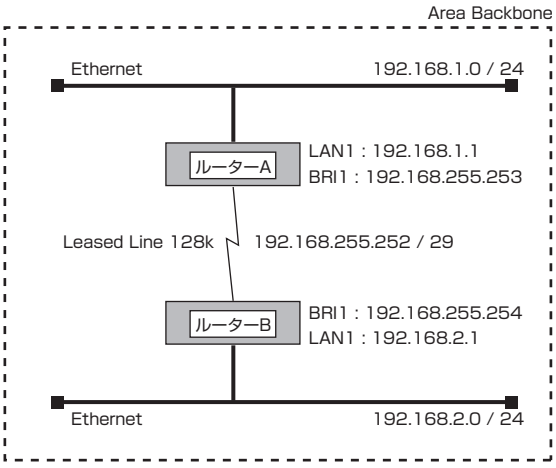
16. OSPF 設定例

本章では OSPF 設定例を示します。

1. バックボーンエリアに所属する 2 拠点間を PPP で結ぶ
2. 異なるエリアに分かれた 2 拠点間を PPP で結ぶ
3. 多拠点間を FR で結ぶ
4. 静的経路、RIP との併用

16.1 バックボーンエリアに所属する２拠点間を PPP で結ぶ

[構成図]



[ルーター A の設定手順]

```
# line type bri1 l128

# ospf use on
# ospf area backbone

# ip lan1 address 192.168.1.1/24
# ip lan1 ospf area backbone

# pp select 1
pp1# pp bind bri1
pp1# ip pp address 192.168.255.253/29
pp1# ip pp ospf area backbone
pp1# ppp ipcp ipaddress on
pp1# pp enable 1
pp1# pp select none
# save
# interface reset bri1
# ospf configure refresh
```

[ルーター B の設定手順]

```
# line type bri1 l128

# ospf use on
# ospf area backbone

# ip lan1 address 192.168.2.1/24
# ip lan1 ospf area backbone

# pp select 1
pp1# pp bind bri1
pp1# ip pp address 192.168.255.254/29
pp1# ip pp ospf area backbone
pp1# ppp ipcp ipaddress on
pp1# pp enable 1
pp1# pp select none
# save
# interface reset bri1
# ospf configure refresh
```

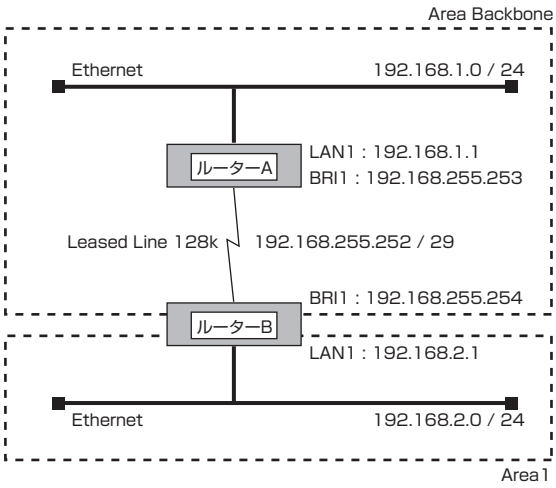
[解説]

バックボーンエリアに所属する 2 台のルーターを専用線で結んだ例です。

1. **line type** コマンドを使用して、回線種別を 128k bit/s ディジタル専用線に指定します。
2. **ospf use** コマンドを使用して、ospf を有効にします。
3. **ospf area** コマンドを使用して、ルーターの所属する OSPF エリアを設定します。バックボーンの場合は backbone と指定します。
4. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。
5. **ip lan1 ospf area** コマンドを使用して、**lan1** の所属する OSPF エリアの設定をします。バックボーンの場合は backbone と指定します。
6. **pp select** コマンドを使用して、相手先番号を選択します。
7. **pp bind** コマンドを使用して、選択した相手番号に BRI ボードをバインドします。
8. **ip pp address** コマンドを使用して、回線側インタフェースの IP アドレスを設定します。
9. **ip pp ospf area** コマンドを使用して、回線側インタフェースの所属する OSPF エリアの設定をします。バックボーンの時は backbone と指定します。
10. **ppp ipcp ipaddress** コマンドを使用して、相手側の回線インタフェースの IP アドレスを取得できるようにします。
11. **pp enable** コマンドを使用して、pp 側のインタフェースを有効にします。
12. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。
13. **interface reset** コマンドを使用して、回線のハードウェアを切替えます。
14. **ospf configure refresh** コマンドを使用して、OSPF の設定を有効にします。

16.2 異なるエリアに分かれた 2 拠点間を PPP で結ぶ

[構成図]



[ルーター A の設定手順]

```
# line type bri1 l128

# ospf use on
# ospf area backbone

# ip lan1 address 192.168.1.1/24
# ip lan1 ospf area backbone

# pp select 1
pp1# pp bind bri1
pp1# ip pp address 192.168.255.253/29
pp1# ip pp ospf area backbone
pp1# ppp ipcp ipaddress on
pp1# pp enable 1
pp1# pp select none
# save
# interface reset bri1
# ospf configure refresh
```

[ルーター B の設定手順]

```
# line type bri1 1128

# ospf use on
# ospf area backbone
# ospf area 1

# ip lan1 address 192.168.2.1/24
# ip lan1 ospf area 1

# pp select 1
pp1# pp bind bri1
pp1# ip pp address 192.168.255.254/29
pp1# ip pp ospf area backbone
pp1# ppp ipcp ipaddress on
pp1# pp enable 1
pp1# pp select none
# save
# interface reset bri1
# ospf configure refresh
```

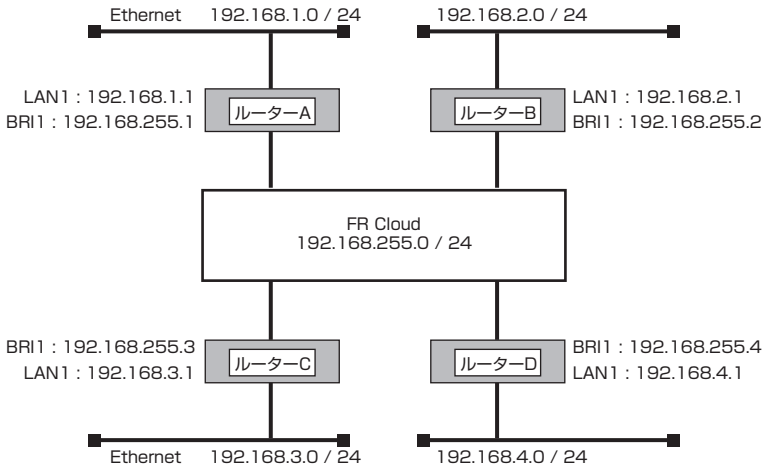
[解説]

バックボーンエリアとエリア 1 を 2 台のルーターで専用線で結んだ例です。

1. **line type** コマンドを使用して、回線種別を 128k bit/s ディジタル専用線に指定します。
2. **ospf use** コマンドを使用して、ospf を有効にします。
3. **ospf area** コマンドを使用して、ルーターの所属する OSPF エリアを設定します。バックボーンの場合は backbone と指定します。ルーター 2 のように複数の OSPF エリアに所属する場合は、すべて設定します。
4. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。
5. **ip lan1 ospf area** コマンドを使用して、lan1 の所属する OSPF エリアの設定をします。バックボーンの場合は backbone と指定します。
6. **pp select** コマンドを使用して、相手先番号を選択します。
7. **pp bind** コマンドを使用して、選択した相手番号に BRI ボードをバインドします。
8. **ip pp address** コマンドを使用して、回線側インタフェースの IP アドレスを設定します。
9. **ip pp ospf area** コマンドを使用して、回線側インタフェースの所属する OSPF エリアの設定をします。バックボーンの時は backbone と指定します。
10. **ppp ipcp ipaddress** コマンドを使用して、相手側の回線インタフェースの IP アドレスを取得できるようにします。
11. **pp enable** コマンドを使用して、pp 側のインタフェースを有効にします。
12. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。
13. **interface reset** コマンドを使用して、回線のハードウェアを切替えます。
14. **ospf configure refresh** コマンドを使用して、OSPF の設定を有効にします。

16.3 多拠点間を FR で結ぶ

[構成図]



[ルーター A の設定手順]

```
# line type bri1 l128

# ospf use on
# ospf area backbone

# ip lan1 address 192.168.1.1/24
# ip lan1 ospf area backbone

# pp select 1
pp1# pp bind bri1
pp1# pp encapsulation fr
pp1# ip pp address 192.168.255.1/24
pp1# ip pp ospf area backbone type=point-to-multipoint
pp1# pp enable 1
pp1# pp select none
# save
# interface reset bri1
# ospf configure refresh
```

[ルーター B の設定手順]

```
# line type bri1 l128

# ospf use on
# ospf area backbone

# ip lan1 address 192.168.2.1/24
# ip lan1 ospf area backbone

# pp select 1
pp1# pp bind bri1
pp1# pp encapsulation fr
pp1# ip pp address 192.168.255.2/24
pp1# ip pp ospf area backbone type=point-to-multipoint
pp1# pp enable 1
pp1# pp select none
# save
# interface reset bri1
# ospf configure refresh
```

[ルーター C の設定手順]

```
# line type bri1 l128

# ospf use on
# ospf area backbone

# ip lan1 address 192.168.3.1/24
# ip lan1 ospf area backbone

# pp select 1
pp1# pp bind bri1
pp1# pp encapsulation fr
pp1# ip pp address 192.168.255.3/24
pp1# ip pp ospf area backbone type=point-to-multipoint
pp1# pp enable 1
pp1# pp select none
# save
# interface reset bri1
# ospf configure refresh
```

[ルーター D の設定手順]

```
# line type bri1 l128

# ospf use on
# ospf area backbone

# ip lan1 address 192.168.4.1/24
# ip lan1 ospf area backbone

# pp select 1
pp1# pp bind bri1
pp1# pp encapsulation fr
pp1# ip pp address 192.168.255.4/24
pp1# ip pp ospf area backbone type=point-to-multipoint
pp1# pp enable 1
pp1# pp select none
# save
# interface reset bri1
# ospf configure refresh
```

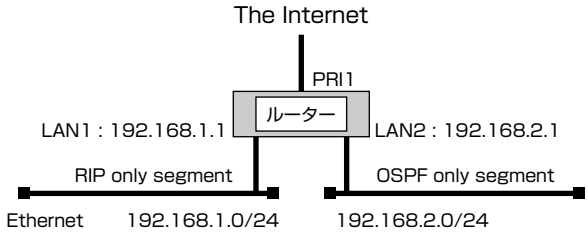
[解説]

バックボーンエリアに所属する 4 台のルーターをフレームリレーで結んだ例です。

1. **line type** コマンドを使用して、回線種別を指定します。
2. **ospf use** コマンドを使用して、ospf を有効にします。
3. **ospf area** コマンドを使用して、ルーターの所属する OSPF エリアを設定します。バックボーンの場合は backbone と指定します。
4. **ip lan1 address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。
5. **ip lan1 ospf area** コマンドを使用して、lan1 の所属する OSPF エリアの設定をします。バックボーンの場合は backbone と指定します。
6. **pp select** コマンドを使用して、相手先番号を選択します。
7. **pp bind** コマンドを使用して、選択した相手番号に BRI ボードをバインドします。
8. **pp encapsulation** コマンドを使用して、pp 側のカプセル化の種類としてフレームリレーを設定します。
9. **ip pp address** コマンドを使用して、回線側インタフェースの IP アドレスを設定します。
10. **ip pp ospf area** コマンドを使用して、回線側インタフェースの所属する OSPF エリアと type を設定します。フレームリレーの場合、type はポイント・マルチポイントをしてします。
11. **pp enable** コマンドを使用して、pp 側のインタフェースを有効にします。
12. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。
13. **interface reset** コマンドを使用して、回線のハードウェアを切替えます。
14. **ospf configure refresh** コマンドを使用して、OSPF の設定を有効にします。

16.4 静的経路、RIP との併用

[構成図]



[ルーターの設定]

```
# pri leased channel 1/1 1 24
# ip route default gateway pp 1
# rip use on
# ospf use on
# ospf area backbone
# ospf import from static
# ospf import from rip
# ip lan1 address 192.168.1.1/24
# ip lan1 ospf area backbone passive
# ip lan2 address 192.168.2.1/24
# ip lan2 ospf area backbone
# ip lan2 rip send off
# ip lan2 rip receive off
# pp select 1
pp1# pp bind pri1/1
pp1# pp enable 1
pp1# ospf configure refresh
```

[解説]

1. **pri leased channel** コマンドを使用して、PRI の情報チャネルとタイムスロットを設定します。
2. **ip route** コマンドを使用して、遠隔地の LAN への経路情報を設定します。
3. **rip use** コマンドを使用して、rip を有効にします。
4. **ospf use** コマンドを使用して、て ospf を有効にします。
5. **ospf area** コマンドを使用して、ルーターの所属する OSPF エリアを設定します。バックボーンの場合は backbone と指定します。
6. **ospf import from** コマンドを使用して、静的設定から経路情報を導入します。
7. **ospf import from** コマンドを使用して、て rip で得た経路情報を導入します。
8. **ip lan1 address** コマンドを使用して、lan1 側の IP アドレスとネットマスクを設定します。
9. **ip lan1 ospf area** コマンドを使用して、lan1 の所属する OSPF エリアを設定します。バックボーンの場合は backbone と指定します。passive 指定で lan1 に OSPF パケットを送出しないように設定します。
10. **ip lan2 address** コマンドを使用して、lan2 側の IP アドレスをネットマスクを設定します。
11. **ip lan2 ospf area** コマンドを使用して、lan2 の所属する OSPF エリアを設定します。バックボーンの場合は backbone と指定します。
12. **ip lan2 rip send** コマンドを使用して、lan2 で rip 情報を送出しないように設定します。

13. **ip lan2 rip receive** コマンドを使用して、lan2 で rip 情報を受け取らないように設定します。

14. **pp select** コマンドを使用して、相手先番号を選択します。

15. **pp bind** コマンドを使用して、選択した相手番号に PRI ポートと指定チャネルをバインドします。

16. **pp enable** コマンドを使用して、pp 側のインタフェースを有効にします。

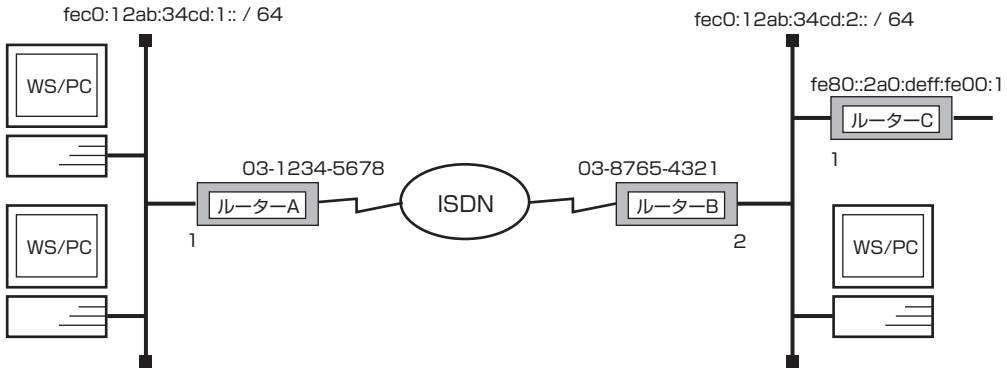
17. IPv6 設定例

1. IPv6LAN 間接続 (静的経路設定、ISDN)
2. IPv6LAN 間接続 (動的経路設定、専用線)
3. IPv6 over IPv4 トンネリング

17.1 IPv6LAN 間接続 (静的経路設定、ISDN)

RT 自身の LAN 側アドレスとして IPv6 アドレスを手動設定します。LAN 側ホストからの RS(Router Solicitation) に対して RA(Router Advertisement) を広告し、ルーターとしての存在と LAN のプレフィックスを通知します。
ルーティング情報として静的なデフォルトルートを設定し、ISDN 回線を介した LAN 間接続を行います。

[構成図]



・ルーター B 側の LAN のデフォルトゲートウェイはルーター C とする

[ルーター A の設定手順]

```
# ipv6 lan1 address fec0:12ab:34cd:1::1/64
# ipv6 prefix 1 fec0:12ab:34cd:1::/64
# ipv6 lan1 rtadv send 1
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 0387654321
pp1# pp enable 1
pp1# pp select none
# ipv6 route default gateway pp 1
# save
```

[ルーター B の設定手順]

```
# ipv6 lan1 address fec0:12ab:34cd:2::2/64
# ipv6 prefix 1 fec0:12ab:34cd:2::/64
# ipv6 lan1 rtadv send 1
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 0312345678
pp1# pp enable 1
pp1# pp select none
# ipv6 route fec0:12ab:34cd:1::/64 gateway pp 1
# ipv6 route default gateway fe80::2a0:deff:fe00:1%1
# save
```

[解説]

■ルーター A

1. # ipv6 lan1 address fec0:12ab:34cd:1::1/64
   ルーターの IPv6 アドレスを設定します。

2. # ipv6 prefix 1 fec0:12ab:34cd:1::/64
   # ipv6 lan1 rtadv send 1
   LAN 側に広告するプレフィックスを設定します。

3. # pp select 1
   pp1# pp bind bri1
   pp1# isdn remote address call 0387654321
   pp1# pp enable 1
   pp1# pp select none
   相手先情報を設定します。

4. # ipv6 route default gateway pp 1
   # save
   宛先が LAN 外であるすべてのパケットを送るためのデフォルトルートを pp1 に設定します。

■ルーター B

1. 経路情報以外の基本的な設定はルーター A と同じです。
   ルーターの IPv6 アドレスを設定します。

2. # ipv6 prefix 1 fec0:12ab:34cd:2::/64
   # ipv6 lan1 rtadv send 1
   LAN 側に広告するプレフィックスを設定します。

3. # pp select 1
   pp1# pp bind bri1
   pp1# isdn remote address call 0312345678
   pp1# pp enable 1
   pp1# pp select none
   相手先情報を設定します。

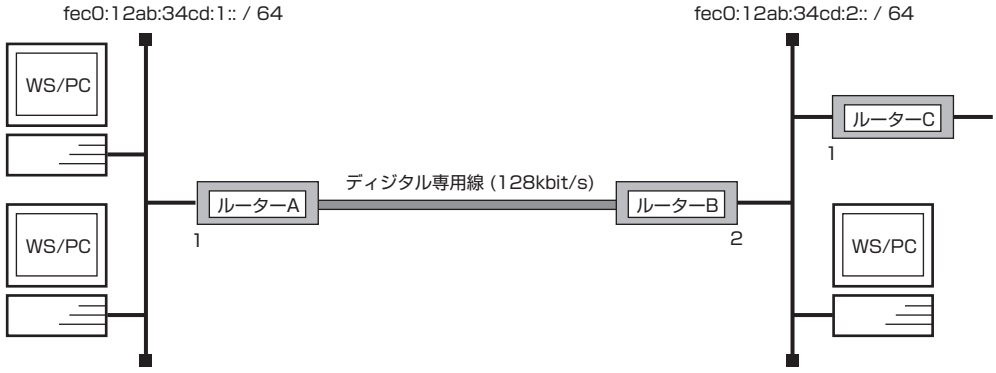
4. # ipv6 route fec0:12ab:34cd:1::/64 gateway pp 1
   相手側 LAN の経路情報を設定します。

5. # ipv6 route default gateway fe80::2a0:deff:fe00:1%1
   # save
   宛先が LAN 外であるすべてのパケットを送るためのデフォルトルートを LAN 側のデフォルトゲートウェイに設定します。

17.2 IPv6LAN 間接続 (動的経路設定、専用線)

RT 自身の LAN 側アドレスとして IPv6 アドレスを手動設定します。LAN 側ホストからの RS(Router Solicitation) に対して RA(Router Advertisement) を広告し、ルーターとしての存在と LAN のプレフィックスを通知します。
ルーティング制御として RIPng を使用し、128k 専用線を介した LAN 間接続を行います。

[構成図]



・ルーター B 側の LAN のデフォルトゲートウェイはルーター C とする

[ルーター A の設定手順]

```
# line type bri1 l128
# ipv6 lan1 address fec0:12ab:34cd:1::1/64
# ipv6 prefix 1 fec0:12ab:34cd:1::/64
# ipv6 lan1 rtadv send 1
# ipv6 rip use on
# pp select 1
pp1# pp bind bri1
pp1# ipv6 pp rip connect send interval
pp1# pp enable 1
pp1# pp select none
# save
# interface reset bri1
```

[ルーター B の設定手順]

```
# line type bri1 l128
# ipv6 lan1 address fec0:12ab:34cd:2::2/64
# ipv6 prefix 1 fec0:12ab:34cd:2::/64
# ipv6 lan1 rtadv send 1
# ipv6 rip use on
# pp select 1
pp1# pp bind bri1
pp1# ipv6 pp rip connect send interval
pp1# pp enable 1
pp1# pp select none
# save
# interface reset bri1
```

[解説]

■ルーター A

1. # line type bri1 l128
   回線種別を設定します。この設定はインタフェースリセットあるいは装置の再起動を行った後に有効になります。

2. # ipv6 lan1 address fec0:12ab:34cd:1::1/64
   ルーターの IPv6 アドレスを設定します。

3. # ipv6 prefix 1 fec0:12ab:34cd:1::/64
   # ipv6 lan1 rtadv send 1
   LAN 側に広告するプレフィックスを設定します。

4. # ipv6 rip use on
   RIPng の使用を設定します。LAN/PP 側共に使用します。

5. # pp select 1
   pp1# pp bind bri1
   pp1# ipv6 pp rip connect send interval
   pp1# pp enable 1
   pp1# pp select none
   相手先情報を設定します。

6. # save
   # interface reset bri1
   回線種別がデフォルトと異なるのでインタフェースをリセットします。**restart** コマンドによる装置全体の再起動でもかまいません。

■ルーター B

1. 経路情報以外の基本的な設定はルーター A と同じです。
   # line type bri1 l128
   回線種別を設定します。この設定はインタフェースリセットあるいは装置の再起動を行った後に有効になります。

2. # ipv6 lan1 address fec0:12ab:34cd:2::2/64
   ルーターの IPv6 アドレスを設定します。

3. # ipv6 prefix 1 fec0:12ab:34cd:2::/64
   # ipv6 lan1 rtadv send 1
   LAN 側に広告するプレフィックスを設定します。

4. # ipv6 rip use on
   RIPng の使用を設定します。LAN/PP 側共に使用します。

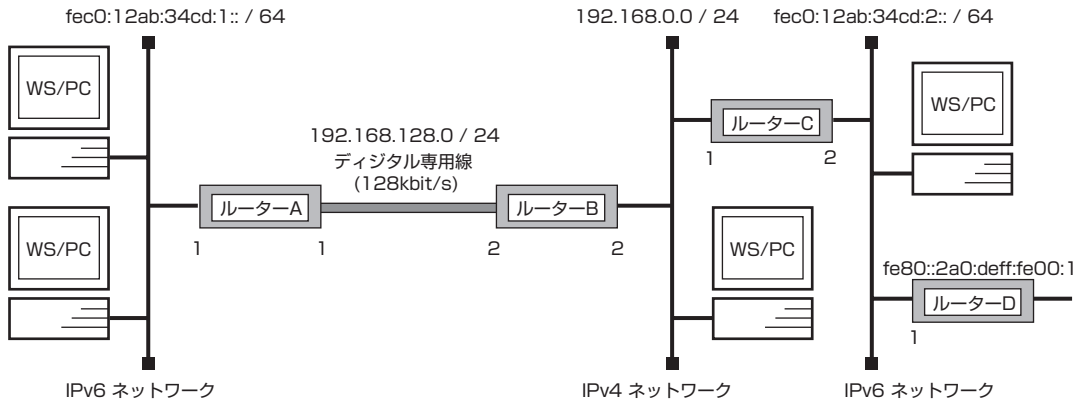
5. # pp select 1
   pp1# pp bind bri1
   pp1# ipv6 pp rip connect send interval
   pp1# pp enable 1
   pp1# pp select none
   相手先情報を設定します。

6. # save
   # interface reset bri1
   回線種別がデフォルトと異なるのでインタフェースをリセットします。**restart** コマンドによる装置全体の再起動でもかまいません。

17.3 IPv6 over IPv4 トンネリング

IPv6 ネットワーク間に IPv4 ネットワークがある場合、IPv6 over IPv4 トンネルとして IPv6 パケットの送出が可能です。両 IPv6 ネットワーク間のパケットは、IPv4 ネットワーク内においては IPv4 パケットとして通過することになります。トンネルのエンドポイントとなるルーターは IPv4 アドレスを持つ必要がありますので、回線を経由する場合には numbered 接続となります。

[構成図]



・ルーター A の LAN とルーター C の一方の LAN が IPv6 ネットワーク
・ルーター B の LAN は IPv4 ネットワーク
・ルーター A とルーター C 間で IPv6 over IPv4 トンネリングを行う
・ルーター D を IPv6 ネットワークのデフォルトゲートウェイとする

[ルーター A の設定手順]

```
# line type bri1 l128
# ipv6 lan1 address fec0:12ab:34cd:1::1/64
# ipv6 prefix 1 fec0:12ab:34cd:1::/64
# ipv6 lan1 rtadv send 1
# pp select 1
pp1# pp bind bri1
pp1# ip pp address 192.168.128.1/24
pp1# ip pp remote address 192.168.128.2
pp1# pp enable 1
pp1# tunnel select 1
tunnel1# tunnel encapsulation ipip
tunnel1# tunnel endpoint address 192.168.128.1 192.168.0.1
tunnel1# tunnel enable 1
tunnel1# tunnel select none
# ipv6 route default gateway tunnel 1
# ip route 192.168.0.0/24 gateway pp 1
# save
# interface reset bri1
```

[ルーター B の設定手順]

```
# line type bri1 l128
# ip lan1 address 192.168.0.2/24
# pp select 1
pp1# pp bind bri1
pp1# pp enable 1
pp1# ip pp address 192.168.128.2/24
pp1# ip pp remote address 192.168.128.1
pp1# pp select none
# save
# interface reset bri1
```

[ルーター C の設定手順]

```
# ip lan1 address 192.168.0.1/24
# ipv6 lan2 address fec0:12ab:34cd:2::2/64
# ipv6 prefix 1 fec0:12ab:34cd:2::/64
# ipv6 lan2 rtadv send 1
# tunnel select 1
tunnel1# tunnel encapsulation ipip
tunnel1# tunnel endpoint address 192.168.0.1 192.168.128.1
tunnel1# tunnel enable 1
tunnel1# tunnel select none
# ipv6 route fec0:12ab:34cd:1::/64 gateway tunnel 1
# ipv6 route default gateway fe80::2a0:deff:fe00:1%2
# ip route 192.168.128.0/24 gateway 192.168.0.2
# save
```

[解説]

■ルーター A

1. LAN 側が IPv6 ネットワーク、PP 側が IPv4 ネットワークとなります。
   # line type bri1 l128
   回線種別を設定します。この設定はインタフェースリセットあるいは装置の再起動を行った後に有効になります。

2. # ipv6 lan1 address fec0:12ab:34cd:1::1/64
   # ipv6 prefix 1 fec0:12ab:34cd:1::/64
   # ipv6 lan1 rtadv send 1
   LAN 側は IPv6 ネットワークです。IPv6 アドレスとプレフィックスを設定します。

3. # pp select 1
   pp1# pp bind bri1
   pp1# ip pp address 192.168.128.1/24
   pp1# ip pp remote address 192.168.128.2
   pp1# pp enable 1
   pp 側に IPv4 アドレスを設定します。このインタフェース経由で IPv6 over IPv4 トンネリングを行います。

4. pp1# tunnel select 1
   tunnel1# tunnel encapsulation ipip
   トンネル経路に IPv6 over IPv4 トンネリングのカプセル化を設定します。

5. tunnel1# tunnel endpoint address 192.168.128.1 192.168.0.1
   tunnel1# tunnel enable 1
   tunnel1# tunnel select none
   IPv6 over IPv4 トンネリングのエンドポイントの IPv4 アドレスを設定します。ローカル側のアドレスは自身の pp 側アドレスです。

6. # ipv6 route default gateway tunnel 1
   IPv6 パケットに関しては LAN 外へのパケットはすべてトンネルの先の LAN へ送る経路をデフォルト経路として設定します。

7. # ip route 192.168.0.0/24 gateway pp 1
   カプセル化されたパケットは 192.168.0.1 宛に送られます。
   このための経路情報を IPv4 の経路として設定します。

8. # save
   # interface reset bri1
   回線種別がデフォルトと異なるのでインタフェースをリセットします。**restart** コマンドによる装置全体の再起動でもかまいません。

■ルーター B

1. IPv4 ネットワークにのみ存在するルーターです。IPv6 に関する設定は一切不要です。
   # line type bri1 l128
   回線種別を設定します。この設定はインタフェースリセットあるいは装置の再起動を行った後に有効になります。

2. # ip lan1 address 192.168.0.2/24
   # pp select 1
   pp1# pp bind bri1
   pp1# pp enable 1
   pp1# ip pp address 192.168.128.2/24
   pp1# ip pp remote address 192.168.128.1
   pp1# pp select none
   LAN 側アドレスと PP 側アドレスを設定します。この時点で LAN/PP 双方に対するネットワークが設定され、IPv4 パケットの両ネットワーク間でのルーティングが可能となります。

3. # save
   # interface reset bri1
   回線種別がデフォルトと異なるのでインタフェースをリセットします。**restart** コマンドによる装置全体の再起動でもかまいません。

■ルーター C

1. LAN1 側が IPv4 ネットワークに属し、IPv6 over IPv4 トンネルのエンドポイントとなります。LAN2 側が IPv6 ネットワークに属します。
   # ip lan1 address 192.168.0.1/24
   LAN1 側は IPv4 ネットワークです。IPv4 アドレスを設定します。
   IPv6 over IPv4 トンネリングのエンドポイントとなります。

2. # ipv6 lan2 address fec0:12ab:34cd:2::2/64
   # ipv6 prefix 1 fec0:12ab:34cd:2::/64
   # ipv6 lan2 rtadv send 1

   LAN2 側は IPv6 ネットワークです。IPv6 アドレスを設定します。

3. # tunnel select 1
   tunnel1# tunnel encapsulation ipip
   トンネル経路に IPv6 over IPv4 トンネリングのカプセル化を設定します。

4. tunnel1# tunnel endpoint address 192.168.0.1 192.168.128.1
   tunnel1# tunnel enable 1
   tunnel1# tunnel select none
   IPv6 over IPv4 トンネリングのエンドポイントの IPv4 アドレスを設定します。ローカル側のアドレスは自身の LAN1 側アドレスです。

5. # ipv6 route fec0:12ab:34cd:1::/64 gateway tunnel 1
   IPv6 over IPv4 トンネルの先の IPv6 ネットワークへの経路を設定します。

6. # ipv6 route default gateway fe80::2a0:deff:fe00:1%2
   IPv6 ネットワークのデフォルト経路を設定します。

7. # ip route 192.168.128.0/24 gateway 192.168.0.2
   # save
   カプセル化されたパケットは 192.168.128.1 宛に送られます。
   このための経路情報を IPv4 の経路として設定します。

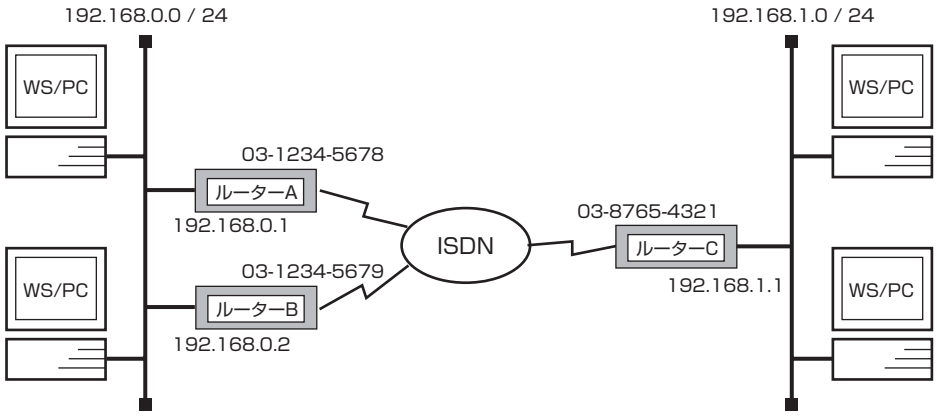
18. VRRP (Virtual Router Redundancy Protocol) 設定例

1. VRRP で 2 台のルーターの冗長構成
2. VRRP で 2 台のルーターの冗長構成 (シャットダウントリガ)
3. VRRP + IPsec

18.1 VRRP で 2 台のルーターの冗長構成

VRRP により、冗長性の確保が可能となります。VRRP ルーターのグループは、実際にパケット配送を行うマスタルーターと、そのバックアップとなるバックアップルーターとからなります。VRRP ルーターは 1 つの仮想的な IP アドレス /MAC アドレスを共有し、その仮想アドレスを持つ仮想ルーターをデフォルトゲートウェイとして動作する PC のトラフィックを、協調して処理します。

[構成図]



・ルーター A がマスタルーター、ルーター B がバックアップルーター
・ルーター C に対するダイヤルアップ環境において、192.168.0.1/24 側ルーターの冗長性を確保する

[ルーター A の設定手順]

```
# isdn local address bri1 0312345678
# ip lan1 address 192.168.0.1/24
# ip lan1 vrrp 1 192.168.0.128 priority=200
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 0387654321
pp1# pp enable 1
pp1# pp select none
# ip route 192.168.1.0/24 gateway pp 1
# save
```

[ルーター B の設定手順]

```
# isdn local address bri1 0312345679
# ip lan1 address 192.168.0.2/24
# ip lan1 vrrp 1 192.168.0.128
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 0387654321
pp1# pp enable 1
pp1# pp select none
# ip route 192.168.1.0/24 gateway pp 1
# save
```

[ルーター C の設定手順]

```
# isdn local address bri1 0387654321
# ip lan1 address 192.168.1.1/24
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 0312345678 0312345679
pp1# pp enable 1
pp1# pp select none
# ip route 192.168.0.0/24 gateway pp 1
# save
```

[解説]

■ルーター A

1. # isdn local address bri1 0312345678
   # ip lan1 address 192.168.0.1/24
   # ip lan1 vrrp 1 192.168.0.128 priority=200
   LAN 側アドレスと VRRP の設定を行います。LAN 側 IP アドレスと違う IP アドレスを仮想ルーターの IP アドレスとして設定します。
   このルーターをマスタとするように優先度を 200 に設定します。
   優先度の値はデフォルトで 100 です。

2. # pp select 1
   pp1# pp bind bri1
   pp1# isdn remote address call 0387654321
   pp1# pp enable 1
   回線接続先の情報を設定します。

3. pp1# pp select none
   # ip route 192.168.1.0/24 gateway pp 1
   # save
   経路情報を設定します。

■ルーター B

1. # isdn local address bri1 0312345679
   # ip lan1 address 192.168.0.2/24
   # ip lan1 vrrp 1 192.168.0.128
   LAN 側アドレスと VRRP の設定を行います。優先度の値はデフォルトで 100 ですので、この設定では仮想 IP アドレス 192.168.0.128 のバックアップルーターとして働きます。
   マスタルーターからのパケットを一定時間受け取らなくなると、自身がマスタルーターとなりパケットを処理し始めます。

2. # pp select 1
   pp1# pp bind bri1
   pp1# isdn remote address call 0387654321
   pp1# pp enable 1
   回線接続先の情報を設定します。この例の場合接続先はマスタルーターと同じですので、設定も同一となります。

3. pp1# pp select none
   # ip route 192.168.1.0/24 gateway pp 1
   # save
   経路情報を設定します。このように経路情報もマスタルーターと同じものとなりますので、LAN 側で動的経路制御を使用することはできません。

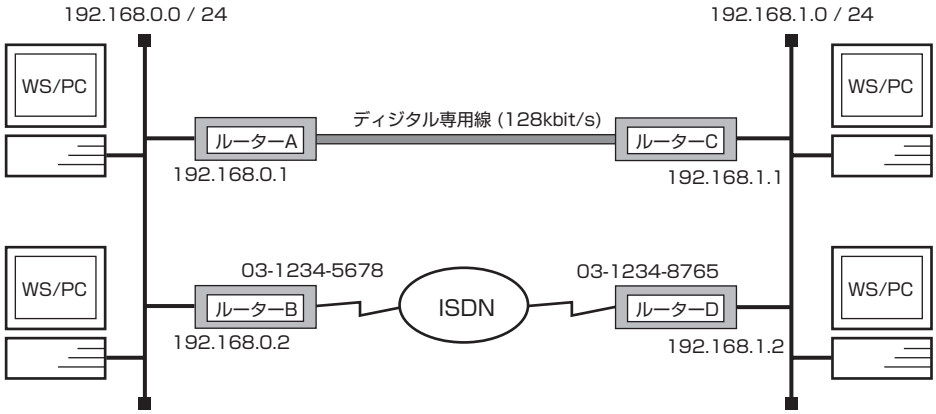
■ルーター C

1. # isdn local address bri1 0387654321
   # ip lan1 address 192.168.1.1/24
   # pp select 1
   pp1# pp bind bri1
   pp1# isdn remote address call 0312345678 0312345679
   pp1# pp enable 1
   pp1# pp select none
   # ip route 192.168.0.0/24 gateway pp 1
   # save
   相手側のバックアップ動作には関知せず、同一の pp として扱います。

18.2 VRRP で２台のルーターの冗長構成 (シャットダウントリガ)

マスタルーターはＬＡＮから切り離されたり、電源が落ちたりした場合には不可避的にシャットダウンしますが、回線側での通信が何らかの理由でできなくなった場合に積極的にシャットダウンし、それをバックアップルーターに通知し、マスタを切り替えることもできます。

[構成図]



・ルーター A がマスタルーター、ルーター B がバックアップルーター
・192.168.0.1/24 側ルーターの冗長性を確保する
・192.168.1.0/24 側では RIP を使って経路を切り替える

[ルーター A の設定手順]

```
# line type bri1 l128
# ip lan1 address 192.168.0.1/24
# rip use on
# ip lan1 rip send off
# ip lan1 rip receive off
# ip lan1 vrrp 1 192.168.0.128 priority=200
# ip lan1 vrrp shutdown trigger 1 pp 1
# pp select 1
pp1# pp bind bri1
pp1# pp keepalive use lcp-echo
pp1# ip pp rip connect send interval
pp1# pp enable 1
pp1# pp select none
# ip route 192.168.1.0/24 gateway pp 1
# save
# interface reset bri1
```

[ルーター B の設定手順]

```
# isdn local address bri1 0312345678
# ip lan1 address 192.168.0.2/24
# rip use on
# ip lan1 rip send off
# ip lan1 rip receive off
# ip lan1 vrrp 1 192.168.0.128
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 0312348765
pp1# ip pp rip connect send interval
pp1# ip pp rip hop out 2
pp1# pp enable 1
pp1# pp select none
# ip route 192.168.1.0/24 gateway pp 1
# save
```

[ルーター C の設定手順]

```
# line type bri1 l128
# ip lan1 address 192.168.1.1/24
# rip use on
# pp select 1
pp1# pp bind bri1
pp1# pp keepalive use lcp-echo
pp1# pp enable 1
pp1# pp select none
# save
# interface reset bri1
```

[ルーター D の設定手順]

```
# isdn local address bri1 0312348765
# ip lan1 address 192.168.1.2/24
# rip use on
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 0312345678
pp1# pp enable 1
pp1# pp select none
# save
```

[解説]

■ルーター A

1. # line type bri1 l128
   回線種別を設定します。この設定はインタフェースリセットあるいは装置の再起動を行った後に有効になります。

2. # ip lan1 address 192.168.0.1/24
   # rip use on
   # ip lan1 rip send off
   # ip lan1 rip receive off
   LAN 側アドレスと RIP の使用を設定します。バックアップ回線に相手側からの経路を向かせるために、pp 側に対して RIP を使います。LAN 側は VRRP を使用するため、RIP は使用しないように制限します。

3. # ip lan1 vrrp 1 192.168.0.128 priority=200
   # ip lan1 vrrp shutdown trigger 1 pp 1
   VRRP の設定を行います。LAN 側 IP アドレスと違う IP アドレスを仮想ルーターの IP アドレスとして設定します。
   このルーターをマスタとするように優先度を 200 に設定します。
   pp1 のインターフェースがダウンした場合にバックアップルーターに切りかえるよう、シャットダウントリガを設定します。

4. # pp select 1
   pp1# pp bind bri1
   pp1# pp keepalive use lcp-echo
   専用線のダウンを検出するためにキープアライブを設定します。

5. pp1# ip pp rip connect send interval
   デフォルトでは経路の変更があった場合のみ広告することになっており、VRRP の動作に追従しないことがありますので、経路は定期的に広告するものとします。

6. pp1# pp enable 1
   pp1# pp select none
   # ip route 192.168.1.0/24 gateway pp 1
   pp 側への経路を静的に設定します。

7. # save
   # interface reset bri1
   回線種別がデフォルトと異なるのでインタフェースをリセットします。**restart** コマンドによる装置全体の再起動でもかまいません。

■ルーター B

1. # isdn local address bri1 0312345678
   # ip lan1 address 192.168.0.2/24
   # rip use on
   # ip lan1 rip send off
   # ip lan1 rip receive off
   マスタ側と同様の設定です。LAN 側では RIP を使用しません。

2. # ip lan1 vrrp 1 192.168.0.128
   仮想 IP アドレス 192.168.0.128 のバックアップルーターとして働きます。
   優先度を省略した場合には、デフォルト値の 100 が優先度として与えられます。
   マスタルーターからのパケットを一定時間受け取らなくなると、自身がマスタルーターとなりパケットを処理し始めます。

3. # pp select 1
   pp1# pp bind bri1
   pp1# isdn remote address call 0312348765
   pp1# ip pp rip connect send interval
   pp1# ip pp rip hop out 2
   相手側 LAN 上の経路情報を VRRP の動作に追従させるため、経路は定期的に広告するものとします。またバックアップ経路からの復帰をスムーズに行うために、バックアップ経路で広告するホップ数を多く設定します。

4. pp1# pp enable 1
   pp1# pp select none
   # ip route 192.168.1.0/24 gateway pp 1
   # save
   pp 側への経路を静的に設定します。

■ルーター C

1. # line type bri1 l128
   回線種別を設定します。この設定はインタフェースリセットあるいは装置の再起動を行った後に有効になります。

2. # ip lan1 address 192.168.1.1/24
   # rip use on
   LAN 側および PP 側で RIP を使用します。これにより、LAN 上の複数のルーター間で pp 側の経路情報の交換が可能となり、経路が切り替わった場合にも対応できることになります。

3. # pp select 1
   pp1# pp bind bri1
   pp1# pp keepalive use lcp-echo
   専用線のダウンを検出するためにキープアライブを設定します。

4. pp1# pp enable 1
   pp1# pp select none
   # save
   # interface reset bri1
   回線種別がデフォルトと異なるのでインタフェースをリセットします。**restart** コマンドによる装置全体の再起動でもかまいません。

■ルーター D

1. # isdn local address bri1 0312348765
   # ip lan1 address 192.168.1.2/24
   # rip use on
   LAN 側および PP 側で RIP を使用します。これにより、LAN 上の複数のルーター間で pp 側の経路情報の交換が可能となり、経路が切り替わった場合にも対応できることになります。

2. # pp select 1
   pp1# pp bind bri1
   pp1# isdn remote address call 0312345678
   pp1# pp enable 1
   pp1# pp select none
   # save
   バックアップ用回線の受け側として、相手先情報を設定します。

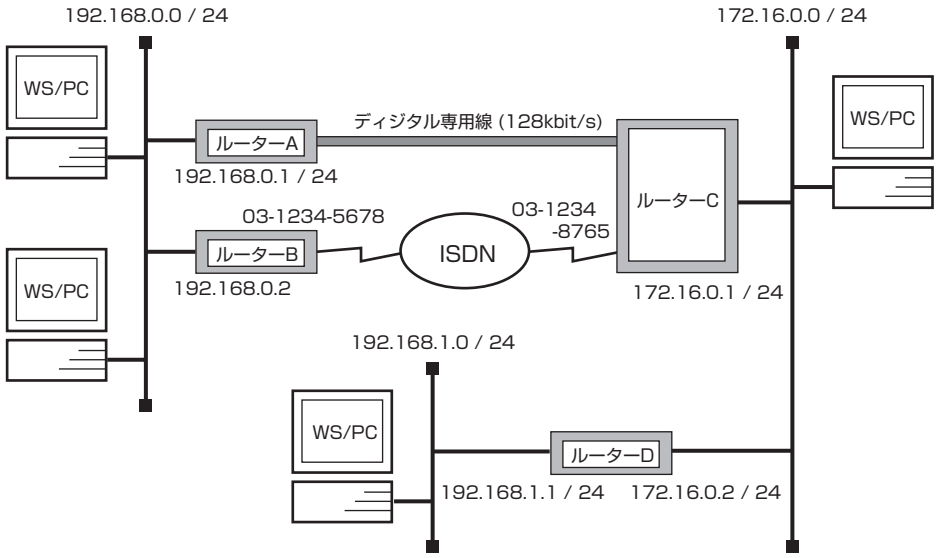
なお、192.168.1.0/24 側の 2 台のルーターを複数ポートモデル 1 台に置き換えた場合の設定手順は、以下のようになります。

```
# ip lan1 address 192.168.1.1/24
# line type bri1 l128
# rip use on
# pp select 1
pp1# pp bind bri1
pp1# pp keepalive use lcp-echo
pp1# pp enable 1
pp1# pp select none
# interface reset bri1
# pp select 2
pp2# pp bind bri2
pp2# isdn local address bri2 0312348765
pp2# isdn remote address call 0312345678
pp2# pp enable 2
pp2# pp select none
# save
```

18.3 VRRP + IPsec

VRRP で運用されるルーターをセキュリティゲートウェイとしても動作させることが可能です。

[構成図]



・ルーター A がマスタルーター、ルーター B がバックアップルーター
・192.168.0.1/24 側ルーターの冗長性を確保する
・192.168.0.0/24 と 192.168.1.0/24 との間で IPsec を行う
・ルーター A,B 及びルーター D がセキュリティゲートウェイとなる

[ルーター A の設定手順]

```
# line type bri1 l128
# ip lan1 address 192.168.0.1/24
# rip use on
# ip lan1 rip send off
# ip lan1 rip receive off
# ip lan1 vrrp 1 192.168.0.128 priority=200
# ip lan1 vrrp shutdown trigger 1 pp 1
# pp select 1
pp1# pp bind bri1
pp1# pp keepalive use lcp-echo
pp1# ip filter 1 reject 192.168.1.0/24 *
pp1# ip filter 2 pass * *
pp1# ip pp rip filter out 1 2
pp1# ip pp rip connect send interval
pp1# pp enable 1
pp1# pp select none
# ipsec ike local address 1 vrrp lan1 1
# ipsec ike remote address 1 172.16.0.2
# ipsec ike pre-shared-key 1 text IKEsecretPASS
# ipsec sa policy 101 1 esp des-cbc md5-hmac
# tunnel select 1
tunnel1# ip route 192.168.1.0/24 gateway tunnel 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel enable 1
tunnel1# ipsec auto refresh on
tunnel1# tunnel select none
# ip route default gateway pp 1
# save
# interface reset bri1
```

[ルーター B の設定手順]

```
# ip lan1 address 192.168.0.2/24
# rip use on
# ip lan1 rip send off
# ip lan1 rip receive off
# ip lan1 vrrp 1 192.168.0.128
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 0312348765
pp1# ip filter 1 reject 192.168.1.0/24 *
pp1# ip filter 2 pass * *
pp1# ip pp rip filter out 1 2
pp1# ip pp rip connect send interval
pp1# ip pp rip hop out 2
pp1# pp enable 1
pp1# pp select none
# ipsec ike local address 1 vrrp lan1 1
# ipsec ike remote address 1 172.16.0.2
# ipsec ike pre-shared-key 1 text IKEsecretPASS
# ipsec sa policy 101 1 esp des-cbc md5-hmac
# tunnel select 1
tunnel1# ip route 192.168.1.0/24 gateway tunnel 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel enable 1
tunnel1# ipsec auto refresh on
tunnel1# tunnel select none
# ip route default gateway pp 1
# save
```

[ルーター C の設定手順]

```
# line type bri2.1 l128
# ip lan1 address 172.16.0.1/24
# rip use on
# pp select 1
pp1# pp bind bri2.1
pp1# pp keepalive use lcp-echo
pp1# pp enable 1
pp1# pp select 2
pp2# pp bind bri2.2
pp2# isdn local address bri2.2 0312348765
pp2# isdn remote address call 0312345678
pp2# pp enable 2
# save
# interface reset bri2.1
```

[ルーター D の設定手順]

```
# ip lan1 address 172.16.0.2/24
# ip lan2 address 192.168.1.1/24
# rip use on
# ip filter 1 reject 192.168.0.0/24 *
# ip filter 2 pass * *
# ip lan1 rip filter out 1 2
# ipsec ike remote address 1 192.168.0.128
# ipsec ike pre-shared-key 1 text IKEsecretPASS
# ipsec sa policy 101 1 esp des-cbc md5-hmac
# tunnel select 1
tunnel1# ip route 192.168.0.0/24 gateway tunnel 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel enable 1
tunnel1# ipsec auto refresh on
tunnel1# tunnel select none
# ip route 192.168.0.128 gateway 172.16.0.1
# save
```

[解説]

■ルーター A

1. # line type bri1 l128
   回線種別を設定します。この設定はインタフェースリセットあるいは装置の再起動を行った後に有効になります。

2. # ip lan1 address 192.168.0.1/24
   # rip use on
   # ip lan1 rip send off
   # ip lan1 rip receive off
   LAN 側アドレスと RIP の使用を設定します。バックアップ回線に相手側の経路を向かせるために、pp 側に対して RIP を使います。LAN 側は VRRP を使用するため、RIP は使用しないように制限します。

3. # ip lan1 vrrp 1 192.168.0.128 priority=200
   # ip lan1 vrrp shutdown trigger 1 pp 1
   VRRP の設定を行います。このルーターをマスタとするように優先度を 200 に設定します。優先度の値はデフォルトでは 100 です。また pp1 のインタフェースがダウンした場合にバックアップルーターに切りかえるよう、シャットダウントリガを設定します。

4. # pp select 1
   pp1# pp bind bri1
   pp1# pp keepalive use lcp-echo
   専用線のダウンを検出するためにキープアライブを設定します。

5. pp1# ip filter 1 reject 192.168.1.0/24 *
   pp1# ip filter 2 pass * *
   pp1# ip pp rip filter out 1 2
   RIP でトンネル向けの経路を pp 側に送らないようにフィルタリングします。合致しない経路情報はすべて遮断されることになりますので、該当経路以外の情報を送るためにフィルタ 2 の設定が必要です。

6. pp1# ip pp rip connect send interval
   デフォルトでは経路の変更があった場合のみ広告することになっており、VRRP の動作に追従しないことがありますので、経路は定期的に広告するものとします。

7. pp1# pp enable 1
   pp1# pp select none
   # ipsec ike local address 1 vrrp lan1 1
   # ipsec ike remote address 1 172.16.0.2
   # ipsec ike pre-shared-key 1 text IKEsecretPASS
   # ipsec sa policy 101 1 esp des-cbc md5-hmac
   IPsec の定義を設定します。自分側のセキュリティゲートウェイアドレスとして vrrp を指定し、VRRP マスターとして動作している時のみ、VRRP の仮想 IP アドレスを自分側セキュリティゲートウェイアドレスとして鍵交換を行います。pre-shared-key は相手側と同じものを設定する必要があります。暗号化を行い、アルゴリズムに des-cbc を、かつ認証に md5-hmac を用います。

8. # tunnel select 1
   tunnel1# ip route 192.168.1.0/24 gateway tunnel 1
   tunnel1# ipsec tunnel 101
   tunnel1# tunnel enable 1
   tunnel1# ipsec auto refresh on
   相手側 LAN との通信に IPsec を用いるため、その経路をトンネルルートに設定します。また IPsec 定義の適用と自動鍵交換を行うよう設定します。

9. tunnel1# tunnel select none
   # ip route default gateway pp 1
   その他のパケットは IPsec の対象とせず、pp 側に送ります。

10. # save
    # interface reset bri1
    回線種別がデフォルトと異なるのでインタフェースをリセットします。**restart** コマンドによる装置全体の再起動でもかまいません。

■ルーター B

1. # ip lan1 address 192.168.0.2/24
   # rip use on
   # ip lan1 rip send off
   # ip lan1 rip receive off
   LAN 側アドレスと RIP の使用を設定します。このルーターの回線に相手側からの経路を向かせるために、pp 側に対して RIP を使います。LAN 側は VRRP を使用するため、RIP は使用しないように制限します。

2. # ip lan1 vrrp 1 192.168.0.128
   仮想 IP アドレス 192.168.0.128 のバックアップルーターとして働きます。マスタルーターからのパケットを一定時間受け取らなくなると、自身がマスタルーターとなりパケットを処理し始めます。

3. # pp select 1
   pp1# pp bind bri1
   pp1# isdn remote address call 11
   pp1# ip filter 1 reject 192.168.1.0/24 *
   pp1# ip filter 2 pass * *
   pp1# ip pp rip filter out 1 2
   RIP でトンネル向けの経路を pp 側に送らないようにフィルタリングします。合致しない経路情報はすべて遮断されることになりますので、該当経路以外の情報を送るためにフィルタ 2 の設定が必要です。

4. pp1# ip pp rip connect send interval
   pp1# ip pp rip hop out 2
   デフォルトでは経路の変更があった場合のみ広告することになっており、VRRP の動作に追従しないことがありますので、経路は定期的に広告するものとします。またバックアップ経路からの復帰をスムーズに行うために、バックアップ経路で広告するホップ数を多く設定します。

5. pp1# pp enable 1
   pp1# pp select none
   # ipsec ike local address 1 vrrp lan1 1
   # ipsec ike remote address 1 172.16.0.2
   # ipsec ike pre-shared-key 1 text IKEsecretPASS
   # ipsec sa policy 101 1 esp des-cbc md5-hmac
   IPsec に関してルーター A と同じ定義を設定します。自分側のセキュリティゲートウェイアドレスとして vrrp を指定し、VRRP マスターとして動作している時のみ、VRRP の仮想 IP アドレスを自分側セキュリティゲートウェイアドレスとして鍵交換を行います。

6. # tunnel select 1
   tunnel1# ip route 192.168.1.0/24 gateway tunnel 1
   tunnel1# ipsec tunnel 101
   tunnel1# tunnel enable 1
   tunnel1# ipsec auto refresh on
   相手側 LAN との通信に IPsec を用いるため、その経路をトンネルルートに設定します。また IPsec 定義の適用と自動鍵交換を行うよう設定します。

7. tunnel1# tunnel select none
   # ip route default gateway pp 1
   その他のパケットは IPsec の対象とせず、pp 側に送ります。

8. # save

■ルーター C

1. # line type bri2.1 l128
   回線種別を設定します。この設定はインタフェースリセットあるいは装置の再起動を行った後に有効になります。

2. # ip lan1 address 172.16.0.1/24
   # rip use on
   RIP を使います。特に回線側で経路が変わったことを検出するためです。

3. # pp select 1
   pp1# pp bind bri2.1
   pp1# pp keepalive use lcp-echo
   pp1# pp enable 1
   ルーター A と接続するための設定です。専用線のダウンを検出するためにキープアライブを設定します。

4. pp1# pp select 2
   pp2# pp bind bri2.2
   pp2# isdn local address bri2.2 11
   pp2# isdn remote address call 21
   pp2# pp enable 2
   ルーター B と接続するための設定です。

5. # save
   # interface reset bri2.1
   回線種別がデフォルトと異なるのでインタフェースをリセットします。restart コマンドによる装置全体の再起動でもかまいません。

■ルーター D

1. # ip lan1 address 172.16.0.2/24
   # ip lan2 address 192.168.1.1/24
   # rip use on
   # ip filter 1 reject 192.168.0.0/24 *
   # ip filter 2 pass * *
   # ip lan1 rip filter out 1 2

RIP でトンネル向けの経路を lan1 側に送らないようにフィルタリングします。合致しない経路情報はすべて遮断されることになりますので、該当経路以外の情報を送るためにフィルタ 2 の設定が必要です。

2. # ipsec ike remote address 1 192.168.0.128
   # ipsec ike pre-shared-key 1 text IKEsecretPASS
   # ipsec sa policy 101 1 esp des-cbc md5-hmac
   IPsec の定義を設定します。相手側のセキュリティゲートウェイアドレスを相手側の VRRP 仮想 IP アドレスとします。バックアップ動作に関してはこちら側では一切関知しません。pre-shared-key は相手側と同じものを設定する必要があります。暗号化を行い、アルゴリズムに des-cbc を、かつ認証に md5-hmac を用います。

3. # tunnel select 1
   tunnel1# ip route 192.168.0.0/24 gateway tunnel 1
   tunnel1# ipsec tunnel 101
   tunnel1# tunnel enable 1
   tunnel1# ipsec auto refresh on
   相手側 LAN との通信に IPsec を用いるため、その経路をトンネルルートに設定します。また IPsec 定義の適用と自動鍵交換を行うよう設定します。

4. tunnel1# tunnel select none
   # ip route 192.168.0.128 gateway 172.16.0.1
   鍵交換のパケットを暗号化の対象にしないための経路を設定します。

5. # save

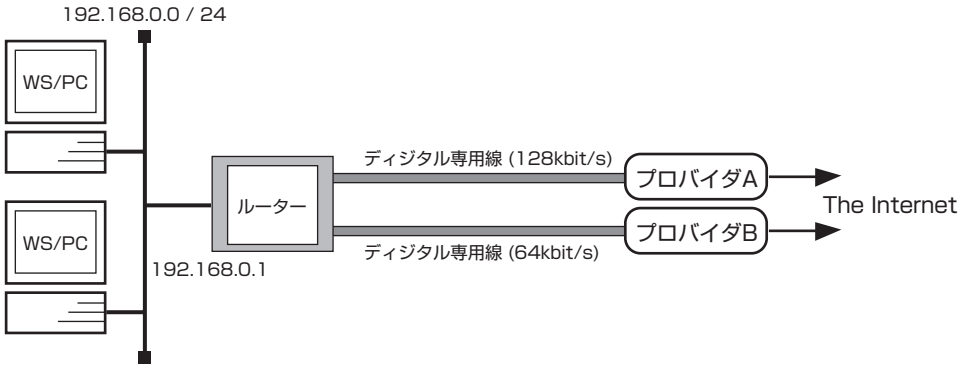
19. マルチホーミング設定例

1. マルチホーミング (専用線 128k + 専用線 64k)
2. マルチホーミング (ISDN + ISDN)

19.1 マルチホーミング (専用線 128k + 専用線 64k)

複数のプロバイダに同時に接続し、インターネットへの通信の負荷を分散させることができます。片側の回線ダウン時の経路切替えや回線速度に応じた負荷の配分も可能です。使用するプロバイダに応じた IP アドレスを使い分けるために、NAT あるいはマスカレードを使う必要があります。

[構成図]



・プロバイダ A から割り当てられた IP アドレス範囲　172.16.0.0/28
・プロバイダ B から割り当てられた IP アドレス範囲　172.16.128.0/28
・ともにネットワーク型接続であり、NAT を使用する。
・LAN 側ネットワークアドレス　192.168.0.0/24

[設定手順]

```
# line type bri2.1 l128
# line type bri2.2 l64
# ip lan1 address 192.168.0.1/24
# nat descriptor type 1 nat
# nat descriptor address outer 1 172.16.0.1-172.16.0.14
# pp select 1
pp1# pp bind bri2.1
pp1# ip pp nat descriptor 1
pp1# pp keepalive use lcp-echo
pp1# pp enable 1
pp1# pp select none
# nat descriptor type 2 nat
# nat descriptor address outer 2 172.16.128.1-172.16.128.14
# pp select 2
pp2# pp bind bri2.2
pp2# ip pp nat descriptor 2
pp2# pp keepalive use lcp-echo
pp2# pp enable 2
pp2# pp select none
# ip route default gateway pp 1 weight 2 hide gateway pp 2 weight 1 hide
# save
# interface reset bri2.1
# interface reset bri2.2
```

[解説]

1. # line type bri2.1 l128
   # line type bri2.2 l64
   回線種別を設定します。この設定はインタフェースリセットあるいは装置の再起動を行った後に有効になります。

2. # ip lan1 address 192.168.0.1/24
   NAT を使用するために LAN 側はプライベートアドレスネットワークとします。

3. # nat descriptor type 1 nat
   # nat descriptor address outer 1 172.16.0.1-172.16.0.14
   # pp select 1
   pp1# pp bind bri2.1
   pp1# ip pp nat descriptor 1
   プロバイダ A に対して使用する NAT を設定します。

4. pp1# pp keepalive use lcp-echo
   pp1# pp enable 1
   pp1# pp select none
   専用線のダウンを検出するためにキープアライブを用います。

5. # nat descriptor type 2 nat
   # nat descriptor address outer 2 172.16.128.1-172.16.128.14
   # pp select 2
   pp2# pp bind bri2.2
   pp2# ip pp nat descriptor 2
   プロバイダ B に対して使用する NAT を設定します。

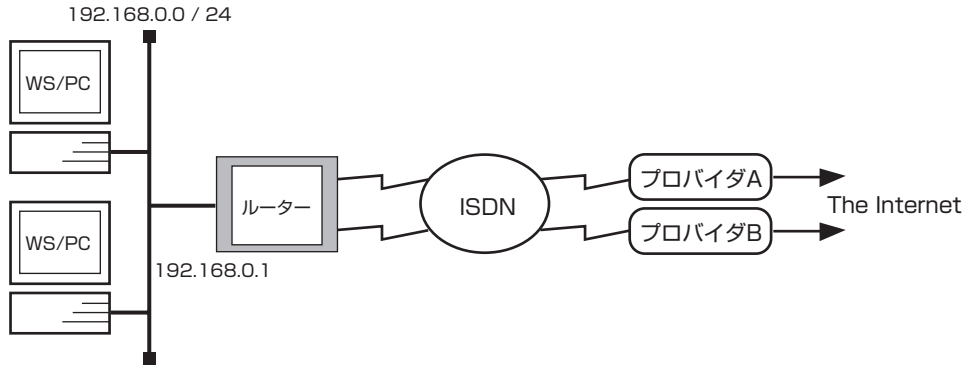
6. pp2# pp keepalive use lcp-echo
   pp2# pp enable 2
   pp2# pp select none
   pp1 同様、専用線のダウンを検出するためにキープアライブを用います。

7. # ip route default gateway pp 1 weight 2 hide gateway pp 2 weight 1 hide
   デフォルト経路をふたつのプロバイダに設定します。weight を指定することで、負荷の割合を各プロバイダへのアクセス回線の速度に応じたものにします。回線速度が同じである場合には weight 指定の必要はありません。また hide 指定でその回線がダウンした場合に経路を隠して他方を使うことで、パケットロスを避けることができます。

8. # save
   # interface reset bri2.1
   # interface reset bri2.2
   回線種別がデフォルトと異なるのでインタフェースをリセットします。**restart** コマンドによる装置全体の再起動でもかまいません。

19.2 マルチホーミング (ISDN + ISDN)

[構成図]



・プロバイダ A から割り当てられた IP アドレス範囲　172.16.0.0/28
・ネットワーク型接続で NAT 使用
・プロバイダ B からは接続時に IP アドレスが割り当てられる
・端末型接続で IP マスカレード使用
・LAN 側ネットワークアドレス　192.168.0.0/24

[設定手順]

```
# ip lan1 address 192.168.0.1/24
# nat descriptor type 1 nat
# nat descriptor address outer 1 172.16.0.1-172.16.0.14
# pp select 1
pp1# pp bind bri2.1
pp1# ip pp nat descriptor 1
pp1# isdn remote address call 0312345678
pp1# pp auth accept chap pap
pp1# pp auth myname userA passA
pp1# ppp ipcp ipaddress on
pp1# pp enable 1
pp1# pp select none
# nat descriptor type 2 masquerade
# pp select 2
pp2# pp bind bri2.2
pp2# ip pp nat descriptor 2
pp2# isdn remote address call 0387654321
pp2# pp auth accept chap pap
pp2# pp auth myname userB passB
pp2# ppp ipcp ipaddress on
pp2# pp enable 2
pp2# pp select none
# ip route default gateway pp 1 gateway pp 2
# save
```

[解説]

1. # ip lan1 address 192.168.0.1/24
   NAT/ マスカレードを使用するために LAN 側はプライベートアドレスネットワークとします。

2. # nat descriptor type 1 nat
   # nat descriptor address outer 1 172.16.0.1-172.16.0.14
   # pp select 1
   pp1# pp bind bri2.1
   pp1# ip pp nat descriptor 1
   プロバイダ A に対して使用する NAT を設定します。

3. pp1# isdn remote address call 0312345678
   pp1# pp auth accept chap pap
   pp1# pp auth myname userA passA
   pp1# ppp ipcp ipaddress on
   pp1# pp enable 1
   pp1# pp select none
   プロバイダ A に接続するための情報を設定します。
   アクセスポイントの電話番号：03-1234-5678
   ユーザ名： userA
   パスワード： passA

4. # nat descriptor type 2 masquerade
   # pp select 2
   pp2# pp bind bri2.2
   pp2# ip pp nat descriptor 2
   プロバイダ B に対して使用する IP マスカレードを設定します。

5. pp2# isdn remote address call 0387654321
   pp2# pp auth accept chap pap
   pp2# pp auth myname userB passB
   pp2# ppp ipcp ipaddress on
   pp2# pp enable 2
   pp2# pp select none
   プロバイダ B に接続するための情報を設定します。
   アクセスポイントの電話番号：03-8765-4321
   ユーザ名： userB
   パスワード： passB

6. # ip route default gateway pp 1 gateway pp 2
   # save
   デフォルト経路をふたつのプロバイダに設定します。

20. 優先 / 帯域制御の設定例

優先制御を使うと、パケットの種類毎に優先順位の高いものから優先して送信することができます。帯域制御を使うと、パケットの種類毎に通信帯域を確保することができます。なお帯域制御は、圧縮と同時に用いた場合には設定どおりの割合にスピードを調整できません。

処理の負荷としては優先制御の方が軽いものとなります。またいずれの制御においても、インタフェースから送出されるパケットのみが制御の対象となりますので、双方向通信において優先 / 帯域制御を行うためにはインタフェースの対向機器双方で設定する必要があります。

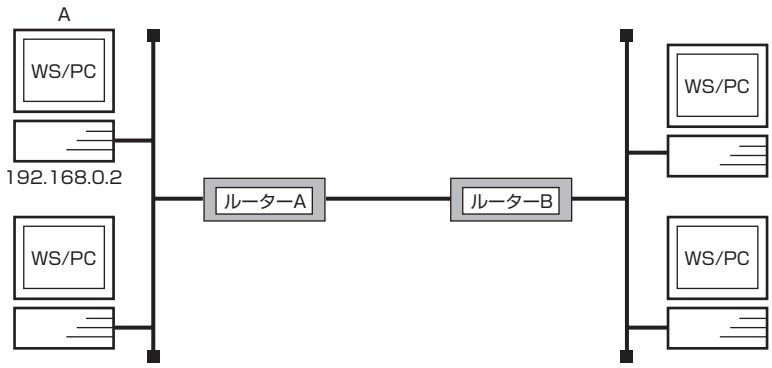
1. 優先制御 (特定ホストのパケットを優先させる)
2. 優先制御 (特定ポートを使用するパケットを優先させる)
3. 帯域制御 (特定ホストのパケットに帯域を確保する)
4. 帯域制御 (特定プロトコルを使用するパケットに帯域を確保する)
5. PPPoE 回線使用時の優先制御
6. PPPoE 回線使用時の帯域制御

次の 2 つの設定例は、ファームウェアが Rev.7.01.26 以降である必要があります。

7. IPsec を用いた VPN 環境での優先制御
8. IPsec を用いた VPN 環境での帯域制御

20.1 優先制御 (特定ホストのパケットを優先させる)

[構成図]



・PC-A が対向 LAN 上のホストと通信するパケットを優先的に送信

[ルーター A の設定手順]

```
# pp select 1
pp1# queue pp type priority
pp1# queue class filter 1 4 ip 192.168.0.2 * * * *
pp1# queue pp class filter list 1
pp1# save
```

[ルーター B の設定手順]

```
# pp select 1
pp1# queue pp type priority
pp1# queue class filter 1 4 ip * 192.168.0.2 * * *
pp1# queue pp class filter list 1
pp1# save
```

[解説]

■ルーター A

1. # pp select 1
   pp1# queue pp type priority
   キュータイプを設定し、この pp に優先制御を適用します。

2. pp1# queue class filter 1 4 ip 192.168.0.2 * * * *
   pp1# queue pp class filter list 1
   PC-A から送信されるパケットをクラス 4(優先度最高) とするフィルタを設定し、この pp に適用します。この pp インタフェースから送出される各パケットはこのフィルタと比較されて優先度が決定されることになります。フィルタにマッチしないパケットは **queue pp default class** コマンドで設定できますが、デフォルトではクラス 2 として扱われます。

3. pp1# save

■ルーター B

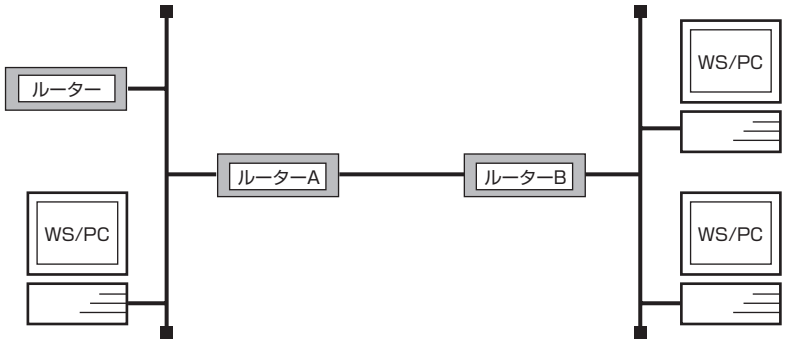
1. # pp select 1
   pp1# queue pp type priority
   キュータイプを設定し、この pp に優先制御を適用します。優先制御はインタフェースから送出されるパケットに対してのみ働きますので、双方向通信の場合にはこのように双方のルーターに優先制御の設定を行う必要があります。

2. pp1# queue class filter 1 4 ip * 192.168.0.2 * * *
   pp1# queue pp class filter list 1
   PC-A に送信されるパケットをクラス 4(優先度最高) とするフィルタを設定し、この pp に適用します。ルーター A のフィルタでは送信元 IP アドレスを指定したのに対して、ルーター B では宛先 IP アドレスを指定します。

3. pp1# save

20.2 優先制御 (特定ポートを使用するパケットを優先させる)

[構成図]



・LAN 間で、以下の優先順位でパケットを送る
・ICMP と TELNET が優先度 4(最優先)
・SMTP と POP3 は優先度 3
・IPX は優先度最低

[ルーター A,B の設定手順]

```
# pp select 1
pp1# queue pp type priority
pp1# queue class filter 1 4 ip * * icmp
pp1# queue class filter 2 4 ip * * tcp telnet *
pp1# queue class filter 3 4 ip * * tcp * telnet
pp1# queue class filter 4 3 ip * * tcp smtp,pop3 *
pp1# queue class filter 5 3 ip * * tcp * smtp,pop3
pp1# queue class filter 10 1 ipx * *
pp1# pp queue class filter list 1 2 3 4 5 10
pp1# save
```

[解説]

両ルーターで同じ設定となります。それぞれのルーターでインタフェースから送出されるパケットが制御されます。

1. # pp select 1
   pp1# queue pp type priority
   キュータイプを設定し、この pp に優先制御を適用します。

2. pp1# queue class filter 1 4 ip * * icmp
   プロトコル指定で ICMP を優先度 4 にクラス分けするフィルタを定義します。

3. pp1# queue class filter 2 4 ip * * tcp telnet *
   pp1# queue class filter 3 4 ip * * tcp * telnet
   TELNET を優先度 4 にクラス分けするフィルタを定義します。
   サーバが双方にある場合を想定しています。

4. pp1# queue class filter 4 3 ip * * tcp smtp,pop3 *
   pp1# queue class filter 5 3 ip * * tcp * smtp,pop3
   メール送受信に関わる SMTP と POP3 を優先度 3 にクラス分けするフィルタを定義します。サーバが双方にある場合を想定しています。

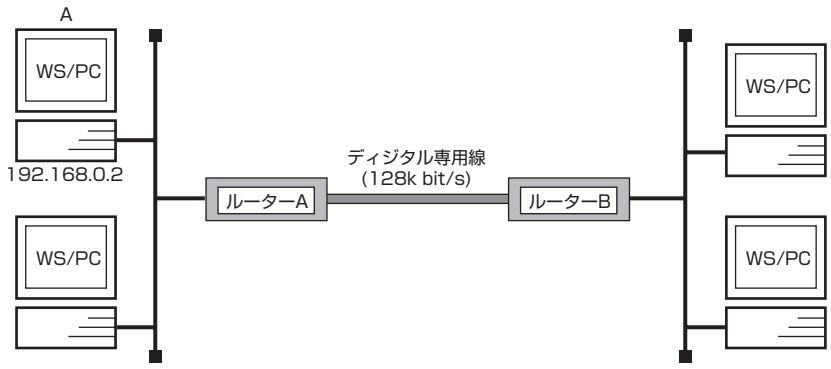
5. pp1# queue class filter 10 1 ipx * *
   プロトコル指定で IPX を優先度 1 に定義します。

6. pp1# pp queue class filter list 1 2 3 4 5 10
   定義された各フィルタをこの pp に適用します。この pp インタフェースから送出される各パケットはこのフィルタと順に比較されて優先度が決定されることになります。フィルタにマッチしないパケットは queue pp default class コマンドで設定できますが、デフォルトではクラス 2 として扱われます。

7. pp1# save

20.3 帯域制御 (特定ホストのパケットに帯域を確保する)

[構成図]



・PC-A が送受信するパケットに帯域の 80% を確保

[ルーター A の設定手順]

```
# pp select 1
pp1# queue pp type cbq
pp1# speed pp 128000
pp1# queue class filter 1 1 ip 192.168.0.2 * * * *
pp1# queue pp class property 1 bandwidth=80%
pp1# queue pp class property 2 bandwidth=20%
pp1# queue pp class filter list 1
pp1# ppp ccp type none
pp1# save
```

[ルーター B の設定手順]

```
# pp select 1
pp1# queue pp type cbq
pp1# speed pp 128000
pp1# queue class filter 1 1 ip * 192.168.0.2 * * *
pp1# queue pp class property 1 bandwidth=80%
pp1# queue pp class property 2 bandwidth=20%
pp1# queue pp class filter list 1
pp1# ppp ccp type none
pp1# save
```

[解説]

■ルーター A

1. # pp select 1
   pp1# queue pp type cbq
   キュータイプを設定し、この pp に帯域制御を適用します。

2. pp1# speed pp 128000
   回線速度を設定します。この値を元に帯域を計算します。

3. pp1# queue class filter 1 1 ip 192.168.0.2 * * * *
   PC-A から送信するパケットをクラス 1 とするフィルタを設定します。通過する各パケットはこのフィルタと比較されてクラス分けされることになります。帯域制御の場合クラス間に優先順位はありません。各クラスの属性は次の **queue pp class property** コマンドで決定されます。

4. pp1# queue pp class property 1 bandwidth=80%
   クラス 1 のパケットに対して帯域の 80% を確保します。

5. pp1# queue pp class property 2 bandwidth=20%
   フィルタにマッチしないパケットは **queue pp default class** コマンドで設定できますが、デフォルトではクラス 2 となります。このクラスのパケットに対して帯域の残りの 20% を確保するよう設定します。この設定がないとクラス 2 には 100% の帯域が与えられることになり、帯域制御が設定通りに働きません。

6. pp1# queue pp class filter list 1
   queue class filter コマンドで設定したフィルタをこの pp に適用します。これで、この pp インタフェースから送出されるパケットに対して帯域制御が行われます。

7. pp1# ppp ccp type none
   帯域制御では圧縮機能は使用できませんので、圧縮機能を使用しないように設定します。

8. pp1# save

■ルーター B

1. # pp select 1
   pp1# queue pp type cbq
   キュータイプを設定し、この pp に帯域制御を適用します。
   帯域制御はインタフェースから送出されるパケットに対してのみ働きますので、双方向通信の場合にはこのように双方のルーターに帯域制御の設定を行う必要があります。

2. pp1# speed pp 128000
   回線速度を設定します。この値を元に帯域を計算します。

3. pp1# queue class filter 1 1 ip * 192.168.0.2 * * *
   PC-A を宛先とするパケットをクラス 1 とするフィルタを設定します。インタフェースから送出されるパケットが対象となりますので、ルーター A のフィルタでは送信元 IP アドレスを指定したのに対して、ルーター B では宛先 IP アドレスを指定します。

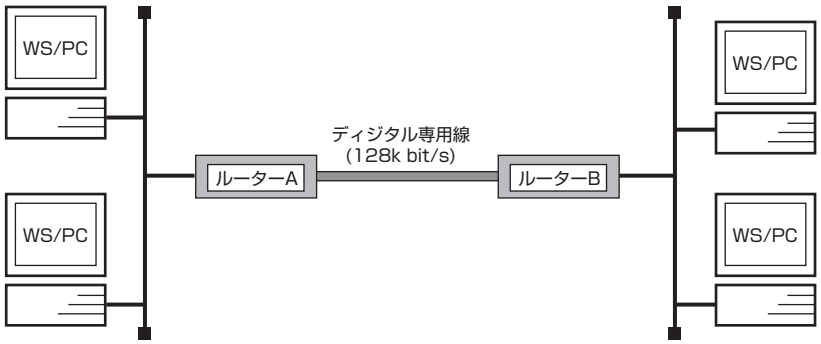
4. pp1# queue pp class property 1 bandwidth=80%
   pp1# queue pp class property 2 bandwidth=20%
   pp1# queue pp class filter list 1
   ルーター A の設定同様、対象パケットに帯域の 80%、その他のパケットに帯域の 20% を割り当て、フィルタをこの pp に適用します。

5. pp1# ppp ccp type none
   帯域制御では圧縮機能は使用できませんので、圧縮機能を使用しないように設定します。

6. pp1# save

20.4 帯域制御 (特定プロトコルを使用するパケットに帯域を確保する)

[構成図]



・UDP を使用する通信に帯域の 50% を確保

[ルーター A,B の設定手順]

```
# pp select 1
pp1# queue pp type cbq
pp1# speed pp 128000
pp1# queue class filter 1 1 ip * * udp * *
pp1# queue pp class property 1 bandwidth=50%
pp1# queue pp class property 2 bandwidth=50%
pp1# queue pp class filter list 1
pp1# ppp ccp type none
pp1# save
```

[解説]

両ルーターで同じ設定となります。それぞれのルーターでインタフェースから送出されるパケットが制御されます。

1. # pp select 1
   pp1# queue pp type cbq
   キュータイプを設定し、この pp に帯域制御を適用します。

2. pp1# speed pp 128000
   回線速度を設定します。この値を元に帯域を計算します。

3. pp1# queue class filter 1 1 ip * * udp * *
   UDP を使用するパケットをクラス 1 とするフィルタを設定します。ここでは UDP のどのポートを使用するパケットであってもクラス 1 へのクラス分けの対象となりますが、アスタリスク「*」の代わりに使用するポート番号まで指定して対象パケットを限定することもできます。その場合は送信元ポートと宛先ポートの違いに注意してください。
   通過する各パケットはこのフィルタと比較されてクラス分けされることになります。帯域制御の場合クラス間に優先順位はありません。各クラスの属性は次の **queue pp class property** コマンドで決定されます。

4. pp1# queue pp class property 1 bandwidth=50%
   上記フィルタに合致したクラス 1 のパケットに対して帯域の 50% を確保します。

5. pp1# queue pp class property 2 bandwidth=50%
   フィルタにマッチしないパケットは **queue pp default class** コマンドで設定できますが、デフォルトではクラス 2 となります。このクラスのパケットに対して帯域の残りの 50% を確保するよう設定します。この設定がないとクラス 2 には 100% の帯域が与えられることになり、帯域制御が設定通りに働きません。

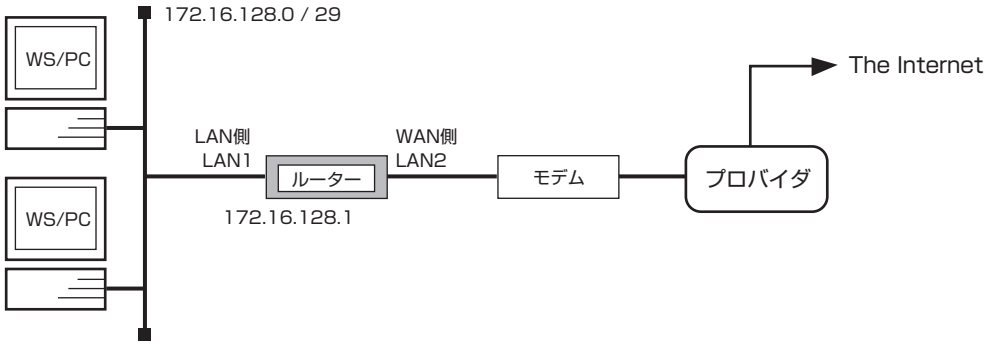
6. pp1# queue pp class filter list 1
   queue class filter コマンドで設定したフィルタをこの pp に適用します。これで、この pp インタフェースから送出されるパケットに対して帯域制御が行われます。

7. pp1# ppp ccp type none
   帯域制御では圧縮機能は使用できませんので、圧縮機能を使用しないように設定します。

8. pp1# save

20.5 PPPoE 回線使用時の優先制御

[構成図]



[ルーターの設定手順]

```
# ip lan1 address 172.16.128.1/29
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ppp ipcp ipaddress on
pp1# ip pp mtu 1454
pp1# pp enable 1
pp1# pp select none
# ip route default gateway pp 1
# queue lan2 type priority
# speed lan2 10m
# queue class filter 1 4 ip * * tcp telnet *
# queue class filter 2 4 ip * * tcp * telnet
# queue class filter 3 3 ip * * tcp www *
# queue class filter 4 3 ip * * tcp * www
# queue class filter 5 1 ip * * tcp ftp *
# queue class filter 6 1 ip * * tcp * ftp
# pp select 1
pp1# queue pp class filter list 1 2 3 4 5 6
pp1# save
```

[解説]

LAN 側ネットワークには 172.16.128.0/29 のグローバルアドレスが割当てられ、WWW サーバ、FTP サーバ、WS/PC が複数台設置されています。この例では優先制御を使用し、FTP 通信、WWW 通信が回線帯域を占有し、TELNET の操作性を損なうことがないようにしています。

優先度は TELNET > WWW > 指定以外の通信 > FTP としています。

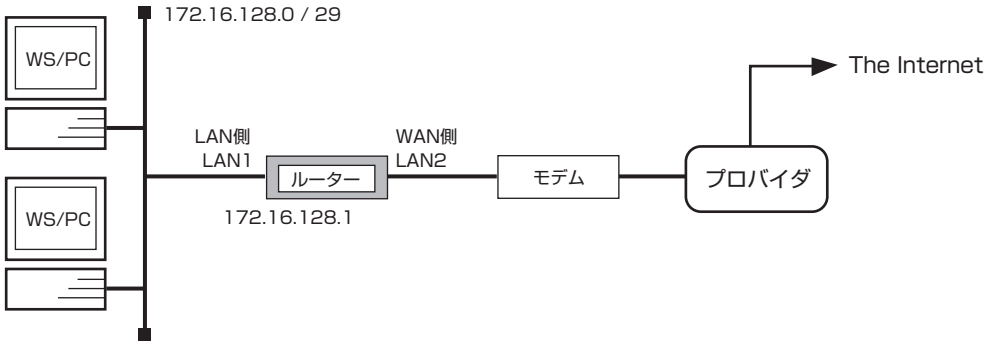
1. # queue lan2 type priority
   # speed lan2 10m
   優先制御機能の使用と回線帯域を設定します。

2. # queue class filter 1 4 ip * * tcp telnet *
   # queue class filter 2 4 ip * * tcp * telnet
   # queue class filter 3 3 ip * * tcp www *
   # queue class filter 4 3 ip * * tcp * www
   # queue class filter 5 1 ip * * tcp ftp *
   # queue class filter 6 1 ip * * tcp * ftp
   サービス毎に使用するキュー番号を設定します。ここで設定されていないサービスはデフォルトクラス (クラス 2) に入ります。クラス番号の大きいキューに入っているパケットが優先して送出されます。

3. # pp select 1
   pp1# queue pp class filter list 1 2 3 4 5 6
   pp インタフェース対し優先制御を適用します。

20.6 PPPoE 回線使用時の帯域制御

[構成図]



[ルーターの設定手順]

```
# ip lan1 address 172.16.128.1/29
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ppp ipcp ipaddress on
pp1# ip pp mtu 1454
pp1# pp enable 1
pp1# pp select none
# ip route default gateway pp 1
# queue lan2 type shaping
# queue lan2 class property 1 bandwidth=3m
# queue lan2 class property 2 bandwidth=5m
# queue lan2 class property 3 bandwidth=2m
# queue class filter 1 1 ip * * tcp www *
# queue class filter 2 1 ip * * tcp * www
# queue class filter 3 3 ip * * tcp ftp *
# queue class filter 4 3 ip * * tcp * ftp
# pp select 1
pp1# queue pp class filter list 1 2 3 4
pp1# save
```

[解説]

LAN 側ネットワークには 172.16.128.0/29 のグローバルアドレスが割当てられ、WWW サーバ、FTP サーバ、WS/PC が複数台設置されています。この例では帯域制御を使用し、WWW 通信、FTP 通信、その他の通信サービスが回線帯域の全てを占有しないようにしています。

各通信サービスが使用できる帯域は、

クラス 1	: WWW 通信	: 3Mbit/s
クラス 2（デフォルト）	: その他の通信	: 5Mbit/s
クラス 3	: FTP 通信	: 2Mbit/s

としています。

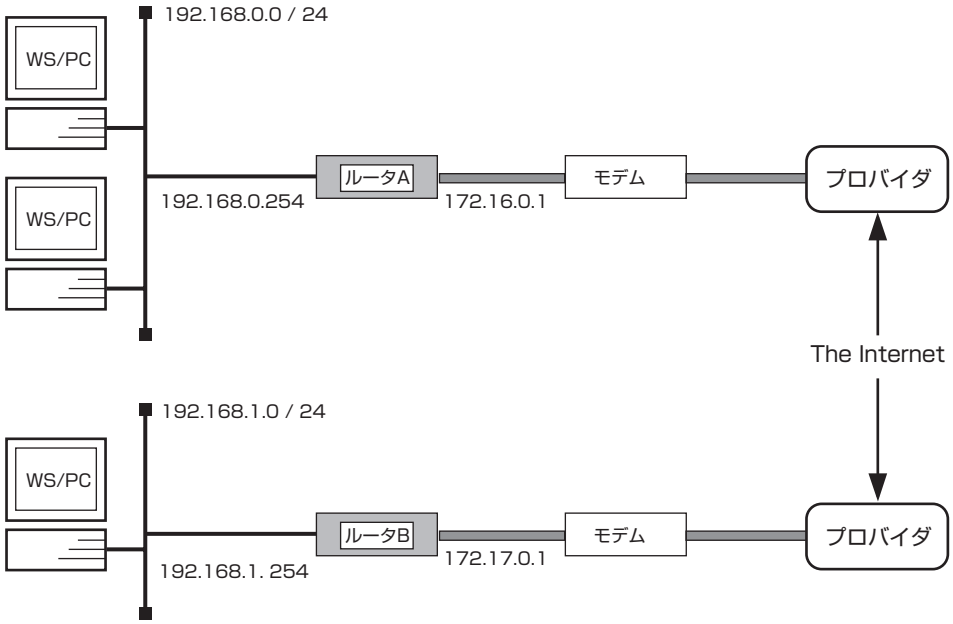
1. # queue lan2 type shaping
   # queue lan2 class property 1 bandwidth=3m
   # queue lan2 class property 2 bandwidth=5m
   # queue lan2 class property 3 bandwidth=2m
   帯域制御機能の使用と各キューで使用できる回線帯域を設定します。

2. # queue class filter 1 1 ip * * tcp www *
   # queue class filter 2 1 ip * * tcp * www
   # queue class filter 3 3 ip * * tcp ftp *
   # queue class filter 4 3 ip * * tcp * ftp
   サービス毎に使用するキュー番号を設定します。ここで設定されていないサービスはデフォルトクラス (2) に入ります。

3. # pp select 1
   pp1# queue tunnel class filter list 1 2 3 4
   pp インタフェース対し帯域制御を適用します。

20.7 IPsec を用いた VPN 環境での優先制御

[構成図]



[ルーター A の設定手順]

```
# ip lan1 address 192.168.0.254/24
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ip pp address 172.16.0.1/32
pp1# ip pp mtu 1454
pp1# pp enable 1
pp1# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
anti-replay-check=off
tunnel1# ipsec ike pre-shared-key 1 text IKEKEYPASS
tunnel1# ipsec ike local address 1 172.16.0.1
tunnel1# ipsec ike remote address 1 172.17.0.1
tunnel1# tunnel enable 1
tunnel1# tunnel select none
# ipsec auto refresh on
# ip route 172.17.0.1 gateway pp 1
# ip route 192.168.1.0/24 gateway tunnel 1
# queue lan2 type priority
# speed lan2 10m
# queue class filter 1 4 ip * * tcp telnet *
# queue class filter 2 4 ip * * tcp * telnet
# queue class filter 3 3 ip * * tcp www *
# queue class filter 4 3 ip * * tcp * www
# queue class filter 5 1 ip * * tcp ftp *
# queue class filter 6 1 ip * * tcp * ftp
```

```
# tunnel select 1
tunnel1# queue tunnel class filter list 1 2 3 4 5 6
tunnel1# tsave
```

[ルーター B の設定手順]

```
# ip lan1 address 192.168.1.254/24
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ip pp address 172.17.0.1/32
pp1# ip pp mtu 1454
pp1# pp enable 1
pp1# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# ipsec sa policy 101 1 esp 3des-cbc md5-hmac anti-replay-check=off
tunnel1# ipsec ike pre-shared-key 1 text IKEKEYPASS
tunnel1# ipsec ike local address 1 172.17.0.1
tunnel1# ipsec ike remote address 1 172.16.0.1
tunnel1# tunnel enable 1
tunnel1# tunnel select none
# ipsec auto refresh on
# ip route 172.16.0.1 gateway pp 1
# ip route 192.168.0.0/24 gateway tunnel 1
# queue lan2 type priority
# speed lan2 10m
# queue class filter 1 4 ip * * tcp telnet *
# queue class filter 2 4 ip * * tcp * telnet
# queue class filter 3 3 ip * * tcp www *
# queue class filter 4 3 ip * * tcp * www
# queue class filter 5 1 ip * * tcp ftp *
# queue class filter 6 1 ip * * tcp * ftp
# tunnel select 1
tunnel1# queue tunnel class filter list 1 2 3 4 5 6
tunnel1# save
```

[解説]

本社側が 172.16.0.1、支店側が 172.17.0.1 の固定アドレスの割り当てを受けており、本社と支店は IPsec で接続されています。本社側 LAN、支店側 LAN にはそれぞれ WWW サーバ、FTP サーバ、WS/PC が複数台設置され、お互いに業務データの送受信が行われています。また、TELNET を使用したサーバのメンテナンス業務も行われます。この例では優先制御を使用し、FTP 通信、WWW 通信が回線帯域を占有し、TELNET によるサーバのメンテナンス業務に支障を与える事がないようにしています。

優先度は TELNET > WWW > 指定以外の通信 > FTP としています。

1. # queue lan2 type priority
   # speed lan2 10m
   優先制御機能の使用と回線帯域を設定します。

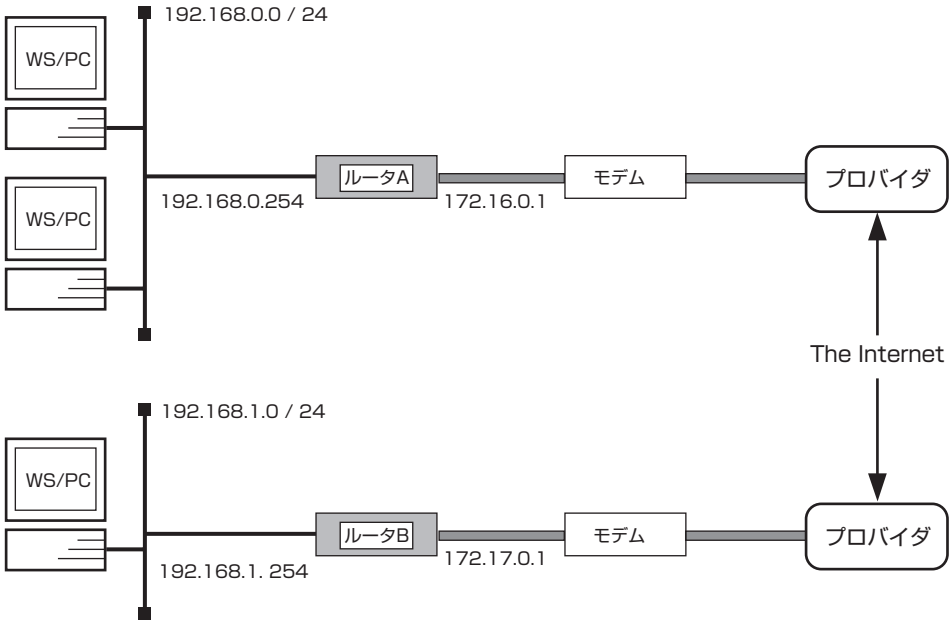
2. # queue class filter 1 4 ip * * tcp telnet *
   # queue class filter 2 4 ip * * tcp * telnet
   # queue class filter 3 3 ip * * tcp www *
   # queue class filter 4 3 ip * * tcp * www
   # queue class filter 5 1 ip * * tcp ftp *
   # queue class filter 6 1 ip * * tcp * ftp
   サービス毎に使用するキュー番号を設定します。ここで設定されていないサービスはデフォルトクラス (2) に入ります。
   番号の大きいキューに入っているパケットが優先して送出されます。

3. # tunnel select 1
   tunnel1# queue tunnel class filter list 1 2 3 4 5 6
   トンネルインタフェース対し優先制御を適用します。

4. # ipsec sa policy 101 1 esp 3des-cbc md5-hmac anti-replay-check=off
   優先制御を使用するとパケットの順番の入れ替わりが発生します。IPsec 通信において順番の入れ替わりを監視する機能を使用しない設定にします。

20.8 IPsec を用いた VPN 環境での帯域制御

[構成図]



[ルーター A の設定手順]

```
# ip lan1 address 192.168.0.254/24
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ip pp address 172.16.0.1/32
pp1# ip pp mtu 1454
pp1# pp enable 1
pp1# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# ipsec sa policy 101 1 esp 3des-cbc md5-hmac anti-replay-check=off
tunnel1# ipsec ike pre-shared-key 1 text IKEKEYPASS
tunnel1# ipsec ike local address 1 172.16.0.1
tunnel1# ipsec ike remote address 1 172.17.0.1
tunnel1# tunnel enable 1
tunnel1# tunnel select none
# ipsec auto refresh on
# ip route 172.17.0.1 gateway pp 1
# ip route 192.168.1.0/24 gateway tunnel 1
# queue lan2 type shaping
# queue lan2 class property 1 bandwidth=3m
# queue lan2 class property 2 bandwidth=5m
# queue lan2 class property 3 bandwidth=2m
# queue class filter 1 1 ip * * tcp www *
# queue class filter 2 1 ip * * tcp * www
# queue class filter 3 3 ip * * tcp ftp *
# queue class filter 4 3 ip * * tcp * ftp
```

```
# tunnel select 1
tunnel1# queue tunnel class filter list 1 2 3 4
tunnel1# save
```

[ルーター B の設定手順]

```
# ip lan1 address 192.168.1.254/24
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ip pp address 172.17.0.1/32
pp1# ip pp mtu 1454
pp1# pp enable 1
pp1# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# ipsec sa policy 101 1 esp 3des-cbc md5-hmac anti-replay-check=off
tunnel1# ipsec ike pre-shared-key 1 text IKEKEYPASS
tunnel1# ipsec ike local address 1 172.17.0.1
tunnel1# ipsec ike remote address 1 172.16.0.1
tunnel1# tunnel enable 1
tunnel1# tunnel select none
# ipsec auto refresh on
# ip route 172.16.0.1 gateway pp 1
# ip route 192.168.0.0/24 gateway tunnel 1
# queue lan2 type shaping
# queue lan2 class property 1 bandwidth=3m
# queue lan2 class property 2 bandwidth=5m
# queue lan2 class property 3 bandwidth=2m
# queue class filter 1 1 ip * * tcp www *
# queue class filter 2 1 ip * * tcp * www
# queue class filter 3 3 ip * * tcp ftp *
# queue class filter 4 3 ip * * tcp * ftp
# tunnel select 1
tunnel1# queue tunnel class filter list 1 2 3 4
tunnel1# save
```

[解説]

本社側が 172.16.0.1、支店側が 172.17.0.1 の固定アドレスの割り当てを受けており、本社と支店は IPsec で接続されています。本社側 LAN、支店側 LAN にはそれぞれ WWW サーバ、FTP サーバ、WS/PC が複数台設置され、お互いに業務データの送受信が行われています。またその他に、独自のソフトウェアによる通信サービスも提供されています。
この例では帯域制御を使用し、WWW 通信、FTP 通信、その他の通信サービスが回線帯域の全てを占有しないようにしています。

各通信サービスが使用できる帯域は、

クラス 1	: WWW 通信	: 3Mbit/s
クラス 2（デフォルト）	: その他の通信	: 5Mbit/s
クラス 3	: FTP 通信	: 2Mbit/s

としています。

1. # queue lan2 type shaping
   # queue lan2 class property 1 bandwidth=3m
   # queue lan2 class property 2 bandwidth=5m
   # queue lan2 class property 3 bandwidth=2m
   帯域制御機能の使用と各キューで使用できる回線帯域を設定します。

2. # queue class filter 1 1 ip * * tcp www *
   # queue class filter 2 1 ip * * tcp * www
   # queue class filter 3 3 ip * * tcp ftp *
   # queue class filter 4 3 ip * * tcp * ftp
   サービス毎に使用するキュー番号を設定します。ここで設定されていないサービスはデフォルトクラス (クラス 2) に入ります。

3. # tunnel select 1
   tunnel1# queue tunnel class filter list 1 2 3 4
   トンネルインタフェース対し帯域制御を適用します。

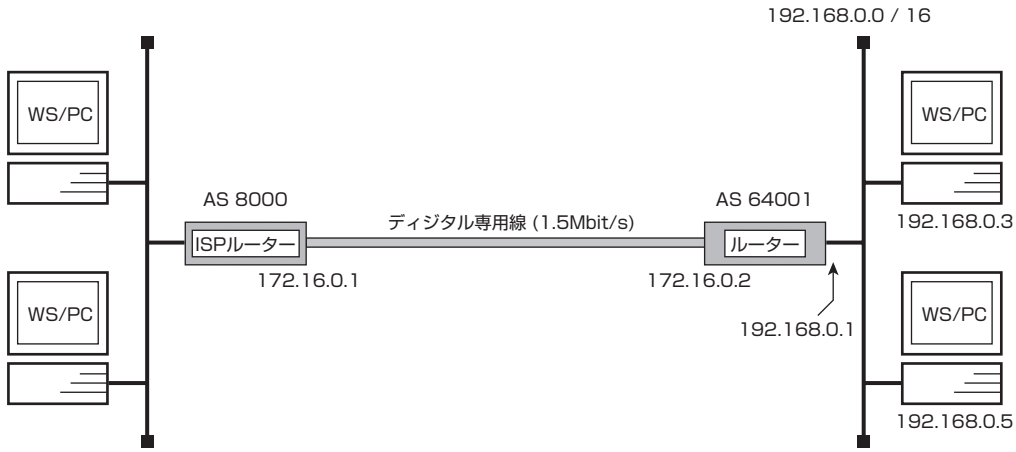
4. # tunnel select 1
   tunnel1# ipsec sa policy 101 1 esp 3des-cbc md5-hmac anti-replay-check=off
   帯域制御を使用するとパケットの順番の入れ替わりが発生します。IPsec 通信において順番の入れ替わりを監視する機能を使用しない設定にします。

21. BGP 設定例

1. BGP と RIP の組み合わせ
2. BGP と OSPF の組み合わせ
3. VRRP による多重化
4. ISDN によるバックアップ

21.1 BGP と RIP の組み合わせ

[構成図]



[設定手順]

```
# line type pri1 leased
# pri leased channel 1/1 1 24
# ip lan1 address 192.168.0.1/16
# rip use on
# ip lan1 rip send on version 2
# ip lan1 rip receive on version 2
# pp select 1
pp1# pp bind pri1/1
pp1# ip pp address 172.16.0.2/32
pp1# ip pp remote address 172.16.0.1
pp1# ip pp rip send off
pp1# ip pp rip receive off
pp1# pp enable 1
pp1# pp select none
# bgp use on
# bgp autonomous-system 64001
# bgp neighbor 1 8000 172.16.0.1
# bgp import filter 1 include 192.168.0.0/16
# bgp import 8000 rip filter 1
# bgp export filter 1 include all
# bgp export 8000 filter 1
# save
# interface reset pri1
# bgp configure refresh
```

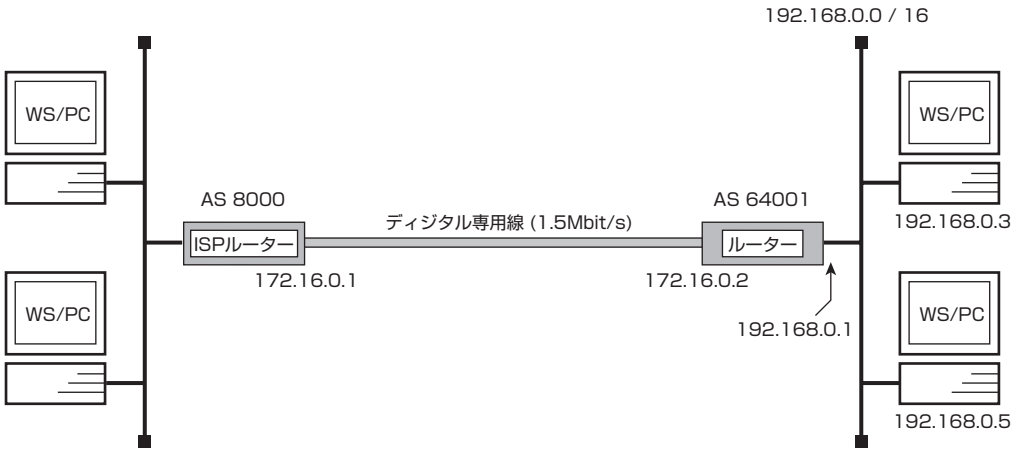
[解説]

この例は、BGP のもっとも簡単な設定例です。ユーザネットワークを RIP で運用しており、その経路を BGP で広告します。一方、BGP で受信した経路をすべて取り込みます。

- RIP で受信した 192.168.0.0/16 の範囲内の経路のみを広告する。
- すべての経路を受け取る。
- 経路の集約はしない。

21.2 BGP と OSPF の組み合わせ

[構成図]



[設定手順]

```
# line type pri1 leased
# pri leased channel 1/1 1 24
# ip lan1 address 192.168.0.1/16
# ospf use on
# ospf area backbone
# ip lan1 ospf area backbone
# pp select 1
pp1# pp bind pri1/1
pp1# ip pp address 172.16.0.2/32
pp1# ip pp remote address 172.16.0.1
pp1# pp enable 1
pp1# pp select none
# bgp use on
# bgp autonomous-system 64001
# bgp neighbor 1 8000 172.16.0.1
# bgp aggregate filter 1 ospf include 192.168.0.0/16
# bgp aggregate 192.168.0.0/16 filter 1
# bgp import filter 1 include 192.168.0.0/16
# bgp import filter 2 reject include 192.168.0.0/16
# bgp import filter 3 include all
# bgp import 8000 aggregate filter 1
# bgp import 8000 ospf filter 2 3
# bgp export filter 1 include 10.0.0.0/8
# bgp export 8000 filter 1
# save
# interface reset pri1
# ospf configure refresh
# bgp configure refresh pp 1
```

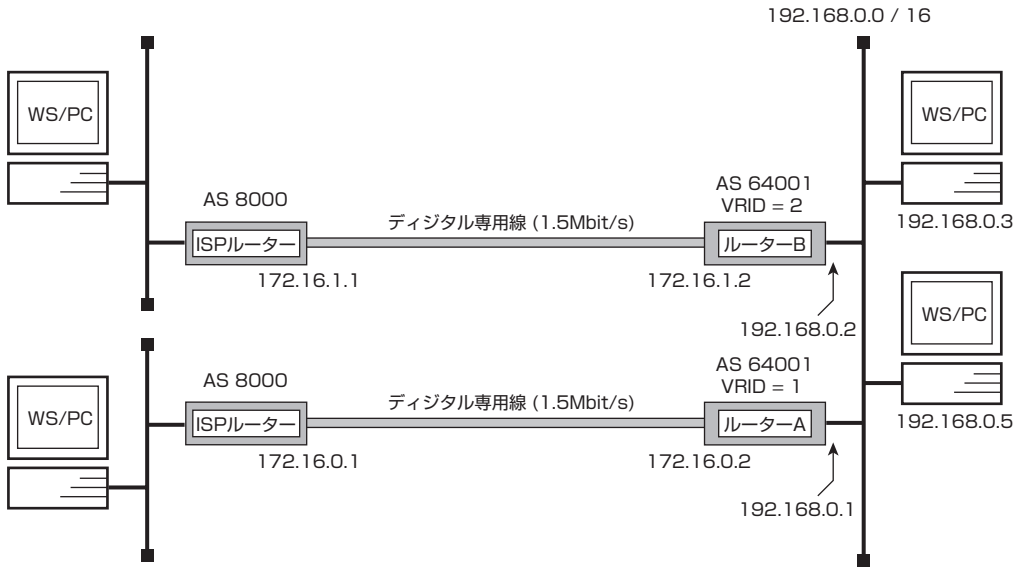
[解説]

この例は、1. の RIP を OSPF に置き換えた設定例です。また、経路集約や、受信経路に対するフィルタリングの設定を追加しています。

・OSPF で受信した 192.168.0.0/16 の範囲内の経路を集約して広告し、それ以外の経路はそのまま広告する。
・10.0.0.0/8 の範囲の経路のみを受け取る。

21.3 VRRP による多重化

[構成図]



[ルーター A の設定手順]

```
# line type pri1 leased
# pri leased channel 1/1 1 24
# ip lan1 address 192.168.0.1/16
# pp select 1
pp1# pp bind pri1/1
pp1# ip pp address 172.16.0.2/32
pp1# ip pp remote address 172.16.0.1
pp1# pp enable 1
pp1# pp select none
# bgp use on
# bgp autonomous-system 64001
# bgp neighbor 1 8000 172.16.0.1
# bgp export filter 1 include all
# bgp export 8000 filter 1
# ip lan1 vrrp 1 192.168.0.1
# ip lan1 vrrp shutdown trigger 1 route 10.0.0.0/16
# ip lan1 vrrp 2 192.168.0.2
# ip lan1 vrrp shutdown trigger 2 route 10.0.0.0/16
# dhcp service server
# dhcp scope 1 192.168.0.100-192.168.0.125/24 gateway 192.168.0.1
# dhcp scope 1 192.168.0.200-192.168.0.225/24 gateway 192.168.0.2
# save
# interface reset pri1
# bgp configure refresh
```

[ルーター B の設定手順]

```
# line type pri1 leased
# pri leased channel 1/1 1 24
# ip lan1 address 192.168.0.2/16
# pp select 1
pp1# pp bind pri1/1
pp1# ip pp address 172.16.1.2/32
pp1# ip pp remote address 172.16.1.1
pp1# pp enable 1
pp1# pp select none
# bgp use on
# bgp autonomous-system 64001
# bgp neighbor 1 8000 172.16.1.1
# bgp export filter 1 include all
# bgp export 8000 filter 1
# ip lan1 vrrp 1 192.168.0.1
# ip lan1 vrrp shutdown trigger 1 route 10.0.0.0/16
# ip lan1 vrrp 2 192.168.0.2
# ip lan1 vrrp shutdown trigger 2 route 10.0.0.0/16
# save
# interface reset pri1
# bgp configure refreshe
```

[解説]

2 台の BGP ルーターを用意し VRRP によって多重化します。回線が正常なときには 2 台のルーターを平均的に使用し、一方の回線が故障したときには、もう一方のルーターだけを使用します。

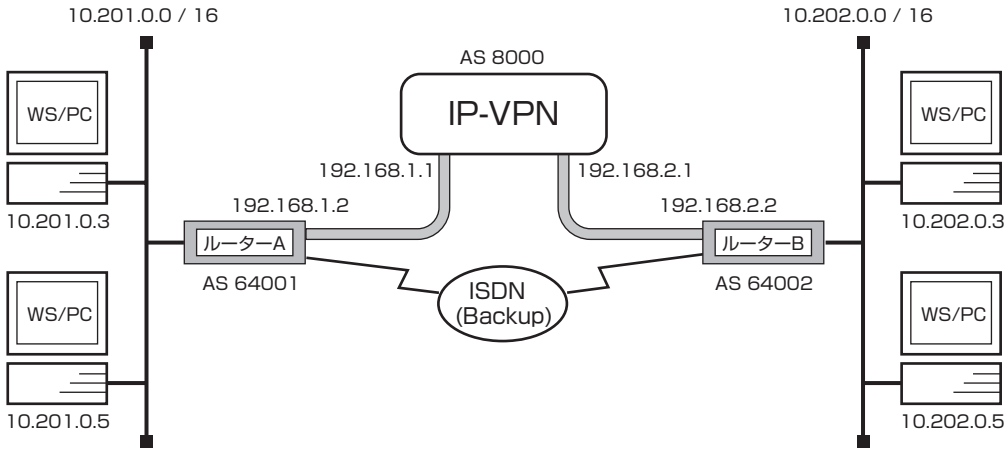
ルーターの BGP の設定については、IP アドレスなどの細かい点を除けば全く同じです。多重化に関する処理は VRRP によって実現されるので、BGP の設定で多重化を意識することはありません。

ルーター A とルーター B は、10.0.0.0/16 という経路を BGP で受け取ることができなくなった、という事象を VRRP のシャットダウントリガとして利用しています。つまり、ISP から BGP 経由で 10.0.0.0/16 という経路を受信できるようになっている必要があります。

- IP アドレスなどの細かい部分を除けば、2 台のルーターの BGP の設定はほとんど同じ。
- ルーター A は VRID=1 のマスターであり、VRID=2 のバックアップ。
- ルーター B は VRID=2 のマスターであり、VRID=1 のバックアップ。
- BGP ですべての経路を受信する。
- BGP で経路を送信しない。

21.4 ISDN によるバックアップ

[構成図]



[ルーター A の設定手順]

```
# line type bri1 l128
# isdn local address bri2 11111111
# ip lan1 address 10.201.0.1/16
# ip lan1 ospf area backbone
# pp select 1
pp1# pp bind bri1
pp1# ip pp address 192.168.1.2/32
pp1# ip pp remote address 192.168.1.1
pp1# pp enable 1
pp1# pp select 2
pp2# pp bind bri2
pp2# isdn remote address call 22222222
pp2# pp enable 2
pp2# pp select none
# ip route 10.202.0.0/16 gateway pp 2
# ospf use on
# ospf area backbone
# bgp use on
# bgp autonomous-system 64001
# bgp neighbor 1 8000 192.168.1.1
# bgp import filter 1 include 10.201.0.0/16
# bgp import 8000 static filter 1
# bgp import 8000 ospf filter 1
# bgp export filter 1 include all
# bgp export 8000 filter 1
# bgp preference 20000
# save
# interface reset bri1
# bgp configure refresh
```

[ルーター B の設定手順]

```
# line type bri1 l128
# isdn local address bri2 22222222
# ip lan1 address 10.202.0.1/16
# ip lan1 ospf area backbone
# pp select 1
pp1# pp bind bri1
pp1# ip pp address 192.168.2.2/32
pp1# ip pp remote address 192.168.2.1
pp1# pp enable 1
pp1# pp select 2
pp2# pp bind bri2
pp2# isdn remote address call 11111111
pp2# pp enable 2
pp2# pp select none
# ip route 10.201.0.0/16 gateway pp 2
# ospf use on
# ospf area backbone
# bgp use on
# bgp autonomous-system 64002
# bgp neighbor 1 8000 192.168.2.1
# bgp import filter 1 include 10.202.0.0/16
# bgp import 8000 static filter 1
# bgp import 8000 ospf filter 1
# bgp export filter 1 include all
# bgp export 8000 filter 1
# bgp preference 20000
# save
# interface reset bri1
# bgp configure refresh
```

[解説]

ISDN 回線をバックアップとして使用します。通常は BGP によって経路が広告されるので、その経路を生かし、BGP の経路が消失したら、ISDN 回線に対する経路が生きるようにします。このためには、ISDN 回線にスタティックな経路を設定し、その優先度 (プリファレンス) が BGP の経路よりも低くなるようにします。

- IP-VPN の障害を ISDN でバックアップする。
- ユーザネットワークの内部は OSPF で運用する。
- 自分のネットワークに属する経路を BGP で広告する。
- BGP で受信した経路を OSPF で広告する。

22. ブロードバンドルーターの設定例 (PPPoE 利用の非 VPN 接続)

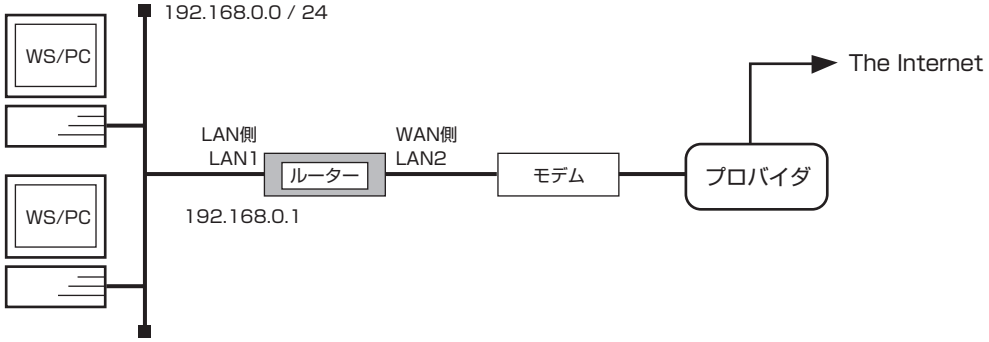
本章では、VPN を利用しないで、PPPoE によるブロードバンド接続を行うための設定例を示します。PPPoE と IPsec を利用して VPN 環境を構築する場合については第２２章を、PPPoE と PPTP を利用して VPN 環境を構築する場合は第２４章を参照してください。また、PPPoE 環境で優先制御・帯域制御を行う場合は第１９章も合わせて参照してください。

1. 端末型接続
2. ネットワーク型接続
3. 特定ポートをサーバ公開用セグメントとして使用 (RT105e)
4. プロバイダ端末型接続を ISDN によるプロバイダ端末型接続でバックアップ
5. LAN 側ネットワークをプライベート IP アドレス+グローバル IP アドレスで構成する
6. LAN 側ネットワークをプライベート IP アドレスで構成する
7. LAN 側ネットワークをグローバル IP アドレスで構成する
8. LAN 側ネットワークをプライベート IP アドレス+グローバル IP アドレスで構成する
9. LAN 側ネットワークをプライベート IP アドレスで構成する
10. LAN 側ネットワークをグローバル IP アドレスで構成する

22.1 端末型接続

ブロードバンドインタフェースのアクセス等において、イーサネットの LAN 経由で PPP 接続することができます。例えば、従来の PP への IP マスカレード接続の様に、LAN 経由で PPPoE サーバ (Access Consentrator) に PPP 接続することで IP アドレスの割り当てや DNS サーバアドレスの通知を受け、割り当てられた IP アドレスを outer アドレスとした IP マスカレード接続により、同時に複数ホストの通信が可能となります。切断タイマはデフォルトで off ですが、切断の必要がある場合には **pppoe disconnect time** コマンドと **pppoe auto disconnect** コマンドで設定します。実装されている PPPoE 機能はクライアントとして動作しますので、サーバに対するアクセスは可能ですが、接続のない状態からアクセスを受けることはできません。また MP と圧縮機能は使用できません。なお、PPPoE は RFC2516 で規定されています。

[構成図]



・LAN1 を LAN 側、LAN2 側を WAN 側とする
・LAN1 側では DHCP サーバとしても機能する
・LAN2 側はブロードバンド回線モデム等からのイーサネット回線に接続する

[設定手順]

```
# ip lan1 address 192.168.0.1/24
# nat descriptor type 1 masquerade
# pp select 1
pp1# pppoe use lan2
pp1# pp auth accept chap pap
pp1# pp auth myname ID PASSWORD
pp1# ppp ipcp ipaddress on
pp1# ppp ipcp msext on
pp1# ip pp nat descriptor 1
pp1# ppp lcp mru on 1454
pp1# ip pp mtu 1454
pp1# ppp ccp type none
pp1# pp enable 1
pp1# pp select none
# ip route default gateway pp 1
# dns server pp 1
# dns private address spoof on
# dhcp service server
# dhcp scope 1 192.168.0.2-192.168.0.254/24
# save
```

[解説]

1. # ip lan1 address 192.168.0.1/24
   LAN1 側をプライベートアドレスネットワークとします。

2. # nat descriptor type 1 masquerade
   pp1 に IP マスカレード機能を適用するための NAT ディスクリプタを定義します。

3. # pp select 1
   pp1# pppoe use lan2
   LAN2 側に対して PPPoE を使用するよう設定します。
   この 1 行以外の設定は、基本的にはダイヤルアップで端末型接続する場合と同じです。

4. pp1# pp auth accept chap pap
   pp1# pp auth myname ID PASSWORD
   PPPoE サーバとの認証情報を設定します。

5. pp1# ppp ipcp ipaddress on
   接続時にサーバからアドレスを得るよう設定します。

6. pp1# ppp ipcp msext on
   この設定により接続時にサーバから DNS サーバアドレスの通知を受けることができます。

7. pp1# ip pp nat descriptor 1
   IP マスカレード機能を定義した NAT ディスクリプタを pp1 に適用します。

8. pp1# ppp lcp mru on 1454
   LCP のネゴシエーションで Maximum-Receive-Unit オプションを使用し、パケットの最大長を制限します。

9. pp1# ppp ccp type none
   圧縮機能は使用できません。デフォルトでは stac 圧縮を使うようネゴシエーションすることになりますので、 none に設定する必要があります。

10. pp1# pp enable 1
    pp1# pp select none
    # ip route default gateway pp 1
    宛先が LAN 外であるすべてのパケットを送るためのデフォルトルートを pp1 に設定します。

11. # dns server pp 1
    DNS サーバアドレスは、pp1 から取得するアドレスを使用します。

12. # dns private address spoof on
    プライベートアドレスの DNS アドレス解決要求を DNS サーバに転送しないよう設定します。

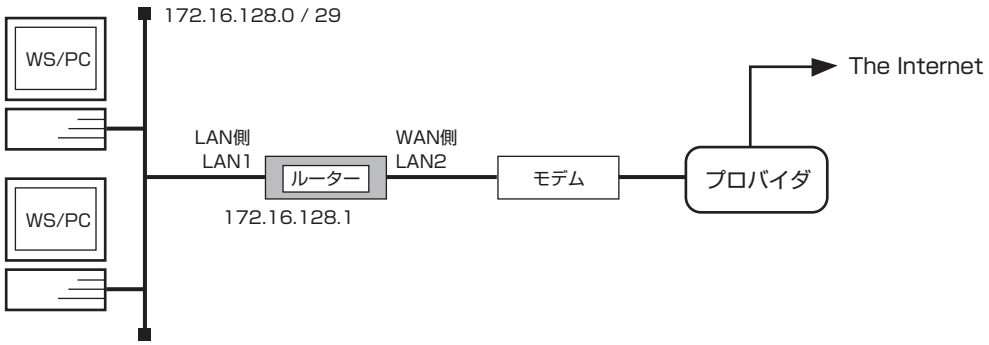
13. # dhcp service server
    # dhcp scope 1 192.168.0.2-192.168.0.254/24
    LAN1 側のホストにプライベートアドレスをリースするための DHCP サーバ機能を設定します。

14. # save

22.2 ネットワーク型接続

複数のグローバルアドレスが予め与えられるネットワーク型接続の例です。LAN 側のすべてのホストはグローバルアドレスを持つものとし、NAT は使用しません。切断タイマはデフォルトで off ですが、切断の必要がある場合には **pppoe disconnect time** コマンドと **pppoe auto disconnect** コマンドで設定します。実装されているPPPoE 機能はクライアントとして動作しますので、サーバに対するアクセスは可能ですが、接続のない状態からアクセスを受けることはできません。

[構成図]



・LAN1 を LAN 側、LAN2 側を WAN 側とする
・PPPoE サーバに対してはネットワーク型接続を行うものとする
・LAN1 側で使用可能なグローバルアドレスを 172.16.128.0/29 とする
・LAN2 側はブロードバンド回線モデム等からのイーサネット回線に接続する

[設定手順]

```
# ip lan1 address 172.16.128.1/29
# pp select 1
pp1# pppoe use lan2
pp1# pp auth accept chap pap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ip pp mtu 1454
pp1# ppp ccp type none
pp1# pp enable 1
pp1# pp select none
# ip route default gateway pp 1
# dns server SERVER
# save
```

[解説]

1. # ip lan1 address 172.16.128.1/29
   LAN1 側アドレスを設定します。また LAN 側のすべてのホストは、このネットワーク内のグローバルアドレスを持ちます。

2. # pp select 1
   pp1# pppoe use lan2
   LAN2 側に対して PPPoE を使用するよう設定します。
   この 1 行以外の設定は、基本的にはダイヤルアップでネットワーク型接続する場合と同じです。

3. pp1# pp auth accept chap pap
   pp1# pp auth myname ID PASSWORD
   PPPoE サーバとの認証情報を設定します。

4. pp1# ppp lcp mru on 1454
   LCP のネゴシエーションで Maximum-Receive-Unit オプションを使用し、パケットの最大長を制限します。

5. pp1# ppp ccp type none
   圧縮機能は使用できません。デフォルトでは stac 圧縮を使うようネゴシエーションすることになりますので、none に設定する必要があります。

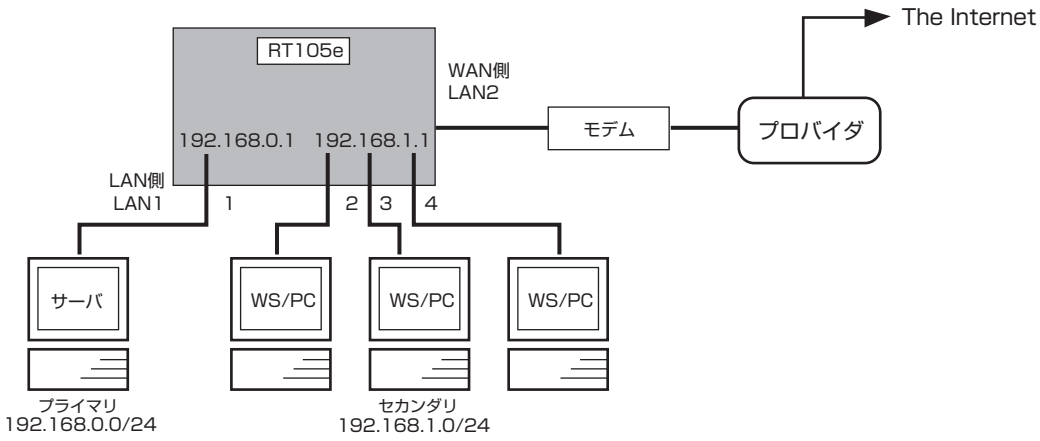
6. pp1# pp enable 1
   pp1# pp select none
   # ip route default gateway pp 1
   宛先が LAN 外であるすべてのパケットを送るためのデフォルトルートを相手先情報番号 "pp1" に設定します。

7. # dns server SERVER
   プロバイダが提供する DNS サーバの IP アドレスを設定します。

8. # save

22.3 特定ポートをサーバ公開用セグメントとして使用 (RT105e)

[構成図]



・接続時に ipcp で得る 1 グローバルアドレスを使用
・WAN 接続には PPPoE 使用

[設定手順]

```
# lan type lan1 port-based-ks8995e primary 1 secondary 2 3 4
# ip lan1 address 192.168.0.1/24
# ip lan1 secondary address 192.168.1.1/24
# nat descriptor type 1 masquerade
# nat descriptor masquerade static 1 1 192.168.0.2 tcp www
# pp select 1
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname USERID PASSWORD
pp1# ppp ipcp ipaddress on
pp1# ppp ipcp msext on
pp1# ppp lcp mru on 1454
pp1# ip pp mtu 1454
pp1# ppp ccp type none
pp1# ip route default gateway pp 1
pp1# pp enable 1
pp1# ip pp nat descriptor 1
pp1# save
```

[解説]

公開サーバはプライベートアドレスを持ちますが、接続時に得られるグローバルアドレスと静的 IP マスカレードを使って公開します。セカンダリセグメント機能を利用して公開サーバ用のネットワークを独立させます。LAN1 側でブロードキャストドメインが分けられます。LAN2 での WAN 接続には PPPoE を使用します。

プライマリ / セカンダリ間の相互通信のパケットは必ず RT のルーティング処理を経由することになります。フィルタや NAT 処理も可能です。
LAN1 の両ネットワークから LAN2 経由 WAN へのアクセスが可能です。
LAN1 に対する RT 自身からのブロードキャストパケットは LAN1 全ポートに送出されます。
RIP はプライマリアドレスネットワークにしか使用できません。

1. # lan type lan1 port-based-ks8995e primary 1 secondary 2 3 4
   LAN1 のポート 1 を公開サーバ用のプライマリネットワーク、ポート 2,3,4 をセカンダリネットワークとします。
   プライマリネットワークには 192.168.0.0/24 のネットワークアドレスを持つホストを接続し、セカンダリネットワークには 192.168.1.0/24 のネットワークアドレスを持つホストを接続します。

2. # ip lan1 address 192.168.0.1/24
   # ip lan1 secondary address 192.168.1.1/24
   それぞれのネットワークに適用する IP アドレスを設定します。

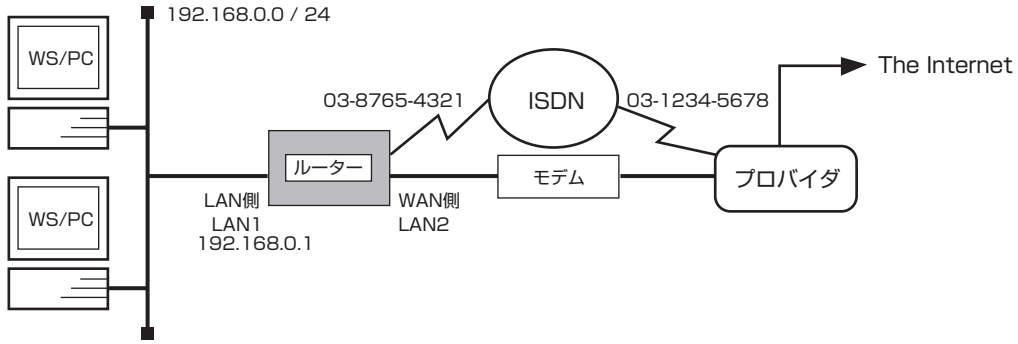
3. # nat descriptor type 1 masquerade
   # nat descriptor masquerade static 1 1 192.168.0.2 tcp www
   LAN1 からの WAN アクセスのために IP マスカレードを定義します。公開サーバ用に静的マスカレードを設定します。
   公開サーバの持つプライベートアドレスを 192.168.0.2 としています。

4. # pp select 1
   pp1# pppoe use lan2
   pp1# pp auth accept pap chap
   pp1# pp auth myname USERID PASSWORD
   pp1# ppp ipcp ipaddress on
   pp1# ppp ipcp msext on
   pp1# ppp lcp mru on 1454
   pp1# ip pp mtu 1454
   pp1# ppp ccp type none
   pp1# ip route default gateway pp 1
   pp1# pp enable 1
   pp1 に対して PPPoE の設定を行います。詳しくは PPPoE の設定例を参照してください。

5. pp1# ip pp nat descriptor 1
   pp1# save
   IP マスカレード機能を定義した NAT ディスクリプタを pp1 に適用します。

22.4 プロバイダ端末型接続を ISDN によるプロバイダ端末型接続でバックアップ

[構成図]



[設定手順]

```
# isdn local address bri1 0387654321
# ip lan1 address 192.168.0.1/24
# nat descriptor type 1 masquerade
# pp select 1
pp1# pp backup pp 2
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname name-orig pass-orig
pp1# ppp ipcp ipaddress on
pp1# ppp ipcp msext on
pp1# ppp ccp type none
pp1# ppp lcp mru on 1454
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# ip route default gateway pp 1
pp1# pp enable 1
pp1# pp select 2
pp2# pp bind bri1
pp2# isdn remote address call 0312345678
pp2# pp auth accept chap
pp2# pp auth myname name-back pass-back
pp2# ppp ipcp ipaddress on
pp2# ppp ipcp msext on
pp2# ip pp nat descriptor 1
pp2# pp enable 2
pp2# save
```

[解説]

プロバイダ接続のバックアップを行います。PPPoE 接続で常時接続状態を保持しますが、何らかの原因でその接続が切れた場合には ISDN でプロバイダに接続します。プロバイダへの接続は端末型接続であり、IP マスカレードを使用します。

1. # isdn local address bri1 0387654321
   # ip lan1 address 192.168.0.1/24
   自側 ISDN 番号と LAN 側のアドレスを設定します。LAN2 側は PPPoE を使用するので IP アドレスは付与しません。

2. # nat descriptor type 1 masquerade
   IP マスカレード機能を適用するための NAT ディスクリプタを定義します。

3. # pp select 1
   pp1# pp backup pp 2
   バックアップの pp を設定します。

4. pp1# pp always-on on
   キープアライブによる切断検知と障害時の復旧操作を行うために常時接続機能を設定します。

5. pp1# pppoe use lan2
   pp1# pp auth accept pap chap
   pp1# pp auth myname name-orig pass-orig
   pp1# ppp ipcp ipaddress on
   pp1# ppp ipcp msext on
   pp1# ppp ccp type none
   pp1# ppp lcp mru on 1454
   pp1# ip pp mtu 1454
   pp1 に対して PPPoE の設定を行います。詳しくは PPPoE の設定例を参照してください。

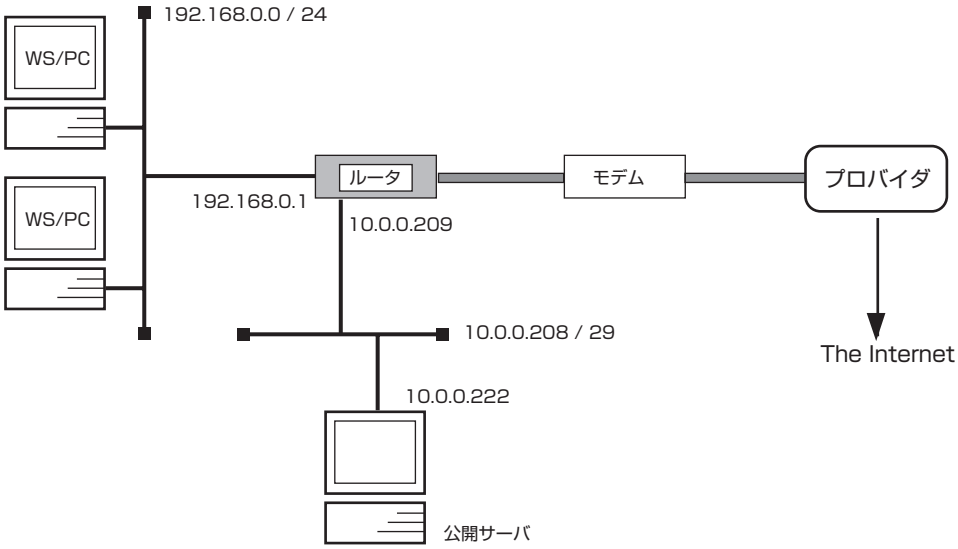
6. pp1# ip pp nat descriptor 1
   IP マスカレード機能を定義した NAT ディスクリプタを pp1 に適用します。

7. pp1# ip route default gateway pp 1
   pp1# pp enable 1
   デフォルト経路を設定します。バックアップに切り替わると経路情報もバックアップ先に引き継がれますので、バックアップ先に対して経路設定は不要です。

8. pp1# pp select 2
   pp2# pp bind bri1
   pp2# isdn remote address call 0312345678
   pp2# pp auth accept chap
   pp2# pp auth myname name-back pass-back
   pp2# ppp ipcp ipaddress on
   pp2# ppp ipcp msext on
   pp2# ip pp nat descriptor 1
   pp2# pp enable 2
   pp2# save
   pp2 に対して ISDN 経由のプロバイダ接続設定を行います。IP マスカレード機能を定義した NAT ディスクリプタを pp2 にも適用します。バックアップ回線に切り替わった時にはこちらの NAT/ マスカレードテーブルが使われます。

22.5 LAN 側ネットワークをプライベート IP アドレス+グローバル IP アドレスで構成する

[構成図]



[設定手順]

```
# ip lan1 address 10.0.0.209/28
# ip lan1 secondary address 192.168.0.1/24
# pp select 1
pp1# pppoe use lan2
pp1# pp auth accept chap pap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ip pp mtu 1454
pp1# ppp ccp type none
pp1# ip pp nat descriptor 1
pp1# pp enable 1
pp1# ip route default gateway pp 1
pp1# nat descriptor type 1 masquerade
pp1# nat descriptor address outer 1 10.0.0.210
pp1# nat descriptor address inner 1 192.168.0.1-192.168.0.254
pp1# dns server SERVER
pp1# dhcp service server
pp1# dhcp scope 1 192.168.0.2-192.168.0.254/24
pp1# save
```

[解説]

LAN 側をプライベートアドレス空間とグローバルアドレス空間の 2 つのネットワークで構成します。公開サーバはグローバルアドレス空間に置くため、動的アドレス変換は使用しません。プライベートアドレス空間の ネットワークに接続した端末は IP マスカレードを使用して複数同時接続を行います。ブロードバンドルーターの LAN 側はプライマリ / セカンダリアドレスで 2 つのネットワークに接続します。公開サーバをファイアウォール機能で守りつつ、WAN 側と同じアドレスを付与できます。

インターネットは、有益な情報もありますが、危険もあります。最低限のフィルタなどを適用して、自分のネットワークを守る必要があります。特にサーバを公開するにあたってはしっかりとセキュリティ設定を行ってください。ここで示す設定例にはセキュリティ設定は含まれていません。お使いの 環境に合わせたセキュリティ設定を行ってください。

- LAN1 を LAN 側、LAN2 を WAN 側とします。
- LAN 側のプライベートネットワークでは複数端末からの同時接続を可能とするため、WAN 側に対して IP マスカレード機能を使用します。
- コンピュータの IP アドレスの割り当て管理のために DHCP サーバ機能が利用できます。

プロバイダから割り当てられたグローバルアドレスを 10.0.0.208/28 のネットワークとすると、IP アドレスの割り当ては次の表のようになります。

IP アドレス	用途
ルーターのプライマリ・ネットワーク (グローバルアドレス空間)	
10.0.0.208	network address
10.0.0.209	ルーター
10.0.0.222	公開サーバ
10.0.0.210	ＮＡＴ ディスクリプタ用アドレス
10.0.0.211 ～ 10.0.0.221	固定割り当て
10.0.0.223	(directed) broadcast address
255.255.255.240	subnet mask
ルーターのセカンダリ・ネットワーク (プライベートアドレス空間)	
192.168.0.0	network address
192.168.0.1	ルーター
192.168.0.2 ～ 192.168.0.254	DHCP 割り当て
192.168.0.255	(directed) broadcast address
255.255.255.0	subnet mask

1. # ip lan1 address 10.0.0.209/28
   LAN1 側のプライマリ・ネットワークアドレスを設定します。また LAN 側のプライマリ・ネットワークのホストは、このネットワーク内のグローバルアドレスを持ちます。

2. # ip lan1 secondary address 192.168.0.1/24
   LAN1 側のセカンダリ・ネットワークアドレスを設定します。また LAN 側のセカンダリ・ネットワークのホストは、このネットワーク内のプライベートアドレスを持ちます。

3. # pp select 1
   PP1 インタフェースを設定します。

4. pp1# pppoe use lan2
   LAN2 側（WAN 側）に対して PPPoE を使用するよう設定します。この 1 行以外の設定は、基本的にはダイヤルアップでネットワーク型接続をする場合と同じです。

5. pp1# pp auth accept chap pap
   pp1# pp auth myname ID PASSWORD
   PPPoE サーバとの認証情報を設定します。

6. pp1# ppp lcp mru on 1454
   LCP のネゴシエーションで Maximum-Receive-Unit オプションを使用し、パケットの最大長を制限します。

7. pp1# ip pp mtu 1454
   このコマンドは、接続相手から LCP で MRU オプションを受ける場合には必要ありません。PP1 に対する MTU(Maximum Transfer Unit) を設定します。

8. pp1# ppp ccp type none
   圧縮機能は PPPoE では使用できません。none に設定する必要があります。

9. pp1# ip pp nat descriptor 1
   IP マスカレード機能を定義した NAT ディスクリプタを PP1 に適用します。

10. pp1# pp enable 1
    PP1 を有効にします。

11. pp1# ip route default gateway pp 1
    宛先が LAN 外である全てのパケットを送るためのデフォルトルートを PP1 に設定します。

12. pp1# nat descriptor type 1 masuquerade
    PP1 に IP マスカレード機能を適用するための NAT ディスクリプタを定義します。

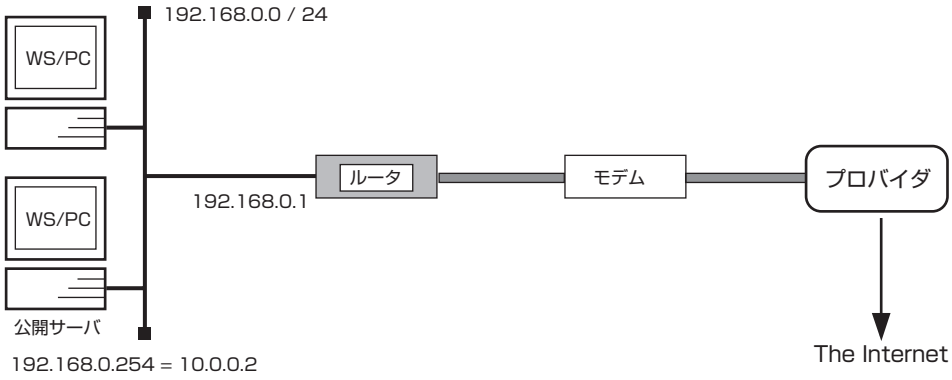
13. pp1# nat descriptor address outer 1 10.0.0.210
    pp1# nat descriptor address inner 1 192.168.0.1-192.168.0.254
    NAT ディスクリプタで使用される外側と内側の IP アドレスを指定します。

14. pp1# dns server SERVER
    プロバイダ側から指定された DNS サーバを設定します。

15. pp1# dhcp service server
    pp1# dhcp scope 1 192.168.0.2-192.168.0.254/24
    DHCP サーバとして動作させ、LAN 側セカンダリ・ネットワークの DHCP 機能で割り当てる IP アドレスの範囲を指定します。

22.6 LAN 側ネットワークをプライベート IP アドレスで構成する

[構成図]



[設定手順]

```
# ip lan1 address 192.168.0.1/24
# pp select 1
pp1# pppoe use lan2
pp1# pp auth accept chap pap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ip pp mtu 1454
pp1# ppp ccp type none
pp1# ip pp nat descriptor 1
pp1# pp enable 1
pp1# ip route default gateway pp 1
pp1# nat descriptor type 1 masquerade
pp1# nat descriptor address outer 1 10.0.0.1
pp1# nat descriptor address inner 1 192.168.0.1-192.168.0.254
pp1# nat descriptor static 1 1 10.0.0.2=192.168.0.254 1
pp1# dns server SERVER
pp1# dhcp service server
pp1# dhcp scope 1 192.168.0.2-192.168.0.253/24
pp1# save
```

[解説]

公開サーバを含め、LAN 側をすべてプライベートアドレス空間のネットワークで構成します。インターネットとのアクセスは NAT 変換や IP マスカレードを使用します。公開サーバには静的 NAT で固定のグローバルアドレスを 割り当てる必要があります。その他の LAN 側端末とブロードバンドルーターはブロードバンドルーターの WAN 側アドレス（グローバルアドレス）を使用し、IP マスカレード機能を使って複数同時接続を行います。

公開サーバを置くということは、外部からアクセスが可能であるということです。インターネットは、有益な情報もありますが、危険もあります。最低限のフィルタなどを適用して、自分のネットワークを守る必要があります。特にサーバを公開するにあたってはしっかりとセキュリティ設定を行ってください。ここで示す設定例にはセキュリティ設定は含まれていません。お使いの 環境に合わせたセキュリティ設定を行ってください。

- LAN1 を LAN 側、LAN2 を WAN 側とします。
- LAN 側の複数端末からの同時接続を可能とするため、WAN 側に対して IP マスカレード機能を使用します。
- プロバイダから割り当てられたグローバルアドレスを 2 個とし、1 つは NAT ディスクリプタの外側アドレス、もう 1 つは公開サーバ専用の IP アドレスとします。
- コンピュータの IP アドレスの割り当て管理のために DHCP サーバ機能が利用できます。

プロバイダから割り当てられたグローバルアドレスを 10.0.0.1, 10.0.0.2 とすると、IP アドレスの割り当ては次の表のようになります。

IP アドレス	用途
グローバルアドレスの割り当て	
10.0.0.1	IP マスカレード機能用外側アドレス
10.0.0.2	公開サーバ（静的 NAT）
LAN 側ネットワーク (プライベートアドレス空間)	
192.168.0.0	network address
192.168.0.1	ルーター
192.168.0.2 ～ 192.168.0.253	DHCP 割り当て
192.168.0.254	公開サーバ
192.168.0.255	(directed) broadcast address
255.255.255.0	subnet mask

1. # ip lan1 address 192.168.0.1/24
   LAN1 側 IP アドレスを設定します。また LAN 側のすべてのホストは、このネットワーク内のプライベートアドレスを持ちます。

2. # pp select 1
   pp1# pppoe use lan2
   LAN2 側（WAN 側）に対して PPPoE を使用するよう設定します。この 1 行以外の設定は、基本的にはダイヤルアップで端末型接続をする場合と同じです。

3. pp1# pp auth accept chap pap
   pp1# pp auth myname ID PASSWORD
   PPPoE サーバとの認証情報を設定します。

4. pp1# ppp lcp mru on 1454
   LCP のネゴシエーションで Maximum-Receive-Unit オプションを使用し、パケットの最大長を制限します。

5. pp1# ip pp mtu 1454
   このコマンドは、接続相手から LCP で MRU オプションを受ける場合には必要ありません。PP1 に対する MTU(Maximum Transfer Unit) を設定します。

6. pp1# ppp ccp type none
   圧縮機能は PPPoE では使用できません。none に設定する必要があります。

7. pp1# ip pp nat descriptor 1
   IP マスカレード機能を定義した NAT ディスクリプタを PP1 に適用します。

8. pp1# pp enable 1
   PP1 を有効にします。

9. pp1# ip route default gateway pp 1
   宛先が LAN 外である全てのパケットを送るためのデフォルトルートを PP1 に設定します。

10. pp1# nat descriptor type 1 masquerade
    pp1# nat descriptor address outer 1 10.0.0.1
    pp1# nat descriptor address inner 1 192.168.0.1-192.168.0.254
    PP1 に IP マスカレード機能を適用するための NAT ディスクリプタを定義し、NAT ディスクリプタで使用される外側と内側の IP アドレスを指定します。

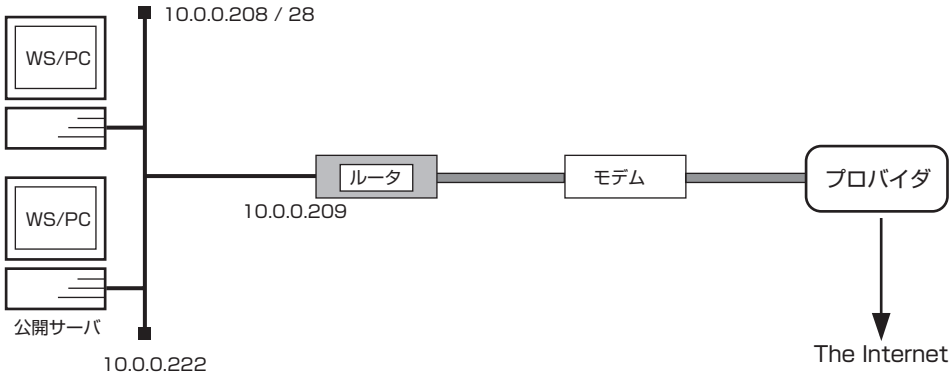
11. pp1# nat descriptor static 1 1 10.0.0.2=192.168.0.254 1
    NAT ディスクリプタで固定割付する IP アドレスの組み合わせを指定します。

12. pp1# dns server SERVER
    プロバイダ側から指定された DNS サーバを設定します。

13. pp1# dhcp service server
    pp1# dhcp scope 1 192.168.0.2-192.168.0.253/24
    DHCP サーバとして動作させ、プライベートネットワークに対して DHCP 機能で割り当てる IP アドレスの範囲を指定します。

22.7 LAN 側ネットワークをグローバル IP アドレスで構成する

[構成図]



[設定手順]

```
# ip lan1 address 10.0.0.209/28
# pp select 1
pp1# pppoe use lan2
pp1# pp auth accept chap pap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ip pp mtu 1454
pp1# ppp ccp type none
pp1# pp enable 1
pp1# ip route default gateway pp 1
pp1# dns server SERVER
pp1# dhcp service server
pp1# dhcp scope 1 10.0.0.210-10.0.0.221/28
pp1# save
```

[解説]

LAN 側をすべてグローバルアドレス空間のネットワークで構成します。すべてグローバルアドレスで構成するため、動的アドレス変換をする必要がありません。逆にいえばすべての LAN 側端末と IP アドレスで直接通信できることになりますのでセキュリティには 十分に対処する必要があります。

インターネットは、有益な情報もありますが、危険もあります。最低限のフィルタなどを適用して、自分のネットワークを守る必要があります。特にサーバを公開するにあたってはしっかりとセキュリティ設定を行ってください。ここで示す設定例にはセキュリティ設定は含まれていません。お使いの 環境に合わせたセキュリティ設定を行ってください。

・LAN1 を LAN 側、LAN2 を WAN 側とします。
・コンピュータの IP アドレスの割り当て管理のために DHCP サーバ機能が利用できます。

プロバイダから割り当てられたグローバルアドレスを 10.0.0.208/28 のネットワークとすると、IP アドレスの割り当ては次の表のようになります。

IP アドレス	用途
LAN 側ネットワーク (グローバルアドレス空間)	
10.0.0.208	network address
10.0.0.209	ルーター
10.0.0.210 ～ 10.0.0.221	DHCP 割り当て
10.0.0.222	公開サーバ
10.0.0.223	(directed) broadcast address
255.255.255.240	subnet mask

1. # ip lan1 address 10.0.0.209/28
   LAN1 側 IP アドレスを設定します。また LAN 側のすべてのホストは、このネットワーク内のグローバルアドレスを持ちます。

2. # pp select 1
   PP1 インタフェースを設定します。

3. pp1# pppoe use lan2
   LAN2 側（WAN 側）に対して PPPoE を使用するよう設定します。この 1 行以外の設定は、基本的にはダイヤルアップでネットワーク型接続をする場合と同じです。

4. pp1# pp auth accept chap pap
   pp1# pp auth myname ID PASSWORD
   PPPoE サーバとの認証情報を設定します。

5. pp1# ppp lcp mru on 1454
   LCP のネゴシエーションで Maximum-Receive-Unit オプションを使用し、パケットの最大長を制限します。

6. pp1# ip pp mtu 1454
   このコマンドは、接続相手から LCP で MRU オプションを受ける場合には必要ありません。PP1 に対する MTU(Maximum Transfer Unit) を設定します。

7. pp1# ppp ccp type none
   圧縮機能は PPPoE では使用できません。none に設定する必要があります。

8. pp1# pp enable 1
   PP1 を有効にします。

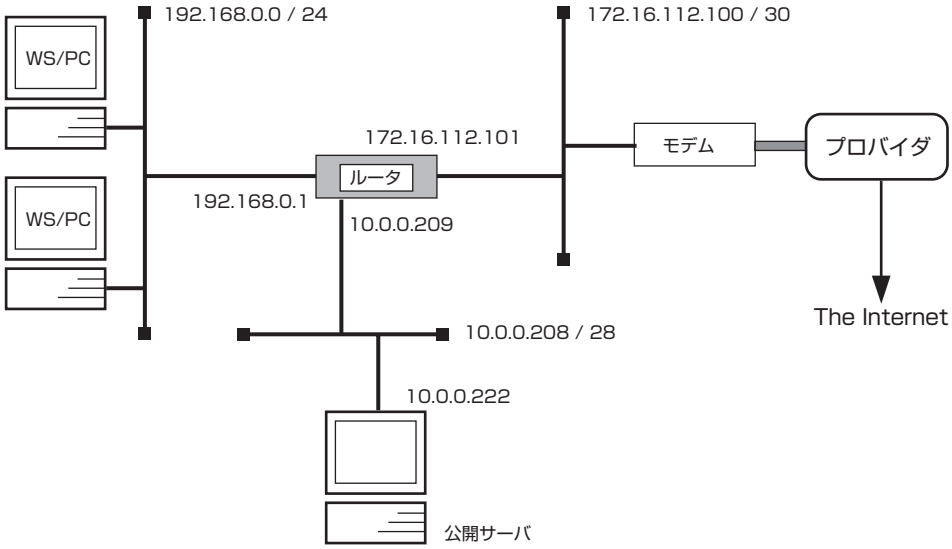
9. pp1# ip route default gateway pp 1
   宛先が LAN 外である全てのパケットを送るためのデフォルトルートを PP1 に設定します。

10. pp1# dns server (プロバイダ側から指定された IP アドレス）
    DNS サーバを設定します。

11. pp1# dhcp service server
    pp1# dhcp scope 1 10.0.0.210-10.0.0.221/28
    DHCP サーバとして動作させ、LAN 側ネットワークに対して DHCP 機能で割り当てる IP アドレスの範囲を指定します。

22.8 LAN 側ネットワークをプライベート IP アドレス+グローバル IP アドレスで構成する

[構成図]



[設定手順]

```
# ip lan1 address 10.0.0.209/28
# ip lan1 secondary address 192.168.0.1/24
# ip lan2 address 172.16.112.101/30
# ip lan2 nat descriptor 1
# ip route default gateway GATEWAY
# nat descriptor type 1 masquerade
# nat descriptor address outer 1 10.0.0.210
# nat descriptor address inner 1 192.168.0.1-192.168.0.254
# dns server SERVER
# dhcp service server
# dhcp scope 1 10.0.0.211-10.0.0.221/28
# dhcp scope 2 192.168.0.2-192.168.0.254/24
# save
```

[解説]

LAN 側をプライベートアドレス空間とグローバルアドレス空間の 2 つのネットワークで構成します。公開サーバはグローバルアドレス空間に置くため、動的アドレス変換は使用しません。プライベートアドレス空間のネットワークに接続した端末は IP マスカレードを使用して複数同時接続を行います。ブロードバンドルーターの LAN 側はプライマリ / セカンダリアドレスで 2 つのネットワークに接続します。公開サーバをファイアウォール機能で守りつつ、WAN 側と同じアドレスを付与できます。

インターネットは、有益な情報もありますが、危険もあります。最低限のフィルタなどを適用して、自分のネットワークを守る必要があります。特にサーバを公開するにあたってはしっかりとセキュリティ設定を行ってください。ここで示す設定例にはセキュリティ設定は含まれていません。お使いの 環境に合わせたセキュリティ設定を行ってください。

- LAN1 を LAN 側、LAN2 を WAN 側とします。
- LAN 側のプライベートネットワークでは複数端末からの同時接続を可能とするため、WAN 側に対して IP マスカレード機能を使用します。
- プロバイダから割り当てられたグローバルアドレス (10.0.0.208/28) を LAN 側に割り当てます。
- プロバイダから割り当てられたプライベートアドレス (172.16.112.100/30) を WAN 側に割り当てます。
- コンピュータの IP アドレスの割り当て管理のために DHCP サーバ機能が利用できます。

プロバイダから割り当てられたグローバルアドレスを 10.0.0.208/28、プロバイダから割り当てられたプライベートアドレスを 172.16.112.100/30 すると、IP アドレスの割り当ては次の表のようになります。

P アドレス	用途
ルーターの WAN 側ネットワーク (プライベートアドレス空間)	
172.16.112.100	network address
172.16.112.101	ルーター
172.16.112.103	(directed) broadcast address
255.255.255.252	subnet mask
ルーターの LAN 側プライマリ・ネットワーク (グローバルアドレス空間)	
10.0.0.208	network address
10.0.0.209	ルーター
10.0.0.210	NAT ディスクリプタ用アドレス
10.0.0.211 ～ 10.0.0.221	DHCP 割り当て
10.0.0.222	公開サーバ
10.0.0.223	(directed) broadcast address
255.255.255.240	subnet mask
ルーターの LAN 側セカンダリ・ネットワーク (プライベートアドレス空間)	
192.168.0.0	network address
192.168.0.1	ルーター
192.168.0.2 ～ 192.168.0.254	DHCP 割り当て
192.168.0.255	(directed) broadcast address
255.255.255.0	subnet mask

1. # ip lan1 address 10.0.0.209/28
   LAN1 側のプライマリ・ネットワークアドレスを設定します。また LAN 側のプライマリ・ネットワークのホストは、このネットワーク内のグローバルアドレスを持ちます。

2. # ip lan1 secondary address 192.168.0.1/24
   LAN1 側のセカンダリ・ネットワークアドレスを設定します。また LAN 側のセカンダリ・ネットワークのホストは、このネットワーク内のプライベートアドレスを持ちます。

3. # ip lan2 address 172.16.112.101/30
   LAN2 側 IP アドレスを設定します。

4. # ip lan2 nat descriptor 1
   IP マスカレード機能を定義した NAT ディスクリプタを LAN2 に適用します。

5. # ip route default gateway GATEWAY
   宛先が LAN 外である全てのパケットを送るためのデフォルトルートを設定します。(プロバイダから指定されたゲートウェイアドレス)

6. # nat descriptor type 1 masquerade
   LAN2 に IP マスカレード機能を適用するための NAT ディスクリプタを定義します。

7. # nat descriptor address outer 1 10.0.0.210
   # nat descriptor address inner 1 192.168.0.1-192.168.0.254
   NAT ディスクリプタで使用される外側と内側のの IP アドレスを指定します。

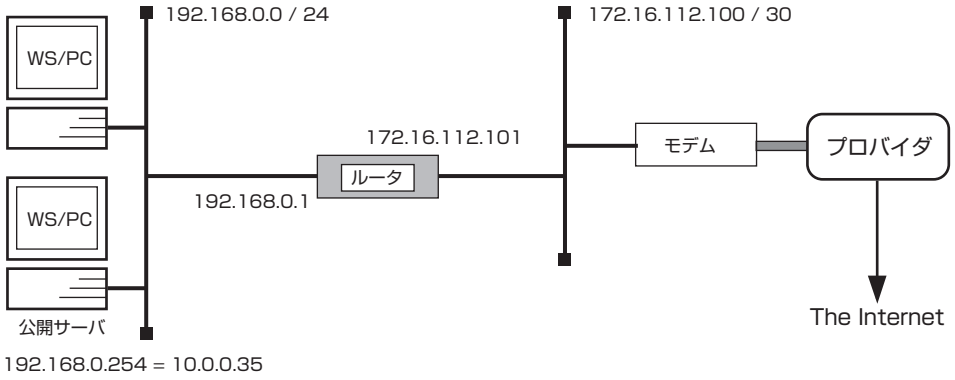
8. # dns server SERVER
   プロバイダから指定された DNS サーバを設定します。

9. # dhcp service server
   # dhcp scope 1 10.0.0.211-10.0.0.221/28
   DHCP サーバとして動作させ、LAN 側プライマリ・ネットワークの DHCP 機能で割り当てる IP アドレスの範囲を指定します。

   # dhcp scope 2 192.168.0.2-192.168.0.254/24
   LAN 側セカンダリ・ネットワークの DHCP 機能で割り当てる IP アドレスの範囲を指定します。

22.9 LAN 側ネットワークをプライベート IP アドレスで構成する

[構成図]



[設定手順]

```
# ip lan1 address 192.168.0.1/24
# ip lan2 address 172.16.112.101/30
# ip lan2 nat descriptor 1
# ip route default gateway GATEWAY
# nat descriptor type 1 masquerade
# nat descriptor address outer 1 10.0.0.34
# nat descriptor address inner 1 192.168.0.1-192.168.0.253
# nat descriptor static 1 1 10.0.0.35=192.168.0.254 1
# dns server SERVER
# dhcp service server
# dhcp scope 1 192.168.0.2-192.168.0.253/24
# save
```

[解説]

公開サーバを含め、LAN 側をすべてプライベートアドレス空間のネットワークで構成します。インターネットとのアクセスは NAT 変換や IP マスカレードを使用します。公開サーバには静的 NAT で固定のグローバルアドレスを 割り当てる必要があります。その他の LAN 側端末とブロードバンドルーターは別のグローバルアドレスを 使用し、IP マスカレード機能を使って複数同時接続を行います。

公開サーバを置くということは、外部からアクセスが可能であるということです。インターネットは、有益な情報もありますが、危険もあります。最低限のフィルタなどを適用して、自分のネットワークを守る必要があります。特にサーバを公開するにあたってはしっかりとセキュリティ設定を行ってください。ここで示す設定例にはセキュリティ設定は含まれていません。お使いの 環境に合わせたセキュリティ設定を行ってください。

- LAN1 を LAN 側、LAN2 を WAN 側とします。
- LAN 側の複数端末からの同時接続を可能とするため、WAN 側に対して IP マスカレード機能を使用します。
- プロバイダから割り当てられたグローバルアドレスを 2 個とし、1 つは NAT ディスクリプタ用、もう 1 つは公開サーバ専用の IP アドレスとします。
- コンピュータの IP アドレスの割り当て管理のために DHCP サーバ機能が利用できます。

プロバイダから割り当てられたグローバルアドレスを 10.0.0.34, 10.0.0.35 とすると、IP アドレスの割り当ては次の表のようになります。

IP アドレス	用途
グローバルアドレスの割り当て	
10.0.0.34	NAT ディスクリプタ用アドレス
10.0.0.35	公開サーバ（静的 NAT）
LAN 側ネットワーク (プライベートアドレス空間)	
192.168.0.0	network address
192.168.0.1	ルーター
192.168.0.2 ～ 192.168.0.253	DHCP 割り当て
192.168.0.254	公開サーバ
192.168.0.255	(directed) broadcast address
255.255.255.0	subnet mask

1. # ip lan1 address 192.168.0.1/24
   LAN1 側 IP アドレスを設定します。また LAN 側のすべてのホストは、このネットワークアドレス内のプライベートアドレスを持ちます。

2. # ip lan2 address 172.16.112.101/30
   LAN2 側 IP アドレスを設定します。

3. # ip lan2 nat descriptor 1
   IP マスカレード機能を定義した NAT ディスクリプタを LAN2 に適用します。

4. # ip route default gateway GATEWAY
   宛先が LAN 外である全てのパケットを送るためのデフォルトルートを設定します (プロバイダから指定されたゲートウェイアドレス)。

5. # nat descriptor type 1 masquerade
   LAN2 に IP マスカレード機能を適用するための NAT ディスクリプタを定義します。

6. # nat descriptor address outer 1 10.0.0.34
   # nat descriptor address inner 1 192.168.0.1-192.168.0.253
   NAT ディスクリプタで使用される外側と内側の IP アドレスを指定します。

7. # nat descriptor static 1 1 10.0.0.35=192.168.0.254 1
   NAT ディスクリプタで固定割付する IP アドレスの組み合わせを指定します。

8. # dns serverSERVER
   プロバイダから指定された DNS サーバを設定します。

9. # dhcp service server
   # dhcp scope 1 192.168.0.2-192.168.0.253/24
   DHCP サーバとして動作させ、LAN 側ネットワークに対して DHCP 機能で割り当てる IP アドレスの範囲を指定します。

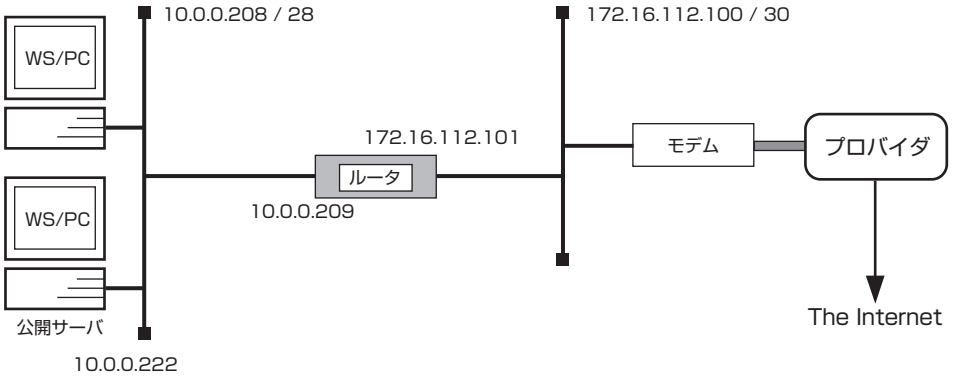
プライベートネットワークの端末から公開サーバに静的 NAT で割り当てられている IP アドレスに対しては通信できません。
192.168.0.2 <==> 10.0.0.35 の通信はできません。(192.168.0.2 <==> 192.168.0.254 は可能)
公開サーバを WWW サーバとした場合、プライベートネットワークの端末 (PC) で公開サーバのホスト名（URL) を指定して公開サーバ内の WWW ページを閲覧するには

・端末 (PC) の DNS サーバのアドレスをブロードバンドルーターのアドレス (192.168.0.1) に設定する。
・ブロードバンドルーターで公開サーバの名前解決の設定をする。
　[コマンド] ip host (サーバの名前）192.168.0.254
・サーバが DNS の逆引きを行うのであれば、クライアントの端末 (PC) についても設定する。
　[コマンド] ip host (PC の名前）192.168.0.2

という手順が必要になります。

22.10 LAN 側ネットワークをグローバル IP アドレスで構成する

[構成図]



[設定手順]

```
# ip lan1 address 10.0.0.209/28
# ip lan2 address 172.16.112.101/30
# ip route default gateway GATEWAY
# dns server SERVER
# dhcp service server
# dhcp scope 1 10.0.0.210-10.0.0.221/28
# save
```

[解説]

LAN 側をすべてグローバルアドレス空間のネットワークで構成します。すべてグローバルアドレスで構成するため、動的アドレス変換をする必要がありません。逆にいえばすべての LAN 側端末と IP アドレスで直接通信できることになりますのでセキュリティには 十分に対処する必要があります。

インターネットは、有益な情報もありますが、危険もあります。最低限のフィルタなどを適用して、自分のネットワークを守る必要があります。特にサーバを公開するにあたってはしっかりとセキュリティ設定を行ってください。ここで示す設定例にはセキュリティ設定は含まれていません。お使いの 環境に合わせたセキュリティ設定を行ってください。

- LAN1 を LAN 側、LAN2 を WAN 側とします。
- プロバイダから割り当てられたグローバルアドレス (10.0.0.208/28) を LAN 側に割り当てます。
- プロバイダから割り当てられたプライベートアドレス (172.16.112.100/30) を WAN 側に割り当てます。
- コンピュータの IP アドレスの割り当て管理のために DHCP サーバ機能が利用できます。

プロバイダから割り当てられたグローバルアドレスを 10.0.0.208/28、プロバイダから割り当てられたプライベートアドレスを 172.16.112.100/30 のネットワークとすると、IP アドレスの割り当ては次の表のようになります。

IP アドレス	用途
ルーターの WAN 側ネットワーク (プライベートアドレス空間)	
172.16.112.100	network address
172.16.112.101	ルーター
172.16.112.103	(directed) broadcast address
255.255.255.252	subnet mask
ルーターの LAN 側ネットワーク (グローバルアドレス空間)	
10.0.0.208	network address
10.0.0.209	ルーター
10.0.0.210 ～ 10.0.0.221	DHCP 割り当て
10.0.0.222	公開サーバ
10.0.0.223	(directed) broadcast address
255.255.255.240	subnet mask

1. # ip lan1 address 10.0.0.209/28
   LAN1 側 IP アドレスを設定します。また LAN 側のすべてのホストは、このネットワーク内のグローバルアドレスを持ちます。

2. # ip lan2 address 172.16.112.101/30
   LAN2 側 IP アドレスを設定します。

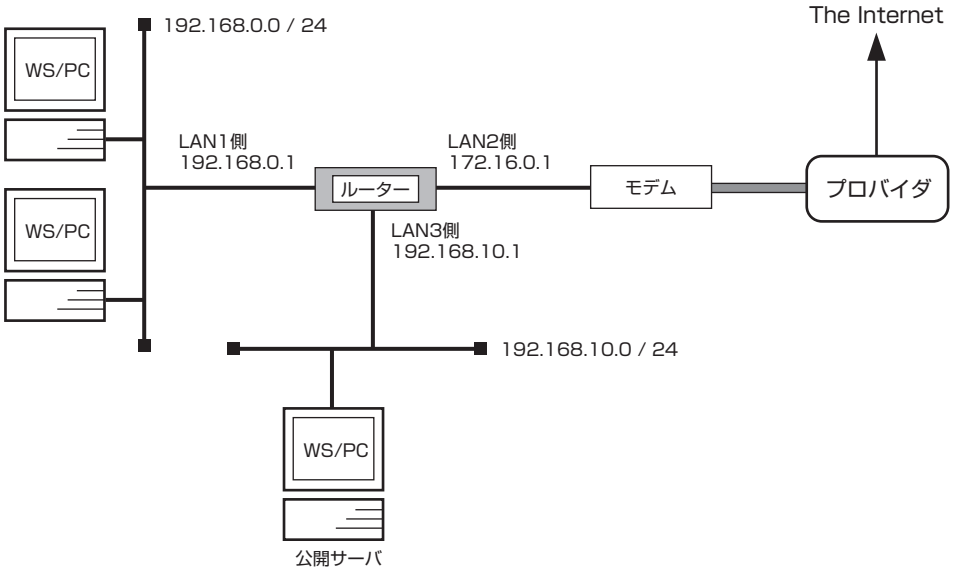
3. # ip route default gateway GATEWAY
   宛先が LAN 外である全てのパケットを送るためのデフォルトルートを設定します (プロバイダから指定されたゲートウェイアドレス)。

4. # dns server SERVER
   プロバイダから指定された DNS サーバを設定します。

5. # dhcp service server
   # dhcp scope 1 10.0.0.210-10.0.0.221/24
   DHCP サーバとして動作させ、LAN 側ネットワークに対して DHCP 機能で割り当てる IP アドレスの範囲を指定します。

22.11 DMZ ポートをサーバ公開用セグメントとして使用

[構成図]



[設定手順]

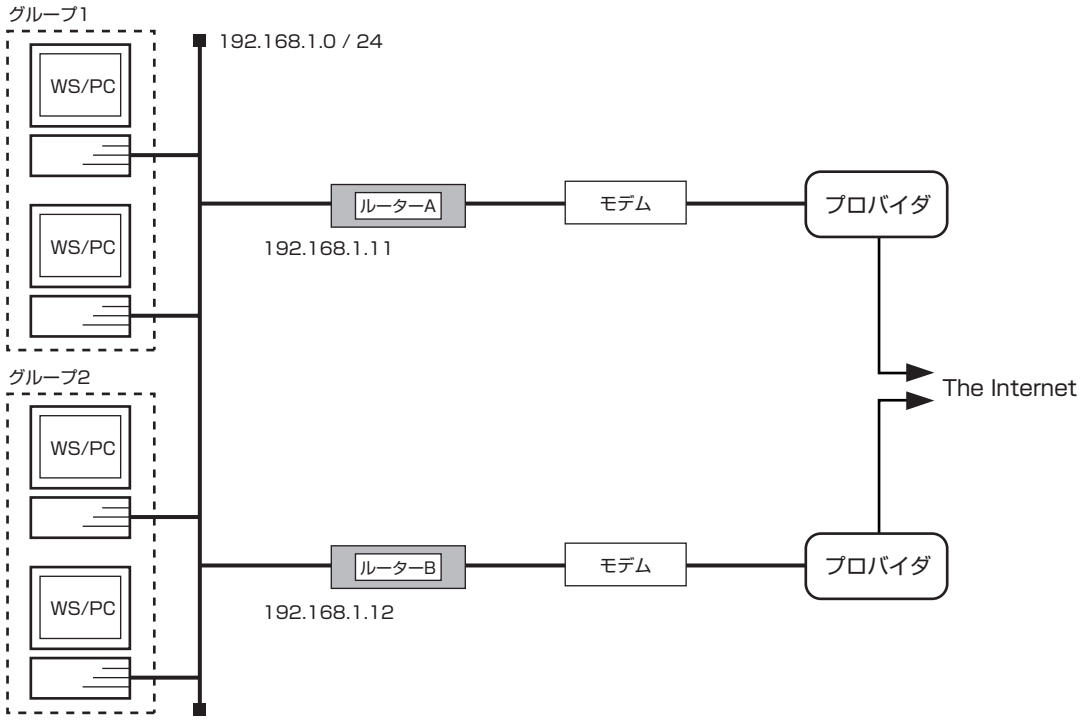
```
# ip lan1 address 192.168.0.1/24
# ip lan3 address 192.168.10.1/24
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ipcp msext on
pp1# ip pp mtu 1454
pp1# ip pp address 172.16.0.1/32
pp1# ip pp nat descriptor 1
pp1# ip pp intrusion detection in on
pp1# pp enable 1
# ip route default gateway pp 1
# nat descriptor type 1 masquerade
# nat descriptor address outer 1 172.16.0.1
# nat descriptor masquerade static 1 1 192.168.10.2 tcp www
# nat descriptor masquerade static 1 2 192.168.10.3 tcp 21
# dhcp service server
# dhcp scope 1 192.168.0.2-192.168.0.100/24
# dns server SERVER
# dns private address spoof on
```

[解説]

LAN1 を LAN ポート、LAN2 を WAN ポート、LAN3 を DMZ ポートとします。
公開サーバはプライベートアドレスを持ちますが、 1 つの固定グローバルアドレスと静的 IP マスカレードを使って公開します。
ファイアウォールの機能が、インターネットからの不正な侵入を防ぎ、公開サーバに対する攻撃を検知します。
3 つ以上のイーサネットインタフェースが必要となりますので、RTX3000、RTX2000、RTX1500、RTX1100、RTX1000、RT300i の利用を前提とした設定例となります。

22.12 2 つのゲートウェイで運用する

[構成図]



[ルーター A の設定手順]

```
# ip route default gateway pp 1
# ip lan1 address 192.168.1.11/24
# ip lan1 vrrp 1 192.168.1.1 priority=200
# ip lan1 vrrp shutdown trigger 1 pp 1
# ip lan1 vrrp 2 192.168.1.2 priority=100
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ipcp ipaddress on
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
# nat descriptor type 1 masquerade
# dns server SERVER
# dns private address spoof on
```

[ルーター B の設定手順]

```
# ip route default gateway pp 1
# ip lan1 address 192.168.1.12/24
# ip lan1 vrrp 1 192.168.1.1 priority=100
# ip lan1 vrrp 2 192.168.1.2 priority=200
# ip lan1 vrrp shutdown trigger 2 pp 1
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ipcp ipaddress on
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
# nat descriptor type 1 masquerade
# dns server SERVER
# dns private address spoof on
```

[解説]

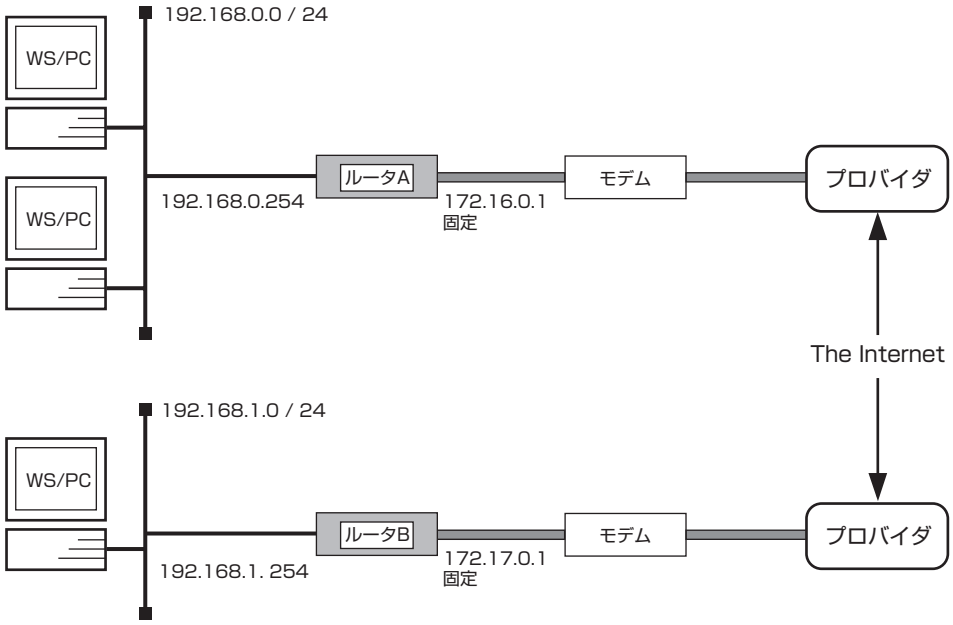
VRRP 機能を利用したルーター及び、WAN 回線冗長化構成です。
PC のグループ 1 はルーター A を、グループ 2 はルーター B をデフォルトゲートウェイとして設定をし、ルーターあるいは WAN 回線に障害が発生した場合に自動的に一方のルーターがカバーする設定になっています。
ルーター A とルーター B は WAN 側と LAN 側にそれぞれイーサネットインタフェースが必要となりますので、RTX3000、RTX2000、RTX1500、RTX1100、RTX1000、RT300i、RT107e の利用を前提とした設定例となります。

23. PPPoE+IPsec を用いたインターネット VPN 環境の設定例

1. VPN 接続したい拠点がすべて固定 IP アドレスの割り当てを受けている場合
2. VPN 環境の中心となる拠点のみが固定 IP アドレスを割り振られている場合
3. インターネット接続を併用する場合（固定 IP アドレス使用）
4. ダイヤルアップ VPN でインターネット接続を併用する場合
5. ダイヤルアップ VPN 環境でセンタ側から拠点方向への通信を行いたい場合

23.1 VPN 接続したい拠点がすべて固定 IP アドレスの割り当てを受けている場合

[構成図]



・インターネットアクセス無し

[ルーター A の設定手順]

```
# ip lan1 address 192.168.0.254/24
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ip pp address 172.16.0.1/32
pp1# ip pp mtu 1454
pp1# pp enable 1
pp1# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel enable 1
tunnel1# ip route 192.168.1.0/24 gateway tunnel 1
tunnel1# ip route default gateway pp 1
tunnel1# ipsec ike pre-shared-key 1 text IKEKEYPASS
tunnel1# ipsec ike remote address 1 172.17.0.1
tunnel1# ipsec ike local address 1 172.16.0.1
tunnel1# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
tunnel1# ipsec auto refresh on
tunnel1# save
```

[ルーター B の設定手順]

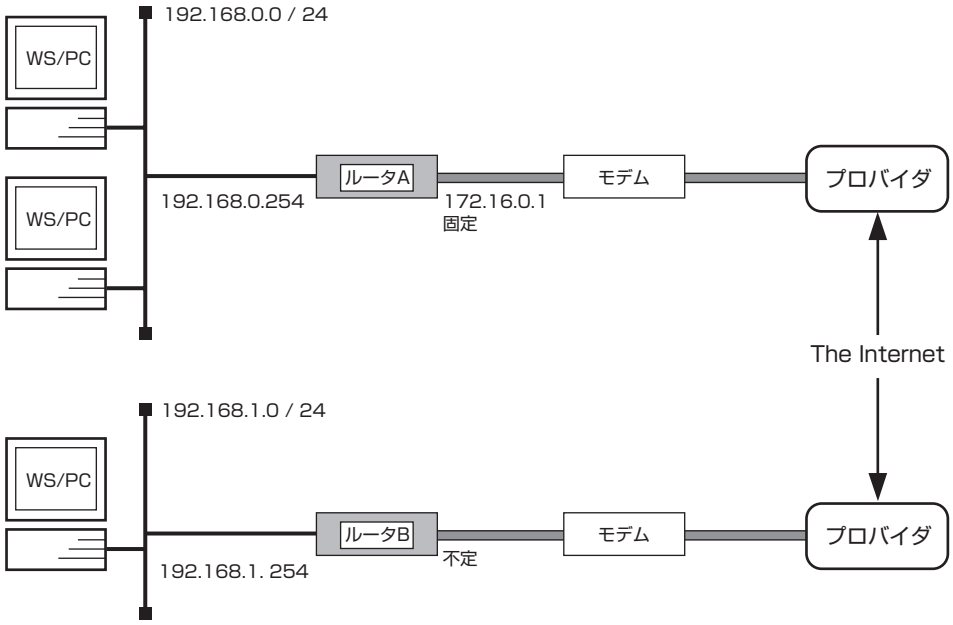
```
# ip lan1 address 192.168.1.254/24
# pp select 1
pp1# pppoe use lan2
pp1# pp always-on on
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ip pp address 172.17.0.1/32
pp1# ip pp mtu 1454
pp1# pp enable 1
pp1# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel enable 1
tunnel1# ip route 192.168.0.0/24 gateway tunnel 1
tunnel1# ip route default gateway pp 1
tunnel1# ipsec ike pre-shared-key 1 text IKEKEYPASS
tunnel1# ipsec ike remote address 1 172.16.0.1
tunnel1# ipsec ike local address 1 172.17.0.1
tunnel1# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
tunnel1# ipsec auto refresh on
tunnel1# save
```

[解説]

本社側が 172.16.0.1、支店側が 172.17.0.1 の固定アドレスの割り当てを受けていると仮定します。本社側 (センタネットワーク（192.168.0.0/24）と支社側（拠点側）ネットワーク（192.168.1.0/24）の間を VPN でつなぐための設定です。WAN 側と LAN 側にそれぞれイーサネットインタフェースが必要となりますので、RTX3000、RTX2000、RTX1500、RTX1100、RTX1000、RT300i、RT140e、RT140f、RT107e、RT105e の利用を前提とした設定例となります。

23.2 VPN 環境の中心となる拠点のみが固定 IP アドレスを割り振られている場合

[構成図]



・インターネットアクセス無し

[ルーター A の設定手順]

```
# ip lan1 address 192.168.0.254/24
# pp select 1
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# pp always-on on
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ip pp mtu 1454
pp1#  ip pp address 172.16.0.1/32
pp1# pp enable 1
pp1# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel enable 1
tunnel1# ip route 192.168.1.0/24 gateway tunnel 1
tunnel1# ip route default gateway pp 1
tunnel1# ipsec ike pre-shared-key 1 text IKEKEYPASS
tunnel1# ipsec ike remote address 1 any
tunnel1# ipsec ike remote name 1 kyoten1
tunnel1# ipsec ike local address 1 172.16.0.1
tunnel1# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
tunnel1# ipsec auto refresh on
tunnel1# save
```

[ルーター B の設定手順]

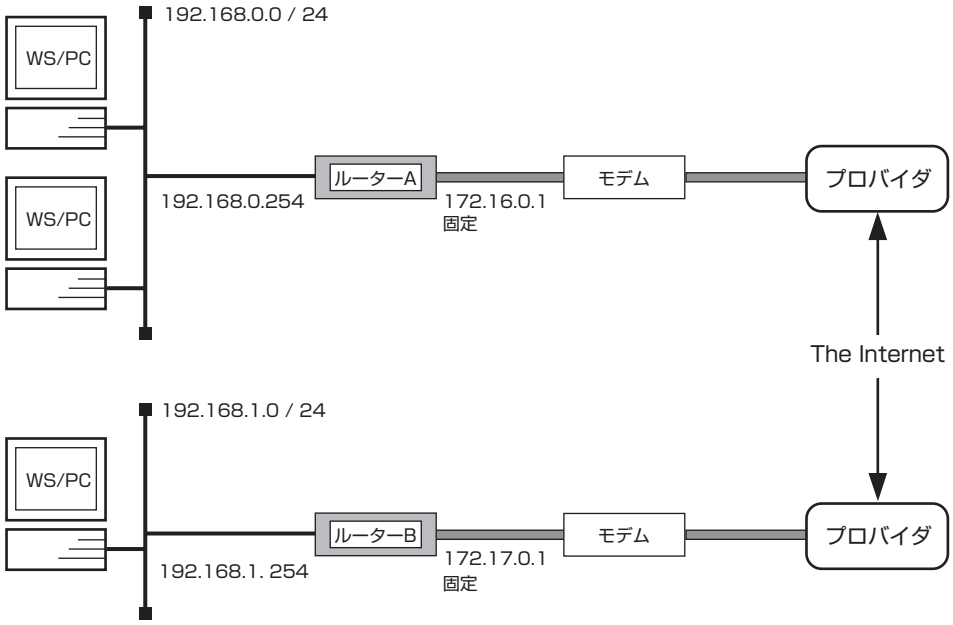
```
# ip lan1 address 192.168.1.254/24
# pp select 1
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# pp always-on on
pp1# ppp ipcp ipaddress on
pp1# ppp ipcp msext on
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
pp1# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel enable 1
tunnel1# ip route 192.168.0.0/24 gateway tunnel 1
tunnel1# ip route default gateway pp 1
tunnel1# ipsec ike local address 1 192.168.1.254
tunnel1# nat descriptor type 1 masquerade
tunnel1# nat descriptor masquerade static 1 1 192.168.1.254 udp 500
tunnel1# nat descriptor masquerade static 1 2 192.168.1.254 esp
tunnel1# ipsec ike local name 1 kyoten1
tunnel1# ipsec ike pre-shared-key 1 text IKEKEYPASS
tunnel1# ipsec ike remote address 1 172.16.0.1
tunnel1# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
tunnel1# ipsec auto refresh on
tunnel1# save
```

[解説]

各拠点では固定 IP アドレスの割り当てを受けていない場合です。センタ（この例ではルーター A）の固定アドレスは前述のケースと同じ（172.16.0.1/32) とします。鍵交換を始めるのは常に拠点側であり、拠点側でトンネルを介した通信が発生した際に鍵交換が行われます。この機能の詳細に関してはダイヤルアップ VPN 機能の仕様を参照ください。

23.3 インターネット接続を併用する場合（固定 IP アドレス使用）

[構成図]



[ルーター A の設定手順]

```
# ip lan1 address 192.168.0.254/24
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ip pp address 172.16.0.1/32
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
pp1# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel enable 1
tunnel1# ip route 192.168.1.0/24 gateway tunnel 1
tunnel1# ip route default gateway pp 1
tunnel1# ipsec ike pre-shared-key 1 text IKEKEYPASS
tunnel1# ipsec ike remote address 1 172.17.0.1
tunnel1# ipsec ike local address 1 192.168.0.254
tunnel1# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
tunnel1# nat descriptor type 1 masquerade
tunnel1# nat descriptor masquerade static 1 1 192.168.0.254 udp 500
tunnel1# nat descriptor masquerade static 1 2 192.168.0.254 esp
tunnel1# nat descriptor address outer 1 172.16.0.1
tunnel1# ipsec auto refresh on
tunnel1# save
```

[ルーター B の設定手順]

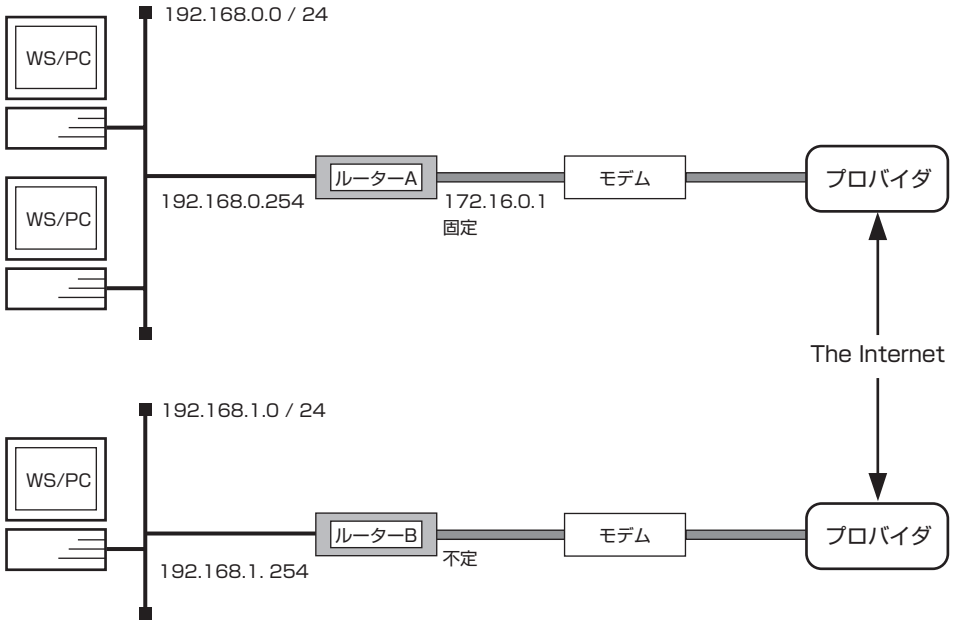
```
# ip lan1 address 192.168.1.254/24
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ip pp address 172.17.0.1/32
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
pp1# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel enable 1
tunnel1# ip route 192.168.0.0/24 gateway tunnel 1
tunnel1# ip route default gateway pp 1
tunnel1# ipsec ike pre-shared-key 1 text IKEKEYPASS
tunnel1# ipsec ike remote address 1 172.16.0.1
tunnel1# ipsec ike local address 1 192.168.1.254
tunnel1# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
tunnel1# nat descriptor type 1 masquerade
tunnel1# nat descriptor masquerade static 1 1 192.168.1.254 udp 500
tunnel1# nat descriptor masquerade static 1 2 192.168.1.254 esp
tunnel1# nat descriptor address outer 1 172.17.0.1
tunnel1# ipsec auto refresh on
tunnel1# save
```

[解説]

「VPN 接続したい拠点がすべて固定 IP アドレスの割り当てを受けている場合」のケースで、センタ及び拠点において VPN 接続の他にインターネット接続も併せて利用したい場合の設定例です。このケースでは NAT 機能を利用します。

23.4 ダイヤルアップ VPN でインターネット接続を併用する場合

[構成図]



[ルーター A の設定手順]

```
# ip lan1 address 192.168.0.254/24
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ip pp address 172.16.0.1/32
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
pp1# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel enable 1
tunnel1# ip route 192.168.1.0/24 gateway tunnel 1
tunnel1# ip route default gateway pp 1
tunnel1# ipsec ike pre-shared-key 1 text IKEKEYPASS
tunnel1# ipsec ike remote address 1 any
tunnel1# ipsec ike local address 1 192.168.0.254
tunnel1# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
tunnel1# ipsec ike remote name 1 kyoten1
tunnel1# nat descriptor type 1 masquerade
tunnel1# nat descriptor masquerade static 1 1 192.168.0.254 udp 500
tunnel1# nat descriptor masquerade static 1 2 192.168.0.254 esp
tunnel1# nat descriptor address outer 1 172.16.0.1
tunnel1# ipsec auto refresh on
tunnel1# save
```

[ルーター B の設定手順]

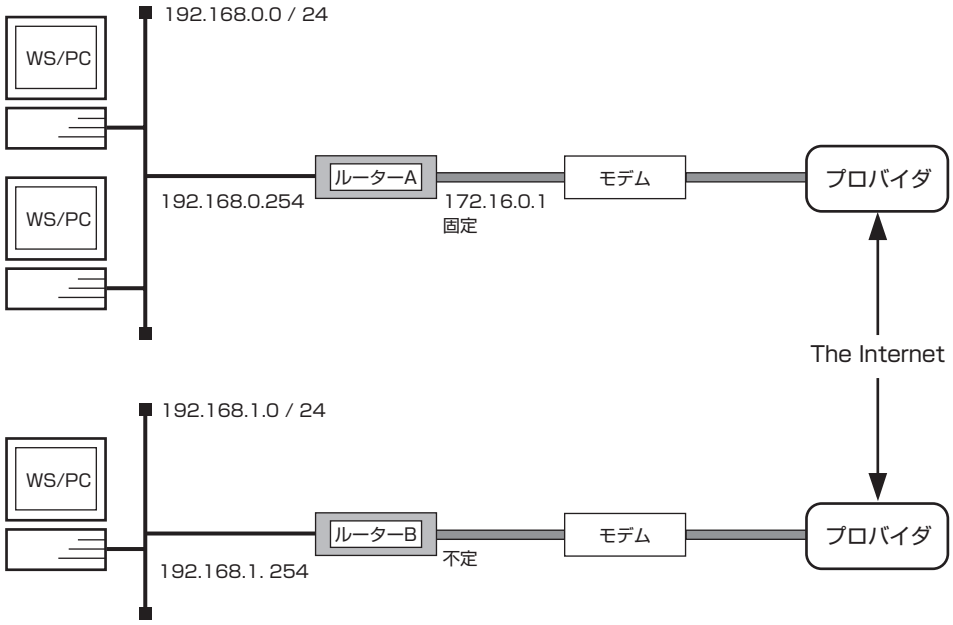
```
# ip lan1 address 192.168.1.254/24
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ppp ipcp ipaddress on
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
pp1# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel enable 1
tunnel1# ip route 192.168.0.0/24 gateway tunnel 1
tunnel1# ip route default gateway pp 1
tunnel1# ipsec ike pre-shared-key 1 text IKEKEYPASS
tunnel1# ipsec ike remote address 1 172.16.0.1
tunnel1# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
tunnel1# ipsec ike local name 1 kyoten1
tunnel1# ipsec ike local address 1 192.168.1.254
tunnel1# nat descriptor type 1 masquerade
tunnel1# nat descriptor masquerade static 1 1 192.168.1.254 udp 500
tunnel1# nat descriptor masquerade static 1 2 192.168.1.254 esp
tunnel1# ipsec auto refresh on
tunnel1# save
```

[解説]

「VPN 環境の中心となる拠点のみが固定 IP アドレスを割り振られている場合」のケースで、センタ及び拠点において VPN 接続の他にインターネット接続も併せて利用したい場合の設定例です。このケースでは NAT 機能を利用します。なお、ダイヤルアップ ＶＰＮ の形態をとりますので、ダイヤルアップ ＶＰＮ の仕様もご確認いただきますようお願いいたします。

23.5 ダイヤルアップ VPN 環境でセンタ側から拠点方向への通信を行いたい場合

[構成図]



・インターネットアクセス無し

[ルーター A の設定手順]

```
# ip lan1 address 192.168.0.254/24
# pp select 1
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# pp always-on on
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ip pp mtu 1454
pp1# ip pp address 172.16.0.1/32
pp1# pp enable 1
pp1# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel enable 1
tunnel1# ip route 192.168.1.0/24 gateway tunnel 1
tunnel1# ip route default gateway pp 1
tunnel1# ipsec ike pre-shared-key 1 text IKEKEYPASS
tunnel1# ipsec ike remote address 1 any
tunnel1# ipsec ike remote name 1 kyoten1
tunnel1# ipsec ike local address 1 172.16.0.1
tunnel1# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
tunnel1# ipsec ike keepalive use 1 on
tunnel1# ipsec auto refresh on
tunnel1# save
```

[ルーター B の設定手順]

```
# ip lan1 address 192.168.1.254/24
# pp select 1
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# pp always-on on
pp1# ppp ipcp ipaddress on
pp1# ppp ipcp msext on
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
pp1# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel enable 1
tunnel1# ip route 192.168.0.0/24 gateway tunnel 1
tunnel1# ip route default gateway pp 1
tunnel1# ipsec ike local address 1 192.168.1.254
tunnel1# nat descriptor type 1 masquerade
tunnel1# nat descriptor masquerade static 1 1 192.168.1.254 udp 500
tunnel1# nat descriptor masquerade static 1 2 192.168.1.254 esp
tunnel1# ipsec ike local name 1 kyoten1
tunnel1# ipsec ike pre-shared-key 1 text IKEKEYPASS
tunnel1# ipsec ike remote address 1 172.16.0.1
tunnel1# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
tunnel1# ipsec ike keepalive use 1 on
tunnel1# ipsec auto refresh on
tunnel1# save
```

[解説]

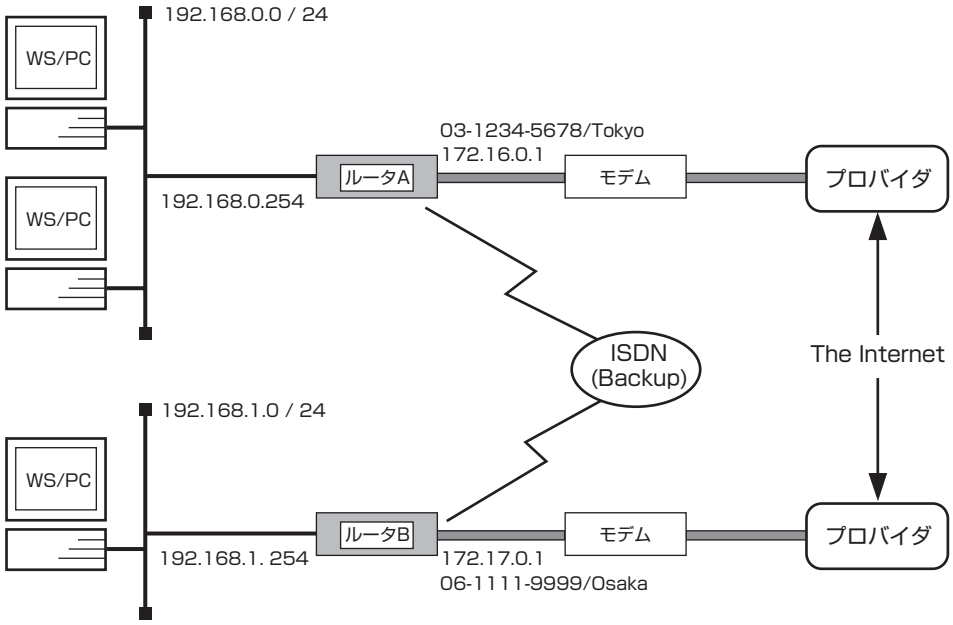
VPN 環境の中心となる拠点のみが固定 IP アドレスを割り振られている場合のケースと同じで、基本的には VPN トンネルを生成するためには拠点側からの通信の発生が必要となります。キープアライブの設定（**ipsec ike keepalive use 1 on**）は本来は VPN トンネルの状態を監視し、何かしらの原因でトンネルが壊れてしまった場合に VPN トンネルを再生成するための設定ですが、この設定をいれることにより拠点は常にセンタ側と接続し続けようとします。従って、拠点・センタ間の VPN トンネルは常に生成されている状態となるため、センタを起点とした拠点方向への通信が可能となることになります。この機能の詳細についてはダイヤルアップ VPN 機能の仕様を参照ください。

24. バックアップ回線による通信断からの自動復旧のための設定例

1. ADSL 回線接続による VPN トンネルの ISDN 回線によるバックアップ
2. VRRP、OSPF による ISDN 回線バックアップ
3. VRRP、RIP による ISDN 回線バックアップ

24.1 ADSL 回線接続による VPN トンネルの ISDN 回線によるバックアップ

[構成図]



[ルーター A の設定手順]

```
# ip lan1 address 192.168.0.254/24
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ip pp address 172.16.0.1/32
pp1# ip pp mtu 1454
pp1# pp enable 1
pp1# isdn local address bri1 03-1234-5678/Tokyo
pp1# pp select 2
pp2# pp bind bri1
pp2# isdn remote address arrive 06-1111-9999/Osaka
pp2# pp enable 2
pp2# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel backup pp 2
tunnel1# tunnel enable 1
tunnel1# ip route 192.168.1.0/24 gateway tunnel 1
tunnel1# ip route 172.17.0.1 gateway pp 1
tunnel1# ipsec auto refresh on
tunnel1# ipsec ike pre-shared-key 1 text IKEKEYPASS
tunnel1# ipsec ike remote address 1 172.17.0.1
tunnel1# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
tunnel1# ipsec ike keepalive use 1 on
tunnel1# save
```

[ルーター B の設定手順]

```
# ip lan1 address 192.168.1.254/24
# pp select 1
pp1# pppoe use lan2
pp1# pp always-on on
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ip pp address 172.17.0.1/32
pp1# ip pp mtu 1454
pp1# pp enable 1
pp1# isdn local address bri1 06-1111-9999/Osaka
pp1# pp select 2
pp2# pp bind bri1
pp2# isdn remote address call 03-1234-5678/Tokyo
pp2# pp enable 2
pp2# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel backup pp 2
tunnel1# tunnel enable 1
tunnel1# ip route 192.168.0.0/24 gateway tunnel 1
tunnel1# ip route 172.16.0.1 gateway pp 1
tunnel1# ipsec auto refresh on
tunnel1# ipsec ike pre-shared-key 1 text IKEKEYPASS
tunnel1# ipsec ike remote address 1 172.16.0.1
tunnel1# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
tunnel1# ipsec ike keepalive use 1 on
tunnel1# save
```

[解説]

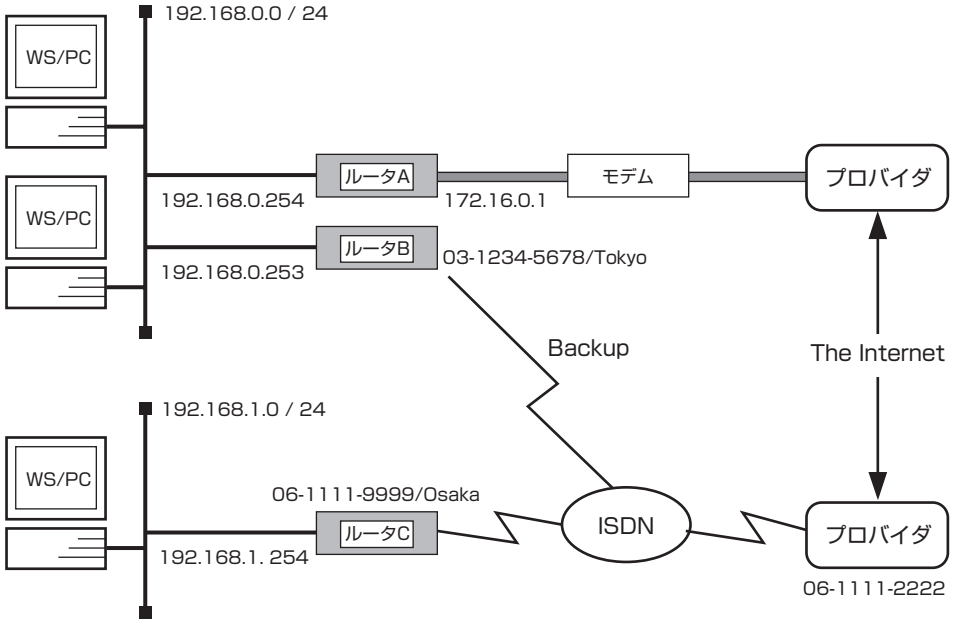
VPN 接続をしたい拠点がすべて固定 IP アドレスの割り当てを受けている場合の例を元にこの設定に対して ISDN 回線によるバックアップの設定を追加します。この設定は WAN 側と LAN 側にそれぞれイーサネットインタフェース、そして BRI インタフェースが必要となりますので、RTX3000、RTX1500、RTX1100、RTX1000、RT300i、RT140e、RT140f の利用を前提とした設定例となります。

-- 注意点 --
気をつけなければいけない点は "keepalive" の設定です。この設定は通信する対向側にも設定されていないと意味がありません。設定する時は ＶＰＮ をはる両側の ＲＴ に対して設定するようにして下さい。この設定により、ADSL 回線経由の VPN トンネルが不通となってから約 1 分程（注）でルーターは VPN 断と判断し ISDN 回線経由で経路を確立します。逆に ADSL 回線経由の経路が復旧すると ISDN 回線の接続を切断し、本来の経路に自動で復旧します。

注）**ipsec ike keepalive use xxxx auto heatbeat xxxx 10 6** コマンドの設定による。

24.2 VRRP、OSPFによる ISDN 回線バックアップ

[構成図]



[ルーター A の設定手順]

```
# ip lan1 address 192.168.0.254/24
# ip lan1 vrrp 1 192.168.0.254 priority=200
# ip lan1 vrrp shutdown trigger 1 pp 1
# pp select 1
pp1# pp keepalive use lcp-echo
pp1# pp keepalive interval 10 3
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ip pp address 172.17.0.1/32
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
pp1# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# ip tunnel ospf area backbone
tunnel1# tunnel enable 1
tunnel1# ip route default gateway pp 1
tunnel1# ip route 192.168.1.0/24 gateway 192.168.0.253
tunnel1# nat descriptor type 1 masquarade
tunnel1# nat descriptor masquerade static 1 1 192.168.0.254 udp 500
tunnel1# nat descriptor masquerade static 1 2 192.168.0.254 esp
tunnel1# ipsec auto refresh on
tunnel1# ipsec ike keepalive use 1 on
tunnel1# ipsec ike local address 1 192.168.0.254
tunnel1# ipsec ike pre-shared-key 1 text IKEKEYPASS
tunnel1# ipsec ike remote address 1 any
tunnel1#  ipsec ike remote name 1 kyoten
tunnel1# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
```

```
tunnel1# ospf use on
tunnel1# ospf preference 10001
tunnel1# ospf router id 192.168.0.254
tunnel1# ospf area backbone
tunnel1# ip lan1 ospf area backbone passive
tunnel1# save
```

[ルーター B の設定手順]

```
# ip lan1 address 192.168.0.253/24
# ip lan1 vrrp 1 192.168.0.254
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 06-1111-9999/Osaka
pp1# pp auth request chap
pp1# pp auth accept chap
pp1# pp auth user name kyoten kyoten
pp1# pp auth myname center center
pp1# pp enable 1
pp1# ip route 192.168.1.0/24 gateway pp 1
pp1# save
```

[ルーター C の設定手順]

```
# ip lan1 address 192.168.1.254/24
# isdn local address bri1 06-1111-9999/Osaka
# pp select 1
pp1# pp bind bri1
pp1# pp always-on on
pp1# isdn remote address call 06-1111-2222
pp1# isdn disconnect time off
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp ipcp ipaddress on
pp1# ip pp nat descriptor 1
pp1# pp enable 1
pp1# pp select 2
pp2# pp bind bri1
pp2# isdn remote address call 03-1234-5678/Tokyo
pp2# pp auth request chap
pp2# pp auth accept chap
pp2# pp auth myname kyoten kyoten
pp2# pp auth user name center center
pp2# pp enable2
pp2# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# ip tunnel ospf area backbone
tunnel1# tunnel enable 1
tunnel1# ip route default gateway pp 1
tunnel1# ip route 192.168.0.0/24 gateway pp 2
tunnel1# nat descriptor type 1 masquarade
tunnel1# nat descriptor masquerade static 1 1 192.168.1.254 udp 500
tunnel1# nat descriptor masquerade static 1 2 192.168.1.254 esp
tunnel1# ipsec auto refresh on
tunnel1# ipsec ike keepalive use 1 on
```

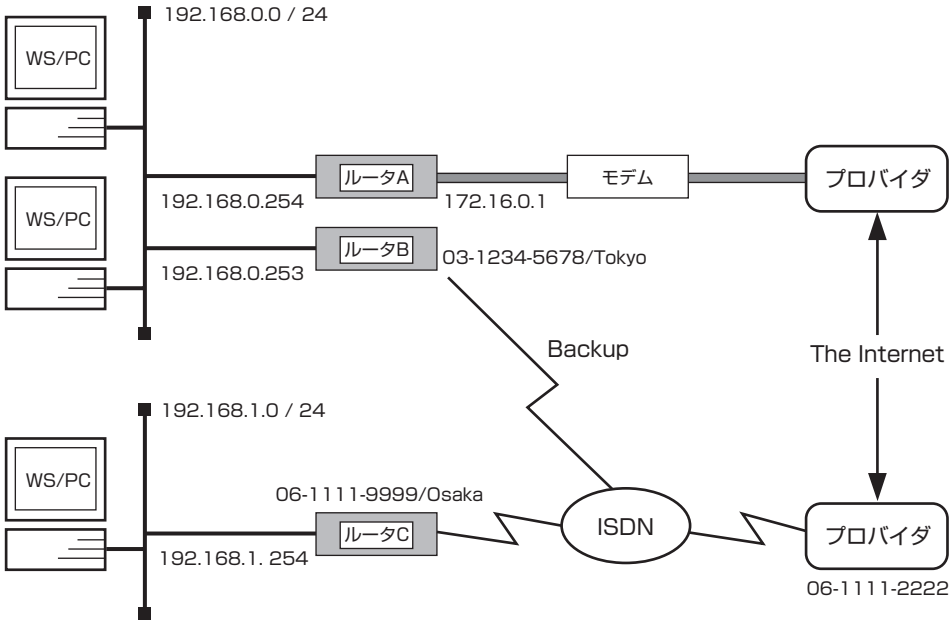
```
tunnel1# ipsec ike local address 1 192.168.1.254
tunnel1# ipsec ike local name 1 kyoten
tunnel1# ipsec ike pre-shared-key 1 text IKEKEYPASS
tunnel1# ipsec ike remote address 1 172.17.0.1
tunnel1# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
tunnel1# ospf use on
tunnel1# ospf preference 10001
tunnel1# ospf router id 192.168.1.254
tunnel1# ospf area backbone
tunnel1# ip lan1 ospf area backbone passive
tunnel1# save
```

[解説]

本設定例では本社側は ADSL 回線で固定アドレスの割り当てを受けてインターネット接続をしていて、拠点は ISDN 常時接続でインターネット接続していると仮定します。本社と拠点の間をインターネット VPN で接続し、かつ ISDN 回線によって本社と拠点の間の通信経路をバックアップします。設定内容について簡単に説明しますと、基本的な経路は本社と拠点を直結する ISDN 回線に向けます。そこで "**ospf preference 10001**" として static な経路より OSPF により導入される経路の優先順位を高くします。(static な経路の優先度は 10000 固定です) そして、接続されたインターネット VPN トンネル内で OSPF で経路のやり取りをするようにすれば、本社側、拠点側ともに OSPF により対向より通知された経路が導入され、優先順位の高いそちらの経路を使って通信することになります。もしインターネット VPN トンネルが切断された場合、OSPF の機能により対向より通知された経路は破棄され、static な経路が有効となります。つまり本社と拠点を結ぶ ISDN 回線です。
ルーター A は WAN 側と LAN 側にそれぞれイーサネットインタフェースが必要となりますので、RTX3000、RTX2000、RTX1500、RTX1100、RTX1000、RT300i、RT140e、RT140f、RT107e、RT105e の利用を前提とした設定例となります。
ルーター B、ルーター C は WAN 側にそれぞれ BRI インタフェースが必要ですので、RTX3000、RTX1500、RTX1100、RTX1000、RT300i、RT140 シリーズ、RT105i の利用を前提としています。

24.3 VRRP、RIP による ISDN 回線バックアップ

[構成図]



[ルーター A の設定手順]

```
# ip lan1 address 192.168.0.254/24
# ip lan1 vrrp 1 192.168.0.254 priority=200
# ip lan1 vrrp shutdown trigger 1 pp 1
# pp select 1
pp1# pp keepalive use lcp-echo
pp1# pp keepalive interval 10 3
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ip pp address 172.17.0.1/32
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# ip pp rip send on
pp1# ip pp rip receive on
pp1# pp enable 1
pp1# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# ip tunnel rip send on
tunnel1# ip tunnel rip receive on
tunnel1# ip tunnel rip filter out 1
tunnel1# tunnel enable 1
tunnel1# ip route default gateway pp 1
tunnel1# ip route 192.168.1.0/24 gateway 192.168.0.253
tunnel1# ip filter 1 pass 192.168.0.0/24
tunnel1# nat descriptor type 1 masquarade
tunnel1# nat descriptor masquerade static 1 1 192.168.0.254 udp 500
tunnel1# nat descriptor masquerade static 1 2 192.168.0.254 esp
tunnel1# ipsec auto refresh on
```

```
tunnel1# ipsec ike keepalive use 1 on
tunnel1# ipsec ike local address 1 192.168.0.254
tunnel1# ipsec ike pre-shared-key 1 text IKEKEYPASS
tunnel1# ipsec ike remote address 1 any
tunnel1# ipsec ike remote name 1 kyoten
tunnel1# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
tunnel1# rip use on
tunnel1# rip preference 10001
tunnel1# save
```

[ルーターB の設定手順]

```
# ip lan1 address 192.168.0.253/24
# ip lan1 vrrp 1 192.168.0.254
# pp select 1
pp1# pp bind bri1
pp1# isdn remote address call 06-1111-9999/Osaka
pp1# pp auth request chap
pp1# pp auth accept chap
pp1# pp auth user name kyoten kyoten
pp1# pp auth myname center center
pp1# pp enable 1
pp1# ip route 192.168.1.0/24 gateway pp 1
pp1# save
```

[ルーターC の設定手順]

```
# ip lan1 address 192.168.1.254/24
# isdn local address bri1 06-1111-9999/Osaka
# pp select 1
pp1# pp bind bri1
pp1# pp always-on on
pp1# isdn remote address call 06-1111-2222
pp1# isdn disconnect time off
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp ipcp ipaddress on
pp1# ip pp nat descriptor 1
pp1# ip pp rip send on
pp1# ip pp rip receive on
pp1# pp enable 1
pp1# pp select 2
pp2# pp bind bri1
pp2# isdn remote address call 03-1234-5678/Tokyo
pp2# pp auth request chap
pp2# pp auth accept chap
pp2# pp auth myname kyoten kyoten
pp2# pp auth user name center center
pp2# pp enable2
pp2# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# ip tunnel rip send on
tunnel1# ip tunnel rip receive on
tunnel1# ip tunnel rip filter out 1
tunnel1# tunnel enable 1
```

```
tunnel1# ip route default gateway pp 1
tunnel1# ip route 192.168.0.0/24 gateway pp 2
tunnel1# ip filter 1 pass 192.168.1.0/24
tunnel1# nat descriptor type 1 masquarade
tunnel1# nat descriptor masquerade static 1 1 192.168.1.254 udp 500
tunnel1# nat descriptor masquerade static 1 2 192.168.1.254 esp
tunnel1# ipsec auto refresh on
tunnel1# ipsec ike keepalive use 1 on
tunnel1# ipsec ike local address 1 192.168.1.254
tunnel1# ipsec ike local name 1 kyoten
tunnel1# ipsec ike pre-shared-key 1 text IKEKEYPASS
tunnel1# ipsec ike remote address 1 172.17.0.1
tunnel1# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
tunnel1# rip use on
tunnel1# rip preference 10001
tunnel1# save
```

[解説]

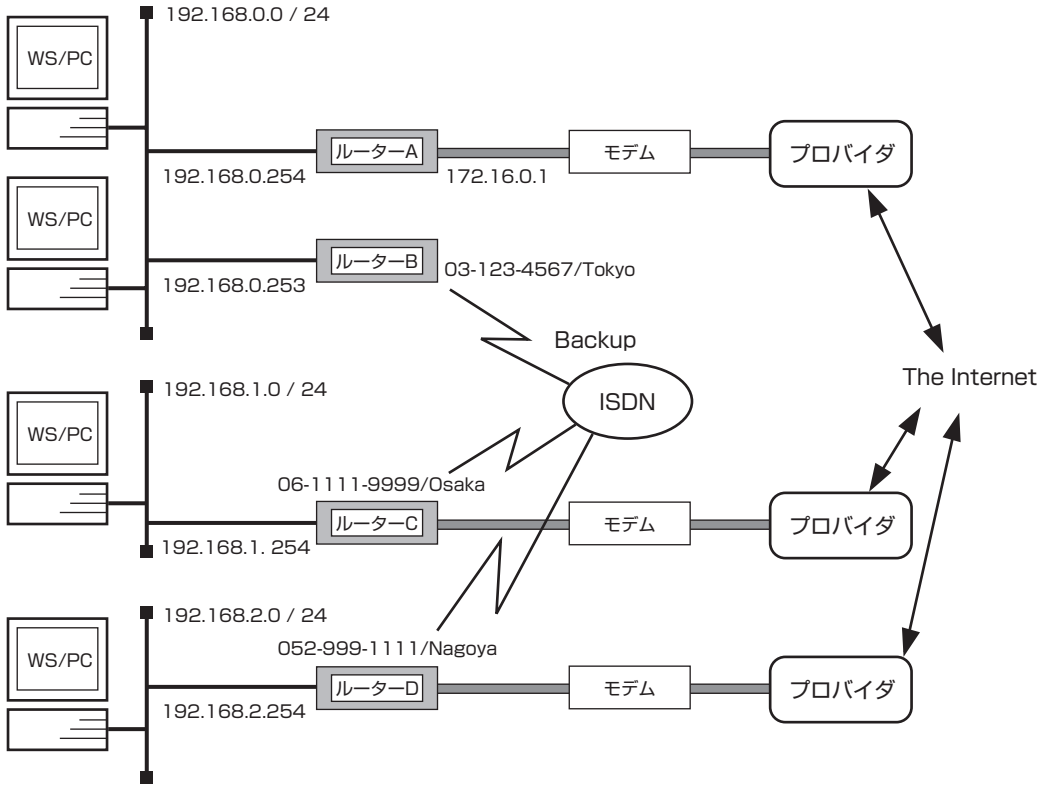
本設定例では本社側は ADSL 回線で固定アドレスの割り当てを受けてインターネット接続をしていて、拠点は ISDN 常時接続でインターネット接続していると仮定します。本社と拠点の間をインターネット VPN で接続し、かつ ISDN 回線によって本社と拠点の間の通信経路をバックアップします。設定内容の説明については「VRRP、OSPF による ISDN 回線バックアップ」の説明の「OSPF」を「RIP」に読み替えるだけです。

ルーター A は WAN 側と LAN 側にそれぞれイーサネットインタフェースが必要となりますので、RTX3000、RTX2000、RTX1500、RTX1100、RTX1000、RT300i、RT107e、RT105e の利用を前提とした設定例となります。

ルーター B、ルーター C は WAN 側にそれぞれ BRI インタフェースが必要ですので、RTX3000、RTX1500、RTX1100、RTX1000、RT300i、RT140 シリーズ、RT105i の利用を前提としています。

24.4 ISDN 回線によるインターネット VPN のバックアップ

[構成図]



[ルーター A の設定手順]

```
# ip lan1 address 192.168.0.254/24
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ip pp address 172.16.0.1/32
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
# ip route default gateway pp 1
# ipsec autorefresh on
# ospf use on
# ospf area backbone
# ospf preference 10001
# ospf router id 192.168.0.254
# ip lan1 ospf area backbone passive
# nat descriptor type 1 masquerade
# nat descriptor masquerade static 1 1 192.168.0.254 udp 500
# nat descriptor masquerade static 1 2 192.168.0.254 esp
# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# ip tunnel ospf area backbone
tunnel1# tunnel enable 1
```

```
# ip route 192.168.1.0/24 gateway 192.168.0.253
# ipsec ike keepalive use 1 on
# ipsec ike local address 1 192.168.0.254
# ipsec ike pre-shared-key 1 text ABC
# ipsec ike remote address 1 any
# ipsec ike remote name 1 kyoten1
# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
tunnel2# tunnel select 2
tunnel2# ipsec tunnel 102
tunnel2# ip tunnel ospf area backbone
tunnel2# tunnel enable 2
# ip route 192.168.2.0/24 gateway 192.168.0.253
# ipsec ike keepalive use 2 on
# ipsec ike local address 2 192.168.0.254
# ipsec ike pre-shared-key 2 text ABC
# ipsec ike remote address 2 any
# ipsec ike remote name 2 kyoten2
# ipsec sa policy 102 2 esp 3des-cbc md5-hmac
```

[ルーター B の設定手順]

```
# ip lan1 address 192.168.0.253/24
# isdn local address bri1 03-1234-5678/Tokyo
# pp select anonymous
anonymous# pp bind bri1
anonymous# pp auth request chap
anonymous# pp auth username kyoten1 kyoten1 06-1111-9999/Osaka
anonymous# pp auth username kyoten2 kyoten2 052-999-1111/Nagoya
anonymous# pp enable anonymous
# ip route 192.168.1.0/24 gateway pp anonymous name=kyoten1
# ip route 192.168.2.0/24 gateway pp anonymous name=kyoten2
```

[ルーター C の設定手順]

```
# ip lan1 address 192.168.1.254/24
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ppp ipcp ipaddress on
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
# isdn local address bri1 06-1111-9999/Osaka
# pp select 2
pp2# pp bind bri1
pp2# isdn remote address call 03-123-4567/Tokyo
pp2# pp auth accept chap
pp2# pp auth myname kyoten1 kyoten1
pp2# pp enable 2
```

```
# ip route default gateway pp 1
# ip route 192.168.0.0/24 gateway pp 2
# ospf user on
# ospf area backbone
# ospf preference 10001
# ospf router id 192.168.1.254
# ip lan1 ospf area backbone passive
# nat descriptor type 1 masquerade
# nat descriptor masquerade static 1 1 192.168.1.254 udp 500
# nat descriptor masquerade static 1 2 192.168.1.254 esp
# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# ip tunnel ospf area backbone
tunnel1# tunnel enable 1
# ipsec autorefresh on
# ipsec ike keepalive use 1 on
# ipsec ike local address 1 192.168.1.254
# ipsec ike local name 1 kyoten1
# ipsec ike pre-shared-key 1 text ABC
# ipsec ike remote address 1 172.16.0.1
# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
```

[ルーター D の設定手順]

```
# ip lan1 address 192.168.2.254/24
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ppp ipcp ipaddress on
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
# isdn local address bri1 052-999-1111/Nagoya
# pp select 2
pp2# pp bind bri1
pp2# isdn remote address call 03-123-4567/Tokyo
pp2# pp auth accept chap
pp2# pp auth myname kyoten2 kyoten2
pp2# pp enable 2
# ip route default gateway pp 1
# ip route 192.168.0.0/24 gateway pp 2
# ospf user on
# ospf area backbone
# ospf preference 10001
# ospf router id 192.168.2.254
# ip lan1 ospf area backbone passive
# nat descriptor type 1 masquerade
# nat descriptor masquerade static 1 1 192.168.2.254 udp 500
# nat descriptor masquerade static 1 2 192.168.2.254 esp
# tunnel select 1
```

```
tunnel1# ipsec tunnel 101
tunnel1# ip tunnel ospf area backbone
tunnel1# tunnel enable 1
# ipsec autorefresh on
# ipsec ike keepalive use 1 on
# ipsec ike local address 1 192.168.2.254
# ipsec ike local name 1 kyoten2
# ipsec ike pre-shared-key 1 text ABC
# ipsec ike remote address 1 172.16.0.1
# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
```

[解説]

センター、拠点共に ADSL 回線にてプロバイダと PPPoE 接続しており、センター側は固定のアドレス割り当てを受けているものとします。

通常運用時はインターネット VPN 通信を行っているとします。

センター側ルーター A では、拠点方向への static 経路はバックアップ回線側ルーターであるルーター B に向けます。拠点側ではセンター方向への static 経路は ISDN 回線方向に向けます。設定上の経路はバックアップ回線を使用するように設定し、OSPF による経路導入との連係で拠点間通信を冗長化します。

例えば、拠点 2 とインターネットを結ぶ回線がダウンしたとします。するとルーター D は自動的に ISDN 回線を通してセンターのルーター B と接続を試みます。

このケースのように拠点側で回線障害が発生し、VPN トンネルが不通となると、設定された OSPF による経路情報のやりとりも停止します。これにより OSPF で学習した経路情報がルーターの経路テーブルより削除されることになります。(デフォルトの設定ならば回線断から最大で 40 秒程で削除されます)　OSPF により学習された経路情報が消えるということは static に設定した対向側への経路 (ISDN 回線側に向けた経路です) が用いられるようになります。つまり、バックアップ経路である ISDN 回線を通した通信が始まることになります。

バックアップからの復旧については、メイン回線での VPN トンネルの復旧とともに OSPF による経路情報を受けるようになれば、自動的に通信経路が切り替わり正常運用に戻ります。

センター側のメインルーターであるルーター A とインターネットを結ぶ回線がダウンした場合には、拠点 1、拠点 2 ともにバックアップ側へ切り替わります。

拠点にて回線障害発生の時と動作は同じです。VPN トンネル断により OSPF 経路情報が削除されることでバックアップ経路に切り替わります。バックアップからの復旧についても拠点にて回線障害発生と同じです。

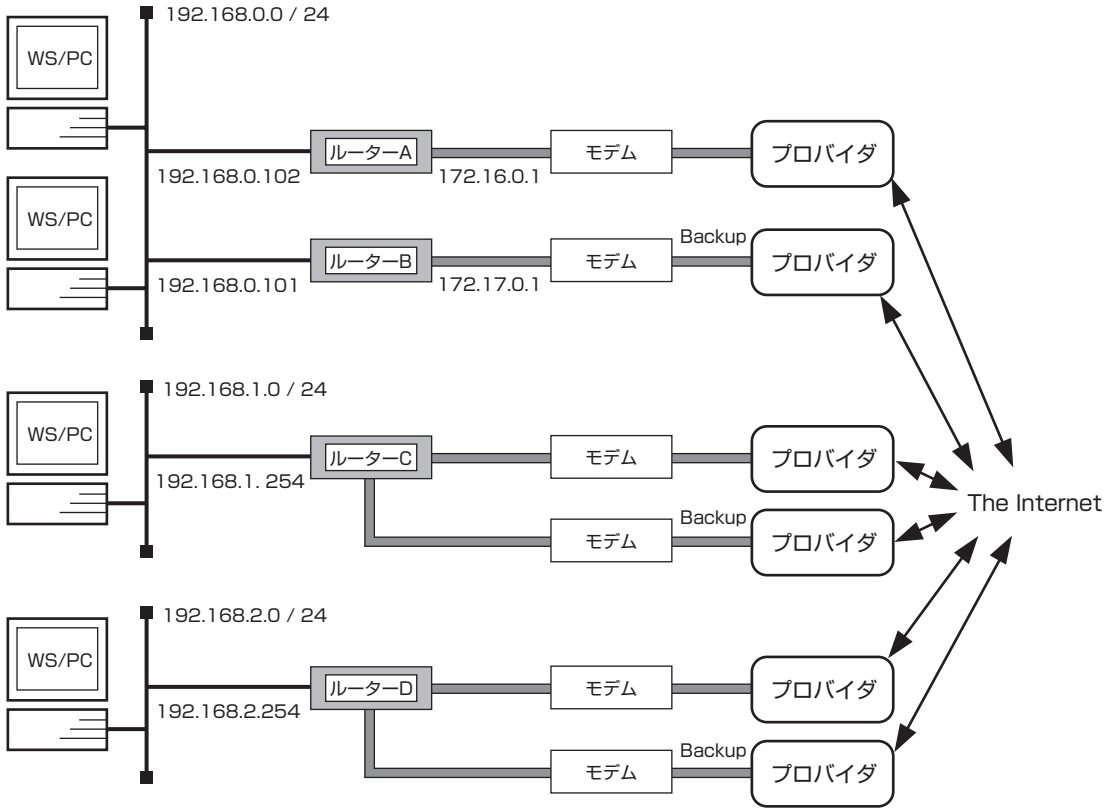
ルーター A は RTX3000、RTX2000、RTX1500、RTX1100、RTX1000、RT300i、RT107e の利用を前提とした設定例となります。

ルーター B は RTX3000、RTX1500、RTX1100、RTX1000、RT300i、RT250i の利用を前提とした設定例となります。

ルーター C、ルーター D は RTX3000、RTX1500、RTX1100、RTX1000 の利用を前提とした設定例となります。

24.5 インターネット VPN によるインターネット VPN のバックアップ

[構成図]



[ルーター A の設定手順]

```
# ip lan1 address 192.168.0.102/24
# ip lan1 vrrp 1 192.168.0.100 priority=200
# ip lan1 vrrp shutdown trigger 1 pp 1
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ip pp address 172.16.0.1/32
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
# ip route default gateway pp 1
# ipsec autorefresh on
# ospf use on
# ospf area backbone
# ospf preference 10001
# ospf router id 192.168.0.102
# ip lan1 ospf area backbone passive
# nat descriptor type 1 masquerade
# nat descriptor masquerade static 1 1 192.168.0.102 udp 500
# nat descriptor masquerade static 1 2 192.168.0.102 esp
# tunnel select 1
```

```
tunnel1# ipsec tunnel 101
tunnel1# ip tunnel ospf area backbone
tunnel1# tunnel enable 1
# ip route 192.168.1.0/24 gateway 192.168.0.101
# ipsec ike keepalive use 1 on
# ipsec ike local address 1 192.168.0.102
# ipsec ike pre-shared-key 1 text ABC
# ipsec ike remote address 1 any
# ipsec ike remote name 1 kyoten1-1
# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
# tunnel select 2
tunnel2# ipsec tunnel 102
tunnel2# ip tunnel ospf area backbone
tunnel2# tunnel enable 2
# ip route 192.168.2.0/24 gateway 192.168.0.101
# ipsec ike keepalive use 2 on
# ipsec ike local address 2 192.168.0.102
# ipsec ike pre-shared-key 2 text ABC
# ipsec ike remote address 2 any
# ipsec ike remote name 2 kyoten2-1
# ipsec sa policy 102 2 esp 3des-cbc md5-hmac
```

[ルーター B の設定手順]

```
# ip lan1 address 192.168.0.101/24
# ip lan1 vrrp 1 192.168.0.100 priority=100
# pp select 1
# pp always-on on
# pppoe use lan2
# pp auth accept pap chap
# pp auth myname ID PASSWORD
# ppp lcp mru on 1454
# ppp ccp type none
# ip pp address 172.17.0.1/32
# ip pp mtu 1454
# ip pp nat descriptor 1
# pp enable 1
# ip route default gateway pp 1
# ipsec autorefresh on
# nat descriptor type 1 masquerade
# nat descriptor masquerade static 1 1 192.168.0.101 udp 500
# nat descriptor masquerade static 1 2 192.168.0.101 esp
# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel enable 1
# ip route 192.168.1.0/24 gateway tunnel 1
# ipsec ike keepalive use 1 on
# ipsec ike local address 1 192.168.0.101
# ipsec ike pre-shared-key 1 text ABC
# ipsec ike remote address 1 any
# ipsec ike remote name 1 kyoten1-2
# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
# tunnel select 2
tunnel2# ipsec tunnel 102
```

```
tunnel2# tunnel enable 2
# ip route 192.168.2.0/24 gateway tunnel 2
# ipsec ike keepalive use 2 on
# ipsec ike local address 2 192.168.0.101
# ipsec ike pre-shared-key 2 text ABC
# ipsec ike remote address 2 any
# ipsec ike remote name 2 kyoten2-2
# ipsec sa policy 102 2 esp 3des-cbc md5-hmac
```

[ルーター C の設定手順]

```
#  ip route default gateway pp 1
# ip lan1 address 192.168.1.254/24
# pp select 1
pp1# pp backup pp 2
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ppp ipcp ipaddress on
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
# pp select 2
pp2# pppoe use lan3
pp2# pp auth accept pap chap
pp2# pp auth myname ID PASSWORD
pp2# ppp lcp mru on 1454
pp2# ppp ccp type none
vppp ipcp ipaddress on
pp2# ip pp mtu 1454
pp2# ip pp nat descriptor 1
pp2# pp enable 2
# ipsec autorefresh on
# ip route default gateway pp 1
# ip route 192.168.0.0/24 gateway tunnel 2
# ospf use on
# ospf area backbone
# ospf preference 10001
# ospf router id 192.168.1.254
# ip lan1 ospf area backbone passive
# nat descriptor type 1 masquerade
# nat descriptor masquerade static 1 1 192.168.1.254 udp 500
# nat descriptor masquerade static 1 2 192.168.1.254 esp
# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# ip tunnel ospf area backbone
tunnel1# tunnel enable 1
# ipsec ike keepalive use 1 on
# ipsec ike local address 1 192.168.1.254
# ipsec ike local name 1 kyoten1-1
# ipsec ike pre-shared-key 1 text ABC
```

```
# ipsec ike remote address 1 172.16.0.1
# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
# tunnel select 2
tunnel2# ipsec tunnel 102
tunnel2# tunnel enable 2
# ipsec ike keepalive use 2 on
# ipsec ike local address 2 192.168.1.254
# ipsec ike local name 2 kyoten1-2
# ipsec ike pre-shared-key 2 text ABC
# ipsec ike remote address 2 172.17.0.1
# ipsec sa policy 102 2 esp 3des-cbc md5-hmac
```

[ルーター D の設定手順]

```
# ip lan1 address 192.168.2.254/24
# pp select 1
pp1# pp backup pp 2
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ppp ipcp ipaddress on
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
# pp select 2
pp2# pppoe use lan3
pp2# pp auth accept pap chap
pp2# pp auth myname ID PASSWORD
pp2# ppp lcp mru on 1454
pp2# ppp ccp type none
pp2# ppp ipcp ipaddress on
pp2# ip pp mtu 1454
pp2# ip pp nat descriptor 1
pp2# pp enable 2
# ipsec autorefresh on
# ip route default gateway pp 1
# ip route 192.168.0.0/24 gateway tunnel 2
# ospf use on
# ospf area backbone
# ospf preference 10001
# ospf router id 192.168.2.254
# ip lan1 ospf area backbone passive
# nat descriptor type 1 masquerade
# nat descriptor masquerade static 1 1 192.168.2.254 udp 500
# nat descriptor masquerade static 1 2 192.168.2.254 esp
# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# ip tunnel ospf area backbone
tunnel1# tunnel enable 1
# ipsec ike keepalive use 1 on
# ipsec ike local address 1 192.168.2.254
```

```
# ipsec ike local name 1 kyoten2-1
# ipsec ike pre-shared-key 1 text ABC
# ipsec ike remote address 1 172.16.0.1
# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
# tunnel select 2
tunnel2# ipsec tunnel 102
tunnel2# tunnel enable 2
# ipsec ike keepalive use 2 on
# ipsec ike local address 2 192.168.2.254
# ipsec ike local name 2 kyoten2-2
# ipsec ike pre-shared-key 2 text ABC
# ipsec ike remote address 2 172.17.0.1
# ipsec sa policy 102 2 esp 3des-cbc md5-hmac
```

[解説]

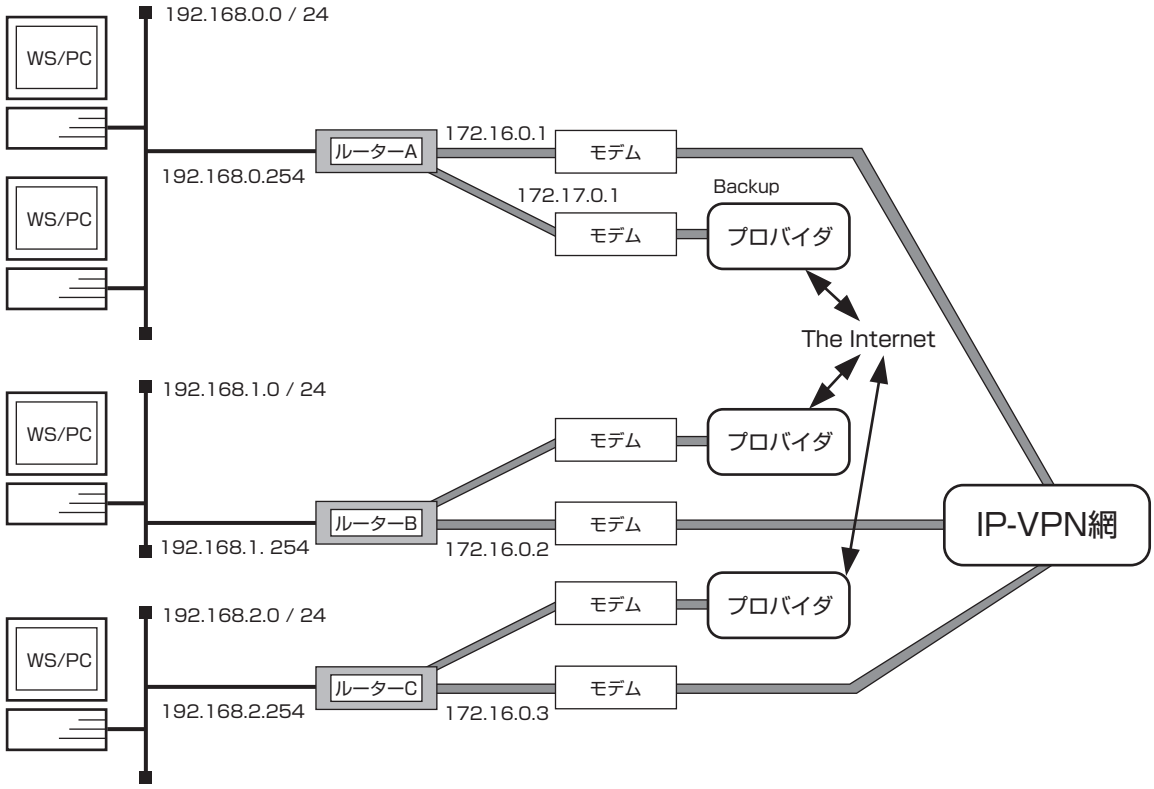
センター、拠点共に ADSL 回線にてプロバイダと PPPoE 接続を 2 本確保しており、センター側はメイン回線、バックアップ回線ともに固定のアドレス割り当てを受けているものとします。
通常運用時はメイン回線インターネット VPN 通信を行っているとします。
センターでは機器障害、回線障害に備えて、2 台のルーターによる VRRP 構成をとっています。これにより、ルーター A もしくはメイン回線に障害が発生すると自動的に外部との接続はルーター B が行うようになります。拠点側では回線障害に備えて、2 本の別々の回線を通してインターネット接続を設定しています。メイン回線障害発生時には自動的にバックアップ回線に切り替わり、インターネット接続および VPN 接続を行います。センターと拠点の間の VPN トンネルは拠点毎に 2 本ずつつながっています。拠点 1 を例にとればルーター A- ルーター C 間とルーター B- ルーター C 間に VPN トンネルがつながっています。(同時に使用されることはありません)
例えば、拠点 2 とインターネットを結ぶメイン回線がダウンしたとします。するとルーター D は自動的にバックアップ回線を通してセンターのルーター A と接続を試みます。
拠点側ではメイン回線で障害発生を検知し、バックアップ回線によるインターネット接続に切り替わります。この際、VPN トンネルも一時的に切断されることになりますが、バックアップ回線によるインターネット接続確立後に再度センターとの間にトンネルが生成されます。メイン回線が復旧するとインターネットへの接続はバックアップ回線からメイン回線に戻ることになります。この時 VPN トンネルも一旦切断されることになりますが、すぐに復旧したメイン回線を通してセンターと再接続され、正常運用に戻ります。
センター側のメインルーターであるルーター A で障害が発生した場合には、拠点 1、拠点 2 ともにセンターとの通信をセンターのバックアップルーターであるルーター B との VPN に切替えます。
センターではルーター A がダウンすることにより、VRRP 設定されているルーター B が自動的にバックアップ動作を開始します。拠点側ではセンター側のルーター A との VPN トンネルが切断されることにより OSPF により通知されていたセンターへの経路が経路テーブルより削除されます。すると、static に設定していたバックアップトンネルへの経路が使用されるようになります。つまりセンターとの通信にはルーター B との VPN トンネルを使用するようになります。センターのメインルーター（ルーター A）が復旧すれば、ルーター B は再び待機状態に戻ります。拠点側もルーター A との間の VPN トンネルが復旧すれば OSPF による経路導入がなされ、センターとの通信にメイントンネルを使用するようになり、正常運用に戻ります。

本設定例では拠点数は 2 としていますが、設定例内の拠点に関する設定を増やすことで複数の拠点との VPN 通信をバックアップする設定を行うことが可能です。

ルーター A、ルーター B は RTX3000、RTX2000、RTX1500、RTX1100、RTX1000、RT300i、RT107e の利用を前提とした設定例となります。
ルーター C、ルーター D は RTX3000、RTX1500、RTX1100、RTX1000 の利用を前提とした設定例となります。

24.6 インターネット VPN による IP-VPN のバックアップ

[構成図]



[ルーター A の設定手順]

```
# ip lan1 address 192.168.0.254/24
# pp select1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ipcp msext on
pp1# ip pp address 172.16.0.1/32
pp1# ip pp mtu 1454
pp1# pp enable 1
# pp select 2
pp2# pp always-on on
pp2# pppoe use lan2
pp2# pp auth accept pap chap
pp2# pp auth myname ID PASSWORD
pp2# ppp lcp mru on 1454
pp2# ppp ipcp msext on
pp2# ip pp address 172.17.0.1/32
pp2# ip pp mtu 1454
pp2# ip pp nat descriptor 1
pp2# pp enable 2
# bgp use on
# bgp autonomous-system 64001
# bgp neighbor 1 8000 172.16.0.2
# bgp preference 10001
```

```
# bgp import filter 1 include all
# bgp import 8000 statuc filter 1
# bgp export filter 1 include all
# bgp export 8000 filter 1
# nat descriptor type 1 masquerade
# nat descriptor masquerade static 1 1 192.168.0.254 udp 500
# nat descriptor masquerade static 1 2 192.168.0.254 esp
# ip route default gateway pp 2
# ipsec autorefresh on
# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel enable 1
# ip route 192.168.1.0/24 gateway tunnel 1
# ipsec ike keepalive use 1 on
# ipsec ike local address 1 192.168.0.254
# ipsec ike pre-shared-key 1 text ABC
# ipsec ike remote address 1 any
# ipsec ike remote name 1 kyoten1
# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
# tunnel select 2
tunnel2# ipsec tunnel 102
tunnel2# tunnel enable 2
# ip route 192.168.2.0/24 gateway tunnel 2
# ipsec ike keepalive use 2 on
# ipsec ike local address 2 192.168.0.254
# ipsec ike pre-shared-key 2 text ABC
# ipsec ike remote address 2 any
# ipsec ike remote name 2 kyoten2
# ipsec sa policy 102 2 esp 3des-cbc md5-hmac
```

[ルーターB の設定手順]

```
# ip lan1 address 192.168.1.254/24
# pp select1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ipcp msext on
pp1# ip pp address 172.16.0.2/32
pp1# ip pp mtu 1454
pp1# pp enable 1
# pp select 2
pp2# pp always-on on
pp2# pppoe use lan2
pp2# pp auth accept pap chap
pp2# pp auth myname ID PASSWORD
pp2# ppp lcp mru on 1454
pp2# ppp ipcp msext on
pp2# ppp ipcp ipaddress on
pp2# ip pp mtu 1454
pp2# ip pp nat descriptor 1
pp2# pp enable 1
```

```
# bgp use on
# bgp autonomous-system 8000
# bgp neighbor 1 64001 172.16.0.1
# bgp preference 10001
# bgp import filter 1 include all
# bgp import 64001 statuc filter 1
# bgp export filter 1 include all
# bgp export 64001 filter 1
# nat descriptor type 1 masquerade
# nat descriptor masquerade static 1 1 192.168.1.254 udp 500
# nat descriptor masquerade static 1 2 192.168.1.254 esp
# ip route default gateway pp 2
# ip route 192.168.0.0/24 gateway tunnel 1
# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel enable 1
# ipsec autorefresh on
# ipsec ike keepalive use 1 on
# ipsec ike local address 1 192.168.1.254
# ipsec ike local name 1 kyoten1
# ipsec ike pre-shared-key 1 text ABC
# ipsec ike remote address 1 172.17.0.1
# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
```

[ルーター C の設定手順]

```
# ip lan1 address 192.168.2.254/24
# pp select1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ipcp msext on
pp1# ip pp address 172.16.0.3/32
pp1# ip pp mtu 1454
pp1# pp enable 1
# pp select 2
pp2# pp always-on on
pp2# pppoe use lan2
pp2# pp auth accept pap chap
pp2# pp auth myname ID PASSWORD
pp2# ppp lcp mru on 1454
pp2# ppp ccp type none
pp2# ppp ipcp ipaddress on
pp2# ip pp mtu 1454
pp2# ip pp nat descriptor 1
pp2# pp enable 1
# bgp use on
# bgp autonomous-system 8000
# bgp neighbor 1 64001 172.16.0.1
# bgp preference 10001
# bgp import filter 1 include all
# bgp import 64001 statuc filter 1
```

```
# bgp export filter 1 include all
# bgp export 64001 filter 1
# nat descriptor type 1 masquerade
# nat descriptor masquerade static 1 1 192.168.2.254 udp 500
# nat descriptor masquerade static 1 2 192.168.2.254 esp
# ip route default gateway pp 2
# ip route 192.168.0.0/24 gateway tunnel 1
# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel enable 1
# ipsec autorefresh on
# ipsec ike keepalive use 1 on
# ipsec ike local address 1 192.168.2.254
# ipsec ike local name 1 kyoten2
# ipsec ike pre-shared-key 1 text ABC
# ipsec ike remote address 1 172.17.0.1
# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
```

[解説]

センター、拠点共に ADSL 回線にてプロバイダと PPPoE 接続を確保しており、センター側は固定のアドレス割り当てを受けているものとします。

本設定例では、IP-VPN 網との接続方法とし ADSL 回線を使用しています。

通常運用時は IP-VPN 通信を行っているとします。

センター側では、拠点への経路はバックアップ回線となるインターネット側の VPN トンネルに static に設定します。拠点側でもセンター方向への経路はインターネット接続側の VPN トンネルに static に設定します。設定上の経路はバックアップ回線を使用するように設定し、BGP による経路導入との連係で拠点間通信を冗長化します。

例えば、拠点 2 と IP-VPN 網を結ぶ回線がダウンしたとします。するとルーター C は自動的にセンターとの通信を IP-VPN 接続からインターネット VPN 接続による方法に切り替えます。

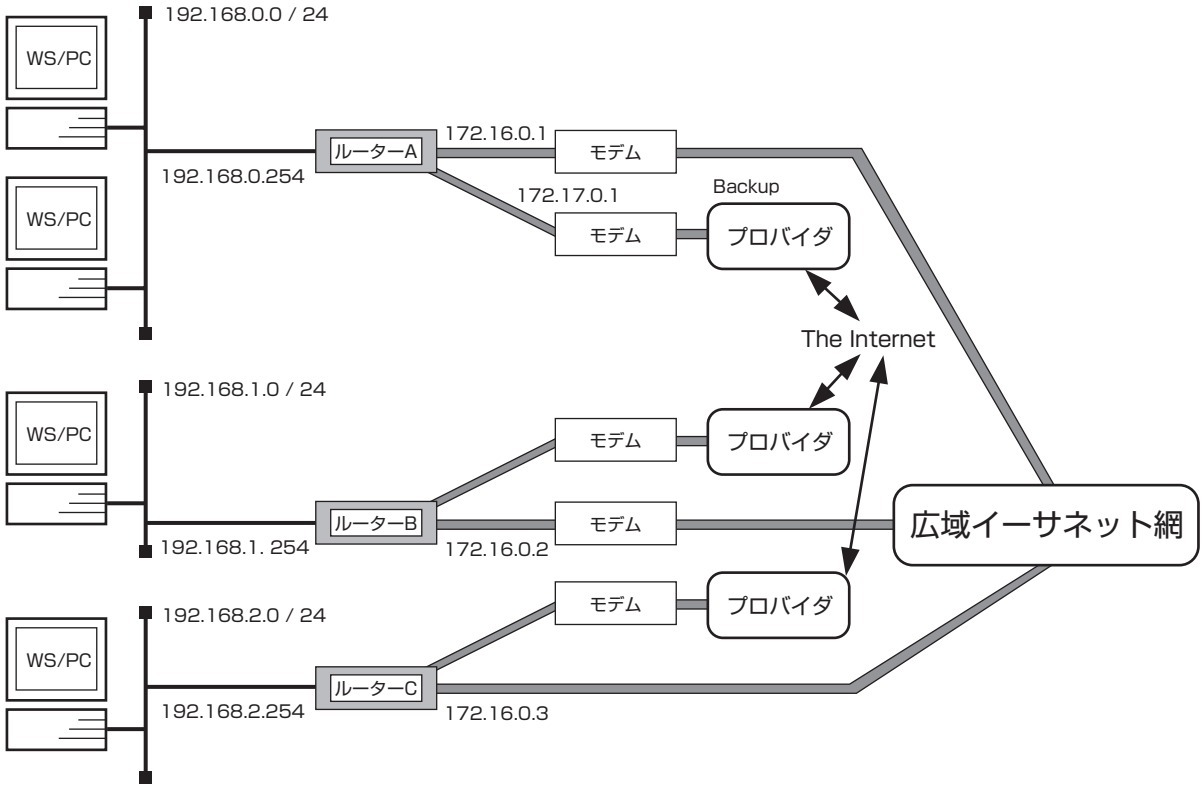
IP-VPN 網とのアクセス回線で障害が発生することにより、IP-VPN 網との BGP のセッションが切れます。これにより、BGP にて導入されていたセンターへの経路情報がルーター C より失われ、static に設定されていたインターネット VPN を通したセンターへの通信経路が有効となります。バックアップ回線からの復旧については、IP-VPN 網との接続が復旧することで、BGP による経路を再度導入します。これによりセンターへの通信経路は再び IP-VPN 網経由のものとなり、正常運用状態に戻ります。

本設定例では拠点数は 2 としていますが、設定例内の拠点に関する設定を増やすことで複数の拠点との VPN 通信をバックアップする設定を行うことが可能です。

RTX3000、RTX2000、RTX1500、RTX1100、RTX1000、RT300i の利用を前提とした設定例となります。

24.7 インターネット VPN による広域イーサネットのバックアップ

[構成図]



[ルーター A の設定手順]

```
# ip lan1 address 192.168.0.254/24
# ip lan2 address 172.16.0.1/24
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan3
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ip pp address 172.17.0.1/32
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
# ospf use on
# ospf preference 10001
# ospf router id 192.168.0.254
# ospf area backbone
# ip lan1 ospf area backbone passive
# ip lan2 ospf area backbone
# nat descriptor type 1 masquerade
# nat descriptor masquerade static 1 1 192.168.0.254 udp 500
# nat descriptor masquerade static 1 2 192.168.0.254 esp
# ip route default gateway pp 1
# ipsec autorefresh on
# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel enable 1
```

```
# ip route 192.168.1.0/24 gateway tunnel 1
# ipsec ike keepalive use 1 on
# ipsec ike local address 1 192.168.0.254
# ipsec ike pre-shared-key 1 text ABC
# ipsec ike remote address 1 any
# ipsec ike remote name 1 kyoten1
# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
# tunnel select 2
tunnel2# ipsec tunnel 102
tunnel2# tunnel enable 2
# ip route 192.168.2.0/24 gateway tunnel 2
# ipsec ike keepalive use 2 on
# ipsec ike local address 2 192.168.0.254
# ipsec ike pre-shared-key 2 text ABC
# ipsec ike remote address 2 any
# ipsec ike remote name 2 kyoten2
# ipsec sa policy 102 2 esp 3des-cbc md5-hmac
```

[ルーターB の設定手順]

```
# ip lan1 address 192.168.1.254/24
# ip lan2 address 172.16.0.2
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ppp ipcp ipaddress on
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
# ospf use on
# ospf router id 192.168.1.254
# ospf preference 10001
# ospf area backbone
# ip lan1 ospf area backbone passive
# ip lan2 ospf area backbone
# nat descriptor type 1 masquerade
# nat descriptor masquerade static 1 1 192.168.1.254 udp 500
# nat descriptor masquerade static 1 2 192.168.1.254 esp
# ip route default gateway pp 1
# ip route 192.168.0.0/24 gateway tunnel 1
# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel enable 1
# ipsec autorefresh on
# ipsec ike keepalive use 1 on
# ipsec ike local address 1 192.168.1.254
# ipsec ike local name 1 kyoten1
# ipsec ike pre-shared-key 1 text ABC
# ipsec ike remote address 1 172.17.0.1
# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
```

[ルーター C の設定手順]

```
# ip lan1 address 192.168.2.254/24
# ip lan2 address 172.16.0.3
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan3
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ppp ipcp ipaddress on
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
# ospf use on
# ospf router id 192.168.2.254
# ospf preference 10001
# ospf area backbone
# ip lan1 ospf area backbone passive
# ip lan2 ospf area backbone
# nat descriptor type 1 masquerade
# nat descriptor masquerade static 1 1 192.168.2.254 udp 500
# nat descriptor masquerade static 1 2 192.168.2.254 esp
# ip route default gateway pp 1
# ip route 192.168.0.0/24 gateway tunnel 1
# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel enable 1
# ipsec autorefresh on
# ipsec ike keepalive use 1 on
# ipsec ike local address 1 192.168.2.254
# ipsec ike local name 1 kyoten2
# ipsec ike pre-shared-key 1 text ABC
# ipsec ike remote address 1 172.17.0.1
# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
```

[解説]

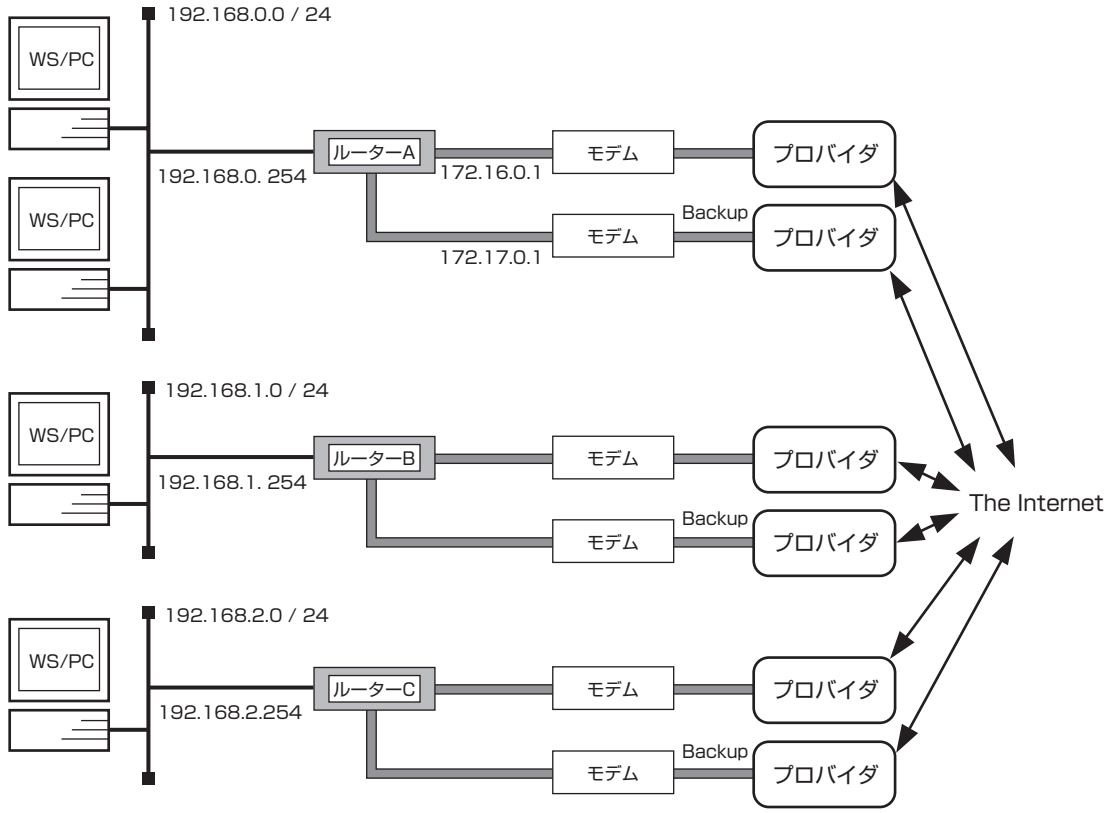
センター、拠点共に ADSL 回線にてプロバイダと PPPoE 接続をしており、センター側は固定のアドレス割り当てを受けているものとします。
通常運用時は広域イーサネットによる通信を行っているとします。
センター側では、拠点への経路はバックアップ回線となるインターネット側の VPN トンネルに static に設定します。拠点側でもセンター方向への経路はインターネット接続側の VPN トンネルに static に設定します。設定上の経路はバックアップ回線を使用するように設定し、OSPF による経路導入との連係で拠点間通信を冗長化します。
例えば、拠点 2 と広域イーサネット網を結ぶ回線がダウンしたとします。ルーター C は自動的にセンターとの通信路を広域イーサネット接続からインターネット VPN 接続による方法に切り替えます。
広域イーサネットとのアクセス回線で障害が発生することにより、OSPF による経路情報のやりとりが不能となります。これにより OSPF で導入されていた経路情報がルーター C より削除され、static に設定されていたインターネット VPN 経路が有効となります。バックアップ回線からの復旧については、広域イーサネットとの接続が復旧することで、OSPF による経路を再度導入します。これによりセンターへの通信経路は再び広域イーサネット経由のものとなり、正常運用状態に戻ります。

本設定例では拠点数は 2 としていますが、設定例内の拠点に関する設定を増やすことで複数の拠点との VPN 通信をバックアップする設定を行うことが可能です。

RTX3000、RTX2000、RTX1500、RTX1100、RTX1000、RT300i の利用を前提とした設定例となります。

24.8 インターネット VPN によるインターネット VPN のバックアップ（センタールーターを 1 台で構成）

[構成図]



[ルーター A の設定手順]

```
# ip lan1 address 192.168.0.254/24
# pp select 1
pp1# pp backup pp 2
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ip pp address 172.16.0.1/32
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
# pp select 2
pp2# pppoe use lan3
pp2# pp auth accept pap chap
pp2# pp auth myname ID PASSWORD
pp2# ppp lcp mru on 1454
pp2# ppp ccp type none
pp2# ip pp address 172.17.0.1/32
pp2# ip pp mtu 1454
pp2# ip pp nat descriptor 2
pp2# pp enable 2
# ip route default gateway pp 1
# ipsec autorefresh on
```

```
# nat descriptor type 1 masquerade
# nat descriptor address outer 1 172.16.0.1
# nat descriptor masquerade static 1 1 192.168.0.254 udp 500
# nat descriptor masquerade static 1 2 192.168.0.254 esp
# nat descriptor type 2 masquerade
# nat descriptor address outer 2 172.17.0.1
# nat descriptor masquerade static 2 1 192.168.0.254 udp 500
# nat descriptor masquerade static 2 2 192.168.0.254 esp
# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel backup tunnel 2 switch-interface=on
tunnel1# tunnel enable 1
# ip route 192.168.1.0/24 gateway tunnel 1
# ipsec ike keepalive use 1 on
# ipsec ike local address 1 192.168.0.254
# ipsec ike pre-shared-key 1 text ABC
# ipsec ike remote address 1 any
# ipsec ike remote name 1 kyoten1-1
# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
# tunnel select 2
tunnel2# ipsec tunnel 102
tunnel2# tunnel enable 2
# ipsec ike local address 2 192.168.0.254
# ipsec ike pre-shared-key 2 text ABC
# ipsec ike remote address 2 any
# ipsec ike remote name 2 kyoten1-2
# ipsec sa policy 102 2 esp 3des-cbc md5-hmac
# tunnel select 3
tunnel3# ipsec tunnel 103
tunnel3# tunnel backup tunnel 4 switch-interface=on
tunnel3# tunnel enable 3
# ip route 192.168.2.0/24 gateway tunnel 3
# ipsec ike keepalive use 3 on
# ipsec ike local address 3 192.168.0.254
# ipsec ike pre-shared-key 3 text ABC
# ipsec ike remote address 3 any
# ipsec ike remote name 3 kyoten2-1
# ipsec sa policy 103 3 esp 3des-cbc md5-hmac
# tunnel select 4
tunnel4# ipsec tunnel 104
tunnel4# tunnel enable 4
# ipsec ike local address 4 192.168.0.254
# ipsec ike pre-shared-key 4 text ABC
# ipsec ike remote address 4 any
# ipsec ike remote name 4 kyoten2-2
# ipsec sa policy 104 4 esp 3des-cbc md5-hmac
```

[ルーター B の設定手順]

```
# ip lan1 address 192.168.1.254/24
# pp select 1
pp1# pp backup pp 2
pp1# pp always-on on
pp1# pppoe use lan2
```

```
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ppp ipcp ipaddress on
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
# pp select 2
pp2# pppoe use lan3
pp2# pp auth accept pap chap
pp2# pp auth myname ID PASSWORD
pp2# ppp lcp mru on 1454
pp2# ppp ccp type none
pp2# ppp ipcp ipaddress on
pp2# ip pp mtu 1454
pp2# ip pp nat descriptor 1
pp2# pp enable 2
# ipsec autorefresh on
# ip route default gateway pp 1
# nat descriptor type 1 masquerade
# nat descriptor masquerade static 1 1 192.168.1.254 udp 500
# nat descriptor masquerade static 1 2 192.168.1.254 esp
# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel backup tunnel 2 switch-interface=on
tunnel1# tunnel enable 1
# ip route 192.168.0.0/24 gateway tunnel 1
# ipsec ike keepalive use 1 on
# ipsec ike local address 1 192.168.1.254
# ipsec ike local name 1 kyoten1-1
# ipsec ike pre-shared-key 1 text ABC
# ipsec ike remote address 1 172.16.0.1
# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
# tunnel select 2
tunnel2# ipsec tunnel 102
tunnel2# tunnel enable 2
# ipsec ike local address 2 192.168.1.254
# ipsec ike local name 2 kyoten1-2
# ipsec ike pre-shared-key 2 text ABC
# ipsec ike remote address 2 172.17.0.1
# ipsec sa policy 102 2 esp 3des-cbc md5-hmac
```

[ルーター C の設定手順]

```
# ip lan1 address 192.168.2.254/24
# pp select 1
pp1# pp backup pp 2
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
```

```
pp1# ppp ipcp ipaddress on
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
# pp select 2
pp2# pppoe use lan3
pp2# pp auth accept pap chap
pp2# pp auth myname ID PASSWORD
pp2# ppp lcp mru on 1454
pp2# ppp ccp type none
pp2# ppp ipcp ipaddress on
pp2# ip pp mtu 1454
pp2# ip pp nat descriptor 1
pp2# pp enable 2
# ipsec autorefresh on
# ip route default gateway pp 1
# nat descriptor type 1 masquerade
# nat descriptor masquerade static 1 1 192.168.2.254 udp 500
# nat descriptor masquerade static 1 2 192.168.2.254 esp
# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel backup tunnel 2 switch-interface=on
tunnel1# tunnel enable 1
# ip route 192.168.0.0/24 gateway tunnel 1
# ipsec ike keepalive use 1 on
# ipsec ike local address 1 192.168.2.254
# ipsec ike local name 1 kyoten2-1
# ipsec ike pre-shared-key 1 text ABC
# ipsec ike remote address 1 172.16.0.1
# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
# tunnel select 2
tunnel2# ipsec tunnel 102
tunnel2# tunnel enable 2
# ipsec ike local address 2 192.168.2.254
# ipsec ike local name 2 kyoten2-2
# ipsec ike pre-shared-key 2 text ABC
# ipsec ike remote address 2 172.17.0.1
# ipsec sa policy 102 2 esp 3des-cbc md5-hmac
```

[解説]

センター、拠点共に ADSL 回線にてプロバイダと PPPoE 接続を 2 本確保しており、センター側はメイン回線、バックアップ回線ともに固定のアドレス割り当てを受けているものとします。

通常運用時はメイン回線でインターネット VPN 通信を行っているとします。

センター側、拠点側ともに回線障害に備えて、2 本の別々の回線を通してインターネット接続を設定しています。メイン回線障害発生時には自動的にバックアップ回線に切り替わり、インターネット接続および VPN 接続を行います。

例えば、拠点 2 とインターネットを結ぶメイン回線がダウンしたとします。するとルーター C は自動的にバックアップ回線を通してセンターのルーター A と接続を試みます。

拠点側ではメイン回線で障害発生を検知し、バックアップ回線によるインターネット接続に切り替わります。この際、VPN トンネルも一時的に切断されることになりますが、バックアップ回線によるインターネット接続確立後に再度センターとの間にトンネルが生成されます。メイン回線が復旧するとインターネットへの接続はバックアップ回線からメイン回線に戻ることになります。この時 VPN トンネルも一旦切断されることになりますが、すぐに復旧したメイン回線を通してセンターと再接続され、正常運用に戻ります。

センターとインターネットを結ぶメイン回線がダウンしたとします。すると拠点側ルーター (ルーター B、ルーター C) はセンターとの VPN トンネルを確立します。

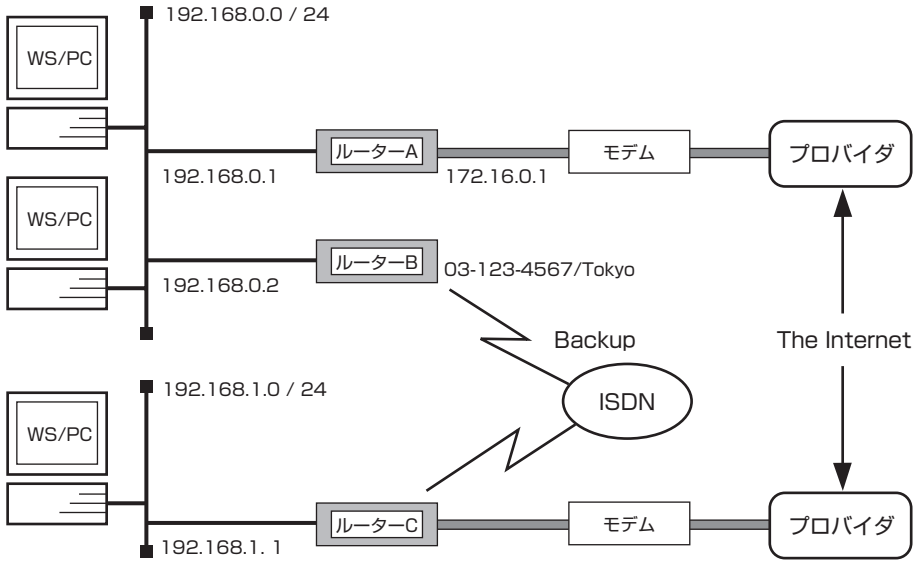
センターではメイン回線で障害が発生することにより、バックアップ回線でのインターネット接続を開始します。拠点側ではセンター側のルーター A との VPN トンネルが切断されたことを検知し、自動的にバックアップトンネルの起動を行い、センターとの間に新たな VPN トンネルを生成します。センターのメイン回線が復旧すれば、拠点側 (ルーター B、ルーター C) ではセンターとの間のメイントンネルが復旧します。復旧されれば自動的にセンターとの通信には復旧されたメイントンネルを使うようになり、正常運用に戻ります。

本設定例では拠点数は 2 としていますが、設定例内の拠点に関する設定を増やすことで複数の拠点との VPN 通信をバックアップする設定を行うことが可能です。

RTX3000、RTX2000、RTX1500、RTX1100、RTX1000、RT300i の利用を前提とした設定例となります。

24.9 ISDN 回線によるトンネルバックアップ

[構成図]



[ルーター A の設定手順]

```
# ip lan1 address 192.168.0.1/24
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ipcp msext on
pp1# ip pp address 172.16.0.1/32
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
# ip route default gateway pp 1
# nat descriptor type 1 masquerade
# nat descriptor address outer 1 172.16.0.1
# nat descriptor masquerade static 1 1 192.168.0.1 udp 500
# nat descriptor masquerade static 1 2 192.168.0.1 esp
# ipsec auto refresh on
# ipsec ike keepalive use 1 on
# ipsec ike local address 1 192.168.0.1
# ipsec ike pre-shared-key 1 text ABC
# ipsec ike remote address 1 any
# ipsec ike remote name 1 kyoten1
# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel backup lan1 192.168.0.2
tunnel1# tunnel enable 1
# ip route 192.168.1.0/24 gateway tunnel 1
```

[ルーター B の設定手順]

```
# ip lan1 address 192.168.0.2/24
# isdn local address bri1 03-123-4567/Tokyo
# pp select anonymous
anonymous# pp bind bri1
anonymous# pp auth request chap
anonymous# pp auth username kyoten1 kyoten1
anonymous# pp enable anonymous
# ip route 192.168.1.0/24 gateway pp anonymous name=kyoten1
```

[ルーター C の設定手順]

```
# ip lan1 address 192.168.1.1/24
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ipcp msext on
pp1# ppp ipcp ipaddress on
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
# ip route default gateway pp 1
# pp select 2
pp2# pp bind bri1
pp2# isdn remote address call 03-123-4567/Tokyo
pp2# pp auth accept chap
pp2# pp auth myname kyoten1 kyoten1
pp2# pp enable 2
# nat descriptor type 1 masquerade
# nat descriptor masquerade static 1 1 192.168.1.1 udp 500
# nat descriptor masquerade static 1 2 192.168.1.1 esp
# ipsec auto refresh on
# ipsec ike keepalive use 1 on
# ipsec ike local address 1 192.168.1.1
# ipsec ike local name 1 kyoten1
# ipsec ike pre-shared-key 1 text ABC
# ipsec ike remote address 1 172.16.0.1
# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel backup pp 2 switch-router=on
tunnel1# tunnel enable 1
# ip route 192.168.0.0/24 gateway tunnel 1
```

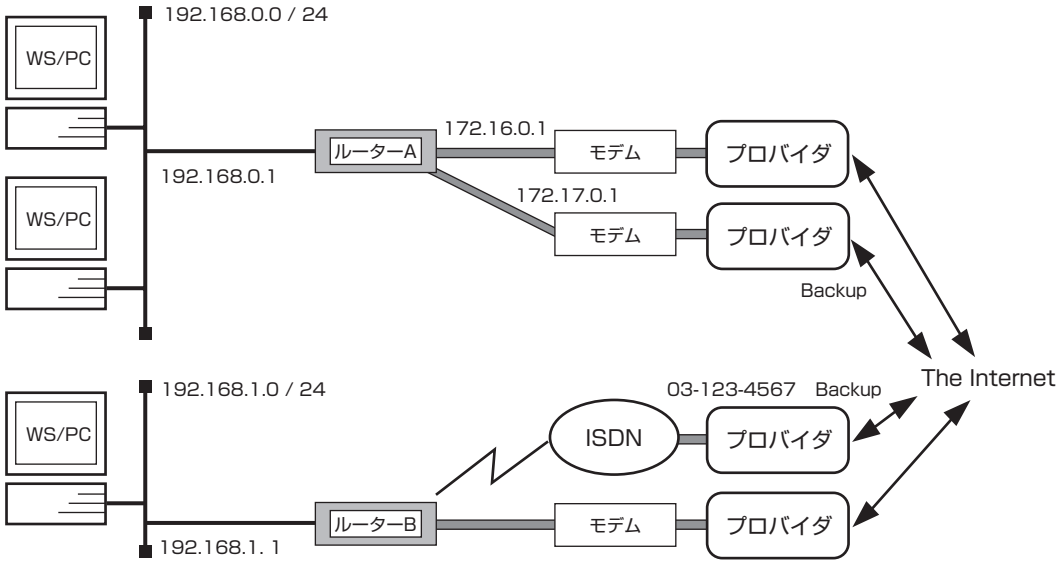
[解説]

センター、拠点共に ADSL 回線にてプロバイダと PPPoE 接続しており、センター側は固定のアドレス割り当てを受けているものとします。
通常運用時はインターネット VPN 通信を行っているとします。
拠点側では 1 台のルーターで 2 本の回線を収容し、回線の障害に応じて自動的に回線を切り替えます。VPN トンネルに障害が発生したときには、ISDN を使ってセンターと拠点を直結します。

ルーター A は RTX3000、RTX2000、RTX1500、RTX1100、RTX1000、RT300i、RT107e の利用を前提とした設定例となります。
ルーター B は RTX3000、RTX1500、RTX1100、RTX1000、RT300i、RT250i の利用を前提とした設定例となります。
ルーター C は RTX3000、RTX1500、RTX1100、RTX1000、RT300i の利用を前提とした設定例となります。

24.10 インターネット VPN によるトンネルバックアップ

[構成図]



[ルーター A の設定手順]

```
# ip lan1 address 192.168.0.1/24
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp backup pp 2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ipcp msext on
pp1# ip pp address 172.16.0.1/32
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
# ip route default gateway pp 1
# pp select 2
pp1# pp always-on on
pp1# pppoe use lan3
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ipcp msext on
pp1# ip pp address 172.17.0.1/32
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 2
pp1# pp enable 1
# nat descriptor type 1 masquerade
# nat descriptor address outer 1 172.16.0.1
# nat descriptor masquerade static 1 1 192.168.0.1 udp 500
# nat descriptor masquerade static 1 2 192.168.0.1 esp
# nat descriptor type 2 masquerade
# nat descriptor address outer 2 172.17.0.1
# nat descriptor masquerade static 2 1 192.168.0.1 udp 500
# nat descriptor masquerade static 2 2 192.168.0.1 esp
```

```
# ipsec auto refresh on
# ipsec ike keepalive use 1 on
# ipsec ike local address 1 192.168.0.1
# ipsec ike pre-shared-key 1 text ABC
# ipsec ike remote address 1 any
# ipsec ike remote name 1 kyoten1-1
# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel backup tunnel 2 switch-interface=on
tunnel1# tunnel enable 1
# ip route 192.168.1.0/24 gateway tunnel 1
# ipsec ike local address 2 192.168.0.1
# ipsec ike pre-shared-key 2 text ABC
# ipsec ike remote address 2 any
# ipsec ike remote name 2 kyoten1-2
# ipsec sa policy 102 2 esp 3des-cbc md5-hmac
# tunnel select 2
tunnel2# ipsec tunnel 102
tunnel2# tunnel enable 2
```

[ルーター B の設定手順]

```
# ip lan1 address 192.168.1.1/24
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp backup pp 2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ipcp msext on
pp1# ppp ipcp ipaddress on
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
# ip route default gateway pp 1
# pp select 2
pp2# pp bind bri1
pp2# isdn remote address call 03-123-4567
pp2# pp auth accept chap
pp2# pp auth myname ID PASSWORD
pp2# ppp ipcp ipaddress on
pp2# ppp ipcp msext on
pp2# ip pp nat descriptor 1
pp2# pp enable 2
# nat descriptor type 1 masquerade
# nat descriptor masquerade static 1 1 192.168.1.1 udp 500
# nat descriptor masquerade static 1 2 192.168.1.1 esp
# ipsec auth refresh on
# ipsec ike keepalive use 1 on
# ipsec ike local address 1 192.168.1.1
# ipsec ike local name 1 kyoten1-1
# ipsec ike pre-shared-key 1 text ABC
```

```
# ipsec ike remote address 1 172.16.0.1
# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel backup tunnel 2 switch-interface=on
tunnel1# tunnel enable 1
# ip route 192.168.0.0/24 gateway tunnel 1
# ipsec ike local address 2 192.168.1.1
# ipsec ike local name 2 kyoten1-2
# ipsec ike pre-shared-key 1 text ABC
# ipsec ike remote address 2 172.17.0.1
# ipsec sa policy 102 2 esp 3des-cbc md5-hmac
# tunnel select 2
tunnel2# ipsec tunnel 102
tunnel2# tunnel enable 2
```

[解説]

センター、拠点共に ADSL 回線にてプロバイダと PPPoE 接続しており、センター側は固定のアドレス割り当てを受けているものとします。

通常運用時はメイン回線のインターネット VPN 通信を行っているとします。

1 台のルーターで 2 本の回線を収容し、回線の障害に応じて自動的に回線を切り替えます。

拠点側のバックアップ回線は ISDN でインターネットに接続します。

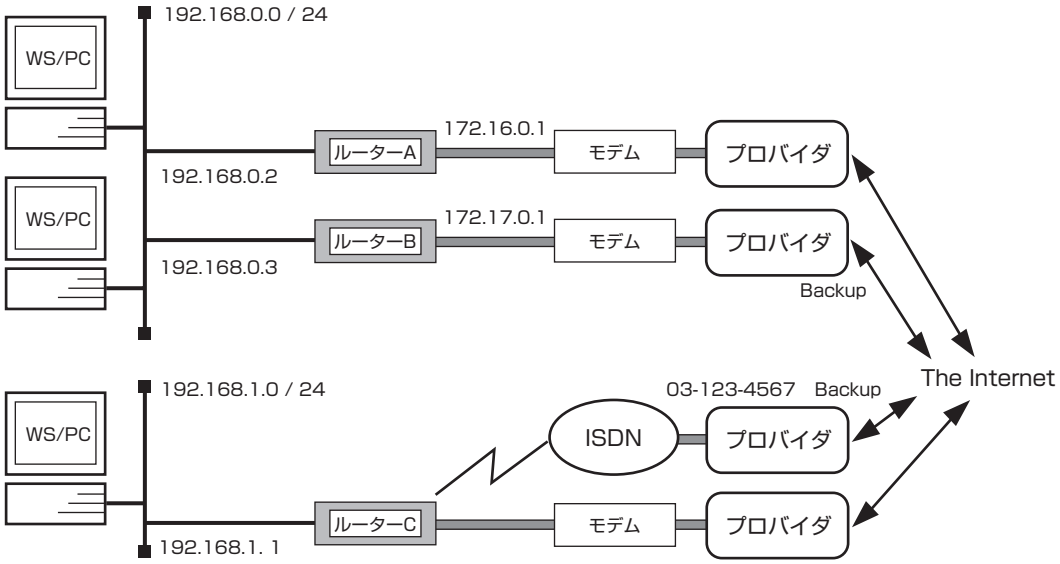
メイン回線の VPN トンネルに障害が発生したときには、バックアップ回線の VPN トンネルへ切り替えます。切り替えた後でも通信は暗号化されたままであり、回線の状態に関係なく安全なインターネット接続を維持することができます。

ルーター A は RTX3000、RTX2000、RTX1500、RTX1100、RTX1000、RT300i の利用を前提とした設定例となります。

ルーター B は RTX3000、RTX1500、RTX1100、RTX1000、RT300i の利用を前提とした設定例となります。

24.11　VRRP とインターネット VPN によるトンネルバックアップ

[構成図]



[ルーター A の設定手順]

```
# ip lan1 address 192.168.0.2/24
# ip lan1 vrrp 1 192.168.0.1 priority=200
# ip lan1 vrrp shutdown trigger 1 pp 1
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ipcp msext on
pp1# ip pp address 172.16.0.1/32
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
# ip route default gateway pp 1
# nat descriptor type 1 masquerade
# nat descriptor address outer 1 172.16.0.1
# nat descriptor masquerade static 1 1 192.168.0.2 udp 500
# nat descriptor masquerade static 1 2 192.168.0.2 esp
# ipsec auto refresh on
# ipsec ike keepalive use 1 on
# ipsec ike local address 1 192.168.0.2
# ipsec ike pre-shared-key 1 text ABC
# ipsec ike remote address 1 any
# ipsec ike remote name 1 kyoten1-1
# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel backup lan1 192.168.0.3
tunnel1# tunnel enable 1
# ip route 192.168.1.0/24 gateway tunnel 1
```

[ルーター B の設定手順]

```
# ip lan1 address 192.168.0.3/24
# ip lan1 vrrp 1 192.168.0.1 priority=100
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ipcp msext on
pp1# ip pp address 172.17.0.1/32
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
# ip route default gateway pp 1
# nat descriptor type 1 masquerade
# nat descriptor address outer 1 172.17.0.1
# nat descriptor masquerade static 1 1 192.168.0.3 udp 500
# ipsec auto refresh on
# ipsec ike local address 1 192.168.0.3
# ipsec ike pre-shared-key 1 text ABC
# ipsec ike remote address 1 any
# ipsec ike remote name 1 kyoten1-2
# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel enable 1
tunnel1# ip route 192.168.1.0/24 gateway tunnel 1
```

[ルーター C の設定手順]

```
# ip lan1 address 192.168.1.1/24
# pp select 1
pp1# pp backup pp 2
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ipcp msext on
pp1# ppp ipcp ipaddress on
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
# ip route default gateway pp 1
# pp select 2
pp2# pp bind bri1
pp2# isdn remote address call 03-123-4567
pp2# pp auth accept chap
pp2# pp auth myname ID PASSWORD
pp2# ppp ipcp ipaddress on
pp2# ppp ipcp msext on
pp2# ip pp nat descriptor 1
pp2# pp enable 2
```

```
# nat descriptor type 1 masquerade
# nat descriptor masquerade static 1 1 192.168.1.1 udp 500
# nat descriptor masquerade static 1 2 192.168.1.1 esp
# ipsec auto refresh on
# ipsec ike keepalive use 1 on
# ipsec ike local address 1 192.168.1.1
# ipsec ike local name 1 kyoten1-1
# ipsec ike pre-shared-key 1 text ABC
# ipsec ike remote address 1 172.16.0.1
# ipsec sa policy 101 1 esp 3des-cbc md5-hmac
# tunnel select 1
tunnel1# ipsec tunnel 101
tunnel1# tunnel backup tunnel 2 switch-interface=on
tunnel1# tunnel enable 1
# ip route 192.168.0.0/24 gateway tunnel 1
# ipsec ike local address 2 192.168.1.1
# ipsec ike local name 2 kyoten1-2
# ipsec ike pre-shared-key 2 text ABC
# ipsec ike remote address 2 172.17.0.1
# ipsec sa policy 102 2 esp 3des-cbc md5-hmac
# tunnel select 2
tunnel2# ipsec tunnel 102
tunnel2# tunnel enable 2
```

[解説]

センター、拠点共に ADSL 回線にてプロバイダと PPPoE 接続しており、センター側は固定のアドレス割り当てを受けているものとします。

通常運用時はメイン回線のインターネット VPN 通信を行っているとします。

拠点側では 1 台のルーターで 2 本の回線を収容し、回線の障害に応じて自動的に回線を切り替えます。拠点側のバックアップ回線は ISDN でインターネットに接続します。

センター側ではルーターを二重化し、回線だけでなく、機器のトラブルにも対応します。

メイン回線の VPN トンネルに障害が発生したときには、バックアップ回線の VPN トンネルへ切り替えます。切り替えた後でも通信は暗号化されたままであり、回線の状態に関係なく安全なインターネット接続を維持することができます。

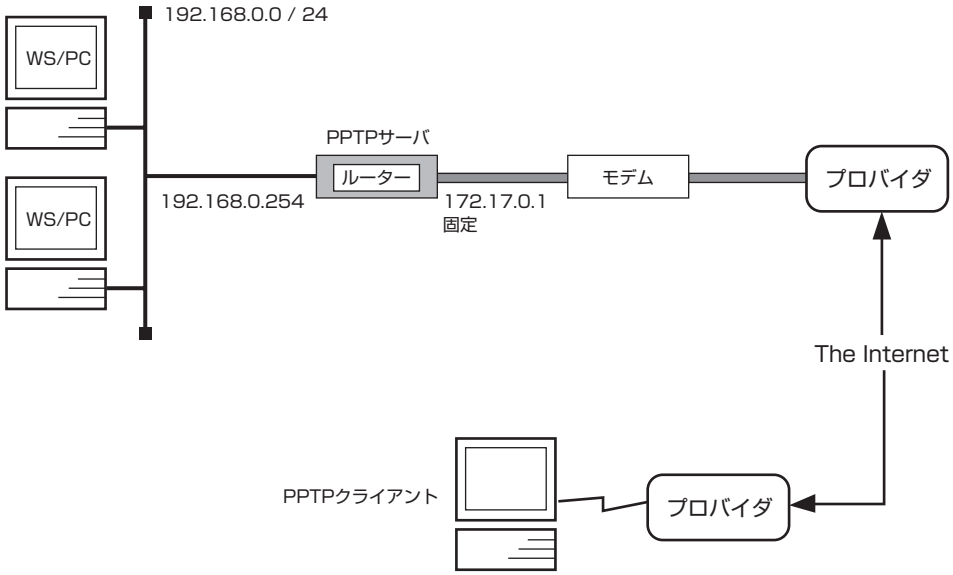
ルーター A、ルーター B は RTX3000、RTX2000、RTX1500、RTX1100、RTX1000、RT300i、RT107e の利用を前提とした設定例となります。

ルーター C は RTX3000、RTX1500、RTX1100、RTX1000、RT300i の利用を前提とした設定例となります。

25. PPTP を用いたインターネット VPN 環境の設定例

25.1 リモートアクセス VPN 接続の設定例

[構成図]



[設定手順]

```
# ip lan1 address 192.168.0.254/24
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ip pp address 172.17.0.1/32
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
pp1# pp select anonymous
anonymous# pp bind tunnel1 tunnel2 tunnel3
anonymous# pp auth request mschap
anonymous# pp auth username test1 test1
anonymous# pp auth username test2 test2
anonymous# pp auth username test3 test3
anonymous# ppp ipcp ipaddress on
anonymous# ppp ipcp msext on
anonymous# ppp ccp type mppe-any
anonymous# ip pp remote address pool 192.168.1.100-192.168.1.102
anonymous# ip pp mtu 1280
anonymous# pptp service type server
anonymous# pp enable anonymous
anonymous# pptp service on
anonymous# tunnel select 1
tunnel1# tunnel encapsulation pptp
tunnel1# tunnel enable 1
tunnel1# tunnel select 2
tunnel2# tunnel encapsulation pptp
tunnel2# tunnel enable 2
```

```
tunnel2# tunnel select 3
tunnel3# tunnel encapsulation pptp
tunnel3# tunnel enable 3
tunnel3# tunnel select none
# ip route default gateway pp 1
# nat descriptor type 1 masquerade
# nat descriptor masquerade static 1 1 192.168.0.254 tcp 1723
# nat descriptor masquerade static 1 2 192.168.0.254 gre
# save
```

[解説]

本社側は ADSL によるインターネット接続をしており、プロバイダより 172.17.0.1 の固定アドレスの割り当てを受けていると仮定します。本社側 (センタ 側) ネットワーク（192.168.0.0/24）に動作確認の取れている PPTP クライアント (Windows パソコン や MacOS X パソコン) がインターネットを介した VPN 接続をするための設定例です。この例では WAN 側と LAN 側にそれぞれイーサネットインタフェースが必要となりますので、RTX1100、RTX1000、RT300i、RT105e の利用を前提とした設定例となります。

```
anonymous# pp bind tunnel1 tunnel2 tunnel3
anonymous# pp auth username test1 test1
anonymous# pp auth username test2 test2
anonymous# pp auth username test3 test3
anonymous# ip pp remote address pool 192.168.1.100-192.168.1.102
```

同時に 3 クライアントの接続を収容するためのアカウントとトンネルを 3 つ準備します。

```
anonymous# pp auth request mschap
```

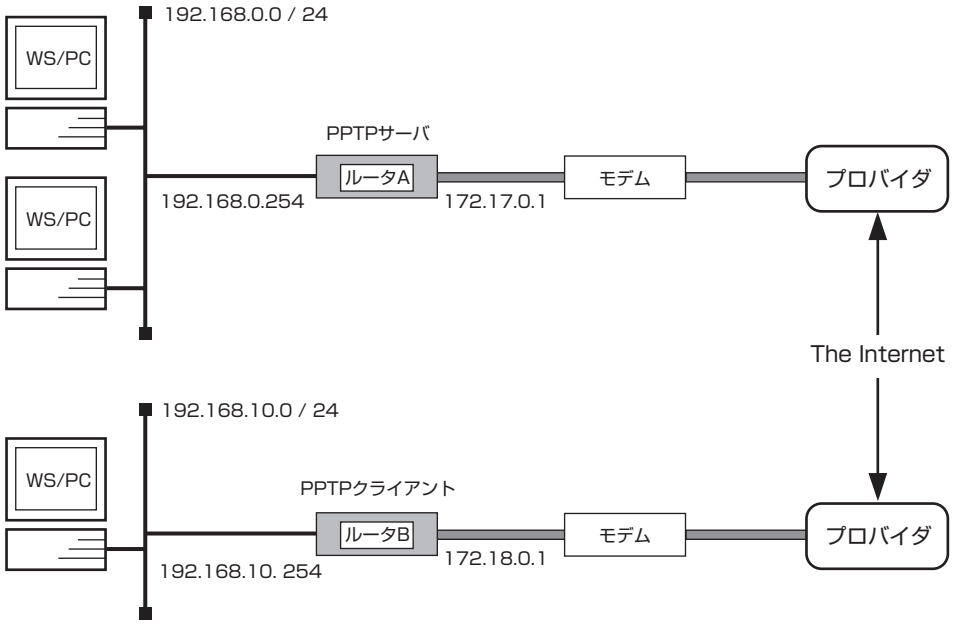
PPTP クライアントの認証方式に合わせます。
Windows 98SE/Me の場合は mschap です。
Windows 2000/XP の場合は mschap と mschap-ve の両方がパソコン側で指定可能です。
MacOS X（10.2 以降) の場合は mschap-v2 です。

```
# nat descriptor masquerade static 1 1 192.168.0.254 tcp 1723
# nat descriptor masquerade static 1 2 192.168.0.254 gre
```

PPTP パススルーの設定です。NAT を使用する場合は必須です。

25.2 LAN 間接続 VPN の設定例（PPPoE でインターネット接続の場合）

[構成図]



[ルーター A の設定手順]

```
# ip lan1 address 192.168.0.254/24
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ip pp address 172.17.0.1/32
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
pp1# pp select 2
pp2# pp bind tunnel1
pp2# pp auth request mschap-v2
pp2# pp auth username test1 test1
pp2# ppp ipcp ipaddress on
pp2# ppp ccp type mppe-any
pp2# ip pp mtu 1280
pp2# pptp service type server
pp2# pp enable 2
pp2# pptp service on
pp2# tunnel select 1
tunnel1# tunnel encapsulation pptp
tunnel1# tunnel endpoint address 172.18.0.1
tunnel1# tunnel enable 1
tunnel1# ip route 192.168.10.0/24 gateway pp 2
tunnel1# ip route default gateway pp 1
tunnel1# nat descriptor type 1 masquerade
tunnel1# nat descriptor masquerade static 1 1 192.168.0.254 tcp 1723
tunnel1# nat descriptor masquerade static 1 2 192.168.0.254 gre
tunnel1# save
```

[ルーター B の設定手順]

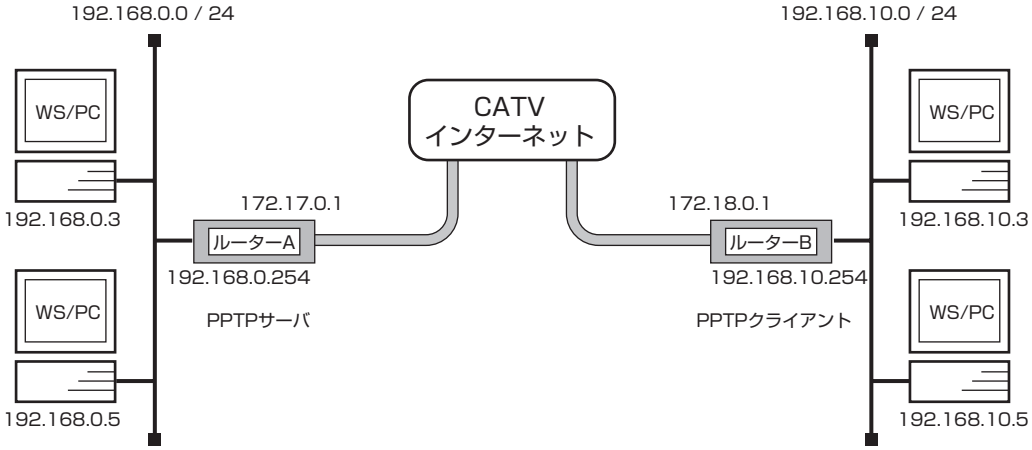
```
# ip lan1 address 192.168.10.254/24
# pp select 1
pp1# pp always-on on
pp1# pppoe use lan2
pp1# pp auth accept pap chap
pp1# pp auth myname ID PASSWORD
pp1# ppp lcp mru on 1454
pp1# ppp ccp type none
pp1# ip pp address 172.18.0.1/32
pp1# ip pp mtu 1454
pp1# ip pp nat descriptor 1
pp1# pp enable 1
pp1# pp select 2
pp2# pp bind tunnel1
pp2# pp keepalive use lcp-echo
pp2# pp auth accept mschap-v2
pp2# pp auth myname test1 test1
pp2# ppp ipcp ipaddress on
pp2# ppp ccp type mppe-any
pp2# ip pp mtu 1280
pp2# pptp service type client
pp2# pp enable 2
pp2# pptp service on
pp2# tunnel select 1
tunnel1# tunnel encapsulation pptp
tunnel1# tunnel endpoint address 172.17.0.1
tunnel1# tunnel enable 1
tunnel1# ip route 192.168.0.0/24 gateway pp 2
tunnel1# ip route default gateway pp 1
tunnel1# nat descriptor type 1 masquerade
tunnel1# nat descriptor masquerade static 1 1 192.168.10.254 tcp 1723
tunnel1# nat descriptor masquerade static 1 2 192.168.10.254 gre
tunnel1# save
```

[解説]

インターネット接続に ADSL を利用している拠点間で PPTP による VPN を使用するための設定例です。なお、この例では WAN 側と LAN 側にそれぞれイーサネットインタフェースが必要となりますので、RTX1100、RTX1000、RT300i、RT105e の利用を前提とした設定例となります。

25.3 LAN 間接続 VPN の設定例（CATV でインターネット接続の場合）

[構成図]



[ルーター A の設定手順]

```
# ip lan1 address 192.168.0.254/24
# ip lan2 address 172.17.0.1/24
# ip lan2 nat descriptor 1
# pp select 1
pp1# pp bind tunnel1
pp1# pp auth request mschap
pp1# pp auth username test1 test1
pp1# ppp ipcp ipaddress on
pp1# ppp ccp type mppe-any
pp1# ip pp mtu 1280
pp1# pptp service type server
pp1# pp enable 1
pp1# pptp service on
pp1# tunnel select 1
tunnel1# tunnel encapsulation pptp
tunnel1# tunnel endpoint address 172.18.0.1
tunnel1# tunnel enable 1
tunnel1# ip route 192.168.10.0/24 gateway pp 1
tunnel1# ip route default gateway GATEWAY
tunnel1# nat descriptor type 1 masquerade
tunnel1# nat descriptor address outer 1 primary
tunnel1# nat descriptor masquerade static 1 1 192.168.0.254 tcp 1723
tunnel1# nat descriptor masquerade static 1 2 192.168.0.254 gre
tunnel1# save
```

[ルーター B の設定手順]

```
# ip lan1 address 192.168.10.254/24
# ip lan2 address 172.18.0.1/24
# ip lan2 nat descriptor 1
# pp select 1
pp1# pp bind tunnel1
pp1# pp keepalive use lcp-echo
pp1# pp auth accept mschap
pp1# pp auth myname test1 test1
pp1# ppp ipcp ipaddress on
pp1# ppp ccp type mppe-any
pp1# ip pp mtu 1280
pp1# pptp service type client
pp1# pp enable 1
pp1# pptp service on
pp1# tunnel select 1
tunnel1# tunnel encapsulation pptp
tunnel1# tunnel endpoint address 172.17.0.1
tunnel1# tunnel enable 1
tunnel1# ip route 192.168.0.0/24 gateway pp 1
tunnel1# ip route default gateway GATEWAY
tunnel1# nat descriptor type 1 masquerade
tunnel1# nat descriptor address outer 1 primary
tunnel1# nat descriptor masquerade static 1 1 192.168.10.254 tcp 1723
tunnel1# nat descriptor masquerade static 1 2 192.168.10.254 gre
tunnel1# save
```

[解説]

インターネット接続に CATV を利用している拠点間で PPTP による VPN を使用するための設定例です。なお、この例では WAN 側と LAN 側にそれぞれイーサネットインタフェースが必要となりますので、RTX1100、RTX1000、RT300i、RT105e の利用を前提とした設定例となります。

26. モバイルインターネット接続の接続例

1. mopera で使用する場合の設定
2. プロバイダに mopera U を指定し、上限以上の通信を制限する
3. IIJ モバイル / タイプ D で使用する場合の設定

[注意事項]

本機能にて携帯端末からパケット通信を行う場合、定額制プランの対象外となり、別料金が必要な従量課金となります。

例えば、NTT ドコモの「定額データプラン HIGH-SPEED」、「定額データプラン 64K」、「パケ・ホーダイ」、「パケ・ホーダイフル」、「Biz・ホーダイ」などのプランでは本機能による通信は対象外となり、別途料金が発生しますので十分ご注意ください。
料金プランにつきましては携帯各社とのご契約内容をご確認ください。

FOMA 端末の取扱説明書をよく読んで、正しい使用方法のもとでお使いください。

[FOMA のデータ通信の種類]

FOMA 端末には主に以下の 2 つのデータ通信の形態があります。

(1) パケット通信

送受信したデータ量に応じて通信料がかかる通信形態です。(ハイスピードでは受信最大 3.6Mbps、送信最大 384Kbps)
FOMA USB ケーブルにてパソコンと接続し、各種設定を行うと利用できます。
NTT ドコモのインターネット接続サービス「mopera」「mopera U」など、FOMA パケット通信に対応したプロバイダが必要です。データ量が多いと非常に高額な通信料となるためご注意ください。

(2) 64K データ通信

接続している時間に応じて、通信料がかかる通信形態です。(通信速度 64Kbps)

本機能では、このうちのパケット通信を使用します。本来パソコンで行う設定をルーターのコマンドから行う必要があります。
FOMA のデータ通信の詳細はお手持ちの FOMA 端末の取扱説明書をご覧ください。

接続までの流れ

FOMA 端末をパソコンに FOMA USB ケーブルで接続してパケット通信を行うときと同様に、ルーターがパソコンの代わりに設定や発信動作を行います。

1. FOMA 端末をルーターに FOMA USB ケーブルで接続します。
2. FOMA のパケット通信に対応した、ご利用になりたい任意のプロバイダを設定し、ルーターから発信させます。
3. ルーターが FOMA 対応プロバイダを経由してインターネットへ接続できるようになります。

mopera 以外のプロバイダを指定することも可能ですが別途契約が必要です。着信させることはできません。

[設定・接続方法]

プロバイダの指定

FOMA で発信するには、発信先の情報として APN (Access Point Name) と CID (Context Identifier) が必要となります。
また、NTT ドコモが提供する mopera や mopera U では発信者番号を通知する必要があります。
発信する番号情報や APN、CID 情報は、いずれも AT コマンドによって FOMA 端末に発行されます。
パソコンを使って発信するときは端末に付属のアプリケーションから実行できますが、ルーターから発信する場合はルーターが FOMA 端末に対して AT コマンドを発行します。
現時点では GUI (かんたん設定ページ) からの設定はできません。

■ NTT ドコモ提供の APN の例

プロバイダ名	APN	説明
mopera	mopera.ne.jp	NTT ドコモが提供する無料のインターネット接続サービスです。 申し込み不要で利用可能です。ハイスピードには対応していません。
mopera U	mopera.net	NTT ドコモが提供する有料のハイスピードにも対応したインターネット接続サービスです。別途申し込みが必要です。

■ CID

発信時には、上記の APN が何番の CID に相当するか指定してから発信する必要があります。
FOMA 端末は、初期状態では以下のように割り当てられています。

CID	APN
1	mopera.ne.jp
2	未設定
3	mopera.net
4-10	未設定

発信に必要なルーターのコマンド

FOMA 端末から指定プロバイダに対して発信するのに必要な主なコマンドは以下の 3 つです。

mobile access-point name APN cid=CID..... 選択された相手先の接続プロバイダを設定します
mobile display caller id DISPLAY..... 発番号を通知するかどうかの指定
connect PP_NUM ..... 実際に FOMA に対して発信を指示します

mobile auto connect on を設定すると、パケット発生時に自動で発信させることも可能です。

明示的にハイスピード指定するコマンドはありません。
以下の条件下で発信したときに自動でハイスピードになります。

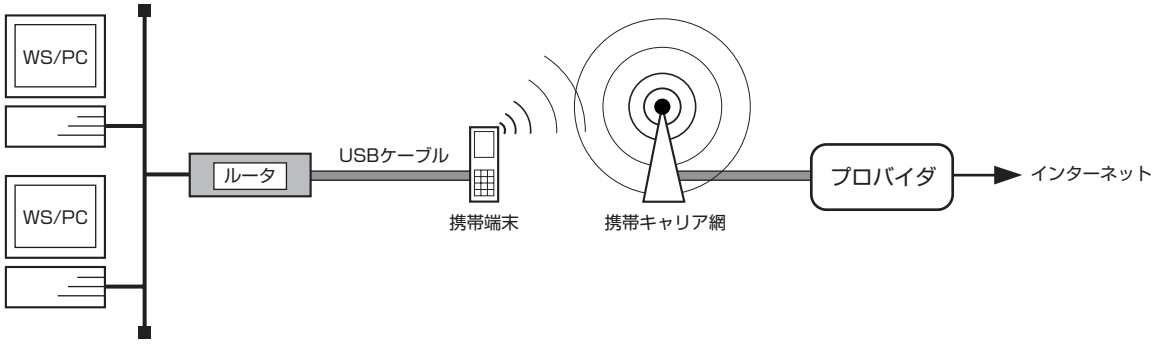
a. ハイスピードに対応した携帯端末
b. 対応したプロバイダを指定 (mopera U 等)
c. ハイスピードエリア内

接続中の下り最大速度は **show status pp** コマンドで確認可能です。
機種によってはルーターと携帯端末間の速度 (DTE 速度) しか表示できないものもあります。

RTX1200 の利用を前提とした設定例となります。

26.1 mopera で使用する場合の設定

[構成図]



[設定手順]

```
# mobile use usb1 on
# mobile type usb1 auto
# pp select 1
pp1# pp bind usb1
pp1# pp auth accept pap chap
pp1# pp auth myname xxxxx yyyyy
pp1# ppp lcp mru off 1792
pp1# ppp lcp accm on
pp1# ppp lcp pfc on
pp1# ppp lcp acfc on
pp1# ppp ipcp ipaddress on
pp1# ppp ipcp msext on
pp1# ppp ipv6cp use off
pp1# ip pp nat descriptor 1000
pp1# mobile access-point name mopera.ne.jp cid=1
pp1# mobile display caller id on
pp1# pp enable 1
pp1# pp select none
# ip route default gateway pp 1
# dns server pp 1
# nat descriptor type 1000 masquerade
# save
```

[解説]

APN として mopera を指定し、CID 1 番で発信します。
パケット通信量制限とパケット通信時間制限はデフォルト値とした場合の設定例です。

本例ではパケット通信量制限とパケット通信時間制限はデフォルト値を使用した設定ですが、実際のご利用状況に合わせて制限をかけてください。

1. # mobile use usb1 on
   USB ポートをモバイルインターネット接続用に設定します。

2. # mobile type usb1 auto
   USB ポートに接続する携帯端末の種類を自動認識に設定します。

3. # pp select 1
   pp1# pp bind usb1
   USB ポートを pp1 にバインドします。

4. pp1# pp auth accept pap chap
   pp1# pp auth myname xxxxx yyyyy
   任意の ID/Password を指定します。

5. pp1# ppp lcp mru off 1792
   通信量削減のため推奨します。
   pp1# ppp lcp accm on
   通信量削減のため推奨します。
   pp1# ppp lcp pfc on
   通信量削減のため推奨します。
   pp1# ppp lcp acfc on
   通信量削減のため推奨します。

6. pp1# ppp ipcp ipaddress on
   pp1# ppp ipcp msext on
   pp1# ppp ipv6cp use off
   pp1# ip pp nat descriptor 1000

   pp1# mobile access-point name mopera.ne.jp cid=1
   cid を 1 に割り当て pp1 は mopera への発信に設定します。

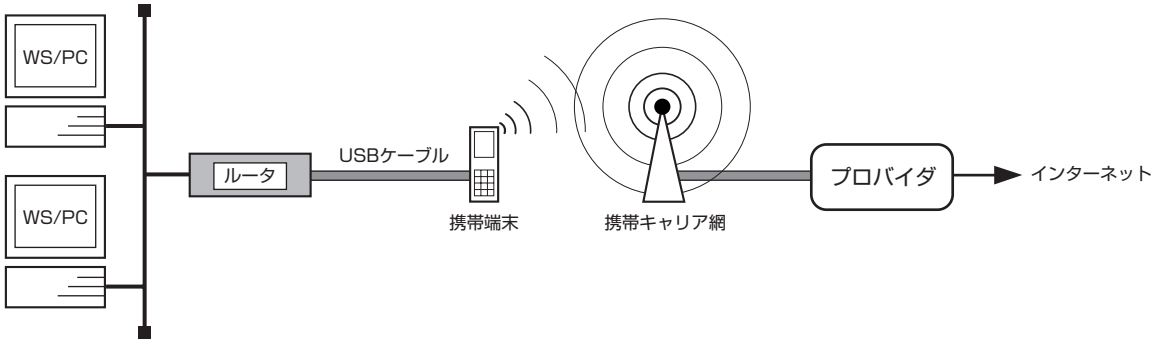
7. pp1# mobile display caller id on
   発信者番号を通知します。("186" を付けて発信)

8. pp1# pp enable 1
   pp1# pp select none
   # ip route default gateway pp 1
   # dns server pp 1
   # nat descriptor type 1000 masquerade
   # save

手動で発信するには
connect 1
コマンドを使用します。
なお、mobile auto connect on を設定すると、パケット発生時に自動で発信させることも可能です。

26.2 プロバイダに mopera U を指定し、上限以上の通信を制限する

[構成図]



[設定手順]

```
# mobile use usb1 on
# mobile type usb1 auto
# pp select 2
pp2# pp bind usb1
pp2# pp auth accept pap chap
pp2# pp auth myname xxxxx yyyyy
pp2# ppp lcp mru off 1792
pp2# ppp lcp accm on
pp2# ppp lcp pfc on
pp2# ppp lcp acfc on
pp2# ppp ipcp ipaddress on
pp2# ppp ipcp msext on
pp2# ppp ipv6cp use off
pp2# ip pp nat descriptor 1000
pp2# mobile access-point name mopera.net cid=3
pp2# mobile display caller id on
pp2# mobile access limit length 10000
pp2# mobile access limit time 3600
pp2# mobile disconnect time 120
pp2# pp enable 2
pp2# pp select none
# ip route default gateway pp 2
# dns server pp 2
# nat descriptor type 1000 masquerade
# save
```

[解説]

APN として mopera U を指定し、CID 3 番で発信します。
パケット通信量制限とパケット通信時間制限を設定した場合の設定例です。

本例のパケット通信量制限とパケット通信時間制限の設定値は例であり、
実際のご利用状況に合わせて制限をかけてください。

1. # mobile use usb1 on
   USB ポートをモバイルインターネット接続用に設定します。

2. # mobile type usb1 auto
   USB ポートに接続する携帯端末の種類を自動認識に設定します。

3. # pp select 2
   pp2# pp bind usb1
   USB ポートを pp2 にバインドします。

4. pp2# pp auth accept pap chap
   pp2# pp auth myname xxxx yyyy
   任意の ID/Password を指定します。

5. pp2# ppp lcp mru off 1792
   通信量削減のため推奨します。
   pp2# ppp lcp accm on
   通信量削減のため推奨します。
   pp2# ppp lcp pfc on
   通信量削減のため推奨します。
   pp2# ppp lcp acfc on
   通信量削減のため推奨します。

6. pp2# ppp ipcp ipaddress on
   pp2# ppp ipcp msext on
   pp2# ppp ipv6cp use off
   pp2# ip pp nat descriptor 1000

7. pp2# mobile access-point name mopera.net cid=3
   cid を 3 に割り当て pp2 は mopera U への発信に設定します。

8. pp2# mobile display caller id on
   発信者番号を通知します。("186" を付けて発信)

9. pp2# mobile access limit length 10000
   累積パケット長が 10,000 を超えたら通信を強制終了し、その後の通信もブロックします。

   FOMA のパケット定額サービス「定額データプラン HIGH-SPEED」、「定額データプラン 64K」、「パケ・ホーダイ」「パケ・ホーダイフル」「Biz・ホーダイ」の定額対象外となります。
   制限を解除しないでください。

   pp2# mobile access limit time 3600
   累積通信時間が 3,600 秒を超えたら通信を強制終了し、その後の通信もブロックします。

   FOMA のパケット定額サービス「定額データプラン HIGH-SPEED」、「定額データプラン 64K」、「パケ・ホーダイ」「パケ・ホーダイフル」「Biz・ホーダイ」の定額対象外となります。
   制限を解除しないでください。

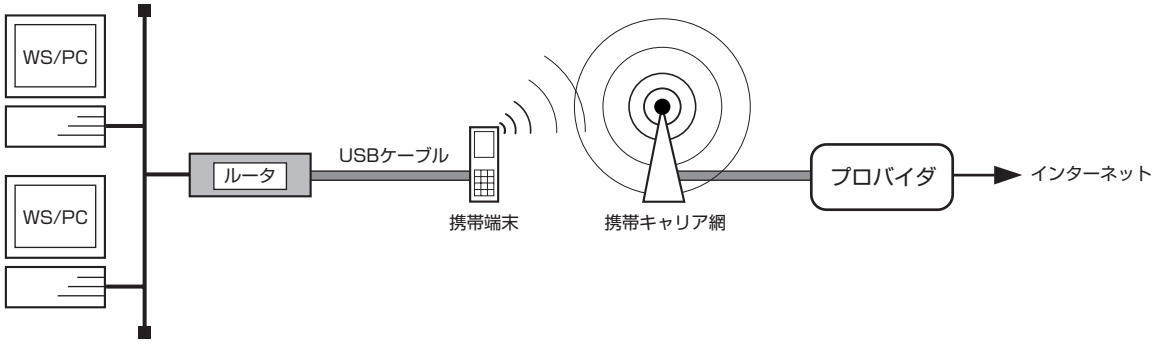
   pp2# mobile disconnect time 120
   120 秒間パケットの送受信がなければ切断します。

10. pp2# pp enable 2
    pp2# pp select none
    # ip route default gateway pp 2
    # dns server pp 2
    # nat descriptor type 1000 masquerade
    # save

手動で発信するには
connect 2
コマンドを使用します。
なお、mobile auto connect on を設定すると、パケット発生時に自動で発信させることも可能です。

26.3 IIJ モバイル / タイプ D で使用する場合の設定

[構成図]



[設定手順]

```
# mobile use usb1 on
# mobile type usb1 auto
# pp select 3
pp3# pp bind usb1
pp3# pp auth accept pap chap
pp3# pp auth myname xxxxx@iijmobile.jp yyyyy
pp3# ppp lcp mru off 1792
pp3# ppp lcp accm on
pp3# ppp lcp pfc on
pp3# ppp lcp acfc on
pp3# ppp ipcp ipaddress on
pp3# ppp ipcp msext on
pp3# ppp ipv6cp use off
pp3# ip pp nat descriptor 1000
pp3# mobile access-point name iijmobile.jp cid=2
pp3# mobile display caller id off
pp3# mobile access limit length off
pp3# mobile access limit time off
pp3# mobile disconnect time 600
pp3# pp enable 3
pp3# pp select none
# ip route default gateway pp 3
# dns server pp 3
# nat descriptor type 1000 masquerade
# save
```

[解説]

APNとして IIJ モバイルを指定し、CID 2 番に割り当てて発信します。
パケット通信量制限とパケット通信時間制限の制限を解除した場合の設定例です。

1. # mobile use usb1 on
   USB ポートをモバイルインターネット接続用に設定します。

2. # mobile type usb1 auto
   USB ポートに接続する携帯端末の種類を自動認識に設定します。

3. # pp select 3
   pp3# pp bind usb1
   USB ポートを pp3 にバインドします。

4. pp3# pp auth accept pap chap
   pp3# pp auth myname xxxxx@iijmobile.jp yyyyy
   IIJ モバイル契約の ID/Password を指定します。

5. pp3# ppp lcp mru off 1792
   通信量削減のため推奨します。
   pp3# ppp lcp accm on
   通信量削減のため推奨します。
   pp3# ppp lcp pfc on
   通信量削減のため推奨します。
   pp3# ppp lcp acfc on
   通信量削減のため推奨します。

6. pp3# ppp ipcp ipaddress on
   pp3# ppp ipcp msext on
   pp3# ppp ipv6cp use off
   pp3# ip pp nat descriptor 1000

7. pp3# mobile access-point name iijmobile.jp cid=2
   cid を 2 に割り当て pp3 は IIJ モバイルへの発信に設定します。

8. pp3# mobile display caller id off
   "186" を付けずに発信します。
   注 :IIJ モバイルでは off にしないと接続できません

9. pp3# mobile access limit length off
   累積パケット長の制限を解除します。
   IIJ モバイル／タイプ D のように完全定額制サービスの場合は制限を解除することも可能です。

10. pp3# mobile access limit time off
    累積通信時間の制限を解除します。
    IIJ モバイル／タイプ D のように完全定額制サービスの場合は制限を解除することも可能です。

11. pp3# mobile disconnect time 600
    600 秒間パケットの送受信がなければ切断するように設定します。

12. pp3# pp enable 3
    pp3# pp select none
    # ip route default gateway pp 3
    # dns server pp 3
    # nat descriptor type 1000 masquerade
    # save

本書は大豆油インクで印刷しています。
本書は無塩素紙(ECF:無塩素紙漂白パルプ)を使用しています。

WQ86300 0809 第9版