第 5 章　相手情報の設定

5.1　相手共通情報

5.1.1　remote delete

[機能]

相手ネットワークの削除

[入力形式]

remote delete <number>

[パラメタ]

<number>

削除する相手ネットワークを指定します。

- 相手定義番号
  削除する相手ネットワークの通し番号を指定します。
- all
  すべての相手ネットワークを削除する場合に指定します。

[説明]

相手ネットワークを削除します。

5.1.2 remote name

[機能]

相手ネットワーク名称の設定

[入力形式]

remote [<number>] name <network_name>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<network_name>

- 相手ネットワーク名
  相手ネットワーク名を、0x21,0x23～0x7e の 8 文字以内の ASCII 文字列で指定します。

[説明]

相手ネットワーク名を設定します。

[注意]

既に同一名称の相手ネットワークが登録されている場合は、異常終了します。

[未設定時]

相手ネットワーク名を設定しないものとみなされます。

5.1.3　remote autodial

[機能]

自動ダイヤル可否の設定

[入力形式]

remote [<number>] autodial <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

自動的にダイヤルするかどうかを指定します。

- enable
  送信すべきパケットが発生した場合に、自動ダイヤルを行います。
- disable
  送信すべきパケットが発生しても、自動ダイヤルを行いません。

[説明]

指定した相手に対して、自動的にダイヤルするかどうかを設定します。

[注意]

“3.2.7 wan isdn autodial” で<mode>に disable を指定している場合は、自動ダイヤルを行えません。
自動ダイヤルを行う場合は、<mode>に enable を指定しておいてください。

[未設定時]

自動ダイヤルを行うものとみなされます。

```
remote <number> autodial enable
```

5.1.4 remote mtu

[機能]

送信パケット最大長 (MTU 値) の設定

[入力形式]

remote [<number>] mtu <mtu>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mtu>

- MTU 値
  MTU 値を、200～1500 の 10 進数値で指定します。

[説明]

リモートに対して送信するパケットの MTU 値を設定します。
MTU 値を変更すると、このリモートに対して送信するパケットの最大長が変更されます。また、PPP ネゴシエーションにおいて相手 MRU 値、相手 MRRU 値が MTU 値まで小さくなることを許すようになります。

[未設定時]

MTU 値に 1500 を指定したものとみなされます。

```
remote <number> mtu 1500
```

5.1.5　remote shaping

[機能]

シェーピング機能の設定

[入力形式]

remote [<number>] shaping <mode> [<rate>]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

- on
  シェーピングを使用します。
- off
  シェーピングを使用しません。

<rate>

- 最大送出レート
  最大送出レートを、1k〜128k の範囲の 10 進数値と単位文字で指定します。
  10 進数値の末尾に k の単位文字を付与することで単位を指定できます。
  単位文字を付与しない場合、単位は Kbps となります。
  単位文字 k を付与した場合、単位は Kbps となります。
  1Kbps は 1000bps です。

[説明]

シェーピング機能について設定します。
<mode>が on の場合、<rate>で設定したレートに送信を抑制します。回線速度を上回る値を設定した場合には、実質的にシェーピングは機能しません。
<mode>が off の場合、<rate>は設定できません。

[未設定時]

シェーピングを使用しないものとみなされます。

```
remote <number> shaping off
```

5.2 アクセスポイント情報

5.2.1 remote ap name

[機能]

アクセスポイントの名称の設定

[入力形式]

remote [<number>] ap [<ap_number>] name <ap_name>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_name>

- アクセスポイント名
  アクセスポイント名を、0x22(ダブルクォーテーション) を除く [0x21-0x7e] の範囲のコードで構成される ASCII 文字列で指定します。指定範囲は、1～8 文字です。

[説明]

アクセスポイント名を設定します。

[注意]

アクセスポイントの情報をすべて未設定時の値で使用する場合には必ずアクセスポイント名を設定してください。すべての値が未設定時値の場合にはアクセスポイントの情報は削除されます。

[未設定時]

アクセスポイント名を設定しないものとみなされます。

5.2.2　remote ap move

[機能]

アクセスポイントの優先順序の変更

[入力形式]

remote [<number>] ap move <ap_number> <new_ap_number>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- 対象アクセスポイント定義番号
  優先順序を変更するアクセスポイント定義番号を指定します。

<new_ap_number>

- 移動先アクセスポイント定義番号
  対象アクセスポイントを移動させる先のアクセスポイント定義番号を指定します。
  対象アクセスポイントは、ここで指定したアクセスポイントの前に移動されます。

[説明]

アクセスポイントの順序を変更します。

5.2.3 remote ap delete

[機能]

アクセスポイントの削除

[入力形式]

remote [<number>] ap delete <ap_number>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

削除するアクセスポイント定義番号を指定します。

- アクセスポイント定義番号
  削除するアクセスポイント定義番号を指定します。
- all
  すべてアクセスポイント定義番号を削除する場合に指定します。

[説明]

アクセスポイントを削除します。

5.2.4　remote ap datalink type

[機能]

パケット転送方法の設定

[入力形式]

remote [<number>] ap [<ap_number>] datalink type <type>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<type>

パケットの転送方式を指定します。

- physical
  bind 命令 (“5.2.5 remote ap datalink bind” を参照) によって決定された利用回線のデフォルトの転送方式を提供する場合に指定します。以下に各回線のデフォルトの転送方式を示します。

ISDN	PPP
HSD	PPP
FR	RFC2427 方式

- ip
  IPv6 over IPv4 tunnel を使用する場合に指定します。
- ipsec
  IPsec を使用する場合に指定します。
- discard
  このアクセスポイント利用時にはすべてのパケットが破棄されます。

[説明]

指定したアクセスポイントを利用してパケットを転送する場合の転送方式を設定します。

[未設定時]

転送方式として physical を設定するものとみなされます。

```
remote <number> ap 0 datalink type physical
```

5.2.5 remote ap datalink bind

[機能]

パケット転送回線の設定

[入力形式]

remote [<number>] ap [<ap_number>] datalink bind <kind> [<conf_number>]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<kind>

- wan
  wan 定義によって指定される回線を利用する場合に指定します。
- lan
  lan 定義によって指定される回線を利用する場合に指定します。

<conf_number>

- wan 定義または lan 定義の定義番号
  利用する wan 定義番号として 0、または lan 定義番号として 0 を指定します。

[説明]

指定したアクセスポイント定義を利用してパケットを転送する場合の回線を設定します。
本コマンドは、“5.2.4 remote ap datalink type” の<type>で physical を指定した場合にだけ有効です。

[注意]

本コマンドは設定はできますが、無効です。

[未設定時]

<kind>に wan を、<conf_nubmer>に 0 を指定するものとみなされます。

```
remote <number> ap 0 datalink bind wan 0
```

5.2.6　remote ap limit time

[機能]

接続時間累計制限の設定

[入力形式]

remote [<number>] ap [<ap_number>] limit time <time>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time>

- 接続時間累計上限
  接続時間累計の上限時間を、0 秒～999 時間の範囲で指定します。単位は、d(日)、h(時)、m(分)、s(秒)のいずれかを指定します。0 秒を指定した場合は、上限を設定しません。

[説明]

指定したアクセスポイントに対する接続時間累計の上限値を設定します。
発信時に、このアクセスポイントに対する接続時間累計が指定した上限値を超えていた場合は、このアクセスポイントに対する自動発信を行いません。次の優先度のアクセスポイントに対して処理を移します。

[未設定時]

接続時間累計の上限値を設定しないものとみなされます。

```
remote <number> ap <ap_number> limit time 0s
```

5.2.7 remote ap ppp auth type

[機能]

認証方法の設定

[入力形式]

remote [<number>] ap [<ap_number>] ppp auth type <authtype>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<authtype>

認証プロトコルのタイプを指定します。

- off
  認証を要求しない場合に指定します。
- pap
  PAP による認証を要求する場合に指定します。
- chap_md5
  MD5-CHAP による認証を要求する場合に指定します。
- any
  MD5-CHAP または PAP による認証を要求し、実際に利用する認証プロトコルはネゴシエーションによって決定する場合に指定します。

[説明]

接続時に要求する認証プロトコルのタイプを設定します。
ここでの設定は、着信し、かつ CLID 相手判定が行われた場合に有効となります。

[未設定時]

着信時の認証プロトコルに MD5-CHAP または PAP を用います。

```
remote <number> ap 0 called ppp auth type any
```

5.2.8　remote ap ppp auth send

[機能]

送信認証情報の設定

[入力形式]

remote [<number>] ap [<ap_number>] ppp auth send <id> <password> [encrypted]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<id>

- 認証 ID
  認証 ID を、0x21,0x23〜0x7e の文字で構成される 64 文字以内の文字列を指定します。"delete"は指定できません。

<password>

- 認証パスワード
  認証パスワードを、0x21,0x23〜0x7e の文字で構成される 64 文字以内の文字列を指定します。
  show コマンドで表示される暗号化された認証パスワード文字列を encrypted とともに指定することもできます。その場合、表示された文字列をそのまま正確に入力してください。文字列は 64 文字を超えていてもかまいません。
- 暗号化された認証パスワード
  show コマンドで表示される暗号化された認証パスワードを encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化認証パスワード指定
  <password>に暗号化された認証パスワードを設定する場合に指定します。

[説明]

指定したアクセスポイントに接続するときに送信する認証情報 (認証 ID およびパスワード) を設定します。

[注意]

認証 ID およびパスワードが設定されていない場合、接続相手からの認証要求を拒否します。
show コマンドでは、暗号化された認証パスワードが encrypted と共に表示されます。

[未設定時]

送信する認証情報を定義しないものとみなされます。

5.2.9 remote ap ppp auth send delete

[機能]

認証情報の削除

[入力形式]

remote [<number>] ap [<ap_number>] ppp auth send delete

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

[説明]

認証情報 (認証 ID およびパスワード) を削除します。

5.2.10　remote ap ppp auth receive

[機能]

受諾認証情報の設定

[入力形式]

remote [<number>] ap [<ap_number>] ppp auth receive <id> <password> [encrypted]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<id>

- 認証 ID
  認証 ID を、0x21,0x23～0x7e の文字で構成される 64 文字以内の文字列を指定します。"delete"は指定できません。

<password>

- 認証パスワード
  認証パスワードを、0x21,0x23～0x7e の文字で構成される 64 文字以内の文字列を指定します。
  show コマンドで表示される暗号化された認証パスワードを encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化認証パスワード指定
  <password>に暗号化された認証パスワードを設定する場合に指定します。

[説明]

認証プロトコル使用時に受諾する、認証情報 (認証 ID および認証パスワード) を設定します。

[注意]

show コマンドでは、暗号化された認証パスワードが encrypted と共に表示されます。

[未設定時]

受諾する認証情報を設定しないものとみなされます。

5.2.11 remote ap ppp auth receive delete

[機能]

受諾認証情報の削除

[入力形式]

remote [<number>] ap [<ap_number>] ppp auth receive delete

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

[説明]

認証プロトコル使用時に受諾する、認証情報 (認証 ID および認証パスワード) を削除します。

5.2.12　remote ap ppp mp use

[機能]

発信時の MP 利用の可否の設定

[入力形式]

remote [<number>] ap [<ap_number>] ppp mp use <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

MP を利用するかどうかを指定します。

- off
  MP を利用しない場合に指定します。
- on
  MP を利用する場合に指定します。

[説明]

発信時に MP を利用するかどうかを設定します。
着信時は、CLID 相手判定によって指定したアクセスポイントへの接続が決定された場合に、MP を利用するかどうかを設定します。

[未設定時]

MP を利用しないものとみなされます。

```
remote <number> ap 0 ppp mp use off
```

5.2.13 remote ap ppp mp bap use

[機能]

発信時の BAP/BACP 利用の可否の設定

[入力形式]

remote [<number>] ap [<ap_number>] ppp mp bap use <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

BAP/BACP を利用するかどうかを指定します。

- off
  BAP/BACP を利用しない場合に指定します。
- on
  BAP/BACP を利用する場合に指定します。

[説明]

MP を利用する場合に BAP/BACP を利用するかどうかを設定します。
着信時は、CLID 相手判定によってこのアクセスポイントへの接続が決定された場合に、BAP/BACP を利用するかどうかを設定します。

[未設定時]

BAP/BACP を利用しないものとみなされます。

```
remote <number> ap 0 ppp mp bap use off
```

5.2.14　remote ap dial number

[機能]

アクセスポイントの電話番号の設定

[入力形式]

remote [<number>] ap [<ap_number>] dial <count> number <dial_number> [<subaddress>]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

ダイヤル定義番号として、以下のいずれかを指定します。

- 0
- 1
- 2

<dial_number>

- 相手電話番号
  相手の電話番号を、0～9 の数字と、*、#、-、(、) の文字で構成される 32 桁以内の ASCII 文字列で指定します。

<subaddress>

- 相手サブアドレス
  相手のサブアドレスを、0x21,0x23～0x7e の文字で構成される 19 桁以内の ASCII 文字列で指定します。

[説明]

アクセスポイントの電話番号を設定します。

[未設定時]

アクセスポイントの電話番号を設定しないものとみなされます。

5.2.15 remote ap dial speed

[機能]

アクセスポイントの通信速度の設定

[入力形式]

remote [<number>] ap [<ap_number>] dial <count> speed <speed> [<carrier>]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

ダイヤル定義番号として、以下のいずれかを指定します。

- 0
- 1
- 2

<speed>

通信速度、通信手順を指定します。

- 64K
  同期 PPP 64Kbps の場合に指定します。
- PIAFS
  PIAFS(32Kbps) 接続の場合に指定します。
- PIAFS64K
  PIAFS(64Kbps) 接続の場合に指定します。

<carrier>

通信速度に "PIAFS64K" を指定した場合に通信事業者を指定します。省略した場合は、"docomo" を指定したものとみなされます。なお、通信速度に "PIAFS64K" 以外を指定した場合には、本パラメタを指定しないでください。

- docomo
  NTT DoCoMo の PIAFS(64Kbps) 接続の場合に指定します。
- ddip
  DDI Pocket の PIAFS(64Kbps) 接続の場合に指定します。

[説明]

アクセスポイントの通信速度および通信手順を設定します。

[未設定時]

通信速度に 64kbps を指定したものとみなされます。

```
remote <number> ap 0 dial <count> speed 64K
```

5.2.16 remote ap dial delete

[機能]

アクセスポイントの電話番号および通信速度の削除

[入力形式]

remote [<number>] ap [<ap_number>] dial delete <count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

削除するダイヤル定義を指定します。

- ダイヤル定義番号
  削除する電話番号のダイヤル定義番号を、0〜2 の範囲で指定します。
- all
  すべてのダイヤル定義を削除する場合に指定します。

[説明]

アクセスポイントの電話番号および通信速度を削除します。

[注意]

削除は、ダイヤル定義番号の単位で行われます。したがって、アクセスポイント電話番号 (“5.2.14 remote ap dial number” を参照) および通信速度 (“5.2.15 remote ap dial speed” を参照) の設定は同時に削除されます。

5.2.17　remote ap callback

[機能]

コールバック要求動作の設定

[入力形式]

remote [<number>] ap [<ap_number>] callback <mode> [<kind> <time> [<callback_number> [<subaddress>]]]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

- enable
  発信時にコールバックを要求します。
- disable
  発信時にコールバックを要求しません。

<kind>

- clid
  コールバック方式に「無課金方式」を指定します。
- cbcp
  コールバック方式に「CBCP 方式」を指定します。

<time>

- コールバック待ち時間
  コールバック要求が受理された後、相手からのコールバック応答着信を待つ時間を、0 秒～60 秒の範囲で指定します。
  単位は、m(分)、s(秒) のいずれかを指定します。

<callback_number>

- コールバック電話番号
  コールバック要求時に相手に伝える自側の電話番号を、0～9 の数字と、*、#、-、(、) の文字で構成される 32 桁以内の ASCII 文字列で指定します。

<subaddress>

- コールバックサブアドレス
  コールバック要求時に相手に伝える自側の電話番号に対するサブアドレスを、0x21, 0x23～0x7e の文字で構成される 19 桁以内の ASCII 文字列で指定します。
-

[説明]

このアクセスポイントに対して発信する際のコールバック要求動作を設定します。

<callback_number> および <subaddress> の設定はコールバック方式に「cbcp」を設定し、相手システムがコールバック要求側からの電話番号指定を許可した場合に有効です。

[未設定時]

発信時にコールバック要求しないものとみなされます。

```
remote <number> ap <ap_number> callback disable
```

5.2.18　remote ap called accept

[機能]

アクセスポイントからの着信許可の設定

[入力形式]

remote [<number>] ap <ap_number> called accept <incoming>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<incoming>

着信を許可するかどうかを指定します。

- enable
  着信を許可する場合に指定します。
- disable
  着信を許可しない場合に指定します。

[説明]

指定したアクセスポイントから送られてきたと判断されたデータに対して、着信を許可するかどうかを設定します。

[未設定時]

着信を許可するものとみなされます。

```
remote <number> ap 0 called accept enable
```

5.2.19 remote ap called clid

[機能]

CLID 相手判断利用の可否の設定

[入力形式]

remote [<number>] ap <ap_number> called clid <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

着信時に CLID 相手判定をするかどうかを指定します。

- enable
  着信時に CLID 相手判定をする場合に指定します。
- disable
  着信時に CLID 相手判定をしない場合に指定します。

[説明]

着信時に、相手電話番号を判定するかどうかを設定します。相手電話番号を判定することを、CLID 相手判定と呼びます。

- 以下の定義の相手電話番号を利用して、着信時に相手を判定します。
  1) “5.2.20 remote ap called number” による定義が存在する場合は、その定義の相手電話番号。
  2) 1) の定義が存在せず、“5.2.14 remote ap dial number” による定義が存在する場合は、その定義の相手電話番号。
- 本コマンドの<mode>で enable を指定した場合に上記の番号が発信者番号として通知されたときは、指定したアクセスポイントから着信したものとみなされます。

[未設定時]

着信時に、CLID 相手判定を行うものとみなされます。

```
remote <number> ap 0 called clid enable
```

5.2.20　remote ap called number

[機能]

CLID の設定

[入力形式]

remote [<number>] ap [<ap_number>] called number <called_number> [<subaddress>]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<called_number>

相手電話番号

- 相手電話番号
  相手の電話番号を、0～9 の数字と、*、#、-、(、) の文字で構成される 32 桁以内の ASCII 文字列で指定します。
- any
  着信時の CLID 相手判定に、"“5.2.14 remote ap dial number”"で設定した相手電話番号を使用する場合に指定します。

<subaddress>

- 相手サブアドレス
  相手のサブアドレスを、0x21,0x23～0x7e の文字で構成される 19 桁以内の ASCII 文字列で指定します。

[説明]

CLID 相手判定で、チェックする番号を設定します。

[未設定時]

着信時の CLID 相手判定に、"“5.2.14 remote ap dial number”"で設定された相手電話番号を使用します。

```
remote <number> ap 0 called number any
```

5.2.21 remote ap called callback

[機能]

コールバック応答動作の設定

[入力形式]

remote [<number>] ap [<ap_number>] called callback <mode> [<kind> <time> [<callback_number> [<subaddress>]]]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

- enable
  着信時にコールバックを行います。
- disable
  着信時にコールバックを行いません。

以下のパラメタは、<mode>が disable の場合は省略できます。

<kind>

- clid
  コールバック方式として「無課金方式」を指定します。
- cbcp
  コールバック方式として「CBCP 方式」を指定します。

<time>

- コールバック待ち時間
  コールバック要求着信を受理した後、相手にコールバック応答発信を行うまでの待ち時間を、0 秒～60 秒の範囲で指定します。
  単位は、m(分)、s(秒) のいずれかを指定します。

<callback_number>

- コールバック電話番号
  コールバック要求着信を受理した後、コールバック応答発信で利用する電話番号を、0～9 の 10 進数値と ( ) \ - # * の区切り文字で構成される 32 桁以内の ASCII 文字列で指定します。

<subaddress>

- コールバックサブアドレス
  コールバック応答発信で利用する電話番号に対するサブアドレスを、0x21,0x23～0x7e の文字で構成される 19 桁以内の ASCII 文字列で指定します。

[説明]

このアクセスポイントに着信を受けた場合のコールバック応答動作の設定を行います。
この設定は発信者番号 (CLID) で相手識別が行われた場合に利用します。
コールバック方式に「cbcp」を指定し，<callback_number> の指定を行なった場合には、コールバック要求側からの電話番号指定を許可しません。

[未設定時]

着信時にコールバック応答動作を行わないものとみなされます。

```
remote <number> ap <ap_number> called callback disable
```

5.2.22 remote ap idle

[機能]

無通信監視タイマの設定

[入力形式]

remote [<number>] ap [<ap_number>] idle <time>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time>

- 無通信監視時間
  無通信監視時間を、0 秒～3600 秒の範囲で指定します。単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。0 秒を指定した場合は、監視を行いません。

[説明]

指定したアクセスポイントと接続したときの無通信監視時間を設定します。

[未設定時]

監視を行わないものとみなされます。

```
remote [<number>] ap [<ap_number>] idle 0d
```

5.2.23　remote ap step

[機能]

平日昼間時間帯の課金単位時間の設定

[入力形式]

remote [<number>] ap [<ap_number>] step <time>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time>

- 課金単位時間
  平日昼間時間帯 (月〜金曜日 8:00〜19:00) の課金単位時間 (秒) の 10 倍の値を、0〜36000 の 10 進数値で指定します (例: 180 秒=1800、16.5 秒=165)。0 を指定した場合は、課金単位に応じた接続保持を行いません。

[説明]

ISDN 回線を利用して通信するときの平日昼間時間帯 (月〜金曜日 08:00〜19:00) の課金単位時間を設定します。課金単位時間を設定すると、無通信の場合でも接続時間が設定値の整数倍になるまで接続を保持します。

[注意]

課金単位時間を設定する場合、本装置の時刻を正しく設定してください。
祝日の料金には対応していません。

[未設定時]

課金単位時間を設定しないものとみなされます。

5.2.24 remote ap step2

[機能]

夜間・休日時間帯の課金単位時間の設定

[注意]

課金単位時間を設定する場合、本装置の時刻を正しく設定してください。

[入力形式]

remote [<number>] ap [<ap_number>] step2 <time2>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time2>

- 課金単位時間
  夜間・休日時間帯 (月〜金曜日 19:00〜23:00)、土 / 日曜日 (08:00〜23:00) の課金単位時間 (秒) の 10 倍の値を、0〜36000 の 10 進数値で指定します (例: 180 秒=1800、16.5 秒=165)。

[説明]

ISDN 回線を利用して通信するときの夜間・休日時間帯 (月〜金曜日 19:00〜23:00、土 / 日曜日 08:00〜23:00) の課金単位時間を設定します。課金単位時間を設定すると、無通信の場合でも接続時間が設定値の整数倍になるまで接続を保持します。

[注意]

この設定は、"“5.2.23 remote ap step”"を設定した場合にのみ有効です。祝日の料金には対応していません。

[未設定時]

課金単位時間を設定していないものとみなされ、"remote ap step"で設定した値が使用されます。

5.2.25　remote ap step3

[機能]

深夜時間帯の課金単位時間の設定

[注意]

課金単位時間を設定する場合、本装置の時刻を正しく設定してください。

[入力形式]

remote [<number>] ap [<ap_number>] step3 <time3>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time3>

- 課金単位時間
  深夜時間帯 (全日 23:00〜08:00) の課金単位時間 (秒) の 10 倍の値を、0〜36000 の 10 進数値で指定します (例: 180 秒=1800、16.5 秒=165)。

[説明]

ISDN 回線を利用して通信するときの深夜時間帯 (全日 23:00〜08:00) の課金単位時間を設定します。課金単位時間を設定すると、無通信の場合でも接続時間が設定値の整数倍になるまで接続を保持します。

[注意]

この設定は、"“5.2.23 remote ap step”"を設定した場合にのみ有効です。祝日の料金には対応していません。

[未設定時]

課金単位時間を設定していないものとみなされ、"“5.2.24 remote ap step2”"で設定した値が使用されます。この設定も無い場合には、"“5.2.23 remote ap step”"で設定した値が使用されます。

5.2.26 remote ap keep

[機能]

テレホーダイ (回線接続保持) 機能の設定

[入力形式]

remote [<number>] ap [<ap_number>] keep <keep>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<keep>

回線接続保持の方式を設定します。

- on
  回線接続を保持します。
- off
  回線接続を保持しません。
- connect
  常時接続機能を使用します。

[説明]

回線接続保持の方式を設定します。
"on"の時には回線接続保持の方式として、テレホーダイ機能による制御を行います。
"connect"の時には回線接続保持の方式として、常時接続機能による制御を行います。

[未設定時]

回線接続保持機能を使用しないものとみなされます。

```
remote <number> ap 0 keep off
```

5.2.27　remote ap ipsec type

[機能]

IPsec 情報のタイプの設定

[入力形式]

remote [<number>] ap [<ap_number>] ipsec type <type>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<type>

IPsec 情報のタイプを設定します。

- off
  IPsec を使用しません。
- ike
  IPsec の Aggressive Mode を使用します。

[説明]

IPsec を使用するかどうかを設定します。
IPsec の Aggressive Mode を使用する場合は、以下の設定も行ってください。

- remote ap ipsec ike protocol
- remote ap ipsec ike range
- remote ap ipsec ike encrypt
- remote ap ipsec ike auth
- remote ap ipsec ike pfs
- remote ap ipsec ike lifetime
- remote ap ipsec ike newsa initiator
- remote ap ipsec ike newsa responder
- remote ap ike port
- remote ap ike shared key
- remote ap ike proposal encrypt
- remote ap ike proposal hash
- remote ap ike proposal pfs
- remote ap ike proposal lifetime
- remote ap ike retry

- remote ap ike idtype
- remote ap ike name local
- remote ap ike release
- remote ap ike initial
- remote ap ike sessionwatch

IPsec の Main Mode を使用する場合は、「10 VPN 情報の設定」を参照してください。

IPsec 区間について

IPsec 区間は、tunnel 利用時の自側の tunnel endpoint アドレスと tunnel 利用時の相手側の tunnel endpoint アドレスの定義で指定します。

自動鍵設定 (交換) の場合、事前に tunnel endpoint アドレスが決定している時は指定してください。

tunnel endpoint アドレスの設定例

双方の IP アドレスが固定で決まっている場合:

- remote 0 ap 0 tunnel local 192.168.1.1
- remote 0 ap 0 tunnel remote 172.168.1.1

自側の tunnel endpoint アドレスが不定である場合:

- remote 0 ap 0 tunnel remote 172.168.1.1

IPsec 対象パケットについて

自動鍵設定 (交換) の場合は、<number>で設定された相手情報に range 指定があればその範囲の IP パケットが IPsec 対象となります。range 指定がなければ<number>で設定された相手情報を使用する IP パケットすべてが IPsec 対象となります。

[注意]

1 つの相手情報に対して複数のアクセスポイント情報が設定されている場合、先頭に設定されているアクセスポイント情報の IPsec 情報と IKE 情報が有効になります。

[未設定時]

IPsec を使用しないものとみなされます。

```
remote <number> ap <ap_number> ipsec type off
```

5.2.28　remote ap ipsec ike protocol

[機能]

自動鍵交換用 IPsec 情報のセキュリティプロトコルの設定

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike protocol <protocol>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<protocol>

自動鍵交換用 IPsec SA のセキュリティプロトコルを指定します。

- none
  セキュリティプロトコル未指定
- esp
  暗号
- ah
  認証

[説明]

自動鍵交換用 IPsec SA の、セキュリティプロトコルの設定を行います。

[未設定時]

自動鍵交換用 IPsec 情報のセキュリティプロトコルは未指定となります。

```
remote <number> ap <ap_number> ipsec ike protocol none
```

5.2.29 remote ap ipsec ike encrypt

[機能]

自動鍵交換用 IPsec 情報の暗号情報の設定

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike encrypt <enc_algo>[,<enc_algo>...]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<enc_algo>

暗号アルゴリズムを指定します。
複数のアルゴリズムを指定することができます。複数定義する時は、アルゴリズムを空白なしでカンマ','で区切ります。

- des-cbc
- 3des-cbc
- null
- none

[説明]

送受信パケットを暗号化／復号化するための、暗号アルゴリズムの設定を行います。
暗号鍵は自動生成されるので、設定は不要です。
暗号アルゴリズムを複数指定する場合、指定順序に関わらず以下の優先順位となります。

1) 3des-cbc
2) des-cbc
3) null

[未設定時]

IPsec によるパケット暗号は行われません。

```
remote <number> ap <ap_number> ipsec ike encrypt none
```

5.2.30　remote ap ipsec ike auth

[機能]

自動鍵交換用 IPsec 情報の認証情報の設定

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike auth <auth_algo>[,<auth_algo>...]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<auth_algo>

認証アルゴリズムを指定します。
複数のアルゴリズムを指定することができます。複数定義する時は、アルゴリズムを空白なしでカンマ','で区切ります。

- hmac-md5
- hmac-sha1
- none

[説明]

送受信パケットを認証するための、認証アルゴリズムと鍵の設定を行います。
認証鍵は自動生成されるので、設定は不要です。
認証アルゴリズムを複数指定する場合、指定順序に関わらず以下の優先順位となります。

1) hmac-md5
2) hmac-sha1

[未設定時]

IPsec によるパケット認証は行われません。

```
remote <number> ap <ap_number> ipsec ike auth none
```

5.2.31 remote ap ipsec ike pfs

[機能]

自動鍵交換用 IPsec 情報の PFS グループの設定

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike pfs <pfs_group>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<pfs_group>

Diffie-Hellman グループについて指定します。

- modp768
  Diffie-Hellman グループの MODP768
- modp1024
  Diffie-Hellman グループの MODP1024
- off
  Diffie-Hellman グループを使用しません。

[説明]

IPsec セッションの鍵素材を保護する、PFS グループの設定を行います。

[未設定時]

PFS による鍵交換データ保護は行いません。セキュア通信を行いたい場合は適切な PFS グループを設定して下さい。

```
remote <number> ap <ap_number> ipsec ike pfs off
```

5.2.32　remote ap ipsec ike lifetime

[機能]

自動鍵交換用 IPsec 情報の SA 有効時間の設定

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike lifetime <lifetime>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<lifetime>

- SA 有効時間
  SA 有効時間を、600 秒 (10 分)～86400 秒 (1 日) の範囲で指定します。単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。

[説明]

IPsec セッションの通信データを保護する、IPsec SA の SA 有効時間 (秒) の設定を行います。

[未設定時]

IPsec SA の有効時間として 8h(8 時間) が設定されたものとして扱います。

```
remote <number> ap <ap_number> ipsec ike lifetime 8h
```

5.2.33 remote ap ipsec ike newsa initiator

[機能]

自動鍵交換用 IPsec 情報の New SA Initiator(更新時間) の設定

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike newsa initiator <time>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time>

- Initiator SA 更新時間
  Initiator SA 更新時間を、30 秒～180 秒 (3 分) の範囲で指定します。単位は、m(分)、s(秒) のいずれかを指定します。

[説明]

自側が Initiator の場合に、IPsec SA の有効時間が満了になる前に、IPsec SA の更新を行うための時間の設定を行います。
相手側の New SA Responder と同じ時間にならないように設定して下さい。

[未設定時]

Initiator SA 更新時間として 90s(90 秒) が設定されたものとして扱います。

```
remote <number> ap <ap_number> ipsec ike newsa initiator 90s
```

5.2.34　remote ap ipsec ike newsa responder

[機能]

自動鍵交換用 IPsec 情報の New SA Responder(更新時間) の設定

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike newsa responder <time>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time>

- Responder SA 更新時間
  Responder SA 更新時間を、30 秒～180 秒 (3 分) の範囲で指定します。単位は、m(分)、s(秒) のいずれかを指定します。
- off
  Responder 側からの SA 更新は行いません。

[説明]

自側が Responder の場合に、IPsec SA の有効時間が満了になる前に、IPsec SA の更新を行うための時間の設定を行います。
相手側の New SA Initiator と同じ時間にならないように設定して下さい。
また、off 指定時には Responder 側からの SA 更新は行いません。

[未設定時]

Responder SA 更新時間として 30s(30 秒) が設定されたものとして扱います。

```
remote <number> ap <ap_number> ipsec ike newsa responder 30s
```

5.2.35 remote ap ipsec ike range

[機能]

自動鍵交換用 IPsec 情報の対象範囲の設定

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike range <src_addr>/<mask> <dst_addr>/<mask>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<src_addr>/<mask>

IPsec 対象となる送信元 IP アドレス、マスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  IPsec 対象となる送信元 IP アドレスとマスクビット数の組み合わせを指定します。
- any4
  すべての IPv4 アドレスを IPsec 対象に含めます。0.0.0.0/0(0.0.0.0/0.0.0.0) と同意。

<dst_addr>/<mask>

IPsec 対象となる宛先 IP アドレス、マスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  IPsec 対象となる宛先 IP アドレスとマスクビット数の組み合わせを指定します。
- any4
  すべての IPv4 アドレスを IPsec 対象に含めます。0.0.0.0/0(0.0.0.0/0.0.0.0) と同意。

[説明]

IPsec を適用するセッションの範囲を設定します。(Security Policy Database の情報)

[未設定時]

<src_addr>,<dst_addr>共に any4 が設定されたものとして扱います。

```
remote <number> ap <ap_number> ipsec ike range any4 any4
```

5.2.36　remote ap ike port

[機能]

IKE 情報の相手側 IKE ポート番号の設定

[入力形式]

remote [<number>] ap [<ap_number>] ike port <port>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<port>

- 相手側 IKE ポート番号
  相手側 IKE ポート番号を指定します。(デフォルト: 500 番)

[説明]

SA 確立のネゴシエーションを行う、相手 IKE サーバのポート番号の設定を行います。

[未設定時]

相手側 IKE ポート番号に標準ポート番号である 500 を指定したものとみなされます。

```
remote <number> ap <ap_number> ike port 500
```

5.2.37 remote ap ike shared key

[機能]

IKE セッション確立時の共通鍵 (Pre-shared key) の設定

[入力形式]

remote [<number>] ap [<ap_number>] ike shared key <kind> <shared_key>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<kind>

鍵種別を指定します。

- hex
  16 進数鍵を使用します。
- text
  文字列鍵を使用します。

<shared_key>

共通鍵を指定します。

- 暗号化されていない共通鍵を指定します。
  文字列鍵の場合は、0x22(ダブルクォーテーション) を除く [0x20-0x7e] の範囲のコードで構成される ASCII 文字列で指定します。ただし、文字列鍵で 0x20(空白文字) を使用する場合には、文字列鍵をダブルクォーテーション (") で囲う必要があります。以下に、入力範囲を示します。

鍵種別	16進数鍵	文字列鍵
共通鍵	1〜256桁	1〜128文字

- 暗号化された共通鍵を指定します。
  show コマンドで表示される暗号化された共通鍵を encrypted と共に指定します。show コマンドで表示される文字列をそのまま正確に指定してください。

<encrypted>

- 暗号化共通鍵指定
  <shared_key>に暗号化された共通鍵を指定する場合に指定します。

[説明]

SA 確立のネゴシエーションの時に接続相手を認証するための、共通鍵の設定を行います。

[未設定時]

共通鍵が設定されません。IKE により鍵交換を行う場合は必ず設定してください。

5.2.38　remote ap ike proposal delete

[機能]

IKE 情報の Proposal 定義の削除

[入力形式]

remote [<number>] ap [<ap_number>] ike proposal delete <proposal_number>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<proposal_number>

削除する Proposal 定義を指定します。

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。
- all
  <ap_number>で指定した IKE 情報のすべての Proposal 定義を削除対象とします。

[説明]

IKE 情報の Proposal 定義を削除します。

5.2.39 remote ap ike proposal move

[機能]

IKE セッション用 Proposal 定義優先順序の変更

[入力形式]

remote [<number>] ap [<ap_number>] ike proposal move <proposal_number> <new_number>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<proposal_number>

- 移動元の Proposal 定義優先順序を指定します。

<new_number>

- 移動先の Proposal 定義優先順序を指定します。

[説明]

<ap_number>で指定したアクセスポイント情報の IKE セッション用の Proposal 定義優先順序を変更します。

IKE セッション用 Proposal 定義とネゴシエーションの関係

	ネゴシエーション情報	Proposal	Proposal	...
a	暗号情報	3des-cbc	des-cbc	...
b	ハッシュ情報	hmac-md5	0	...
c	PFSグループ	modp768	modp1024	...
d	SA有効時間	600s	0	...

※ a を複数指定 (<proposal_number>0,1,2 を定義) した場合、他の情報は定義しなければ各情報のデフォルト値を採用します。

IKE セッションのネゴシエーションは、Proposal 単位 (a〜d を一組) として行います。その中で a〜c は相手装置の定義と一致することが条件となります。

自側が Responder の場合は、相手の Proposal が許容できるかを判断するため、自装置の定義は参照されません。

本装置を Aggressive Mode で動作させる時に、IKE セッション用 Proposal 定義を複数設定する場合、PFS の設定はすべて同じ値を設定して下さい。

これは、Aggressive Mode が Diffie-Hellman のグループについてネゴシエーションができないためです。(Initiator が最初の ISAKMP パケットに載せる鍵素材の計算に使用するため、Diffie-Hellman のグループは同じである必要があります) Aggressive Mode は、相手 (リモート) 情報 tunnel 利用時の自側の tunnel endpoint address を未設定にし、IKE 情報の自装置名を設定します。

5.2.40　remote ap ike proposal encrypt

[機能]

IKE セッション用暗号情報の設定

[入力形式]

remote [<number>] ap [<ap_number>] ike proposal [<proposal_number>] encrypt <enc_algo>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<proposal_number>

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。
  省略した場合は、0 を指定したものとみなされます。

<enc_algo>

暗号アルゴリズムを指定します。

- des-cbc
- 3des-cbc

[説明]

IKE セッションの送受信パケットを暗号化／復号化するための、暗号アルゴリズムの設定を行います。
コマンドによる定義を行う場合は、必ず設定して下さい。
IKE セッション用暗号情報設定が未定義ですと IKE が動作しません。

[未設定時]

IKE セッション用暗号情報が設定されません。IKE により鍵交換を行う場合は必ず設定してください。

5.2.41 remote ap ike proposal hash

[機能]

IKE セッション用ハッシュ情報の設定

[入力形式]

remote [<number>] ap [<ap_number>] ike proposal [<proposal_number>] hash <hash_algo>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<proposal_number>

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。
  省略した場合は、0 を指定したものとみなされます。

<hash_algo>

ハッシュアルゴリズムを指定します。

- hmac-md5
- hmac-sha1

[説明]

IKE セッションのネゴシエーションパケットを認証するための、ハッシュアルゴリズムの設定を行います。

[未設定時]

ハッシュアルゴリズムに hmac-md5 を指定したものとみなされます。

```
remote <number> ap <ap_number> ike proposal <count> hash hmac-md5
```

5.2.42　remote ap ike proposal pfs

[機能]

IKE セッション用 PFS グループの設定

[入力形式]

remote [<number>] ap [<ap_number>] ike proposal [<proposal_number>] pfs <pfs_group>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<proposal_number>

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。
  省略した場合は、0 を指定したものとみなされます。

<pfs_group>

Diffie-Hellman グループについて指定します。

- modp768
  MODP768 の Diffie-Hellman グループ
- modp1024
  MODP1024 の Diffie-Hellman グループ

[説明]

IKE セッションのネゴシエーションパケットを保護するための、PFS グループの設定を行います。

[未設定時]

PFS グループに modp768 を指定したものとみなされます。

```
remote <number> ap <ap_number> ike proposal <count> pfs modp768
```

5.2.43 remote ap ike proposal lifetime

[機能]

IKE 情報の SA 有効時間の設定

[入力形式]

remote [<number>] ap [<ap_number>] ike proposal [<proposal_number>] lifetime <lifetime>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<proposal_number>

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。
  省略した場合は、0 を指定したものとみなされます。

<lifetime>

- SA 有効時間
  SA 有効時間を、600 秒 (10 分)～86400 秒 (1 日) の範囲で指定します。単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。

[説明]

IKE セッションのネゴシエーションパケットを保護するための、SA 有効時間 (秒) の設定を行います。

[未設定時]

IKE SA の有効時間として 24h(24 時間) が設定されたものとして扱われます。

```
remote <number> ap <ap_number> ike proposal <count> lifetime 24h
```

5.2.44　remote ap ike retry

[機能]

IKE 情報の初回再送時間および再送回数の設定

[入力形式]

remote [<number>] ap [<ap_number>] ike retry <time> <count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time>

- 初回再送時間初回再送時間を、1 秒～60 秒 (1 分) の範囲で指定します。単位は、m(分)、s(秒) のいずれかを指定します。

<count>

- 再送回数
  再送回数を、1～10 の範囲で指定します。

[説明]

IKE セッションのネゴシエーションパケットに対する初回再送時間および再送回数の設定を行います。

[未設定時]

初回再送時間に 10 秒、再送回数に 3 回を設定したものとみなされます。

```
remote <number> ap <ap_number> ike retry 10s 3
```

5.2.45 remote ap ike idtype

[機能]

IKE 情報の送信 ID タイプの設定

[入力形式]

remote [<number>] ap [<ap_number>] ike idtype <id_type>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<id_type>

ネゴシエーションの交換タイプを指定します。

- fqdn
  省略なしドメイン名
- user_fqdn
  省略なしユーザ識別名

[説明]

IKE セッションを確立する、ネゴシエーションの ID タイプの設定を行います。
IKE セッション確立のネゴシエーションパケットの ID payload に使用されます。

[未設定時]

IKE セッション確立のネゴシエーションパケットの ID タイプとして FQDN が設定されたものとして扱われます。

```
remote <number> ap <ap_number> ike idtype fqdn
```

5.2.46　remote ap ike name local

[機能]

IKE 情報の自装置名の設定

[入力形式]

remote [<number>] ap [<ap_number>] ike name local <name>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<name>

- 自装置名
  自装置を識別する名前を指定します。指定範囲は、1～64 文字です。
  名前は、0x22(ダブルクォーテーション) を除く [0x21-0x7e] の範囲のコードで構成される ASCII 文字列で指定します。但し、"delete"を指定することはできません。

[説明]

IKE セッションを確立する、自装置の IP アドレスが不定の場合に名前の設定を行います。

IKE 情報の自装置名および相手装置名の設定と、相手 (リモート) 情報の tunnel endpoint address の設定により、ISAKMP SA のネゴシエーション交換タイプが以下のように決定します。

相手情報 IKE情報	tunnel local	tunnel remote
name local	動作しない	Aggressive Mode

tunnel local : tunnel 利用時の自側の tunnel endpoint address の設定
tunnel remote: tunnel 利用時の相手側の tunnel endpoint address の設定

[未設定時]

IKE セッション用自装置名が設定されません。Aggressive Mode により鍵交換を行う場合は必ず設定してください。

5.2.47 remote ap ike name local delete

[機能]

IKE 情報の自装置名の削除

[入力形式]

remote [<number>] ap [<ap_number>] ike name local delete

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

[説明]

IKE セッションを確立する自装置名の削除を行います。

5.2.48　remote ap ike release

[機能]

IPsec / IKE 情報の解放動作の設定

[入力形式]

remote [<number>] ap [<ap_number>] ike release <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

IPsec / IKE の SA 情報の解放動作設定を指定します。

- on
  回線切断時に解放処理を行います。
- off
  解放処理は行いません。

[説明]

自動鍵設定で作成された SA 情報の解放動作設定を行います。
on を指定した場合は、回線切断時に自動鍵設定が使用している SA 情報の解放動作を行います。
off を指定した場合は、回線切断時に自動鍵設定が使用している SA 情報の解放動作を行いません。

[注意]

本コマンド は、以下の回線切断動作時に有効です。

- ISDN(回線交換) を使用した時の回線切断時

[未設定時]

回線切断時に IKE SA 情報の解放を行うものとみなされます。

```
remote <number> ap <ap_number> ike release on
```

5.2.49 remote ap ike initial

[機能]

IKE ネゴシエーション開始動作の設定

[入力形式]

remote [<number>] ap [<ap_number>] ike initial <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

IKE ネゴシエーション開始動作を指定します。

- forward
  IPsec 対象パケットの送信を契機として、IPsec/IKE SA の確立動作を開始します。
- connect
  対象回線の接続または IPsec 対象パケットの送信を契機として、IPsec/IKE SA の確立動作を開始します。

[説明]

IKE ネゴシエーションを開始する契機を設定します。
<mode>に connect を指定した場合、回線接続または IPsec 対象パケットの送信を契機として、IKE ネゴシエーションを開始し、IPsec/IKE SA の確立を行います。

[注意]

本コマンドは、以下の回線接続時に有効です。

- ISDN(回線交換) を使用した時

[未設定時]

IPsec 対象パケットの送信を契機として、IPsec/IKE SA の確立を行なうものとみなされます。

```
remote <number> ap <ap_number> ike initial forward
```

5.2.50　remote ap ike sessionwatch

[機能]

IKE セッション監視の設定

[入力形式]

remote [<number>] ap [<ap_number>] ike sessionwatch <address> [<normal_interval> [<abnormal_interval>]]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<address>

- ICMP ECHO パケットの宛先 IP アドレス
  ICMP ECHO パケットの宛先 IP アドレスを指定します。
  IPsec 対象範囲に含まれる IP アドレスを指定してください。
  0.0.0.0 を指定した場合は、IKE セッションを監視しないものとみなされます。

<normal_interval>

- ICMP ECHO パケットの正常時送信間隔
  ICMP ECHO パケットの正常時送信間隔を、1 秒～60 秒 (1 分) の範囲で指定します。
  単位は、m(分)、s(秒) のいずれかを指定します。
  省略した場合は、10 秒を指定したものとみなされます。

<abnormal_interval>

- ICMP ECHO パケットの異常時送信間隔
  ICMP ECHO パケットの異常時送信間隔を、60 秒～600 秒 (10 分) の範囲で指定します。
  単位は、m(分)、s(秒) のいずれかを指定します。
  省略した場合は、180 秒 (3 分) を指定したものとみなされます。

[説明]

IKE セッションの生存確認を行うための動作情報を設定します。
指定した宛先 IP アドレスに対して ICMP ECHO パケットの送受信で生存確認を行います。
ICMP ECHO パケットの応答が正常に受信できている間は正常時送信間隔で監視を行いますが、ICMP ECHO パケットの応答が受信できなくなると、障害発生とみなし監視先に関連する IPsec / IKE SA を解放し、異常時送信間隔で監視を行います。
ICMP ECHO パケットの応答が受信できた時を復旧とみなし、監視先に関連する IPsec / IKE SA の確立を行い、正常送信間隔での監視に戻ります。

[未設定時]

IKE セッションの生存を監視しないものとみなされます。

```
remote <number> ap <ap_number> ike sessionwatch 0.0.0.0 10s 3m
```

5.2.51　remote ap tunnel local

[機能]

トンネル利用時の自側のトンネルエンドポイントアドレスの設定

[入力形式]

remote [<number>] ap [<ap_number>] tunnel local <address>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<address>

- 自側のトンネルエンドポイントアドレス
  自側のトンネルエンドポイントとなる IPv4 アドレスを指定します。本装置に設定されている IP アドレスを指定してください。
  0.0.0.0 を指定した場合は、設定を削除します。
  なお、IPv6 アドレスは指定できません。

[説明]

指定したアクセスポイント定義にトンネル利用が設定されている場合に、そのトンネルの自側エンドポイントアドレスを設定します。
トンネルを利用して通信を行う場合は、本コマンドを必ず実行してください。

[未設定時]

自側のトンネルエンドポイントアドレスを設定しないものとみなされます。

5.2.52 remote ap tunnel remote

[機能]

トンネル利用時の相手側のトンネルエンドポイントアドレスの設定

[入力形式]

remote [<number>] ap [<ap_number>] tunnel remote <address>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<address>

- 相手側のトンネルエンドポイントアドレス
  相手側のトンネルエンドポイントとなる IPv4 アドレスを指定します。
  0.0.0.0 を指定した場合は、設定を削除します。
  なお、IPv6 アドレスは指定できません。

[説明]

指定したアクセスポイント定義にトンネル利用が設定されている場合に、そのトンネルの相手側エンドポイントアドレスを設定します。
トンネルを利用して通信を行う場合は、本コマンドを必ず実行してください。

[未設定時]

相手側のトンネルエンドポイントアドレスを設定しないものとみなされます。

5.3　PPP 関連情報

5.3.1　remote ppp compress

[機能]

データ圧縮機能の設定

[入力形式]

remote [<number>] ppp compress <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

- off
  データ圧縮機能を使用しない場合に指定します。
- on
  データ圧縮機能を使用する場合に指定します。

[説明]

データ圧縮機能を使用するかどうか設定します。

[注意]

MP を使用する場合、受信順序制御 (“5.3.7 remote ppp mp order” を参照) を有効にしてください。MP を使用し、かつ受信順序制御を使用しないと定義している場合、ヒストリ機能 (高圧縮のための機能) を使用できません。

[未設定時]

データ圧縮機能を使用しないものとみなされます。

```
remote <number> ppp compress off
```

5.3.2 remote ppp mp start

[機能]

MP 利用時における初期接続リンク数の設定

[入力形式]

remote [<number>] ppp mp start <link>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<link>

- MP 利用時の初期接続リンク数
  MP 利用時の初期接続リンク数を指定します。

[説明]

MP 利用時の初期接続リンク数を設定します。
MP 利用時に自装置から発信する場合、最初から接続を試みるリンク数を設定します。なお、発信に失敗した場合、再試行は行いません。

[未設定時]

初期接続リンク数として 1 を指定したものとみなされます。

```
remote <number> ppp mp start 1
```

5.3.3　remote ppp mp resource analog

[機能]

アナログ発着信時の縮退動作の設定

[入力形式]

remote [<number>] ppp mp resource analog <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<mode>

- on
  アナログ発着信時に縮退動作を行います。
- off
  アナログ発着信時に縮退動作を行いません。

[説明]

MP 接続時に、アナログ発着信による縮退動作を行うかどうかを設定します。

[注意]

着信において縮退を行う場合には、「通信中着信通知」の契約が必要です。

[未設定時]

アナログ発着信時に縮退動作を行わないものとみなされます。

```
remote <number> ppp mp resource analog off
```

5.3.4 remote ppp mp traffic use

[機能]

自動チャネル数制御の可否の設定

[入力形式]

remote [<number>] ppp mp traffic use <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

- on
  スループット BOD の機能を使用します。
- off
  スループット BOD の機能を使用しません。

[説明]

スループット BOD 機能を使用するかどうかを設定します。

[未設定時]

スループット BOD 機能を使用しないとみなされます。

```
remote <number> ppp mp traffic use off
```

5.3.5　remote ppp mp traffic increase

[機能]

リンク増加閾値の設定

[入力形式]

remote [<number>] ppp mp traffic increase <traffic> <time>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<traffic>

- 回線増加閾値
  単位時間当たりにおけるチャネル利用率を、0〜100 の 10 進数値で指定します。
  以下に、回線増加閾値の計算式を示します。
  チャネル利用率 (%) = 転送バイト量 ÷ 転送可能バイト数 × 100

<time>

- 増加猶予時間
  トラフィックが回線増加閾値を超え続けた場合に、発信するまでの猶予時間を 0 秒〜3600 秒の範囲で指定します。単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。

[説明]

スループット BOD 機能使用時におけるリンク増加閾値を設定します。
スループット BOD 機能を使用する場合は、本コマンドを必ず設定してください。

[注意]

指定した増加猶予時間の間、チャネル利用率が回線増加閾値を超え続けた場合にチャネル増加のための発信が行われます。

[未設定時]

回線増加閾値および猶予時間を設定しないものとみなされます。

5.3.6 remote ppp mp traffic decrease

[機能]

リンク減少閾値の設定

[入力形式]

remote [<number>] ppp mp traffic decrease <traffic> <time>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<traffic>

- 回線減少閾値
  単位時間当たりにおけるチャネル利用率を、0～100 の 10 進数値で指定します。
  以下に、回線減少閾値の計算式を示します。
  チャネル利用率 (%) = 転送バイト量 ÷ 転送可能バイト数 × 100

<time>

- 減少猶予時間
  トラフィックが回線減少閾値を超え続けた場合に、切断するまでの猶予時間を 0 秒～3600 秒の範囲で指定します。単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。

[説明]

スループット BOD 利用時におけるリンク減少閾値を設定します。
スループット BOD 機能を使用する場合は、本コマンドを必ず設定してください。

[注意]

設定された減少猶予時間の間、チャネル利用率が回線減少閾値を下回り続けた場合にチャネル減少が行われます。

[未設定時]

回線減少閾値および猶予時間を設定しないものとみなされます。

5.3.7　remote ppp mp order

[機能]

受信パケット順序制御の有無の設定

[入力形式]

remote [<number>] ppp mp order <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

- off
  順序制御をしない場合に指定します。
- on
  順序制御をする場合に指定します。

[説明]

MP 受信パケットの順序制御を行うかどうか設定します。

[注意]

以下に、MP 受信パケットの順序制御が無効になっていると動作に影響が出る機能を示します。

- ブリッジ機能
  順序に依存するプロトコルをブリッジによって通信する場合、通信が停止することがあります。
- VJ ヘッダ圧縮機能
  設定にかかわらず、常に VJ ヘッダ圧縮を使用しません。
- IP ヘッダ圧縮機能
  設定にかかわらず、常に IP ヘッダ圧縮を使用しません。
- データ圧縮機能
  LZS アルゴリズムで、ヒストリ機能 (高効率圧縮の機能) を使用しません。

[未設定時]

MP 受信パケットの順序制御をしないものとみなされます。

```
remote <number> ppp mp order off
```

5.3.8 remote ppp ipcp vjcomp

[機能]

VJ-Compression の利用の有無の設定

[入力形式]

remote [<number>] ppp ipcp vjcomp <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

- enable
  VJ ヘッダ圧縮を使用する場合に指定します。
- disable
  VJ ヘッダ圧縮を使用しない場合に指定します。

[説明]

VJ ヘッダ圧縮機能 (VJCOMP) を使用するかどうかを設定します。VJ ヘッダ圧縮機能は、RFC1144 に準拠しています。

[注意]

MP を使用する場合は、“5.3.7 remote ppp mp order” の<mode>に on を指定して、受信順序制御を使用してください。
MP を使用するにもかかわらず受信順序制御を使用しないと定義している場合、VJ ヘッダ圧縮機能は無条件に無効となります。

[未設定時]

VJ ヘッダ圧縮機能を使用するものとみなされます。

```
remote <number> ppp ipcp vjcomp enable
```

5.3.9　remote ppp ipcp iphc

[機能]

IPv4 における IP ヘッダ圧縮 (IPHC) の設定

[入力形式]

remote [<number>] ppp ipcp iphc <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

- enable
  IP ヘッダ圧縮を使用する場合に指定します。
- disable
  IP ヘッダ圧縮を使用しない場合に指定します。

[説明]

IPv4 において、IP ヘッダ圧縮 (IPHC) を使用するかどうかを設定します。IP ヘッダ圧縮機能は、圧縮方法が RFC2507 / RFC2508 に、ネゴシエーション方法が RFC2509 に準拠しています。

[注意]

MP を使用する場合は、“5.3.7 remote ppp mp order” の<mode>に on を指定して、受信順序制御を使用してください。

MP を使用するにもかかわらず受信順序制御を使用しないと定義している場合、IP ヘッダ圧縮機能は無条件に無効となります。

[未設定時]

IP ヘッダ圧縮機能を使用しないものとみなされます。

```
remote <number> ppp ipcp iphc disable
```

5.3.10 remote ppp ipv6cp iphc

[機能]

IPv6 における IP ヘッダ圧縮 (IPHC) の設定

[入力形式]

remote [<number>] ppp ipv6cp iphc <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

- enable
  IP ヘッダ圧縮を使用する場合に指定します。
- disable
  IP ヘッダ圧縮を使用しない場合に指定します。

[説明]

IPv6 において、IP ヘッダ圧縮 (IPHC) の使用するかどうかを設定します。
IP ヘッダ圧縮機能は、圧縮方法が RFC2507 / RFC2508 に、ネゴシエーション方法が RFC2509 に準拠しています。

[注意]

MP を使用する場合は、“5.3.7 remote ppp mp order” の<mode>に on を指定して、受信順序制御を使用してください。
MP を使用するにもかかわらず受信順序制御を使用しないと定義している場合、IP ヘッダ圧縮機能は無条件に無効となります。

[未設定時]

IPv6 ヘッダ圧縮機能を使用しないものとみなされます。

```
remote <number> ppp ipv6cp iphc disable
```

5.4　IP 関連情報

5.4.1　remote ip address local

[機能]

自側 IP アドレスの設定

[入力形式]

remote [<number>] ip address local <address>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<address>

- 自側 IP アドレス
  相手ネットワークでの自側 IP アドレスを指定します。
  0.0.0.0 を指定した場合は、設定を削除します。

[説明]

相手ネットワークでの自側 IP アドレスを設定します。

[未設定時]

IP アドレスなし (unnumbered) として動作します。

5.4.2 remote ip address remote

[機能]

相手側 IP アドレスの設定

[入力形式]

remote [<number>] ip address remote <address>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<address>

- 相手側 IP アドレス
  相手ネットワークでの相手側 IP アドレスを指定します。
  0.0.0.0 を指定した場合は、設定を削除します。

[説明]

相手ネットワークでの相手側 IP アドレスを設定します。

[未設定時]

相手装置のアドレスが任意のアドレスであるものとして扱います。相手装置にアドレスがない場合、IP アドレスを割り当てません。

5.4.3　remote ip route add

[機能]

IPv4 スタティックルーティング情報 (静的経路情報) の設定

[入力形式]

remote [<number>] ip route add <address> / <mask> [<metric> [<distance>]]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<address>/<mask>

- IPv4 アドレス / マスクビット数 (またはマスク値)
  宛先ネットワークを IPv4 アドレスとマスクビット数の組み合わせで指定します。
  マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。
  - IPv4 アドレス / マスクビット数 (例: 192.168.1.0 / 24)
  - IPv4 アドレス / マスク値 (例: 192.168.1.0 / 255.255.255.0)
- default
  宛先ネットワークとしてデフォルトルートを設定する場合に指定します。
  0.0.0.0 / 0(0.0.0.0 / 0.0.0.0) を指定するのと同じ意味になります。

<metric>

- RIP メトリック値
  このスタティックルーティング情報を RIP で広報する場合のメトリック値を、1～15 の 10 進数値で指定します。
  省略した場合は、1 を指定したものとみなされます。RIP 広報メトリック値は、以下の計算式で決定されます。
  - RIP 広報メトリック値=出力インタフェースの設定メトリック値+1+<metric>

<distance>

- 優先度
  このスタティックルーティング情報の優先度を、0～254 の 10 進数値で指定します。優先度は値が小さい方が高い優先度を示します。
  省略した場合は、0 を指定したものとみなされます。

[説明]

相手ネットワークに対して、IPv4 スタティックルーティング (静的経路) を設定します。<distance>で設定した優先度は、IPv4 ルーティングプロトコルで受信した経路の優先度と比較され同じ経路の場合は優先度の高い方が選択されます。

IPv4 スタティックルーティング情報は、本装置全体で 64 個まで定義できます。

[注意]

<address> / <mask>がまったく同じ宛先に対し、1 つのスタティックルーティング情報が設定できます。

[未設定時]

IPv4 スタティックルーティング情報を設定しないものとみなされます。

5.4.4 remote ip route modify

[機能]

IPv4 スタティックルーティング情報 (静的経路情報) の修正

[入力形式]

remote [<number>] ip route modify <old_address>/<old_mask> <new_address>/<new_mask> [<new_metric> [<new_distance>]]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<old_address>/<old_mask>

- IPv4 アドレス/マスクビット数 (またはマスク値)
  修正前の宛先ネットワークを IPv4 アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。
  以下に、有効な記述形式を示します。
  - IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
  - IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)
- default
  修正前の宛先ネットワークにデフォルトルートを設定している場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<new_address>/<new_mask>

- IPv4 アドレス/マスクビット数 (またはマスク値)
  新しい宛先ネットワークを IPv4 アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。
  - IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
  - IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)
- default
  新しい宛先ネットワークとしてデフォルトルートを設定する場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<new_metric>

- 新しいメトリック値
  新しいメトリック値を、1〜15 の 10 進数値で指定します。
  省略した場合は、1 を指定したものとみなされます。

<new_distance>

- 新しい優先度
  新しい優先度を、0〜254 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

[説明]

IPv4 スタティックルーティング情報を修正します。

5.4.5　remote ip route delete

[機能]

IPv4 スタティックルーティング情報 (静的経路情報) の削除

[入力形式]

remote [<number>] ip route delete <address> / <mask>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<address>/<mask>

- IPv4 アドレス / マスクビット数 (またはマスク値)
  削除する宛先ネットワークを IPv4 アドレスとマスクビット数の組み合わせで指定します。
- default
  デフォルトルートを削除する場合に指定します。
  0.0.0.0 / 0(0.0.0.0 / 0.0.0.0) を指定するのと同じ意味になります。
- all
  すべてのスタティックルーティングを削除する場合に指定します。

[説明]

IPv4 スタティックルーティング情報を削除します。

5.4.6 remote ip rip

[機能]

ダイナミックルーティング情報 (RIP) の設定

[入力形式]

remote [<number>] ip rip <send> <receive> <metric> [<ignore> [<password>]]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<send>

RIP の送信について指定します。

- v1
  RIPv1(Unicast または Broadcast) を送信します。自側 IP アドレスが設定されている場合は Unicast で送信します。設定されていない場合 (unnumbered) は Broadcast で送信します。
- v2
  RIPv2(Unicast または Broadcast) を送信します。自側 IP アドレスが設定されている場合は Unicast で送信します。設定されていない場合 (unnumbered) は Broadcast で送信します。
- v2m
  RIPv2(Multicast) を送信します。
- off
  RIP を送信しません。

<receive>

RIP の受信について指定します。

- v1
  RIPv1 を受信します。
- v2
  RIPv1, RIPv2 を受信します。
- off
  RIP を受信しません。

<metric>

- 加算メトリック値
  RIP 情報の加算メトリック値を、0〜16 の 10 進数値で指定します。
  RIP 広報メトリック値は、以下の計算式で決定されます。
  - RIP 広報メトリック値=RIP 受信パケットのメトリック値+1+<metric>

<ignore>

自装置に<password>を設定していないときに、パスワード付きの RIPv2 パケットを受信したときの破棄の動作を指定します。

省略した場合は、off を指定したものとみなされます。

- on

  受信した RIPv2 パケットを破棄します。

- off

  受信した RIPv2 パケットを破棄しません。

<password>

- RIPv2 パスワード

  <send>または<receive>に v2 を指定した場合のパスワードを、0x21,0x23～0x7e のコードで構成される 16 文字以内の ASCII 文字列で指定します。

  省略した場合は、パスワードなしとみなされます。

[説明]

相手ネットワークに、IPv4 ダイナミックルーティング情報 (RIP) を設定します。ダイナミックルーティングとはルータ間でルーティング情報をやりとりすることで、その都度最適なルートを選択してデータ通信を行う方法です。

[注意]

ISDN またはフレームリレー (従量課金) の場合、RIP 情報を送信すると、思わぬ課金 (定期発信または長時間接続) が発生します。

"remote mtu"で MTU 値を 576 よりも小さい値に設定すると、RIPv1(Broadcast), RIPv2(Broadcast) のパケットを送信しない場合があります。MTU 値は 576 以上を設定してください。

[未設定時]

IPv4 ダイナミックルーティング (RIP) を使用しないものとみなされます。

```
remote <number> ip rip off off 0 off
```

5.4.7 remote ip nat mode

[機能]

アドレス変換の設定

[入力形式]

remote [<number>] ip nat mode <mode> [<address> <addr_number> [<time>]]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

アドレス変換 (NAT) を使用するかどうかを設定します。

- off
  NAT を使用しません。
- nat
  NAT を使用します。
- multi
  マルチ NAT を使用します。

<address>

- 先頭グローバル IP アドレス
  動的変換に使用するグローバル IP アドレスの先頭アドレスを指定します。
- any
  グローバル IP アドレスの先頭アドレスとして IPCP ネゴシエーションの結果を使用します。

<addr_number>

- グローバル IP アドレスの個数
  動的変換に使用するグローバル IP アドレスの個数を、1～16 の 10 進数値で指定します。

<time>

- 割当時間
  割り当てられた変換テーブルを解放するための無通信監視時間を、0 秒～86400 秒 (1 日) の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。0 秒を指定した場合は、変換テーブル解放のための監視を行いません。
  省略した場合は、5 分を指定したものとみなされます。

[説明]

相手ネットワークに対するアドレス変換 (NAT) の動作を設定します。

[未設定時]

アドレス変換は使用しないものとみなされます。

```
remote <number> ip nat mode off
```

5.4.8　remote ip nat static

[機能]

静的アドレス変換の設定

[入力形式]

remote [<number>] ip nat static <count> <private_addr> <private_port>
<global_addr> <global_port> [<protocol>]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 静的アドレス変換定義番号
  静的アドレス変換定義番号を、0〜63 の 10 進数値で指定します。

<private_addr>

- プライベート IP アドレス
  静的アドレス変換の対象となるプライベート側の IP アドレスを指定します。

<private_port>

- プライベートポート番号
  静的アドレス変換の対象となるプライベート側のポート番号を、1〜65535 の 10 進数値で指定します。
  グローバルポート番号に複数ポート番号を指定した場合には、変換後の複数ポートの先頭ポート番号を指定します。
- any すべてのプライベートポート番号に対して有効な設定となります。

<global_addr>

- グローバル IP アドレス
  静的アドレス変換の対象となるグローバル側の IP アドレスを指定します。
- any すべてのグローバル IP アドレスに対して有効な設定となります。

<global_port>

- グローバルポート番号
  静的アドレス変換の対象となるグローバル側のポート番号を、1〜65535 の 10 進数値で指定します。
  複数個のアドレスを設定する場合には 1000-1200 のようにハイフンで結んで指定します。なお、ポート番号の範囲指定は一組のみ指定可能です。
- any
  すべてのグローバルポート番号に対して有効な設定となります。

<protocol>

- プロトコル番号
  静的アドレス変換の対象となるプロトコル番号を指定します。
  省略した場合は、any を指定したものとみなされます。
- any
  すべてのプロトコル番号に対して有効な設定となります。

[説明]

相手ネットワークに対する静的アドレス変換を設定します。

静的アドレス変換の対象となるパケットは、プロトコル番号<protocol>のプライベート側の IP アドレス <private_addr> とポート番号 <private_port>、グローバル側の IP アドレス<global_addr>とポート番号 <global_port>の指定内容により交換されます。

静的アドレス変換は、本装置全体で 64 個まで定義できます。

[未設定時]

静的アドレス変換は設定されません。

5.4.9　remote ip nat static delete

[機能]

静的アドレス変換の削除

[入力形式]

remote [<number>] ip nat static delete <count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 静的アドレス変換定義番号
  静的アドレス変換定義番号を、0～63 の 10 進数値で指定します。
- all
  すべての静的アドレス変換定義番号を削除対象とします。

[説明]

指定した静的アドレス変換を削除します。

5.4.10 remote ip nat rule

[機能]

アドレス変換ルールの設定

[入力形式]

remote [<number>] ip nat rule <count> ftp <server_addr>
[<server_start_port>]-[<server_end_port>] [<check>]
remote [<number>] ip nat rule <count> ftp <server_addr> <server_port> [<check>]
remote [<number>] ip nat rule <count> irc <server_addr>
[<server_start_port>]-[<server_end_port>]
remote [<number>] ip nat rule <count> irc <server_addr> <server_port>
remote [<number>] ip nat rule <count> dns <server_addr>
[<server_start_port>]-[<server_end_port>] [<check>]
remote [<number>] ip nat rule <count> dns <server_addr> <server_port> [<check>]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 変換ルール番号
  変換ルール番号を、0～31 の 10 進数値で指定します。

ftp, irc, dns

変換ルールの対象となるアプリケーションを指定します。

<server_addr>

- IP アドレス
  NAT に割り当てたグローバルアドレス以外のアドレスを指定します。ここで指定したアドレスを変換ルールの対象とします。
- any
  すべての IP アドレスを変換ルールの対象とします。
  any を指定した場合は、グローバル側とプライベート側の両方のアプリケーションサーバに対応します。
- global
  NAT に割り当てたグローバルアドレス以外のすべてのアドレスを変換ルールの対象とします。
  global を指定した場合には、グローバル側のアプリケーションサーバに対応します。
- local
  NAT に割り当てたグローバルアドレスを変換ルールの対象とします。local を指定した場合には、プライベート側のアプリケーションサーバに対応します。
- off
  指定したアプリケーションに対する変換ルールを無効にします。

<server_start_port>

アプリケーションサーバで待ち受けるポートの範囲指定の開始番号を示します。

<server_end_port>

アプリケーションサーバで待ち受けるポートの範囲指定の終了番号を示します。

<server_port>

アプリケーションサーバで待ち受けるポート番号を示します。

<check>

- on

  アプリケーションに ftp を指定した場合、ftp サーバのデータ転送用 IP アドレス及びポート番号のチェックを行います。

  アプリケーションに dns を指定した場合、グローバル側にサーバが存在するときのみ有効となります。DNS の応答の UDP パケットのソース IP アドレス及びソースポート番号が問い合わせの UDP パケットのディスティネーション IP アドレス及びディスティネーションポート番号と同一かどうかチェックします。

  省略した場合は、on を指定したものとみなされます。

- off

  アプリケーションに ftp を指定した場合、ftp サーバのデータ転送用 IP アドレス及びポート番号のチェックを行いません。

  アプリケーションに dns を指定した場合、IP アドレス及びポート番号のチェックを行いません。

[説明]

相手ネットワークに対するアドレス変換ルールを設定します。

指定 IP アドレス、指定ポート番号で動作する指定アプリケーションに対応するサーバに対するアドレス変換の特殊対応の設定を行います。

アドレス変換ルールは、本装置全体で 32 個まで定義できます。

[未設定時]

アドレス変換ルールは設定されません。

5.4.11 remote ip nat rule delete

[機能]

アドレス変換ルールの削除

[入力形式]

remote [<number>] ip nat rule delete <count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 変換ルール番号
  削除する変換ルール番号を、0～31 の 10 進数値で指定します。
- all
  すべての変換ルールを削除対象とします。

[説明]

指定したアドレス変換ルールを削除します。

5.4.12　remote ip filter

[機能]

IP フィルタの設定

[入力形式]

remote [<number>] ip filter <count> <action> <src_addr>/<mask> <src_port> <dst_addr>/<mask> <dst_port> <protocol> <tcpconnect> [<tos>]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す番号を、0〜63 の 10 進数値で指定します。指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つフィルタリング定義が既に存在する場合は、既存の定義を変更します。

<action>

フィルタリング対象に該当するパケットを透過するかどうかを設定します。

- pass
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。
- restrict
  該当するパケットを、回線が接続されていれば透過し、切断されていれば遮断します。

<src_addr>/<mask>

フィルタリング対象とする送信元 IP アドレスとマスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  フィルタリング対象とする送信元 IP アドレスとマスクビット数の組み合わせを指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。
  以下に、有効な記述形式を示します。
  - IP アドレス/マスクビット数 (例: 192.168.1.1/24)
  - IP アドレス/マスク値 (例: 192.168.1.1/255.255.255.0)
- any
  すべての送信元 IP アドレスをフィルタリング対象とする場合に指定します。0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<src_port>

フィルタリング対象とする送信元ポート番号を指定します。

- ポート番号

  フィルタリング対象とする送信元ポート番号を、1〜65535 の 10 進数値で指定します。複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。

  ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。

  以下に、有効な記述形式を示します。

  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)

- any

  すべての送信元ポート番号をフィルタリング対象とする場合に指定します。

<dst_addr>/<mask>

フィルタリング対象とする宛先 IP アドレスとマスクビット数を指定します。

- IP アドレス / マスクビット数 (またはマスク値)

  フィルタリング対象とする宛先 IP アドレスとマスクビット数の組み合わせを指定します。

  記述形式は、<src_addr> / <mask>と同様です。

- any

  すべての宛先 IP アドレスをフィルタリング対象とする場合に指定します。0.0.0.0 / 0(0.0.0.0 / 0.0.0.0) を指定するのと同じ意味になります。

<dst_port>

フィルタリング対象とする宛先ポート番号を指定します。

- ポート番号

  フィルタリング対象とする宛先ポート番号を、1〜65535 の 10 進数値で指定します。

  記述形式は、<src_port>と同様です。

- any

  すべての宛先ポート番号をフィルタリング対象とする場合に指定します。

<protocol>

フィルタリング対象とするプロトコル番号を指定します。

- プロトコル番号

  フィルタリング対象とするプロトコル番号を、0〜255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。

  0 を指定した場合は、すべてのプロトコルをフィルタリング対象とします。

<tcpconnect>

- yes

  TCP プロトコルでコネクション接続要求をフィルタリング対象に含めます。

- no

  TCP プロトコルでコネクション接続要求をフィルタリング対象に含めません。

<tos>

フィルタリング対象とする TOS 値を指定します。
省略した場合は、any を指定したものとみなされます。

- TOS 値
  フィルタリング対象とする TOS 値を、0〜ff の 16 進数値で指定します。複数の TOS 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。
  TOS 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 00〜ff の 16 進数値 (例: ff = ff の TOS 値)
  - TOS 値-TOS 値 (例: 32-64 = 32 から 64 までの TOS 値)
  - TOS 値- (例: 80- = 80 から ff までの TOS 値)
  - -TOS 値 (例: -7f = 0 から 7f までの TOS 値)
  - TOS 値,TOS 値,… (例: 10,20,30- = 10 と 20 と 30 以降の TOS 値)
- any
  すべての TOS 値をフィルタリング対象とする場合に指定します。

[説明]

相手ネットワークに対する IP フィルタを設定します。
IP フィルタは、指定したアドレス、ポート番号、プロトコル、TOS 値と一致するパケットを透過あるいは遮断します。設定した優先度順に一致するか調べ、一致した時点でフィルタリングされ、それ以降の設定は参照されません。
IP フィルタは、本装置全体で 64 個まで定義できます。

[未設定時]

IP フィルタを設定しないものとみなされ、すべてのパケットが透過します。

5.4.13 remote ip filter move

[機能]

IP フィルタの優先順序の変更

[入力形式]

remote [<number>] ip filter move <count> <new_count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義の番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
  <count>に対する新しい順序を、0～63 の 10 進数値で指定します。
  既にこの定義番号を持つ定義が存在する場合には、その定義の前に挿入されます。

[説明]

IP フィルタの優先順序を変更します。

5.4.14　remote ip filter delete

[機能]

IP フィルタの削除

[入力形式]

remote [<number>] ip filter delete <count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

削除するフィルタリングを指定します。

- フィルタリング定義番号
  削除するフィルタリングの定義番号を指定します。
- all
  すべてのフィルタリングを削除する場合に指定します。

[説明]

IP フィルタを削除します。

5.4.15 remote ip tos

[機能]

TOS 値書き換え条件の設定

[入力形式]

remote [<number>] ip tos <count> <src_addr>/<mask> <src_port> <dst_addr>/<mask> <dst_port> <protocol> <tos> <new_tos>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- TOS 値書き換え定義番号
  TOS 値書き換え条件の優先度を表す定義番号を、0〜31 の 10 進数値で指定します。
  指定した値は、設定完了時に順方向にソートされてリナンバリングされます。また、指定した定義番号と同じ値を持つ TOS 値書き換え定義が既に存在する場合は、既存定義の値を変更します。

<src_addr>/<mask>

- IP アドレス/マスクビット数 (またはマスク値)
  TOS 値書き換え対象となる送信元 IP アドレスとマスクビット数の組み合わせを指定します。マスク値は最上位ビットから 1 で連続した値にしてください。
  以下に、有効な記述形式を示します。
  - IP アドレス/マスクビット数 (例: 192.168.1.1/24)
  - IP アドレス/マスク値 (例: 192.168.1.1/255.255.255.0)
- any
  すべての送信元 IP アドレスを TOS 値書き換えの対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<src_port>

TOS 値書き換え対象となる送信元ポート番号を指定します。

- ポート番号
  TOS 値書き換え対象となる送信元ポート番号を、1〜65535 の 10 進数値で指定します。複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。
  ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)
- any
  すべてのポート番号を対象とする場合に指定します。

<dst_addr>/<mask>

TOS 値書き換え対象となる宛先 IP アドレス、マスクビット数を指定します。

- IP アドレス / マスクビット数 (またはマスク値)
  TOS 値書き換え対象となる宛先 IP アドレスとマスクビット数の組み合わせを指定します。
  記述形式は、<src_addr>/<mask>と同様です。
- any
  すべての宛先 IP アドレスを TOS 値書き換えの対象とする場合に指定します。0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<dst_port>

TOS 値書き換え対象となる宛先ポート番号を指定します。

- ポート番号
  TOS 値書き換え対象となる宛先ポート番号を、1〜65535 の 10 進数値で指定します。
  記述形式は、<src_port>と同様です。
- any
  すべてのポート番号を対象とする場合に指定します。

<protocol>

- プロトコル番号
  TOS 値書き換え対象となるプロトコル番号を、0〜255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。0 を指定した場合は、すべてのプロトコルを対象とします。

<tos>

- TOS 値
  書き換え対象となる TOS 値を、0〜ff の 16 進数値で指定します。複数の TOS 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。
  TOS 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 00〜ff の 16 進数値 (例: ff = ff の TOS 値)
  - TOS 値-TOS 値 (例: 32-64 = 32 から 64 までの TOS 値)
  - TOS 値- (例: 80- = 80 から ff までの TOS 値)
  - -TOS 値 (例: -7f = 0 から 7f までの TOS 値)
  - TOS 値,TOS 値,… (例: 10,20,30- = 10 と 20 と 30 以降の TOS 値)
- any
  すべての TOS 値を、TOS 値書き換えの対象とする場合に指定します。

<new_tos>

- TOS 値
  書き換える TOS 値を、0〜ff の 16 進数値で指定します。

[説明]

TOS 値書き換え条件を設定します。
条件に一致したパケットの TOS 値を、指定した TOS 値に書き換えます。TOS 値書き換え条件は、本装置全体で 32 個まで定義できます。

[未設定時]

TOS 値書き換えを行わないものとみなされます。

5.4.16 remote ip tos move

[機能]

TOS 値書き換え条件の優先度の変更

[入力形式]

remote [<number>] ip tos move <count> <new_count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 対象 TOS 値書き換え定義番号
  優先順序を変更する前の TOS 値書き換え定義番号を指定します。

<new_count>

- 移動先 TOS 値書き換え定義番号
  <count>に対する新しい順序を、0～31 の 10 進数値で指定します。
  既にこの定義番号を持つ定義が存在する場合には、その定義の前に挿入されます。

[説明]

TOS 値書き換え条件の優先度を変更します。

5.4.17　remote ip tos delete

[機能]

TOS 値書き換え条件の削除

[入力形式]

remote [<number>] ip tos delete <count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- TOS 値書き換え定義番号
  削除する TOS 値書き換え定義番号を指定します。
- all
  すべての TOS 値書き換え定義を削除する場合に指定します。

[説明]

TOS 値書き換え条件を削除します。

5.4.18 remote ip priority

[機能]

帯域制御の設定

[入力形式]

remote [<number>] ip priority <count> <src_addr>/<mask> <src_port> <dst_addr>/<mask> <dst_port> <protocol> <tos> <width>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 帯域制御定義番号
  帯域制御定義番号を、0〜63 の 10 進数値で指定します。

<src_addr>/<mask>

帯域制御の対象となる送信元 IP アドレス、マスクビット数を指定します。

- 送信元 IP アドレス/マスクビット数 (またはマスク値)
  帯域制御の対象となる送信元 IP アドレスとマスクビット数の組み合わせを指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。
  以下に、有効な記述形式を示します。
  - IP アドレス/マスクビット数 (例: 192.168.1.1/24)
  - IP アドレス/マスク値 (例: 192.168.1.1/255.255.255.0)
- any
  すべての IP アドレスを帯域制御の対象とする場合に指定します。0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<src_port>

帯域制御の対象となる送信元ポート番号を指定します。

- ポート番号
  帯域制御の対象となる送信元ポート番号を、1〜65535 の 10 進数値で指定します。複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)
- any
  すべてのポート番号を対象とする場合に指定します。

<dst_addr>/<mask>

帯域制御の対象となる宛先 IP アドレス、マスクビット数を指定します。

- 宛先 IP アドレス/マスクビット数 (またはマスク値)
  帯域制御の対象となる宛先 IP アドレスとマスクビット数の組み合わせを指定します。
  記述形式は<src_addr>/<mask>と同様です。
- any
  すべての IP アドレスを帯域制御の対象とする場合に指定します。0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<dst_port>

帯域制御の対象となる宛先ポート番号を指定します。

- ポート番号
  帯域制御の対象となる宛先ポート番号を、1〜65535 の 10 進数値で指定します。
  記述形式は<src_port>と同様です。
- any
  すべてのポート番号を対象とする場合に指定します。

<protocol>

- プロトコル番号
  帯域制御の対象となるプロトコル番号を、0〜255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。
  0 を指定した場合は、すべてのプロトコルを対象とします。

<tos>

- TOS 値
  帯域制御の対象となる TOS 値を、0〜ff の 16 進数値で指定します。複数の TOS 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。
  TOS 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 00〜ff の 16 進数値 (例: ff = ff の TOS 値)
  - TOS 値-TOS 値 (例: 32-64 = 32 から 64 までの TOS 値)
  - TOS 値- (例: 80- = 80 から ff までの TOS 値)
  - -TOS 値 (例: -7f = 0 から 7f までの TOS 値)
  - TOS 値,TOS 値,… (例: 10,20,30- = 10 と 20 と 30 以降の TOS 値)
- any
  すべての TOS 値を、帯域制御の対象とする場合に指定します。

<width>

- 帯域
  0〜100 の 10 進数値で指定した場合、0 は非優先 (ベストエフォート)、100 は最優先、1〜99 は同じ相手ネットワーク中の定義となり、それぞれ指定した値の比で帯域を割り当てます。例えば、同じ相手ネットワーク中の定義が 3 つあり、それぞれ<width>の値が 30、30、60 であった場合、帯域として 25%、25%、50%が割り当てられます。なお、1〜99 を指定した定義のそれぞれの合計値が 100 未満の場合、残った帯域は定義に合致しないデータ用の帯域となります。

[説明]

帯域制御を設定します。任意のプロトコル、アドレス、ポート、TOS 値を指定して、割り当てる帯域を指定します。

帯域制御は、本装置全体で 64 個まで定義できます。

[注意]

IPv4 以外のパケットは、すべて非優先 (ベストエフォート) として扱われます。

[未設定時]

帯域制御を行わないものとみなされます。

5.4.19　remote ip priority delete

[機能]

帯域制御の削除

[入力形式]

remote [<number>] ip priority delete <count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

削除する帯域制御を指定します。

- 削除する帯域制御定義番号
  削除する帯域制御定義番号を指定します。
- all
  すべての帯域制御を削除する場合に指定します。

[説明]

帯域制御を削除します。

5.4.20 remote ip msschange

[機能]

MSS 書き換えの設定

[入力形式]

remote [<number>] ip msschange <mss>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mss>

- MSS 値
  MSS の書き換え値を、0 または 160～1460 の 10 進数値で指定します。
  0 を指定した場合は、MSS を書き換えません。

[説明]

MSS 書き換え機能を利用する場合の、書き換え値を設定します。

[未設定時]

MSS 書き換え機能を利用しないものとみなされます。

```
remote <number> ip msschange 0
```

5.5　IPv6 関連情報

5.5.1　remote ip6 use

[機能]

IPv6 機能の設定

[入力形式]

remote [<number>] ip6 use <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

IPv6 パケットの送受信を行うかどうか指定します。

- on
  このインタフェースで、IPv6 パケットの送受信を行います。
- off
  このインタフェースで、IPv6 パケットの送受信を行いません。

[説明]

このインタフェースで、IPv6 機能を利用するかどうかを設定します。

[未設定時]

IPv6 機能を利用しないものとみなされます。

```
remote <number> ip6 use off
```

5.5.2 remote ip6 ifid

[機能]

IPv6 インタフェース ID の設定

[入力形式]

remote [<number>] ip6 ifid <interfaceID>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<interfaceID>

このインタフェースで利用する ID を指定します。

- auto
  本装置が持つ MAC アドレスから、EUI-64 形式の ID を自動生成する場合に指定します。
- インタフェース ID
  このインタフェースで利用する ID を、16 進数値で指定します。4 桁ずつ":"(コロン) で区切ってください。なお、各フィールドの先頭の 0 は省略できます (例: 2a0:c9ff:fe84:759)。

通常は auto を指定してください。特定のインタフェース ID を指定する場合は、同一の link 上でホストと衝突しない値を指定してください。

[説明]

このインタフェースで利用する、インタフェース ID を設定します。

[未設定時]

インタフェース ID を自動生成するものとみなされます。

```
remote <number> ip6 ifid auto
```

5.5.3　remote ip6 address

[機能]

IPv6 アドレスの設定

[入力形式]

remote [<number>] ip6 address <count> <address> / <prefixlen> <valid> <preferred> [<flags>]

[パラメタ]

<number>

- remote 定義番号
  remote 定義の通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- IPv6 アドレス定義番号
  IPv6 アドレスの定義番号を、0〜3 の 10 進数値で指定します。

<address>

- IPv6 アドレス
  128-bit の IPv6 アドレスを指定します。

<prefixlen>

- プレフィックス長
  IPv6 アドレスに対するプレフィックス長として、64 を指定します。

<valid>

- valid lifetime の時間
  このインタフェースから RA(Router Advertisement メッセージ) を送信するときに、このプレフィックスに対する valid lifetime を、0 秒〜365 日の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。
- infinity
  このインタフェースから RA を送信するときに、このプレフィックスに対する valid lifetime を無限とする場合に指定します。

<preferred>

- preferred lifetime の時間
  このインタフェースから RA を送信する場合に、このプレフィックスに対する preferred lifetime を、0 秒〜365 日の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。<preferred>は、<valid>よりも短い時間となるように設定してください。<preferred>が<valid>よりも大きい場合、<valid>と同じ時間として扱われます。
- infinity
  このインタフェースから RA を送信する場合に、このプレフィックスに対する preferred lifetime を無限とします。

<flags>

- RA Prefix Information に付与されるフラグ
  このインタフェースから RA を送出する場合に、この prefix に対する flags フィールドの値を 16 進数値で設定します。
  省略した場合は、c0 を指定したものとみなされます。

[説明]

このインタフェースにおける IPv6 アドレスを設定します。<address>の指定において、<prefixlen>以降がすべて 0 の場合には、指定した値は IPv6 プレフィックスであると判断されます。この IPv6 プレフィックスとインタフェース ID によって、IPv6 アドレスが生成されます。

[未設定時]

Link local アドレス以外の IPv6 アドレスを設定しないものとみなされます。

5.5.4　remote ip6 address delete

[機能]

IPv6 アドレスの削除

[入力形式]

remote [<number>] ip6 address delete <count>

[パラメタ]

<number>

- remote 定義番号
  remote 定義の通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- IPv6 アドレス定義番号
  削除する IPv6 アドレスの定義番号を指定します。
- all
  すべての IPv6 アドレスを削除する場合に指定します。

[説明]

IPv6 アドレスを削除します。

5.5.5 remote ip6 ra mode

[機能]

Router Advertisement の動作の設定

[入力形式]

remote [<number>] ip6 ra mode <mode>

[パラメタ]

<number>

- remote 定義番号
  lan 定義の通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

- off
  RA の送信を行いません。
  定期送信、および host からの RS に対する RA の送信を行いません。
- send
  RA の送信を行います。
  定期送信、および host からの RS に対する RA の送信を行います。

[説明]

RA(Router Advertisement メッセージ) を送信するかどうかを設定します。

[未設定時]

RA の送信を行わないものとみなされます。

```
remote <number> ip6 ra mode off
```

5.5.6　remote ip6 ra interval

[機能]

Router Advertisement メッセージ送信間隔の設定

[入力形式]

remote [<number>] ip6 ra interval <max> <min> <lifetime>

[パラメタ]

<number>

- remote 定義番号
  remote 定義の通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<max>

- 最大送信間隔
  RA を定期送信する場合の最大送信間隔 (秒) を、4〜1800 の 10 進数値で設定します。

<min>

- 最小送信間隔
  RA を定期送信する場合の最小送信間隔 (秒) を、3〜<max>× 3/4 の 10 進数値で設定します。

<lifetime>

- Router Lifetime の値
  送信する RA の Router Lifetime の値を、0 または<max>〜9000 の 10 進数値で設定します。

[説明]

RA の送信間隔、および RA の Router Lifetime の値の設定を行います。RA は<min>〜<max>でランダムに決定された間隔で定期送信されます。

[未設定時]

最大送信間隔に 600 秒、最小送信間隔に 200 秒、Router Lifetime の値に 1800 が設定されたものとみなされます。

```
remote <number> ip6 ra interval 600 200 1800
```

5.5.7 remote ip6 ra mtu

[機能]

Router Advertisement メッセージに含める MTU option の設定

[入力形式]

remote [<number>] ip6 ra mtu <mtu>

[パラメタ]

<number>

- remote 定義番号
  remote 定義の通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mtu>

- MTU option の内容
  RA に含める MTU option の値を、0 または 1280～1500 の 10 進数値で設定します。
  0 を指定した場合は、RA に MTU option を含めません。

[説明]

RA に含める MTU option の値を設定します。

[未設定時]

送信する RA に MTU option を含めないものとみなされます。

```
remote <number> ip6 ra mtu 0
```

5.5.8　remote ip6 ra reachabletime

[機能]

Router Advertisement メッセージに含める Reachable Time の設定

[入力形式]

remote [<number>] ip6 ra reachabletime <time>

[パラメタ]

<number>

- remote 定義番号
  remote 定義の通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time>

- Reachable Time の値
  RA に含める Reachable Time の値を、0～3600000 の 10 進数値で設定します。

[説明]

RA に含める Reachable Time の値を設定します。

[未設定時]

Reachable Time の値として 0 が設定されたものとみなされます。

```
remote <number> ip6 ra reachabletime 0
```

5.5.9 remote ip6 ra retranstimer

[機能]

Router Advertisement メッセージに含める Retrans Timer の設定

[入力形式]

remote [<number>] ip6 ra retranstimer <time>

[パラメタ]

<number>

- remote 定義番号
  remote 定義の通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time>

- Retrans Timer の値
  RA に含める Retrans Timer の値を、0～4294967295 の 10 進数値で設定します。

[説明]

RA に含める Retrans Timer の値を設定します。

[未設定時]

Retrans Timer の値として 0 が設定されたものとみなされます。

```
remote <number> ip6 ra retranstimer 0
```

5.5.10　remote ip6 ra curhoplimit

[機能]

Router Advertisement メッセージに含める Cur Hop Limit の設定

[入力形式]

remote [<number>] ip6 ra curhoplimit <CurHopLimit>

[パラメタ]

<number>

- remote 定義番号
  remote 定義の通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<CurHopLimit>

- Cur Hop Limit の値
  RA に含める Cur Hop Limit の値を、0～255 の 10 進数値で設定します。

[説明]

RA に含める Cur Hop Limit の値を設定します。

[未設定時]

Cur Hop Limit の値として 64 が設定されたものとみなされます。

```
remote <number> ip6 ra curhoplimit 64
```

5.5.11 remote ip6 ra flags

[機能]

Router Advertisement メッセージに含める flags field の設定

[入力形式]

remote [<number>] ip6 ra flags <flags>

[パラメタ]

<number>

- remote 定義番号
  remote 定義の通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<flags>

- flags field の値
  RA に含める flags field の値を、00～ff の 16 進数値で設定します。

[説明]

RA に含める flags field の値を設定します。

[未設定時]

flags field の値として 00 が設定されたものとみなされます。

```
remote <number> ip6 ra flags 00
```

5.5.12　remote ip6 route add

[機能]

IPv6 スタティックルーティング情報 (静的経路情報) の設定

[入力形式]

remote [<number>] ip6 route add <address>/<prefixlen> [<metric>]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<address>/<prefixlen>

- IPv6 アドレス/プレフィックス
  宛先ネットワークを IPv6 アドレスとプレフィックスの組み合わせを指定します。
- default
  宛先ネットワークとしてデフォルトルートを設定する場合に指定します。::/0 を指定するのと同じ意味になります。

<metric>

- メトリック値
  このスタティックルーティング情報を RIPng で広報する場合のメトリック値を、1〜15 の 10 進数値で指定します。
  省略した場合は、1 を指定したものとみなされます。
  RIPng 広報メトリック値は、以下の計算式で決定されます。
  - RIPng 広報メトリック値=出力インタフェースの設定メトリック値+1+<metric>

[説明]

IPv6 スタティックルーティング情報 (静的経路情報) を設定します。
IPv6 スタティックルーティング情報は、本装置全体で 64 個まで定義できます。

[未設定時]

IPv6 スタティックルーティング情報を設定しないものとみなされます。

5.5.13 remote ip6 route modify

[機能]

IPv6 スタティックルーティング情報 (静的経路情報) の修正

[入力形式]

remote [<number>] ip6 route modify <old_address> / <old_prefixlen>
<new_address> / <new_prefixlen> [<new_metric>]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<old_address>/<old_prefixlen>

修正前の IPv6 アドレスとプレフィックスの組み合わせを指定します。

- IPv6 アドレス/プレフィックス
  既に定義されている宛先ネットワークの IPv6 アドレスとプレフィックスの組み合わせを指定します。
- default
  宛先ネットワークとしてデフォルトルートを登録する場合に指定します。
  :: / 0 を指定するのと同じ意味になります。

<new_address>/<new_prefixlen>

新しい IPv6 アドレスとプレフィックスの組み合わせを指定します。

- IPv6 アドレス/プレフィックス長
  新しい宛先ネットワークを IPv6 アドレスとプレフィックス長の組み合わせで指定します。
- default
  宛先ネットワークとしてデフォルトルートを登録する場合に指定します。
  :: / 0 を指定するのと同じ意味になります。

<new_metric>

- 新しいメトリック値
  新しいメトリック値を、1〜15 の 10 進数値で指定します。
  省略した場合は、1 を指定したものとみなされます。

[説明]

IPv6 スタティックルーティング情報 (静的経路情報) を修正します。

5.5.14　remote ip6 route delete

[機能]

IPv6 スタティックルーティング情報 (静的経路情報) の削除

[入力形式]

remote [<number>] ip6 route delete <address>/<prefixlen>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<address>/<prefixlen>

削除する IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス/プレフィックス長
  削除する IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- all
  すべてのスタティックルーティングを削除する場合に指定します。

[説明]

IPv6 スタティックルーティング情報 (静的経路情報) を削除します。

5.5.15 remote ip6 ripng

[機能]

ダイナミックルーティング情報 (RIPng) の設定

[入力形式]

remote [<number>] ip6 ripng <send> <receive> [<site> [<metric>]]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<send>

RIPng パケットを定期送信するかどうか指定します。

- on
  RIPng パケットを定期送信します。
- off
  RIPng パケットを定期送信しません。

<receive>

RIPng パケットを受信するかどうか指定します。

- on
  RIPng パケットを受信します。
- off
  RIPng パケットを受信しません。

<site>

site-local prefix を送受信するかどうか指定します。

- on
  site-local prefix を送受信します。
- off
  site-local prefix を送受信しません。

<send>および<receive>に off を指定した場合は、本パラメタにも off を指定してください。
省略した場合は、off を指定したものとみなされます。

<metric>

- 加算メトリック値
  RIPng 情報の加算メトリック値を、0～16 の 10 進数値で指定します。<send>に off を指定した場合は省略できます。
  省略した場合は、0 を指定したものとみなされます。
  RIPng 広報メトリック値は、以下の計算式で決定されます。
  - RIPng 広報メトリック値=RIPng 受信パケットのメトリック値+1+<metric>

[説明]

IPv6 ダイナミックルーティングの動作を設定します。

[未設定時]

IPv6 ダイナミックルーティング機能を使用しないものとみなされます。

```
remote <number> ip6 ripng off off off 0
```

5.5.16 remote ip6 aggregate

[機能]

ダイナミックルーティング情報 (RIPng) における経路集約の設定

[入力形式]

remote [<number>] ip6 aggregate <count> <address> / <prefixlen> <rejectroute>

[パラメタ]

<number>

- remote 定義番号
  remote 定義の通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 集約経路定義番号
  集約経路の定義番号を、0〜3 の 10 進数値で指定します。

<address>/<prefixlen>

- IPv6 アドレス/プレフィックス長
  集約経路の宛先ネットワークを IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- default
  集約経路としてデフォルトルートを登録する場合に指定します。
  :: / 0 を指定するのと同じ意味になります。

<rejectroute>

- on
  集約経路に対する破棄経路を設定します。
- off
  集約経路に対する破棄経路を設定しません。

[説明]

RIPng における集約経路の設定を行います。
集約経路が設定された場合には、設定された集約経路に含まれる個々の経路は広報されず、集約経路だけを広報します。また、集約経路と等しいネットワークに対する経路情報を持たない場合には、実際に持たない宛先に対するパケットを破棄するために、設定された集約経路に対する破棄経路を設定することもできます。
同一 remote 定義内に同一の集約経路は設定できません。

[未設定時]

経路集約は行わないものとみなされます。

5.5.17　remote ip6 aggregate delete

[機能]

ダイナミックルーティング情報 (RIPng) における経路集約の削除

[入力形式]

remote [<number>] ip6 aggregate delete <count>

[パラメタ]

<number>

- remote 定義番号
  remote 定義の通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 集約経路定義番号
  削除する集約経路の定義番号を、0〜3 の 10 進数値で指定します。
- all
  すべての集約経路を削除する場合に指定します。

[説明]

集約経路の削除を行います。

5.5.18 remote ip6 filter

[機能]

IPv6 フィルタの設定

[入力形式]

remote [<number>] ip6 filter <count> <action> <src_addr>/<prefixlen> <src_port> <dst_addr>/<prefixlen> <dst_port> <protocol> <tcpconnect>

[パラメタ]

<number>

- 相手定義番号

  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。

  省略した場合は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号

  フィルタリングの優先度を表す番号を、0〜63 の 10 進数値で指定します。指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つフィルタリング定義が既に存在する場合は、既存の定義を変更します。

<action>

フィルタリング対象に該当するパケットを透過するかどうかを設定します。

- pass

  該当するパケットを透過します。

- reject

  該当するパケットを遮断します。

- restrict

  該当するパケットを、回線が接続されていれば透過し、切断されていれば遮断します。

<src_addr>/<prefixlen>

フィルタリング対象とする送信元 IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス/プレフィックス長

  フィルタリング対象とする送信元 IPv6 アドレスとプレフィックス長の組み合わせを指定します。

- any

  すべての送信元 IPv6 アドレスをフィルタリング対象とする場合に指定します。

  ::/0 を指定するのと同じ意味になります。

<src_port>

フィルタリング対象とする送信元ポート番号を指定します。

- ポート番号

  フィルタリング対象とする送信元ポート番号を、1〜65535 の 10 進数値で指定します。複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。

  ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。

  以下に、有効な記述形式を示します。

- 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
- ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
- ポート番号- (例: 1- = 1 から 65535 までのポート)
- -ポート番号 (例: -1000 = 1 から 1000 までのポート)
- ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)

- any
  すべての送信元ポート番号をフィルタリング対象とする場合に指定します。

<dst_addr>/<prefixlen>

フィルタリング対象とする宛先 IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス/プレフィックス長
  フィルタリング対象とする宛先 IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- any
  すべての宛先 IPv6 アドレスをフィルタリング対象とする場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<dst_port>

フィルタリング対象とする宛先ポート番号を指定します。

- ポート番号
  フィルタリング対象とする宛先ポート番号を、1〜65535 の 10 進数値で指定します。
  記述形式は、<src_port>と同様です。
- any
  すべての宛先ポート番号をフィルタリング対象とする場合に指定します。

<protocol>

フィルタリング対象とするプロトコル番号を指定します。

- プロトコル番号
  フィルタリング対象とするプロトコル番号を、0〜255 の 10 進数値で指定します。
  255 を指定した場合は、すべてのプロトコルをフィルタリング対象とします。

<tcpconnect>

- yes
  TCP プロトコルでコネクション接続要求をフィルタリング対象に含めます。
- no
  TCP プロトコルでコネクション接続要求をフィルタリング対象に含めません。

[説明]

相手ネットワークに対する IPv6 フィルタを設定します。各パラメタに設定された値によって、動作が変化する場合があります。以下に説明します。

- <protocol>に指定した値によって、IPv6 拡張ヘッダの扱いが以下のように変化します。
  - 255 を指定した場合は、0 個以上の IPv6 拡張ヘッダを含む、あらゆる upper-layer protocol(upper-layer protocol なしを含む) に合致します。
  - 以下の IPv6 拡張ヘッダの値を指定した場合は、その拡張ヘッダが付与されている、あらゆる upper-layer protocol(upper-layerprotocol なしを含む) のパケットが合致します。

    0　　Hop-by-Hop Options Header

43 Routing Header

44 Fragment Header

60 Destination Options Header

- 以下の値を指定した場合は、0 個以上の IPv6 拡張ヘッダ (AH、ESP、IPComp を除く) を含む、upper-layer protocol ヘッダが付与されていないパケットが合致します。

  59 no next header

- その他の値が設定されている場合は、upper-layer protocol ヘッダの protocol 番号に等しい値であるパケットが合致します。この場合、AH、ESP、IPComp を除くすべての IPv6 拡張ヘッダは無視されます。パケット中に AH、ESP が設定されている場合は、それ以降の拡張ヘッダおよび upper-layer protocol ヘッダの解釈は行いません。

- <src_port>、<dst_port>に指定した値によって、<protocol>の扱いが以下のように変化します。
  - <protocol>に 255 を指定し、かつ<src_port>、<dst_port>のいずれか、または両方を指定している場合、TCP および UDP パケットの該当ポート番号を持つパケットのみが合致します。
  - <protocol>に TCP(6) または UDP(17) を指定し、かつ<src_port>、<dst_port>のいずれか、または両方を指定している場合、指定プロトコルの該当ポート番号を持つパケットのみが合致します。
  - <protocol>に TCP(6) または UDP(17) 以外を指定し、かつ<src_port>、<dst_port>のいずれか、または両方を指定している場合、あらゆるパケットが合致しません。

- <tcpconnect>の扱いを以下に示します。
  - <protocol>に any を指定した場合、TCP パケットのときにこの設定値が適用されます。
  - <protocol>に TCP(6) を指定した場合、常にこの設定値が適用されます。
  - <protocol>に any または TCP(6) 以外を指定した場合、この設定値は適用されません。

IPv6 フィルタは、本装置全体で 64 個まで定義できます。

[未設定時]

IPv6 フィルタを設定しないものとみなされ、すべてのパケットが透過します。

5.5.19　remote ip6 filter move

[機能]

IPv6 フィルタの優先順序の変更

[入力形式]

remote [<number>] ip6 filter move <count> <new_count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義の番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
  <count>に対する新しい順序を、0～63 の 10 進数値で指定します。
  既にこの定義番号を持つ定義が存在する場合には、その定義の前に挿入されます。

[説明]

IPv6 フィルタの優先順序を変更します。

5.5.20 remote ip6 filter delete

[機能]

IPv6 フィルタの削除

[入力形式]

remote [<number>] ip6 filter delete <count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

削除するフィルタリングを指定します。

- フィルタリング定義番号
  削除するフィルタリングの定義番号を指定します。
- all
  すべてのフィルタリングを削除する場合に指定します。

[説明]

IPv6 フィルタを削除します。

5.6　ブリッジ関連情報

5.6.1　remote bridge use

[機能]

ブリッジ機能の設定

[入力形式]

remote [<number>] bridge use <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

ブリッジを使用するかどうかを指定します。

- on
  ブリッジを使用する場合に指定します。
- off
  ブリッジを使用しない場合に指定します。

[説明]

ブリッジを使用するかどうかを設定します。
ブリッジを使用する場合、IP および IPv6 のパケット以外をすべてブリッジします。
ただし、接続先との接続時に BCP のネゴシエーションを行い、ネゴシエーションが成功した場合にブリッジデータの送受信が可能となります。

[注意]

IP および IPv6 以外のネットワークプロトコル (IPX など) をルーティングしているネットワークでブリッジを使用する場合は、ブリッジによって中継されることでネットワークがダウンすることがあります。ルーティングと併用する場合は、ルーティングによって転送するプロトコルをフィルタリングするよう設定してください。

[未設定時]

ブリッジを使用しないものとみなされます。

```
remote <number> bridge use off
```

5.6.2 remote bridge stp use

[機能]

STP モードの設定

[入力形式]

remote [<number>] bridge stp use <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

- on
  STP を使用する場合に指定します。
- off
  STP を使用しない場合に指定します。

[説明]

スパニングツリーアルゴリズムで経路制御を行うかどうかを設定します。
本コマンドは、ブリッジを使用している場合にだけ有効です。

[未設定時]

STP を使用しないものとみなされます。

```
remote <number> bridge stp use off
```

5.6.3　remote bridge stp cost

[機能]

パスコストの設定

[入力形式]

remote [<number>] bridge stp cost <path_cost>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<path_cost>

接続先と通信する場合のパスコストを指定します。

- auto
  インタフェースの速度に応じて、パスコストが自動決定されます。
  以下に、本パラメタ指定時のパスコストを示します。

回線種別	パスコスト
Ethernet(10Mbps)	100
HSD(64kbps)	15620
HSD(128kbps)	7810
FR(64kbps)	16000
FR(128kbps)	8500
ISDN(64kbps)	16000

- パスコスト
  パスコストを、1～65535 の 10 進数値で指定します。値が小さいほど、優先度が高くなります。

通常は auto を指定してください。ただし、ブリッジネットワークを構築する上で、優先ブリッジ決定のために任意のパスコストを指定することができます。

[説明]

スパニングツリーアルゴリズムで使用するパスコストを設定します。
本コマンドは、STP を使用する場合にだけ有効です。

[未設定時]

パスコストを自動決定するとみなされます。

```
remote <number> bridge stp cost auto
```

5.6.4 remote bridge stp priority

[機能]

インタフェース優先度の設定

[入力形式]

remote [<number>] bridge stp priority <port_priority>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<port_priority>

- インタフェース優先度
  インタフェースごとの優先度を、0～255 の 10 進数値で指定します。値が小さいほど、優先度が高くなります。

[説明]

スパニングツリーアルゴリズムで使用する、インタフェースごとの優先度を設定します。通常、設定する必要はありません。

本コマンドは、STP を使用する場合にだけ有効です。

本コマンドを設定しない場合は、<number>で指定したインタフェースが優先となり、remote 定義で定義されたインタフェースが非優先となります。lan 定義内で定義されたインタフェースでは、定義番号の最も小さいものが優先されます。

[未設定時]

インタフェース優先度に 128 が設定されたものとみなされます。

```
remote <number> bridge stp priority 128
```

5.6.5　remote bridge filter

[機能]

MAC フィルタの設定

[入力形式]

remote [<number>] bridge filter <count> <action> <src_mac> <dst_mac> <format> <value>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す番号を、0〜127 の 10 進数値で指定します。指定した値は、設定完了時に順方向にソートされリナンバリングされます。
  指定した定義番号と同じ値を持つ定義が既に存在する場合は、既存の設定に対する修正とみなされます。指定した値を持つ定義が存在しない場合は、追加とみなされます。

<action>

フィルタリング対象に該当するパケットを透過するかどうかを指定します。

- pass
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。
- restrict
  該当するパケットを、回線が接続されていれば透過し、切断されていれば遮断します。

<src_mac>

フィルタリング対象とする送信元 MAC アドレスを指定します。

- any
  すべての MAC アドレスを対象とする場合に指定します。
- bcast
  ブロードキャスト MAC アドレスを対象とする場合に指定します。
- mcast
  マルチキャスト MAC アドレスを対象とする場合に指定します。
- 上記以外
  対象とする MAC アドレスを指定します。フィルタリング対象とする送信元 MAC アドレスを、xx:xx:xx:xx:xx:xx(xx は 2 桁の 16 進数値) の形式で指定します。

<dec_mac>

フィルタリング対象とする宛先 MAC アドレスを指定します。

- any
  すべての MAC アドレスを対象とする場合に指定します。
- bcast
  ブロードキャスト MAC アドレスを対象とする場合に指定します。
- mcast
  マルチキャスト MAC アドレスを対象とする場合に指定します。
- 上記以外
  対象とする MAC アドレスを指定します。フィルタリング対象とする送信元 MAC アドレスを、xx:xx:xx:xx:xx:xx(xx は 2 桁の 16 進数値) の形式で指定します。

<format> <value>

- llc
  <value>の値と LSAP が一致する LLC 形式パケットを対象とする場合に指定します。<value>には、0～ffff の 16 進数値を指定します。
- ether
  <value>の値とタイプが一致する Ethernet 形式パケットを対象とする場合に指定します。<value>には、5dd～ffff の 16 進数値を指定します。
- any
  すべてのパケットを対象とする場合に指定します。<value>は、指定不要です。

[説明]

MAC フィルタを設定します。
本コマンドは、ブリッジ機能を使用する場合にだけ有効です。
指定した条件に一致するパケットを、指定した<action>に従って遮断または通過させます。
MAC フィルタは、本装置全体で 128 個まで定義できます。

[注意]

IP および IPv6 以外のネットワークプロトコル (IPX など) をルーティングしているネットワークでブリッジを使用する場合は、ブリッジによって中継されることでネットワークがダウンすることがあります。ルーティングと併用する場合は、ルーティングによって転送するプロトコルをフィルタリングするよう設定してください。

[未設定時]

MAC フィルタを設定しないものとみなされ、すべてのパケットが透過します。

5.6.6　remote bridge filter move

[機能]

MAC フィルタの優先順序の変更

[入力形式]

remote [<number>] bridge filter move <count> <new_count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 対象フィルタリング定義番号
  優先順序を変更する前のフィルタリング定義の番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
  <count>に対する新しい順序を、0～127 の 10 進数値で指定します。
  既にこの定義番号を持つ定義が存在する場合には、その定義の前に挿入されます。

[説明]

MAC フィルタの優先順序を変更します。

5.6.7 remote bridge filter delete

[機能]

MAC フィルタ情報の削除

[入力形式]

remote [<number>] bridge filter delete <count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  削除するフィルタリングの定義番号を指定します。
- all
  すべてのフィルタリング情報を削除する場合に指定します。

[説明]

MAC フィルタ情報を削除します。

5.7　マルチホーミング関連情報

5.7.1　remote multihoming mode

[機能]

マルチホーミング機能の設定

[入力形式]

remote [<number>] multihoming mode <mode> [<judge>]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

マルチホーミングのセッション切り分け方式を指定します。

- off
  マルチホーミング機能を使用しません。
- onebyone
  順次方式を使用します。
- roundrobin
  ラウンドロビン方式を使用します。
- both
  双方方式を使用します。

<judge>

<mode>が onebyone(順次方式) または both(双方方式) の場合にだけ有効であり、それ以外の場合に<judge>があればエラーとなります。

- session
  セッション数を閾値として使用します。
- rate
  WAN の回線使用率を閾値として使用します。
- speed
  WAN の回線使用速度を閾値として使用します。

[説明]

マルチホーミング機能 (負荷分散・高信頼性機能) を使用する場合のセッションの切分け方式を設定します。
"onebyone"、"roundrobin"、"both"の場合はマルチホーミング機能を使用します。"off"の場合は使用しません。

- onebyone (順次方式)
  順次方式ではセッション数または WAN 側経路使用率が設定値を超えるまでは新しいセッションを WAN 側セッションとし、設定値を超えてからは転送セッションとします。
  切分けの閾値は"remote multihoming session"と"remote multihoming rate"と"remote multihoming speed"コマンドにより設定します。

- roundrobin (ラウンドロビン方式)
  ラウンドロビン方式では WAN 側セッションと転送セッションの比率が指定した割合になるようにセッションを切り分けます。
  セッション数の割合は"remote multihoming ratio"コマンドにより設定します。
- both (双方方式)
  双方方式では閾値 (セッション数または回線使用率) を超えるまでは順次方式、閾値を超えてからはラウンドロビン方式を使用します。
  切分けの閾値は"remote multihoming session"と"remote multihoming rate"と"remote multihoming speed"コマンドにより設定します。

[未設定時]

マルチホーミング機能を使用しないものとみなされます。

```
remote <number> multihoming off
```

5.7.2　remote multihoming session

[機能]

最大セッション数の設定

[入力形式]

remote [<number>] multihoming session <value>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<value>

- 最大セッション数
  最大セッション数を、0～256 の範囲で指定します。

[説明]

順次方式と双方方式で閾値として使用するセッション数を指定します。

[未設定時]

最大セッション数として、0 を設定したものとみなされます。

```
remote <number> multihoming session 0
```

5.7.3 remote multihoming rate

[機能]

最大回線使用率の設定

[入力形式]

remote [<number>] multihoming rate <value>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<value>

- 最大回線使用率
  最大回線使用率 [%] を、0～100 の範囲で指定します。

[説明]

順次方式と双方方式で閾値として使用する回線使用率を指定します。

[未設定時]

最大回線使用率として、0[%] を設定したものとみなされます。

```
remote <number> multihoming rate 0
```

5.7.4　remote multihoming speed

[機能]

最大回線使用速度の設定

[入力形式]

remote [<number>] multihoming speed <value>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<value>

- 最大回線使用速度
  最大回線使用速度を、0k〜128K の範囲の 10 進数値と単位文字で指定します。
  10 進数値の末尾に k の単位文字を付与することで単位を指定できます。
  単位文字を付与しない場合、単位は Kbps となります。
  単位文字 k を付与した場合、単位は Kbps となります。
  1Kbps は 1000bps です。

[説明]

順次方式と双方方式で閾値として使用する回線使用速度を指定します。

[未設定時]

最大回線使用速度として、0 Kbps を設定したものとみなされます。

```
remote <number> multihoming speed 0k
```

5.7.5 remote multihoming ratio

[機能]

WAN 側セッションと転送側セッションの比率の設定

[入力形式]

remote [<number>] multihoming ratio <ratio>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ratio>

- WAN 側セッションの割合
  WAN 側セッションの割合を、0～10 の範囲で指定します。

[説明]

ラウンドロビン方式で使用します。WAN 側セッションの割合を設定します。
<ratio>を x と設定した場合、2 つのセッションの比率は次のようになります。

- WAN 側セッション数 : 転送セッション数 = x : (10 - x)

[未設定時]

WAN 側セッションの割合として、0 を設定したものとみなされます。

```
remote <number> multihoming ratio 0
```

5.7.6　remote multihoming timeout

[機能]

セッションタイムアウト時間の設定

[入力形式]

remote [<number>] multihoming timeout <time>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time>

- セッションタイムアウト時間
  セッションタイムアウト時間を、60 秒 (1 分)～86400 秒 (1 日) の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。

[説明]

動的マルチホーミング情報テーブルのセッション情報がタイムアウトとなり削除される時間を設定します。
テーブルに記録されているセッションについて無通信状態が設定された時間継続した場合に該当セッション情報をテーブルから削除します。

[未設定時]

セッションタイムアウト時間として、5 分を設定したものとみなされます。

```
remote <number> multihoming timeout 5m
```

5.7.7 remote multihoming router

[機能]

転送先ルータ IP アドレスの設定

[入力形式]

remote [<number>] multihoming router <address>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<address>

- 転送先ルータ IP アドレス
  転送先ルータ IP アドレスを指定します。
  0.0.0.0 を指定した場合、転送セッション (LAN 側の転送先ルータ経由のセッション) となったパケットは破棄されます。

[説明]

転送先ルータの IP アドレスを設定します。
転送セッションのパケットは本装置からこの IP アドレスを持つ転送先ルータに転送されます。

[未設定時]

転送先ルータの IP アドレスとして、0.0.0.0 を設定したものとみなされます。

```
remote <number> multihoming router 0.0.0.0
```

5.7.8　remote multihoming watchdog address

[機能]

転送セッション経路監視用 IP アドレスの設定

[入力形式]

remote [<number>] multihoming watchdog address <address>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<address>

- 転送セッション経路監視用 IP アドレス
  転送セッション経路監視用 IP アドレスを指定します。
  0.0.0.0 を指定した場合は、監視しません。

[説明]

転送セッションの経路状態を監視するための ping(ICMP Echo) の宛先 IP アドレスを設定します。
この IP アドレスに対して転送先ルータ経由で指定した間隔で ping を実行し、WAN 経路の状態を監視します。
ping を実行する間隔は、"multihoming watchdog interval"で設定します。

[未設定時]

転送セッション経路を監視しないものとみなされます。

```
remote <number> multihoming watchdog address 0.0.0.0
```

5.7.9 remote multihoming watchdog interval

[機能]

転送セッション経路監視用の ping 実行間隔の設定

[入力形式]

remote [<number>] multihoming watchdog interval <time>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time>

- 転送セッション経路監用 ping 実行間隔
  転送セッション経路を監視するための ping(ICMP Echo) 実行間隔を、1 秒～255 秒の範囲で指定します。
  単位は、m(分)、s(秒) のいずれかを指定します。

[説明]

転送セッション経路監視のための ping の実行間隔を設定します。

[未設定時]

転送セッション経路監視用 ICMP Echo (ping) の送信間隔として 10 秒を設定したものとみなされます。

```
remote <number> multihoming watchdog interval 10s
```

5.7.10　remote multihoming watchdog response

[機能]

障害認識無応答回数と障害復旧判断応答回数の設定

[入力形式]

remote [<number>] multihoming watchdog response <error> <recovery>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<error>

- 障害認識無応答回数
  ICMP Echo Reply を連続して受信しなかった場合に障害を認識する回数を、1〜16 の範囲の 10 進数で指定します。

<recovery>

- 障害復旧判断応答回数
  ICMP Echo Reply を連続して受信した場合に障害からの復旧を認識する回数を、1〜16 の範囲の 10 進数で指定します。

[説明]

転送セッション経路監視用 ping の応答を<error>で設定した回数連続して受信できなかった場合に転送セッションの経路に障害が発生したと認識します。

転送セッションの経路に障害があると認識されている状態で、転送セッション経路監視用 ping の応答を<recovery>で設定した回数連続して受信した場合に障害から復旧したと認識します。

[未設定時]

障害認識無応答回数は 3 回、障害復旧判断応答回数は 1 回を設定したものとみなされます。

```
remote <number> multihoming watchdog response 3 1
```

5.7.11 remote multihoming static

[機能]

静的マルチホーミングの設定

[入力形式]

remote [<number>] multihoming static <count> <route> <change> <src_port> <dst_port> <protocol>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 静的マルチホーミング定義番号
  静的マルチホーミング情報の定義番号を、0〜63 の 10 進数値で指定します。
  指定した値は、順番にソートされてリナンバリングされます。また、同じ値をもつフィルタリング定義が既に存在する場合は、既存の定義を変更します。

<route>

静的マルチホーミング対象のパケットを転送する経路を指定します。

- wan
  対象パケットを本装置の WAN 側に送出します。
- lan
  対象パケットを LAN 側の転送先ルータに転送します。

<change>

障害時に経路を変更するかどうかを指定します。

- enable <route>で指定した経路に障害が発生した場合に経路を変更します。・disable <route>で指定した経路に障害が発生した場合に対象パケットを破棄します。

<src_port>

静的マルチホーミング対象となる送信元ポート番号を指定します。

- 送信元ポート番号
  静的マルチホーミング対象となる送信元ポート番号を、1〜65535 の 10 進数値で指定します。複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。
  ポート番号は、","(カンマ) または"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号 … (例: 10,20,30- = 10 と 20 と 30 以降のポート)
- any
  すべてのポート番号を対象とする場合に指定します。

<dst_port>

静的マルチホーミング対象となる宛先ポート番号を指定します。

- 宛先ポート番号

  静的マルチホーミング対象となる宛先ポート番号を、1〜65535 の 10 進数値で指定します。複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。

  ポート番号は、","(カンマ) または"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。

  以下に、有効な記述形式を示します。

  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号 … (例: 10,20,30- = 10 と 20 と 30 以降のポート)

- any

  すべてのポート番号を対象とする場合に指定します。

<protocol>

- プロトコル番号

  静的マルチホーミング対象のプロトコル番号を、0〜255 の 10 進数値で指定します。(例: ICMP:1、TCP:6、UDP:17 など)。

  255 を指定すると、以下の any を指定したのと同じ意味になります。

- any

  すべてのプロトコル番号を対象とする場合に指定します。

[説明]

条件に一致するパケットは設定に従って WAN に送出されるか、あるいは LAN 側の転送先ルータに転送されます。

[未設定時]

静的マルチホーミング情報を設定しないものとみなされます。

5.7.12 remote multihoming static move

[機能]

静的マルチホーミングの優先順序の変更

[入力形式]

remote [<number>] multihoming static move <count> <new_count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 対象静的マルチホーミング定義番号
  優先順序を変更する静的マルチホーミング情報の定義番号を指定します。

<new_count>

- 移動先マルチホーミング定義番号
  <count>に対する新しい順序を、0～64 の 10 進数値で指定します。すでにこの番号を持つ定義が存在する場合には、その定義の前に挿入されます。

[説明]

静的マルチホーミング情報の優先順序を変更します。

5.7.13　remote multihoming static delete

[機能]

静的マルチホーミングの削除

[入力形式]

remote [<number>] multihoming static delete <count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

削除する静的マルチホーミング情報の定義番号を指定します。

- 削除する転送可否定義番号
  削除する静的マルチホーミング情報の定義番号を指定します。
- all
  すべての静的マルチホーミング情報を削除する場合に指定します。

[説明]

指定した静的マルチホーミング情報を削除します。

5.7.14 remote multihoming alive

[機能]

WAN 側セッション経路監視の設定

[入力形式]

remote [<number>] multihoming alive <dst_addr> [<resend_time> [<time_out> [<normal_interval> [<error_interval>]]]]

[パラメタ]

<number>

- 相手定義番号

  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<dst_addr>

- ICMP ECHO パケットの宛先 IP アドレス

  WAN 側セッションの経路を監視するために実行する ICMP ECHO パケットの宛先 IP アドレスを指定します。

  0.0.0.0 を指定した場合は、WAN 側セッション経路を監視しません。

<resend_time>

- ICMP ECHO パケットの再送間隔

  ICMP ECHO パケットの再送間隔を、1 秒～60 秒の範囲で指定します。

  単位は、m(分)、s(秒) のいずれかを指定します。

  省略した場合は、5 秒を指定したものとみなされます。

<time_out>

- ICMP ECHO のタイムアウト時間

  ICMP ECHO のタイムアウト時間を、<resend_time>+1 秒～240 秒の範囲で指定します。

  単位は、m(分)、s(秒) のいずれかを指定します。

  省略した場合は、<resend_time>× 3 ＋ 1 秒を指定したものとみなされます。

<normal_interval>

- ICMP ECHO パケットの正常時送信間隔

  ICMP ECHO パケットの正常時送信間隔を、<time_out>+1 秒～255 秒の範囲で指定します。

  単位は、m(分)、s(秒) のいずれかを指定します。

  省略した場合は、<time_out>+1 秒を指定したものとみなされます。

<error_interval>

- ICMP ECHO パケットの異常時送信間隔

  ICMP ECHO パケットの異常時送信間隔を、1 秒～255 秒の範囲で指定します。

  単位は、m(分)、s(秒) のいずれかを指定します。

  省略した場合は、30 秒を指定したものとみなされます。

[説明]

WAN 側セッションの経路を監視するための動作情報を設定します。

<dst_addr>で指定した宛先に ICMP ECHO パケットを送出し、<time_out>時間応答がない場合、WAN 側経路がダウンしたものとみなされます。

[未設定時]

WAN 側セッション経路を監視しないものとみなされます。

```
remote <number> multihoming alive 0.0.0.0 5s 16s 17s 30s
```

5.8 フレームリレー関連情報

5.8.1 remote fr dlci

[機能]

フレームリレーにおける DLCI の設定

[入力形式]

remote [<number>] fr dlci <dlci_number>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<dlci_number>

- DLCI
  自局で使用する DLCI を、16～991 の 10 進数値で指定します。
  なお、設定を削除する場合は、0 を指定します。

[説明]

フレームリレーにおける DLCI(データリンクコネクション識別子) を設定します。
フレームリレーを使用する場合は、本コマンドを必ず実行してください。

[未設定時]

DLCI を設定しないものとみなされます。

5.8.2　remote fr cir

[機能]

フレームリレーにおける CIR の設定

[入力形式]

remote [<number>] fr cir <cir>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<cir>

- CIR 値
  CIR 値を、0〜アクセス速度 / 2 で指定します。

[説明]

フレームリレーにおける、DLCI ごとの CIR 値 (認定情報速度) を設定します。

[未設定時]

CIR 値として 0 を指定したものとみなされます。

```
remote <number> fr cir 0
```