目次

コマンド索引

L

N

O

P

Q

R

S

T

W

1　コマンドリファレンスの見方

1.1　対応するプログラムのリビジョン

このコマンドリファレンスは **RT300i** プログラムの **Rev.6.00.14** に対応しています。
このコマンドリファレンスの印刷より後にリリースされた最新のプログラムや、マニュアル類及び差分については以下に示す URL の WWW サーバにある情報を参照してください。

http://rtpro.yamaha.co.jp/RT300i/

1.2　コマンドリファレンスの見方

このコマンドリファレンスは、ルータのコンソールから入力するコマンドを説明しています。
1 つ 1 つのコマンドは次の項目の組合せで説明します。

項目	説明
［入力形式］	コマンドの入力形式を説明します。キー入力時には大文字と小文字のどちらを使用しても構いません。 コマンドの名称部分は太字 **(Bold face)** で表します。 パラメータ部分は斜体 *(italic face)* で表します。 キーワードは標準文字で表します。 括弧([　])で囲まれたパラメータは省略可能であることを表します。
［パラメータ］	コマンドのパラメータの種類とその意味を説明します。
［説明］	コマンドの解説部分です。
［ノート］	このコマンドを使用する場合に特に注意すべき事柄を述べます。
［デフォルト値］	このコマンドのデフォルト値を示します。
［設定例］	このコマンドの具体例を示します。

1.3　インタフェース名について

コマンドでは、ルータの各インタフェースを指定するためにインタフェース名を利用します。インタフェース名は、インタフェース種別とインタフェース番号を間に空白をおかずに続けて表記します。インタフェース種別には、‘lan’、‘bri’、‘pri’があります。インタフェース番号は、インタフェースの種別ごとに、起動時に検出された順番で振られていきます。
また、BRI 拡張モジュールのように、1 つのモジュールに複数のインタフェースがある場合には、インタフェース番号はモジュールに振られた番号とモジュール内の番号をピリオド(.)でつなげた形式となります。

例：

メインモジュール上の LAN　lan1
メインモジュール上の BRI　bri1
1 つ目の LAN モジュール　lan2
1 つ目の 8BRI モジュール　bri2.1, bri2.2, ..., bri2.8
2 つ目の 8BRI モジュール　bri3.1, bri3.2, ..., bri3.8
1 つ目の PRI モジュール　pri1

1.4 no で始まるコマンドの入力形式について

コマンドの入力形式に **no** で始まる形のものが並記されているコマンドが多数あります。**no** で始まる形式を使うと、特別な記述がない限り、そのコマンドの設定を削除し、デフォルト値に戻します。また、**show config** コマンドでの表示からも外します。言い換えれば、**no** で始まる形式を使わない限り、入力されたコマンドは、たとえデフォルト値をそのまま設定する場合でも、**show config** コマンドでの表示の対象となります。

コマンドの入力形式で、**no** で始まるものに対して、省略可能なパラメータが記載されていることがあります。これらは、パラメータを指定してもエラーにならないという意味で、パラメータとして与えられた値は **no** コマンドの動作になんら影響を与えません。

2. ヘルプ

2.1 コンソールに対する簡易説明の表示

［入力形式］ **help**
［パラメータ］ なし
［説明］ コンソールの使用方法の簡単な説明を表示する。

2.2 コマンド一覧の表示

［入力形式］ **show command**
［パラメータ］ なし
［説明］ コマンドの名称とその簡単な説明を一覧表示する。

3. 機器の設定

3.1 ログインパスワードの設定

［入力形式］ **login password**

no login password

［パラメータ］ なし

［説明］ 一般ユーザとしてログインするためのパスワードを 32 文字以内で設定する。パラメータはなく、コマンド入力後にプロンプトに応じて改めてパスワードを入力する形になる。

3.2 管理パスワードの設定

［入力形式］ **administrator password**

no administrator password

［パラメータ］ なし

［説明］ 管理ユーザとしてルータの設定を変更する為の管理パスワードを 32 文字以内で設定する。パラメータはなく、コマンド入力後にプロンプトに応じて改めてパスワードを入力する形になる。

3.3 セキュリティクラスの設定

［入力形式］ **security class** *level forget telnet*

no security class [*level forget telnet*]

［パラメータ］
- *level*
  - 1 ... シリアルでも TELNET でも、遠隔地のルータからでもログインできる
  - 2 ... シリアルと TELNET からは設定できるが、遠隔地のルータからはログインできない
  - 3 ... シリアルからのみログインできる
- *forget*
  - on ... 設定したパスワードの代わりに “w,lXlma”でもログインでき、設定の変更も可能になる。ただしシリアルのみ
  - off ... パスワードを入力しないとログインできない
- *telnet*
  - on ... TELNET クライアントとして telnet コマンドが使用できる
  - off ... telnet コマンドは使用できない

［説明］ セキュリティクラスを設定する。

［デフォルト値］ *level* = 1

forget = on

telnet = off

3.4 ログインタイマの設定

［入力形式］ **login timer** *time*

no login time [*time*]

［パラメータ］ • *time*

◦秒数 ... キー入力がない時に自動的にログアウトするまでの秒数 (30 .. 21474836)

◦clear ... ログインタイマを設定しない

［説明］ キー入力がない時に自動的にログアウトするまでの時間を設定する。

［ノート］ TELNET でログインした場合、clear が設定されていてもタイマ値は 300 秒として扱う。

［デフォルト値］ 300

3.5 タイムゾーンの設定

［入力形式］ **timezone** *timezone*

no timezone [*timezone*]

［パラメータ］ • *timezone*

◦-12:00 〜 +11:59 ... その地域と世界標準時との差

◦jst ... 日本標準時 (+09:00)

◦utc ... 世界標準時 (+00:00)

［説明］ タイムゾーンを設定する。

［デフォルト値］ jst

3.6 現在の日付けの設定

［入力形式］ **date** *date*

［パラメータ］ • *date* ... yyyy-mm-dd または yyyy/mm/dd

［説明］ 現在の日付けを設定する。

3.7 現在の時刻の設定

［入力形式］ **time** *time*

［パラメータ］ • *time* ... hh:mm:ss

［説明］ 現在の時刻を設定する。

3.8 コンソールの言語とコードの設定

［入力形式］ **console character** *code*

［パラメータ］ • *code*

- ascii ... 英語で表示する、文字コードは ASCII
- euc ... 日本語で表示する、文字コードは EUC
- sjis ...日本語で表示する、文字コードはシフト JIS

［説明］ コンソールに表示する言語とコードを設定する。
このコマンドは一般ユーザでも実行できる。

［デフォルト値］ sjis

3.9 コンソールの表示文字数の設定

［入力形式］ **console columns** *col*

no console columns [*col*]

［パラメータ］ • *col* ... コンソールの表示文字数 (80..200)

［説明］ コンソールの表示文字数を設定する。
このコマンドは一般ユーザでも実行できる。

［デフォルト値］ 80

3.10 コンソールの表示行数の設定

［入力形式］ **console lines** *lines*

no console lines [*lines*]

［パラメータ］ • *lines* ... コンソールの表示行数

- 10 ... 100 の整数
- infinity ... スクロールを止めない

［説明］ コンソールの表示行数を設定する。
このコマンドは一般ユーザでも実行できる。

［デフォルト値］ 24

3.11 コンソールにシステムメッセージを表示するか否かの設定

［入力形式］ **console info** *info*

no console info [*info*]

［パラメータ］ • *info*

- on ... 表示する
- off ... 表示しない

［説明］ コンソールにシステムのメッセージを表示するか否かを設定する。

［ノート］ キーボード入力中にシステムメッセージがあると、表示画面が乱れるが、Ctrl+r で入力中の文字列を再表示できる。

［デフォルト値］ off

3.12 コンソールのプロンプト表示の設定

［入力形式］ **console prompt** *prompt*

no console prompt [*prompt*]

［パラメータ］ • *prompt* ... コンソールのプロンプトの先頭文字列 (16 文字以内)

［説明］ コンソールのプロンプト表示を設定する。空文字列も設定できる。

［デフォルト値］ 空文字列

3.13 SYSLOGを受けるホストの IP アドレスの設定

［入力形式］ **syslog host** *host*

no syslog host [*host*]

［パラメータ］ • *host*

◦ IP アドレス ... SYSLOG を受けるホストの IP アドレス

◦ clear ... ログを SYSLOG でレポートしない

［説明］ SYSLOG を受けるホストの IP アドレスを設定する。

［ノート］ syslog debug on にすると大量のデバッグメッセージが送信されるので、このコマンドで設定するホストには十分なディスク領域を確保しておくことが望ましい。

［デフォルト値］ clear

3.14 SYSLOGファシリティの設定

［入力形式］ **syslog facility** *facility*

no syslog facility [*facility*]

［パラメータ］ • *facility*

◦ 0 ... 23

◦ user ... 1

◦ local0 〜 local7 ... 16 〜 23

［説明］ SYSLOG のファシリティを設定する。

［デフォルト値］ user

3.15 NOTICEタイプの SYSLOGを出力するか否かの設定

［入力形式］ **syslog notice** *notice*

no syslog notice [*notice*]

［パラメータ］ • *notice*

◦ on ... 出力する

◦ off ... 出力しない

［説明］ IP フィルタ、IPX フィルタ、ブリッジフィルタで落したパケット情報等を SYSLOG で出力するか否か設定する。

［デフォルト値］ off

3.16 INFOタイプの SYSLOGを出力するか否かの設定

［入力形式］ **syslog info** *info*

no syslog info [*info*]

［パラメータ］ • *info*

◦ on ... 出力する

◦ off ... 出力しない

［説明］ ISDN の呼制御情報等を SYSLOG で出力するか否か設定する。

［デフォルト値］ on

3.17 DEBUGタイプの SYSLOGを出力するか否かの設定

［入力形式］ **syslog debug** *debug*

no syslog debug [*debug*]

［パラメータ］ • *debug*

◦ on ... 出力する

◦ off ... 出力しない

［説明］ ISDN 及び、PPP のデバッグ情報等を SYSLOG で出力するか否か設定する。

［ノート］ *debug* を on にすると大量のデバッグメッセージを送信するので、**syslog host** に設定するホスト側には十分なディスク領域を確保しておき、必要なデータが得られたらすぐに off にすること。

［デフォルト値］ off

3.18 SYSLOGパケットの始点ポート番号の設定

［入力形式］ **syslog srcport** *port*

no syslog srcport [*port*]

［パラメータ］ • *port* ... ポート番号(1..65535)

［説明］ 本機が送信する SYSLOG パケットの始点ポート番号を設定する。

［デフォルト値］ 514

3.19 LAN/PP インタフェースパケットのダンプを SYSLOGへ出力するか否かの設定

［入力形式］ **packetdump** *lan_interface* [*count*]

packetdump pp [*peer_number*] [*count*]

［パラメータ］ • *lan_interface* ... LAN インタフェース名

• *peer_number*

◦相手先情報番号

◦anonymous

◦leased (1BRI モデルのみ)

• *count*

◦パケット数 (1..21474836)

◦off ... 出力しない

◦infinity ... off にするまで出力する

［説明］ LAN/PP インタフェースを入出力するパケットのダンプ情報を DEBUG タイプ SYSLOG で出力するか否か設定する。

［デフォルト値］ *count* ... 100

peer_number ... 選択されている相手について表示する

3.20 TFTPによりアクセスできるホストの IPアドレスの設定

［入力形式］ **tftp host** *host*

no tftp host [*host*]

［パラメータ］ • *host*

◦IP アドレス ...TFTP によりアクセスできるホストの IP アドレス

◦any ... すべてのホストから TFTP によりアクセスできる

◦none ... すべてのホストから TFTP によりアクセスできない

［説明］ TFTP によりアクセスできるホストの IP アドレスを設定する。

［ノート］ セキュリティの観点から、プログラムのリビジョンアップや設定ファイルの読み書きが終了したらすぐに none にすること。

［デフォルト値］ none

3.21 マスタクロック用インタフェースの設定

［入力形式］ **line masterclock auto**

line masterclock *wan-interface*

no line masterclock

［パラメータ］ *wan-interface* ... BRI/PRI インタフェース名

［説明］ RT300i では、装備されているすべての BRI/PRI インタフェースは 1 つのマスタクロックに同期している必要がある。マスタクロックは通常、BRI/PRI インタフェースに接続された WAN 回線から供給される。このコマンドでは、どのインタフェースからマスタクロックを得るかを指定することができる。

auto を設定した場合は、実際に回線が接続されている BRI/PRI インタフェースの中からマスタクロックを供給するインタフェースを自動的に選択する。選択基準は、BRI よりは PRI を優先し、同じ回線種別の中ではより若番のポート番号を持つインタフェースを優先する。マスタとなるインタフェースの回線がダウンしてクロックを得られなくなった時には、同じモジュール内のインタフェースを優先して、次のマスタクロック供給インタフェースを選択する。全ての回線がダウンしている時には内部クロックを用いたフリーラン状態となる。

インタフェースを指定している場合には、そのインタフェースからマスタクロックを得る。そのインタフェースに接続されている回線がダウンした時には、常に bri1 をマスタとする。bri1 もダウンした時には内部クロックを用いたフリーラン状態となる。

［デフォルト］ auto

［ノート］ すべての BRI/PRI はマスタクロックに同期するので、それらに接続されている回線もお互いに同期している必要がある。日本国内の通信事業者が提供する実回線は、すべて NTT を基準として同期しているはずなので、その点では問題はない。一部の BRI/PRI に、構内網など独自に構築した回線や、疑似交換機などを接続する場合には、マスタクロックと同期していない回線ではクロックシフトによるビットエラーが発生する可能性があることに注意しなくてはいけない。

3.22 マスタクロックを得ている回線の表示

［入力形式］ **show line masterclock**

［説明］ 通信に使用しているクロックを得ている回線を表示する。フリーラン状態の場合はその旨を表示する。

3.23 LAN インタフェースの種類を指定

［入力形式］ **lan type** *lan-interface type*

［パラメータ］

- *lan-interface* ... LAN インタフェース名
- *type*
  - auto ... 速度自動設定
  - 100-fdx ... 100BASE-TX 全二重
  - 100-hdx ... 100BASE-TX 半二重
  - 10-fdx ... 10BASE-T 全二重
  - 10-hdx ... 10BASE-T 半二重

［説明］ 指定した LAN インタフェースの種類を設定する

［デフォルト］ auto

3.24 電源 2 の設定

［入力形式］ **system power 2 use** *sw*

no system power 2 use [*sw*]

［パラメータ］ . *sw* ... 電源 2 の装着状態

- on ... 電源 2 を装着している
- off ... 電源 2 を装着していない

［説明］ 電源 2 を装着しているかどうかを設定する。RT300i のみで有効なコマンドである。

電源 2 からの電源供給自体は実際に装着すればこのコマンドに関係なく機能するが、このコマンドを設定することで電源 2 の監視機能が正しく働くようになる。

［ノート］ 電源 2 を装着していないのにこのコマンドを on に設定すると、監視機能が働き、電源 2 の異常を報告する。

［デフォルト値］ off

3.25 温度監視の閾値の設定

［入力形式］ **system temperature threshold** *t1 t2*

no system temperature threshold *t1 t2*

［パラメータ］ . *t1* ... 警告を発する温度 (℃)

. *t2* ... 警告を解除する温度 (℃)

［説明］ RT300i でのみ有効なコマンドである。

本体内部の温度を監視して、*t1* 以上の温度になると SYSLOG や ALM ランプで警告を発する。一度、警告が発せられると、温度が *t2* を下回らない限り、ALM ランプは消えない。

［デフォルト値］ *t1* = 80、*t2* = 75

4. ISDN関連の設定

4.1 自分側の設定

4.1.1 BRI回線の種類の指定

［入力形式］ **line type** *bri_interface type* [*channels*]

no line type *bri_interface type* [*channels*]

［パラメータ］
- *bri_interface* ... BRI インタフェース名
- *type*
  - isdn , isdn-ntt ... ISDN 回線交換
  - l64 ... ディジタル専用線、64kbit/s
  - l128 ... ディジタル専用線、128kbit/s
- *channels* ... *type* が *isdn*、*isdn-ntt* の時だけ指定できる
  - 1b ... B チャネルは 1 チャネルだけ使用
  - 2b ... B チャネルは 2 チャネルとも使用する

［説明］ BRI 回線の種類を指定する。設定の変更は、再起動か、あるいは該当インタフェースに対する **interface reset** コマンドの発行により反映される。

［ノート］ 別の通信機器の発着信のために 1b チャネルを確保したい時は *channels* を 1b にする。

［デフォルト値］ *type* = isdn

channels = 2b

4.1.2 自分の ISDN番号の設定

［入力形式］ **isdn local address** *wan_interface* [*isdn_number*][*/sub_address*]

no isdn local address *wan_interface* [*isdn_number*][*/sub_address*]

［パラメータ］
- *wan_interface* ... BRI/PRI インタフェース名
- *isdn_number* ... ISDN 番号
- *sub_address* ... ISDN サブアドレス(0x21 から 0x7e の ASCII 文字)

［説明］ 自分の ISDN 番号とサブアドレスを設定する。ISDN 番号、サブアドレスとも完全に設定して運用することが推奨される。また、ISDN 番号は市外局番も含めて設定する。

［ノート］ 他機種との相互接続のために、ISDN サブアドレスに英文字や記号を使わず数字だけにしなければいけないことがある。

4.1.3 課金額による発信制限の設定

［入力形式］

account threshold *yen*

account threshold *wan_interface yen*

account threshold pp *yen*

no account threshold [*yen*]

no account threshold *wan_interface* [*yen*]

no account threshold pp [*yen*]

［パラメータ］

• *yen*

◦課金額 ...円 (10..21474836)

◦off ... 発信制限機能を使わない

• *wan_interface* ... BRI/PRI インタフェース名

［説明］

網から通知される課金の合計の累計が指定した金額に達したらそれ以上の発信を行わないようにする。

account threshold の形式では、ルータ全体の合計金額で、*wan_interface* を指定するものはそれぞれのインタフェースでの合計金額で、**account threshold pp** の形式では選択している相手先に対する発信での合計金額で制御を行う。

課金が網から通知されるのは通信切断時なので、長時間の接続の途中切断することはできず、この場合は制限はできない。この場合に対処するには、**isdn forced disconnect time** コマンドで通信中でも時間を監視して強制的に回線を切るような設定にしておく方法がある。また、課金合計は **clear account** コマンドで 0 にリセットできるので、**schedule at** コマンドで定期的に **clear account** を実行するようにしておくと、毎月一定額以内に課金を抑えるといったことが自動で可能になる。

［ノート］

電源 OFF や再起動により、それまでの課金情報がクリアされることに注意。課金額は通信の切断時に NTT から ISDN で通知される料金情報に基づくため、割引サービスなどを利用している場合には、最終的に NTT から請求される料金とは異なる場合がある。また、NTT 以外の通信事業者を利用して通信した場合には料金情報は通知されない。

［デフォルト値］

off

4.1.4 専用線がダウンした時にバックアップする相手先情報番号の設定

［入力形式］

leased backup *peer_number*

no leased backup [*peer_number*]

［パラメータ］

• *peer_number*

◦バックアップする相手先情報番号

◦none ... ISDN でバックアップをしない

［説明］

選択した相手先に対する専用線がダウンした時に ISDN でバックアップする、バックアップ用の相手先情報番号を設定する。

［デフォルト値］

none

4.1.5 バックアップからの復帰待ち時間の設定

［入力形式］ **leased backup recovery time** *time*

no leased backup recovery time [*time*]

［パラメータ］ • *time*

◦秒数 (1..21474836)

◦off ... すぐに復帰

［説明］ バックアップから復帰するときに、すぐに復帰させるか、設定された時間だけ待ってから復帰するかを設定する。

［ノート］ この設定はすべての PP で共通に用いられる。また、専用線バックアップでも FR バックアップでもこの設定が共通に用いられる。

［デフォルト値］ off

4.1.6 終端抵抗の設定

［入力形式］ **isdn terminator** *bri terminator*

no isdn terminator *bri* [*terminator*]

［パラメータ］ • *bri* ... BRI インタフェース名

• *terminate*

◦on ... ON にする

◦off ... OFF にする

［説明］ 指定した BRI インタフェースの終端抵抗を ON または OFF にする。

［ノート］ DSU に直結する場合には必ず on にする。

バス配線されている場合、バスの終端でなければ off にする。

［デフォルト値］ off

4.1.7 PPで使用するインタフェースの設定

［入力形式］ **pp bind** *wan_interface* [*wan-interface...*]

no pp bind [*wan_interface...*]

［パラメータ］ • *wan_interface* ... BRI/PRI インタフェース名

［説明］ 選択されている相手先に対して実際に使用するインタフェースを設定する。

［デフォルト値］ どのインタフェースともバインドされていない

4.1.8 PIAFSの発信方式の設定

［入力形式］ **isdn piafs call** *speed* [*mode*]

no isdn piafs call [*speed* [*mode*]]

［パラメータ］ • *speed*

- 32k ... PIAFS 32kbit/s で発信
- 64k ... PIAFS 64kbit/s で発信
- off ... 同期 PPP で発信

• *mode*

- guarantee ... PIAFS 64kbit/s ギャランティー方式
- best-effort ... PIAFS 64kbit/s ベストエフォート方式

［説明］ PIAFS の発信方式を設定する。*mode* は PIAFS64k の場合のみ指定できる。guarantee/best-effort はそれぞれ、PIAFS2.0/PIAFS2.1 と呼ばれることもある。

［ノート］ PIAFS 64kbit/s の通信では特別なサブアドレスが使用されるため、**isdn local address/isdn remote address** コマンドなどでユーザが指定したサブアドレスは無視される。

［デフォルト値］ off

4.1.9 PIAFSの着信を許可するか否かの設定

［入力形式］ **isdn piafs arrive** *arrive*

no isdn piafs arrive [*arrive*]

［パラメータ］ • *arrive*

- on ... 許可する
- off ... 拒否する

［説明］ PIAFS の着信を許可するか否かを設定する。着信が許可されている場合には、すべての PIAFS の方式が着信できる。

［ノート］ PHS 端末側で発信者番号を通知するようになっている必要がある。

PIAFS 64kbit/s の通信では特別なサブアドレスが使用されるため、**isdn local address/isdn remote address** コマンドなどでユーザが指定したサブアドレスは無視される。

［デフォルト値］ on

4.2 相手毎の設定

4.2.1 相手 ISDN番号の設定

［入力形式］ **isdn remote address** *call_arrive isdn_number*[*/sub_address*] [*isdn_number_list*]

no isdn remote address *call_arrive* [*isdn_number*[*/sub_address*] [*isdn_number_list*]]

［パラメータ］ • *call_arrive*

◦ call ... 発着信用

◦ arrive ... 着信専用

• *isdn_number* ... ISDN 番号

• *sub_address* ... ISDN サブアドレス(0x21 から 0x7e の ASCII 文字)

• *isdn_number_list* ... ISDN 番号だけまたは ISDN 番号とサブアドレスを空白で区切った並び

［説明］ 選択されている相手の ISDN 番号とサブアドレスを設定する。ISDN 番号には市外局番も含めて設定する。

選択されている相手が anonymous または leased の時は無意味である。

複数の ISDN 番号が設定されている場合、まず先頭の ISDN 番号での接続に失敗すると次に指定された ISDN 番号が使われる。同様に、それに失敗すると次の ISDN 番号を使うという動作を続ける。

MP のように相手先に対して複数チャネルで接続しようとする際に発信する順番は、**isdn remote call order** コマンドで設定する。

4.2.2 相手への発信順序の設定

［入力形式］ **isdn remote call order** *order*

no isdn remote call order [*order*]

［パラメータ］ • *order*

◦ round ... ラウンドロビン方式

◦ serial ... 順次サーチ方式

［説明］ **isdn remote address call** コマンドで複数の ISDN 番号が設定されている場合に意味を持つ。MP を使用する場合などのように、相手先に対して同時に複数のチャネルで接続しようとする際に、どのような順番で ISDN 番号を選択するかを設定する。

round の場合は、**isdn remote address call** コマンドで最初に設定した ISDN 番号で発信した次の発信時には、このコマンドで次に設定された ISDN 番号を使う。このように順次ずれていき、最後に設定された番号で発信した次には、最初に設定された ISDN 番号を使い、これを繰り返す。

serial の場合は、発信時には必ず最初に設定された ISDN 番号を使い、何らかの理由で接続できなかった場合は次に設定された ISDN 番号で発信し直す。

なお round、serial いずれの設定の場合でも、どことも接続されていない状態や相手先とすべてのチャネルで切断された後では、最初に設定された ISDN 番号から発信に使用される。

［ノート］ MP を使用する場合は、round にした方が効率がよい。

［デフォルト値］ serial

4.2.3 自動接続の設定

［入力形式］ **isdn auto connect** *auto*

no isdn auto connect [*auto*]

［パラメータ］ • *auto*

◦ on ... 自動接続する

◦ off ... 自動接続しない

［説明］ 選択されている相手について自動接続するか否かを設定する。

［デフォルト値］ on

4.2.4 自動切断の設定

［入力形式］ **isdn auto disconnect** *auto*

no isdn auto disconnect [*auto*]

［パラメータ］ • *auto*

◦ on ... 自動切断する

◦ off ... 自動切断しない

［説明］ 選択されている相手について自動切断するか否かを設定する。

各種切断タイマの設定を変更せずに、自動切断を無効にしたい場合に使用する。

［ノート］ **schedule at** コマンドと併用して、テレホーダイ時間中に自動切断しないようにしたい場合等に有効。

anonymous に対して使用する事はできない。

［デフォルト値］ on

4.2.5 着信許可の設定

［入力形式］ **isdn arrive permit** *arrive*

no isdn arrive permit [*arrive*]

［パラメータ］ • *arrive*

◦ on ... 許可する

◦ off ... 許可しない

［説明］ 選択されている相手からの着信を許可するか否かを設定する。

［ノート］ **isdn arrive permit**、**isdn call permit** とも off を設定した時は通信できない。

［デフォルト値］ on

4.2.6 発信許可の設定

［入力形式］ **isdn call permit** *permit*

no isdn call permit [*permit*]

［パラメータ］ • *permit*

◦ on ... 許可する

◦ off ... 許可しない

［説明］ 選択されている相手への発信を許可するか否かを設定する。

［ノート］ **isdn arrive permit**、**isdn call permit** とも off を設定した時は通信できない。

［デフォルト値］ on

4.2.7 再発信抑制タイマの設定

［入力形式］ **isdn call block time** *time*

no isdn call block time [*time*]

［パラメータ］ • *time* ... 秒数(0..15)

［説明］ 選択されている相手との通信が切断された後、同じ相手に対し再度発信するのを禁止する時間を設定する。秒数は 0.1 秒単位で設定できる。

isdn call prohibit time コマンドによるタイマはエラーで切断された時だけに適用されるが、このコマンドによるタイマは正常切断でも適用される点が異なる。

［ノート］ 切断後すぐに発信ということを繰り返す状況では適当な値を設定すべきである。

isdn forced disconnect time コマンドと併用するとよい。

［デフォルト値］ 0

4.2.8 エラー切断後の再発信禁止タイマの設定

［入力形式］ **isdn call prohibit time** *time*

no isdn call prohibit time [*time*]

［パラメータ］ • *time* ... 秒数 (60..21474836)

［説明］ 選択されている相手に発信しようとして失敗した時に、同じ相手に対し再度発信するのを禁止する時間を設定する。秒数は 0.1 秒単位で設定できる。

isdn call block time コマンドによるタイマは切断後に常に適用されるが、このコマンドによるタイマはエラー切断にのみ適用される点が異なる。

［デフォルト値］ 60

4.2.9 相手にコールバック要求を行うか否かの設定

［入力形式］ **isdn callback request** *callback_request*

no isdn callback request [*callback_request*]

［パラメータ］ • *callback_request*

◦ on ... 要求する

◦ off ... 要求しない

［説明］ 選択されている相手に対してコールバック要求を行うか否かを設定する。

［デフォルト値］ off

4.2.10 コールバック要求タイプの設定

［入力形式］ **isdn callback request type** *type*

no isdn callback request type [*type*]

［パラメータ］ • *type*

◦ yamaha ... ヤマハ方式

◦ mscbcp ... MS コールバック

［説明］ コールバックを要求する時のコールバック方式を設定する。

［デフォルト値］ yamaha

4.2.11 相手からのコールバック要求に応じるか否かの設定

［入力形式］ **isdn callback permit** *callback_permit*

no isdn callback permit [*callback_permit*]

［パラメータ］ • *callback_permit*

◦ on ... 応じる

◦ off ... 応じない

［説明］ 選択されている相手からのコールバック要求に対してコールバックするか否かを設定する。

［デフォルト値］ off

4.2.12 コールバック受け入れタイプの設定

［入力形式］ **isdn callback permit type** *type1* [*type2*]

no isdn callback permit type [*type1* [*type2*]]

［パラメータ］ • *type1*、*type2*

◦ yamaha ... ヤマハ方式

◦ mscbcp ... MS コールバック

［説明］ 受け入れることのできるコールバック方式を設定する。

［デフォルト値］ *type1* = yamaha

type2 = mscbcp

4.2.13 MS コールバックでユーザからの番号指定を許可するか否かの設定

［入力形式］ **isdn callback mscbcp user-specify** *specify*

no isdn callback mscbcp user-specify [*specify*]

［パラメータ］ • *specify*

◦ on ... 許可する

◦ off ... 拒否する

［説明］ サーバ側として動作する時にはコールバックするために利用可能な電話番号が一つでもあればそれに対してのみコールバックする。しかし、anonymous への着信で、発信者番号通知がなく、コールバックのためにつかえる電話番号が全く存在しない場合に、コールバック要求側(ユーザ)からの番号指定によりコールバックするかどうかを設定する。

［ノート］ 設定が off でコールバックできない時には、コールバックせずにそのまま接続する。

［デフォルト値］ off

4.2.14 コールバックタイマの設定

［入力形式］ **isdn callback response time** 1b *time*

no isdn callback response time [1b *time*]

［パラメータ］ • *time* ... 秒数(0..15)

［説明］ 選択されている相手からのコールバック要求を受け付けてから、実際に相手に発信するまでの時間を設定する。秒数は 0.1 秒単位で設定できる。

［デフォルト値］ 0

4.2.15 コールバック待機タイマの設定

［入力形式］ **isdn callback wait time** *time*

no isdn callback wait time [*time*]

［パラメータ］ • *time* ... 秒数(1..60)

［説明］ 選択されている相手にコールバックを要求し、それが受け入れられていったん回線が切断されてから、このタイマがタイムアウトするまで相手からのコールバックによる着信を受け取れなかった場合には接続失敗とする。秒数は 0.1 秒単位で設定できる。

［デフォルト値］ 60

4.2.16 ISDN回線を切断するタイマ方式の指定

［入力形式］ **isdn disconnect policy** *type*

no isdn disconnect policy [*type*]

［パラメータ］ • *type*

- 1 ... 単純トラフィック監視方式
- 2 ... 課金単位時間方式

［説明］ 単純トラフィック監視方式は従来型の方式であり、**isdn disconnect time**、**isdn disconnect input time**、**isdn disconnect output time** の 3 つのタイマコマンドでトラフィックを監視し、一定時間パケットが流れなくなった時点で回線を切断する。

課金単位時間方式では、課金単位時間と監視時間を **isdn disconnect interval time** コマンドで設定し、監視時間中にパケットが流れなければ課金単位時間の倍数の時間で回線を切断する。通信料金を減らす効果が期待できる。

［デフォルト値］ 1

4.2.17 切断タイマの設定（ノーマル）

［入力形式］ **isdn disconnect time** *time*

no isdn disconnect time [*time*]

［パラメータ］ • *time*

- 秒数 (1..21474836)
- off ... タイマを設定しない

［説明］ 選択されている相手について PP 側のデータ送受信がない時の切断までの時間を設定する。秒数は 0.1 秒単位で設定できる。

［ノート］ 以下のような設定が行われている場合：

isdn disconnect time X

isdn disconnect input time IN

isdn disconnect output time OUT

X >IN または X >OUT と設定すると、パケットの入出力が観測されないと X 秒で切断される。

［デフォルト値］ 60

4.2.18 入力切断タイマの設定（ノーマル）

［入力形式］ **isdn disconnect input time** *time*

no isdn disconnect input time [*time*]

［パラメータ］ • *time*

◦ 秒数 (1..21474836)

◦ off ... タイマを設定しない

［説明］ 選択されている相手について PP 側からデータ受信がない時の切断までの時間を設定する。秒数は 0.1 秒単位で設定できる。

［ノート］ 例えば、UDP パケットを定期的に出すようなプログラムが暴走したような時、このタイマを設定しておくことにより回線を切断することができる。

以下のような設定が行われている場合：

isdn disconnect time X

isdn disconnect input time IN

isdn disconnect output time OUT

X >IN または X >OUT と設定すると、パケットの入出力が観測されないと X 秒で切断される。

［デフォルト値］ 120

4.2.19 出力切断タイマの設定（ノーマル）

［入力形式］ **isdn disconnect output time** *time*

no isdn disconnect output time [*time*]

［パラメータ］ • *time*

◦ 秒数(1..21474836)

◦ off ... タイマを設定しない

［説明］ 選択されている相手について PP 側へのデータ送信がない時の切断までの時間を設定する。秒数は 0.1 秒単位で設定できる。

［ノート］ 例えば、UDP パケットを定期的に出すようなプログラムが暴走したような時、このタイマを設定しておくことにより回線を切断することができる。

以下のような設定が行われている場合：

isdn disconnect time X

isdn disconnect input time IN

isdn disconnect output time OUT

X >IN または X >OUT と設定すると、パケットの入出力が観測されないと X 秒で切断される。

［デフォルト値］ 120

4.2.20 課金単位時間方式での課金単位時間と監視時間の設定

［入力形式］

isdn disconnect interval time *unit watch spare*

no isdn disconnect interval time [*unit watch spare*]

［パラメータ］

• *unit* ... 課金単位時間

◦秒数 (1..21474836)

◦off

• *watch* ... 監視時間

◦秒数 (1..21474836)

◦off

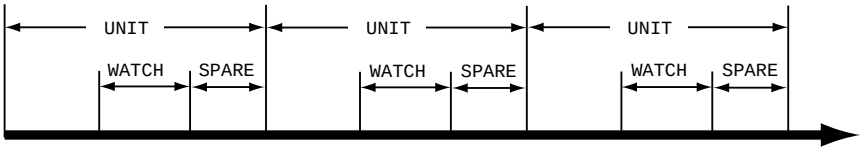
• *spare* ... 切断余裕時間

◦秒数 (1..21474836)

◦off

［説明］

課金単位時間方式で使われる、課金単位時間と監視時間を設定する。秒数は 0.1 秒単位で設定できる。それぞれの意味は下図の通り：



WATCH で示した間だけトラフィックを監視し、この間にパケットが流れなければ回線を切断する。SPARE は切断処理に時間がかかりすぎて、実際の切断が単位時間を越えないように余裕を持たせるために使う。

回線を接続している時間が UNIT の倍数になるので、単純トラフィック監視方式よりも通信料金を減らす効果が期待できる。

［デフォルト値］

unit = 180

watch = 6

spare = 2

4.2.21 切断タイマの設定（ファスト）

［入力形式］ **isdn fast disconnect time** *time*

no isdn fast disconnect time [*time*]

［パラメータ］ • *time*

◦ 秒数 (1..21474836)

◦ off ... タイマを設定しない

［説明］ ある宛先について、パケットがルーティングされ、そこへ発信しようとしたが、ISDN 回線が他の接続先により塞がっていて発信できない時に、ISDN 回線を塞いでいる相手先についてこのタイマが動作を始める。このタイマで指定した時間の間、パケットが全く流れなかったらその相手先を切断して、発信待ちの宛先を接続する。秒数は 0.1 秒単位で設定できる。

なお、**isdn auto connect** コマンドが off の時はこのタイマは無視される。

［デフォルト値］ 20

4.2.22 切断タイマの設定（強制）

［入力形式］ **isdn forced disconnect time** *time*

no isdn forced disconnect time [*time*]

［パラメータ］ • *time*

◦ 秒数 (1..21474836)

◦ off ... タイマを設定しない

［説明］ 選択されている相手に接続する最大時間を設定する。秒数は 0.1 秒単位で設定できる。

パケットをやりとりしていても、このコマンドで設定した時間が経過すれば強制的に回線を切断する。

［ノート］ ダイヤルアップ接続でインターネット側からの無効なパケット (ping アタック等)が原因で回線が自動切断できない場合に有効。**isdn call block time** コマンドと併用するとよい。

［デフォルト値］ off

4.2.23 相手先毎の課金額による発信制限の設定

［入力形式］ **account threshold pp** *yen*

no account threshold pp [*yen*]

［パラメータ］ • *yen*

◦ 課金額 ... 円 (10..21474836)

◦ off ... 課金額による発信制限機能を使わない

［説明］ 選択されている相手において、網から通知される課金累計額 (これは **show pp account** コマンドで表示される金額) が指定した金額に達したら、それ以上の発信を行わないようにする。

［デフォルト値］ off

5. フレームリレー関連の設定

本機は、アクセス回線として BRI/PRI を利用したフレームリレーに対応しています。

PPP によるダイヤルアップ接続と専用線接続、フレームリレー接続では同じ HDLC[1] フレームを使用して通信しますが、PPP とフレームリレーでは HDLC フレーム内のフォーマットが異なるため、フレームリレーで運用を開始する前にはカプセル化プロトコルを指定する必要があります。カプセル化の指定は **pp encapsulation** コマンドで設定します。

DLCI[2] はフレームリレーで相手先を指定するための識別子です。1 本の回線で複数の DLCI を利用することができ、回線を論理多重化してそれぞれが仮想的な専用線のようにネットワークを構築することができます。具体的な DLCI の値はフレームリレーネットワーク提供者との契約時に決まります。

DLCI をルータに設定する方法は、ルータによる自動取得と管理者による手動設定の 2 種類があります。手動設定は **fr dlci** コマンドで行います。

自動取得の場合には PVC[3] 状態確認手順の LMI[4] により行われます。本機は JT-Q933 と ANSI の 2 種類の LMI をサポートしており、**fr lmi** コマンドを使用していずれかを指定します。手動設定の場合、DLCI は最大 96 個まで設定できます。自動取得の場合には、制限はありません。DLCI は **show dlci** コマンドで確認することができます。

一般に、フレームリレーでのルーティングは1つの相手先情報番号に複数の相手先（DLCI）が接続するためにPP側はnumberedとなります。相手の PP 側の IP アドレスと DLCI の対応を解決するプロトコルが InARP[5] です。InARP を使用するか否かは **fr inarp** コマンドで設定します。

本機の特徴として、直接 DLCI を指定してルーティングすることが可能です。この場合は PP 側の IP アドレス (**ip pp address** コマンド)を設定せず、PP 側 unnumbered のスタティックルーティングとなり InARP も使用されません。

YAMAHA リモートルータ同士であれば、unnumbered でダイナミックルーティングが可能です。

データ圧縮機能によってフレームリレー回線上での通信負荷を最大 2/5 程度まで軽減することが可能です。

本機能の実装は Frame Relay Forum の FRF.9 に基づいており、特に、FRF.9 のモード 1 に対応しています。データの圧縮と伸長アルゴリズムは Stac LZS を使用します。

このデータ圧縮機能を使用するか否かは **fr compression use** コマンドで設定します。

なお、このデータ圧縮機能が適用できる対地の最大数は、本機では50であり、これを超える数の対地に対して本機能を適用することはできません。

同じフレームリレー回線に PP インタフェースを複数バインドする場合、1BRI モデルでは leased インタフェースが代表となり、それ以外のモデルでは最も若い PP インタフェースが代表となります。

pp encapsulation fr の設定は、関係する全てのインタフェースに対して設定する必要があります。一方、**fr lmi** 、**fr inarp** 、**fr congestion control**、そして、**fr pp dequeue type** の各コマンドは代表のインタフェースにのみ設定します。

データリンクの DLCI 値が **fr dlci** コマンドで明示的に設定されているときには、その設定のあるインタフェースにデータリンクが収容されます。その DLCI 値が複数のインタフェースで設定されているときには、まず代表のインタフェースが優先され、その後の優先順位は番号の若い順となります。

データリンクの DLCI 値が、**fr dlci** コマンドで明示的に設定されていないときには、**fr dlci auto** が設定されているインタフェースにデータリンクが収容されます。**fr dlci auto** の設定されたインタフェースがないときにはどのインタフェースにも収容されません。**fr dlci auto** の設定されたインタフェースが複数あるときは、まず代表のインタフェースが優先され、その後の優先順位は番号の若い順となります。

---

1 High level Data Link Control procedure

2 Data Link Connection Identifier

3 Permanent Virtial Circuit

4 Local Management Interface

5 Inverse Address Resolution Protocol; RFC1293

5.1 PP側でのカプセル化の種類の設定

［入力形式］ **pp encapsulation** *type*

no pp encapsulation [*type*]

［パラメータ］ • *type*

◦ ppp ... PPP でカプセル化する

◦ fr ... フレームリレーでカプセル化する

［説明］ 選択されている相手のカプセル化の種類を設定する。

［ノート］ フレームリレーでは IPXWAN の設定は無効 (常に OFF)

［デフォルト値］ ppp

5.2 PP側フレームリレーでの DLCIの設定

［入力形式］ **fr dlci** *dlci_num*

no fr dlci [*dlci_num*]

［パラメータ］ • *dlci_num*

◦ auto ... DLCI を自動取得する

◦ DLCI 値(16..991) を空白で区切って並べたもの (96 個以内)

［説明］ 選択されている相手で使用する DLCI を自動設定するか、または手動設定する。

auto の場合は PVC 状態確認手順により DLCI を自動取得する。

［ノート］ fr lmi off でない場合にこのコマンドで DLCI を手動設定した場合には、網から通知された DLCI の中で手動設定されているものだけが有効となる。

［デフォルト値］ auto

［設定例］ # fr dlci 16 17 18

5.3 PP側フレームリレーでの PVC 状態確認手順の設定

［入力形式］ **fr lmi** *lmi*

no fr lmi [*lmi*]

［パラメータ］ • *lmi*

◦ q933 ... TTC 標準 JT-Q933 付属資料 A に基づいて状態確認を行う

◦ ansi ... ANSI T1.617 AnnexD に基づいて状態確認を行う

◦ off ... PVC 状態確認手順は行わない

［説明］ 選択されている相手に対するフレームリレーでの PVC 状態確認手順を設定する。

［ノート］ 網との契約で LMI が無い場合に fr lmi off に設定しておかないと、回線ダウンとみなされるので注意。

［デフォルト値］ q933

5.4 PP側フレームリレーでのInARP使用の設定

［入力形式］ **fr inarp** *inarp*

no fr inarp [*inarp*]

［パラメータ］ • *inarp*

◦ on ... 使用する

◦ off ... 使用しない

［説明］ 選択されている相手について、InARP (Inverse Address Resolution Protocol)を使用して、相手の IP アドレスを自動取得するかどうかを設定する。この設定が on の場合でも、自分の PP 側のローカル IP アドレスが設定されていない場合 (unnumbered) は InARP は使用しない。

また、自分の PP 側ローカル IP アドレスが設定されていれば、相手から InARP のリクエストが来た場合、この設定に関わらず常にレスポンスを返す。

［ノート］ **ip pp address** コマンドを参照。

［デフォルト値］ on

5.5 フレームリレーがダウンした時にバックアップする相手先情報番号の設定

［入力形式］ **fr backup dlci**=*dlci_num peer_number*

no fr backup dlci=*dlci_num* [*peer_number*]

［パラメータ］ • *dlci_num*

◦ DLCI 値 (16..991)

• *peer_number* ... バックアップする相手先情報番号

［説明］ 指定した DLCI がダウンした時にバックアップする相手先情報番号を設定する。

［ノート］ 同じ相手先情報番号に、専用線バックアップ (**leased backup** コマンド)とフレームリレーバックアップの両方を設定することはできない。

5.6 FR圧縮機能の設定

［入力形式］ **fr compression use dlci**=*dlci_num type*

no fr compression use dlci=*dlci_num* [*type*]

［パラメータ］ • *dlci_num*

◦ DLCI 値(16..991)

◦ * (すべてのデータリンク)

• *type*

◦ stac ... Stac LZS 方式を用いてデータを圧縮する

◦ cstac ... cstac 方式を用いてデータを圧縮する

◦ none ... データを圧縮しない

［説明］ FR のデータ圧縮機能の方式を設定する。dlci_num パラメータには、対象となるリンクに付された自分側の DLCI 値を指定する。なお、このコマンドを設定している場合でも、交渉に失敗した場合には圧縮機能は働かない。

［デフォルト値］ *type* = none

5.7 DLCIごとのパラメータの設定

［入力形式］ **fr cir dlci**=*dlci_num cir* [slowstart-idle= *idle*] [bc= *bc_size*] [be= *be_size*] [s=*step_count*]

no fr cir dlci=*dlci_num* [*cir* [**...**]]

［パラメータ］
- *dlci_num* ... DLCI 値 (16..991)
- *cir* ... CIR 値 (bit/s 単位)
- *idle* ...スロースタート状態に戻るまでのアイドル時間
  - 秒数 (1..21474836)
  - 0 ... スロースタート動作を行わない
- *bc_size* ... 認定バーストサイズ (ビット)
- *be_size* ... 超過バーストサイズ (ビット)
- *step_count* ... ステップカウント

［説明］ DLCI 毎のパラメータを設定する。PP 毎に設定し、その PP に所属する DLCI 値に対して設定が有効となる。

［デフォルト値］ slowstart-idle = 20

bc = be = 7000

s = *cir*/*bc size*/*be size* から計算される値

5.8 輻輳制御をするか否かの設定

［入力形式］ **fr congestion control** *control*

no fr congestion control [*control*]

［パラメータ］
- *control*
  - on ... 輻輳制御を行う
  - off ... 輻輳制御を行わない

［説明］ フレームリレーの輻輳制御を行うかどうかを設定する。CIR が設定されていない DLCI に対しては、回線速度の半分の CIR が設定されているものとして動作する。

［ノート］ 輻輳制御は、BECN および CLLM の通知に基づいて行う。暗黙的輻輳検出および FECN による明示的輻輳通知は扱わない。

［デフォルト値］ off

5.9 回線に対する送信順序方式の設定

［入力形式］ **fr pp dequeue type** *type*

no fr pp dequeue type [*type*]

［パラメータ］ • *type*

◦ serial ... 順次サーチ方式

◦ round-robin ... ラウンドロビン方式

［説明］ 同じフレームリレー回線に複数の PP インタフェースがバインドされている時の送信順序方式を設定する。serial の場合には、同じフレームリレー回線にバインドされた PP インタフェースに対して順位を与え、順位の高い PP インタフェースから優先してパケットを送信する。round-robin の場合には、優先順位を設定せずに全ての PP インタフェースから均等にパケットを送信する。

［ノート］ 相手先情報番号の若い PP インタフェースがより高い順位を持つものと定義する。1BRI モデルでは、これに加えて、leased が最も高い順位を持つものと定義する。

［デフォルト値］ round-robin

5.10 指定パケットに DE ビットを立てるか否かの設定

［入力形式］ **fr de** *protocol* filter dlci=*dlci num_filter number_list*

no fr de *protocol* filter dlci=*dlci* [*num_filter number_list*]

［パラメータ］ • *protocol*

◦ ip ... IP パケット

◦ ipx ... IPX パケット

◦ bridge ... ブリッジするパケット

• filter ... (固定のキーワード)

• *dlci_num*

◦ DLCI 値(16..991)

◦ * (すべてのデータリンク)

• *filter_number_list* ... フィルタの番号(1..100)の列

［説明］ 指定パケットに DE ビットを立てるか否かを設定する。

filter_number_list で指定したフィルタを順番にパケットに対して適用し、マッチしたところでそのフィルタが pass、pass-log、pass-nolog、restrict、restrict-log、restrict-nolog のいずれかであれば DE ビットを立てる。reject、reject-log または reject-nolog である場合は DE ビットを立てない。フィルタ列の最後までマッチしなかった時には DE ビットを立てない。

［デフォルト値］ DE ビットは立てない

6. PRI関連の設定

本機は、オプションのPRI拡張モジュールを装着することにより一次群速度インタフェース(PRI:Primary Rate Interface) に対応します。多重化非対応の PRI 拡張モジュール (製品番号：YBA-1PRI-N)は、多重化されていない 192kbit/s 〜 1.5Mbit/s の高速ディジタル専用線や DA1500、およびフレームリレーサービスなどに最適です。多重化対応の PRI 拡張モジュール (製品番号：YBA-1PRI-M)を利用すると、それに加えて最大 24 対地まで多重化された高速ディジタル専用線や、INS1500 を利用することができます。

PRI 専用線を使用するには、PRI ネットワーク提供者との契約で指定された情報チャネルやタイムスロットなどを **pri leased channel** コマンドで設定します。PRI を通してパケットをやりとりするためには、**pp bind** コマンドで相手先情報番号と関連付けます。
また、現在の PRI 関連の情報は **show status pri** コマンドで確認することができます。

PRI 専用線に対してループバック試験を行うことができます。ループバック試験は、指定したデータを指定したループバックポイントで折り返して、送信データと折り返されたデータを比較して正常性の検証を行います。
ループバックポイントは、主にハードウェアに対して行うループバックAと回線上にデータを流して折り返し試験を行うタイムスロットループバックがあります。
ループバックAでは試験ルータのPRI コネクタ部分で折り返し、タイムスロットループバックでは指定したタイムスロットを使用して相手ルータからデータを折り返し受信します。

本機でループバックを実行するには、コンソールコマンドから実行します。ループバック試験を行う前に、通常の通信を **pp disable** コマンド等で停止させてから行うようにします。
タイムスロットループバックでは、相手側ルータは**pri loopback passive**コマンドで待ち受け状態にしておく必要があります。
なお、ループバック試験中のメッセージはデータ送信側のコンソールにだけ表示されます。

6.1 PRI回線の種類の設定

［入力形式］ **line type** *pri_interface type*

no line type *pri_interface type*

［パラメータ］
- *pri_interface* ... PRI インタフェース名
- *type*
  - isdn , isdn-ntt ... ISDN 回線交換
  - leased ... ディジタル専用線

［説明］ PRI 回線の種類を指定する。設定の変更は、再起動か、あるいは該当インタフェースに対する **interface reset** コマンドの発行により反映される。

［デフォルト値］ leased

6.2 情報チャネルとタイムスロットの設定

［入力形式］ **pri leased channel** *pri/info timeslot_head timeslot_num*

no pri leased channel *pri/info* [*timeslot_head timeslot_num*]

［パラメータ］ • *pri* ...PRI インタフェース名

• *info* ... 情報チャネル番号(1..24)

• *timeslot_head* ... 先頭タイムスロット番号 (1..24)

• *timeslot_num* ... タイムスロット数 (1..24)

以下のニーモニックが使用可能

ニーモニック速度 (bit/s)	タイムスロット数
64k	1
128k	2
192k	3
256k	4
384k	6
512k	8
768k	12
1024k	16
1536k	24

［説明］ 指定した PRI 回線内の情報チャネルを、先頭タイムスロット番号とタイムスロット数(通信速度) で設定する。

［ノート］ 同じ情報チャネルに対する設定を変更するには、あらかじめ **no pri leased channel** で設定を削除しておく必要がある。設定変更時には再起動か、対象の PRI インタフェースに対する **interface reset** コマンドが必要である。多重化非対応の PRI 拡張モジュール (YBA-1PRI-N)では 2 つ以上の情報チャネルの設定はできない。

6.3 PPで使用するインタフェースの設定

［入力形式］ **pp bind** *wan-interface* [*wan_interface...*]

no pp bind [*wan_interface...*]

［パラメータ］ • *wan_interface* ... BRI/PRI インタフェース名

［説明］ 選択されている相手先に対して実際に使用するインタフェースを設定する。

［デフォルト値］ どのインタフェースともバインドされていない

7. IPの設定

7.1 インタフェース共通の設定

7.1.1 IPパケットを扱うか否かの設定

［入力形式］ **ip routing** *routing*

no ip routing [*routing*]

［パラメータ］ • *routing*

◦ on ... IP パケットを処理対象として扱う

◦ off ... IP パケットを処理対象として扱わない

［説明］ IP パケットをルーティングするかどうかを設定する。

［ノート］ off の場合でも TELNET による設定や TFTP によるアクセス、PING 等は可能。

［デフォルト値］ on

7.1.2 IPアドレスの設定

［入力形式］ **ip *interface* address** *ip_address/netmask* [broadcast *broadcast_ip*]

no ip *interface* address [*ip_address/netmask* ...]

［パラメータ］ • ***interface*** ... LAN インタフェース名、もしくは pp

• *ip_address* ... IP アドレス xxx.xxx.xxx.xxx (xxx は 10 進数)

• *netmask* ... ネットマスク長をあらわす 10 進数

• *broadcast_ip* ... ブロードキャスト IP アドレス

［説明］ インタフェースの IP アドレスとネットマスクを設定する。“ broadcast *broadcast_ip* ” を指定すると、ブロードキャストアドレスを指定できる。省略した場合には、ディレクティッドブロードキャストアドレスが使われる。

［ノート］ LAN インタフェースに IP アドレスを設定していない場合には、RARP により IP アドレスを得ようとする。

PP インタフェースに IP アドレスを設定していない場合には、そのインタフェースは unnumbered として動作する。

［デフォルト値］ IP アドレスは設定されていない。

ディレクティッドブロードキャストアドレスが使われる。

7.1.3 経路情報の設定

［入力形式］

ip route *network* gateway *gateway* [*options*...] [[gateway *gateway* [*options*...]]...]

no ip route *network* [gateway ...]

［パラメータ］

• *network*

◦ default ... デフォルト経路

◦ ip_address/mask ... ネットワーク経路

◦ ip_address ... ホスト経路

• *gateway*

◦ ip_address ... ゲートウェイの IP アドレス

◦ pp *pp_num* [dlci=*dlci*]... PP インタフェースへの経路

“ dlci=*dlci* ”が指定された時は、フレームリレーの DLCI への経路

◦ pp anonymouns name=*name* ... 名前によるルーティング

◦ tunnel *tunnel_num* ... Tunnel インタフェースへの経路

• *options* ... 経路情報のオプション

◦ metric *metric*... *metric* はメトリックを 1 ～ 15 の範囲で指定する。指定がない時は 1。

◦hide ... 出力インタフェースが PP インタフェースの場合にのみ有効なオプションで、回線がつながっている時だけ経路が有効となることを意味する。

◦filter *filter_num_list* ... フィルタ型経路を指定する。*filter_num_list* はフィルタ番号の列を空白で区切って複数指定できる

［説明］

IP の静的経路を設定する。

filterが指定されている“ gateway ... ”が記述されている場合には、記述されている順にフィルタを適用していき、マッチしたゲートウェイが選択される。

マッチするゲートウェイが存在しない場合や、filterが指定されているゲートウェイが一つも記述されていない場合には、filterが指定されていないゲートウェイが選択される。

filterが指定されていないゲートウェイも存在しない場合には、その経路は存在しないものとして処理が継続される。

filterが指定されていないゲートウェイが複数記述された場合で、それらの経路を使うべき時にどちらを使うかは、ラウンドロビンにより決定される。

いずれの場合でも、hideが指定されている PP インタフェースへのゲートウェイは回線がつながっている時だけ有効で、回線がつながっていない時には参照されない。

［ノート］

既に存在する経路を上書きすることができる。

［設定例］

デフォルトゲートウェイを 192.168.0.1 とする

```
ip route default gateway 192.168.0.1
```

PP1 で接続している相手のネットワークは 192.168.1.0/24 である

```
ip route 192.168.1.0/24 gateway pp 1
```

7.1.4 IPパケットのフィルタの設定

［入力形式］ **ip filter** *filter_number pass_reject src_addr*[*/mask*] [*dest_addr*[*/mask*][*proto* [*src_port_list* [*dest_port_list*]]]]

no ip filter *filter_number* [*pass_reject ...*]

［パラメータ］ • *filter_number ...* フィルタの番号(1..100)

• *pass_reject*

キーワード	通過条件	ログへの記録
pass	一致すれば通す	記録しない
pass-log		記録する
pass-nolog		記録しない
reject	一致すれば破棄する	記録する
reject-log		
reject-nolog		記録しない
restrict	回線が接続されていれば通し、切断されていれば破棄する	パケットを破棄した時だけ記録する
restrict-log		記録する
restrict-nolog		記録しない

• *src_addr ...* IP パケットの始点 IP アドレス

◦ xxx.xxx.xxx.xxx、xxx は

▻ 10 進数

▻ * (ネットマスクの対応するビットが 8 ビットとも 0 と同じ)

◦ 間に－をはさんだ 2 つの上項目、－を前につけた上項目、－を後ろにつけた上項目、これらは範囲を指定する。

◦ * (すべての IP アドレスに対応)

• *dest_addr ...* IP パケットの終点 IP アドレス(*src_addr* と同じ形式)。

省略した時は 1 個の * と同じ。

• *mask ...* IP アドレスのビットマスク、省略した時は 0xffffffff と同じ。*src_addr* 及び *dest_addr* がネットワークアドレスの場合にのみ指定可

◦ xxx.xxx.xxx.xxx (xxx は 10 進数)

◦ 0x に続く 16 進数

◦ マスクビット数

• *proto ...* フィルタリングするパケットの種類

◦ プロトコルを表す 10 進数

◦ プロトコルを表すニーモニック

icmp	1
tcp	6
udp	17

◦ 上項目のカンマで区切った並び (5 個以内)

◦ * (すべてのプロトコル)

◦ established

省略した時は * と同じ。

• *src_port* ... UDP 、TCP のソースポート番号

◦ポート番号を表す 10 進数

◦ポート番号を表すニーモニック(一部)

ニーモニック	ポート番号
ftp	20, 21
ftpdata	20
telnet	23
smtp	25
domain	53
gopher	70
finger	79
www	80
pop3	110
sunrpc	111
ident	113
ntp	123
nntp	119
snmp	161
syslog	514
printer	515
talk	517
route	520
uucp	540

◦間に－ をはさんだ 2 つの上項目、－を前につけた上項目、－を後ろにつけた上項目、これらは範囲を指定する。

◦上項目のカンマで区切った並び(10 個以内)

◦* (すべてのポート)

省略した時は * と同じ。

• *dest_port* ... UDP 、TCP のデスティネーションポート番号

［説明］ IP パケットのフィルタを設定する。このコマンドで設定されたフィルタは **ip route** コマンド、**ip *interface* secure filter** コマンド、**ip tos supersede** コマンド及び **ip *interface* rip filter** コマンドで用いられる。

［ノート］ restrict-log 及び restrict-nolog を使ったフィルタは、回線が接続されている時だけ通せば十分で、そのために回線に発信するまでもないようなパケットに対して有効である。例えば、時計をあわせる NTP パケット。

“ ip filter pass * * icmp,tcp telnet ” などのように、TCP/UDP 以外のプロトコルとポート番号の両方が指定されている場合、TCP/UDP 以外のパケットに関しては、ポート番号の指定をチェックしない。

“ ip filter pass * * *telnet ” などのように、TCP/UDP と明記せずにポート番号を指定していた場合、TCP/UDP 以外もフィルタに該当する。

［設定例］ # ip filter 3 pass-nolog 172.20.10.* 172.21.192.0/18 tcp ftp

7.1.5 フィルタリングによるセキュリティの設定

［入力形式］ **ip *interface* secure filter** *direction filter_list*

no ip *interface* secure filter *direction* [*filter_list*]

［パラメータ］ • ***interface*** ... LAN インタフェース名、pp、tunnel

• *direction*

◦ in ... 受信したパケットのフィルタリング

◦ out ... 送信するパケットのフィルタリング

• *filter_list* ... 100 個以内の、空白で区切られたフィルタ番号の並び

［説明］ **ip filter** コマンドによるパケットのフィルタを組み合わせて、インタフェースで送受信するパケットの種類を制限する。

［ノート］ フィルタリストを走査して、一致すると通過、破棄が決定する。

ip filter 1 pass 192.168.0.0/24 *

ip filter 2 reject 192.168.0.1

ip lan1 secure filter in 1 2

この設定の場合では、始点 IP アドレスが 192.168.0.1 であるパケットは、最初のフィルタ 1 で通過が決定してしまうため、フィルタ 2 での検査は行われない。そのため、フィルタ 2 は何も意味を持たない。

フィルタリストを操作した結果、どのフィルタにも一致しないパケットは破棄される。

［デフォルト値］ フィルタは設定されていない。

7.1.6 Source-route オプション付き IP パケットをフィルタアウトするか否かの設定

［入力形式］ **ip filter source-route** *filter_out*

no ip filter source-route [*filter_out*]

［パラメータ］ • *filter_out*

◦ on ... フィルタアウトする

◦ off ... フィルタアウトしない

［説明］ Source-route オプション付き IP パケットをフィルタアウトするか否かを設定する。

［デフォルト値］ on

7.1.7 Directed-Broadcast パケットをフィルタアウトするか否かの設定

［入力形式］ **ip filter directed-broadcast** *filter_out*

no ip filter directed-broadcast [*filter_out*]

［パラメータ］ • *filter_out*

◦ on ... フィルタアウトする

◦ off ... フィルタアウトしない

［説明］ 終点 IP アドレスが Directed-Broadcast アドレス宛になっている IP パケットをルータが接続されているネットワークにブロードキャストするか否かを設定する。

［ノート］ いわゆる smurf 攻撃を防止するためには on にしておく。

［デフォルト値］ on

7.1.8 IPパケットのTOSフィールドの書き換えの設定

［入力形式］ **ip tos supersede** *N tos* [precedence=*precedence*] *filter_number* [*filter_number_list*]

no ip tos supersede *N* [*tos* ...]

［パラメータ］ • *N* ... 識別番号(1..65535)

• *tos* ... 書き換える TOS 値(0-15)

以下のニーモニックが利用できる

normal	0
min-monetary-cost	1
max-reliability	2
max-throughput	4
min-delay	8

• *precedence*

◦ PRECEDENCE 値 (0..7)

◦ *precedence* を省略した場合は PRECEDENCE 値は変更しない

• *filter_number*、*filter_number_list* ... フィルタの番号(1..100)

［説明］ IP パケットを中継するときに TOS フィールドを指定した値に書き換える。

識別番号順にリストをチェックし、*filter_number* リストのフィルタを順次適用していく。そして、最初にマッチした IP フィルタが pass、pass-log、pass-nolog、restrict、restrict-log、restrict-nolog のいずれかであれば TOS フィールドが書き換えられる。

reject、reject-log または reject-nolog である場合は書き換えずに処理を終わる。

7.1.9 インタフェースの MTU の設定

［入力形式］ **ip** *interface* mtu *mtu*

no ip *interface* mtu [*mtu*]

［パラメータ］ • *interface* ... LAN インタフェース名、もしくは pp

• *mtu* ... MTU の値(64..1500)

［説明］ 各インタフェースの MTU の値を設定する。

［ノート］ 実際にはこの設定が適用されるのは IP パケットだけである。他のプロトコルには適用されず、それらではデフォルトのまま 1500 の MTU となる。

［デフォルト値］ 1500

7.2 LAN側の設定

7.2.1 セカンダリIPアドレスの設定

［入力形式］ **ip *interface* secondary address** *ip_address/netmask*

no ip *interface* secondary address [*ip_address/netmask*]

［パラメータ］ • ***interface*** ... LANインタフェース名

• *ip_address* ... セカンダリIPアドレス xxx.xxx.xxx.xxx (xxxは10進数)

• *netmask* ... ネットマスク長をあらわす10進数

［説明］ LAN側のセカンダリIPアドレスとネットマスクを設定する。

［ノート］ セカンダリのネットワークでのブロードキャストアドレスは必ずディレクティッドブロードキャストアドレスが使われる。

PPインタフェースに対してはセカンダリアドレスは設定できない。

7.2.2 代理ARPの設定

［入力形式］ **ip *interface* proxyarp** *proxyarp*

no ip *interface* proxyarp [*proxyarp*]

［パラメータ］ • ***interface*** ... LANインタフェース名

• *proxyarp*

◦ on ... 代理ARP動作をする

◦ off ... 代理ARP動作をしない

［説明］ 代理ARP動作をするか否か設定する。

［デフォルト値］ off

7.3 PP 側相手毎の IP の設定

7.3.1 相手の PP 側 IP アドレスの設定

［入力形式］ **ip pp remote address** *ip_address*

no ip pp remote address [*ip_address*]

［パラメータ］ • *ip_address*

◦ IP アドレス ... xxx.xxx.xxx.xxx (xxx は 10 進数)

◦ dhcp ... 自分自身の DHCP サーバ機能より IP アドレスを割り当てる

［説明］ 選択されている相手の PP 側の IP アドレスを設定する。

［ノート］ 実際に設定される IP アドレスは **ppp ipcp ipaddress** コマンドと相手の設定により決まる。自分側で設定した IP アドレスを xxx.xxx.xxx.xxx 、相手先が要求してくる IP アドレスを yyy.yyy.yyy.yyy とすると実際に設定される IP アドレスは次のようになる。

ip pp remote address の設定	**ppp ipcp ipaddress on**		**ppp ipcp ipaddress off**
	相手側 設定あり	相手側 設定なし	
なし	yyy.yyy.yyy.yyy	Unnumbered	Unnumbered
xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx または接続不可	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx

［デフォルト値］ 相手側 IP アドレスは設定されていない。

［設定例］ 例えば、ルータ A 側が no ip pp remote address、ppp ipcp ipaddress on と設定し、接続するルータ B 側が ip pp local address yyy.yyy.yyy.yyy と設定している場合には、実際のルータ A の PP 側の IP アドレスは yyy.yyy.yyy.yyy になることを意味します。

7.3.2 リモート IP アドレスプールの設定

［入力形式］ **ip pp remote address pool** *ip_address* [*ip_address...*]

ip pp remote address pool *ip_address-ip_address*

ip pp remote address pool dhcp

no ip pp remote address pool [...]

［パラメータ］ • *ip_address* ... anonymous のためにプールする IP アドレス

• *ip_address-ip_address* ... IP アドレスの範囲

• dhcp ... 自分自身の DHCP サーバ機能を利用する

［説明］ anonymous で相手に割り当てるための IP アドレスプールを設定する。

dhcp を設定した場合は、自分自身が DHCP サーバとして動作している必要がある。自分で管理している DHCP スコープの中から、IP アドレスを割り当てる。

RT300i では装着されている BRI/PRI インタフェースで利用できる ISDN Bch の数まで設定できる。

RT200i では 16 個まで、RT140p では 8 個まで、RT140i、RT140e、RT140f では 4 個まで、それ以外では 2 個までとなる。

PP として anonymous が選択された時のみ有効である。

7.4 RIPの設定

7.4.1 RIPを使用するか否かの設定

［入力形式］ **rip use** *rip_use*

no rip use *rip_use*

［パラメータ］ • *rip_use*

◦ on ... RIP を使用する

◦ off ... RIP を使用しない

［説明］ RIP を使用するか否かを設定する。この機能を off にすると、すべてのインタフェースに対して RIP パケットを送信することはなくなり、受信した RIP パケットは無視される。

［デフォルト値］ off

7.4.2 RIPによる経路の優先度の設定

［入力形式］ **rip preference** *rip_preference*

no rip preference *rip_preference*

［パラメータ］ • *rip_preference* ... 1 以上の数値

［説明］ RIP により得られた経路の優先度を設定する。経路の優先度は 1 以上の数値で表され、数字が小さい程優先度が高い。スタティックと RIP など複数のプロトコルで得られた経路が食い違う場合には、優先度が高い方が採用される。優先度が同じ場合には時間的に先に採用された経路が有効となる。

［ノート］ スタティック経路の優先度は 10000 で固定である。

［デフォルト値］ 1000

7.4.3 RIPパケットの受信に関する設定

［入力形式］ **ip *interface* rip receive** *rip_receive* [verion *version* [*version*]]

no ip *interface* rip receive [*rip_receive...*]

［パラメータ］ • *interface* ... LAN インタフェース名、もしくは pp

• *rip_receive*

◦ on ... RIP パケットを受信する

◦ off ... RIP パケットを受信しない

• *version* ... RIP のバージョンを表し、1 または 2

［説明］ 指定したインタフェースに対し、RIP パケットを受信するか否かを設定する。
“ version *version* ” で受信する RIP のバージョンを指定できる。指定しない場合は、RIP1/2 ともに受信する。

［デフォルト値］ on version 1 2

7.4.4 RIPに関して信用できるゲートウェイの設定

［入力形式］ **ip *interface* rip trust gateway** [except] *gateway_list*

no ip *interface* rip trust gateway [[except] *gateway_list*]

［パラメータ］ • *interface* ... LAN インタフェース名、もしくは pp

• *gateway_list* ... 10 個以内の IP アドレスの並び

［説明］ RIP に関して信用できる、あるいは信用できないゲートウェイを設定する。

“ except ” を指定していない時には、列挙したゲートウェイを信用できるゲートウェイとし、それらからの RIP だけを受信する。

“ except ” を指定した場合は、列挙したゲートウェイを信用できないゲートウェイとし、それらを除いた他のゲートウェイからの RIP だけを受信する。

［デフォルト値］ 信用できる、あるいは信用できないゲートウェイは設定されておらず、すべてのホストからの RIP を信用できるものとして扱う。

7.4.5 RIPのフィルタリングの設定

［入力形式］ **ip *interface* rip filter** *direction filter_list*

no ip *interface* rip filter *direction filter_list*

［パラメータ］ • ***interface*** ... LAN インタフェース名、もしくは pp

• *direction*

◦ in ... 受信した RIP のフィルタリング

◦ out ... 送信する RIP のフィルタリング

• *filter_list*

◦ 空白で区切られた filter_number の並び(100 個以内)

［説明］ インタフェースで送受信する RIP のフィルタリングを設定する。

ip filter コマンドで設定されたフィルタの始点 IP アドレスが、送受信する RIP の経路情報にマッチする時は、フィルタが pass であればそれを処理し、reject であればその経路情報だけを破棄する。

［デフォルト値］ フィルタは設定されていない

7.4.6 RIPで加算するホップ数の設定

［入力形式］ **ip *interface* rip hop** *direction hop*

no ip *interface* rip hop *direction hop*

［パラメータ］ • ***interface*** ... LAN インタフェース名、もしくは pp

• *direction*

◦ in ... 受信した RIP に加算する

◦ out ... 送信する RIP に加算する

• *hop* ... 加算する値 (0..15)

［説明］ インタフェースで送受信する RIP に加算するホップ数を設定する。

［デフォルト値］ 0

7.4.7 RIP2での認証の設定

［入力形式］ **ip *interface* rip auth type** *type*

no ip *interface* rip auth type [*type*]

［パラメータ］ • ***interface*** ... LAN インタフェース名、もしくは pp

• *type*

◦ none ... 認証しない

◦ text ... テキスト型の認証を行なう

［説明］ RIP2 を使用する時のインタフェースでの認証の設定をする。none の場合は認証なし。text の時はテキスト型の認証を行う。

［デフォルト値］ none

7.4.8 RIP2での認証キーの設定

［入力形式］ **ip *interface* rip auth key** *hex_key*

ip *interface* rip auth key text *text_key*

no ip *interface* rip auth key [...]

［パラメータ］ • *interface* ... LAN インタフェース名、もしくは pp

• *hex_key* ... 16 進数の列で表現された認証キー

• *text_key* ... 文字列で表現された認証キー

［説明］ RIP2 を使用する時のインタフェースの認証キーを設定する。

［設定例］ # ip lan1 rip auth key text testing123

ip pp rip auth key text "hello world"

ip lan2 rip auth key 01 02 ff 35 8e 49 a8 3a 5e 9d

7.4.9 RIPによる経路を回線が切れても保持し続けるか否かの設定

［入力形式］ **ip pp rip hold routing** *rip_hold*

no ip pp rip hold routing [*rip_hold*]

［パラメータ］ • *rip_hold*

◦ on ... 回線が切断されても RIP による経路を保持し続ける

◦ off ... 回線が切断されたら RIP による経路を破棄する

◦ *version* ... RIP のバージョンを表し、1 または 2

［説明］ PP インタフェースから RIP で得られた経路を、回線が切断された時に保持し続けるかどうかを設定する。

［デフォルト値］ off

7.4.10 回線接続時の PP 側の RIP の動作の設定

［入力形式］ **ip pp rip connect send** *rip_action*

no ip pp rip connect send [*rip_action*]

［パラメータ］ • *rip_action*

◦ interval ... **ip pp rip connect interval** コマンドで設定された時間間隔で RIP を送出する

◦ update ... 経路情報が変わった時にのみ RIP を送出する

［説明］ 選択されている相手について回線接続時に RIP を送出する条件を設定する。

［デフォルト値］ update

7.4.11 回線接続時の PP 側の RIP 送出の時間間隔の設定

［入力形式］ **ip pp rip connect interval** *time*

no ip pp rip connect interval [*time*]

［パラメータ］ • *time* ... 秒数 (30..21474836)

［説明］ 選択されている相手について回線接続時に RIP を送出する時間間隔を設定する。

ip pp routing protocol コマンドが rip 、**ip pp rip connect send** コマンドが interval の時に有効である。

［デフォルト値］ 30

7.4.12 回線切断時の PP 側の RIP の動作の設定

［入力形式］ **ip pp rip disconnect send** *rip_action*

no ip pp rip disconnect send [*rip_action*]

［パラメータ］ • *rip_action*

◦ none ... 回線切断時に RIP を送出しない

◦ interval ...**ip pp rip disconnect interval** コマンドで設定された時間間隔で RIP を送出する

◦ update ... 経路情報が変わった時にのみ RIP を送出する

［説明］ 選択されている相手について回線切断時に RIP を送出する条件を設定する。

［デフォルト値］ none

7.4.13 回線切断時の PP 側の RIP 送出の時間間隔の設定

［入力形式］ **ip pp rip disconnect interval** *time*

no ip pp rip disconnect interval [*time*]

［パラメータ］ • *time* ... 秒数(30..21474836)

［説明］ 選択されている相手について回線切断時に RIP を送出する時間間隔を設定する。

ip pp routing protocol コマンドが rip 、**ip pp rip disconnect send** コマンドが interval の時に有効である。

［デフォルト値］ 3600

8 IPsecの設定

本機は、暗号化によりIP通信に対するセキュリティを保証するIPsec機能を実装しています。IPsecでは、鍵交換プロトコルIKE (Internet Key Exchange)を使用します。必要な鍵はIKEにより自動的に生成されますが、鍵の種となる事前共有鍵は**ipsec ike pre-shared-key**コマンドで事前に登録しておく必要があります。この鍵はセキュリティ・ゲートウェイごとに設定できます。また、鍵交換の要求に応じるかどうかは、**ipsec ike remote address**コマンドで設定します。

鍵や鍵の寿命、暗号や認証のアルゴリズムなどを登録した管理情報は、SA (Security Association)で管理します。SAを区別するIDは自動的に付与されます。SAのIDや状態は**show ipsec sa**コマンドで確認することができます。SAには、鍵の寿命に合わせた寿命があります。SAの属性のうちユーザが指定可能なパラメータをポリシーと呼びます。またその番号はポリシーIDと呼び、**ipsec sa policy**コマンドで定義し、**ipsec ike duration ipsec-sa**、**ipsec ike duration isakmp-sa**コマンドで寿命を設定します。

SAの削除は**ipsec sa delete**コマンドで、SAの初期化は**ipsec refresh sa**コマンドで行います。**ipsec auto refresh**コマンドにより、SAを自動更新させることも可能です。

IPsecによる通信には、大きく分けてトンネルモードとトランスポートモードの2種類があります。

トンネルモードはIPsecによるVPN (Virtual Private Network)を利用するためのモードです。ルータがセキュリティ・ゲートウェイとなり、LAN上に流れるIPパケットデータを暗号化して対向のセキュリティ．ゲートウェイとの間でやりとりします。ルータがIPsecに必要な処理をすべて行うので、LAN上の始点や終点となるホストには特別な設定を必要としません。

トンネルモードを用いる場合は、トンネルインタフェースという仮想的なインタフェースを定義し、処理すべきIPパケットがトンネルインタフェースに流れるように経路を設定します。個々のトンネルインタフェースはトンネルインタフェース番号で管理されます。設定のためにトンネル番号を切替えるには**tunnel select**コマンドを使用します。トンネルインタフェースを使用するか使用しないかは、それぞれ**tunnel enable**、**tunnel disable**コマンドを使用します。

相手先情報番号による設定		トンネルインタフェース番号による設定
pp enable		**tunnel enable**
pp disable	⇔	**tunnel disable**
pp select		**tunnel select**

トランスポートモードは特殊なモードであり、ルータ自身が始点または終点になる通信に対してセキュリティを保証するモードです。ルータからリモートのルータへtelnetで入るなどの特殊な場合に利用できます。トランスポートモードを使用するには**ipsec transport**コマンドで定義を行い、使用をやめるには**no ipsec transport**コマンドで定義を削除します。

トンネルモードとトランスポートモードは併用が可能ですが、それぞれを二重に適用することはできません。

IPsecによる通信では、セキュリティ・ゲートウェイとなる本機のプログラムのリビジョンに注意してください。これらはリビジョンにより以下のように区別されます。IPsecリリース2とIPsecリリース3は相互接続性がありますが、後者の設定を前者に適合させる必要があります。

リビジョン系列	IPsec リリース 1	IPsec リリース 2	IPsec リリース 3
3.00	3.00.09 〜 11	-	-
3.01	3.01.07	3.01.11 〜	-
4.00	-	4.00.02 〜 4.00.14	4.00.18 〜
6.00	-	-	6.00.01 〜

8.1 事前共有鍵の登録

［入力形式］ **ipsec ike pre-shared-key** *gateway_id key*

ipsec ike pre-shared-key *gateway_id* text *text*

no ipsec ike pre-shared-key *gateway_id* [...]

［パラメータ］ • *gateway_id...* セキュリティ・ゲートウェイの識別子となる 1 以上の数値
最大値は、RT300i で 100、RT200i/RT140 で 20、その他は 10。

• *key ...* 鍵となる 0x ではじまる 16 進数列 (最大 32 バイト)

• *text ...* ASCII 文字列で表した鍵 (最大 32 文字)

［説明］ 鍵交換に必要な事前共有鍵を登録する。これが設定されていない場合、鍵交換は行われない。鍵交換を行う相手ルータには同じ事前共有鍵が設定されている必要がある。

［デフォルト値］ 事前共有鍵は設定されていない。

［設定例］ ipsec ike pre-shared-key 1 text himitsu

ipsec ike pre-shared-key 8 0xCDEEEDC0CDEDCD

8.2 相手側セキュリティ・ゲートウェイの IP アドレスの設定

［入力形式］ **ipsec ike remote address** *gateway_id ip_address*

no ipsec ike remote address *gateway_id* [*ip_address*]

［パラメータ］ • *gateway_id...* セキュリティ・ゲートウェイの識別子となる 1 以上の数値
最大値は、RT300i で 100、RT200i/RT140 で 20、その他は 10。

• *ip_address*

◦相手側セキュリティ・ゲートウェイの IP アドレス

◦any ... 自動選択

［説明］ 相手側セキュリティ・ゲートウェイの IP アドレスを設定する。相手側セキュリティ・ゲートウェイ 1 つに対して 1 つ設定可能である。

8.3 相手側のセキュリティゲートウェイの名前の設定

［入力形式］ **ipsec ike remote name** *gateway name*

no ipsec ike remote name *gateway* [*name*]

［パラメータ］ • *gateway ...* セキュリティゲートウェイの識別子となる 1 以上の数値。
最大値は、RT300i では 100、RT200i/RT140 では 20、その他では 10。

• *name ...* 名前 (最大 32 文字)

［説明］ 相手側のセキュリティゲートウェイの名前を設定する。

8.4 自分側セキュリティ・ゲートウェイの IP アドレスの設定

［入力形式］ **ipsec ike local address** *gateway_id ip_address*

no ipsec ike local address *gateway_id* [*ip_address*]

［パラメータ］ • *gateway_id*... セキュリティ・ゲートウェイの識別子となる 1 以上の数値

最大値は、RT300i で 100、RT200i/RT140 で 20、その他は 10。

• *ip_address*

◦自分側セキュリティ・ゲートウェイの IP アドレス

◦any ... 自動選択

［説明］ 自分側セキュリティ・ゲートウェイの IP アドレスを設定する。

［ノート］ このコマンドが設定されていないときには、相手側のセキュリティ・ゲートウェイに近いインタフェースの IP アドレスを用いて IKE を起動する。

8.5 自分側のセキュリティゲートウェイの名前の設定

［入力形式］ **ipsec ike local name** *gateway_id name*

no ipsec ike local name *gateway_id* [*name*]

［パラメータ］ • *gateway_id* ... セキュリティゲートウェイの識別子となる 1 以上の数値。

最大値は、RT300i では 100、RT200i/RT140 では 20、その他は 10。

• *name* ... 名前 (最大 32 文字)

［説明］ 自分側のセキュリティゲートウェイの名前を設定する。

8.6 鍵交換の再送回数と間隔の設定

［入力形式］ **ipsec ike retry** *count interval*

no ipsec ike retry [*count interval*]

［パラメータ］ • *count* ... 再送回数 (1..50)

• *interval* ... 再送間隔の秒数 (1..100)

［説明］ 鍵交換が失敗した時に鍵交換を繰り返す回数とその時間間隔を設定する。

［デフォルト値］ *count* = 10

interval = 5

8.7 IKEが用いる暗号アルゴリズムの設定

［入力形式］ **ipsec ike encryption** *gateway_id algorithm*

no ipsec ike encryption *gateway_id* [*algorithm*]

［パラメータ］ • *gateway_id...* セキュリティ・ゲートウェイの識別子となる 1 以上の数値

最大値は、RT300i で 100、RT200i/RT140 で 20、その他は 10。

• *algorithm ...* 暗号アルゴリズム

◦ 3des-cbc ... 3DES-CBC

◦ des-cbc ... DES-CBC

［説明］ IKE が用いる暗号アルゴリズムを設定する。

［ノート］ IKE で始動側として働くときには、このコマンドで設定されたアルゴリズムを提案する。応答側として働くときはこのコマンドの設定に関係なく、DES-CBC と 3DES-CBC を用いることができる。

［デフォルト値］ des-cbc

8.8 IKEが用いるグループの設定

［入力形式］ **ipsec ike group** *gateway_id group* [*group*]

no ipsec ike group *gateway_id* [*group* [*group*]]

［パラメータ］ • *gateway_id...* セキュリティ・ゲートウェイの識別子となる 1 以上の数値

最大値は、RT300i で 100、RT200i/RT140 で 20、その他は 10。

• *group ...* グループ識別子

◦ modp768

◦ modp1024

［説明］ IKE で用いるグループを設定する。

［ノート］ IKE で始動側として働くときにはこのコマンドで設定されたグループを提案する。応答側として働くときはこのコマンドの設定に関係なく、MODP768 と MODP1024 を用いることができる。
2 種類のグループを設定したときには、1 つ目がフェーズ 1 で、2 つ目がフェーズ 2 で提案される。グループを 1 種類しか設定しないときは、フェーズ 1 とフェーズ 2 の両方で、設定したグループが提案される。

［デフォルト値］ modp768

8.9 IKEが用いるハッシュアルゴリズムの設定

［入力形式］ **ipsec ike hash** *gateway_id algorithm*

no ipsec ike hash *gateway_id* [*algorithm*]

［パラメータ］ • *gateway_id*... セキュリティ・ゲートウェイの識別子となる 1 以上の数値

最大値は、RT300i で 100、RT200i/RT140 で 20、その他は 10。

• *algorithm* ... ハッシュアルゴリズム

◦ md5 ... MD5

◦ sha ... SHA-1

［説明］ IKE が用いるハッシュアルゴリズムを設定する。

［ノート］ IKE で始動側として働くときには、このコマンドで設定されたアルゴリズムを提案する。応答側として働くときはこのコマンドの設定に関係なく、MD5 と SHA-1 を用いることができる。

［デフォルト値］ md5

8.10 自分側の ID の設定

［入力形式］ **ipsec ike local id** *gateway_id ip_address*[*/mask*]

no ipsec ike local id *gateway_id* [*ip_address*[*/mask*]]

［パラメータ］ • *gateway_id*... セキュリティ・ゲートウェイの識別子となる 1 以上の数値

最大値は、RT300i で 100、RT200i/RT140 で 20、その他は 10。

• *ip_address* ... IP アドレス

• *mask* ... ネットマスク

［説明］ IKE のフェーズ 2 で用いる自分側の ID を設定する。

［ノート］ このコマンドが設定されていないときには、ID を送信しない。*mask* パラメータを省略したときは、タイプ 1 の ID が送信される。また、*mask* パラメータを指定したときは、タイプ 4 の ID が送信される。

8.11 IKEのログの種類の設定

［入力形式］ **ipsec ike log** *gateway_id type* [*type* ...]

no ipsec ike log *gateway_id* [*type* ...]

［パラメータ］ • *gateway_id*... セキュリティ・ゲートウェイの識別子となる 1 以上の数値

最大値は、RT300i で 100、RT200i/RT140 で 20、その他は 10。

• *type* ... 出力するログの種類

◦ message-info ... IKE メッセージの内容

◦ payload-info ... ペイロードの処理内容

◦ key-info ... 鍵計算の処理内容

［説明］ 出力するログの種類を設定する。ログはすべて、syslog の debug レベルで出力される。

［ノート］ このコマンドが設定されていないときには、最小限のログしか出力しない。複数の *type* パラメータを設定することもできる。

8.12 IKEペイロードのタイプの設定

［入力形式］ **ipsec ike payload type** *gateway_id type*

no ipsec ike payload type *gateway_id* [*type*]

［パラメータ］ •*gateway_id*... セキュリティ・ゲートウェイの識別子となる 1 以上の数値
最大値は、RT300i で 100、RT200i/RT140 で 20、その他は 10。

• *type* ... ペイロードのタイプ

◦ 1 ... IPsec リリース 2 以前

◦ 2 ... IPsec リリース 3

［説明］ IKE ペイロードのタイプを設定する。YAMAHA リモートルータの古いリビジョンと接続するときには、タイプを 1 に設定する必要がある。

［デフォルト値］ 2

8.13 PFSを用いるか否かの設定

［入力形式］ **ipsec ike pfs** *gateway_id pfs*

no ipsec ike pfs *gateway_id* [*pfs*]

［パラメータ］ • *gateway_id*... セキュリティ・ゲートウェイの識別子となる 1 以上の数値
最大値は、RT300i で 100、RT200i/RT140 で 20、その他は 10。

• *pfs*

◦ on ... 用いる

◦ off ... 用いない

［説明］ IKE で PFS を用いるか否かを設定する。

［ノート］ 相手側のセキュリティ・ゲートウェイと同じように設定する必要がある。

［デフォルト値］ off

8.14 相手側の ID の設定

［入力形式］ **ipsec ike remote id** *gateway_id ip_address*[*/mask*]

no ipsec ike remote id *gateway_id* [*ip_address*[*/mask*]]

［パラメータ］ • *gateway_id*... セキュリティ・ゲートウェイの識別子となる 1 以上の数値
最大値は、RT300i で 100、RT200i/RT140 で 20、その他は 10。

• *ip_address* ... IP アドレス

• *mask* ... ネットマスク

［説明］ IKE のフェーズ 2 で用いる相手側の ID を設定する。

［ノート］ このコマンドが設定されていないときには ID を送信しない。
mask パラメータを省略したときは、タイプ 1 の ID が送信される。また、*mask* パラメータを指定したときは、タイプ 4 の ID が送信される。

8.15 IKEの情報ペイロードを送信するか否かの設定

［入力形式］ **ipsec ike send info** *gateway_id info*

no ipsec ike send info *gateway_id* [*info*]

［パラメータ］ • *gateway_id*... セキュリティ・ゲートウェイの識別子となる 1 以上の数値

最大値は、RT300i で 100、RT200i/RT140 で 20、その他は 10。

• *info*

◦ on ... 送信する

◦ off ... 送信しない

［説明］ IKE の情報ペイロードを送信するか否かを設定する。受信に関しては、この設定に関わらず、すべての情報ペイロードを解釈する。

［ノート］ このコマンドは、接続性の検証などの特別な目的で使用される。定常の運用時は on に設定する必要がある。

［デフォルト値］ on

8.16 SA 関連の設定

再起動されるとすべての SA がクリアされることに注意しなくてはいけない。

8.16.1 SA のポリシーの定義

［入力形式］ **ipsec sa policy** *policy_id gateway_id* ah *ah_algorithm*

ipsec sa policy *policy_id gateway_id* esp *esp_algorithm* [*ah_algorithm*]

no ipsec sa policy *policy_id* [*gateway_id ...*]

［パラメータ］
- *policy_id ...* ポリシー ID (1..255)
- *gateway_id...* セキュリティ・ゲートウェイの識別子となる 1 以上の数値
  最大値は、RT300i で 100、RT200i/RT140 で 20、その他は 10。
- ah ... 認証ヘッダ (Authentication Header)を示すキーワード
- esp ... 暗号ペイロード (Encapsulating Security Payload)を示すキーワード
- *ah_algorithm*
  - md5-hmac ... HMAC-MD5
  - sha-hmac ... HMAC-SHA
- *esp_algorithm*
  - 3des-cbc ... 3DES-CBC
  - des-cbc ... DES-CBC

［説明］ SA のポリシーを定義する。この定義はトンネルモード及びトランスポートモードの設定に必要である。この定義は複数のトンネルモード及びトランスポートモードで使用できる。

8.16.2 IPsec SAの寿命の設定

［入力形式］ **ipsec ike duration ipsec-sa** *gateway_id second* [*kbytes*]

no ipsec ike duration ipsec-sa *gateway_id* [*second* [*kbytes*]]

［パラメータ］
- *gateway_id...* セキュリティ・ゲートウェイの識別子となる 1 以上の数値
  最大値は、RT300i で 100、RT200i/RT140 で 20、その他は 10。
- *second ...* 秒数(300..691200)
- *kbytes ...* キロ単位のバイト数(100..100000)

［説明］ IKE で提案する IPsec SA の寿命を設定する。

kbytes パラメータを指定した場合には、*second* パラメータで指定した時間を経過するか指定したバイト数のデータが処理された後に SA は消滅する。

［デフォルト値］ 28800

8.16.3 ISAKMP SAの寿命の設定

［入力形式］ **ipsec ike duration isakmp-sa** *gateway_id second* [*kbytes*]

no ipsec ike duration isakmp-sa *gateway_id* [*second* [*kbytes*]]

［パラメータ］ • *gateway_id*... セキュリティ・ゲートウェイの識別子となる 1 以上の数値

最大値は、RT300i で 100、RT200i/RT140 で 20、その他は 10。

• *second* ... 秒数 (300..691200)

• *kbytes* ... キロ単位のバイト数 (100..100000)

［説明］ IKE で提案する ISAKMP SA の寿命を設定する。

kbytes パラメータを指定した場合には、*second* パラメータで指定した時間を経過するか指定したバイト数のデータが処理された後に SA は消滅する。

［デフォルト値］ 28800

8.16.4 SA の削除

［入力形式］ **ipsec sa delete** *id*

［パラメータ］ • *id*

◦ SA の ID (1 以上の整数)

◦ all ... すべての SA

［説明］ 指定した SA を削除する。

SA の ID は自動的に付与され、**show ipsec sa** コマンドで確認することができる。

8.16.5 SA の手動更新

［入力形式］ **ipsec refresh sa**

［パラメータ］ なし

［説明］ SA を手動で更新する。

［ノート］ 管理されている SA をすべて削除して、IKE の状態を初期化する。

8.16.6 SA を自動更新するか否かの設定

［入力形式］ **ipsec auto refresh** *refresh*

no ipsec auto refresh [*refresh*]

［パラメータ］ • *refresh*

◦ on ... 自動更新する

◦ off ... 自動更新しない

［説明］ SA を自動更新するか否かを設定する。

［ノート］ 古い SA を削除せずに新しい SA を生成する。

［デフォルト値］ off

8.17 トンネルインタフェース関連の設定

8.17.1 使用する SA のポリシーの設定

［入力形式］ **ipsec tunnel** *policy_id*

no ipsec tunnel [*policy_id*]

［パラメータ］ • *policy_id* ... 1 ～ 255 の整数

［説明］ 選択されているトンネルインタフェースで使用する SA のポリシーを設定する。

［デフォルト値］ SA のポリシーは設定されていない。

8.17.2 IPCompによるデータ圧縮の設定

［入力形式］ **ipsec ipcomp type** *type*

no ipsec ipcomp type [*type*]

［パラメータ］ • *type*

◦ deflate ... deflate 圧縮でデータを圧縮する

◦ none ... データ圧縮を行わない

［説明］ IPComp でデータ圧縮を行うかどうかを設定する。サポートしているアルゴリズムは deflate のみである。

受信した IPComp パケットを展開するためには、特別な設定を必要としない。すなわち、サポートしているアルゴリズムで圧縮された IPComp パケットを受信したときには、設定に関係なく展開する。

必ずしもセキュリティ．ゲートウェイの両方にこのコマンドを設定する必要はない。片側にのみ設定した場合には、そのセキュリティ．ゲートウェイから送信される IP パケットのみが圧縮される。

トランスポートモードのみを使用する場合には、IPComp を使用することはできない。

［ノート］ データ圧縮には、PPP で使われる CCP や、フレームリレーで使われる FRF.9 もある。圧縮アルゴリズムとして、IPComp で使われる deflate と、CCP/FRF.9 で使われる Stac-LZS との間に基本的な違いはない。しかし、CCP/FRF.9 でのデータ圧縮は IPsec による暗号化の後に行われる。このため、暗号化でランダムになったデータを圧縮しようとすることになり、ほとんど効果がない。一方、IPComp は IPsec による暗号化の前にデータ圧縮が行われるため、一定の効果が得られる。また、CCP/FRF.9 とは異なり、対向のセキュリティ．ゲートウェイまでの全経路で圧縮されたままのデータが流れるため、例えば本機の出力インタフェースが LAN であってもデータ圧縮効果を期待できる。

［デフォルト値］ none

8.18 トランスポートモード関連の設定

8.18.1 トランスポートモードの定義

［入力形式］ **ipsec transport** *id policy_id* [*proto* [*src_port_list* [*dst_port_list*]]]

no ipsec transport *id* [*policy_id* [*proto* [*src_port_list* [*dst_port_list*]]]]

［パラメータ］
- *id* ... トランスポート ID (1..255)
- *policy_id* ... ポリシー ID(1..255)
- *proto* ... プロトコル
- *src_port_list* ... UDP、TCP のソースポート番号列
  - ポート番号を表す 10 進数
  - ポート番号を表すニーモニック
  - * (すべてのポート)
- *dst_port_list* ... UDP、TCP のデスティネーションポート番号列
  - ポート番号を表す 10 進数
  - ポート番号を表すニーモニック
  - * (すべてのポート)

［説明］ トランスポートモードを定義する。

定義後、*proto*、*src_port_list*、*dst_port_list* パラメータに合致する IP パケットに対してトランスポートモードでの通信を開始する。

［設定例］ 192.168.112.25 のルータへの telnet のデータをトランスポートモードで通信。

```
# ipsec sa policy 102 192.168.112.25 esp des-cbc sha-hmac
# ipsec transport 1 102 tcp * telnet
```

9. IPXの設定

9.1 LAN、PP共通の設定

9.1.1 IPXパケットを扱うか否かの設定

［入力形式］ **ipx routing** *routing*

no ipx routing [*routing*]

［パラメータ］ • *routing*

◦on ... IPX パケットを処理対象として扱う

◦off ... IPX パケットを処理対象として扱わない

［説明］ IPX パケットをルーティングするかどうかを設定する。このスイッチを on にしないと IPX 関連は一切動作しない。

［デフォルト値］ off

9.1.2 IPXパケットのフィルタの設定

［入力形式］ **ipx filter** *filter_number pass_reject src_net*[*src_node*[*dst_net*[*dst_node*[*type*[*src_socket* [*dst_socket*]]]]]]

no ipx filter *filter_number* [*pass_reject ...*]

［パラメータ］ • *filter_number ...* フィルタの番号(1..100)

• *pass_reject*

◦pass-log ... 一致すれば通す (ログに記録する)

◦pass-nolog ... 一致すれば通す (ログに記録しない)

◦reject-log ... 一致すれば破棄する (ログに記録する)

◦reject-nolog ... 一致すれば破棄する (ログに記録しない)

◦restrict-log ... 回線が接続されていれば通し、切断されていれば破棄する (ログに記録する)

◦restrict-nolog ... 回線が接続されていれば通し、切断されていれば破棄する (ログに記録しない)

• *src_net ...* 始点 IPX ネットワーク番号

◦0:0:0:1 ... FF:FF:FF:FE (2 桁以内の 16 進数以外に '*' も指定可)

◦ * (すべての IPX ネットワーク番号)

• *src_node ...* 始点 IPX ノード番号

◦ 0:0:0:0:0:1 ... FF:FF:FF:FF:FF:FE(2 桁以内の 16 進数以外に '*' も指定可)

◦ * (すべての IPX ノード番号)

◦省略した時は一個の * と同じ

• *dst_net ...* 終点 IPX ネットワーク番号 src_net と同じ形式。

• *dst_node ...* 終点 IPX ノード番号 src_node と同じ形式。

• *type* ...IPX パケットタイプ

◦ 10 進数(0..255)

◦ 16 進数(0x0..0xFF)

◦ ニーモニック文字列

unknown	0
rip	1
sap	4
spx	5
ncp	17
netbios	20

◦ 間に - をはさんだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。

◦ 上項目のカンマで区切った並び (5 個以内)

◦ * (すべての IPX パケットタイプ)

◦ 省略した時は一個の * と同じ

• *src_socket* ... 始点ソケット番号

◦ 10 進数(0..65535)

◦ 0x を先頭に持つ 4 桁以内の 16 進数

◦ プロトコルを表すニーモニック

ncp	0x0451
sap	0x0452
rip	0x0453
netbios	0x0455
diag	0x0456
serialization	0x0457

◦ 間に - をはさんだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。

◦ 上項目のカンマで区切った並び (5 個以内)

◦ * (すべてのソケット番号)

◦ 省略した時は一個の * と同じ

• *dst_socket* ... 終点ソケット番号 *src_socket* と同じ形式。

［説明］ IPX パケットに対するフィルタを設定する。
このコマンドで設定されたフィルタは、**ipx lan secure filter** コマンド、**ipx pp secure filter** コマンドで用いられる。

［ノート］ IPX パケットタイプでは、"-xxx" は "0-xxx" の意味に、また "yyy-" は "yyy-255" の意味に取る。
ソケット番号では、"yyy-" は "yyy-65535" の意味に取る。
restrict-log 及び restrict-nolog を使ったフィルタは、回線が接続されている時だけ通せば十分で、そのために回線に発信するまでもないようなパケットに対して有効である。

9.1.3 静的な SAPテーブルの設定

［入力形式］ **ipx sap** *service_type server_name network node_number socket hop*

no ipx sap *service_type server_name* [*network node_number socket hop*]

［パラメータ］
- *service_type* ... サービスタイプ
  - 10 進数(0..65535)
  - 0x に続く 4 桁以内の 16 進数
  - file ...0x0004 のニーモニック
  - printer ...0x0007 のニーモニック
- *server_name* ... サーバ名
  - 'A' 〜 'Z','0' 〜 '9',' ','-','@' で構成された 47 文字以内の文字列
- *network* ... サーバの IPX ネットワーク番号(0:0:0:1 .. FF:FF:FF:FE)
- *node_number* ... サーバの IPX ノード番号(0:0:0:0:0:1 .. FF:FF:FF:FF:FF:FE)
- *socket* ... ソケット番号
  - 10 進数(0..65535)
  - 0x に続く 4 桁以内の 16 進数
  - プロトコルを表すニーモニック

ncp	0x0451
sap	0x0452
rip	0x0453
netbios	0x0455
diag	0x0456
serialization	0x0457

- *hop* ... ホップカウント(1..14)

［説明］ SAP テーブルを設定する。

9.1.4 IPX SAP Get Nearest Server Requestに応答するか否かの設定

［入力形式］ **ipx sap response** *response*

no ipx sap response [*response*]

［パラメータ］
- *response*
  - on ... 応答する
  - off ... 応答しない

［説明］ IPX SAP Get Nearest Server Request に応答するか否かを設定する。

［デフォルト値］ on

9.2 LAN側の設定

9.2.1 イーサネットフレームタイプの設定

［入力形式］ **ipx *interface* frame type** *type*

no ipx *interface* frame type [*type*]

［パラメータ］ • ***interface*** ... LANインタフェース名

• *type*

◦ 0 ... IEEE 802.3 Raw

◦ 1 ... Ethernet II, イーサネットタイプは0x8137

◦ 2 ... IEEE 802.3 + IEEE 802.2, SAPは0xE0

◦ 3 ... IEEE 802.3 + IEEE 802.2 SNAP, プロトコルIDは0x0000008137

［説明］ IPXが用いるイーサネットでのフレームタイプを設定する。
同じイーサネット上にあるNetwareサーバやNetwareワークステーションの設定と一致させる必要がある。

type	NetWareでの表現
0	ETHERNET 802.3
1	ETHERNET II
2	ETHERNET 802.2
3	ETHERNET SNAP

［デフォルト値］ 0

9.2.2 LAN側のIPXネットワーク番号の設定

［入力形式］ **ipx *interface* network** *network*

no ipx *interface* network [*network*]

［パラメータ］ • ***interface*** ... LANインタフェース名

• *network*

◦ IPXネットワーク番号 (0:0:0:1 .. FF:FF:FF:FE)

［説明］ LANインタフェースに割り当てるIPXネットワーク番号を設定する。

［デフォルト値］ IPXネットワーク番号は設定されていない。

9.2.3 経路情報の追加

［入力形式］ **ipx *interface* route** *network gateway hop* [*ticks*]

no ipx *interface* route *network* [*gateway hop* [*ticks*]]

［パラメータ］ • ***interface*** ... LAN インタフェース名

• *network* ... 終点 IPX ネットワーク番号 (0:0:0:1 ..FF:FF:FF:FE)

• *gateway* ... ゲートウェイの IPX ノード番号 (0:0:0:0:0:1 .. FF:FF:FF:FF:FF:FE)

• *hop* ... ホップカウント(1..14)

• *ticks* ... ティック(1..65535)

［説明］ IPX の経路情報テーブルに LAN 側の経路情報を追加する。

［ノート］ ティックを省略した時はホップカウントと同じになる。

9.2.4 LAN 側の RIP/SAP ブロードキャストの設定

［入力形式］ **ipx *interface* ripsap broadcast** *broadcast*

no ipx *interface* ripsap broadcast [*broadcast*]

［パラメータ］ • ***interface*** ... LAN インタフェース名

• *broadcast*

◦ 秒数(60..21474836)

◦ off ... RIP/SAP をブロードキャストしない

［説明］ LAN に対して RIP/SAP をブロードキャストする間隔を設定する。off を設定すると、ブロードキャストしなくなる。

［ノート］ この設定にかかわらず、RIP/SAP Request に対しては常に Response を返す。

［デフォルト値］ 60

9.2.5 LAN 側でのフィルタリングによるセキュリティの設定

［入力形式］ **ipx *interface* secure filter** *direction filter_list*

no ipx *interface* secure filter *direction* [*filter_list*]

［パラメータ］ • ***interface*** ... LAN インタフェース名

• *direction*

◦ in ... LAN 側から入ってくる方向でフィルタを適用

◦ out ... LAN 側へ出ていく方向でフィルタを適用

• *filter_list* ... 100 個以内の空白で区切られたフィルタ番号の並び

［説明］ LAN 側に対して適用する IPX フィルタを設定する。

［ノート］ フィルタリストを走査して、一致すると通過、破棄が決定する。

ipx filter 1 pass 0:0:1:*

ipx filter 2 reject 0:0:1:1

ipx lan secure filter in 1 2

では、最初のフィルタリスト 1 で通過が決定した後でフィルタリスト 2 の破棄を判断することになるのでフィルタリスト 2 は無効である。
どのフィルタにも一致しない時は破棄になる。

9.3 PP側相手毎のIPXの設定

9.3.1 IPXルーティング許可の設定

［入力形式］ **ipx pp routing** *routing*

no ipx pp routing [*routing*]

［パラメータ］ • *routing*

◦ on ... PP 側に IPX パケットをルーティングする

◦ off ... PP 側に IPX パケットをルーティングしない

［説明］ 選択されている相手について IPX パケットを PP 側にルーティングするかどうかを設定する。

［デフォルト値］ off

9.3.2 PP側IPXネットワーク番号の設定

［入力形式］ **ipx pp network** *network* [*node_number*]

no ipx pp network [*network* [*node_number*]]

［パラメータ］ • *network* ... IPX ネットワーク番号

◦ 0:0:0:1 ... FF:FF:FF:FE

• *node_number* ... IPX ノード番号 (0:0:0:0:0:1 ..FF:FF:FF:FF:FF:FE)

［説明］ PP インタフェースに割り当てる IPX ネットワーク番号を設定する。

［ノート］ IPX ノード番号は通常デフォルトのままとする。

［デフォルト値］ IPX ネットワーク番号は設定されていない。

IPX ノード番号は MAC アドレス

9.3.3 経路情報の追加

［入力形式］ **ipx pp route** *network* [*name*] *hops* [*ticks*]

ipx pp route *network* [dlci=*dlci_num*] *hops* [*ticks*]

no ipx pp route *network* [...]

［パラメータ］ • *network* ... 終点 IPX ネットワーク番号(0:0:0:1 .. FF:FF:FF:FE)

• *name* ... 名前 (16 文字以内)

• *hop* ... ホップカウント (1..14)

• *ticks* ... ティック (1..65535)

• *dlci_num* ... ゲートウェイの DLCI

［説明］ 選択されている相手について経路情報テーブルに PP 側の IPX の経路情報を追加する。フレームリレーの場合は、ゲートウェイを指定するために DLCI を書くことができる。

［ノート］ 通常 PP 側に関してのみ設定する。ティックを省略した時はホップカウントの 55 倍になる。*name* パラメータは、anonymous が選択された時のみ有効である。

9.3.4 回線接続時の PP側の RIP/SAPの動作の設定

［入力形式］ **ipx pp ripsap connect send** *send*

no ipx pp ripsap connect send [*send*]

［パラメータ］ • *send*

◦ none ... 回線接続時に RIP/SAP を送出しない

◦ interval ... **ipx pp ripsap connect interval** コマンドで設定された時間間隔で RIP/SAP を送出する

◦ update ... RIP/SAP テーブルに変更があった時だけ送出する

［説明］ 選択されている相手について回線接続時に RIP/SAP を送出する条件を選択する。

［ノート］ この設定にかかわらず、RIP/SAP Request に対しては Response を返す。

［デフォルト値］ update

9.3.5 回線接続時の PP側の RIP/SAP送出の時間間隔の設定

［入力形式］ **ipx pp ripsap connect interval** *time*

no ipx pp ripsap connect interval [*time*]

［パラメータ］ • *time* ... 秒数(60..21474836)

［説明］ 選択されている相手について回線接続時に PP 側に RIP/SAP を送出する時間間隔を設定する。

［デフォルト値］ 60

9.3.6 回線切断時の PP側の RIP/SAPの動作の設定

［入力形式］ **ipx pp ripsap disconnect send** *send*

no ipx pp ripsap disconnect send [*send*]

［パラメータ］ • *send*

◦ none ... 回線切断時に RIP/SAP を送出しない

◦ interval ... **ipx pp ripsap disconnect interval** コマンドで設定された時間間隔で RIP/SAP を送出する

◦ update ... RIP/SAP テーブルに変更があった時だけ送出する

［説明］ 選択されている相手について回線切断時に RIP/SAP を送出する条件を選択する。

［デフォルト値］ none

9.3.7 回線切断時の PP側の RIP/SAP送出の時間間隔の設定

［入力形式］ **ipx pp ripsap disconnect interval** *interval*

no ipx pp ripsap disconnect interval [*interval*]

［パラメータ］ • *interval* ... 秒数(60..21474836)

［説明］ 選択されている相手について回線切断時に RIP/SAP を送出する時間間隔を設定する。

［デフォルト値］ 60

9.3.8 回線切断時に RIP/SAP情報を保持するか否かの設定

［入力形式］ **ipx pp ripsap hold** *hold*

no ipx pp ripsap hold [*hold*]

［パラメータ］ • hold

◦ on ... 保持する

◦ off ... 保持しない

［説明］ 選択されている相手について回線接続中に取得した動的 RIP/SAP 情報を回線切断後も保持するか否かを設定する。

［デフォルト値］ on

9.3.9 IPXWAN使用の設定

［入力形式］ **ipx pp ipxwan use** *use*

no ipx pp ipxwan use [*use*]

［パラメータ］ • *use*

◦ on ... 接続時に IPXWAN を用いてパラメータのネゴシエーションを行う

◦ off ... パラメータのネゴシエーションは IPXCP で行い、IPXWAN は用いない

［説明］ 回線接続時のパラメータネゴシエーションの手順として IPXWAN を用いるかどうかを設定する。

［デフォルト値］ on

9.3.10 Timer/Information Request の再送間隔と最大再送回数の設定

［入力形式］ **ipx pp ipxwan retry** *interval max*

no ipx pp ipxwan retry [*interval max*]

［パラメータ］ • *interval* ... 秒数(10..21474836)

• *max* ... 最大再送回数(0..10)

［説明］ IPXWAN の Timer/Information Request の再送間隔と最大再送回数を設定する。

［デフォルト値］ *interval* = 20

max = 3

9.3.11 IPXWANプライマリネットワーク番号の設定

［入力形式］ **ipx pp ipxwan primnet** *network*

no ipx pp ipxwan primnet [*network*]

［パラメータ］ • *network* ... IPXWAN プライマリネットワーク番号(0:0:0:1 .. FF:FF:FF:FE)

［説明］ IPXWAN で用いるプライマリネットワーク番号を設定する。

［デフォルト値］ PP 側インタフェースの MAC アドレスの下位 32 ビット

9.3.12 Watchdog パケットに対する代理応答の設定

［入力形式］ **ipx pp watchdog proxy** *proxy*

no ipx pp watchdog proxy [*proxy*]

［パラメータ］ • *proxy*

◦ on ... 代理応答する

◦ off ... 代理応答しない

［説明］ 回線切断時に、PP の向こう側のワークステーションに対してサーバから出された NCP Watchdog Request パケットに対して代理応答するか否かを設定する。

［デフォルト値］ on

9.3.13 Watchdog 代理応答の時間間隔の設定

［入力形式］ **ipx pp watchdog interval** *interval*

no ipx pp watchdog interval [*interval*]

［パラメータ］ • *interval* ... 秒数(1..21474836)

［説明］ PP の向こう側のワークステーションが動作しているかどうかを確認する時間間隔を設定する。

［デフォルト値］ 3600

9.3.14 SPXキープアライブ代理応答を行うか否かの設定

［入力形式］ **ipx pp spx keepalive proxy** *proxy*

no ipx pp spx keepalive proxy [*proxy*]

［パラメータ］ • *proxy*

◦ on ... 代理応答を行う

◦ off ... 代理応答を行わない

［説明］ SPX キープアライブ代理応答を行うか否かを設定する。

［デフォルト値］ on

9.3.16 SPXキープアライブ代理応答のタイマの設定

［入力形式］ **ipx pp spx keepalive timer** *t1* [*t2* [*t3*]]

no ipx pp spx keepalive timer [*t1* [*t2* [*t3*]]]

［パラメータ］ • *t1* ... 秒数(30..21474836)

• *t2* ... 秒数(30..65535)

• *t3* ... 秒数(1..65535)

［説明］ SPX キープアライブ代理応答のためのタイマ値を設定する。それぞれのタイマ値の意味は次の通り。
t1 ... 代理応答を行っていてもこの時間毎に相手に接続し、正常に動作しているかどうか確認する。
t2 ... この時間以内に、ローカルに接続しているサーバ / クライアントから SPX パケットを受信できなかったら正常でないものと判断する。
t3 ... この時間間隔でローカルに接続しているサーバ / クライアントに対してリモートにある筈のマシンの代理で本機が SPX キープアライブパケットを送信する。

［デフォルト値］ *t1* = 7200

t2 = 60

t3 = 10

9.3.17 IPXシリアライゼーションパケットをフィルタアウトするか否かの設定

［入力形式］ **ipx pp serialization filter** *filter*

no ipx pp serialization filter [*filter*]

［パラメータ］ • *filter*

◦ on ... フィルタアウトする

◦ off ... フィルタアウトしない

［説明］ 選択されている相手について IPX シリアライゼーションパケットをフィルタアウトするか否かを設定する。

［デフォルト値］ on

9.3.18 PP側でのフィルタリングによるセキュリティの設定

［入力形式］ **ipx pp secure filter** *direction filter_list*

no ipx pp secure filter *direction* [*filter_list*]

［パラメータ］ • *direction*

◦ in ... PP 側から入って来る方向でフィルタを適用

◦ out ... PP 側へ出て行く方向でフィルタを適用

• *filter_list* ... 30 個以内の空白で区切られたフィルタ番号の並び

［説明］ PP 側に対し適用するフィルタを設定する。

［ノート］ フィルタリストを走査して、一致すると通過、破棄が決定する。

ipx filter 1 pass 0:0:1:*

ipx filter 2 reject 0:0:1:1

ipx pp secure filter in 1 2

では、最初のフィルタリスト 1 で通過が決定した後でフィルタリスト 2 の破棄を判断することになるのでフィルタリスト 2 は無効である。
どのフィルタにも一致しない時は破棄になる。

10. ブリッジの設定

10.1 LAN、PP共通の設定

10.1.1 ブリッジ使用許可の設定

［入力形式］ **bridge use** *use*

no bridge use [*use*]

［パラメータ］ • *use*

- on ... ブリッジする
- off ... ブリッジしない
- multicast ... マルチキャストのみブリッジする

［説明］ ブリッジを行うかどうかを設定する。

［ノート］ このスイッチが on でも、ip routing on であれば、IP パケットはブリッジング対象外となる。同様に ipx routing on であれば、IPX パケットはブリッジング対象外となる。

［デフォルト値］ off

10.1.2 ブリッジするインタフェースの設定

［入力形式］ **bridge group** *interface_list*

no bridge group [*interface_list*]

［パラメータ］ • *interface_list*

- 相手先情報番号
- anonymous
- leased (1BRI モデルのみ)
- LAN インタフェース名

［説明］ ブリッジをする相手先を設定する。
PP の相手先は、WAN 回線数の 2 倍まで設定できる。
LAN の相手先は、LAN インターフェース数まで設定できる。

［ノート］ anonymous を含める場合には、相手先情報番号を同時に指定することはできない。

［デフォルト値］ インタフェースは設定されていない。

［設定例］ LAN1 ポートと LAN2 ポート間でブリッジする。

```
# bridge group lan1 lan2
```

LAN2 ポートと相手先情報番号 3 の間でブリッジする。

```
# bridge group lan2 3
```

10.1.3 ブリッジのフィルタの設定

［入力形式］ **bridge filter** *filter_number pass_reject src_mac*[*dst_mac*[*offset byte_list*]]

no bridge filter *filter_number* [*pass_reject src_mac*[*dst_mac*[*offset byte_list*]]]

［パラメータ］
- *filter_number* ... フィルタの番号(1..100)
- *pass_reject*
  - pass-log ... 一致すれば通す (ログに記録する)
  - pass-nolog ... 一致すれば通す (ログに記録しない)
  - reject-log ... 一致すれば破棄する (ログに記録する)
  - reject-nolog ... 一致すれば破棄する (ログに記録しない)
  - restrict-log ... 回線が接続されていれば通し、切断されていれば破棄する (ログに記録する)
  - restrict-nolog ... 回線が接続されていれば通し、切断されていれば破棄する (ログに記録しない)
- *src_mac* ... 始点 MAC アドレス
  - XX:XX:XX:XX:XX:XX、XX は 16 進数、または *
  - * (すべての MAC アドレスに対応)
- *dst_mac* ... 終点 MAC アドス *src_mac* と同じ形式。省略した時は一個の * と同じ
- *offset* ... オフセットを表す 10 進数 (イーサネットフレームの始点 MAC アドレスの直後を 0 とするバイト数)
- byte list
  - バイト列
    - ▷ XX(XX は 2 桁の 16 進数)
    - ▷ 上項目のカンマで区切った並び(16 個以内)
  - * (すべてのバイト表現)

［説明］ ブリッジのフィルタを設定する。このコマンドで設定されたフィルタは **bridge lan filter** コマンド、**bridge pp filter** コマンドで用いられる。

［ノート］ restrict-log 及び restrict-nolog を使ったフィルタは、回線が接続されている時だけ通せば十分で、そのために回線に発信するまでもないようなパケットに対して有効である。

10.1.4 MAC アドレスのラーニングを行うか否かの設定

［入力形式］ **bridge learning** *learning*

no bridge learning [*learning*]

［パラメータ］
- *learning*
  - on ... 行う
  - off ... 行わない

［説明］ ラーニングとは、インタフェースから受け取った始点 MAC アドレスを覚えておき、別のインタフェースから受け取ったパケットをブリッジする時に終点 MAC アドレスが覚えていた MAC アドレスに一致したならばそのインタフェースにのみパケットを送り出すことを言う。このコマンドではインタフェースから受け取った始点 MAC アドレスを覚えておくかどうかを設定する。

［デフォルト値］ on

10.1.5 ラーニング情報消去タイマの設定

［入力形式］ **bridge learning expire** *time*

no bridge learning expire [*time*]

［パラメータ］ • *time*

◦秒数(1..21474836)

◦off ... タイマを設定しない

［説明］ このコマンドで設定した時間中に、ある始点 MAC アドレスのパケットを受け取らなかった時には、その MAC アドレスに関するラーニング情報を消去する。
off を指定するとラーニング情報は自動的には消去されなくなる。

［デフォルト値］ off

10.2 LAN 側の設定

10.2.1 ラーニング情報の設定

［入力形式］ **bridge *interface* learning** *mac_address*

no bridge *interface* learning *mac_address*

［パラメータ］ • ***interface*** ... LAN インタフェース名

• *mac_address* ... XX:XX:XX:XX:XX:XX (XX は 16 進数)

［説明］ LAN 側インタフェースに対して MAC アドレスのラーニング情報を設定する。

［ノート］ ラーニング情報は全体で 30 個まで設定できる。

10.2.2 LAN 側でのブリッジのフィルタリングの設定

［入力形式］ **bridge *interface* filter** *direction filter_list*

no bridge *interface* filter *direction* [*filter_list*]

［パラメータ］ • ***interface*** ... LAN インタフェース名

• *direction*

◦in ... LAN 側から入ってくるパケットのフィルタリング

◦out ... LAN 側に出ていくパケットのフィルタリング

• *filter_list*

◦空白で区切られた filter_number の並び (100 個以内)

［説明］ LAN 側を通るパケットについて **bridge filter** コマンドによるパケットのフィルタを組み合わせて、ブリッジするパケットの種類の制限を設定する。

［デフォルト値］ フィルタは設定されていない。

10.3 PP側相手毎のブリッジの設定

10.3.1 ラーニング情報の設定

［入力形式］ **bridge pp learning** *mac_address* [dlci=*dlci_num*]

no bridge pp learning *mac_address* [dlci=*dlci_num*]

［パラメータ］ • *mac_address* ... XX:XX:XX:XX:XX:XX (XX は 16 進数)

• *dlci_num* ...DLCI 番号

［説明］ PP 側インタフェースに対して MAC アドレスのラーニング情報を設定する。フレームリレーの場合は、DLCI 番号を指定することが可能である。

［ノート］ ラーニング情報は全体で 30 個まで設定できる。

10.3.2 PP側でのブリッジのフィルタリングの設定

［入力形式］ **bridge pp filter** *direction filter_list*

no bridge pp filter *direction* [*filter_list*]

［パラメータ］ • *direction*

◦ in ... PP 側から入ってくるパケットのフィルタリング

◦ out ... PP 側に出ていくパケットのフィルタリング

• *filter_list*

◦ 空白で区切られた filter_number の並び (100 個以内)

［説明］ PP 側を通るパケットについて **bridge filter** コマンドによるパケットのフィルタを組み合わせて、ブリッジするパケットの種類の制限を設定する。

［デフォルト値］ フィルタは設定されていない。

11. PPPの設定

11.1 要求する認証タイプの設定

［入力形式］ **pp auth request** *auth* [arrive-only]

no pp auth request [*auth* [arrive-only]]

［パラメータ］ • *auth*

◦ none ... 何も要求しない

◦ pap ... PAP による認証を要求する

◦ chap ... CHAP による認証を要求する

◦ chap-pap ... CHAP もしくは PAP による認証を要求する

［説明］ PAP と CHAP による認証を要求するかどうかを設定する。発信時には常に適用される。anonymous でない着信の場合には発番号により PP が選択されてから適用される。anonymous での着信時には、発番号による PP の選択が失敗した時に適用される。

キーワード chap-pap の場合には、最初 CHAP を要求し、それが相手から拒否された場合には改めて PAP を要求するよう動作する。これにより、相手が PAP または CHAP の片方しかサポートしていない場合でも容易に接続できるようになる。

キーワード arrive-only が指定された時には、着信時にのみ PPP による認証を要求するようになり、発信時には要求しない。

PP 毎のコマンドである。

［デフォルト値］ none

11.2 相手の名前とパスワードの設定

［入力形式］ **pp auth username** *username password* [*isdn1*] [clid [*isdn2*]] [mscbcp] [*ip_address*]

no pp auth username *username* [*password* ...]

［パラメータ］ • *username* ... 名前(32 文字以内)

• *password* ... パスワード(32 文字以内)

• *isdn1* ... 相手の ISDN アドレス

• clid ... 発番号認証を利用することを示すキーワード

• *isdn2* ... 発番号認証に用いられる ISDN アドレス

• mscbcp ... MS コールバックを許可することを示すキーワード

• *ip_address* ... 相手の IP アドレス(**ip pp remote address** に対応)

［説明］ 相手の名前とパスワードを設定する。複数設定できる。

オプションで ISDN 番号が設定でき、名前と結びついたルーティングやリモート IP アドレスに対しての発信を可能にする。*isdn1* は発信用の ISDN アドレスである。*isdn1* を省略すると、この相手には発信しなくなる。

名前に '*' を与えた時にはワイルドカードとして扱い、他の名前とマッチしなかった相手に対してその設定を使用する。

キーワード clid は発番号認証を利用することを指示する。このキーワードがない場合は発番号認証は行われない。発番号認証は *isdn2* があれば *isdn2* を用い、または *isdn2* がなければ *isdn1* を用い、一致したら認証は成功したとみなす。

キーワード mscbcp は MS コールバックを許可することを指示する。このユーザからの着信に対しては、同時に isdn callback permit on としてあれば MS コールバックの動作を行う。

11.3 受け入れる認証タイプの設定

［入力形式］ **pp auth accept** *accept*

no pp auth accept [*accept*]

［パラメータ］ • *accept*

- pap ... PAP による認証を受け入れる
- chap ... CHAP による認証を受け入れる
- pap chap ... PAP と CHAP のいずれによる認証も受け入れる
- chap pap ... PAP と CHAP のいずれによる認証も受け入れる

［説明］ 相手からの PPP 認証要求を受け入れるかどうか設定する。発信時には常に適用される。anonymous でない着信の場合には発番号により PP が選択されてから適用される。anonymous での着信時には、発番号による PP の選択が失敗した時に適用される。

このコマンドで認証を受け入れる設定になっていても、**pp auth myname** コマンドで自分の名前とパスワードが設定されていなければ、認証を拒否する。

PP 毎のコマンドである。

［デフォルト値］ 認証を受け入れない

11.4 自分の名前とパスワードの設定

［入力形式］ **pp auth myname** *myname password*

no pp auth myname [*myname password*]

［パラメータ］ • *myname* ... 名前(32 文字以内)

• *password* ... パスワード(32 文字以内)

［説明］ PAP または CHAP で相手に送信する自分の名前とパスワードを設定する。

PP 毎のコマンドである。

11.5 同一 username を持つ相手からの二重接続を禁止するか否かの設定

［入力形式］ **pp auth multi connect prohibit** *prohibit*

no pp auth multi connect prohibit [*prohibit*]

［パラメータ］ • *prohibit*

- on ... 禁止する
- off ... 禁止しない

［説明］ **pp auth username** で登録した同一 username を持つ相手からの二重接続を禁止するか否かを設定する。

［ノート］ 定額制プロバイダを営む時に便利である。ユーザ管理を RADIUS で行う場合には、二重接続の禁止は RADIUS サーバの方で対処する必要がある。

anonymous が選択された時のみ有効である。

［デフォルト値］ off

11.6 LCP関連の設定

11.6.1 Address and Control Field Compressionオプション使用の設定

［入力形式］ **ppp lcp acfc** *acfc*

no ppp lcp acfc [*acfc*]

［パラメータ］ • *acfc*

◦ on ... 用いる

◦ off ... 用いない

［説明］ 選択されている相手について[PPP, LCP]の Address and Control Field Com pression オプションを用いるか否かを設定する。

［ノート］ on を設定していても相手に拒否された時は用いない。また、このオプションを相手から要求された時には、このコマンドの設定に関わらず常にアクセプトする。

［デフォルト値］ off

11.6.2 Magic Numberオプション使用の設定

［入力形式］ **ppp lcp magicnumber** *magicnumber*

no ppp lcp magicnumber [*magicnumber*]

［パラメータ］ • *magicnumber*

◦ on ... 用いる

◦ off ... 用いない

［説明］ 選択されている相手について[PPP,LCP]の Magic Number オプションを用いるか否かを設定する。

［ノート］ on を設定していても相手に拒否された時は用いない。

［デフォルト値］ on

11.6.3 Maximum Receive Uniオプション使用の設定

［入力形式］ **ppp lcp mru** *mru* [*length*]

no ppp lcp mru [*mru* [*length*]]

［パラメータ］ • *mru*

◦ on ... 用いる

◦ off ... 用いない

• *length*

◦ 1500 ... 1500bytes

◦ 1792 ... 1792bytes

［説明］ 選択されている相手について[PPP,LCP]の Maximum Receive Unit オプションを用いるか否かと、MRU の値を設定する。

［ノート］ on を設定していても相手に拒否された時は用いない。一般には on でよいが、このオプションをつけると接続できないルータに接続する時には off にする。

データ圧縮を利用する設定の時には、length パラメータの設定は常に 1792 として動作する。

［デフォルト値］ *mru* = on

length = 1792

11.6.4 Protocol Field Compressionオプション使用の設定

［入力形式］ **ppp lcp pfc** *pfc*

no ppp lcp pfc [*pfc*]

［パラメータ］ • *pfc*

◦ on ... 用いる

◦ off ... 用いない

［説明］ 選択されている相手について[PPP,LCP]の Protocol Field Compression オプションを用いるか否かを設定する。

［ノート］ on を設定していても相手に拒否された時は用いない。また、このオプションを相手から要求された時には、このコマンドの設定に関わらず常にアクセプトする。

［デフォルト値］ off

11.6.5 パラメータ lcp-restart の設定

［入力形式］ **ppp lcp restart** *time*

no ppp lcp restart [*time*]

［パラメータ］ • *time* ... ミリ秒 (20..10000)

［説明］ 選択されている相手について[PPP,LCP]の configure-request、terminate-request の再送時間を設定する。

［デフォルト値］ 3000

11.6.6 パラメータ lcp-max-terminate の設定

［入力形式］ **ppp lcp maxterminate** *count*

no ppp lcp maxterminate [*count*]

［パラメータ］ • *count* ... 回数(1..10)

［説明］ 選択されている相手について[PPP,LCP]の terminate-request の送信回数を設定する。

［デフォルト値］ 2

11.6.7 パラメータ lcp-max-configure の設定

［入力形式］ **ppp lcp maxconfigure** *count*

no ppp lcp maxconfigure [*count*]

［パラメータ］ • *count* ... 回数(1..10)

［説明］ 選択されている相手について[PPP,LCP]の configure-request の送信回数を設定する。

［デフォルト値］ 10

11.6.8 パラメータ lcp-max-failure の設定

［入力形式］ **ppp lcp maxfailure** *count*

no ppp lcp maxfailure [*count*]

［パラメータ］ • *count* ... 回数(1..10)

［説明］ 選択されている相手について[PPP,LCP]の configure-nak の送信回数を設定する。

［デフォルト値］ 10

11.6.9 専用線キープアライブを使用するか否かの設定

［入力形式］ **leased keepalive use** *use*

no leased keepalive use [*use*]

［パラメータ］ • *use*

◦ on ... 使用する

◦ off ... 使用しない

［説明］ 専用線使用時にキープアライブを使用するか否かを設定する。

［ノート］ 複数 WAN ポートモデルでは PP 毎のコマンドである。

［デフォルト値］ off

11.6.10 専用線キープアライブのログをとるか否かの設定

［入力形式］ **leased keepalive log** *log*

no leased keepalive log [*log*]

［パラメータ］ • l*og*

◦ on ... ログをとる

◦ off ... ログをとらない

［説明］ キープアライブ(LCP ECHO)をログにとるか否かを設定する。

［ノート］ 複数 WAN ポートモデルでは PP 毎のコマンドである。

［デフォルト値］ on

11.6.11 専用線キープアライブの時間間隔の設定

［入力形式］ **leased keepalive interval** *interval* [*count*]

no leased keepalive interval [*interval* [*count*]]

［パラメータ］ • *interval* ... キープアライブパケットを送出する時間間隔(1..65535 秒)

• *count* ... この回数連続して応答がなければ相手側のルータをダウンしたと判定する (3..100)

［説明］ LCP ECHO によるキープアライブパケットを送出する時間間隔とダウン検出を判定する回数を設定する。

［ノート］ 複数 WAN ポートモデルでは PP 毎のコマンドである。

一度 LCP ECHO Request に対するリプライが返ってこないのを検出したら、その後の監視タイマは 1 秒に短縮される。

［デフォルト値］ *interval* = 30

count = 6

11.6.12 専用線ダウン検出時の動作の設定

［入力形式］ **leased keepalive down** *action*

no leased keepalive down [*action*]

［パラメータ］ • *action*

◦ silent ... 何もしない

◦ reset ... ルータを再起動する

［説明］ キープアライブによって専用線ダウンを検出した時のルータの動作を設定する。

［デフォルト値］ silent

11.7 PAP関連の設定

11.7.1 パラメータ pap-restart の設定

［入力形式］ **ppp pap restart** *time*

no ppp pap restart [*time*]

［パラメータ］ • *time* ... ミリ秒(20..10000)

［説明］ 選択されている相手について[PPP,PAP] authenticate-request の再送時間を設定する。

［デフォルト値］ 3000

11.7.2 パラメータ pap-max-authreq の設定

［入力形式］ **ppp pap maxauthreq** *count*

no ppp pap maxauthreq [*count*]

［パラメータ］ • *count* ... 回数(1..10)

［説明］ 選択されている相手について[PPP,PAP] authenticate-request の送信回数を設定する。

［デフォルト値］ 10

11.8 CHAP関連の設定

11.8.1 パラメータ chap-restart の設定

［入力形式］ **ppp chap restart** *time*

no ppp chap restart [*time*]

［パラメータ］ • *time* ... ミリ秒(20..10000)

［説明］ 選択されている相手について[PPP,CHAP] challenge の再送時間を設定する。

［デフォルト値］ 3000

11.8.2 パラメータ chap-max-challengeの設定

［入力形式］ **ppp chap maxchallenge** *count*

no ppp chap maxchallenge [*count*]

［パラメータ］ • *count* ... 回数(1..10)

［説明］ 選択されている相手について[PPP,CHAP] challenge の送信回数を設定する。

［デフォルト値］ 10

11.9 IPCP関連の設定

11.9.1 Van Jacobson Compressed TCP/IP使用の設定

［入力形式］ **ppp ipcp vjc** *compression*

no ppp ipcp vjc [*compression*]

［パラメータ］ • *compression*

◦ on ... 使用する

◦ off ... 使用しない

［説明］ 選択されている相手について[PPP,IPCP] Van Jacobson Compressed TCP/IP を使用するか否かを設定する。

［ノート］ on を設定していても相手に拒否された時は用いない。

［デフォルト値］ off

11.9.2 PP側 IP アドレスのネゴシエーションの設定

［入力形式］ **ppp ipcp ipaddress** *negotiation*

no ppp ipcp ipaddress [*negotiation*]

［パラメータ］ • *negotiation*

◦ on ... ネゴシエーションする

◦ off ... ネゴシエーションしない

［説明］ 選択されている相手について PP 側 IP アドレスのネゴシエーションをするか否かを設定する。

［デフォルト値］ off

11.9.3 パラメータ ipcp-restart の設定

［入力形式］ **ppp ipcp restart** *time*

no ppp ipcp restart [*time*]

［パラメータ］ • *time* ... ミリ秒(20..10000)

［説明］ 選択されている相手について[PPP,IPCP]の configure-request、terminate-request の再送時間を設定する。

［デフォルト値］ 3000

11.9.4 パラメータ ipcp-max-terminate の設定

［入力形式］ **ppp ipcp maxterminate** *count*

no ppp ipcp maxterminate [*count*]

［パラメータ］ • *count* ... 回数(1..10)

［説明］ 選択されている相手について[PPP,IPCP]の terminate-request の送信回数を設定する。

［デフォルト値］ 2

11.9.5 パラメータ ipcp-max-configure の設定

［入力形式］ **ppp ipcp maxconfigure** *count*

no ppp ipcp maxconfigure [*count*]

［パラメータ］ • *count* ... 回数(1..10)

［説明］ 選択されている相手について[PPP,IPCP]の configure-request の送信回数を設定する。

［デフォルト値］ 10

11.9.6 パラメータ ipcp-max-failure の設定

［入力形式］ **ppp ipcp maxfailure** *count*

no ppp ipcp maxfailure [*count*]

［パラメータ］ • *count* ... 回数(1..10)

［説明］ 選択されている相手について[PPP,IPCP]の configure-nak の送信回数を設定する。

［デフォルト値］ 10

11.9.7 IPCPの MS拡張オプションを使うか否かの設定

［入力形式］ **ppp ipcp msext** *msext*

no ppp ipcp msext [*msext*]

［パラメータ］ • *msext*

◦ on ... 使用する

◦ off ... 使用しない

［説明］ 選択されている相手について､[PPP,IPCP]の MS 拡張オプションを使うか否かを設定する。

IPCP の Microsoft 拡張オプションを使うように設定すると、DNS サーバの IP アドレスと WINS (Windows Internet Name Service)サーバの IP アドレスを、接続した相手である Windows マシンに渡すことができる。渡すための DNS サーバや WINS サーバの IP アドレスはそれぞれ、**dns server** コマンドおよび **wins server** コマンドで設定する。

［デフォルト値］ off

11.9.8 WINSサーバの IPアドレスの設定

［入力形式］ **wins server** *server1* [*server2*]

no wins server [*server1* [*server2*]]

［パラメータ］ • *server*、 *server ... ip_address* (xxx.xxx.xxx.xxx (xxx は 10 進数))

［説明］ WINS (Windows Internet Name Service)サーバの IP アドレスを設定する。

［ノート］ IPCP の MS 拡張オプションおよび DHCP でクライアントに渡すための WINS サーバの IP アドレスを設定する。ルータはこのサーバに対し WINS クライアントとしての動作は一切行わない。

［デフォルト値］ WINS サーバは設定されていない。

11.10 IPXCP関連の設定

11.10.1 パラメータ ipxcp-restart の設定

［入力形式］ **ppp ipxcp restart** *time*

no ppp ipxcp restart [*time*]

［パラメータ］ • *time* ... ミリ秒(20..10000)

［説明］ 選択されている相手について[PPP、IPXCP]の configure-request、terminate-request の再送時間を設定する。

［デフォルト値］ 3000

11.10.2 パラメータ ipxcp-max-terminate の設定

［入力形式］ **ppp ipxcp maxterminate** *count*

no ppp ipxcp maxterminate [*count*]

［パラメータ］ • *count* ... 回数(1..10)

［説明］ 選択されている相手について[PPP、IPXCP]の terminate-request の送信回数を設定する。

［デフォルト値］ 2

11.10.3 パラメータ ipxcp-max-configureの設定

［入力形式］ **ppp ipxcp maxconfigure** *count*

no ppp ipxcp maxconfigure [*count*]

［パラメータ］ • *count* ... 回数(1..10)

［説明］ 選択されている相手について[PPP、IPXCP] の configure-request の送信回数を設定する。

［デフォルト値］ 10

11.10.4 パラメータ ipxcp-max-failureの設定

［入力形式］ **ppp ipxcp maxfailure** *count*

no ppp ipxcp maxfailure [*count*]

［パラメータ］ • *count* ... 回数(1..10)

［説明］ 選択されている相手について[PPP、IPXCP]の configure-nak の送信回数を設定する。

［デフォルト値］ 10

11.11 BCP関連の設定

11.11.1 LAN Identification 使用の設定

［入力形式］ **ppp bcp lanid** *lan_id*

no ppp bcp lanid [*lan_id*]

［パラメータ］ • *lan_id*

◦ 0x1 .. 0xFFFFFFfe

◦ off ... LAN-Identification を使用しない

［説明］ LAN-Identification の値を設定する。

［デフォルト値］ off

11.11.2 Tinygram compression使用の設定

［入力形式］ **ppp bcp tinycomp** *compression*

no ppp bcp tinycomp [*compression*]

［パラメータ］ • *compression*

◦ on ... 使用する

◦ off ... 使用しない

［説明］ Tinygram compression を使用するか否かを設定する。

［デフォルト値］ on

11.11.3 パラメータ bcp-restart の設定

［入力形式］ **ppp bcp restart** *time*

no ppp bcp restart [*time*]

［パラメータ］ • *time* ... ミリ秒(20..10000)

［説明］ 選択されている相手について[PPP, BCP]の configure-request、terminate-request の再送時間を設定する。

［デフォルト値］ 3000

11.11.4 パラメータ bcp-max-terminate の設定

［入力形式］ **ppp bcp maxterminate** *count*

no ppp bcp maxterminate [*count*]

［パラメータ］ • *count* ... 回数(1..10)

［説明］ 選択されている相手について[PPP, BCP]の terminate-request の送信回数を設定する。

［デフォルト値］ 2

11.11.5 パラメータ bcp-max-configure の設定

［入力形式］ **ppp bcp maxconfigure** *count*

no ppp bcp maxconfigure [*count*]

［パラメータ］ • *count* ... 回数(1..10)

［説明］ 選択されている相手について[PPP, BCP]の configure-request の送信回数を設定する。

［デフォルト値］ 10

11.11.6 パラメータ bcp-max-failure の設定

［入力形式］ **ppp bcp maxfailure** *count*

no ppp bcp maxfailure [*count*]

［パラメータ］ • *count* ... 回数(1..10)

［説明］ 選択されている相手について[PPP、BCP]の configure-nak の送信回数を設定する。

［デフォルト値］ 10

11.12 MSCBCP関連の設定

11.12.1 パラメータ mscbcp-restart の設定

［入力形式］ **ppp mscbcp restart** *time*

no ppp mscbcp restart [*time*]

［パラメータ］ • *time* ... ミリ秒(20..10000)

［説明］ 選択されている相手について[PPP, MSCBCP]の request/Response の再送時間を設定する。

［デフォルト値］ 1000

11.12.2 パラメータ mscbcp-maxretry の設定

［入力形式］ **ppp mscbcp maxretry** *count*

no ppp mscbcp maxretry [*count*]

［パラメータ］ • *count* ... 回数(1..30)

［説明］ 選択されている相手について[PPP, MSCBCP]の request/Response の再送回数を設定する。

［デフォルト値］ 30

11.13 CCP関連の設定

11.13.1 全パケットの圧縮タイプの設定

［入力形式］ **ppp ccp type** *type*

no ppp ccp type [*type*]

［パラメータ］ • *type*

- stac ... Stac LZS で圧縮する
- cstac ... Stac LZS で圧縮する
  （接続相手が Cisco ルータでかつ stac ではうまく動作しない場合）
- none ... 圧縮しない

［説明］ 選択されている相手について[PPP,CCP]圧縮方式を選択する。

［ノート］ Van Jacobson Compressed TCP/IP との併用も可能である。

接続相手が Cisco ルータの場合には stac の設定では、データ転送中に頻繁に CCP のリセットが発生して、データ転送速度が遅くなることがある。そのような場合には、設定を cstac に変更すると状況が改善することがある。

［デフォルト値］ stac

11.13.2 パラメータ ccp-restart の設定

［入力形式］ **ppp ccp restart** *time*

no ppp ccp restart [*time*]

［パラメータ］ • *time* ... ミリ秒(20..10000)

［説明］ 選択されている相手について[PPP, CCP]の configure-request、terminate-request の再送時間を設定する。

［デフォルト値］ 3000

11.13.3 パラメータ ccp-max-terminate の設定

［入力形式］ **ppp ccp maxterminate** *count*

no ppp ccp maxterminate [*count*]

［パラメータ］ • *count* ... 回数(1..10)

［説明］ 選択されている相手について[PPP, CCP]の terminate-request の送信回数を設定する。

［デフォルト値］ 2

11.13.4 パラメータ ccp-max-configure の設定

［入力形式］ **ppp ccp maxconfigure** *count*

no ppp ccp maxconfigure [*count*]

［パラメータ］ • *count* ... 回数(1..10)

［説明］ 選択されている相手について[PPP, CCP]の configure-request の送信回数を設定する。

［デフォルト値］ 10

11.13.5 パラメータ ccp-max-failure の設定

［入力形式］ **ppp ccp maxfailure** *count*

no ppp ccp maxfailure [*count*]

［パラメータ］ • *count* ... 回数(1..10)

［説明］ 選択されている相手について[PPP, CCP]の configure-nak の送信回数を設定する。

［デフォルト値］ 10

11.14 MP関連の設定

11.14.1 MPを使用するか否かの設定

［入力形式］ **ppp mp use** *use*

no ppp mp use [*use*]

［パラメータ］ • *use*

◦ on ... 使用する

◦ off ... 使用しない

［説明］ 選択されている相手について MP を使用するか否かを選択する。

［ノート］ on に設定していても、LCP の段階で相手とのネゴシエーションが成立しなければ MP を使わずに通信する。

［デフォルト値］ off

11.14.2 MPの制御方法の設定

［入力形式］ **ppp mp control** *type*

no ppp mp control [*type*]

［パラメータ］ • *type*

◦ arrive ... 自分が 1B 目の着信側の時に MP を制御する

◦ both ... 自分が 1B 目の発信着信いずれの場合でも MP を制御する

◦ call ... 自分が 1B 目の発信側の時に MP を制御する

［説明］ 選択されている相手について MP を制御して 2B 目の発信 / 切断を行う場合を設定する。通常は default のように自分が 1B 目の発信側の時だけ制御するようにしておく。

［デフォルト値］ call

11.14.3 MPのための負荷閾値の設定

［入力形式］ **ppp mp load threshold** *call_load call_count disc_load disc_count*

no ppp mp load threshold [*call_load call_count disc_load disc_count*]

［パラメータ］ • *call_load* ... 発信負荷閾値 %(1..100)

• *call_count* ... 回数(1..100)

• *disc_load* ... 切断負荷閾値 %(0..50)

• *disc_count* ... 回数(1..100)

［説明］ 選択されている相手について[PPP, MP]の 2B 目を発信したり切断したりする時のデータ転送負荷の閾値を設定する。

負荷は回線速度に対する % で評価し、送受信で大きい方の値を採用する。*call_load* を超える負荷が *call_count* 回繰り返されたら 2B 目の発信を行う。逆に *disc_load* を下回る負荷が *disc_count* 回繰り返されたら 2B 目を切断する。

［デフォルト値］ *call_load* = 70

call_count = 1

disc_load = 30

disc_count = 2

11.14.4 MPの最大リンク数の設定

［入力形式］ **ppp mp maxlink** *number*

no ppp mp maxlink [*number*]

［パラメータ］ • *number* ... リンク数

［説明］ 選択されている相手について[PPP, MP]の最大リンク数を設定する。リンク数の最大値は、使用モデルで使用できる ISDN Bch の数までとなる。

［デフォルト値］ 2

11.14.5 MPの最小リンク数の設定

［入力形式］ **ppp mp minlink** *number*

no ppp mp minlink [*number*]

［パラメータ］ • *number* ... リンク数

［説明］ 選択されている相手について[PPP,MP] の最小リンク数を設定する。

［デフォルト値］ 1

11.14.6 MPのための負荷計測間隔の設定

［入力形式］ **ppp mp timer** *time*

no ppp mp timer [*time*]

［パラメータ］ • *time* ... 秒数(1..21474836)

［説明］ 選択されている相手について[PPP, MP] のための負荷計測間隔を設定する。

単位は秒。負荷計測だけでなく、すべての MP の動作はこのコマンドで設定した間隔で行われる。

［デフォルト値］ 10

11.14.7 MPのパケットを分割するか否かの設定

［入力形式］ **ppp mp divide** *divide*

no ppp mp divide [*divide*]

［パラメータ］ • *divide*

◦ on ... 分割する

◦ off ... 分割しない

［説明］ 選択されている相手について[PPP, MP] に対して、MP パケットの送信時にパケットを分割するか否かを設定する。

［ノート］ 64 バイト以下のパケットはこのコマンドの設定に関わらず分割されない。

［デフォルト値］ on

11.15 BACP関連の設定

11.15.1 パラメータbacp-restart の設定

［入力形式］ **ppp bacp restart** *time*

no ppp bacp restart [*time*]

［パラメータ］ • *time* ... ミリ秒(20..10000)

［説明］ 選択されている相手について[PPP, BACP] の configure-request、terminate-request の再送時間を設定する。

［デフォルト値］ 3000

11.15.2 パラメータbacp-max-terminate の設定

［入力形式］ **ppp bacp maxterminate** *count*

no ppp bacp maxterminate [*count*]

［パラメータ］ • *count* ... 回数(1..10)

［説明］ 選択されている相手について[PPP, BACP] の terminate-request の送信回数を設定する。

［デフォルト値］ 2

11.15.3 パラメータ bacp-max-configure の設定

［入力形式］ **ppp bacp maxconfigure** *count*

no ppp bacp maxconfigure [*count*]

［パラメータ］ • *count* ... 回数(1..10)

［説明］ 選択されている相手について[PPP, BACP] の configure-request の送信回数を設定する。

［デフォルト値］ 10

11.15.4 パラメータ bacp-max-failure の設定

［入力形式］ **ppp bacp maxfailure** *count*

no ppp bacp maxfailure [*count*]

［パラメータ］ • *count* ... 回数(1..10)

［説明］ 選択されている相手について[PPP, BACP] の configure-nak を送る回数を設定する。

［デフォルト値］ 10

11.15.5 パラメータbap-restart の設定

［入力形式］ **ppp bap restart** *time*

no ppp bap restart [*time*]

［パラメータ］ • *time* ... ミリ秒(20..10000)

［説明］ 選択されている相手について[PPP, BAP] の configure-request、terminate-request の再送時間を設定する。

［デフォルト値］ 1000

11.15.6 パラメータbap-max-retry の設定

［入力形式］ **ppp bap maxretry** *count*

no ppp bap maxretry [*count*]

［パラメータ］ • *count* ... 再送回数(1..30)

［説明］ 選択されている相手について[PPP, BAP] の最大再送回数を設定する。

［デフォルト値］ 30

12. DHCPの設定

本機はDHCP[1]機能として、DHCPサーバ機能とDHCPリレーエージェント機能を実装しています。DHCPクライアント機能はWindows 98やWindows NT、Macintosh等で実装されており、これらと本機のDHCPサーバ機能、DHCPリレーエージェント機能を組み合わせることによりDHCPクライアントの基本的なネットワーク環境の自動設定を実現します。

ルータがDHCPサーバとして機能するかDHCPリレーエージェントとして機能するか、どちらとしても機能させないかは**dhcp service**コマンドにより設定します。現在どのようになっているかは**show dhcp**コマンドにより知ることができます。

DHCPサーバ機能は、DHCPクライアントからのコンフィギュレーション要求を受けてIPアドレスの割り当て（リース）や、ネットマスク、DNSサーバの情報等を提供します。

割り当てるIPアドレスの範囲とリース期間は**dhcp scope**コマンドにより設定されたものが使用されます。IPアドレスの範囲は複数の設定が可能であり、それぞれの範囲をDHCPスコープ番号で管理します。DHCPクライアントからの設定要求があるとDHCPサーバはDHCPスコープの中で未割り当てのIPアドレスを自動的に通知します。なお、特定のDHCPクライアントに特定のIPアドレスを固定的にリースする場合には、**dhcp scope**コマンドで定義したスコープ番号を用いて**dhcp scope bind**コマンドで予約します。予約の解除は**no dhcp scope bind**コマンドで行います。IPアドレスのリース期間には時間指定と無期限の両方が可能であり、これは**dhcp scope**コマンドの**expire**及び**maxexpire**キーワードのパラメータで指定します。リース状況は**show status dhcp**コマンドにより知ることができます。DHCPクライアントに通知するDNSサーバのIPアドレス情報は、**dns server**コマンドで設定されたものを通知します。

DHCPリレーエージェント機能は、ローカルセグメントのDHCPクライアントからの要求を、あらかじめ設定されたリモートのネットワークセグメントにあるDHCPサーバへ転送します。リモートセグメントのDHCPサーバは**dhcp relay server**コマンドで設定します。DHCPサーバが複数ある場合には、**dhcp relay select**コマンドにより選択方式を指定することができます。

1 DHCP: Dynamic Host Configuration Protocol; RFC1541

12.1 DHCPの動作の設定

［入力形式］ **dhcp service** *type*

no dhcp service [*type*]

［パラメータ］ • *type*

- server... DHCPサーバとして機能させる
- relay ... DHCPリレーエージェントとして機能させる

［説明］ DHCPに関する機能を設定する。

［ノート］ DHCPリレーエージェント機能使用時には、NAT機能を使用することはできない。

［デフォルト値］ DHCPサービスは機能しない

12.2 DHCPスコープの定義

［入力形式］ **dhcp scope** *N ip-ip/mask* [except *ex_ip* ...] [gateway *gw_ip*] [expire *time*] [maxexpire *time*]

no dhcp scope *N* [*ip-ip/mask* [except *ex_ip* ...] [gateway *gw_ip*] [expire *time*] [maxexpire *time*]]

［パラメータ］
- *N* ... スコープ番号 (1..65535)
- *ip-ip* ... 対象となるネットワークで割り当てる IP アドレスの範囲
- *mask* ... ネットマスク長
- *ex_ip* ... IP アドレス指定範囲の中で除外する IP アドレス (空白で区切って複数指定可能)
- *gw_ip* ... IP アドレス対象ネットワークのゲートウェイの IP アドレス
- *time* ... 時間
  - 分 (1..21474836)
  - 時間: 分
  - infinity ... 無期限リース

［説明］ DHCP サーバとして割り当てる IP アドレスのスコープを設定する。

除外 IP アドレスは複数指定できる。リース期間としては無期限を指定できるほか、DHCP クライアントから要求があった場合の許容最大リース期間を指定できる。

［ノート］ ひとつのネットワークについて複数の DHCP スコープを設定することはできない。複数の DHCP スコープで同一の IP アドレスを含めることはできない。IP アドレス範囲にネットワークアドレス、ブロードキャストアドレスを含む場合、割り当て可能アドレスから除外される。

DHCP リレーエージェントを経由しない DHCP クライアントに対して gateway キーワードによる設定パラメータが省略されている場合にはルータ自身の IP アドレスを通知する。

DHCP スコープを上書きした場合、以前のリース情報および予約情報は消去される。

［デフォルト値］ expire *time* = 72:00

maxexpire *time* = 72:00

12.3 DHCP予約アドレスの設定

［入力形式］ **dhcp scope bind** *scope_num ip_address mac_address*

no dhcp scope bind *scope_num ip_address* [*mac_address*]

［パラメータ］
- *scope_num* ... スコープ番号(1..65535)
- *ip_address* ... 予約する IP アドレス
- *mac_address* ... XX:XX:XX:XX:XX:XX (XX は 16 進数)予約 DHCP クライアントの MAC アドレス

［説明］ IP アドレスをリースする DHCP クライアントを固定的に設定する。

bind された IP アドレスは、たとえ DHCP スコープ中に他に割り当て可能な IP アドレスがなくなった場合でも、その対応する MAC アドレス以外のホストには割り当てられない。

［ノート］ IP アドレスは、*scope_num* パラメータで指定された DHCP スコープ内にあるものでなければならない。ひとつの DHCP スコープ内では、ひとつの MAC アドレスに複数の IP アドレスを設定することはできない。

他の DHCP クライアントにリース中の IP アドレスを予約設定した場合、リース終了後にその IP アドレスの割り当てが行われる。

dhcp scope コマンドを実行した場合、関連する予約はすべて消去される。

124 DHCPオプションの設定

［入力形式］

dhcp scope option *scope_num option=value*

no dhcp scope option *scope_num* [*option=value*]

［パラメータ］

• *scope_num* ... スコープ番号(1..65535)

• *option* ... オプション番号(1..49,64..76,128..254) またはニーモニック

主なニーモニック

router	3
dns	6
hostname	12
domain	15
wins_server	44

• *value* ... オプション値

値としては以下の種類があり、どれが使えるかはオプション番号で決まる。例えば、'router', 'dns', 'wins server' は IP アドレスの配列であり、'hostname', 'domain' は文字列である。

1 オクテット整数	0..255
2 オクテット整数	0..65535
2 オクテット整数の配列	2 オクテット整数をコンマ(,) で並べたもの
4 オクテット整数	0..4294967295
IP アドレス	IP アドレス
IP アドレスの配列	IP アドレスをコンマ(,)で並べたもの
文字列	文字列
スイッチ	"on", "off", "1", "0" のいずれか
バイナリ	2 桁 16 進数をコンマ(,)で並べたもの

［説明］

スコープに対して送信する DHCP オプションを設定する。**dns server** コマンドや **wins server** コマンドなどでも暗黙のうちに DHCP オプションを送信していたが、それを明示的に指定できる。また、暗黙の DHCP オプションではスコープでオプションの値を変更することはできないが、このコマンドを使えばそれも可能になる。

［ノート］

no dhcp scope コマンドでスコープが削除されるとオプションの設定もすべて消える。

12.5 リースするIPアドレスの重複をチェックするか否かの設定

［入力形式］ **dhcp duplicate check** *check1 check2*

［パラメータ］
- *check1*
  - on ... LAN 内を対象とするチェックを行う
  - off ... LAN 内を対象とするチェックを行わない
- *check2*
  - on ... LAN 外 (DHCP リレーエージェント経由)を対象とするチェックを行う
  - off ... LAN 外 (DHCP リレーエージェント経由)を対象とするチェックを行わない

［説明］ DHCP サーバとして機能するとき、IP アドレスを DHCP クライアントにリースする直前に、その IP アドレスを使っているホストが他にいないことをチェックするか否かを設定する。

［ノート］ LAN 内のスコープに対しては arp を、DHCP リレーエージェント経由のスコープに対しては ping を使ってチェックする。

［デフォルト値］ *check* = on

check = on

12.6 DHCPサーバの指定の設定

［入力形式］ **dhcp relay server** *host1* [*host2* [*host3* [*host4*]]]

no dhcp relay server [*host1* [*host2* [*host3* [*host4*]]]]

［パラメータ］ • *host1* ... *host4* ... DHCP サーバの IP アドレス

［説明］ DHCP BOOTREQUEST パケットを中継するサーバを最大 4 つまで設定する。

サーバが複数指定された場合は、BOOTREQUEST パケットを複写してすべてのサーバに中継するか、あるいは一つだけサーバを選択して中継するかは **dhcp relay select** コマンドの設定で決定される。

12.7 DHCPサーバの選択方法の設定

［入力形式］ **dhcp relay select** *type*

no dhcp relay select [*type*]

［パラメータ］
- *type*
  - hash ... Hash 関数を利用して一つだけサーバを選択する
  - all ... すべてのサーバを選択する

［説明］ **dhcp relay server** コマンドで設定された複数のサーバの取り扱いを設定する。

hash が指定された時は、Hash 関数を利用して一つだけサーバが選択されてパケットが中継される。この Hash 関数は、DHCP メッセージの chaddr フィールドを引数とするので、同一の DHCP クライアントに対しては常に同じサーバが選択されるはずである。all が指定された時は、パケットはすべてのサーバに対し複写中継される。

［デフォルト値］ hash

12.8 DHCP BOOTREQUESTパケットの中継基準の設定

［入力形式］ **dhcp relay threshold** *time*

no dhcp relay threshold [*time*]

［パラメータ］ • *time* ... 秒数 (0..65535)

［説明］ DHCP BOOTREQUEST パケットの secs フィールドとこのコマンドによる秒数を比較し、設定値より小さな secs フィールドを持つ DHCP BOOTREQUEST パケットはサーバに中継しないようにする。

これにより、同一 LAN 上に別の DHCP サーバがあるにも関わらず遠隔地の DHCP サーバにパケットを中継してしまうのを避けることができる。

［デフォルト値］ 0

13. SNMPの設定

13.1 読み出し専用のコミュニティ名の設定

［入力形式］ **snmp community read-only** *name*

no snmp community read-only [*name*]

［パラメータ］ • *name* ... SNMP によるアクセスモードが読み出し専用であるコミュニティ名

［説明］ SNMP によるアクセスモードが読み出し専用であるコミュニティ名を設定する。名称は 1 文字以上 16 文字以内。

［デフォルト値］ public

13.2 読み書き可能なコミュニティ名の設定

［入力形式］ **snmp community read-write** *name*

no snmp community read-write [*name*]

［パラメータ］ • *name* ... SNMP によるアクセスモードが読み書き可能であるコミュニティ名

［説明］ SNMP によるアクセスモードが読み書き可能であるコミュニティ名を設定する。名称は 1 文字以上 16 文字以内。

［デフォルト値］ 空文字列

13.3 認証失敗時 (authenticationFailure) にトラップを送信するか否かの設定

［入力形式］ **snmp enableauthentraps** *send*

no snmp enableauthentraps [*send*]

［パラメータ］ • *send*

◦ on ... 送信する

◦ off ... 送信しない

［説明］ MIB 変数 snmpEnableAuthenTraps を設定する。

これを off にすると、誤ったコミュニティ名を持つパケットを受信した時にトラップを送信しない。SNMP トラップは **snmp trap host** コマンドで指定されたホストに対して送信される。

［デフォルト値］ on

13.4 SNMPによるアクセスを許可するホストの設定

［入力形式］ **snmp host** *host*

no snmp host [*host*]

［パラメータ］ • *host*

◦ IP アドレス ... SNMP によるアクセスを許可するホストの IP アドレス

◦ any ... すべてのホストから SNMP によりアクセスできる

◦ none ... すべてのホストから SNMP によりアクセスできない

［説明］ SNMP によるアクセスを許可するホストを設定する。

［デフォルト値］ none

13.5 sysContactの設定

［入力形式］ **snmp syscontact** *name*

no snmp syscontact [*name*]

［パラメータ］ • *name* ... sysContactとして登録する名称

［説明］ MIB変数sysContactを設定する。255文字以内の文字列が設定できる。空白を含ませるためには、パラメータ全体をダブルクォート(")、もしくはシングルクォート(')で囲む。

sysContactは一般的に、管理者の名前や連絡先を記入しておく変数である。

［デフォルト値］ sysContactは設定されていない。

13.6 sysLocationの設定

［入力形式］ **snmp syslocation** *name*

no snmp syslocation [*name*]

［パラメータ］ • *name* ... sysLocationとして登録する名称

［説明］ MIB変数sysLocationを設定する。255文字以内の文字列が設定できる。空白を含ませるためには、パラメータ全体をダブルクォート(")、もしくはシングルクォート(')で囲む。

sysLocationは一般的に、機器の設置場所を記入しておく変数である。

［デフォルト値］ sysLocationは設定されていない。

13.7 sysNameの設定

［入力形式］ **snmp sysname** *name*

no snmp sysname [*name*]

［パラメータ］ • *name* ... sysNameとして登録する名称

［説明］ MIB変数sysNameを設定する。255文字以内の文字列が設定できる。空白を含ませるためには、パラメータ全体をダブルクォート(")、もしくはシングルクォート(')で囲む。

sysNameは一般的に、機器の名称を記入しておく変数である。

［デフォルト値］ sysNameは設定されていない。

13.8 SNMPトラップのコミュニティ名の設定

［入力形式］ **snmp trap community** *name*

no snmp trap community [*name*]

［パラメータ］ • *name* ... 送信トラップのコミュニティ名

［説明］ トラップを送信する際のコミュニティ名を設定する。名称は1文字以上16文字以内。

［デフォルト値］ public

13.9 SNMPトラップの送信先の設定

［入力形式］ **snmp trap host** *host*

no snmp trap host [*host*]

［パラメータ］ • *host*

◦ IP アドレス ... SNMP トラップを送信する先のホストの IP アドレス

［説明］ SNMP トラップを送信する先のホストを設定する。

［デフォルト値］ SNMP トラップを送信しない

13.10 PPインタフェースの情報を MIB2 の範囲で表示するか否か設定

［入力形式］ **snmp yrifppdisplayatmib2** *sw*

［パラメータ］ • *sw*

◦ on ... MIB 変数 yrIfPpDisplayAtMib2 を "enabled(1)" とする

◦ off ... MIB 変数 yrIfPpDisplayAtMib2 を "disabled(2)" とする

［説明］ MIB 変数 yrIfPpDisplayAtMib2 の値をセットする。この MIB 変数は、PP インタフェースを MIB2 の範囲で表示するかどうかを決定する。Rev.4 以前と同じ表示にする場合には、MIB 変数を "enabled(1)" に、つまり、このコマンドで "on" を設定する。

［デフォルト値］ off

14. ICMPの設定

14.1 ICMP Echo Replyを送信するか否かの設定

［入力形式］ **ip icmp echo-reply send** *send*

no ip icmp echo-reply send [*send*]

［パラメータ］ • *send*

◦ on ... 送信する

◦ off ... 送信しない

［説明］ ICMP Echo を受信した時に、ICMP Echo Reply を返すか否かを設定する。

［デフォルト値］ on

14.2 ICMP Mask Replyを送信するか否かの設定

［入力形式］ **ip icmp mask-reply send** *send*

no ip icmp mask-reply send [*send*]

［パラメータ］ • *send*

◦ on ... 送信する

◦ off ... 送信しない

［説明］ ICMP Mask Request を受信した時に、ICMP Mask Reply を返すか否かを設定する。

［デフォルト値］ on

14.3 ICMP Parameter Problemを送信するか否かの設定

［入力形式］ **ip icmp parameter-problem send** *send*

no ip icmp parameter-problem send [*send*]

［パラメータ］ • *send*

◦ on ... 送信する

◦ off ... 送信しない

［説明］ 受信した IP パケットの IP オプションにエラーを検出した時に、ICMP Parameter Problem を送信するか否かを設定する。

［デフォルト値］ on

14.4 ICMP Redirectを送信するか否かの設定

［入力形式］ **ip icmp redirect send** *send*

no ip icmp redirect send [*send*]

［パラメータ］ • *send*

◦ on ... 送信する

◦ off ... 送信しない

［説明］ 他のゲートウェイ宛の IP パケットを受信して、そのパケットを適切なゲートウェイに回送した時に、同時にパケットの送信元に対して ICMP Redirect を送信するか否かを設定する。

［デフォルト値］ on

14.5 ICMP Redirect受信時の処理の設定

［入力形式］ **ip icmp redirect receive** *action*

no ip icmp redirect receive [*action*]

［パラメータ］ • *action*

◦ on ... 処理する

◦ off ... 無視する

［説明］ ICMP Redirect を受信した場合に、それを処理して自分の経路テーブルに反映させるか、あるいは無視するかを設定する。

［デフォルト値］ off

14.6 ICMP Time Exceededを送信するか否かの設定

［入力形式］ **ip icmp time-exceeded send** *send*

no ip icmp time-exceeded send [*send*]

［パラメータ］ • *send*

◦ on ... 送信する

◦ off ... 送信しない

［説明］ 受信した IP パケットの TTL が 0 になってしまったため、そのパケットを破棄した時に、同時にパケットの送信元に対して ICMP Time Exceeded を送信するか否かを設定する。

［デフォルト値］ on

14.7 ICMP Timestamp Replyを送信するか否かの設定

［入力形式］ **ip icmp timestamp-reply send** *send*

no ip icmp timestamp-reply send [*send*]

［パラメータ］ • *send*

◦ on ... 送信する

◦ off ... 送信しない

［説明］ ICMP Timestamp を受信した時に、ICMP Timestamp Reply を返すか否かを設定する。

［デフォルト値］ on

14.8 ICMP Destination Unreachableを送信するか否かの設定

［入力形式］ **ip icmp unreachable send** *send*

no ip icmp unreachable send [*send*]

［パラメータ］ • *send*

◦ on ... 送信する

◦ off ... 送信しない

［説明］ 経路テーブルに宛先が見つからない場合や、あるいは ARP が解決できなくて IP パケットを破棄することになった時に、同時にパケットの送信元に対して ICMP Destination Unreachable を送信するか否かを設定する。

［デフォルト値］ on

14.9 受信したICMPのログを記録するか否かの設定

［入力形式］ **ip icmp log** *log*

no ip icmp log [*log*]

［パラメータ］ • *log*

- on ... 記録する
- off ... 記録しない

［説明］ 受信したICMPをdebugタイプのログに記録するか否かを設定する。

［デフォルト値］ on

15. RADIUSの設定

15.1 RADIUSによる認証を使用するか否かの設定

［入力形式］ **radius auth** *auth*

no radius auth [*auth*]

［パラメータ］ • *auth*

◦ on ... 使用する

◦ off ... 使用しない

［説明］ anonymous に対して何らかの認証を要求する設定の時に、相手から受け取ったユーザネーム(PAP であれば UserID、CHAP であれば NAME)が、自分で持つユーザネーム(**pp auth username** コマンドで指定)の中に含まれていない場合には RADIUS サーバに問い合わせるか否かを設定する。

［ノート］ RADIUS による認証と RADIUS によるアカウントは独立して使用できる。

サポートしているアトリビュートについては、WWW サイトのドキュメント **<http://www.rtpro.yamaha.co.jp>** を参照すること。

［デフォルト値］ off

15.2 RADIUSによるアカウントを使用するか否かの設定

［入力形式］ **radius account** *account*

no radius account [*account*]

［パラメータ］ • *account*

◦ on ... 使用する

◦ off ... 使用しない

［説明］ RADIUS によるアカウントを使用するか否かを設定する。

［ノート］ RADIUS による認証と RADIUS によるアカウントは独立して使用できる。

サポートしているアトリビュートについては、WWW サイトのドキュメント **<http://www.rtpro.yamaha.co.jp>** を参照すること。

［デフォルト値］ off

15.3 RADIUSサーバの指定

［入力形式］ **radius server** *ip1* [*ip2*]

no radius server [*ip1* [*ip2*]]

［パラメータ］ • *ip1* ... RADIUS サーバ (正)の IP アドレス

• *ip2* ... RADIUS サーバ (副)の IP アドレス

［説明］ RADIUS サーバを設定する。2 つまで指定でき、最初のサーバから返事をもらえないときは、2 番目のサーバに問い合わせを行う。

RADIUS には認証とアカウントの 2 つの機能があり、それぞれのサーバは **radius auth server** / **radius account server** コマンドで個別に設定できる。**radius server** コマンドでの設定は、これら個別の設定が行われていない時に有効となり、認証、アカウントいずれでも用いられる。

15.4 RADIUS認証サーバの指定

［入力形式］ **radius auth server** *ip1* [*ip2*]

no radius auth server [*ip1* [*ip2*]]

［パラメータ］ • *ip*1 ... RADIUS 認証サーバ (正)の IP アドレス

• *ip*2 ... RADIUS 認証サーバ (副)の IP アドレス

［説明］ RADIUS 認証サーバを設定する。2 つまで指定でき、最初のサーバから返事をもらえないときは、2 番目のサーバに問い合わせを行う。

［ノート］ このコマンドで RADIUS 認証サーバの IP アドレスが指定されていない時は、**radius server** コマンドで指定した IP アドレスを認証サーバとして用いる。

15.5 RADIUSアカウントサーバの指定

［入力形式］ **radius account server** *ip1* [*ip2*]

no radius account server [*ip1* [*ip2*]]

［パラメータ］ • *ip1* ... RADIUS アカウントサーバ (正)の IP アドレス

• *ip2* ... RADIUS アカウントサーバ (副)の IP アドレス

［説明］ RADIUS アカウントサーバを設定する。2 つまで指定でき、最初のサーバから返事をもらえないときは、2 番目のサーバに問い合わせを行う。

［ノート］ このコマンドで RADIUS アカウントサーバの IP アドレスが指定されていない時は、**radius server** コマンドで指定した IP アドレスを認証サーバとして用いる。

15.6 RADIUS認証サーバの UDPポートの設定

［入力形式］ **radius auth port** *port_number*

no radius auth port [*port_number*]

［パラメータ］ • *port_number*... UDP ポート番号

［説明］ RADIUS 認証サーバの UDP ポート番号を設定する。

［ノート］ 新しい RFC ではポート番号として 1812 を使うことになっている。

［デフォルト値］ 1645

15.7 RADIUSアカウントサーバの UDPポートの設定

［入力形式］ **radius account port** *port_number*

no radius account port [*port_number*]

［パラメータ］ • *port_number*... UDP ポート番号

［説明］ RADIUS アカウントサーバの UDP ポート番号を設定する。

［ノート］ 新しい RFC ではポート番号として 1813 を使うことになっている。

［デフォルト値］ 1646

15.8 RADIUSシークレットの設定

［入力形式］ **radius secret** *secret*

no radius secret [*secret*]

［パラメータ］ • *secret* ... シークレット文字列

［説明］ RADIUS シークレットを設定する。

15.9 RADIUS再送信パラメータの設定

［入力形式］ **radius retry** *count time*

no radius retry [*count time*]

［パラメータ］ • *count* ... 再送回数(1..10)

• *time* ... ミリ秒 (20..10000)

［説明］ RADIUS パケットの再送回数とその時間間隔を設定する。

［デフォルト値］ *count* = 4

time = 3000

16. NAT 機能

NAT 機能は、ルータが転送する IP パケットの始点 / 終点 IP アドレスや、TCP/UDP のポート番号を変換することにより、アドレス体系の異なる IP ネットワークを接続することができる機能である。
NAT 機能を用いると、プライベートアドレス空間とグローバルアドレス空間との間でデータを転送したり、1 つのグローバル IP アドレスに複数のホストを対応させたりすることができる。

ヤマハ RT シリーズでは、始点 / 終点 IP アドレスの変換だけを行うことを NAT と呼び、TCP/UDP のポート番号の変換を伴うものを IP マスカレードと呼んでいる。

アドレス変換規則を表す記述を NAT ディスクリプタと呼ぶ。それぞれの NAT ディスクリプタには、アドレス変換の対象とすべきアドレス空間が定義される。アドレス空間の記述には、**nat descriptor address inner**、**nat descriptor address outer** コマンドを用いる。前者は NAT 処理の内側 (INNER)のアドレス空間を、後者は NAT 処理の外側(OUTER)のアドレス空間を定義するコマンドである。原則的に、これら2つのコマンドを対で設定することにより、変換前のアドレスと変換後のアドレスとの対応づけが定義される。
NAT ディスクリプタはインタフェースに対して適用される。インタフェースに接続された先のネットワークが NAT 処理の外側であり、インタフェースから本機を経由して他のインタフェースから繋がるネットワークが NAT 処理の内側ということになる。

NAT ディスクリプタは動作タイプ属性を持つ。IP マスカレードやアドレスの静的割当てなどの機能を利用するときには、該当する動作タイプを選択する必要がある。

16.1 インタフェースへの NAT ディスクリプタ適用の設定

［入力形式］ **ip *interface* nat descriptor** *nat_descriptor_list*

no ip *interface* nat descriptor [*nat_descriptor_list*]

［パラメータ］ • ***interface*** ... LAN インタフェース名、または、pp、tunnel

• *nat_descriptor_list*

◦ 空白で区切られた NAT ディスクリプタ番号(1..21474836)の並び(16 個以内)

［説明］ インタフェースを通過するパケットに対して、リストに定義された順番で NAT ディスクリプタによって定義された NAT 変換を順番に処理する。

［ノート］ インタフェースが LAN である場合、NAT ディスクリプタの OUTER アドレスに関しては、同一 LAN の ARP 要求に対して ARP 応答する。

16.2 NAT ディスクリプタの動作タイプの設定

［入力形式］ **nat descriptor type** *nat_descriptor type*

no nat descriptor type [*nat_descriptor type*]

［パラメータ］ • *nat_descriptor* ... NAT ディスクリプタ番号 (1..21474836)

• *type*

◦ none ... NAT 変換機能を利用しない

◦ nat ... 動的 NAT 変換と静的 NAT 変換を利用

◦ masquerade ... 静的 NAT 変換と IP マスカレード変換

◦ nat-masquerade ... 動的 NAT 変換と静的 NAT 変換と IP マスカレード変換

［説明］ NAT 変換の動作タイプを指定する。

［ノート］ nat-masquerade は、動的 NAT 変換できなかったパケットを IP マスカレード変換で救う。例えば、外側アドレスが 16 個利用可能の場合は先勝ちで 15 個 NAT 変換され、残りは IP マスカレード変換される。

［デフォルト値］ none

16.3 NAT 処理の外側 IP アドレスの設定

［入力形式］ **nat descriptor address outer** *nat_descriptor outer_ipaddress_list*

no nat descriptor address outer *nat_descriptor* [*outer_ipaddress_list*]

［パラメータ］ • *nat_descriptor* ... NAT ディスクリプタ番号 (1..21474836)

• *outer_ipaddress_list*... NAT 対象の外側 IP アドレス範囲のリストまたはニーモニック

◦ 1 個の IP アドレスまたは間に - をはさんだ IP アドレス (範囲指定) 、及びこれらを任意に並べたもの

◦ ipcp ... PPP の IPCP の IP-Address オプションにより接続先から通知される IP アドレス

◦ primary ... **ip *interface* address** コマンドで設定されている IP アドレス

◦ secondary ... **ip *interface* secondary address** コマンドで設定されている IP アドレス

［説明］ 動的 NAT 処理の対象である外側の IP アドレスの範囲を指定する。IP マスカレードでは、先頭の 1 個の外側の IP アドレスが使用される。

［ノート］ ニーモニックをリストにすることはできない。

適用されるインタフェースにより使用できるパラメータが異なる。

適用インタフェース

	LAN	PP	トンネル
ipcp	×	○	×
primary	○	×	×
secondary	○	×	×
IP アドレス	○	○	○

［デフォルト値］ ipcp

16.4 NAT 処理の内側 IP アドレスの設定

［入力形式］ **nat descriptor address inner** *nat_descriptor inner_ipaddress_list*

no nat descriptor address inner *nat_descriptor* [*inner_ipaddress_list*]

［パラメータ］ • *nat_descriptor* ... NAT ディスクリプタ番号(1..21474836)

• *inner_ipaddress_list*... NAT 対象の内側 IP アドレス範囲のリストまたはニーモニック

◦ 1 個の IP アドレスまたは間に - をはさんだ IP アドレス(範囲指定)、及びこれらを任意に並べたもの

◦ auto ... 全て

［説明］ NAT/IP マスカレード処理の対象である内側の IP アドレスの範囲を指定する。

［デフォルト値］ auto

16.5 静的 NAT エントリの設定

［入力形式］ **nat descriptor static** *nat_descriptor id outer_ip=inner_ip* [*count*]

no nat descriptor static *nat_descriptor id* [*outer_ip=inner_ip* [*count*]]

［パラメータ］ • *nat_descriptor* ... NAT ディスクリプタ番号(1..21474836)

• *id* ... 静的 NAT エントリの識別情報(1..21474836)

• *outer_ip* ... 外側 IP アドレス(1 個)

• *inner_ip* ... 内側 IP アドレス(1 個)

• *count* ... 連続設定する個数(省略時は 1)

［説明］ NAT 変換で固定割り付けする IP アドレスの組み合せを指定する。個数を同時に指定すると指定されたアドレスを始点とした範囲指定とする。

［ノート］ 外側アドレスが NAT 処理対象として設定されているアドレスである必要は無い。

静的 NAT のみを使用する場合には、**nat descriptor address outer** コマンドと **nat descriptor address inner** コマンドの設定に注意する必要がある。デフォルト値がそれぞれ ipcp と auto であるので、例えば何らかの IP アドレスをダミーで設定しておくことで動的動作しないようにする。

16.6 IP マスカレード使用時に rlogin,rcp と ssh を使用するか否かの設定

［入力形式］ **nat descriptor masquerade rlogin** *nat_descriptor use*

no nat descriptor masquerade rlogin *nat_descriptor* [*use*]

［パラメータ］ • *nat_descriptor* ... NAT ディスクリプタ番号(1..21474836)

• *use*

◦ on ... 使用する

◦ off ... 使用しない

［説明］ IP マスカレード使用時に rlogin、rcp、ssh の使用を許可するか否かを設定する。

［ノート］ on にすると、rlogin、rcp と ssh のトラフィックに対してはポート番号を変換しなくなる。

また on の場合に rsh は使用できない。

［デフォルト値］ off

16.7 静的 IP マスカレードエントリの設定

［入力形式］ **nat descriptor masquerade static** *nat_descriptor id inner_ip protocol port*

no nat descriptor masquerade static *nat_descriptor id* [*inner_ip protocol port*]

［パラメータ］
- *nat_descriptor* ... NAT ディスクリプタ番号(1..21474836)
- *id* ... 静的 IP マスカレードエントリの識別情報(1 以上の数値)
- *inner_ip* ... 内側 IP アドレス(1 個)
- *protocol* ... 対象プロトコル
  - tcp ... TCP プロトコル
  - udp ... UDP プロトコル
- *port* ... 固定するポート番号（ニーモニック）、または、ポート番号の範囲指定

［説明］ IP マスカレードによる通信でポート番号変換を行わないようにポートを固定する。

16.8 NAT の IP アドレスマップの消去タイマの設定

［入力形式］ **nat descriptor timer** *nat_descriptor time*

nat descriptor timer *nat_descriptor* [*time*]

［パラメータ］
- *nat_descriptor* ... NAT ディスクリプタ番号(1..21474836)
- *time* ... 消去タイマの秒数(30..21474836)

［説明］ 動的に生成された NAT 管理テーブルから自動的に消去されるまでの時間を設定する。

［デフォルト値］ 900

16.9 動的 NAT ディスクリプタのアドレスマップの表示

［入力形式］ **show nat descriptor address** [*nat_descriptor*]

［パラメータ］
- *nat_descriptor*
  - NAT ディスクリプタ番号(1..21474836)
  - all ... すべての NAT ディスクリプタ番号
- *nat_descriptor* を省略した場合にはすべての NAT ディスクリプタ番号について表示する

［説明］ 動的な NAT ディスクリプタのアドレスマップを表示する。

16.10 動作中の NAT ディスクリプタの適用リストの表示

［入力形式］ **show nat descriptor interface bind**

［パラメータ］ なし

［説明］ NAT ディスクリプタと適用インタフェースのリストを表示する。

16.11 LAN インタフェースの NAT ディスクリプタのアドレスマップの表示

［入力形式］ **show nat descriptor interface address** *interface* [*number*]

［パラメータ］ . *interface* ... LAN インタフェース名、pp、tunnel

. *number* ... pp、tunnel の場合の相手先番号

［説明］ インタフェースに適用されている NAT ディスクリプタのアドレスマップを表示する。

16.12 NAT アドレステーブルのクリア

［入力形式］ **clear nat descriptor dynamic** *nat_descriptor*

［パラメータ］ • *nat_descriptor*

◦ NAT ディスクリプタ番号(1..21474836)

◦ all ... すべての NAT ディスクリプタ番号

［説明］ NAT アドレステーブルをクリアする。

［ノート］ 通信中にアドレス管理テーブルをクリアした場合、通信が一時的に不安定になる可能性がある。

16.13 インタフェースの NAT アドレステーブルのクリア

［入力形式］ **clear nat descriptor interface dynamic** *interface* [*number*]

［パラメータ］ • *interface* ... LAN インタフェース名、pp、tunnel

• *number* ... pp、tunnel の場合の相手先番号

［説明］ インタフェースに適用されている NAT アドレステーブルをクリアする。

17. DNSの設定

本機は、DNS (Domain Name Service)機能として名前解決とリカーシブサーバ機能を持ちます。ネームサーバとなることはできません。

名前解決の機能としては、**ping**や**traceroute**、**rdate**、**ntpdate**、**telnet**コマンドなどのIPアドレスパラメータの代わりに名前を指定したり、SYSLOGなどの表示機能においてIPアドレスを名前で表示したりすることができます。

リカーシブサーバ機能は、DNSサーバとクライアントの間に入って、DNSパケットの中継を行います。本機宛にクライアントから届いたDNS問い合わせパケットを**dns server**コマンドで設定されたDNSサーバに中継します。DNSサーバからの回答は本機宛に届くので、それをクライアントに転送します。最大256件のキャッシュを持ち、キャッシュにあるデータに関してはDNSサーバに問い合わせることなく返事を返すため、DNSによるトラフィックを削減する効果があります。キャッシュは、DNSサーバからデータを得た時にデータに記されていた時間だけ保持されます。

DNSの機能を使用するためには、**dns server**コマンドを設定しておく必要があります。また、この設定はDHCPサーバ機能において、DHCPクライアントの設定情報にも使用されます。

17.1 DNSサーバのIPアドレスの設定

［入力形式］ **dns server** *ip_address* [*ip_address* ...]

no dns server [*ip_address* ...]

［パラメータ］ • *ip_address*

◦ DNS サーバの IP アドレス (空白で区切って最大4ヶ所まで設定可能)

［説明］ DNS サーバの IP アドレスを指定する。

この IP アドレスはルータが DHCP サーバとして機能する場合に DHCP クライアントに通知するためや、IPCP の MS 拡張オプションで相手に通知するためにも使用される。

［デフォルト値］ DNS サーバは設定されていない。

17.2 DNSサーバを通知してもらう相手先情報番号の設定

［入力形式］ **dns server pp** *peer_number*

no dns server pp [*peer_number*]

［パラメータ］ • *peer_number*

◦ DNS サーバを通知してもらう相手先情報番号

［説明］ DNS サーバを通知してもらう相手先情報番号を設定する。このコマンドで相手先情報番号が設定されていると、DNS での名前解決を行うときに、まずこの相手先に発信して、そこで PPP の IPCP MS 拡張機能で通知された DNS サーバに対して問い合わせを行う。

相手先に接続できなかったり、接続できても DNS サーバの通知がなかった場合には名前解決は行われない。

dns server コマンドで DNS サーバが明示的に指定されている場合には、そちらの設定が優先される。**dns server** コマンドに指定したサーバから返事がない場合には、相手先への接続と DNS サーバの通知取得が行われる。

［ノート］ この機能を使用する場合には、**dns server pp** コマンドで指定された相手先情報に、**pppipcp msext on** の設定が必要である。

［デフォルト値］ DNS サーバを通知してもらう相手先は設定されていない。

17.3 DNSドメイン名の設定

［入力形式］ **dns domain** *domain_name*

no dns domain [*domain_name*]

［パラメータ］ • *domain_name* ...DNS ドメインを表す文字列

［説明］ ルータが所属する DNS ドメインを設定する。

名前解決に失敗した場合、このドメイン名を補完して再度解決を試みる。

ルータが DHCP サーバとして機能する場合、設定したドメイン名は DHCP クライアントに通知するためにも使用される。ルータのあるネットワーク及びそれが含むサブネットワークの DHCP クライアントに対して通知する。

17.4 プライベートアドレスに対する問い合わせを処理するか否かの設定

［入力形式］ **dns private address spoof** *spoof*

no dns private address spoof [*spoof*]

［パラメータ］ • *spoof*

◦ on ... 処理する

◦ off ... 処理しない

［説明］ on の場合、DNS リカーシブサーバ機能で、プライベートアドレスの PTR レコードに対する問い合わせに対し、上位サーバに問い合わせを転送することなく、自分でその問い合わせに対し“ NXDomain ”、すなわち「そのようなレコードはない」というエラーを返す。

［デフォルト値］ off

17.5 DHCP/IPCP MS拡張で DNSサーバを通知する順序の設定

［入力形式］ **dns notice order** *protocol server* [*server*]

no dns notice order *protocol* [*server* [*server*]]

［パラメータ］ • *protocol*

◦ dhcp ... DHCP による通知

◦ msext ... IPCP MS 拡張による通知

• *server*

◦ none ... 一切通知しない

◦ me ... 本機自身

◦ server ... **dns server** コマンドに設定したサーバ群

［説明］ DHCP や IPCP MS 拡張では DNS サーバを複数通知できるが、それをどのような順序で通知するかを設定する。

none を設定すれば、他の設定に関わらず DNS サーバの通知を行わなくなる。me は本機自身の DNS リカーシブサーバ機能を使うことを通知する。server では、**dns server** コマンドに設定したサーバ群を通知することになる。IPCP MS 拡張では通知できるサーバの数が最大 2 に限定されているので、後ろに me が続く時は先頭の 1 つだけと本機自身を、server 単独で設定されている時には先頭の 2 つだけを通知する。

［デフォルト値］ dhcp me server

msext me server

17.6 SYSLOG表示でDNSにより名前解決するか否かの設定

［入力形式］ **dns syslog resolv** *resolv*

no dns syslog resolv [*resolv*]

［パラメータ］ • *resolv*

◦ on ... 解決する

◦ off ... 解決しない

［説明］ SYSLOG 表示で DNS により名前解決するか否かを設定する。

［デフォルト値］ off

17.7 静的DNSレコードの登録

［入力形式］ **ip host** *fqdn value*

dns static *type name value*

no ip host *fqdn* [*value*]

no dns static *type name* [*value*]

［パラメータ］ • *type* ... 名前のタイプ

◦ a ... ホストの IP アドレス

◦ ptr ... IP アドレスの逆引き用のポインタ

◦ mx ... メールサーバ

◦ ns ... ネームサーバ

◦ cname ... 別名

• *name, value* ... type パラメータによって以下のように意味が異なる

type パラメータ	*name*	*value*
a	FQDN	IP アドレス
ptr	IP アドレス	FQDN
mx	FQDN	FQDN
ns	FQDN	FQDN
cname	FQDN	FQDN

• *fqdn* ... ドメイン名を含んだホスト名

［説明］ 静的な DNS レコードを定義する。

ip host コマンドは、**dns static** コマンドで a と ptr を両方設定することを簡略化したものである。

［ノート］ 問い合わせに対して返される DNS レコードは以下のような特徴を持つ。

• TTL フィールドには 1 がセットされる

• Answer セクションに回答となる DNS レコードが 1 つセットされるだけで、Authority/Additional セクションには DNS レコードがセットされない

• MX レコードの preference フィールドは 0 にセットされる

［設定例］
```
# ip host pc1.rtpro.yamaha.co.jp 133.176.200.1
# dns static ptr 133.176.200.2 pc2.yamaha.co.jp
# dns static cname mail.yamaha.co.jp mail2.yamaha.co.jp
```

18. 優先制御／帯域制御

優先制御と帯域制御の機能は、インタフェースに入力されたパケットの順序を入れ換えて別のインタフェースに出力します。これらの機能を使用しない場合には、パケットは入力した順番に処理されます。

優先制御は、クラス分けしたキューに優先順位をつけ、まず高位のキューを出力し、そのキューが空になると次の順位のキューのパケットを出力する、という処理を行います。
帯域制御は、クラス分けしたキューをラウンドロビン方式で監視しますが、監視頻度に差を与えてキューごとに利用できる帯域に差をつけます。

クラスは、**queue class filter** コマンドにより、パケットのフィルタリングと同様な定義でパケットを分類します。クラスは 1 から 16 までの番号で識別します。優先制御では 1 から 4 までのクラスが、帯域制御では 1 から 16 までのクラスが使用できます。クラスは番号が大きいほど優先順位が高くなります。

パケットの処理アルゴリズムは、**queue *interface* type** コマンドにより、優先制御、帯域制御、単純 FIFO の中から選択します。これはインタフェースごとに選択することができます。

18.1 インタフェース速度の設定

［入力形式］ **speed** *interface speed*

no speed *interface* [*speed*]

［パラメータ］
- *interface* ... LAN インタフェース名、もしくは pp
- *speed* ... インタフェース速度(bit/s)

［説明］ 指定したインタフェースに対して、インタフェースの速度を設定する。帯域制御のためのパラメータ計算に用いられるもので、実際の速度を設定できるわけではない。物理的な速度と一致しているのが望ましい。MP により動的に回線速度が変動する場合などは、最低限の速度に設定しておく。

［ノート］ *speed* パラメータの後ろに 'k' または 'M' をつけると、それぞれ kbit/s、Mbit/s として扱われる。

［デフォルト値］ 0

18.2 クラス分けのためのフィルタ設定

［入力形式］ **queue class filter** *num class* ip *src_addr* [*dest_addr* [*proto* [*src_port* [*dest_port*]]]]

queue class filter *num class* ipx *src_net* [*src_node* [*dst_net* [*dst_node* [*type* [*src_socket* [*dst_ socket*]]]]]]

queue class filter *num class* bridge *src_mac* [*dst_mac* [*offset byte_list*]]

no queue class filter *num class* [*protocol* ...]

［パラメータ］
- *num* ... クラスフィルタの識別番号(1..100)
- *class* ... クラス(1..16)

IP フィルタ

- *src_addr* ... IP パケットの始点 IP アドレス
  - xxx.xxx.xxx.xxx xxx、xxx は
    - ▷ 10 進数
    - ▷ * (ネットマスクの対応するビットが 8 ビットとも 0 と同じ)
  - * (すべての IP アドレスに対応)

• *dest_addr* ... IP パケットの終点 IP アドレス (*src_address* と同じ形式)。省略した時は一個の * と同じ。

• *proto* ... フィルタリングするパケットの種類

◦ プロトコルを表す 10 進数

◦ プロトコルを表すニーモニック

icmp	1
tcp	6
udp	17

◦ 上項目のカンマで区切った並び(5 個以内)

◦ * (すべてのプロトコル)

◦ established

省略した時は * と同じ。

• *src_port* ... UDP 、TCP のソースポート番号

◦ ポート番号を表す 10 進数

◦ ポート番号を表すニーモニック(一部)

ニーモニック	ポート番号
ftp	20,21
ftpdata	20
telnet	23
smtp	25
domain	53
gopher	70
finger	79
www	80
pop3	110
sunrpc	111
ident	113
ntp	123
nntp	119
snmp	161
syslog	514
printer	515
talk	517
route	520
uucp	540

◦ 間に - をはさんだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。

◦ 上項目のカンマで区切った並び(10 個以内)

◦ * (すべてのポート)

省略した時は * と同じ。

• *dest_port* ... UDP 、TCP のデスティネーションポート番号

IPX フィルタ

• *src_net* ... 始点 IPX ネットワーク番号

◦ 0:0:0:1 ... FF:FF:FF:FE(2 桁以内の 16 進数以外に '*' も指定可)

◦ * (すべての IPX ネットワーク番号)

• *src_node* ... 始点 IPX ノード番号

◦ 0:0:0:0:0:1 ... FF:FF:FF:FF:FF:FE(2 桁以内の 16 進数以外に '*' も指定可)

◦ *(すべての IPX ノード番号)

◦ 省略した時は一個の * と同じ

• *dst_net* ... 終点 IPX ネットワーク番号 *src_net* と同じ形式。

• *dst_node* ... 終点 IPX ノード番号 *src_node* と同じ形式。

• *type* ...IPX パケットタイプ

◦ 10 進数(0..255)

◦ 16 進数(0x0..0xFF)

◦ ニーモニック文字列

unknown	0
rip	1
sap	4
spx	5
ncp	17
netbios	20

◦ 間に - をはさんだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。

◦ 上項目のカンマで区切った並び(5 個以内)

◦ * (すべての IPX パケットタイプ)

省略した時は一個の * と同じ

• *src_socket* ... 始点ソケット番号

◦ 10 進数(0..65535)

◦ 0x を先頭に持つ 4 桁以内の 16 進数

◦ プロトコルを表すニーモニック

ncp	0x0451
sap	0x0452
rip	0x0453
netbios	0x0455
diag	0x0456
serialization	0x0457

◦ 間に - をはさんだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。

◦ 上項目のカンマで区切った並び(5 個以内)

◦ * (すべてのソケット番号)

省略した時は一個の * と同じ

• *dst_socket* ... 終点ソケット番号　　src_socket と同じ形式。

ブリッジフィルタ

• *src_mac* ... 始点 MAC アドレス

◦ X:XX:XX:XX:XX:XX、XX は

⊳ 16 進数

⊳ *

◦ *(すべての MAC アドレスに対応)

• *dst_mac* ... 終点 MAC アドレス *src_mac* と同じ形式。省略した時は一個の * と同じ

• *offset* ... オフセットを表す 10 進数 (イーサネットフレームの始点 MAC アドレスの直後を 0 とするバイト数)

• byte list

◦ バイト列

⊳ XX(XX は 2 桁の 16 進数)

⊳ 上項目のカンマで区切った並び(16 個以内)

◦ *(すべてのバイト表現)

［説明］ クラス分けのためのフィルタを設定する。

パケットフィルタに該当したパケットは、指定したクラスに分類される。このコマンドで設定したフィルタを使用するかどうか、あるいはどのような順番で適用するかは、各インタフェースにおける **queue *interface* class filter list** コマンドで設定する。

18.3 キューイングアルゴリズムタイプの選択

［入力形式］

queue *interface* type *type*

no queue *interface* type [*type*]

［パラメータ］

• ***interface*** ... LAN インタフェース名、もしくは pp

• *type*

◦ fifo ... First In, First Out 形式のキューイング

◦ wfq ... Weighted Fair Queue 形式のキューイング

◦ priority ... 優先制御キューイング

◦ cbq ... 帯域制御キューイング

［説明］

指定したインタフェースに対して、キューイングアルゴリズムタイプを選択する。

fifo は最も基本的なキューである。fifo の場合、パケットは必ず先にルータに到着したものから送信される。パケットの順番が入れ替わることは無い。fifo キューにたまったパケットの数が **queue *interface* length** コマンドで指定した値を越えた場合、キューの再後尾、つまり最も最後に到着したパケットが破棄される。

LAN インタフェースのデフォルトは fifo である。

wfq は、送信待ちのパケットを始点・終点 IP アドレスやプロトコル、ポート番号でフローとしてグループ分けして、それぞれのフローで使用する帯域のバランスが取れるようにするキューイングアルゴリズムである。wfq を使用すると、TELNET のような、帯域はあまり必要としないが速い応答時間を必要とするプロトコルと、FTP のような応答時間よりも広い帯域を必要とするプロトコルを同時に利用した場合に、TELNET の応答時間の落ち込みを fifo に比べて軽減することができる。

wfq のもう一つの特徴は、設定がいらないということである。設定するところがないため、優先制御や帯域制御に比べて細かい調整はできないが、簡単にフロー間での帯域のバランスを図ることができる。

PP インタフェースのデフォルトは wfq である。

priority は優先制御を行う。**queue class filter** コマンドおよび **queue *interface* class filter list** コマンドでパケットをクラス分けし、送信待ちのパケットの中から最も優先順位の高いクラスのパケットを送信する。

cbq は帯域制御を行う。**queue *interface* class property** コマンドで各クラスに割り振る帯域をあらかじめ設定しておき、**queue class filter** コマンドおよび **queue *interface* class filter list** コマンドでクラス分けされたパケットが指定の帯域になるように送信する。

［デフォルト］

fifo (LAN インタフェース)

wfq (PP インタフェース)

18.4 デフォルトクラスの設定

［入力形式］ **queue *interface* default class** *class*

no queue *interface* default class [*class*]

［パラメータ］ • ***interface*** ... LAN インタフェース名、もしくは pp

• *class* ... クラス(1..16)

［説明］ インタフェースに対して、フィルタにマッチしないパケットをどのクラスに分類するかを指定する。

［デフォルト値］ 2

18.5 クラス分けフィルタの適用

［入力形式］ **queue *interface* class filter list** *filter_list*

no queue *interface* class filter list [*filter_list*]

［パラメータ］ • ***interface*** ... LAN インタフェース名、もしくは pp

• *filter_list*

◦空白で区切られたクラスフィルタの並び

［説明］ 指定した LAN インタフェースまたは選択されている PP に対して、**queue class filter** コマンドで設定したフィルタを適用する順番を設定する。フィルタにマッチしなかったパケットは、**queue *interface* default class** コマンドで指定したデフォルトクラスに分類される。

18.6 クラスの属性の設定

［入力形式］

queue *interface* class property *class* bandwidth=*bandwidth* [parent=*parent*] [borrow=*borrow*] [maxburst=*maxburst*] [minburst=*minburst*] [packetsize=*packetsize*]

no queue *interface* class property *class* [bandwidth=*bandwidth* ...]

［パラメータ］

• ***interface*** ... LAN インタフェース名、もしくは pp

• *class* ... クラス(1..16)

• *bandwidth*... クラスに割り当てる帯域(bit/s)

数値の後ろに 'k'、'M' をつけるとそれぞれ kbit/s、Mbit/s として扱われる。また、数値の後ろに '%' をつけると、回線全体の帯域に帯するパーセンテージとなる。

• *parent* ... 親クラスの番号(0 〜 16)

• *borrow* ... 帯域が足りなくなった時に親クラスから帯域を借りるか否か

  ◦ on ... 借りる

  ◦ off ... 借りない

• *maxburst* ... 連続送信できる最大パケット数(1..10000)

• *minburst* ... 安定送信中に連続送信できる最大パケット数(1..10000)

• *packetsize* ... クラスで流れるパケットの平均パケット長(1..10000)

［説明］

指定したクラスの属性を設定する。

［ノート］

bandwidth 属性は必ず指定されなければならない。回線全体の帯域は、**speed** コマンドで設定される。クラスに割り当てる帯域は、親クラス以下の値でなければいけない。

クラス番号 0 はルートクラスを表す。ルートクラスは仮想的なクラスで、常に 100% の帯域を持ち、デフォルトでは他のクラスの親クラスになっている。ルートクラスに直接パケットを割り振ることはできず、その帯域は他のクラスに貸し出すためにだけ割り当てられている。

帯域が足りなくなった時に、親クラスから帯域を借りてくる(borrow=on)と設定すると、このクラスの最大速度は親クラスの最大速度まで増えることができる。通常は 100% の帯域を持つルートクラスを親クラスとするので、クラスの帯域は回線速度一杯に広がることができる。この場合、bandwidth の設定は、回線が混雑している時に他のクラスとどの程度の割り合いで帯域をわけるかの目安として使われる。

帯域を借りてこない設定(borrow=off)だと、このクラスの最大速度は bandwidth の値になり、それ以上の帯域を使わなくなる。特定のトラフィックの帯域を制限したい場合に有効である。

このコマンドが設定されていないクラスには、100% の帯域が割り振られている。そのため、優先制御の設定をする場合には最低限でも対象としているクラスと、デフォルトクラスの 2 つに関してこのコマンドを設定しなくてはいけない。デフォルトクラスの設定を忘れると、デフォルトクラスに 100% の帯域が割り振られるため、対象とするクラスは常にデフォルトクラスより狭い帯域を割り当てられることになる。

［デフォルト値］

parent = 0

borrow = on

maxburst = 20

minburst = *maxburst* / 10

packetsize = 512

18.7 クラス毎のキュー長の設定

［入力形式］ **queue *interface* length** *len1* [*len2 ... len16*]

no queue *interface* length [*len1* [*len2 ... len16*]]

［パラメータ］ • *len1* 〜 *len16 ...* クラス 1 からクラス 16 のキュー長

［説明］ インタフェースに対して、指定したクラスのキューに入ることのできるパケットの個数を指定する。設定を省略したクラスに関しては、最後に指定されたキュー長が残りのクラスにも適用される。

［デフォルト値］ LAN インタフェース

RT300i は 200、その他の YAMAHA リモートルータは 40

PP は全機種共通で 20

18.8 MPインタリーブの設定

［入力形式］ **ppp mp interleave** [*delay*] *sw*

no ppp mp interleave [[*delay*] *sw*]

［パラメータ］ • *delay...* 遅延(ミリ秒)

• *sw*

◦ on... MP インタリーブを使用する

◦ off... MP インタリーブを使用しない

［説明］ MP インタリーブを使用するかどうかを設定する。DELAY では、優先されるプロトコルで許容できる最大遅延を設定する。パケットをどのような大きさに分割するかは、DELAY の値と回線速度により決定される。

［ノート］ • DELAY で設定した遅延が保証されるわけではない。

• データの受信側でも同じ設定をしておかないと、効果が発揮されない。

• 同時に圧縮は利用できない。圧縮を利用する設定の場合、この機能は無視されるので、以下の設定で圧縮を無効にしておく必要がある。

• ppp ccp type none

［デフォルト値］ *sw* = off

delay = 30

［設定例］

```
queue class filter 1 4 ip VOIP-GATEWAY * * * *
queue class filter 2 3 ip * * icmp * *
queue class filter 3 1 ip * * * * *
pp select 1
pp bind bri2.1
queue pp type priority
queue class filter list 1 2 3
isdn remote address call 03-123-4567
ppp mp use on
ppp mp interleave on
ppp mp maxlink 1
ppp ccp type none
pp enable 1
```

19. スケジュール

19.1 スケジュールの設定

［入力形式］

schedule at *id* [*date*] *time* * *command...*

schedule at *id* [*date*] *time* pp *peer_number command...*

schedule at *id* [*date*] *time* tunnel *tunnel_number command...*

no scudule at *id* [[*date*] ...]

［パラメータ］

• *id ...* スケジュール番号

• *date ...* 日付 (省略可)

◦月 / 日

◦省略した時は */* とみなす

月の指定例	意味
1,2	1 月と 2 月
2-	2 月から 12 月まで
2-7	2 月から 7 月まで
-7	1 月から 7 月まで
*	毎月

日の指定例	意味
1	1 日のみ
1,2	1 日と 2 日
2-	2 日から月末まで
2-7	2 日から 7 日まで
-7	1 日から 7 日まで
mon	月曜日のみ
sat,sun	土曜日と日曜日
mon-fri	月曜日から金曜日
-fri	日曜日から金曜日
*	毎日

• *time ...* 時刻

◦時(0..23 または *): 分(0..59 または *)

◦startup ... 起動時

• *peer number*

◦相手先情報番号

◦anonymous

◦ leased

• *tunnel_number ...* トンネルインタフェースの番号

• *command ...* 実行するコマンド(制限あり)

［説明］ *time* で指定した時刻に *command* で指定されたコマンドを実行する。

2、3 番目の形式で指定された時には、それぞれあらかじめ指定された相手先／トンネル番号での、**pp select** / **tunnel select** コマンドが発行済みであるように動作する。

schedule at コマンドは複数指定でき、同じ時刻に指定されたものは *id* の小さな順に実行される。

以下のコマンドは指定できない。

administrator、**administrator password**、**cold start**、**console** で始まるコマンド ,

date、**help**、**login password**、**login timer**、**ping**、**line type**、**quit**、**remote setup**、**save**、**show** で始まるコマンド、**time**、**timezone**、**traceroute**

［ノート］ 入力時、*command* パラメータに対して TAB キーによるコマンド補完は行うが、シンタックスエラーなどは実行時まで検出されない。**schedule at** コマンドにより指定されたコマンドを実行する時には、何を実行しようとしたかを INFO タイプの SYSLOG に出力する。

date に数字と曜日を混在させて指定はできない。

startup を指定したスケジュールはルータ起動時に実行される。電源を入れたらすぐ発信したい時などに便利。

［設定例］ 1. ウィークデイの 8:00 〜 17:00 だけ接続を許可する

```
# schedule at 1 */mon-fri 8:00 pp 1 isdn auto connect on
# schedule at 2 */mon-fri 17:00 pp 1 isdn auto connect off
# schedule at 3 */mon-fri 17:05 * disconnect 1
```

2. 毎時 0 分から 15 分間だけ接続を許可する

```
# schedule at 1 *:00 pp 1 isdn auto connect on
# schedule at 2 *:15 pp 1 isdn auto connect off
# schedule at 3 *:15 * disconnect 1
```

3. 今度の元旦にルーティングを切替える

```
# schedule at 1 1/1 0:0 * ip route NETWORK gateway pp 2
```

20. 操作

20.1 相手先情報番号の選択

［入力形式］ **pp select** *peer_number*

［パラメータ］
- *peer_number*
  - 相手先情報番号
  - none ... 相手を選択しない
  - anonymous ... ISDN 番号が不明である相手の設定
  - leased ... 専用線の設定 (1BRI モデルのみ)

［説明］ 設定や表示の対象となる相手先情報番号を選択する。以降プロンプトには、**console prompt** コマンドで設定した文字列と相手先情報番号が続けて表示される。

none を指定すると、プロンプトに相手先情報番号を表示しない。

［ノート］ この操作コマンドは一般ユーザでも実行できる。

20.2 設定に関する操作

20.2.1 管理ユーザへの移行

［入力形式］ **administrator**

［パラメータ］ なし

［説明］ このコマンドを発行してからでないと、ルータの設定は変更できない。また操作コマンドも実行できない。

コマンド入力後、管理パスワードを入力しなければならない。

20.2.2 終了

［入力形式］ **quit**

quit *save*

exit

exit *save*

［パラメータ］
- *save* ... 管理ユーザから抜ける時に *save* を指定すると、設定内容を不揮発性メモリに保存して終了する

［説明］ ルータへのログインを終了、または管理ユーザから抜ける。

設定を変更して保存せずに管理ユーザから抜けようとすると、新しい設定内容を保存するか否かを問い合わせる。

20.2.3 設定内容の保存

［入力形式］ **save** (RT300i 以外)

save [*filename* [*comment*]] (RT300i のみ)

［パラメータ］ • *filename* ... 設定を保存するファイル名

◦ 0 〜 9 ... 内蔵 Flash ROM の設定ファイル(0..9)

◦ ext0:FILENAME ... PCMCIA Flash ATA カードの設定ファイル

• *comment* ... 設定ファイルのコメント

［説明］ 現在の設定内容を不揮発性メモリに保存する。

本機では設定を保存するファイルを指定することができる。ファイルの指定を省略すると、起動時に使用した設定ファイルに保存する。

20.2.4 設定ファイルの一覧

［入力形式］ **show config list**

［パラメータ］ なし

［説明］ 内蔵 Flash ROM に保存されている設定ファイルの一覧を表示する。

RT300i でのみ動作するコマンドである。

20.2.5 設定の初期化

［入力形式］ **cold start**

［パラメータ］ なし

［説明］ 工場出荷時の設定に戻し、再起動する。

コマンド実行時に管理パスワードを入力する必要がある。

［ノート］ 本機では、内蔵 Flash ROM の設定ファイルがすべて削除される。

20.2.6 遠隔地のルータの設定

［入力形式］ **remote setup** *interface* [*isdn_number*[*/sub_address*]]

remote setup *interface* dlci=*dlci*

［パラメータ］ • *interface* ... BRI、PRI インタフェース名

• *isdn_number* ... ISDN 番号

• *sub_address* ... ISDN サブアドレス(0x21 から 0x7e の ASCII 文字)

• *dlci* ... フレームリレーの DLCI 番号

［説明］ 指定したインタフェースを利用して、遠隔地のルータの設定をする。インタフェースには BRI、PRI とも利用でき、また、ISDN、専用線、フレームリレーいずれの場合でも設定できる。

［ノート］ 遠隔地のルータが RTA50i もしくは RTA52i の場合、それにあらかじめパスワードが設定されていないと遠隔から **remote setup** コマンドを使って設定することはできない。

20.2.7 遠隔地のルータからの設定に対する制限

［入力形式］ **remote setup accept** *isdn_number*[*/sub_address*]
remote setup accept any
remote setup accept none
［パラメータ］ • *isdn number* ... ISDN 番号
• *sub_address* ... ISDN サブアドレス(0x21 から 0x7e の ASCII 文字)
• *isdn_number_list* ... ISDN 番号だけまたは ISDN 番号とサブアドレスを空白で区切った並び
• any ... すべての遠隔地のルータからの設定を許可する
• none ... すべての遠隔地のルータからの設定を拒否する
［説明］ 自分のルータの設定を許可する相手先を設定する。
［デフォルト値］ any

20.3 動的情報のクリア操作

20.3.1 ARPテーブルのクリア

［入力形式］ **clear arp**
［パラメータ］ なし
［説明］ ARP テーブルをクリアする。

20.3.2 IPの動的経路情報のクリア

［入力形式］ **clear ip dynamic routing**
［パラメータ］ なし
［説明］ 動的に設定された IP の経路情報をクリアする。

20.3.3 IPXの動的経路情報のクリア

［入力形式］ **clear ipx dynamic routing**
［パラメータ］ なし
［説明］ 動的に設定された IPX の経路情報をクリアする。

20.3.4 IPXの動的 SAP情報のクリア

［入力形式］ **clear ipx dynamic sap**
［パラメータ］ なし
［説明］ IPX SAP テーブル中、動的に得られた SAP 情報をクリアする。

20.3.5 ブリッジのラーニング情報のクリア

［入力形式］ **clear bridge learning**
［パラメータ］ なし
［説明］ 動的に受け取ったブリッジのラーニング情報をすべて消去する。
［ノート］ **bridge *interface* learning add** コマンドで設定したものは消去されない。

20.3.6 ログのクリア

［入力形式］ **clear log**

［パラメータ］ なし

［説明］ ログをクリアする。

20.3.7 アカウントのクリア

［入力形式］ **clear account**

clear account *wan_interface*

clear account pp [*peer_number*]

［パラメータ］ • *wan_interface* ... BRI、PRI インタフェース名

• *peer_number* ... 相手先情報番号、省略時は現在選択している相手先

［説明］ 指定したインタフェース (1 番目の書式ではすべての合計)に関するアカウントをクリアする。

20.3.8 InARPのクリア

［入力形式］ **clear inarp** [*peer_number*]

［パラメータ］ • *peer_number* ... 相手先情報番号、省略時は現在選択している相手先

［説明］ InARP で得られた相手 IP アドレスをクリアし、InARP が on なら再度 InARP を開始する。

20.3.9 DNSキャッシュのクリア

［入力形式］ **clear dns cache**

［パラメータ］ なし

［説明］ DNS リカーシブサーバで持っているキャッシュをクリアする。

20.3.10 PRIのステータス情報のクリア

［入力形式］ **clear pri status** *pri*

［パラメータ］ • *pri* ...PRI 番号(1)

［説明］ PRI のステータス情報をクリアする。

20.4 その他の操作

20.4.1 相手先の使用許可の設定

［入力形式］ **pp enable** *peer_number*

［パラメータ］ • *peer_number*

- 相手先情報番号
- anonymous
- leased (1BRI モデルのみ)

［説明］ 相手先を使用できる状態にする。

工場出荷時、すべての相手先は disable 状態なので、使用する時は必ずこのコマンドで enable 状態にしなければならない。

20.4.2 相手先の使用不許可の設定

［入力形式］ **pp disable** *peer_number*

［パラメータ］ • *peer_number*

- 相手先情報番号
- anonymous
- leased (1BRI モデルのみ)
- all

［説明］ 相手先を使用できない状態にする。

相手先の設定を行う時は disable 状態であることが望ましい。

20.4.3 再起動

［入力形式］ **restart**

［パラメータ］ なし

［説明］ ルータを再起動する。

20.4.4 インタフェースの再起動

［入力形式］ **interface reset** *interface*

［パラメータ］ • *interface* ... 物理インタフェース名

［説明］ 指定したインタフェースを再起動する。

LAN インタフェースでは、オートネゴシエーションする設定になっていればオートネゴシエーション手順が起動される。

BRI、PRI では、回線種別を **line type** コマンドで変更したら、このコマンドでインタフェースを再起動する必要がある。

［ノート］ **line type**、**pp bind**、経路情報など全ての設定を整えた後に実行する。対象とするインタフェースが bind されているすべての pp の通信を停止した状態で、また回線種別を変更する場合には回線を抜いた状態で実行すること。

20.4.5 発信

［入力形式］ **connect** *peer_number*

［パラメータ］
- *peer_number* ... 発信相手の相手先情報番号

［説明］ 手動で 発信する。

20.4.6 切断

［入力形式］ **disconnect** *peer_number*

［パラメータ］
- *peer_number*
  - 切断する相手先情報番号
  - all ... すべて
  - anonymous ... anonymous のすべて
  - anonymous1..anonymous16 ... 指定した anonymous

［説明］ 手動で切断する。

20.4.7 ping

［入力形式］ **ping** *host* [*count*]

［パラメータ］
- *host*
  - ip address ... ping をかけるホストの IP アドレス(xxx.xxx.xxx.xxx (xxx は 10 進数))
  - ping をかけるホストの名称
- *count*
  - 実行回数 (1..21474836)
  - infinity... Ctrl+C を入力するまで繰り返す

［説明］ ICMP Echo を指定したホストに送出し、ICMP Echo Reply が送られてくるのを待つ。送られてきたら、その旨表示する。コマンドが終了すると簡単な統計情報を表示する。

count パラメータを省略すると、相手からの応答があったかどうかだけを表示する。

20.4.8 traceroute

［入力形式］ **traceroute** *host* [noresolv]

［パラメータ］
- *host*
  - *ip_address* ... traceroute をかけるホストの IP アドレス(xxx.xxx.xxx.xxx (xxx は 10 進数))
  - traceroute をかけるホストの名称

［説明］ 指定したホストまでの経路を調べて表示する。キーワード noresolv を指定した場合には、DNS による解決を行わない。

20.4.9 リモートホストによる時計の設定

［入力形式］ **rdate** *host* [syslog]

［パラメータ］
- *host*
  - ip_address ... リモートホストの IP アドレス(xxx.xxx.xxx.xxx (xxx は 10 進数))
  - ホストの名称
- syslog ... 出力結果を SYSLOG へ出力することを表すキーワード

［説明］ ルータの時計を、パラメータで指定したホストの時間に合わせる。

［ノート］ YAMAHA リモートルータシリーズ及び、多くの UNIX コンピュータをリモートホストに指定できる。

syslog キーワードを指定した場合には、コマンドの出力結果を INFO レベルの SYSLOG へ出力する。

20.4.10 NTP による時計の設定

［入力形式］ **ntpdate** *ntp server* [syslog]

［パラメータ］
- *ntp_server*
  - ip_address ... NTP サーバの IP アドレス(xxx.xxx.xxx.xxx (xxx は 10 進数))
  - NTP サーバの名称
- syslog ... 出力結果を SYSLOG へ出力することを表すキーワード

［説明］ NTP を利用してルータの時計を設定する。

［ノート］ インターネットに接続している時には、**rdate** コマンドを使用した場合よりも精密な時計合わせが可能になる。NTP サーバとしてはできるだけ近くのものを指定した方が良い。利用可能な NTP サーバについてはプロバイダに問い合わせること。
本機自身は NTP サーバとはなれない。

syslog キーワードを指定した場合には、コマンドの出力結果を INFO レベルの SYSLOG へ出力する。

20.4.11 telnet

［入力形式］ **telnet** *host* [*port* [*mode* [*negotiation* [*abort*]]]]

［パラメータ］
- *host* ... TELNET をかける相手のホスト名、もしくは IP アドレス
- *port* ... 使用するポート番号
  - 10 進数
  - ポート番号のニーモニック
  - 省略時は 23　(TELNET)
- *mode* ... telnet 通信(送信) の動作モード
  - character ... 文字単位で通信する
  - line ... 行単位で通信する
  - auto ... port パラメータの設定値により charactor/line を選択
  - 省略時は auto
- *negotiation* ... telnet オプションのネゴシエーションの選択
  - on ... ネゴシエーションする
  - off ... ネゴシエーションしない
  - auto ... port パラメータの設定値により on/off を選択
  - 省略時は auto
- *abort* ... TELNET クライアントを強制的に終了させるためのアボートキー
  - 10 進数の ASCII コード
  - 省略時は 29(^])

［説明］ TELNET クライアントを実行する。

［ノート］ character モードは、通常の TELNET サーバなどへの接続のための透過的な通信を行う。

line モードは、入力行を編集して行単位の通信を行う。行編集の終了は、改行コード (CR:0x0d または LF:0x0a) の入力で判断する。

ポート番号による機能自動選択について。

1. telnet 通信の動作モードの自動選択

   port 番号が 23 の場合は文字単位モードとなり、そうでない場合は行単位モードとなる。

2. telnet オプションのネゴシエーションの自動選択

   port 番号が 23 の場合はネゴシエーションし、そうでない場合はネゴシエーションしない。

［デフォルト値］ *port* = 23

mode = auto

negotiation = auto

abort = 29

21. 設定の表示

21.1 機器設定の表示

21.1.1 機器設定の表示

［入力形式］ **show environment**

［パラメータ］ なし

［説明］ 以下の項目が表示される。

- システムのリビジョン
- CPU、メモリの使用量(%)
- 動作しているファームウェアファイルと起動時に使用した設定ファイルの名前 (RT300i のみ)
- 起動時刻、現在時刻、起動してから現在までの経過時間
- セキュリティクラス
- 電源、ファン、内部温度の状態 (RT300i のみ)

21.1.2 すべての設定内容の表示

［入力形式］ **show config**

less config

［パラメータ］ なし

［説明］ 設定されたすべての設定内容を表示する。

21.1.3 指定した PPの設定内容の表示

［入力形式］ **show config pp** [*peer_number*]

less config pp [*peer_number*]

［パラメータ］
- *peer number*
  - 相手先情報番号
  - anonymous
  - leased
- *peer_number* を省略した時は選択されている相手について表示する

［説明］ **show config** 、**less config** コマンドの表示の中から、指定した相手先情報番号に関するものだけを表示する。

22. 状態の表示

22.1 ARP テーブルの表示

［入力形式］ **show arp**

［パラメータ］ なし

［説明］ ARP テーブルを表示する。

22.2 インタフェースの状態の表示

［入力形式］ **show status** *interface*

［パラメータ］ • *interface* ... LAN、BRI、PRI のインタフェース名

［説明］ インタフェースの状態を表示する。

22.3 各相手先の状態の表示

［入力形式］ **show status pp** [*peer_number*]

［パラメータ］ • *peer_number*

- ◦相手先情報番号
- ◦anonymous
- ◦leased (1BRI モデルのみ)

• *peer_number* を省略した時は選択されている相手について表示する

［説明］ 各相手先の接続中または最後に接続された時の状態を表示する。

- 現在接続されているか否か
- 直前の呼の状態
- 接続 (切断) した日時
- 回線の種類
- 通信時間
- 切断理由
- 通信料金
- 相手とこちらの PP 側 IP アドレス
- 正常に送信したパケットの数
- 送信エラーの数と内分け
- 正常に受信したパケットの数
- 受信エラーの数と内分け
- PPP の状態
- CCP の状態
- その他

22.4 DHCPサーバの状態の表示

［入力形式］ **show status dhcp**

［パラメータ］ なし

［説明］ 各DHCP スコープのリース状況を表示する。以下の項目が表示される。

- DHCP スコープのリース状態
- DHCP スコープ番号
- ネットワークアドレス
- 割り当て中IP アドレス
- 割り当て中クライアントMAC アドレス
- リース残時間
- 予約済(未使用)IP アドレス
- DHCP スコープの全IP アドレス数
- 除外IP アドレス数
- 割り当て中IP アドレス数
- 利用可能アドレス数(うち予約済IP アドレス数

22.5 IPの経路情報テーブルの表示

［入力形式］ **show ip route** [*destination*]

［パラメータ］
- *destination* ... 相手先IP アドレス
- 省略した時は経路情報テーブル全体を表示する。

［説明］ IP の経路情報テーブルまたは相手先IP アドレスへのゲートウェイを表示する。
ネットマスクは設定時の表現に関わらず連続するビット数で表現される。
フレームリレーの場合はDLCI の値が表示される。

22.6 IPX の経路情報テーブルの表示

［入力形式］ **show ipx route**

［パラメータ］ なし

［説明］ IPX の経路情報テーブルを表示する。
フレームリレーの場合はDLCI の値が表示される。

22.7 SAPテーブルの表示

［入力形式］ **show ipx sap**

［パラメータ］ なし

［説明］ IPX SAP テーブルを表示する。

非 ASCII 文字は 8 進数で表示される。

22.8 IPXWANの状態の表示

［入力形式］ **show ipx ipxwan** [*peer_number*]

［パラメータ］ • *peer_number*

- 相手先情報番号
- anonymous
- leased

• *peer_number* を省略した時は選択されている相手先について表示する。

［説明］ IPXWAN の状態を表示する。

［ノート］ 複数 WAN ポートモデルでは leased を指定することはできない。

22.9 ブリッジのラーニング情報の表示

［入力形式］ **show bridge learning**

［パラメータ］ なし

［説明］ ブリッジの MAC アドレスのラーニング情報を表示する。

フレームリレーの場合は DLCI の値が表示される。

22.10 RIPで得られた経路情報の表示

［入力形式］ **show ip rip table**

［パラメータ］ なし

［説明］ RIP で得られた経路情報を表示する。

22.11 IPsecの SA の表示

［入力形式］ **show ipsec sa** [*id*]

［パラメータ］ • *id* ... SA の識別子

［説明］ IPsec の SA の状態を表示する。

id で与えられた識別子を持つ SA の情報を表示する。*id* を指定していない時は、すべての SA を表示する。

23. ロギング

23.1 ログの表示

［入力形式］ **show log**

less log

［パラメータ］ なし

［説明］ パワーオンからのログを表示する。

- パワーオンの日時
- 不揮発性メモリに設定を保存した日時
- 設定のためのログインの記録
- 接続した日時、発着
- 回線の種類
- 接続失敗の原因
- 切断した日時、接続時間、ISDN 料金

23.2 アカウントの表示

［入力形式］ **show account**

show account *interface*

show account pp [*peer_number*]

［パラメータ］
- *interface* ... BRI、PRI インタフェース名
- *peer_number*
  - 相手先情報番号
  - anonymous
  - leased (1BRI モデルのみ)

  peer number を省略した時は選択されている相手について表示する

［説明］ 以下の項目が表示される。

- 発信回数
- 着信回数
- ISDN 料金の総計

［ノート］ 電源 OFF や再起動により、それまでの課金情報がクリアされる .

課金額は通信の切断時に NTT から ISDN で通知される料金情報を集計しているため、割引サービスなどを利用している場合には、最終的に NTT から請求される料金とは異なる場合がある。また、NTT 以外の通信事業者を利用して通信した場合には料金情報は通知されないため、アカウントとしても集計されない。

24. OSPF

OSPFはインテリゲートウェイプロトコルの一種で、グラフ理論をベースとしたリンク状態型の動的ルーティングプロトコルである。

24.1 OSPFの有効設定

［入力形式］ **ospf configure refresh**

［パラメータ］ なし

［説明］ OSPF関係の設定を有効にする。OSPF関係の設定を変更したら、ルータを再起動するか、あるいはこのコマンドを実行しなくてはいけない。

24.2 OSPFの使用設定

［入力形式］ **ospf use** *sw*

no ospf use [*sw*]

［パラメータ］ • *sw*

◦ on ... OSPF を使用する

◦ off ... OSPF を使用しない

［説明］ OSPF を使用するかどうかを設定する。

［デフォルト値］ off

24.3 OSPFによる経路の優先度設定

［入力形式］ **ospf preference** *preference*

no ospf preference [*preference*]

［パラメータ］ • *preference* ... OSPF による経路の優先度を表す 1 以上の数値

［説明］ OSPFによる経路の優先度を設定する。優先度は1以上の数値で表され、数字が大きい程優先度が高い。OSPFとRIPなど複数のプロトコルで得られた経路が食い違う場合には、優先度が高い方が採用される。優先度が同じ場合には時間的に先に採用された経路が有効となる。

［ノート］ 静的経路の優先度は 10000 で固定である。

［デフォルト値］ 2000

24.4 OSPFのルータ ID 設定

［入力形式］ **ospf router id** *router-id*

no ospf router id [*router-id*]

［パラメータ］ • *router_id* ... IP アドレス

［説明］ OSPF のルータ ID を指定する。

［デフォルト値］ LANインタフェースの中でインタフェースの若いものから順にサーチして、プライマリIP アドレスがついているインタフェースの IP アドレスをルータ ID とする。

24.5 外部プロトコルによる経路導入

［入力形式］

ospf import from *protocol* [filter *fnum*...]

no ospf import from [*protocol* [filter *fnum*...]]

［パラメータ］

• *protocol* ... OSPF の経路テーブルに導入する外部プロトコル

◦ static ... 静的経路

◦ rip ... RIP

• *fnum* ... フィルタ番号

［説明］

OSPF の経路テーブルに外部プロトコルによる経路を導入するかどうかを設定する。導入された経路は外部経路として他の OSPF ルータに広告される。

fnum は **ospf import filter** コマンドで定義したフィルタ番号を指定する。外部プロトコルから導入されようとする経路は指定したフィルタにより検査され、フィルタに該当すればその経路は OSPF に導入される。該当するフィルタがない経路は導入されない。また、キーワード filter 以降を省略した場合には、すべての経路が OSPF に導入される。

経路を広告する時のパラメータであるメトリック値、メトリックタイプ、タグは、フィルタの検査で該当した **ospf import filter** コマンドで指定されたものを使う。キーワード filter 以降を省略した場合には、以下のパラメータを使用する。

• metric = 1
• type = 2
• tag = 1

［デフォルト値］

外部経路は導入しない。

24.6 外部経路導入に適用するフィルタ定義

［入力形式］

ospf import filter *fnum* [not] *kind ip-address/mask*...[*parameter*...]

no ospf import filter *fnum* [[not] *kind ip-address/mask*...[*parameter*...]]

［パラメータ］

• *fnum* ... フィルタ番号

• *kind* ... フィルタ種別

◦ include ... 指定したネットワークアドレスに含まれる経路
ネットワークアドレス自身を含む

◦ refines ... 指定したネットワークアドレスに含まれる経路
ネットワークアドレス自身は含まない

◦ equal ... 指定したネットワークアドレスに一致する経路

• *ip-address/mask* ... ネットワークアドレスをあらわす IP アドレスとマスク長

• *parameter*... 外部経路を広告する時のパラメータで以下の種類がある

◦ metric... メトリック値 (0..16777215)

◦ type... メトリックタイプ (1, 2)

◦ tag... タグの値 (0..4294967295)

［説明］

OSPF の経路テーブルに外部経路を導入する際に適用するフィルタを定義する。このコマンドで定義したフィルタは、**ospf import from** コマンドの filter 節で指定されてはじめて効果を持つ。
ip-address/mask では、ネットワークアドレスを設定する。これは、複数設定でき、経路の検査時にはそれぞれのネットワークアドレスに対して検査を行い、一つでも該当するものがあればそれが適用される。

kind では、経路の検査方法を設定する。

• include ... ネットワークアドレスと一致する経路および、ネットワークアドレスに含まれる経路が該当となる。

• refines ... ネットワークアドレスに含まれる経路が該当となるが、ネットワークアドレスと一致する経路が含まれない。

• equal ... ネットワークアドレスに一致する経路だけが該当となる。

kind の前にキーワード not を置くと、該当 / 非該当の判断が反転する。例えば、not equal では、ネットワークアドレスに一致しない経路が該当となる。

parameter では、該当した経路を OSPF の外部経路として広告する時のパラメータとして、メトリック値、メトリックタイプ、タグがそれぞれ metric、type、tag により指定できる。これらを省略した時には、以下の値が採用される。

• metric = 1

• type = 2

• tag = 1

24.7 OSPFエリア設定

［入力形式］ **ospf area** *area* [auth=*auth*] [stub [cost=*cost*]]

no ospf area *area* [auth=*auth*] [stub [cost=*cost*]]

［パラメータ］ • *area*

◦ バックボーンエリア (1 以上の数値)

◦ 非バックボーンエリア ... IP アドレス表記 (0.0.0.0 は不可)

• *auth* ... 認証を行う

◦ text ... プレーンテキスト認証

◦ md5 ... MD5 認証

• *cost* ... 0 以上の数値

［説明］ OSPF エリアを設定する。

stub [cost=*cost*]

スタブエリアであることを指定する。*cost* は 0 以上の数値で、エリアボーダルータがエリア内に広告するデフォルト経路のコストとして使われる。COST を指定しないとデフォルト経路の広告は行われない。

［デフォルト値］ 認証は行わない。スタブエリアではない。

24.8 エリアへの経路広告

［入力形式］ **ospf area network** *area network*/*mask* [restrict]

no ospf area network *area network*/*mask* [restrict]

［パラメータ］ • *area*

◦ バックボーンエリア (1 以上の数値)

◦ 非バックボーンエリア ... IP アドレス表記 (0.0.0.0 は不可)

• *network* ... IP アドレス

• *mask* ... ネットマスク長

［説明］ エリア境界ルータが他のエリアに経路を広告する時に、このコマンドで指定したネットワークの範囲内の経路は 単一のネットワーク経路として広告する。キーワード restrictが指定された時には、範囲内の経路は要約した経路も広告しない。

24.9 スタブ的接続の広告

［入力形式］ **ospf area stubhost** *area host* [cost *cost*]

no ospf area stubhost *area host*

［パラメータ］ • *area*

◦ バックボーンエリア (1 以上の数値)

◦ 非バックボーンエリア ... IP アドレス表記 (0.0.0.0 は不可)

• *host* ... IP アドレス

• *cost* ... 1 以上の数値

［説明］ 指定したホストが指定したコストでスタブ的に接続されていることを エリア内に広告する。

24.10 仮想リンク設定

［入力形式］

ospf virtual-link *router_id area* [*parameters...*]

no ospf virtual-link *router_id* [*router_id* [*parameters...*]]

［パラメータ］

• *router_id* ... 仮想リンクの相手のルータ ID

• *area*

◦非バックボーンエリア (1 以上の数値)

◦IP アドレス表記 (0.0.0.0 は不可)

• *parameters* ... *name=value* の列

［説明］

仮想リンクを設定する。仮想リンクは*router_id*で指定したルータに対して、*area*で指定したエリアを経由して設定される。*parameters* では、仮想リンクのパラメータが設定できる。パラメータは*name=value*の形で指定され、以下の種類がある。

name	*value*	説明
retransimit-interval	秒数	LSA を連続して送る時の再送間隔を秒単位で設定する。
transmit-delay	秒数	リンクの状態が変わってから LSA を送信するまでの時間を秒単位で設定する。
hello-interval	秒数	HELLO パケットの送信間隔を秒単位で設定する。
dead-interval	秒数	相手から HELLO を受け取れない時に、相手がダウンしたと判断するまでの 時間を秒単位で設定する。
authkey	文字列	プレーンテキスト認証の認証鍵を表す文字列を設定する。KEY は文字列で、8 文字以内。
md5key	*ID*, 文字列	MD5 認証の認証鍵を表す ID と鍵文字列を設定する。ID は 10 進数で 0 〜 255、KEY は文字列で 16 文字以内。MD5 認証鍵は 2 つまで設定できる。 複数の MD5 認証鍵が設定されている場合には、送信パケットは同じ内容のパケットを複数個、それぞれの鍵による認証データを付加して送信する。受信時には鍵 ID が一致する鍵が比較対象となる。

［ノート］

hello-interval/dead-interval について

hello-interval/dead-interval の値は、そのインタフェースから直接通信できるすべての近隣ルータとの間で同じ値でなくてはいけない。これらのパラメータの値が設定値とは異なっている OSPF HELLO パケットを受信した場合には、それは無視される。

MD5 認証鍵について

MD5 認証鍵を複数設定できる機能は、MD5 認証鍵を円滑に変更するためである。

通常の運用では、MD5 認証鍵は 1 つだけ設定しておく。MD5 認証鍵を変更する時は、まず 1 つのルータで新旧の MD5 認証鍵を 2 つ設定し、その後、近隣ルータで MD5 認証鍵を新しいものに変更していく。そして、最後に 2 つの鍵を設定したルータで古い鍵を削除すれば良い。

［デフォルト値］

NEIGHBOR??,*area* = なし

retransimit-interval = 5 秒

transmit-delay = 1 秒

hello-interval = 10 秒

dead-interval = 40 秒

authkey = なし

md5key = なし

24.11　指定インタフェースのOSPFエリア設定

［入力形式］

ip *interface* ospf area *area* [*parameters...*]

no ip *interface* ospf area [*area* [*parameters...*]]

［パラメータ］

- ***interface*** ... インタフェース名
  - lan*N*
  - pp
- *area*
  - バックボーンエリア
  - 非バックボーンエリア (1 以上の数値)
  - IP アドレス表記 (0.0.0.0 は不可)
- *parameters* ... *name=value* の列

［説明］

指定したインタフェースの属する OSPF エリアを設定する。
パラメータ *name* の type はインタフェースのネットワークがどのようなタイプであるかを設定する。*parameters* では、リンクパラメータを設定する。パラメータは *name=value* の形で指定され、以下の種類がある。

name	*value*	説明
type	broadcast	ブロードキャスト
	point-to-point	ポイント・ポイント
	point-to-multipoint	ポイント・マルチポイント
	non-broadcast	NBMA
	passive	インタフェースに対して、OSPF パケットを送信しない。該当インタフェースに他のOSPFルータがいない場合に設定する。
cost	コスト	インタフェースのコストを設定する。デフォルト値は、インタフェースの種類と回線速度によって決定される。LAN インタフェースの場合は1、PP インタフェースの場合は、バインドされている回線の回線速度を S[kbit/s]とすると、以下の計算式で決定される。例えば、64kbit/s の場合は 1562、1.536Mbit/s の場合には 65 となる。 • COST = 100000 / S
priority	優先度	指定ルータの選択の際の優先度を設定する。PRIORITY 値が大きいルータが指定ルータに選ばれる。0 を設定すると、指定ルータに選ばれなくなる。
retransimit-interval	秒数	LSA を連続して送る時の再送間隔を秒単位で設定する。
transmit-delay	秒数	リンクの状態が変わってから LSA を送信するまでの時間を秒単位で設定する。
hello-interval	秒数	HELLO パケットの送信間隔を秒単位で設定する。
dead-interval	秒数	近隣ルータから HELLO を受け取れない時に、近隣ルータがダウンしたと判断するまでの時間を秒単位で設定する。
poll-interval	秒数	非ブロードキャストリンクでのみ有効なパラメータで、近隣ルータがダウンしている時の HELLOパケットの送信間隔を秒単位で設定する。

authkey	文字列	プレーンテキスト認証の認証鍵を表す文字列を設定する。KEY は文字列で、8 文字以内。
md5key	*ID*, 文字列	MD5 認証の認証鍵を表す ID と鍵文字列を設定する。ID は 10 進数で 0 〜 255、KEY は文字列で 16 文字以内。MD5 認証鍵は 2 つまで設定できる。 複数の MD5 認証鍵が設定されている場合には、送信パケットは同じ内容のパケットを複数個、それぞれの鍵による認証データを付加して送信する。受信時には鍵IDが一致する鍵が比較対象となる。

［ノート］

• パラメータ *name* の type について

パラメータ *name* の type として、LAN インタフェースは broadcast のみが許される。PP インタフェースは、PPP を利用する時は point-to-point、FR を利用する時は point-to-multipoint と non-broadcast のいずれかが設定できる。

FR で non-broadcast (NBMA)を利用する時には、FR の各拠点間のすべての間で PVC が設定されており、FR に接続された各ルータは他のルータと直接通信できるような状態、すなわちフルメッシュになっていなくてはならない。また、non-broadcast では近隣ルータを自動的に認識することができないため、すべての近隣ルータを **ip pp ospf neighbor** コマンドで設定する必要がある。

point-to-multipoint を利用する場合には、FR の PVC はフルメッシュである必要はなく、一部が欠けたパーシャルメッシュでも利用できる。近隣ルータは InArp を利用して自動的に認識するため、InArp が必須となる。RT では InArp を使うかどうかは **fr inarp** コマンドで制御できるが、デフォルトでは InArp を使用する設定になっているので、**ip pp address** コマンドでインタフェースに適切な IP アドレスを与えるだけでよい。

point-to-multipoint と設定されたインタフェースでは、**ip pp ospfneighbor** コマンドの設定は無視される。

point-to-multipoint の方が non-broadcast よりもネットワークの制約が少なく、また設定も簡単だが、その代わりに回線を流れるトラフィックは大きくなる。non-broadcast では、broadcast と同じように指定ルータが選定され、HELLO などの OSPF トラフィックは各ルータと指定ルータの間だけに限定されるが、point-to-multipoint ではすべての通信可能なルータペアの間に point-to-point リンクがあるという考え方なので、OSPF トラフィックもすべての通信可能なルータペアの間でやりとりされる。

• passive について

passive は、インタフェースが接続しているネットワークに他の OSPF ルータが存在しない時に指定する。passive を指定しておくと、インタフェースから OSPF パケットを送信しなくなるので、無駄なトラフィックを抑制したり、受信側で誤動作の原因になるのを防ぐことができる。

LAN インタフェース(type=broadcast であるインタフェース)の場合には、インタフェースが接続しているネットワークへの経路は、**ip *interface* ospf area** コマンドを設定していないと他の OSPF ルータに広告されない。そのため、OSPF を利用しないネットワークに接続する LAN インタフェースに対しては、passive を付けた **ip *interface* ospf area** コマンドを設定しておくことでそのネットワークでは OSPF を利用しないまま、そこへの経路を他の OSPF ルータに広告することができる。

PP インタフェースに対して **ip *interface* ospf area** コマンドを設定していない場合は、インタフェースが接続するネットワークへの経路は外部経路として扱われる。外部経路なので、他の OSPF ルータに広告するには ospf import コマンドの設定が必要である。

• hello-interval/dead-interva **について**

hello-interval/dead-interval の値は、そのインタフェースから直接通信できるすべての近隣ルータとの間で同じ値でなくてはいけない。これらのパラメータの値が設定値とは異なっている OSPF HELLO パケットを受信した場合には、それは無視される。

• MD5 認証鍵について

MD5 認証鍵を複数設定できる機能は、MD5 認証鍵を円滑に変更するためである。

通常の運用では、MD5 認証鍵は 1 つだけ設定しておく。MD5 認証鍵を変更する時は、まず 1 つのルータで新旧の MD5 認証鍵を 2 つ設定し、その後、近隣ルータで MD5 認証鍵を新しいものに変更していく。そして、最後に 2 つの鍵を設定したルータで古い鍵を削除すれば良い。

［デフォルト値］

area = インタフェースは OSPF エリアに属していない
type = broadcast (LAN インタフェース設定時)
= point-to-point (PP インタフェース設定時)
passive = インタフェースは passive ではない
cost = 1 (lan 設定時)、pp は回線速度に依存
priority = 1
retransimit-interval = 5 秒
transmit-delay = 1 秒
hello-interval = 10 秒 (type = broadcast 設定時)
= 10 秒 (point-to-point 設定時)
= 30 秒 (non-broadcast 設定時)
= 30 秒 (point-to-multipoint 設定時)
dead-interval = hello-interval の 4 倍
poll-interval = 120 秒
authkey = なし
md5key = なし

24.12 非ブロードキャスト型ネットワークに接続されている OSPFルータの指定

［入力形式］ **ip *interface* ospf neighbor** *ip-address* [eligible]

no ip *interface* ospf neighbor *ip-address* [eligible]

［パラメータ］ • *interface* ... インタフェース名

- lan*N*
- pp

• *ip-address* ... 近隣ルータの IP アドレス

［説明］ 非ブロードキャスト型のネットワークに接続されているOSPFルータを指定する。キーワード eligible が指定されたルータは指定ルータとして適格であることを表す。

24.13 OSPF情報の表示

［入力形式］ **show status ospf** *info*

［パラメータ］ • *info* ... 表示する情報の種類

- database ... OSPF のデータベース
- neighbor ... 近隣ルータ
- interface ... 各インタフェースの状態
- virtual-link ... バーチャルリンクの状態

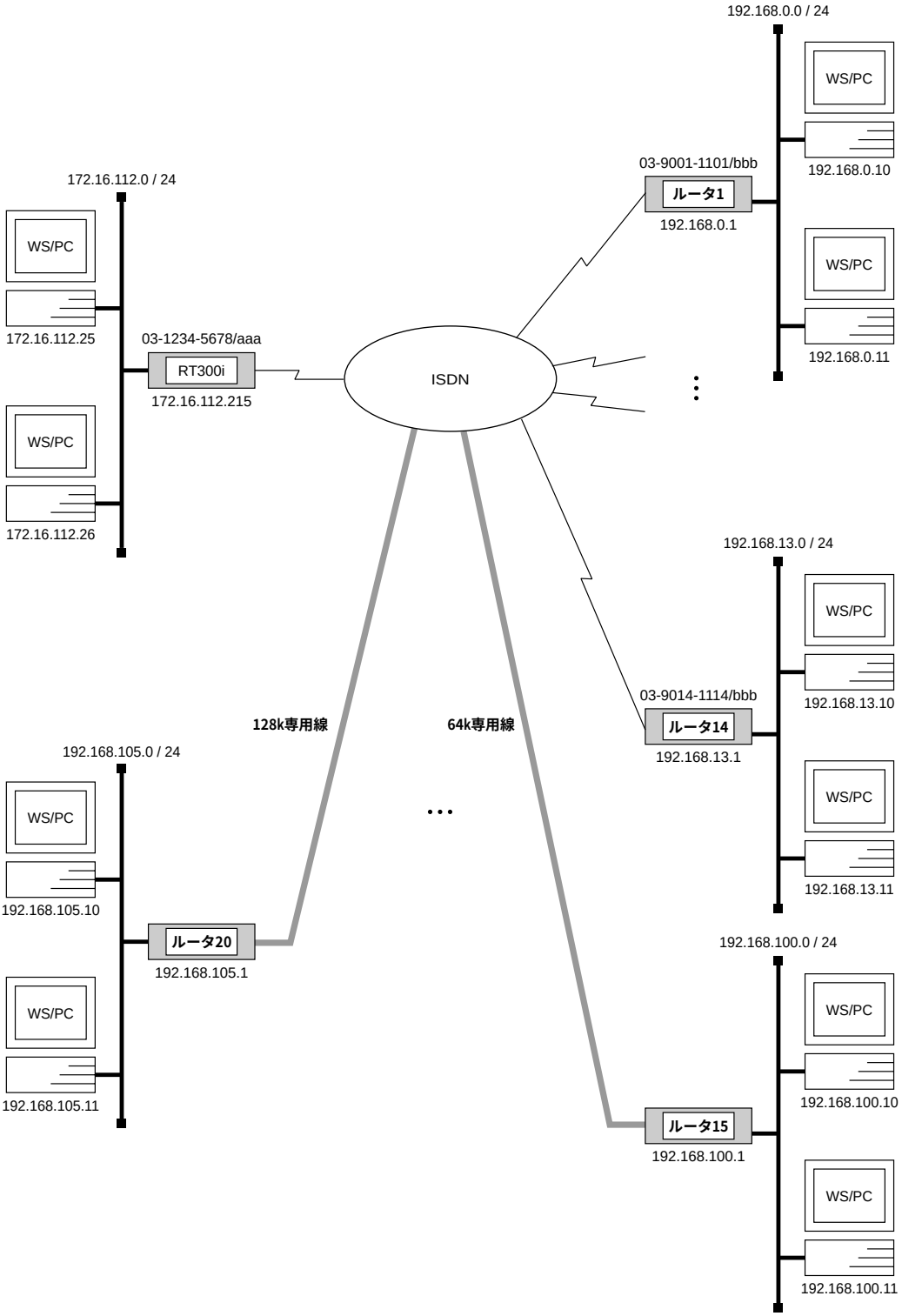
［説明］ OSPF の各種情報を表示する。

25. 設定例

本章で示す設定例は、本機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たものです。インストールの方法、注意事項は別冊の取扱説明書を参照してください。また、コマンドの詳細は前節を参照してください。

25.1 ISDN回線と専用線で 20 ヶ所の LAN を接続

[構成図]



[構成例]

ルータ	ネットワークアドレス	回線種別	ISDN 番号	ISDN サブアドレス
RT300i	172.16.112.0/24	ISDN/ 64k 専用線 / 128k 専用線	03-123-4567	aaa
ルータ 1	192.168.0.0/24	ISDN	03-9001-1101	bbb
ルータ 2	192.168.1.0/24	ISDN	03-9002-1102	bbb
ルータ 3	192.168.2.0/24	ISDN	03-9003-1103	bbb
ルータ 4	192.168.3.0/24	ISDN	03-9004-1104	bbb
ルータ 5	192.168.4.0/24	ISDN	03-9005-1105	bbb
ルータ 6	192.168.5.0/24	ISDN	03-9006-1106	bbb
ルータ 7	192.168.6.0/24	ISDN	03-9007-1107	bbb
ルータ 8	192.168.7.0/24	ISDN	03-9008-1108	bbb
ルータ 9	192.168.8.0/24	ISDN	03-9009-1109	bbb
ルータ 10	192.168.9.0/24	ISDN	03-9010-1110	bbb
ルータ 11	192.168.10.0/24	ISDN	03-9011-1111	bbb
ルータ 12	192.168.11.0/24	ISDN	03-9012-1112	bbb
ルータ 13	192.168.12.0/24	ISDN	03-9013-1113	bbb
ルータ 14	192.168.13.0/24	ISDN	03-9014-1114	bbb
ルータ 15	192.168.100.0/24	64k 専用線		
ルータ 16	192.168.101.0/24	64k 専用線		
ルータ 17	192.168.102.0/24	64k 専用線		
ルータ 18	192.168.103.0/24	64k 専用線		
ルータ 19	192.168.104.0/24	128k 専用線		
ルータ 20	192.168.105.0/24	128k 専用線		

[RT300i の設定手順]

```
# line type bri2.8 l64
# line type bri3.1 l64
# line type bri3.2 l64
# line type bri3.3 l64
# line type bri3.4 l128
# line type bri3.5 l128
# isdn local address bri2.1 03-1234-5678/aaa
# isdn local address bri2.2 03-1234-5678/aaa
# isdn local address bri2.3 03-1234-5678/aaa
# isdn local address bri2.4 03-1234-5678/aaa
# isdn local address bri2.5 03-1234-5678/aaa
# isdn local address bri2.6 03-1234-5678/aaa
# isdn local address bri2.7 03-1234-5678/aaa
# ip lan1 address 172.16.112.215/24
# rip use on
# ip route 192.168.0.0/24 gateway pp 1
# ip route 192.168.1.0/24 gateway pp 2
# ip route 192.168.2.0/24 gateway pp 3
# ip route 192.168.3.0/24 gateway pp 4
# ip route 192.168.4.0/24 gateway pp 5
# ip route 192.168.5.0/24 gateway pp 6
# ip route 192.168.6.0/24 gateway pp 7
# ip route 192.168.7.0/24 gateway pp 8
# ip route 192.168.8.0/24 gateway pp 9
# ip route 192.168.9.0/24 gateway pp 10
# ip route 192.168.10.0/24 gateway pp 11
# ip route 192.168.11.0/24 gateway pp 12
# ip route 192.168.12.0/24 gateway pp 13
# ip route 192.168.13.0/24 gateway pp 14
# ip route 192.168.100.0/24 gateway pp 15
# ip route 192.168.101.0/24 gateway pp 16
# ip route 192.168.102.0/24 gateway pp 17
# ip route 192.168.103.0/24 gateway pp 18
# ip route 192.168.104.0/24 gateway pp 19
# ip route 192.168.105.0/24 gateway pp 20
# pp select 1
pp1# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp1# isdn remote address call 03-9001-1101/bbb
pp1# pp enable 1
pp1# pp select 2
pp2# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp2# isdn remote address call 03-9002-1102/bbb
pp2# pp enable 2
pp2# pp select 3
pp3# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp3# isdn remote address call 03-9003-1103/bbb
pp3# pp enable 3
pp3# pp select 4
```

```
pp4# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp4# isdn remote address call 03-9004-1104/bbb
pp4# pp enable 4
pp4# pp select 5
pp5# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp5# isdn remote address call 03-9005-1105/bbb
pp5# pp enable 5
pp5# pp select 6
pp6# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp6# isdn remote address call 03-9006-1106/bbb
pp6# pp enable 6
pp6# pp select 7
pp7# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp7# isdn remote address call 03-9007-1107/bbb
pp7# pp enable 7
pp7# pp select 8
pp8# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp8# isdn remote address call 03-9008-1108/bbb
pp8# pp enable 8
pp8# pp select 9
pp9# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp9# isdn remote address call 03-9009-1109/bbb
pp9# pp enable 9
pp9# pp select 10
pp10# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp10# isdn remote address call 03-9010-1110/bbb
pp10# pp enable 10
pp10# pp select 11
pp11# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp11# isdn remote address call 03-9011-1111/bbb
pp11# pp enable 11
pp11# pp select 12
pp12# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp12# isdn remote address call 03-9012-1112/bbb
pp12# pp enable 12
pp12# pp select 13
pp13# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp13# isdn remote address call 03-9013-1113/bbb
pp13# pp enable 13
pp13# pp select 14
pp14# pp bind bri2.1 bri2.2 bri2.3 bri2.4 bri2.5 bri2.6 bri2.7
pp14# isdn remote address call 03-9014-1114/bbb
pp14# pp enable 14
pp14# pp select 15
pp15# pp bind bri2.8
pp15# pp enable 15
pp15# pp select 16
```

```
pp16# pp bind bri3.1
pp16# pp enable 16
pp16# pp select 17
pp17# pp bind bri3.2
pp17# pp enable 17
pp17# pp select 18
pp18# pp bind bri3.3
pp18# pp enable 18
pp18# pp select 19
pp19# pp bind bri3.4
pp19# pp enable 19
pp19# pp select 20
pp20# pp bind bri3.5
pp20# pp enable 20
pp20# save
pp20# interface reset bri2.8
pp20# interface reset bri3.1
pp20# interface reset bri3.2
pp20# interface reset bri3.3
pp20# interface reset bri3.4
pp20# interface reset bri3.5
```

[解説]

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

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

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

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

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

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

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

4. **rip use** コマンドを使って rip を有効にします。

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

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

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

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

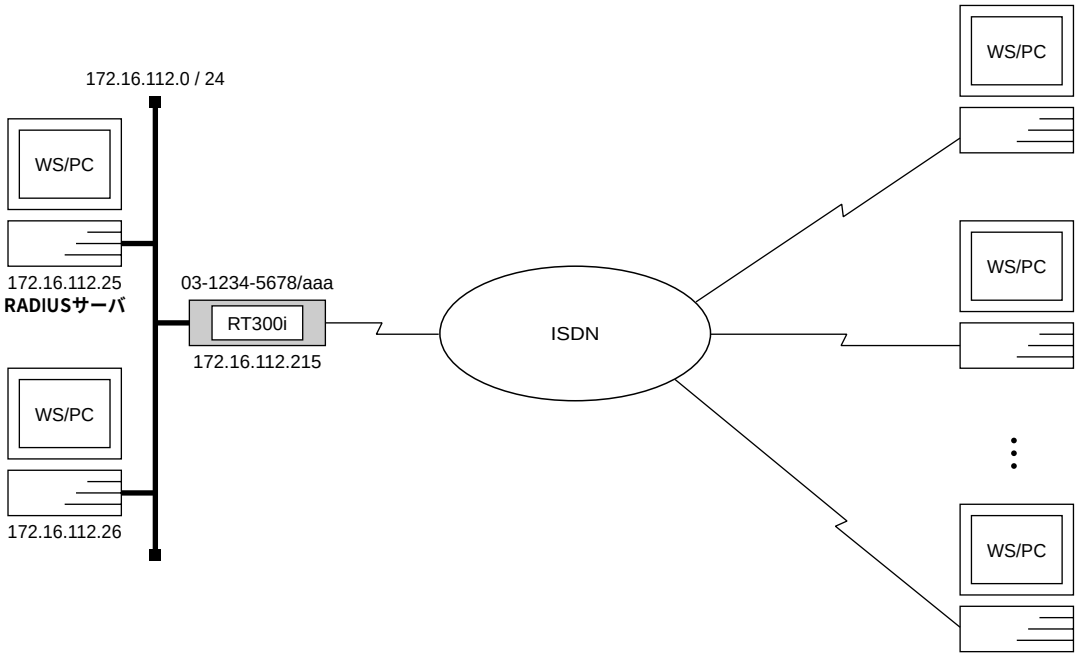
9. **pp enable** コマンドを使って PP 側のインタフェースを有効にします。このコマンドの実行直後にインターフェースは有効になります。

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

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

25.2 PRIモジュールを用いたダイヤルアップ接続(RADIUSによる認証)

[構成図]



[RT300i の設定手順]

```
# line type pri1 isdn
# isdn local address pri1 03-1234-5678/aaa
# ip lan1 address 172.16.112.215/24
# radius auth on
# radius server 172.16.112.25
# radius secret himitsu
# pp select anonymous
anonymous# pp bind pri1
anonymous# pp auth request chap
anonymous# pp enable anonymous
anonymous# save
anonymous# interface reset pri1
```

[解説]

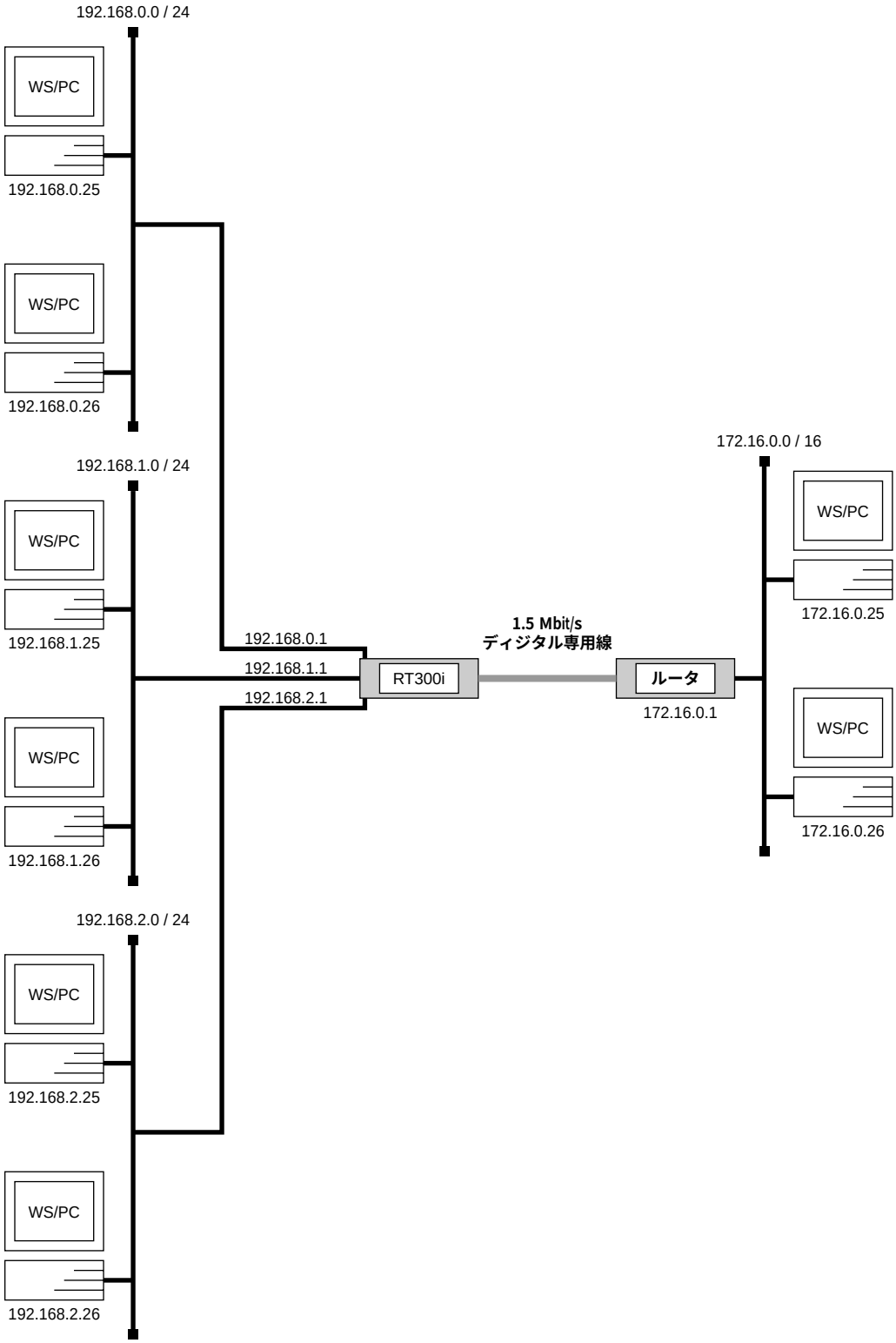
本機の拡張スロット1に装着した多重化対応のPRI拡張モジュール(YBA-1PRI-M)とINSネット1500を用いて、不特定のTAやPHS端末などからのダイヤルアップ接続を受けます。

ユーザの認証、端末側のIPアドレスの管理などはRADIUSサーバで行います。

1. **line type** コマンドを使ってpri1の回線種別をisdnに設定します。
2. **isdn local address** コマンドを使って本機のISDN番号を設定します。aaaはサブアドレスです。
3. **ip lan1 address** コマンドを使ってLAN側のIPアドレスとネットマスクを設定します。
4. **radius auth** コマンドを使ってanonymousのユーザの情報をRADIUSサーバに問い合わせるようにします。
5. **radius server** コマンドを使ってRADIUSサーバのIPアドレスを指定します。
6. **radius secret** コマンドを使ってRADIUSシークレットを設定します。
6. **pp select** コマンドを使って相手先にanonymousを選択します。
7. **pp bind** コマンドを使って選択した相手先情報番号にPRIポートをバインドします。
8. **pp auth request** コマンドを使ってPPPの認証にCHAPを使用するように設定します。
9. **pp enable** コマンドを使ってPP側のインタフェースを有効にします。このコマンドの実行直後にインターフェースは有効になります。
10. **save** コマンドを使って設定を内蔵の不揮発性メモリに書き込みます。
11. **interface reset** コマンドを使って回線種別の変更されたポートをリセットします。**restart** コマンドを使って、ルータを再起動させても回線種別は切り替わります。

25.3 3 つの LAN と遠隔地の LAN を 1.5Mbit/s ディジタル専用線で接続

[構成図]



[RT300i の設定手順]

```
# pri leased channel 1/1 1 24
# ip lan1 address 192.168.0.1/24
# ip lan2 address 192.168.1.1/24
# ip lan3 address 192.168.2.1/24
# ip route 172.16.0.0/16  gateway pp 1
# pp select 1
pp1# pp bind pri1/1
pp1# pp enable 1
pp1# save
pp1# interface reset pri1
```

[解説]

2 枚の LAN 拡張モジュール (YBA-1ETH-TX)と PRI 拡張モジュール (YBA-1PRI-N)を装着し、3 つのローカルセグメントと遠隔地の LAN を接続します。

1. **pri leased channel** コマンドを使って PRI の情報チャネルとタイムスロットを設定します。

2. **ip lan1 address**、**ip lan2 address** コマンド、**ip lan3 address** コマンドを使って、メインボード、本機の拡張スロットに装着されたモジュール上の LAN の IP アドレスを設定します。

3. **ip route** コマンドを使って遠隔地の LAN への経路情報を設定します。

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

5. **pp bind** コマンドを使って選択した相手先情報番号に PRI 情報チャネルをバインドします。

6. **pp enable** コマンドを使って PP 側のインタフェースを有効にします。

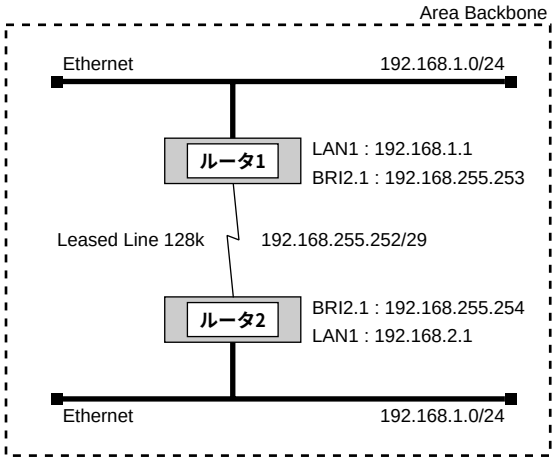
7. **save** コマンドを使って設定を内蔵の不揮発性メモリに書き込みます。

8. **interface reset** コマンドを使って PRI の情報チャネルとタイムスロットの設定を有効にします。**restart** コマンドを使って、ルータを再起動させても PRI の情報チャネルとタイムスロットの設定は有効になります。

26. OSPF設定例

本章ではOSPF設定例を示します。
コマンドの詳細は前節を参照してください。

26.1 バックボーンエリアに所属する2拠点間をPPPで結ぶ



[ルータ1の設定]

```
line type bri2.1 l128

ospf use on
ospf area backbone

ip lan1 address 192.168.1.1/24
ip lan1 ospf area backbone

pp select 1
pp bind bri2.1
ip pp address 192.168.255.243/29
ip pp ospf area backbone
ppp ipcp ipaddress on
pp enable 1
```

[ルータ2の設定]

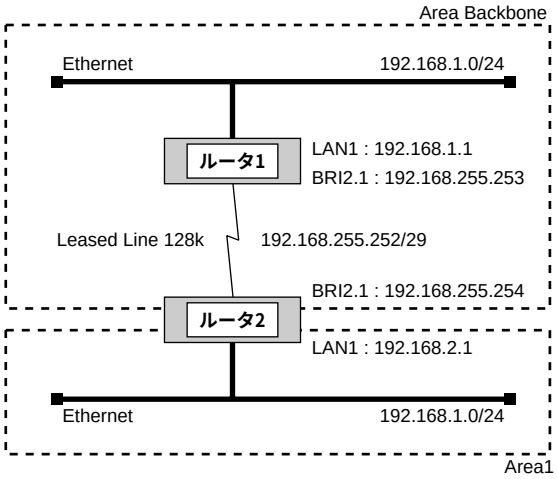
```
line type bri2.1 l128

ospf use on
ospf area backbone

ip lan1 address 192.168.2.1/24
ip lan1 ospf area backbone

pp select 1
pp bind bri2.1
ip pp address 192.168.255.244/29
ip pp ospf area backbone
ppp ipcp ipaddress on
pp enable 1
```

26.2 異なるエリアに分かれた 2 拠点間を PPPで結ぶ



[ルータ 1 の設定]

```
line type bri2.1 l128

ospf use on
ospf area backbone

ip lan1 address 192.168.1.1/24
ip lan1 ospf area backbone

pp select 1
pp bind bri2.1
ip pp address 192.168.255.243/29
ip pp ospf area backbone
ppp ipcp ipaddress on
pp enable 1
```

[ルータ 2 の設定]

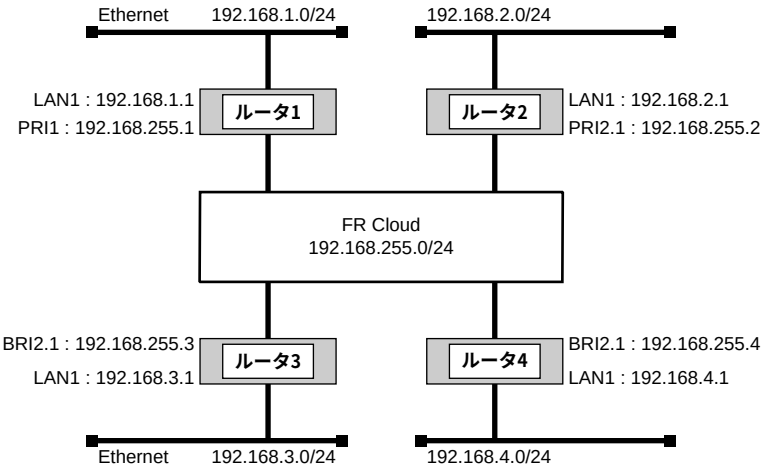
```
line type bri2.1 l128

ospf use on
ospf area backbone
ospf area 1

ip lan1 address 192.168.2.1/24
ip lan1 ospf area 1

pp select 1
pp bind bri2.1
ip pp address 192.168.255.244/29
ip pp ospf area backbone
ppp ipcp ipaddress on
pp enable 1
```

26.3 多拠点間を FR で結ぶ



[ルータ 1 の設定]

```
pri leased channel 1/1 1 24

ospf use on
ospf area backbone

ip lan1 address 192.168.1.1/24
ip lan1 ospf area backbone

pp select 1
pp bind pri1/1
pp encapsulation fr
ip pp address 192.168.255.1/24
ip pp ospf area backbone type=point-to-multipoint
pp enable 1
```

[ルータ 2 の設定]

```
pri leased channel 1/1 1 24

ospf use on
ospf area backbone

ip lan1 address 192.168.2.1/24
ip lan1 ospf area backbone

pp select 1
pp bind pri1/1
pp encapsulation fr
ip pp address 192.168.255.2/24
ip pp ospf area backbone type=point-to-multipoint
pp enable 1
```

[ルータ 3 の設定]

```
line type bri2.1 l128

ospf use on
ospf area backbone

ip lan1 address 192.168.3.1/24
ip lan1 ospf area backbone

pp select 1
pp bind bri2.1
pp encapsulation fr
ip pp address 192.168.255.3/24
ip pp ospf area backbone type=point-to-multipoint
pp enable 1
```

[ルータ 4 の設定]

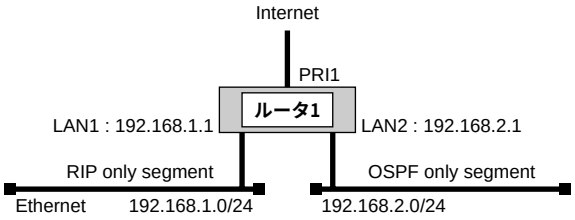
```
line type bri2.1 l128

ospf use on
ospf area backbone

ip lan1 address 192.168.4.1/24
ip lan1 ospf area backbone

pp select 1
pp bind bri2.1
pp encapsulation fr
ip pp address 192.168.255.4/24
ip pp ospf area backbone type=point-to-multipoint
pp enable 1
```

26.4 静的経路、RIPとの併用



[ルータ１の設定]

```
pri leased channel 1/1 1 24

ip route default gateway pp 1

rip use on
ospf use on
ospf area backbone
ospf import from static
ospf import from rip

ip lan1 address 192.168.1.1/24
ip lan1 ospf area backbone passive

ip lan2 address 192.168.2.1/24
ip lan2 ospf area backbone
ip lan2 rip send off
ip lan2 rip receive off

pp select 1
pp bind pri1/1
pp enable 1
```