# YAMAHA
# REMOTE ROUTER
# RT52pro

## 設定例集

2001.7.3

# はじめに

この設定例集では、YAMAHA リモートルータ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

- **本書の記載内容の一部または全部を無断で転載することを禁じます。**
- **本書の記載内容は将来予告なく変更されることがあります。**
- **本製品を使用した結果発生した情報の消失等の損失については、当社では責任を負いかねます。保証は本製品物損の範囲に限ります。あらかじめご了承ください。**
- **本書の内容については万全を期して作成致しておりますが、記載漏れやご不審な点がございましたらご一報くださいますようお願い致します。**

## ご注意

**本機は、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。本機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。**

**YAMAHA リモートルータは「外国為替および外国貿易管理法」に基づいて規制される戦略物資（または役務）に該当します。このため、日本国外への持ち出しには、日本国政府の事前の許可等が必要です。**

### ●通信料金について

本機をダイヤルアップルータ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、YAMAHA REMOTE ROUTER RT300i、RT140 シリーズ、RT105i、RT52pro の総称を、YAMAHA リモートルータと記述しています。

## 商標について

# 目次

# 1.　コンソールと設定

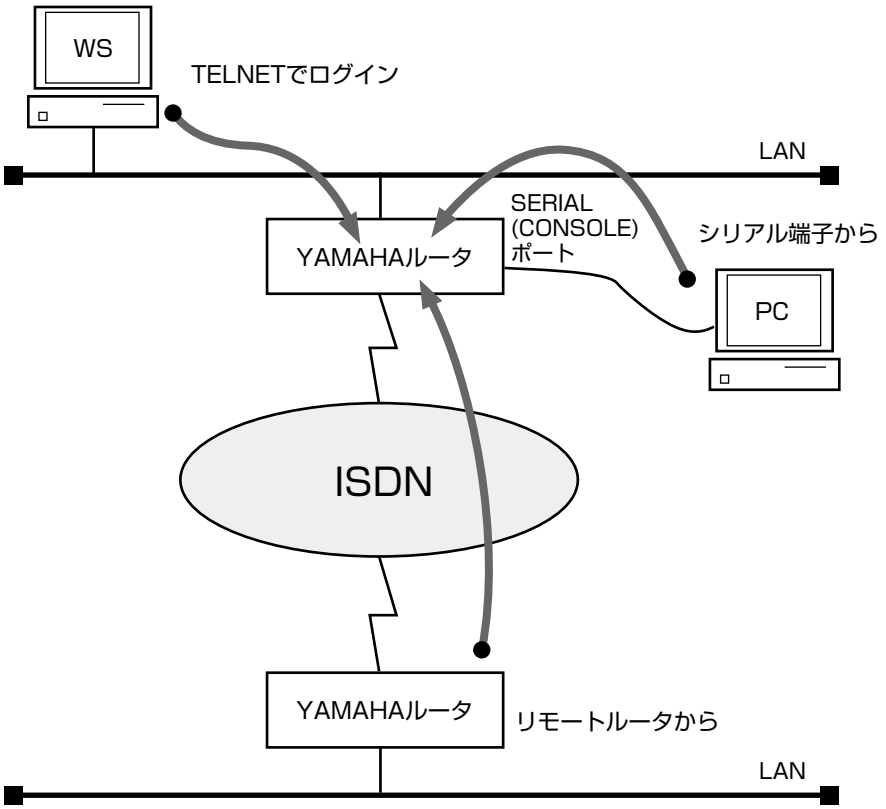
本章では、YAMAHA リモートルータに設定を行うための操作について簡単に説明します。ネットワークを構成するための具体的な設定例は第 2 章以降で説明します。本機のインストールや設定方法の詳細については取扱説明書をよくお読みください。

## 1.1　コンソールの位置付け

YAMAHA リモートルータ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 YAMAHA リモートルータからログインする方法の 3 つがあります。

| YAMAHA リモートルータへのアクセス方法 |
|---|
| YAMAHA リモートルータ本体の 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 YAMAHA リモートルータからログイン |

YAMAHA リモートルータへは、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 YAMAHA リモートルータ | 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 |
| 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 |
| ない | ない | シリアル端末 |

## 1.2　ヘルプ機能

YAMAHA リモートルータでは、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　設定操作の流れ

### 1.3.1　設定の開始から終了

設定の開始から終了までの流れを示します。
コンソールに表示する文字セットはデフォルトで SJIS 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。

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。

YAMAHA リモートルータの電源を ON にすると、ルータ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、RT52pro にログインした場合の表示です。

```
RT52pro Rev.4.02...
  Copyright (c) 1994-2001 Yamaha Corporation.
00:a0:de:00:4c:bd
Memory 8Mbytes, 1LAN, 1BRI
>
```

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。


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。YAMAHA リモートルータのセキュリティ上、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。


YAMAHA リモートルータ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。


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、**pp default** コマンドと **cold start** コマンドがあります。

| コマンド | 説明 |
|---|---|
| **pp default** | 指定した相手先情報の内容のみをデフォルトに戻します。 |
| **cold start** | 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。

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、Unnumbered )
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

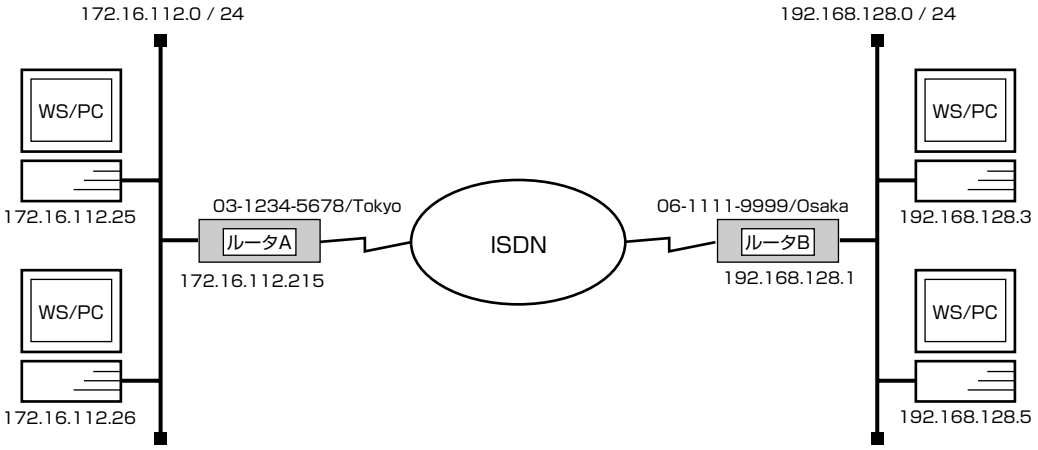
以下の説明では、それぞれのネットワークの接続形態例に対して構成図、手順、解説の順に行います。

**MEMO**

YAMAHA リモートルータを接続する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 lan address** コマンドで設定したYAMAHA リモートルータの**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 A の設定手順]

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

[ルータ B の設定手順]

```
# isdn local address 06-1111-9999/Osaka
# ip lan address 192.168.128.1/24
# ip route 172.16.112.0/24 gateway pp 1
# pp select 1
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に与えます。

ルータ A, ルータ 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 lan 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。

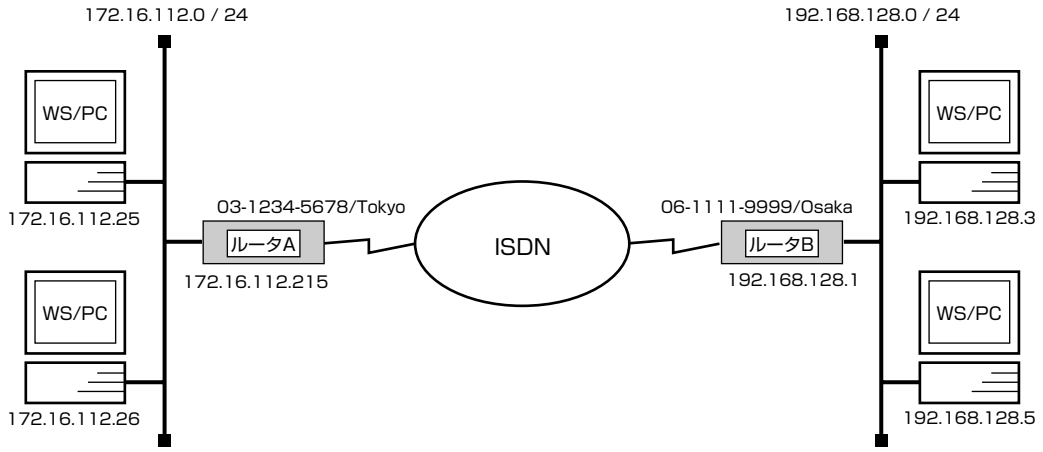
5. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、 サブアドレスを同時に設定する場合には、“/” に続けて入力します。

6. **pp 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。

## 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 A の設定手順]

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

[ルータ B の設定手順]

```
# isdn local address 06-1111-9999/Osaka
# ip lan address 192.168.128.1/24
# ip route 172.16.112.0/24 gateway pp 1
# pp select 1
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に与えます。

ルータ A, ルータ 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 lan 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. **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。

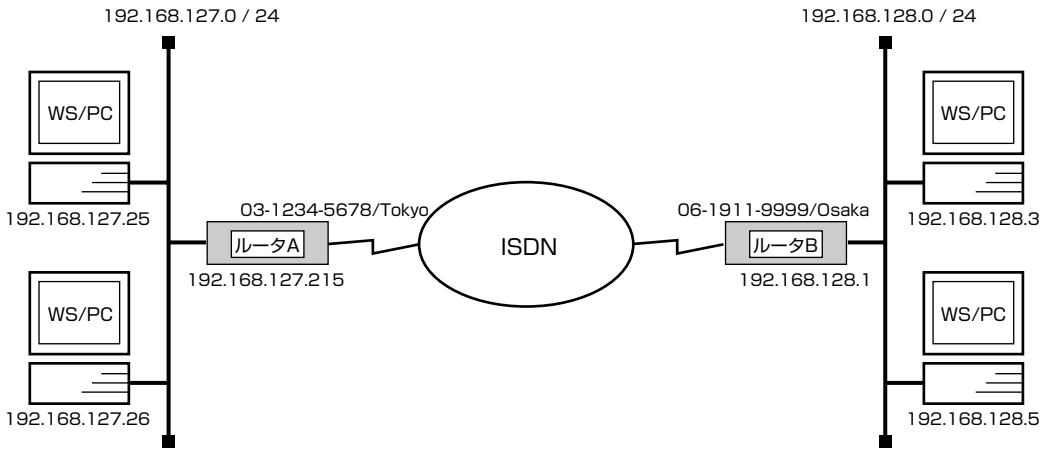
6. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

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。

## 2.3　ISDN 回線で LAN を接続 (PP 側は RIP2 を使用 )

[構成図]




[ルータ A の設定手順]

```
# isdn local address 03-1234-5678/Tokyo
# ip lan address 192.168.127.215/24
# pp select 1
pp1# isdn remote address call 06-1111-9999/Osaka
pp1# ip pp routing protocol rip2
pp1# ip pp hold routing on
pp1# pp enable 1
pp1# save
```

[ルータ B の設定手順]

```
# isdn local address 06-1111-9999/Osaka
# ip lan address 192.168.128.1/24
# pp select 1
pp1# isdn remote address call 03-1234-5678/Tokyo
pp1# ip pp routing protocol rip2
pp1# ip pp 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 B の設定手順を参照 )

■ルータ A

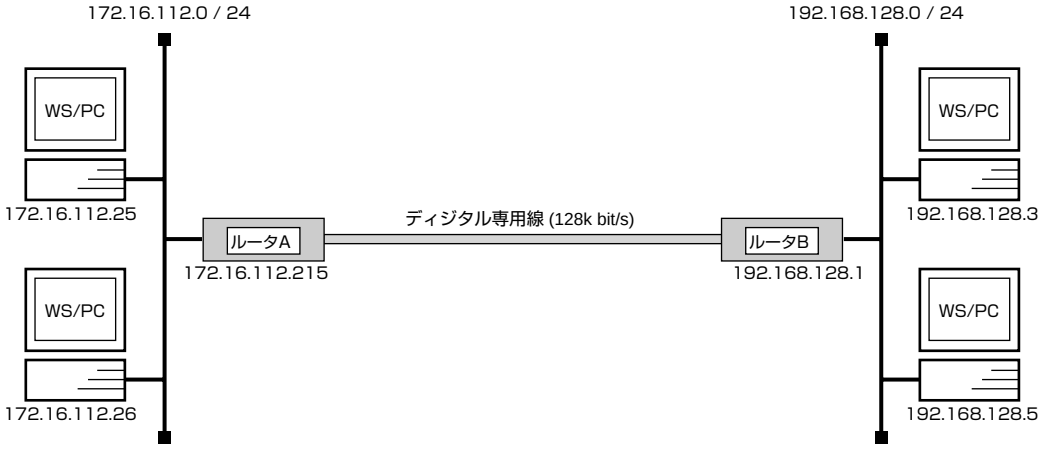
1. **isdn local address** コマンドを使用して、ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。
2. **ip lan address** コマンドを使用して、LAN 側の IP アドレスとネットマスクを設定します。
3. **pp select** コマンドを使用して、相手先情報番号を選択します。
4. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。
5. **ip pp routing protocol** 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。
6. **ip pp 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。
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 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 lan 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. **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。
5. **ip pp routing protocol** 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。
6. **ip pp 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。
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. **connect** コマンドを使用して、手動でルータ A に接続し、RIP 情報を取得します。この時、ルータ A は正しく設定されている必要があります。
10. **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 A の設定手順]

```
# pp line l128
# ip lan address 172.16.112.215/24
# ip route 192.168.128.0/24 gateway pp leased
# pp select leased
leased# pp enable leased
leased# save
leased# restart
```

[ルータ B の設定手順]

```
# pp line l128
# ip lan address 192.168.128.1/24
# ip route 172.16.112.0/24 gateway pp leased
# pp select leased
leased# pp enable leased
leased# save
leased# restart
```

[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。

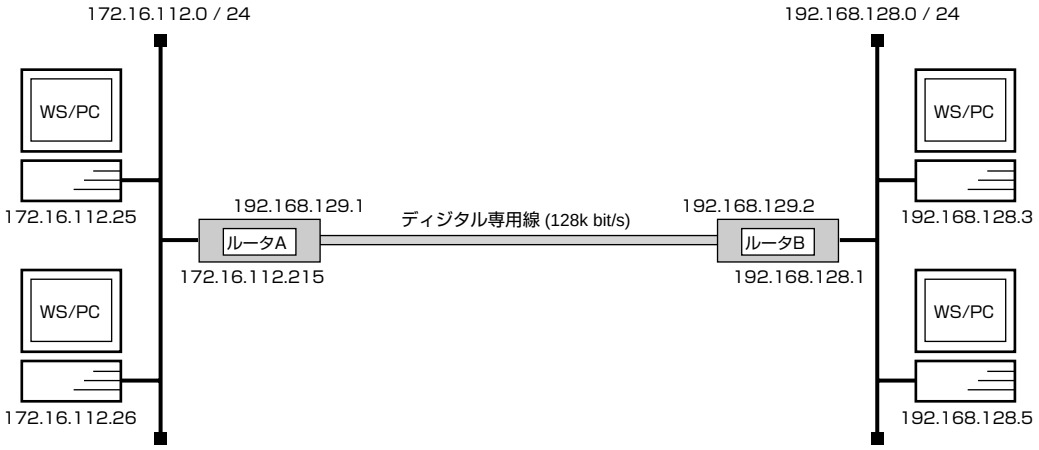
相手のネットワークへの経路情報はコマンドで設定する ( スタティックルーティング ) ことでそれぞれのルータに与えます。
なお、通常は PP 側に IP アドレスを設定する必要はありません。これを Unnumbered といいます。相手側のルータが IP アドレスを必要とする場合にだけ設定してください。

ルータ A, ルータ 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. **pp line** 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 lan 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 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。
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。
7. **restart** 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 A の設定手順]

```
# pp line l128
# ip lan address 172.16.112.215/24
# ip route 192.168.128.0/24 gateway pp leased
# pp select leased
leased# ip pp local address 192.168.129.1/24
leased# ip pp remote address 192.168.129.2
leased# pp enable leased
leased# save
leased# restart
```

[ルータ B の設定手順]

```
# pp line l128
# ip lan address 192.168.128.1/24
# ip route 172.16.112.0/24 gateway pp leased
# pp select leased
leased# ip pp local address 192.168.129.2/24
leased# ip pp remote address 192.168.129.1
leased# pp enable leased
leased# save
leased# restart
```

[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。

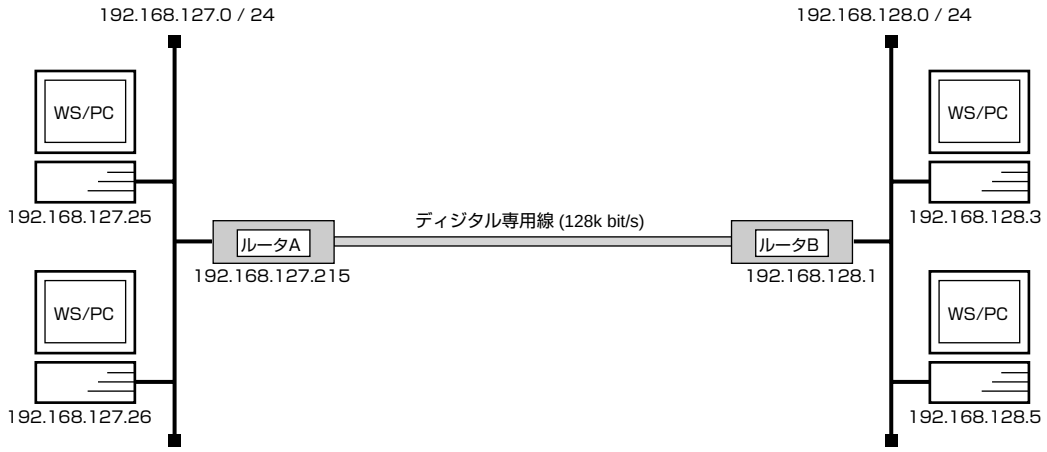
相手のネットワークへの経路情報はコマンドで設定する ( スタティックルーティング ) ことでそれぞれのルータに与えます。
構成図で示す例では、相手側のルータが IP アドレスを必要とするものとして設定しています。これを Numbered といいます。なお、通常は PP 側に IP アドレスを設定する必要はありません。

ルータ A, ルータ 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. **pp line** 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 lan 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. **ip pp local 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。
6. **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。
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. **restart** 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 A の設定手順]

```
# pp line l128
# ip lan address 192.168.127.215/24
# pp select leased
leased# ip pp routing protocol rip2
leased# ip pp rip connect send interval
leased# pp enable leased
leased# save
leased# restart
```

[ルータ B の設定手順]

```
# pp line l128
# ip lan address 192.168.128.1/24
# pp select leased
leased# ip pp routing protocol rip2
leased# ip pp rip connect send interval
leased# pp enable leased
leased# save
leased# restart
```

[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同士の通信 (RIP2) で行います。

ルータ A, ルータ 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. **pp line** 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 lan 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. **ip pp routing protocol** 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。

5. **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。

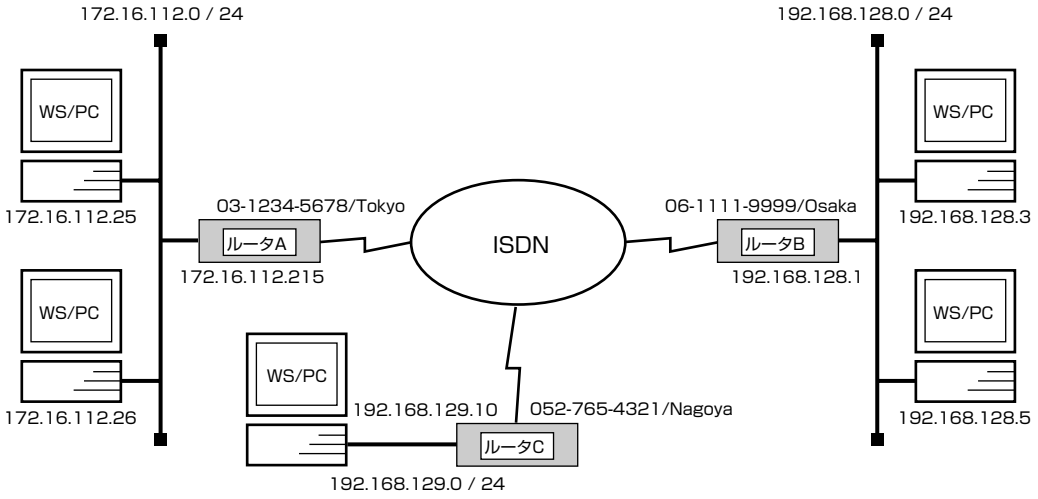
6. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

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。

8. **restart** 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 A の設定手順]

```
# isdn local address 03-1234-5678/Tokyo
# ip lan 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# isdn remote address call 06-1111-9999/Osaka
pp2# pp enable 2
pp2# pp select 3
pp3# isdn remote address call 052-765-4321/Nagoya
pp3# pp enable 3
pp3# save
```

[ルータ B の設定手順]

```
# isdn local address 06-1111-9999/Osaka
# ip lan 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# isdn remote address call 03-1234-5678/Tokyo
pp1# pp enable 1
pp1# pp select 3
pp3# isdn remote address call 052-765-4321/Nagoya
pp3# pp enable 3
pp3# save
```

[ルータ C の設定手順]

```
# isdn local address 052-765-4321/Nagoya
# ip lan 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# isdn remote address call 03-1234-5678/Tokyo
pp1# pp enable 1
pp1# pp select 2
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に与えます。1 台のルータには、その他の 2 地点のルータそれぞれに対する設定を行います。

ルータ A, ルータ B, ルータ 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 lan 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. **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 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. **pp select** コマンドを使用して、相手先情報番号を選択します。

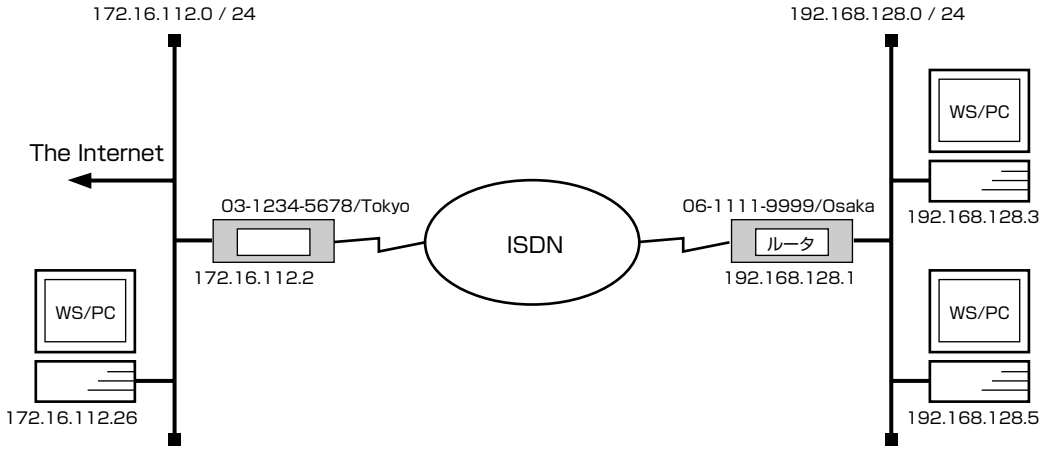
8. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/” に続けて入力します。

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。

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

［解説］

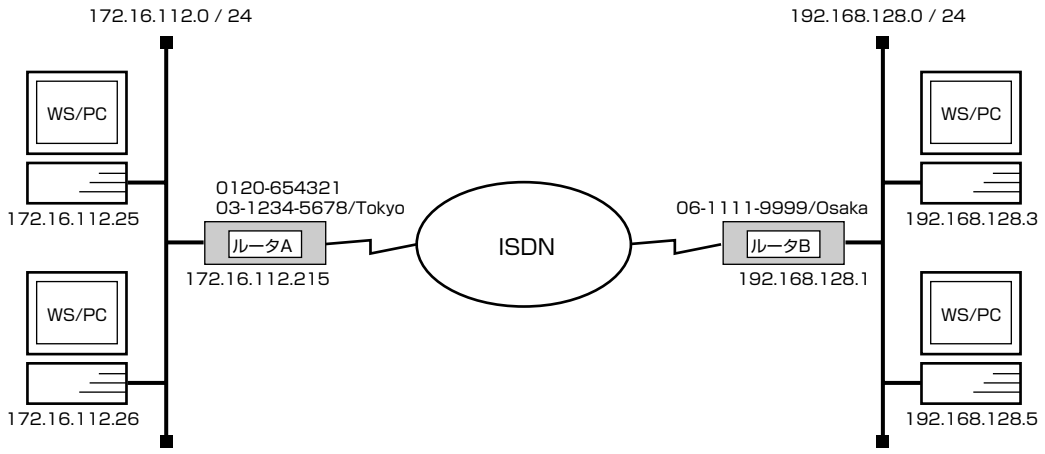
ネットワーク 192.168.128.0 をネットワーク 172.16.112.0 へ ISDN 回線によりデフォルトルート機能を使用して接続するための設定を説明します。

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 lan 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 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. **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 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。

## 2.9　フリーダイヤルで接続

［構成図］




［ルータ A の設定手順］

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

［ルータ B の設定手順］

```
# isdn local address 06-1111-9999/Osaka
# ip lan address 192.168.128.1
# ip route 172.16.112.0/24 gateway pp 1
# pp select 1
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 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 B からルータ 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 A からルータ B に発信する時の発番号には、ルータ A の契約者回線番号が使われます。従って、ルータ B では、ルータ A に発信する番号 ( フリーダイヤルの番号 ) とルータ 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に与えます。

■ルータ 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 lan 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. **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 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。

■ルータ 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 lan 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。

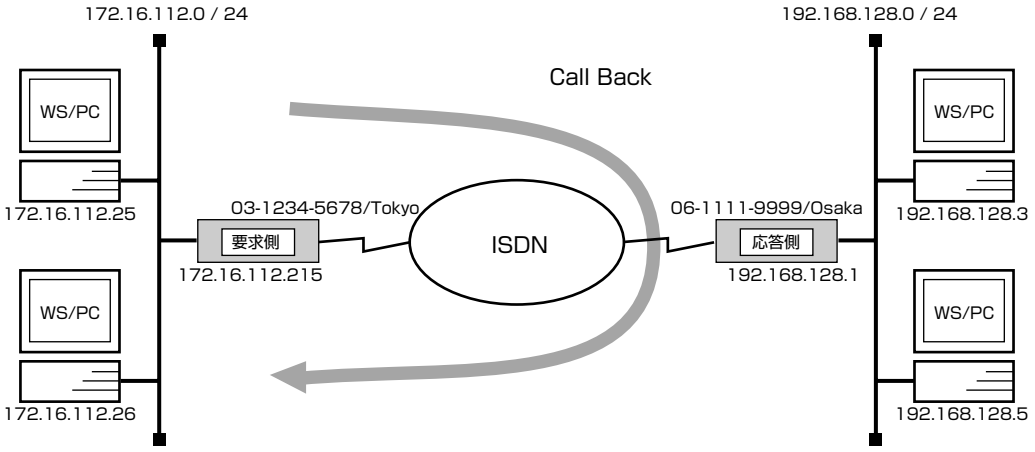
5. **isdn remote address** コマンドを使用して、ルータ A への発信用の番号 ( フリーダイヤルの 0120-654321) と着信用の番号 (03-1234-5678/Tokyo) を設定します。

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。

## 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の設定手順］

```
# isdn local address 03-1234-5678/Tokyo
# ip lan address 172.16.112.215/24
# ip route 192.168.128.0/24 gateway pp 1
# pp select 1
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の設定手順］

```
# isdn local address 06-1111-9999/Osaka
# ip lan address 192.168.128.1/24
# ip route 172.16.112.0/24 gateway pp 1
# pp select 1
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に与えます。

コールバック機能は、接続したい YAMAHA リモートルータ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 YAMAHA リモートルータ ( 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と、コールバックに応答するルータ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 lan 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. **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。

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。

■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 lan 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. **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。

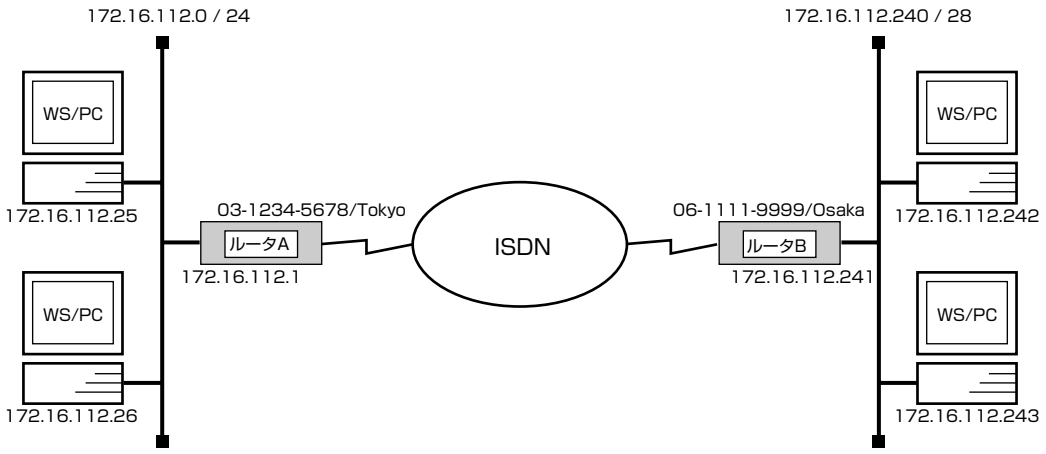
6. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、"/" に続けて入力します。

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。

## 2.11 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 A の設定手順]

```
# isdn local address 03-1234-5678/Tokyo
# ip lan 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 lan proxyarp on
# pp select 1
pp1# isdn remote address call 06-1111-9999/Osaka
pp1# pp enable 1
pp1# save
```

[ルータ B の設定手順]

```
# isdn local address 06-1111-9999/Osaka
# ip lan address 172.16.112.241/28
# ip route default gateway pp 1
# pp select 1
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 A |
| 172.16.112.2<br>:<br>172.16.112.239 | ホスト (238 台分 ) |
| 172.16.112.240<br>:<br>172.16.112.254 | ルータ B の<br>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 B |
| 172.16.112.242<br>:<br>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 A は Proxy ARP を使用して、ルータ B の LAN との通信を行います。ルータ 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 A に向けておきます。

■ルータ 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 lan 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。
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 B に流れることになります。

4. **ip lan 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。

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. **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 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 lan 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。

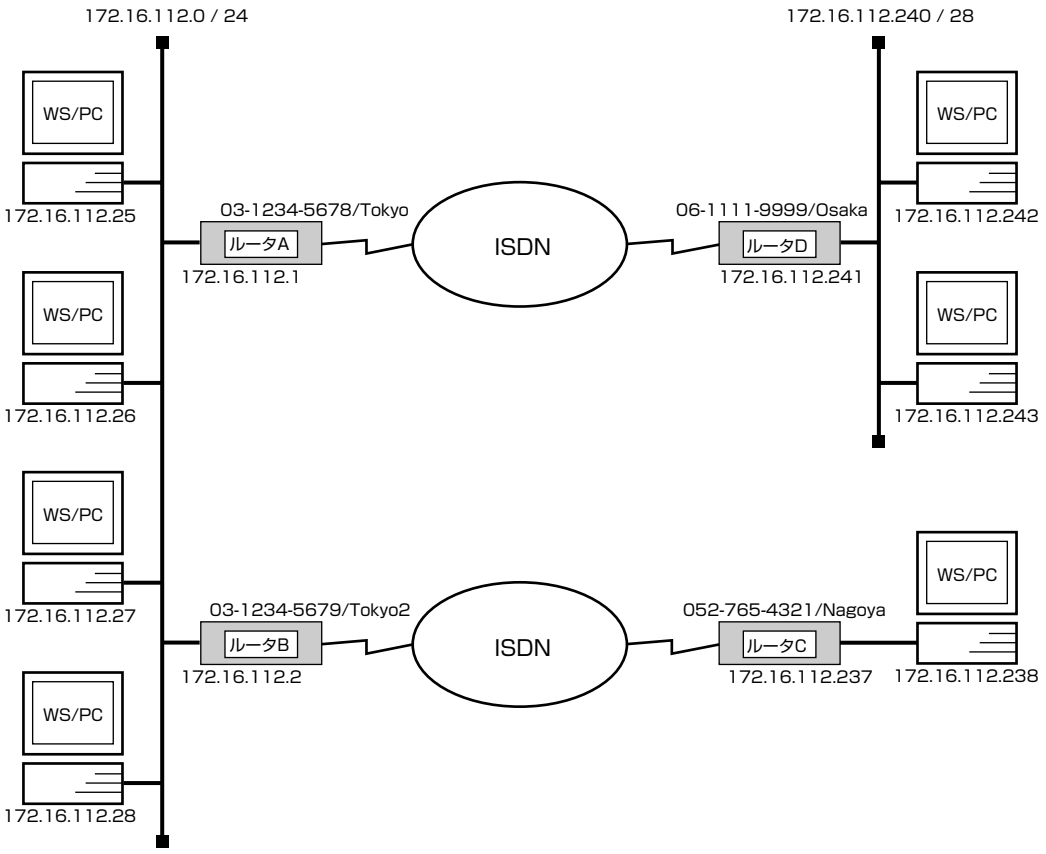
5. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、"/" に続けて入力します。

6. **pp 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。

## 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 A の設定手順］

```
# isdn local address 03-1234-5679/Tokyo
# ip lan 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 lan proxyarp on
# pp select 1
pp1# isdn remote address call 06-1111-9999/Osaka
pp1# pp enable 1
pp1# save
```

[ルータ B の設定手順]

```
# isdn local address 03-1234-5679/Tokyo2
# ip lan 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 enable 1
pp1# save
```

[ルータ C の設定手順]

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

[ルータ D の設定手順]

```
# isdn local address 06-1111-9999/Osaka
# ip lan address 172.16.112.241/28
# ip route default gateway pp 1
# pp select 1
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 A |
| 172.16.112.2 | ルータ B |
| 172.16.112.3<br>:<br>172.16.112.235 | ホスト (233 台分 ) |
| 172.16.112.236<br>:<br>172.16.112.239 | ルータ C の<br>ネットワーク |
| 172.16.112.240<br>:<br>172.16.112.254 | ルータ D の<br>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 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 D |
| 172.16.112.242<br>:<br>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 A とルータ B は Proxy ARP を使用して、それぞれルータ D とルータ C の LAN との通信を行います。ルータ C とルータ 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 B 、ルータ A に向けておきます。
なお、ルータ 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 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 A およびルータ 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 lan 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 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 D に流れることになります。

4. **ip lan 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。

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. **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 C およびルータ 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 lan 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。

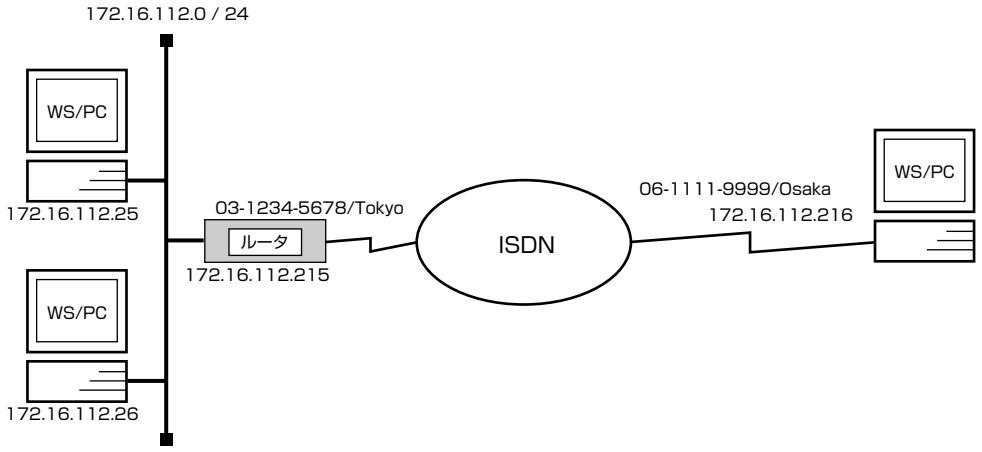
5. **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、“/”に続けて入力します。

6. **pp 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。

## 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 03-1234-5678/Tokyo
# ip lan address 172.16.112.215/24
# ip lan proxyarp on
# pp select 1
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 lan 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 lan 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. **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。

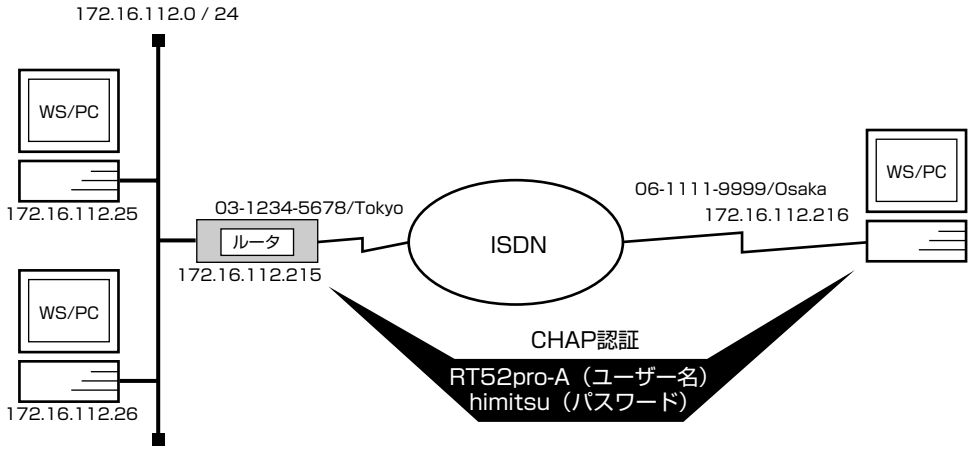
6. **ip pp remote address** コマンドを使用して、選択した PP 側のリモート IP アドレスを設定します。パーソナルコンピュータやワークステーションの方で設定されていればその IP アドレスを設定します。

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。

## 2.14 端末型機器（TA、ISDN ボード等）との接続 ( 相手は不特定 )

［構成図］




［ルータの設定手順］

```
# isdn local address 03-1234-5678/Tokyo
# ip lan address 172.16.112.215/24
# ip lan proxyarp on
# pp select anonymous
anonymous# ip pp remote address pool 172.16.112.216 172.16.112.217
anonymous# pp auth request chap
anonymous# pp auth username RT52pro-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、YAMAHA リモートルータの方から 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“RT52pro-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 lan 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 lan 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. **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。

6. **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。

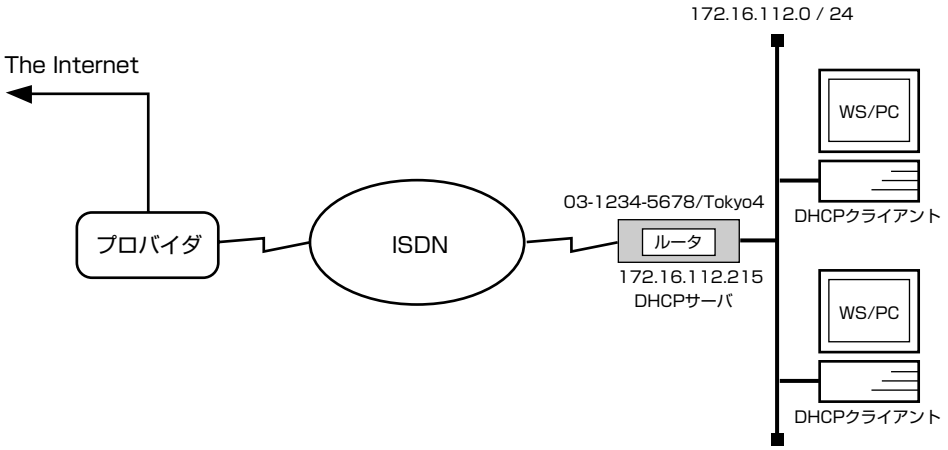
7. **pp auth username** コマンドを使用して、CHAP のユーザ名とパスワードを設定します。

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。

## 2.15 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 03-1234-5678/Tokyo
# ip lan address 172.16.112.215/24
# ip route default gateway pp 1
# nat descriptor type 1 masquerade
# pp select 1
pp1# isdn remote address call 06-1111-9999/Osaka
pp1# isdn call block time 15
pp1# isdn disconnect policy 2
pp1# ip pp nat descriptor 1
pp1# pp auth accept pap chap
pp1# pp auth myname RT52pro-A himitsu
pp1# ppp ipcp ipaddress on
pp1# ppp ipcp msext on
pp1# pp enable 1
pp1# dhcp service server
pp1# dhcp scope 1 172.16.112.1-172.16.112.214/24
pp1# dns server pp 1
pp1# dns private address spoof on
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“RT52pro-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 defauly 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 lan 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. **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. **isdn call block time** コマンドを使用して、再発信の抑制タイマを設定します。

8. **isdn disconnect policy** コマンドを使用して、ISDN 回線を切断するタイマ方式を設定します。2 に設定することで、課金単位時間方式となり、通信料金を減らす効果が期待できます。

9. **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。

10. **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。

11. **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。

12. **ppp ipcp ipaddress** コマンドを使用して、PP 側の 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ます。

13. **ppp ipcp msext** コマンドを使用して、IPCP の MS 拡張オプションを使うように設定します。DNS サーバのアドレスを通知してもらうようにします。

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. **dhcp service** コマンドを使用して、LAN 側に対して DHCP サーバを設定します。各端末は DHCP サーバからアドレスを取得します。

16. **dhcp scope** コマンドを使用して、各端末に割り当てるアドレスの範囲を設定します。

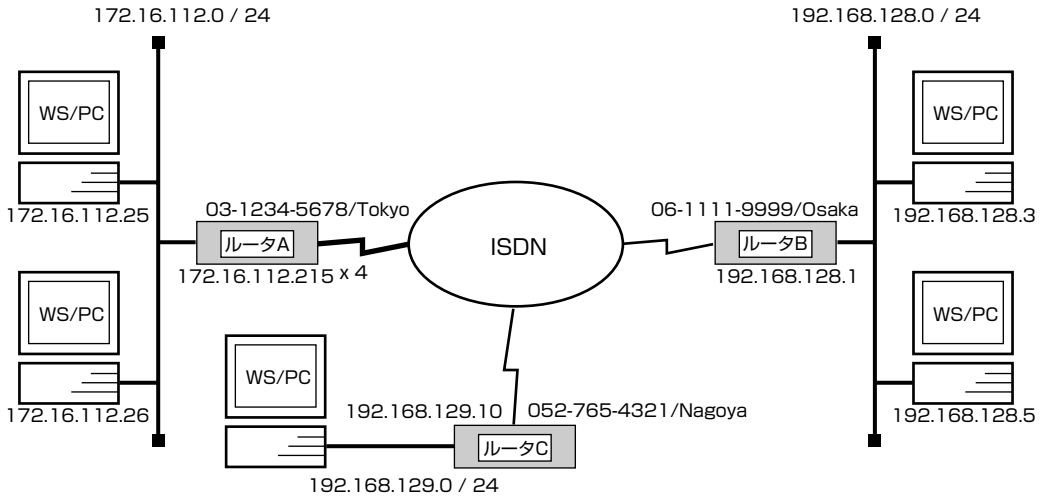
17. **dns server pp** コマンドを使用して、DNS サーバを通知してもらう相手先情報番号を設定します。

18. **dns private address spoof** コマンドを使用して、プライベートアドレスに対する問い合わせを上位サーバに転送しないように設定します。

19. **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 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 B の設定手順 ]

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

[ ルータ C の設定手順 ]

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

[解説]

センター側に複数 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 YAMAHA リモートルータと 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 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 lan 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 bri** 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、接続先のネットワークへの経路を設定します。

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 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 lan 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. **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. **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 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 lan 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. **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. **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。

# 3.　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。

## 3.1　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。

### [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。

## 3.2　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。

**[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。

## 3.3　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。

### [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。

## 3.4 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。

**[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。

## 3.5　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。

**[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。

## 3.6 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。

**[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。

## 3.7　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。

**[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。

## 3.8 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。

**[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。

## 3.9　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。

**[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。

## 3.10 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。

### [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。

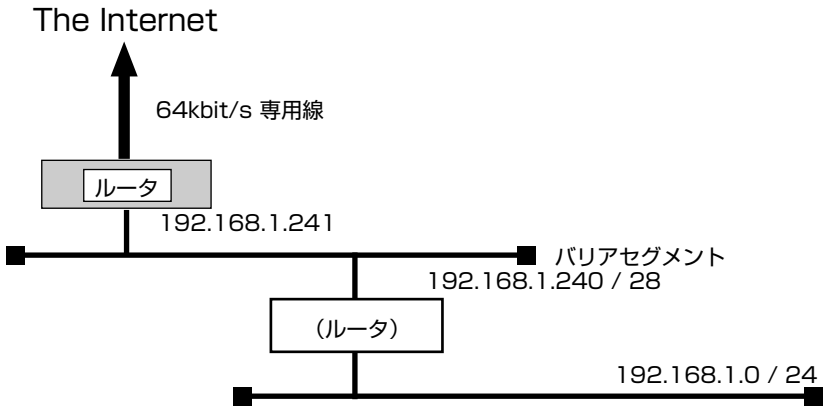
3. **ip pp rip filter** コマンドを使用して、相手先情報番号 1 の相手に対して RIP 情報のフィルタをかけます。PP 側の出口でフィルタをかけるので“**out**”を指定します。また、フィルタは 1, 2 の順番でかけるように指定します。

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。

## 3.11 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 YAMAHA リモートルータで行い、バリアセグメントとサイト内を結ぶルータには特にセキュリティに関する設定は行わない

[手順]

```
# pp line l64
# ip lan address 192.168.1.241/28
# ip route default gateway pp leased
# 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,
   domain,gopher,finger,www,nntp,ntp,33434-33500
# ip filter source-route on
# ip filter directed-broadcast on
# pp select leased
leased# ip pp secure filter in 10 11 12 13 14 15 16
leased# pp enable leased
leased# syslog host 192.168.1.242
leased# syslog notice on
leased# save
leased# restart
```

[解説]

1. **pp line** 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 lan 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. **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。

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. **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。

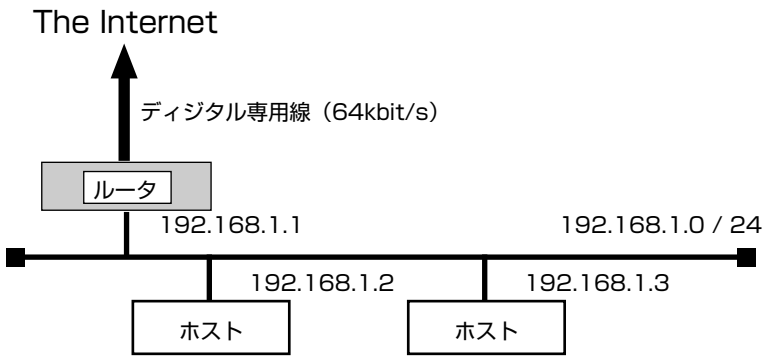
12. **save** コマンドを使用して、以上の設定を不揮発性メモリに書き込みます。

13. **restart** 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。

## 3.12 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 YAMAHA リモートルータで行う

### [手順]

```
# pp line l64
# ip lan address 192.168.1.1/24
# ip route default gateway pp leased
# 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 * telnet,smtp,domain,
   gopher,finger,www,nntp,ntp,33434-33500
# ip filter source-route on
# ip filter directed-broadcast on
# pp select leased
leased# ip pp secure filter in 10 11 12 13 14 15 16
leased# pp enable leased
leased# syslog host 192.168.1.3
leased# syslog notice on
leased# save
leased# restart
```

[解説]

1. **pp line** 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 lan 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. **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。

9. **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。

10. **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。

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. **restart** 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. 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。

## 4.1　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`**
   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。

## 4.2　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 30 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。

## 4.3　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。

## 4.4　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 ]

```
# pp line l128
# ip lan address 192.168.1.241/28
# ip route default gateway pp leased
# 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
# 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 4 pass * * tcp * smtp,pop3
# ip filter 5 pass * * tcp * ident
# ip filter dynamic 4 * * filter 4 in 5
# ip filter dynamic 10 * * tcp
# ip filter dynamic 11 * * udp
# ip filter source-route on
# ip filter directed-broadcast on
# pp select leased
leased# ip pp secure filter in 1 2 3 4 dynamic 20 21 22 30 31
leased# ip pp secure filter out dynamic 1 2 3 4 10 11
leased# pp enable leased
leased# pp select none
# syslog host 192.168.1.242
# syslog notice on
# save
# restart
```

[ 解説 ]

1. **# pp linel128**
   回線種別を設定します。この設定は装置の再起動を行った後に有効になります。

2. **# ip lan address 192.168.1.241/28**
   **# ip route default gateway pp leased**
   **# 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 * tel-net,smtp,gopher,finger,**

```
 www,nntp
# 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 4 pass * * tcp * smtp,pop3**
   **# ip filter 5 pass * * tcp * ident**
   **# ip filter dynamic 4 * * filter 4 in 5**
   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 4 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 5 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 30 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 leased**
   **leased# ip pp secure filter in 1 2 3 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. **leased# 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. **leased# pp enablee leased**
    **leased# pp select none**
    **# syslog host 192.168.1.242**
    **# syslog notice on**
    **# save**
    **# restart**
    回線種別が設定変更前と異なるので **restart** コマンドによって装置を再起動します。

## 4.5　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 ]

```
# pp line l128
# ip lan address 192.168.1.1/24
# ip route default gateway pp leased
# 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,fin-
   ger,
 www,nntp
# 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 4 pass * * tcp * smtp,pop3
# ip filter 5 pass * * tcp * ident
# ip filter dynamic 4 * * filter 4 in 5
# ip filter dynamic 10 * * tcp
# ip filter dynamic 11 * * udp
# ip filter source-route on
# ip filter directed-broadcast on
# pp select leased
leased# ip pp secure filter in 1 2 3 4 dynamic 20 21 22 30 31
leased# ip pp secure filter out dynamic 1 2 3 4 10 11
leased# pp enable leased
leased# pp select none
# syslog host 192.168.1.3
# syslog notice on
# save
# restart
```

[ 解説 ]

1. **# pp line l128**
   回線種別を設定します。この設定は装置の再起動を行った後に有効になります。

2. **# ip lan address 192.168.1.1/24**
   **# ip route default gateway pp leased**
   **# 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 * 192.168.1.2 established * telnet,smtp,gopher,fin-**
   **ger,www,nntp**
   **# ip filter 4 pass * 192.168.1.2 tcp,udp * telnet,smtp,gopher,fingerwww,**

**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 4 pass * * tcp * smtp,pop3**
   **# ip filter 5 pass * * tcp * ident**
   **# ip filter dynamic 4 * * filter 4 in 5**
   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 4 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 5 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 30 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  leased**
   **leased# ip pp secure filter in 1 2 3 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. **leased# 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. **leased# pp enable leased**
    **leased# pp select none**
    **# syslog host 192.168.1.3**
    **# syslog notice on**
    **# save**
    **# restart**
    回線種別が設定変更前と異なるので **restart** コマンドによって装置を再起動します。

# 5. 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。

## 5.1 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。

## 5.2 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。

## 5.3 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。

# 6. 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 uthentication 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

## 6.1　どちらか一方で PAP を用いる場合

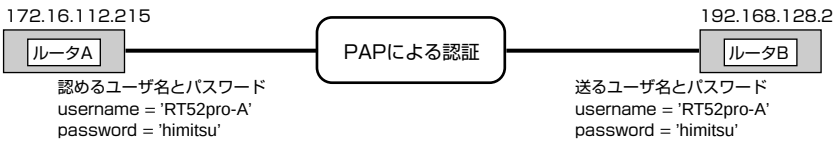
[認証の設定条件]

・ルータ A が認証するなら PAP だけである

・ルータ A が認めるルータ B のユーザ名は 'RT52pro-A' であり、かつそのパスワードは 'himitsu' である

・ルータ B は PAP 認証を認める

・ルータ B がルータ A に送るユーザ名は 'RT52pro-A' であり、かつそのパスワードは 'himitsu' である




[ルータ A ( 認証する側 ) の設定手順]

```
# pp select 1
pp1# pp auth request pap
pp1# pp auth username RT52pro-A himitsu
pp1# pp enable 1
pp1# save
```

[ルータ B ( 認証される側 ) の設定手順]

```
# pp select 1
pp1# pp auth accept pap
pp1# pp auth myname RT52pro-A himitsu
pp1# pp enable 1
pp1# save
```

## 6.2　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 RT52pro-A himitsu
pp1# pp auth username RT52pro-A himitsu
pp1# pp enable 1
pp1# save
```

## 6.3　どちらか一方で CHAP を用いる場合

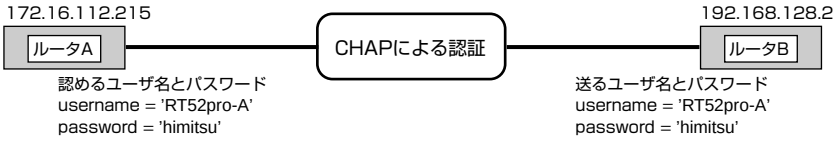
［認証の設定条件］

・ルータ A が認証するなら CHAP だけである

・ルータ A が認めるルータ B のユーザ名は 'RT52pro-A' であり、かつそのパスワードは 'himitsu' である

・ルータ B は CHAP 認証を認める

・ルータ B がルータ A に送るユーザ名は 'RT52pro-A' であり、かつそのパスワードは 'himitsu' である




［ルータ A ( 認証する側 ) の設定手順］

```
# pp select 1
pp1# pp auth request chap
pp1# pp auth username RT52pro-A himitsu
pp1# pp enable 1
pp1# save
```

［ルータ B ( 認証される側 ) の設定手順］

```
# pp select 1
pp1# pp auth accept chap
pp1# pp auth myname RT52pro-A himitsu
pp1# pp enable 1
pp1# save
```

## 6.4　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。

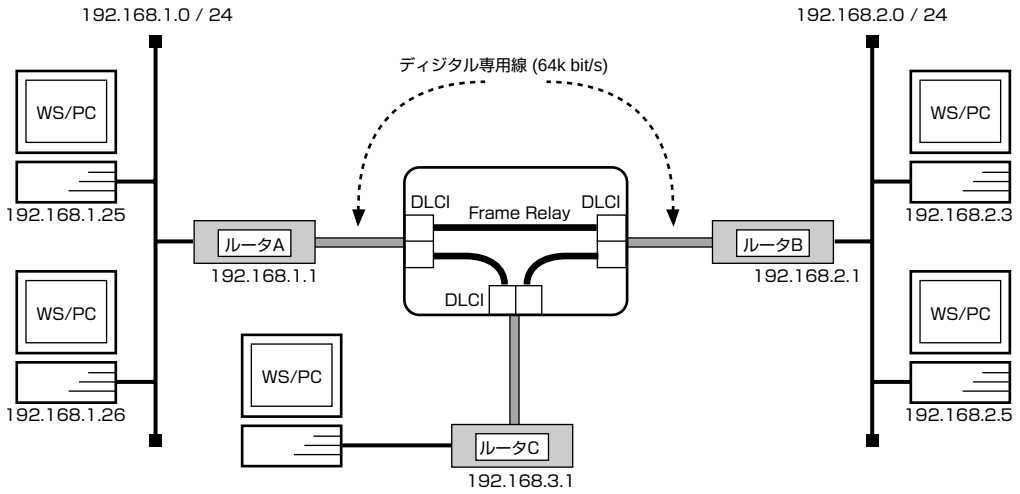
**[認証の設定手順]**

```
# pp select 1
pp1# pp auth request chap
pp1# pp auth accept chap
pp1# pp auth myname RT52pro-A himitsu
pp1# pp auth username RT52pro-A himitsu
pp1# pp enable 1
pp1# save
```

# 7. フレームリレー設定例

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

[構成図]




[ルータ A の設定手順]

```
# pp line l64
# ip lan address 192.168.1.1/24
# pp select leased
leased# pp encapsulation fr
leased# ip pp routing protocol rip2
leased# ip pp rip connect send interval
leased# pp enable leased
leased# save
```

[ルータ B の設定手順]

```
# pp line l64
# ip lan address 192.168.2.1/24
# pp select leased
leased# pp encapsulation fr
leased# ip pp routing protocol rip2
leased# ip pp rip connect send interval
leased# pp enable leased
leased# save
```

### [ルータ C の設定手順]

```
# pp line l64
# ip lan address 192.168.3.1/24
# pp select leased
leased# pp encapsulation fr
leased# ip pp routing protocol rip2
leased# ip pp rip connect send interval
leased# pp enable leased
leased# save
```

### [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. **pp line** 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 lan 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 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。

5. **ip pp routing protocol** コマンドを使用して、回線側に RIP2 を流すようにします。

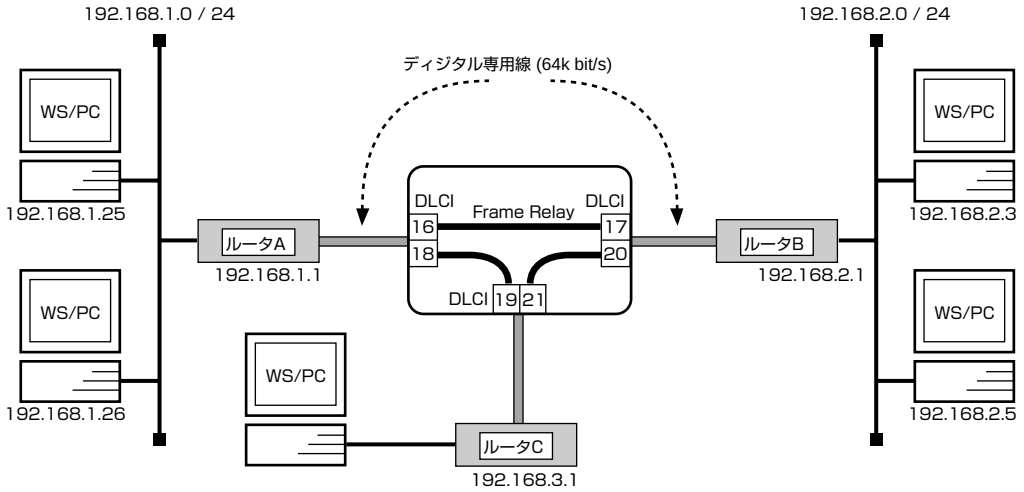
6. **ip pp rip connect send** コマンドを使用して、回線接続時の RIP の送出を **ip pp rip connect interval** コマンドで設定されている時間間隔で行うように設定します。この時間間隔はデフォルトでは 30 秒です。

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。

## 7.2　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 A の設定手順]

```
# pp line l64
# ip lan 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 leased
leased# pp encapsulation fr
leased# pp enable leased
leased# save
```

[ルータ B の設定手順]

```
# pp line l64
# ip lan address 192.168.2.1/24
# ip route 192.168.1.0/24 gateway pp leased dlci=17
# ip route 192.168.3.0/24 gateway pp leased dlci=20
# pp select leased
leased# pp encapsulation fr
leased# pp enable leased
leased# save
```

### [ルータ C の設定手順]

```
# pp line l64
# ip lan 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 leased
leased# pp encapsulation fr
leased# pp enable leased
leased# save
```

### [解説]

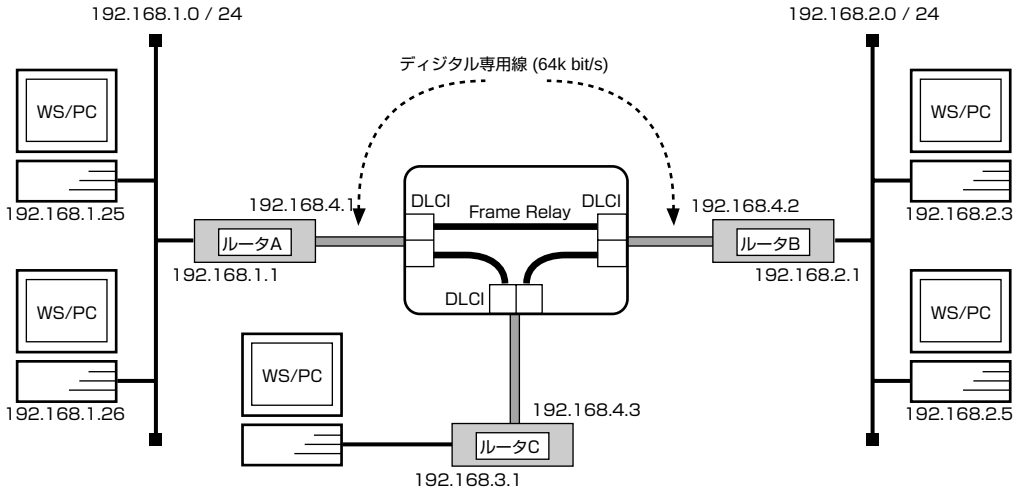
ネットワーク 192.168.1.0 とネットワーク 192.168.2.0 、ネットワーク 192.168.3.0 を 64kbit/s のディジタル専用線をアクセス回線とするフレームリレーで接続するための設定を説明します。

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. **pp line** 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 lan 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 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. **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。

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

[構成図]




[ルータ A の設定手順]

```
# pp line l64
# ip lan address 192.168.1.1/24
# pp select leased
leased# pp encapsulation fr
leased# ip pp local address 192.168.4.1/24
leased# ip pp routing protocol rip2
leased# ip pp rip connect send interval
leased# pp enable leased
leased# save
```

[ルータ B の設定手順]

```
# pp line l64
# ip lan address 192.168.2.1/24
# pp select leased
leased# pp encapsulation fr
leased# ip pp local address 192.168.4.2/24
leased# ip pp routing protocol rip2
leased# ip pp rip connect send interval
leased# pp enable leased
leased# save
```

### [ルータ C の設定手順]

```
# pp line l64
# ip lan address 192.168.3.1/24
# pp select leased
leased# pp encapsulation fr
leased# ip pp local address 192.168.4.3/24
leased# ip pp routing protocol rip2
leased# ip pp rip connect send interval
leased# pp enable leased
leased# save
```

### [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. **pp line** 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 lan 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 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 local 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 routing protocol** 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。

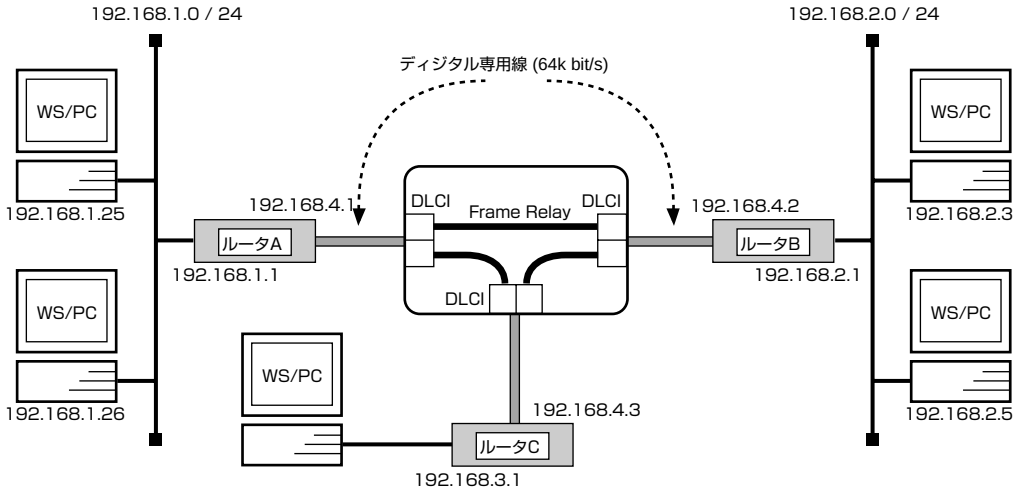
8. **ip pp rip connect send** コマンドを使用して、回線接続時の RIP の送出を **ip pp rip connect interval** コマンドで設定されている時間間隔で行うように設定します。この時間間隔はデフォルトでは 30 秒です。

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。

## 7.4　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 A の設定手順]

```
# pp line l64
# ip lan 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 leased
leased# pp encapsulation fr
leased# ip pp local address 192.168.4.1/24
leased# pp enable leased
leased# save
```

[ルータ B の設定手順]

```
# pp line l64
# ip lan 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 leased
leased# pp encapsulation fr
leased# ip pp local address 192.168.4.2/24
leased# pp enable leased
leased# save
```

### [ルータ C の設定手順]

```
# pp line l64
# ip lan 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 leased
leased# pp encapsulation fr
leased# ip pp local address 192.168.4.3/24
leased# pp enable leased
leased# save
```

### [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. **pp line** 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 lan 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 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 local 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。
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。

# 8. DHCP 機能設定例

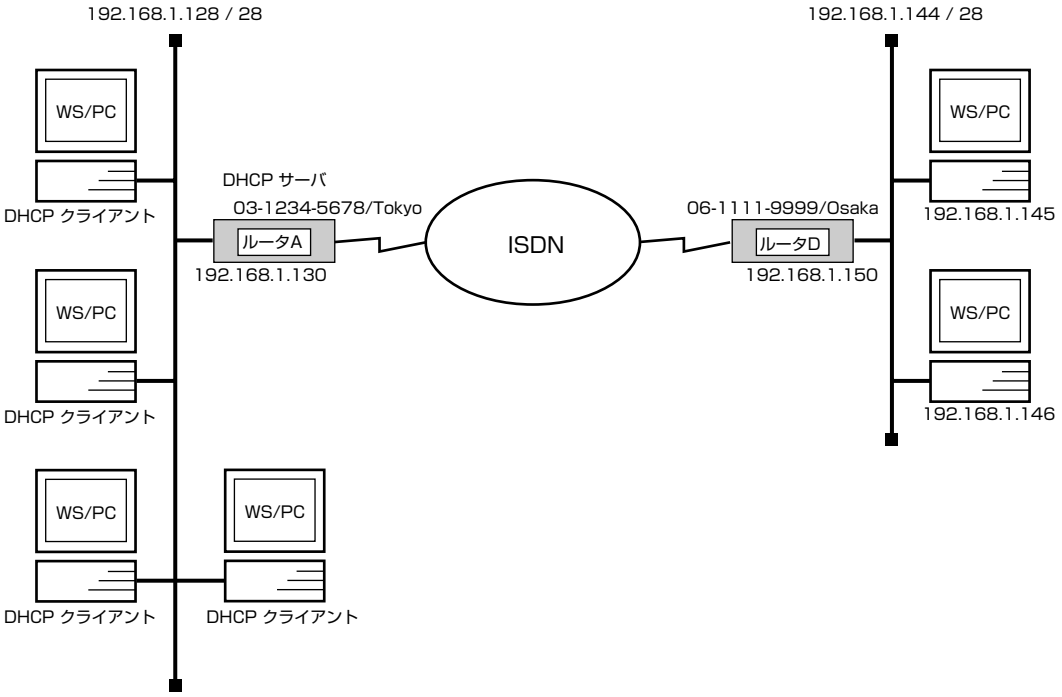
本章で説明するネットワーク接続の形態は、次のようになります。

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

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。

## 8.1　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 A の設定手順］

```
# isdn local address 03-1234-5678/Tokyo
# ip lan 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# isdn remote address call 06-1111-9999/Osaka
pp1# pp enable 1
pp1# save
```

［ルータ B の設定手順］

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

[解説]

ルータ 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 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 サーバルータの LAN インタフェース |
| 192.168.1.131<br>:<br>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 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 lan 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. **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 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 lan 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。

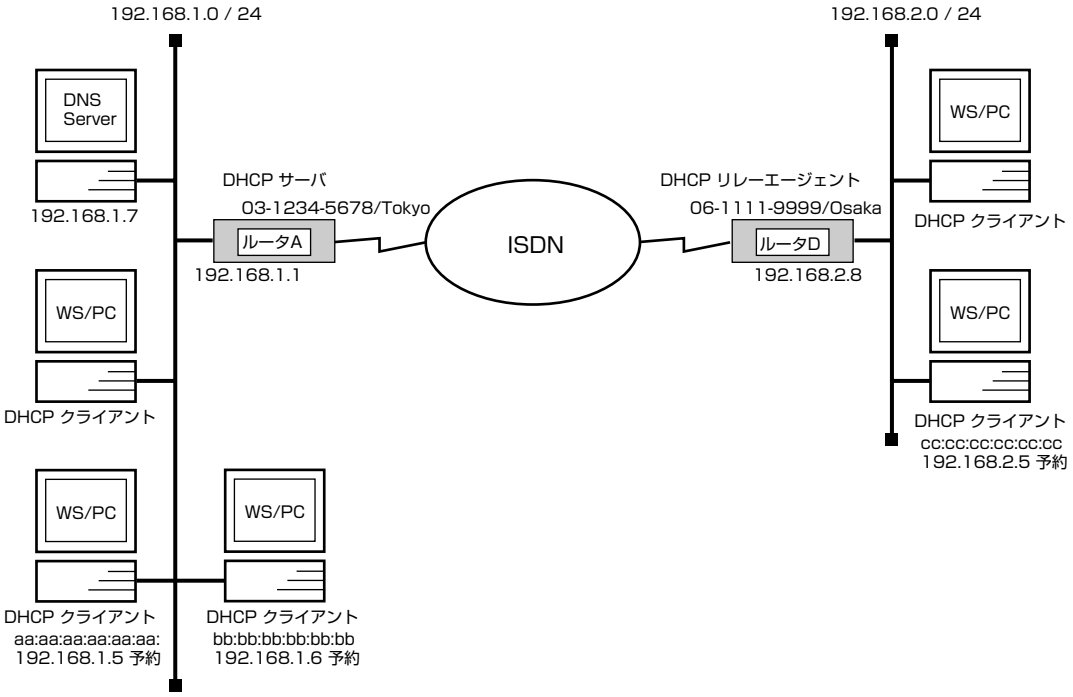
5 **isdn remote address** コマンドを使用して、選択した相手先の ISDN 番号を設定します。市外局番を忘れないようにしてください。また、サブアドレスを同時に設定する場合には、"/" に続けて入力します。

6. **pp 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。

## 8.2　２つのネットワークで DHCP 機能を利用

［構成図］




［ルータ A の設定手順］

```
# isdn local address 03-1234-5678/Tokyo
# ip lan 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# isdn remote address call 06-1111-9999/Osaka
pp1# pp enable 1
pp1# save
```

[ルータ B の設定手順]

```
# isdn local address 06-1111-9999/Osaka
# ip lan 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# isdn remote address call 03-1234-5678/Tokyo
pp1# pp enable 1
pp1# save
```

[解説]

ルータ 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 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 サーバルータの LAN インタフェース | − |
| 192.168.1.2<br>:<br>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<br>:<br>192.168.1.64 | DHCP クライアント (57 台分 ) | 1 |
| 192.168.1.65<br>:<br>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<br>:<br>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の LAN インタフェース | − |
| 192.168.2.9<br>:<br>192.168.2.32 | DHCP クライアント (24 台分 ) | 2 |
| 192.168.2.33<br>:<br>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 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 lan 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。
1 番目の書式で、DHCP パケットの中に Client-Identifier オプションを付けてこない DHCP クライアントへのアドレスを予約します。識別には MAC アドレスを利用します。2、3 番目の書式で、DHCP パケットの中に Client-Identifier オプションを付けてくる DHCP クライアントへのアドレを予約します。識別には Client-Identifier を利用します。

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. **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. **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。

■ルータ 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 lan 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。

# 9. IPsec 機能設定例

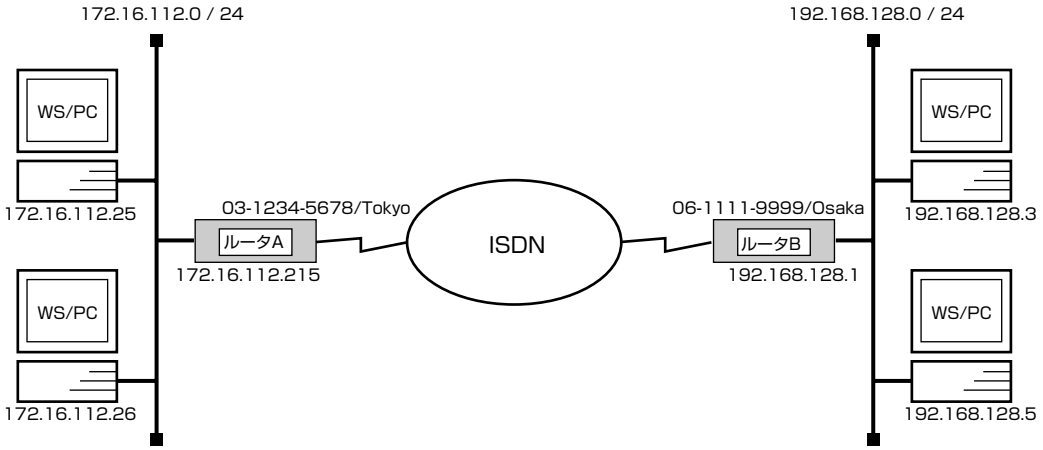
本章で説明するネットワーク接続の形態は、次のようになります。

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。

## 9.1　トンネルモードを利用して LAN を接続

［構成図］




［ルータ A の設定手順］

```
# isdn local address 03-1234-5678/Tokyo
# ip lan 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# 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 B の設定手順]

```
# isdn local address 06-1111-9999/Osaka
# ip lan 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# 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 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 lan 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. **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. **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. **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。

12. **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。

13. **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。

14. **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。

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。

■ルータ 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 lan 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. **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. **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. **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。

12. **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。

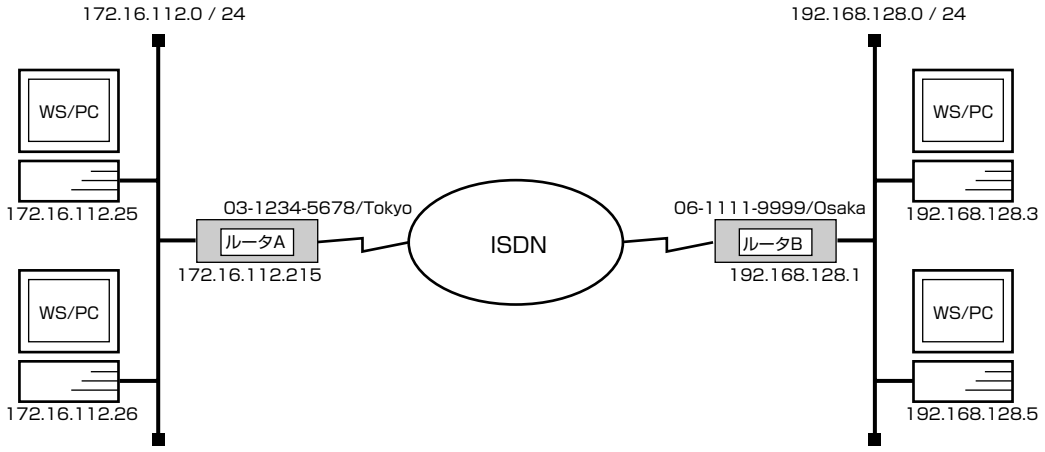
13. **tunnel enable** コマンドを使用して、トンネルインタフェースを有効にします。

14. **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。

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。

## 9.2　トランスポートモードの利用

［構成図］




［ルータ A の設定手順］

```
# isdn local address 03-1234-5678/Tokyo
# ip lan 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# isdn remote address call 06-1111-9999/Osaka
pp1# pp enable 1
pp1# save
```

［ルータ B の設定手順］

```
# isdn local address 06-1111-9999/Osaka
# ip lan 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# save
```

［解説］

IP アドレス 172.16.112.215 のルータ A と IP アドレス 192.168.128.1 のルータ 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 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 lan 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. **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 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 lan 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. **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。

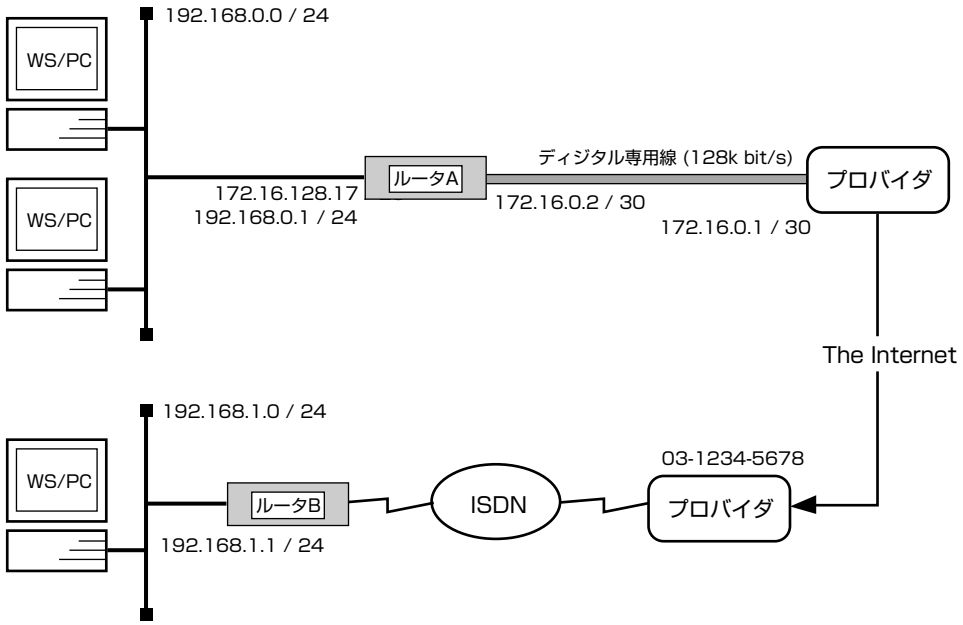
11. **pp enable** コマンドを使用して、PP 側のインタフェースを有効にします。このコマンドを実行した直後に、実際にこのインタフェースをパケットが通過できるようになります。

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。

## 9.3　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 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 A の LAN 側 IP アドレス：172.16.128.17/28
・ルータ A の回線側 IP アドレス ：172.16.0.2/30
・ルータ A の回線対向側 IP アドレス：172.16.0.1/30
・ルータ 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 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 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

・PP 側からは、内部から確立された TCP/UDP の通信パケットを許可する。
・DNS サーバ：172.16.128.2
・メールサーバ：172.16.128.3

[ ルータ A の設定手順 ]

```
# pp line l128
# ip lan address 172.16.128.17/28
# ip lan secondary address 192.168.0.1/24
# ip route default gateway pp leased
# ip route 192.168.1.0/24 gateway tunnel 1
# 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 leased
leased# ip pp nat descriptor 1
leased# ip pp address 172.16.0.2/30
leased# ip pp remote address 172.16.0.1
leased# pp enable leased
leased# 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# ipsec tunnel 101
tunnel1# tunnel enable 1
tunnel1# ipsec auto refresh on
tunnel1# tunnel select none
# save
# restart
```

[ ルータ B の設定手順 ]

```
# ip lan address 192.168.1.1/24
# ip route default gateway pp 1
# ip route 192.168.0.0/24 gateway tunnel 1
# 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# 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# 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# ipsec tunnel 101
tunnel1# tunnel enable 1
tunnel1# ipsec auto refresh on
tunnel1# tunnel select none
# save
```

［解説］

■ルータ A

1. **# pp line l128**
   回線種別を設定します。この設定は装置の再起動を行った後に有効になります。

2. **# ip lan address 172.16.128.17/28**
   **# ip lan secondary address 192.168.0.1/24**
   **# ip route default gateway pp 1**
   **# ip route 192.168.1.0/24 gateway tunnel 1**

   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。

   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。また相手側 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。

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# 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 B での設定は **ipsec ike remote address 172.16.128.17** となります。

5. **pp1# pp enable 1**
   **pp1# pp select none**

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# ipsec tunnel 101**
   **tunnel1# tunnel enable 1**
   **tunnel1# ipsec auto refresh on**
   **tunnel1# tunnel select none**
   IPsec 定義の適用と自動鍵交換を行うよう設定します。

8. **# save**
   **# restart**
   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。

■ルータ B

1. 
```
ip lan address 192.168.1.1/24
# ip route default gateway pp 1
# ip route 192.168.0.0/24 gateway tunnel 1
```
LAN 側をプライベートアドレスネットワークとします。
回線側にデフォルト経路を設定します。また相手側 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。

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# 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# 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。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# ipsec tunnel 101
tunnel1# tunnel enable 1
tunnel1# ipsec auto refresh on
tunnel1# tunnel select none
# save
```
IPsec 定義の適用と自動鍵交換を行うよう設定します。

# 10. NAT ディスクリプタ設定例

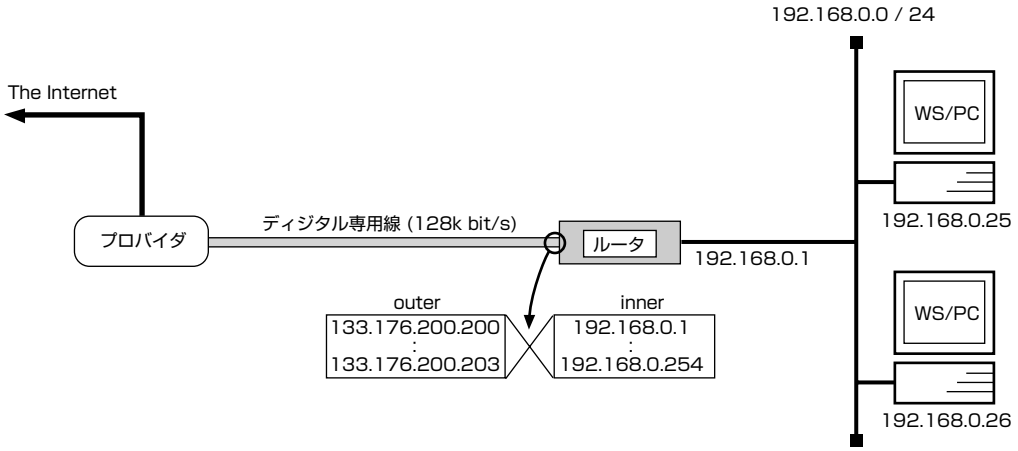
本章では、NAT ディスクリプタ機能の設定方法について、具体例をいくつかあげて説明します。セキュリティの設定や、詳細な各種パラメータなどの付加的な設定に関しては、個々のネットワークの運営方針などに基づいて行ってください。
本章で説明するネットワーク接続の形態は、次のようになります。

1. 動的 NAT と動的 IP マスカレード の併用
2. IP マスカレード でプライマリ - セカンダリ 間を接続

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。

## 10.1 動的 NAT と動的 IP マスカレード の併用

［構成図］




［設定手順］

```
# pp line l128
# ip lan address 192.168.0.1/24
# ip route default gateway pp leased
# nat descriptor type 1 nat-masquerade
# nat descriptor address outer 1 133.176.200.200-133.176.200.203
# nat descriptor address inner 1 192.168.0.1-192.168.0.254
# pp select leased
leased# ip pp nat descriptor 1
leased# pp enable leased
leased pp select none
# dhcp service server
# dhcp scope 1 192.168.0.2-192.168.0.254/24
# save
```

［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 | ルータの LAN インタフェース | − |
| 192.168.0.2<br>:<br>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. **pp line** 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 lan 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. **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。

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. **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. **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。

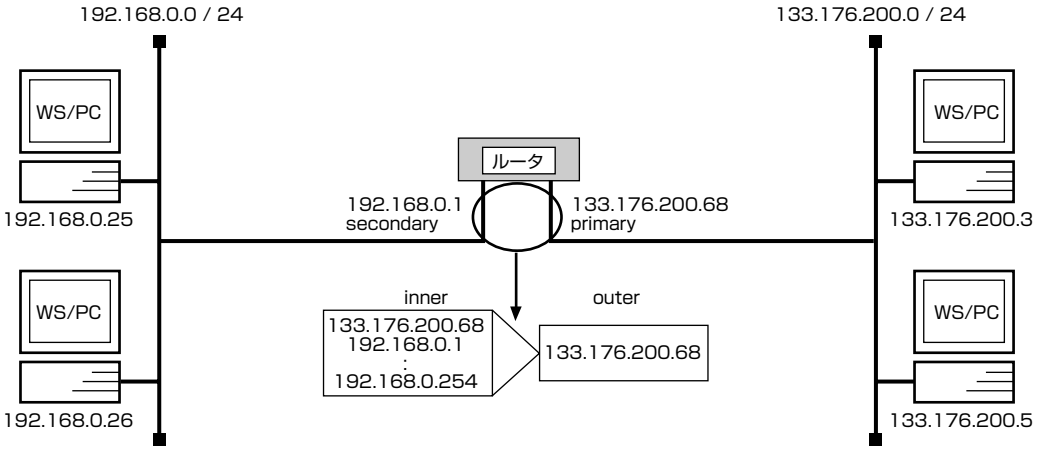
11. **dhcp scope** コマンドを使用して、DHCP スコープを定義します。

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. **restart** 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。

## 10.2 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 lan address 133.176.200.68/24
# ip lan secondary address 192.168.0.1/24
# ip lan nat descriptor 1
# nat descriptor type 1 masquerade
# nat descriptor address outer 1 primary
# nat descriptor address inner 1
   133.176.200.68 192.168.0.2-192.168.0.254
# 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 lan 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 lan 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 lan 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。