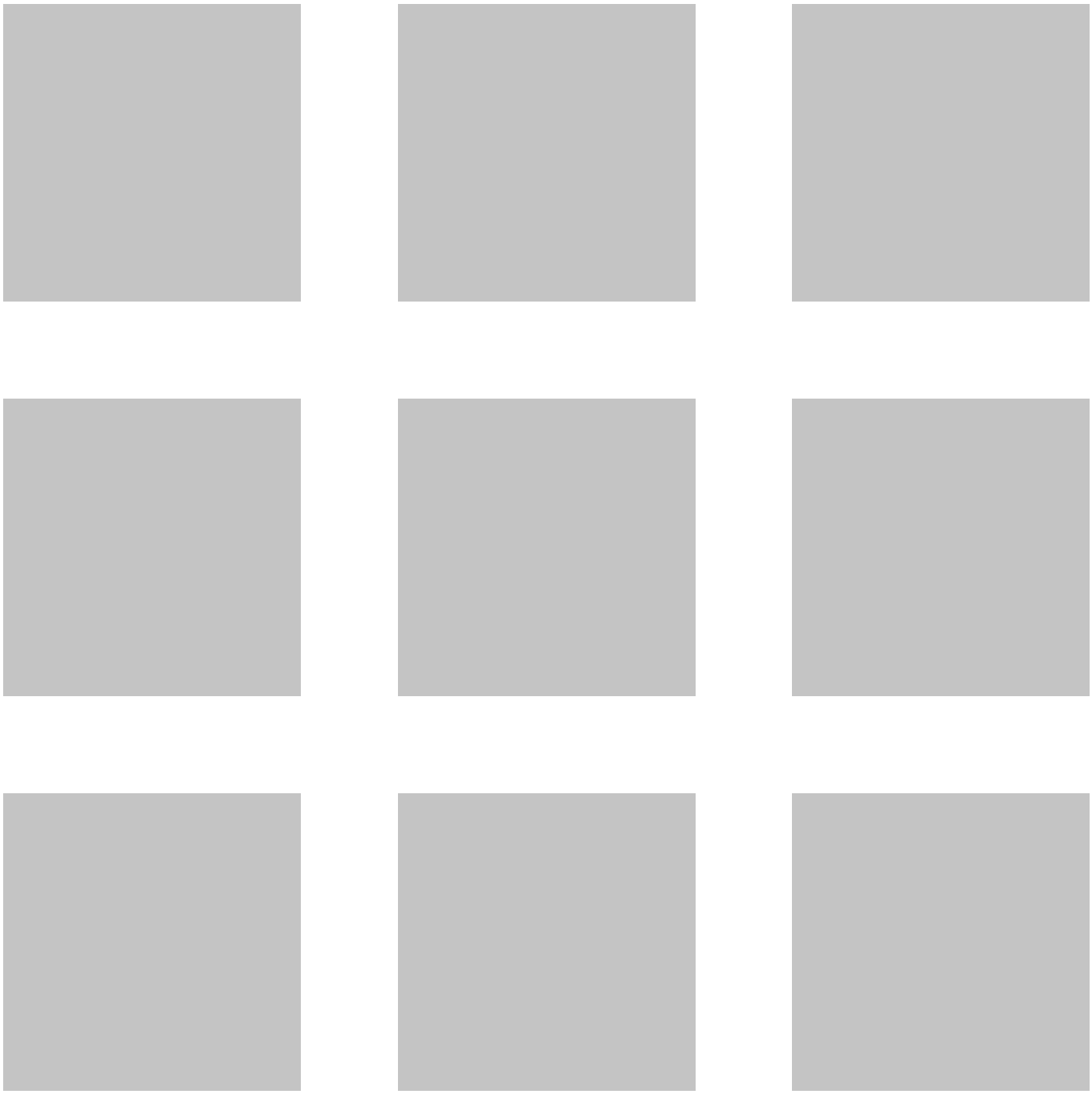


MR1000

取扱説明書

コマンドリファレンス

OMRON

はじめに

このたびは、本装置をお買い上げいただき、まことにありがとうございます。
インターネットやLANをさらに活用するために、本装置をご利用ください。

2005年1月

本書の構成と使いかた

本書は、本装置のコンソールから入力するコマンドについて説明しています。
また、CD-ROMの中のREADMEファイルには大切な情報が記載されていますので、併せてお読みください。

本書の読者と前提知識

本書は、ネットワーク管理を行っている方を対象に記述しています。
本書を利用するにあたって、ネットワークおよびインターネットに関する基本的な知識が必要です。

本書の構成

本書の第1～15章までは、構成定義コマンドを説明しています。第16章は制御コマンドを、第17章は表示コマンドを説明しています。第18～20章は、付録情報を説明しています。

マークについて

[機能]	**コマンドの機能概要を記載しています。**
[入力形式]	**入力形式を記載しています。以下の規約に従って記載しています。** **< > ：パラメタ名称を示しています。** **[ ] ：括弧内のオプションやパラメタを省略できることを示しています。** **{ } ：括弧内のオプションやパラメタのうち、どれかを選択することを示しています。**
[オプション]	**各オプションの意味を記載しています。**
[パラメタ]	**各パラメタの意味を記載しています。**
[説明]	**コマンドの解説を記載しています。**
[注意]	**コマンドの注意事項を記載しています。**
[例]	**コマンドの設定例、実行例または表示例を記載しています。**
[未設定時]	**コマンドの未設定時について説明し、設定したとみなされるコマンドを記載しています。**

本書における商標の表記について

Microsoftは、米国Microsoft Corporationの米国およびその他の国における登録商標です。
MD5は、RSA Security Inc.が開発した暗号およびハッシュアルゴリズムです。
本書に記載されているその他の会社名および製品名は、各社の商標または登録商標です。

使用上の注意事項

構成定義コマンドを使用する場合には、以下の点にご注意ください。

- コマンドの設定および変更が終了したら、save コマンドを実行してから enable コマンドまたは reset コマンドを実行し、設定を有効にしてください。save コマンドを実行せず reset コマンドまたは電源再投入を行った場合にはコマンドの設定が元の状態にもどります。また、save コマンドを実行せずに enable コマンドを実行した場合、一時的に設定は有効になりますが、reset コマンドまたは電源再投入を行った場合にコマンドの設定が元の状態に戻ります。ただし、password, page, env コマンドについては設定直後から有効となります。
- 構成定義コマンドを削除する場合は、delete コマンドを使用します。削除した構成定義コマンドは、show コマンド(コマンド名未指定)を実行しても、構成定義コマンド文字列として表示されません。
  例．ログオンパスワードの削除

```
# delete password set
```

- show コマンドにより構成定義を表示する場合、コマンド未設定時の値と同じ物は表示されません。コマンド未設定時の値を表示したい場合には、show コマンドに続けて、表示したいパラメタの直前のコマンドまで入力します。
  例．LAN インタフェースの IP アドレスの表示

```
# show lan 0 ip address
192.168.1.1/24 3
```

本文中で使用しているコマンドのパラメタに時間を指定する場合には、特別な指示がある場合を除き s（秒）、m（分）、h（時）、d（日）の単位をつけて設定します。
例：1m = 1 分
なお、60s、60m、24h を指定した場合には、それぞれ、1m、1h、1d を指定したものとみなされます。

目　次

第 1 章　WAN 情報の設定

- wan 定義番号の指定範囲
  本章のコマンド の [パラメタ] に記載されている<number>(wan 定義番号) に指定する wan 定義の通し番号 (10 進数値) は、機種ごとに以下に示す範囲で指定してください。

範囲	機種
0	MR1000

1.1 回線共通情報

1.1.1 wan bind

[機能]

利用する物理回線の設定

[入力形式]

wan [<number>] bind <slot> [<line>]

[パラメタ]

<number>

- wan 定義番号
  wan 定義の通し番号を、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。

<slot>

必ず"mb"(基本ボード) を指定してください。

<line>

- 回線番号
  同一のボード に複数の回線がある場合に、どの回線を利用するか指定します。
  省略した場合は、0 を指定したものとみなされます。

[説明]

wan 定義で利用する回線を設定します。
複数の wan 定義で同一の回線を指定すると、一番小さい番号の wan 定義だけが有効になります。
なお、本コマンド で指定した回線が Ethernet の場合、この wan 定義は無効となります。

[未設定時]

基本ボード 上の回線番号が定義番号<number>となる回線を設定するものとみなされます。

```
wan <number> bind mb <number>
```

1.1.2　wan line

[機能]

回線インタフェースおよび通信速度の設定

[入力形式]

wan [<number>] line unuse (未使用)
wan [<number>] line isdn (ISDN)
wan [<number>] line hsd <speed> (専用線)
wan [<number>] line fr <speed> (フレームリレー)

[パラメタ]

<number>

- wan 定義番号
  wan 定義の通し番号を、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。

<speed>

- 回線速度
  専用線またはフレームリレー利用時の回線速度を以下の範囲で指定します。

インタフェース	回線速度(指定範囲)
BRI	64k, 128k

[説明]

wan 定義で利用する回線の、回線種別を設定します。

- ISDN
- 専用線 (64Kbps～128Kbps)
- フレームリレー (64Kbps～128Kbps)

以下を指定した場合、wan 定義は無効となります。

- unuse(未使用) を指定した場合
- “1.1.1 wan bind” で設定した回線では使用できない回線種別を指定した場合
- 専用線またはフレームリレーのときに、“1.1.1 wan bind” で設定した回線では使用できない回線速度を指定した場合

[未設定時]

wan 定義を使用しないものとみなされます。

```
wan <number> line unuse
```

1.2 ISDN 回線情報

1.2.1 wan isdn global

[機能]

グローバル着信の設定

[入力形式]

wan [<number>] isdn global <mode>

[パラメタ]

<number>

- wan 定義番号
  wan 定義の通し番号を、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>

グローバル着信を受け付けるかどうかを指定します。

- accept
  グローバル着信を受け付けます。
- reject
  グローバル着信を受け付けません。

[説明]

グローバル着信を受け付けるかどうかを設定します。
通常は<mode>に accept を指定してください。ただし、ダイヤルイン番号または i・ナンバー宛の着信だけを受け付ける場合は reject を指定し、“1.2.2 wan isdn number” で着信を受け付ける着信番号を指定してください。

[未設定時]

グローバル着信を受け付けるものとみなされます。

```
wan <number> isdn global accept
```

1.2.2　wan isdn number

[機能]

自局電話番号の設定

[入力形式]

wan [<number>] isdn number <count> <tel_number> [<subaddress>]

[パラメタ]

<number>

- wan 定義番号
  wan 定義の通し番号を、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>

着信番号チェックを行う電話番号は、2 組まで設定できます。2 組のうちのどちらを設定するか、番号を指定します。

- 0
  着信番号チェックの電話番号 1 を設定します。
- 1
  着信番号チェックの電話番号 2 を設定します。

<tel_number>

着信番号チェックを行う電話番号を指定します。

- 電話番号
  着信時にチェックする電話番号を、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
  着信時に電話番号のチェックを行わない場合に指定します。
- in1
  i・ナンバーサービス契約時に、i・ナンバー情報 1(契約者回線番号) の着信を受け付ける場合に指定します。
- in2
  i・ナンバーサービス契約時に、i・ナンバー情報 2(追加の番号) の着信を受け付ける場合に指定します。
- in3
  i・ナンバーサービス契約時に、i・ナンバー情報 3(追加の番号) の着信を受け付ける場合に指定します。

<subaddress>

- サブアドレス
  着信時にチェックするサブアドレスを、0x22(ダブルクォーテーション) を除くコードで構成される 19 桁以内の ASCII 文字列で指定します。
  省略した場合は、サブアドレス通知がない着信のみを指定したものとみなされます。

[説明]

着信番号チェックについて設定します。

ダイヤルイン番号、i・ナンバー、サブアドレスを利用して着信機器を識別するかどうかを、<tel_number>と<subaddress>の組み合わせで指定します。着信番号チェックの電話番号は、2 組まで設定できます。

着信時に網から通知される電話番号とサブアドレスが着信番号チェックの電話番号と一致しない場合は、着信を受け付けません。

<tel_number>に any を指定し、かつ<subaddress>を指定した場合は、<subaddress>だけが着信番号チェックの対象となります。また、<tel_number>に any を指定し、<subaddress>が未指定の場合は、サブアドレス通知がないすべての着信を指定したものとみなされます。

i・ナンバーサービス契約時は、<tel_number>に in1、in2、または in3 のどれかを指定してください。

[注意]

任意のサブアドレス通知を着信するように指定することはできません。

[未設定時]

サブアドレス通知のないすべての着信を指定したものとみなされます。

```
wan <number> isdn number 0 any
```

1.2.3　wan isdn numbersend

[機能]

発信者番号通知の設定

[入力形式]

wan [<number>] isdn numbersend <mode> [<tel_number> [<subaddress>]]

[パラメタ]

<number>

- wan 定義番号
  wan 定義の通し番号を、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>

発信者番号の通知形態を指定します。

- specified
  <tel_number>および<subaddress>で指定する電話番号を、発信者番号として通知します。
- default
  網契約に従います。回線の加入契約で選択した内容の設定になります。
- off
  接続先に発信者の電話番号を通知しません。

以下のパラメタは、<mode>に specified を設定した場合にだけ有効です。

<tel_number>

<mode>に specified を設定した場合、必ず以下のどれかを指定してください。

- 通知電話番号
  発信者番号として通知する電話番号を、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。
- in1
  発信者番号として、i・ナンバー情報 1 を通知します。
- in2
  発信者番号として、i・ナンバー情報 2 を通知します。
- in3
  発信者番号として、i・ナンバー情報 3 を通知します。

<subaddress>

- サブアド レス
  発信者番号の一部として通知するサブアド レスを、0x22(ダブルクォーテーション) を除くコード で構成される 19 桁以内の ASCII 文字列で指定します。
  省略した場合は、サブアド レスを通知しません。

[説明]

発信者番号を通知するかどうかを設定します。また、通知する場合の、通知番号を設定します。

[注意]

MR1000 は PIAFS 接続に対応しています。PIAFS(64Kbps) 発信時には、<subaddress> で設定したサブアドレスは無視され、相手に通知されません。

[未設定時]

網契約に従うとみなされます。

```
wan <number> isdn numbersend default
```

1.2.4　wan isdn limit charge

[機能]

上限課金額による (発呼抑止) 条件の設定

[入力形式]

wan [<number>] isdn limit charge <charge> [<diallock>]

[パラメタ]

<number>

- wan 定義番号
  wan 定義の通し番号を、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。

<charge>

- 上限課金額
  自動発信を制限する上限課金額を、0〜999999 の 10 進数値 (単位:円) で指定します。0 を指定した場合は、課金額による自動発信制限を行いません。

<diallock>

自動発信を制限するかどうかを指定します。

- yes
  上限課金額に達した場合に、以降の自動発信を制限します。
  ただし、回線の手動接続は、制限の対象外となります。
- no
  上限課金額に達した場合に、以降の自動発信を制限しません。

省略した場合は、yes を指定したものとみなされます。

[説明]

データ通信において、通信課金の累計が上限課金額に達した場合に、自動発信を制限するかどうかを設定します。
<diallock>の指定内容にかかわらず、<charge>で指定した上限課金額を超えて自動発信しようとした場合は、syslog が採取されます。

[未設定時]

課金額による自動発信制限を行わないとみなされます。

```
wan <number> isdn limit charge 0 yes
```

1.2.5 wan isdn limit time

[機能]

上限通信時間による (発呼抑止) 条件の設定

[入力形式]

wan [<number>] isdn limit time <time> [<diallock>]

[パラメタ]

<number>

- wan 定義番号
  wan 定義の通し番号を、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>

- 上限接続時間
  自動発信を制限する接続時間の上限時間を、0 秒～999 時間の 10 進数値で指定します。単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。
  0 を指定した場合は、接続時間による自動発信制限を行いません。

<diallock>

自動発信を制限するかどうかを指定します。

- yes
  接続時間の上限に達した場合に、以降の自動発信を制限します。
  ただし、回線の手動接続は、制限の対象外となります。
- no
  接続時間の上限に達した場合に、自動発信を制限しません。

省略した場合は、yes を指定したものとみなされます。

[説明]

データ通信において、通信時間の累計が接続時間の上限に達した場合に、自動発信を制限するかどうかを設定します。

<diallock>の指定内容にかかわらず、<time>で指定した上限接続時間を超えて自動発信しようとした場合は、syslog が採取されます。

[未設定時]

接続時間による自動発信制限を行わないとみなされます。

```
wan <number> isdn limit time 0d yes
```

1.2.6　wan isdn accept

[機能]

装置単位の着信可否の設定

[入力形式]

wan [<number>] isdn accept <mode>

[パラメタ]

<number>

- wan 定義番号
  wan 定義の通し番号を、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>

データ着信時の動作について指定します。

- enable
  “4.2.21 remote ap called accept” の設定に従います。
- disable
  着信を禁止します。着信をすべて拒否し、発信専用の装置となります。

[説明]

外部から本装置に着信したときの動作について設定します。

[未設定時]

“4.2.21 remote ap called accept” の設定に従うものとみなされます。

```
wan <number> isdn accept enable
```

1.2.7 wan isdn autodial

[機能]

装置単位の自動発信可否の設定

[入力形式]

wan [<number>] isdn autodial <mode>

[パラメタ]

<number>

- wan 定義番号
  wan 定義の通し番号を、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について指定します。

- enable
  “4.1.2 remote autodial” の設定に従います。
- disable
  本装置からの自動ダイヤルを禁止します。どのような通信データが発生した場合も、自動的にはダイヤルしません。

[説明]

通信データが発生したときに、自動的にダイヤルするかどうかを設定します。

[未設定時]

“4.1.2 remote autodial” の設定に従います。

```
wan <number> isdn autodial enable
```

1.2.8　wan isdn keeptime

[機能]

テレホーダイ機能デフォルト時間の設定

[入力形式]

wan [<number>] isdn keeptime <time>

[パラメタ]

<number>

- wan 定義番号
  wan 定義の通し番号を、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>

- 初期時間
  回線接続保持の初期時間を、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) のどれかを指定します。

[説明]

テレホーダイ機能 (回線接続保持機能) が時間指定なしで起動された場合のデフォルト時間を設定します。0 が設定された場合にはデフォルト時間はないものとして扱われ、timerctl コマンドによりテレホーダイ機能 (回線接続保持時間) を起動するときに接続保持時間の指定が必要となります。

[注意]

この定義は、wan line コマンドで isdn が設定されているもっとも<number>の小さい wan 定義に設定されているものだけが有効です。

[未設定時]

デフォルト時間はありません。

```
wan <number> isdn keeptime 0d
```

1.2.9 wan isdn activation

[機能]

レイヤ 1 起動種別の設定

[入力形式]

wan [<number>] isdn activation <type> [<time>]

[パラメタ]

<number>

- wan 定義番号
  wan 定義の通し番号を、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>

レイヤ 1 起動種別を指定します。

- always
  常時起動動作を指定します。
- per-call
  呼毎起動動作を指定します。

<time>

- 回線停止猶予時間
  <type>に per-call を指定した場合に通信終了後の回線同期停止猶予時間を、1 秒～300 秒の範囲で指定します。単位は、m(分)、s(秒) のどちらかを指定します。省略した場合は、60 秒を指定したものとみなされます。

[説明]

レイヤ 1 起動種別 (回線同期確立手順の方式) を設定します。
また、レイヤ 1 起動種別に呼毎起動動作を指定した場合には、回線停止猶予時間を設定します。

[注意]

呼毎起動動作を指定した場合には、回線同期外れ (線抜けなど) を検出することはできません。
また、回線の発着信が常時起動動作と比べて遅くなる場合があります。
通信終了後、指定した回線停止猶予時間後に D チャネルのデータリンク層 (レイヤ 2) を停止します。
そのあと、ISDN 網の仕様により、一定時間後に物理層 (レイヤ 1) が停止します。
呼毎起動動作を指定し、常時起動回線に接続した場合は、データリンク層 (レイヤ 2) は停止しますが、物理層 (レイヤ 1) は停止しません。
常時起動動作を指定し、呼毎起動回線に接続した場合は、データリンク層、物理層とも停止しません。
PRI インタフェースに対して呼毎起動動作を指定しても、常時起動動作となります。

[未設定時]

常時起動動作を指定したものとみなされます。

```
wan <number> isdn activation always
```

1.3　フレームリレー回線情報

1.3.1　wan fr lmi

[機能]

フレームリレーにおける PVC 状態確認手順の設定

[入力形式]

wan [<number>] fr lmi <type>

[パラメタ]

<number>

- wan 定義番号
  wan 定義の通し番号を、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>

PVC 状態確認の手順を指定します。

- q933a
  ITU-T Q.933 Annex A に準拠します。
- off
  PVC 状態確認を行いません。

[説明]

フレームリレーでの PVC 状態確認手順を、網契約に合わせて設定します。

[注意]

- この機能を使用する場合は、通信事業者との契約が必要です。
- PVC 状態確認の双方向手順はサポートしていません。

[未設定時]

ITU-T Q.933 Annex A に準拠するとみなされます。

```
wan <number> fr lmi q933a
```

1.3.2 wan fr fecn

[機能]

FECN による輻輳制御の設定

[入力形式]

wan [<number>] fr fecn <mode>

[パラメタ]

<number>

- wan 定義番号
  wan 定義の通し番号を、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>

FECN によって輻輳制御を行うかどうかを指定します。

- on
  輻輳制御を行います。
- off
  輻輳制御を行いません。

[説明]

FECN による輻輳制御について設定します。

[未設定時]

FECN によって輻輳制御を行うとみなされます。

```
wan <number> fr fecn on
```

1.3.3　wan fr becn

[機能]

BECN による輻輳制御の設定

[入力形式]

wan [<number>] fr becn <mode>

[パラメタ]

<number>

- wan 定義番号
  wan 定義の通し番号を、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>

BECN によって輻輳制御を行うかどうかを指定します。

- on
  輻輳制御を行います。
- off
  輻輳制御を行いません。

[説明]

BECN による輻輳制御について設定します。

[未設定時]

BECN によって輻輳制御を行うとみなされます。

```
wan <number> fr becn on
```

1.3.4 wan fr cllm

[機能]

CLLM による輻輳制御の設定

[入力形式]

wan [<number>] fr cllm <mode>

[パラメタ]

<number>

- wan 定義番号
  wan 定義の通し番号を、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>

CLLM によって輻輳制御を行うかどうかを指定します。

- on
  輻輳制御を行います。
- off
  輻輳制御を行いません。

[説明]

CLLM による輻輳制御について設定します。

[未設定時]

CLLM によって輻輳制御を行うとみなされます。

```
wan <number> fr cllm on
```

第 2 章　シリアル情報の設定

- serial 定義番号の指定範囲
  本章のコマンド の [パラメタ] に記載されている<number>(serial 定義番号) に指定する serial 定義の通し番号 (10 進数値) は、機種ごとに以下に示す範囲で指定してください。

範囲	機種
0	MR1000

2.1 シリアル共通情報

2.1.1 serial use

[機能]

COM ポート動作モード の設定

[入力形式]

serial [<number>] use <mode>

[パラメタ]

<number>

- serial 定義番号
  serial 定義の通し番号を、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>

COM ポートを利用するかどうかを指定します。

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

[説明]

COM ポートを利用するかどうかを指定します。

[未設定時]

COM ポートを利用しないものとみなされます。

```
serial <number> use off
```

2.1.2　serial speed

[機能]

COM ポート通信速度の設定

[入力形式]

serial [<number>] speed <speed>

[パラメタ]

<number>

- serial 定義番号
  serial 定義の通し番号を、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。

<speed>

- 通信速度
  9600 / 19200 / 38400 / 57600 / 115200 / 230400

[説明]

COM ポートの通信速度を指定します。

[未設定時]

COM ポートの通信速度が 115200bps とみなされます。

```
serial <number> modem speed 115200
```

2.2 モデム関連情報

2.2.1 serial modem dial

[機能]

ダイヤル方式の設定

[入力形式]

serial [<number>] modem dial <type>

[パラメタ]

<number>

- serial 定義番号
  serial 定義の通し番号を、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>

- tone
  トーン式を使用します。
- pulse
  パルス式を使用します。

[説明]

モデムでダイヤルするときにトーン式を使うかパルス式を使うかを設定します。

[未設定時]

モデムでダイヤルするときにトーン式を使用するものとみなされます。

```
serial <number> modem dial tone
```

2.2.2　serial modem tonedetect

[機能]

ダイヤルトーン検出の設定

[入力形式]

serial [<number>] modem tonedetect <mode>

[パラメタ]

<number>

- serial 定義番号
  serial 定義の通し番号を、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
  ダイヤルトーンを検出します。
- off
  ダイヤルトーンを検出しません。

[説明]

ダイヤルする前にダイヤルトーンを検出するかを設定します。

[未設定時]

ダイヤルする前にダイヤルトーンを検出するものとみなされます。

```
serial <number> modem tonedetect on
```

2.2.3 serial modem speaker mode

[機能]

スピーカモード の設定

[入力形式]

serial [<number>] modem speaker mode <mode>

[パラメタ]

<number>

- serial 定義番号
  serial 定義の通し番号を、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
  スピーカを ON にします。
- off
  スピーカを OFF にします。
- dial
  スピーカを呼毎に ON にします。
- setup
  スピーカをダイヤル終了からキャリア検出まで ON にします。

[説明]

スピーカをどのタイミングでならすかを定義します。

[未設定時]

スピーカを呼毎に ON にするものとみなされます。

```
serial <number> modem speaker mode dial
```

2.2.4　serial modem speaker volume

[機能]

スピーカ音量の設定

[入力形式]

serial [<number>] modem speaker volume <mode>

[パラメタ]

<number>

- serial 定義番号
  serial 定義の通し番号を、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>

- high
  スピーカ音量を大に設定します。
- medium
  スピーカ音量を中に設定します。
- low
  スピーカ音量を小に設定します。

[説明]

スピーカの音量を設定します。

[未設定時]

スピーカの音量は中とみなされます。

```
serial <number> modem speaker volume medium
```

第 3 章　LAN 情報の設定

- lan 定義番号の指定範囲
  本章のコマンド の [パラメタ] に記載されている<number>(lan 定義番号) に指定する lan 定義の通し番号 (10 進数値) は、機種ごとに以下に示す範囲で指定してください。

範囲	機種
0〜19	MR1000

3.1　lan 共通情報

3.1.1　lan bind

[機能]

利用する物理回線の設定

[入力形式]

lan [<number>] bind <slot> [<line>]

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<slot>

必ず"mb"(基本ボード) を指定してください。

<line>

- 回線番号
  同一のボード に複数の回線がある場合に、どの回線を利用するか指定します。
  省略した場合は、0 を指定したものとみなされます。

[説明]

lan 定義で利用する物理回線を設定します。
複数の lan 定義で同一の回線を指定すると、もっとも小さい定義番号を持つ lan 定義だけが有効となり、他の lan 定義は無効となります。

[未設定時]

基本ボード 上における、回線番号が定義番号<number>となる回線を設定したものとみなされます。

```
lan <number> bind mb <number>
```

3.1.2 lan mode

[機能]

通信速度および通信モード の設定

[入力形式]

lan [<number>] mode <speed> [<duplex>]

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<speed>

通信速度を指定します。

- auto
  通信速度を自動的に設定する場合に指定します。通信速度と共に、全二重 / 半二重モード が HUB とのネゴシエーションによって自動的に設定されます。
- 通信速度
  通信速度を固定して動作させる場合に、以下のどちらかを指定します。

  10 10Mbps 固定で動作する

  100 100Mbps 固定で動作する

<duplex>

- 全二重 / 半二重モード
  <speed>で通信速度の固定値を指定した場合にだけ指定できます。以下のどちらかを指定します。

  full 全二重 (Full duplex) 固定で動作します。

  half 半二重 (Half duplex) 固定で動作します。

[説明]

Ethernet インタフェースの動作モード を設定します。

[未設定時]

通信速度および全二重 / 半二重モード を自動設定するものとみなされます。

```
lan <number> mode auto
```

3.1.3　lan mdi

[機能]

MDI の設定

[入力形式]

lan [<number>] mdi <mode>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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>

MDI のモードを指定します。

- mdi
  MDI として動作します。
- mdix
  MDI-X として動作します。

[説明]

MDI のモードを設定します。

[注意]

MR1000 の LAN0 ポートでは、MDI のモードを指定しても有効になりません。to HUB to PC スイッチで設定してください。

[未設定時]

MDI として動作します。

```
lan <number> mdi mdi
```

3.1.4 lan mtu

[機能]

送信パケット最大長 (MTU 値) の設定

[入力形式]

lan [<number>] mtu <mtu>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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]

LAN 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 LAN に対して送信するパケットの最大長が変更されます。

[未設定時]

MTU 値に 1500 を指定したものとみなされます。

```
lan <number> mtu 1500
```

3.1.5　lan shaping

[機能]

シェーピング機能の設定

[入力形式]

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

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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～100000k、または 1m～100m 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 または m 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。
  単位文字 m を付与した場合、単位は Mbps となります。
  1Kbps は 1000bps、1Mbps は 1000Kbps 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。

[注意]

シェーピングを使用しない場合、帯域制御は有効に動作しません。

[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。

```
lan <number> shaping off
```

3.2 LAN ポート バックアップ関連情報

3.2.1 lan backup bind

[機能]

バックアップとして利用する物理回線の設定

[入力形式]

lan [<number>] backup bind <slot> [<line>]

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<slot>

必ず"mb"(基本ボード) を指定してください。

<line>

- 回線番号
  同一のボード に複数の回線がある場合に、どの回線を利用するか指定します。

[説明]

LAN ポートバックアップ機能を利用する場合に、lan 定義でバックアップとして利用する物理回線を設定します。ここで、バックアップ用として設定された物理回線は、別の lan 定義で利用することはできません。また、すでに別の lan 定義で利用されている物理回線は、バックアップ用として利用できません。

[未設定時]

LAN ポートバックアップ機能を利用しないものとみなされます。

3.2.2　lan backup mode

[機能]

使用するポートの選択方法の設定

[入力形式]

lan [<number>] backup mode <mode>

[パラメタ]

<mode>

master ポートと backup ポートの両方が使用可能のときに使用するポートの選択方法を指定します。

- master
  master ポートを優先的に使用します。
- earlier
  先にリンクアップして使用可能になったほうのポートを使用します。

[説明]

master ポートと backup ポートの両方が使用可能のときに使用するポートの選択方法を指定します。

[未設定時]

master ポートを優先的に使用します。

```
lan <number> backup mode master
```

3.3 LAN ポート 閉塞関連情報

3.3.1 lan recovery

[機能]

自動復旧モード の設定

[入力形式]

lan [<number>] recovery <mode> <startup>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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>

- auto
  LAN 障害復旧時に自動復旧します。
- manual
  LAN 障害発生時に自動的に閉塞状態となり、LAN 障害が復旧した場合においてもオペレータ指示があるまで復旧させません。

<startup>

- up
  装置起動時、および動的定義反映時は閉塞していない状態で動作を開始します。
- down
  装置起動時、および動的定義反映時は閉塞状態で動作を開始し、オペレータからの閉塞状態解除指示を待ちます。

[説明]

LAN 障害の復旧時の動作モード を設定します。
起動時の動作は以下のようになります。

<mode>/<startup>	起動時のLANポートの状態	
	リンクアップ可能	リンクアップ不可能
auto / up	リンクアップ／通信可能	リンクダウン／通信不可
auto /down	閉塞状態に入り通信不可	閉塞状態に入り通信不可
manual/ up	リンクアップ／通信可能	リンクダウン／通信不可(※)
manual/down	閉塞状態に入り通信不可	閉塞状態に入り通信不可

※ リンクアップ不可であっても、起動時に最初から
閉塞状態に入るわけではないので注意してください

[注意]

VLAN インタフェースに対して本コマンド を設定しても、無効となります。
閉塞状態に入ると、リンクランプは消灯します。
閉塞状態では、LAN 定義が無い場合と同じ状態になります。ランプ表示もそれに準じたものになります。

[未設定時]

装置起動時、および動的定義反映時に閉塞していない状態で動作を開始し、LAN 障害発生時には障害復旧後に自動復旧します。

```
lan <number> recovery auto up
```

3.4 IP 関連情報

3.4.1 lan ip address

[機能]

IP アドレスの設定

[入力形式]

lan [<number>] ip address <address> / <mask> <broadcast>

[パラメタ]

<number>

- lan 定義番号

  lan 定義の通し番号を、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>

- IP アドレス / マスクビット数 (またはマスク値)

  LAN インタフェースに割り当てる 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。

  IP アドレスの指定可能な範囲は以下のとおりです。

  0.0.0.0

  1.0.0.1 ～ 126.255.255.254

  128.0.0.1 ～ 191.255.255.254

  192.0.0.1 ～ 223.255.255.254

  マスクビット数の場合は、2～30 の 10 進数値で指定します。

  マスク値の場合は、192.0.0.0～255.255.255.252 の範囲で指定します。

  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)

<broadcast>

ブロードキャストアドレスを指定します。

- 0

  0.0.0.0 の場合に指定します。

- 1

  255.255.255.255 の場合に指定します。

- 2

  <address> / <mask>から求められる、ネットワークアドレス + オール 0 の場合に指定します。

- 3

  <address> / <mask>から求められる、ネットワークアドレス + オール 1 の場合に指定します。

[説明]

本装置上の LAN インタフェースに、IP アドレス、マスクビット数 (またはマスク値)、およびブロードキャストアドレスを設定します。

LAN インタフェースに割り当てる IP アドレス、ネットマスクを設定します。IP アドレスを設定していないと通信できません。

DHCP クライアントで運用しない LAN インタフェースの場合は、<address>/<mask>に 0.0.0.0/0 を設定すると通信できなくなります。

DHCP クライアントで運用する LAN インタフェースの場合は、DHCP サーバから IP アドレスなどを割り当てられるので、<address>/<mask>に 0.0.0.0/0 を設定しなければなりません。

[未設定時]

IP アドレスがないものとみなされます。

```
lan <number> ip address 0.0.0.0/0 0
```

3.4.2 lan ip alias

[機能]

セカンダリ IP アドレスの設定

[入力形式]

lan [<number>] ip alias <address>/<mask> <broadcast>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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>

- セカンダリ IP アドレス/マスクビット数 (またはマスク値)
  LAN インタフェースに割り当てるセカンダリ 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。
  セカンダリ IP アドレスの指定可能な範囲は以下のとおりです。

  0.0.0.0
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  マスクビット数の場合は、2～30 の 10 進数値で指定します。
  マスク値の場合は、192.0.0.0～255.255.255.252 の範囲で指定します。
  以下に、有効な記述形式を示します。

  - セカンダリ IP アドレス/マスクビット数 (例: 192.168.1.1/24)
  - セカンダリ IP アドレス/マスク値 (例: 192.168.1.1/255.255.255.0)

<broadcast>

ブロードキャストアドレスを指定します。

- 0
  0.0.0.0 の場合に指定します。
- 1
  255.255.255.255 の場合に指定します。
- 2
  <address>/<mask>から求められる、ネットワークアドレス + オール 0 の場合に指定します。
- 3
  <address>/<mask>から求められる、ネットワークアドレス + オール 1 の場合に指定します。

[説明]

本装置上の LAN インタフェースに、セカンダリ IP アドレス、マスクビット数 (またはマスク値)、およびブロードキャストアドレスを設定します。

[注意]

セカンダリ IP アドレスが属するネットワークには、以下の機能を適用できません。

- RIP の送受信機能
- OSPF の送受信機能
- DHCP 機能

[未設定時]

セカンダリ IP アドレスがないものとみなされます。

```
lan <number> ip alias 0.0.0.0 0
```

3.4.3 lan ip dhcp service

[機能]

DHCP 機能の設定

[入力形式]

lan [<number>] ip dhcp service <mode> [<address1> [<address2>]]

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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>

DHCP 機能のモードを指定します。

- server
  LAN インタフェースに対して DHCP サーバサービスを行います。
- relay
  LAN インタフェースに対して DHCP リレーエージェントサービスを行います。
- client
  LAN インタフェースに対して DHCP サービスを要求します。
- off
  LAN インタフェースに対して DHCP 機能を提供しません。

<address1>,<address2>

- DHCP サーバアドレス
  <mode>に relay を指定した場合に有効なパラメタです。DHCP サービス要求を転送する、中継先 DHCP サーバの IP アドレスを 2 つまで指定することができます。
  指定可能な範囲は以下のとおりです。

  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

[説明]

LAN インタフェースに対して、DHCP 機能情報を設定します。

[未設定時]

DHCP サーバ機能を使用しないものとみなされます。

```
lan <number> ip dhcp service off
```

3.4.4　lan ip dhcp info

[機能]

DHCP 配布情報の設定

[入力形式]

lan [<number>] ip dhcp info dns <dns1> [<dns2>]
lan [<number>] ip dhcp info address <address> / <mask> [<num>]
lan [<number>] ip dhcp info time <time>
lan [<number>] ip dhcp info gateway <gateway>
lan [<number>] ip dhcp info domain <domain>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<dns1>

- DNS サーバ IP アドレス
  DHCP クライアントに配布する、DNS サーバの IP アドレスを指定します。
  0.0.0.0 を指定した場合は、設定が削除されます。
  指定可能な範囲は以下のとおりです。

  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

<dns2>

- セカンダリ DNS サーバ IP アドレス
  DHCP クライアントに配布する、セカンダリ DNS サーバの IP アドレスを指定します。
  0.0.0.0 を指定した場合は、設定が削除されます。
  指定可能な範囲は以下のとおりです。

  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

<address>/<mask>

- 割り当て開始 IP アドレス / マスクビット数 (またはマスク値)
  DHCP クライアントにリースする先頭アドレス (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: 192.168.1.2 / 24 注)
  - IP アドレス / マスク値 (例: 192.168.1.2 / 255.255.255.0 注)

<num>が 16、<address>が 192.168.1.2 の場合に、192.168.1.2〜192.168.1.17 のアドレスがリースされます。

0.0.0.0 / 0(0.0.0.0 / 0.0.0.0) を指定した場合は、設定が削除されます。

指定可能な範囲は以下のとおりです。

1.0.0.1 〜 126.255.255.254

128.0.0.1 〜 191.255.255.254

192.0.0.1 〜 223.255.255.254

<num>

- 割り当てアドレス数

  “3.4.3 lan ip dhcp service” の<mode>に server を指定した場合にだけ有効です。

  DHCP サーバサービスの場合に、割り当て可能な IP アドレスの総数を 1〜253 の 10 進数値で指定します。

  省略した場合は、32 を指定したものとみなされます。

ホストデータベース機能を使用すると、特定の DHCP クライアントに対して固有の IP アドレスを割り当てることができます。この場合の IP アドレスは、割当て先頭 IP アドレスと割当てアドレス数によって規定される動的割当て範囲である必要はありません。

<time>

- 割り当て時間

  DHCP クライアントに配布する情報の有効時間を、0 秒〜365 日の範囲で指定します。

  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。

  0 秒を指定した場合は、設定が削除され、有効時間監視なし (無限) とみなされます。

<gateway>

- デフォルトルータ IP アドレス

  DHCP クライアントに配布する、デフォルトルータの IP アドレスを設定します。

  0.0.0.0 を指定した場合は、設定が削除されます。

  指定可能な範囲は以下のとおりです。

  1.0.0.1 〜 126.255.255.254

  128.0.0.1 〜 191.255.255.254

  192.0.0.1 〜 223.255.255.254

<domain>

- ドメイン名

  DHCP クライアントに配布するドメイン名を、0x21,0x23〜0x7e の 80 文字以内の ASCII 文字列で指定します。なお、RFC1034 では英数字、"-"(ハイフン)、"."(ピリオド) でドメイン名をつけることを推奨しています。

[説明]

DHCP サーバ機能を使用する場合に、クライアントに配布する情報を設定します。

[未設定時]

DHCP で配布される情報は設定されないものとみなされます。

3.4.5　lan ip proxyarp

[機能]

ProxyARP 機能の設定

[入力形式]

lan [<number>] ip proxyarp <mode>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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
  ProxyARP 機能を使用します。
- off
  ProxyARP 機能を使用しません。

[説明]

ProxyARP 機能を使用するかどうかを設定します。

[未設定時]

ProxyARP 機能を使用するものとみなされます。

```
lan <number> ip proxyarp on
```

3.4.6 lan ip localproxyarp

[機能]

ローカル ProxyARP 機能の設定

[入力形式]

lan [<number>] ip localproxyarp <mode>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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
  ローカル ProxyARP 機能を使用します。
- off
  ローカル ProxyARP 機能を使用しません。

[説明]

ローカル ProxyARP 機能を使用するかどうかを設定します。
on を設定した場合には，ローカル ProxyARP が動作すると共に ICMP redirect パケットの送出が抑止されます.

[注意]

ローカル ProxyARP 機能は、端末間の直接通信が意図的に禁止されているネットワークでのみ使用してください。

[未設定時]

ローカル ProxyARP 機能を使用しないものとみなされます。

```
lan <number> ip localproxyarp off
```

3.4.7　lan ip route

[機能]

IPv4 スタティック経路情報の設定

[入力形式]

lan [<number>] ip route <count> <address> / <mask> <next_hop> [<metric> [<distance>]]

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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>

- スタティック経路情報定義番号
  スタティック経路情報の定義番号を、10 進数値で指定します。

範囲	機種
0〜255	MR1000

<address>/<mask>

- IPv4 アドレス / マスクビット数 (またはマスク値)
  あて先ネットワークを 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
  あて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。

<next_hop>

- 中継ルータ IPv4 アドレス
  あて先ネットワークへパケットを送信するときの中継ルータの IPv4 アドレスを指定します。

<metric>

- RIP メトリック値
  このスタティック経路情報を RIP に再配布するときのメトリック値を、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。

<distance>

- 優先度
  このスタティック経路情報の優先度を、0〜254 の 10 進数値で指定します。優先度は数値の小さい方がより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]

IPv4 スタティック経路 (静的経路) 情報を設定します。

RIP メトリック値は、スタティック経路情報を RIP に再配布するときのメトリック値を設定します。

RIP に再配布したときは、設定した RIP メトリック値+1 のメトリック値で RIP テーブルに登録されます。

優先度は、同じあて先への経路情報が複数ある場合、優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。各ダイナミックルーティングプロトコルの優先度については、routemanage ip distance コマンドを参照してください。

優先度に 0 が設定されているときは、routemanage interface floating コマンドでのフローティング設定に応じてフローティング動作が切り替わります。優先度に 1 以上が設定されているときは、常にフローティング動作します。

フローティング動作する場合、<next_hop>で指定した中継ルータと隣接しているインタフェースが通信可能な状態（リンクアップなど）であれば、スタティック経路情報をルーティングテーブルに追加します。通信不可能な状態（リンダウンなど）であれば、ルーティングテーブルから削除します。

フローティング動作しない場合は、インタフェースの状態にかかわらず常にスタティック経路情報をルーティングテーブルに追加します。

下記に、各設定値とフローティング動作の関係を示します。

<distance> 設定値	インタフェース経路の フローティング設定	スタティック経路の フローティング動作
0(省略値)	使用しない	しない
0(省略値)	使用する	する
1以上	使用しない	する
1以上	使用する	する

以下のような用途でスタティック経路情報を使用する場合、フローティング動作するとなるように設定してください。

- IP ルーティングおよびダイナミックルーティングでの広報において、スタティック経路の出口インタフェースで異常が発生した場合、ルーティングテーブルよりスタティック経路を削除する。
- あて先が同じ経路をダイナミックルーティングで受信した場合、優先度関係により経路を決定する。

  複数のスタティック経路情報で ECMP 機能を使用するときは、あて先、RIP メトリック値、優先度がそれぞれ同じとなるようにスタティック経路情報を設定します。また、ECMP 機能を使用する場合は、routemanage ip ecmp mode コマンドで ECMP を使用するように設定します。

  ECMP となるスタティック経路情報は、同じあて先への経路情報ごとに装置全体で 4 個まで定義できます。

IPv4 スタティック経路情報は、本装置全体で以下の数まで定義できます。

最大定義数	機種
256	MR1000

[注意]

同じあて先へのスタティック経路情報を複数設定する場合、以下の点に注意してください。

- 優先度が 0 のスタティック経路情報と、優先度が 0 または 1 以上のスタティック経路情報は同時に設定できません。
- 優先度が同じで、RIP メトリック値が違うスタティック経路情報は同時に設定できません。

[未設定時]

IPv4 スタティック経路情報を使用しないものとみなされます。

3.4.8 lan ip rip use

[機能]

RIP 基本情報の設定

[入力形式]

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

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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(Broadcast) を送信します。
- v2
  RIPv2(Broadcast) を送信します。
- 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 パケット送信時の加算メトリック値を、0～16 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。

<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]

RIP の基本的な動作を設定します。
<metric>は、RIP パケットを送信する際に加算するメトリック値を設定します。
RIP(IPv4) を使用するインタフェースは、本装置全体で以下の数まで定義できます。

最大定義数	機種
120	MR1000

[注意]

lan mtu コマンドを使用し、MTU 値を 576 よりも小さい値を設定すると、RIPv1(Broadcast), RIPv2(Broadcast) 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。NAT との併用はできません。

[未設定時]

RIP 機能を使用しないものとみなされます。

```
lan <number> ip rip use off off 0 off
```

3.4.9 lan ip rip filter act

[機能]

RIP フィルタ動作の設定

[入力形式]

lan [<number>] ip rip filter <count> act <action> <direction>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜399	MR1000

<action>

フィルタリング条件に一致した場合の動作を指定します。

- pass
  該当する経路情報を透過します。
- reject
  該当する経路情報を遮断します。

<direction>

フィルタリングを行う方向を指定します。

- in
  受信時にフィルタリングを行います。
- out
  送信時にフィルタリングを行います。

[説明]

RIP での経路情報送受信時に、フィルタリング条件に一致した経路情報を通過 (pass) させるか遮断 (reject) させるかを設定します。フィルタリング条件は優先度順に検索し、条件に一致した経路情報があった時点でフィルタリングが行われ、それ以降の条件は参照されません。全条件に不一致の経路情報は遮断されます。

フィルタリング条件は、lan ip rip filter route コマンドを使用し経路情報を設定します。

<count>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号が既に存在する場合は、既存の定義が上書きされます。

RIP フィルタは、本装置全体で以下の数まで定義できます。

最大定義数	機種
400	MR1000

[注意事項]

フィルタリング条件が設定されていない場合、本コマンドの設定は無効となります。

[未設定時]

RIP フィルタを使用しないものとみなされ、すべての RIP の経路情報が透過します。

3.4.10 lan ip rip filter move

[機能]

RIP フィルタの優先順序の変更

[入力形式]

lan [<number>] ip rip filter move <count> <new_count>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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、10 進数値で指定します。
  すで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。

範囲	機種
0～399	MR1000

[説明]

RIP フィルタの優先順序を変更します。
<new_count>で、既存定義番号を指定した場合、その定義の前に挿入されます。また、<new_count>は順番にソートされてリナンバリングされます。

3.4.11　lan ip rip filter route

[機能]

RIP フィルタの経路情報設定

[入力形式]

lan [<number>] ip rip filter <count> route <address>/<mask> [<prefix_match>]

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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定義番号を、10 進数値で指定します。優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜399	MR1000

<address>/<mask>

- IPv4 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経路情報を、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)
- any
  すべての経路情報をフィルタリング対象とする場合に指定します。
- default
  デフォルトルート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。

<prefix_match>

経路情報 (IPv4 アドレス/マスク) の検索条件を指定します。
省略した場合は、exact を指定したものとみなされます。
<address>/<mask>に"any"または"default"を指定した場合は、<prefix_match>は指定できません。

- exact
  指定した<address>/<mask>と経路情報の IPv4 アドレス/マスクを比較し、一致した場合に、フィルタリング対象とします。
- inexact
  指定した<address>と経路情報の IPv4 アドレスを比較し、<mask>まで一致した場合、フィルタリング対象とします。

[説明]

フィルタリング条件として経路情報を設定します。

[未設定時]

フィルタリング条件が設定されていないものとみなされます。

3.4.12　lan ip rip filter set metric

[機能]

RIP フィルタのメトリック設定

[入力形式]

lan [<number>] ip rip filter <count> set metric <metric>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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定義番号を、10 進数値で指定します。優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜399	MR1000

<metric>

- メトリック値
  メトリック値を、0〜16 の 10 進数値で指定します。

[説明]

フィルタリング条件に一致した経路情報のメトリック値を変更します。<metric>に 1〜16 を設定した場合、メトリック値は設定した値に変更されます。また、この場合、lan ip rip use コマンドで設定した加算メトリック値は加算されません。0 を指定した場合、メトリック値の変更は行われません。

[注意事項]

フィルタリング条件が設定されていない場合、本コマンドの設定は無効となります。
フィルタリング条件の"any"と一致した場合、本コマンドの設定は無効となります。

[未設定時]

フィルタリング条件に一致した経路情報のメトリック値を変更しないものとみなされます。

3.4.13 lan ip ospf use

[機能]

OSPF 利用可否の設定

[入力形式]

lan [<number>] ip ospf use <mode> [<area_number>]

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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
  OSPF を利用しません。
- on
  OSPF を利用します。

<area_number>

- エリア定義番号
  OSPF を利用する場合は、エリアの定義番号を指定します。
  省略した場合は、0 を指定したものとみなされます。

範囲	機種
0〜2	MR1000

[説明]

OSPF を利用するかどうかと、インタフェースが属するエリアの定義番号を設定します。
OSPF を使用するインタフェースは、本装置全体で以下の数まで定義できます。

最大定義数	機種
100	MR1000

[注意]

OSPF の利用は、"ospf ip area id"を設定した場合にだけ有効です。

[未設定時]

OSPF を使用しないものとみなされます。

```
lan <number> ip ospf use off
```

3.4.14　lan ip ospf cost

[機能]

OSPF 出力コストの設定

[入力形式]

lan [<number>] ip ospf cost <cost>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<cost>

- 出力コスト
  出力コストを、1～65535 で指定します。

[説明]

OSPF 出力コストを設定します。

[未設定時]

OSPF 出力コストに 10 が設定されているものとみなされます。

```
lan <number> ip ospf cost 10
```

3.4.15 lan ip ospf hello

[機能]

OSPF Hello パケット送信間隔の設定

[入力形式]

lan [<number>] ip ospf hello <hello_interval>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<hello_interval>

- Hello パケット送信間隔
  Hello パケットの送信間隔時間を、1 秒～65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、1s～65535s、1m～1092m、1h～18h です。

[説明]

OSPF 隣接関係の維持に用いられる Hello パケットの送信間隔を設定します。
hello_interval の値は OSPF 隣接ルータ間で同じ値を設定します。

[注意]

OSPF 隣接ルータ間で異なる Hello パケットの送信間隔を設定した場合、ルーティングが行えません。

[未設定時]

Hello パケット送信間隔に 10 秒が設定されているものとみなされます。

```
lan <number> ip ospf hello 10s
```

3.4.16　lan ip ospf dead

[機能]

OSPF 隣接ルータ停止確認間隔の設定

[入力形式]

lan [<number>] ip ospf dead <dead_interval>

[パラメタ]

<number>

- lan 定義番号

  lan 定義の通し番号を、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。

<dead_interval>

- 隣接ルータ停止確認間隔

  隣接ルータ停止確認の間隔時間を、1 秒～65535 秒の範囲で指定します。

  単位は、h(時)、m(分)、s(秒) のどれかを指定します。

  各単位での設定可能範囲は、1s～65535s、1m～1092m、1h～18h です。

[説明]

OSPF 隣接関係の維持に用いられる隣接ルータ停止確認間隔を設定します。

隣接ルータ停止確認間隔の間に Hello パケットを受信しなかった場合は、そのルータとの隣接関係は解除されます。

dead_interval の値は OSPF 隣接ルータ間で同じ値を設定します。

dead_interval の値は Hello パケット送信間隔よりも大きな値を設定する必要があります。

Hello パケット送信間隔の 4 倍を設定することを推奨します。

[注意]

OSPF 隣接ルータ間で異なる隣接ルータ停止確認間隔を設定した場合、ルーティングが行えません。

隣接ルータ停止確認間隔の設定値は、装置起動時において指定ルータ / 副指定ルータの選出を開始するまでの待機時間にも使用されます。大きな値を設定した場合は、経路交換の開始が遅れます。

[未設定時]

隣接ルータ停止確認間隔に 40 秒が設定されているものとみなされます。

```
lan <number> ip ospf dead 40s
```

3.4.17 lan ip ospf retrans

[機能]

OSPF パケット再送間隔の設定

[入力形式]

lan [<number>] ip ospf retrans <retransmit_interval>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<retransmit_interval>

- パケット再送間隔
  パケットの再送間隔を、3 秒～65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、3s～65535s、1m～1092m、1h～18h です。

[説明]

OSPF パケットを再送する間隔を設定します。

[未設定時]

OSPF パケットの再送間隔に 5 秒が設定されているものとみなされます。

```
lan <number> ip ospf retrans 5s
```

3.4.18　lan ip ospf delay

[機能]

OSPF LSU パケット送信遅延時間の設定

[入力形式]

lan [<number>] ip ospf delay <transmit_delay>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<transmit_delay>

- LSU パケット送信遅延時間
  LSU パケットを送信する場合の遅延時間を、1 秒～65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、1s～65535s、1m～1092m、1h～18h です。

[説明]

LSU(Link State Update) パケットの送信遅延時間を設定します。
LSU パケットでは、LSA(Link State Advertisement) を作成してからの経過時間に<transmit_delay>の値を加算して広報します。

[注意]

一般的な装置では、作成してからの経過時間が 1 時間となった LSA を破棄します。このため、LSU 送信遅延時間に 1 時間以上を設定した場合は、正しくルーティングできない場合があります。

[未設定時]

LSU パケット送信遅延時間に 1 秒が設定されているものとみなされます。

```
lan <number> ip ospf delay 1s
```

3.4.19 lan ip ospf priority

[機能]

OSPF 指定ルータ優先度の設定

[入力形式]

lan [<number>] ip ospf priority <priority>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<priority>

- 指定ルータ優先度
  指定ルータ優先度を、0～255 で指定します。

[説明]

指定ルータ、副指定ルータを決定するための優先度を設定します。
priority の値は、大きいほど優先度が高くなります。値が 0 の場合は、指定ルータ、副指定ルータにはなりません。

[未設定時]

指定ルータ優先度に 1 を指定したものとみなされます。

```
lan <number> ip ospf priority 1
```

3.4.20　lan ip ospf auth type

[機能]

OSPF パケット認証方式の設定

[入力形式]

lan [<number>] ip ospf auth type <authtype>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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>

パケット認証方式を指定します。

- off
  認証を行いません。
- text
  テキスト認証を使用します。
- md5
  MD5 認証を使用します。

[説明]

OSPF パケットに対する認証方式を設定します。

[注意]

テキスト認証の使用は、"lan ip ospf auth textkey"を設定した場合にだけ有効です。MD5 認証の使用は、"lan ip ospf auth md5key"を設定した場合にだけ有効です。

[未設定時]

OSPF パケット認証を使用しないものとみなされます。

```
lan <number> ip ospf auth type off
```

3.4.21 lan ip ospf auth textkey

[機能]

OSPF テキスト認証鍵の設定

[入力形式]

lan [<number>] ip ospf auth textkey <kind> <key> [encrypted]

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

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

<key>

- テキスト認証鍵
  文字列鍵の場合は、0x21,0x23～0x7e のコードで構成される 8 文字以内の ASCII 文字列で指定します。
  16 進数鍵の場合は、16 桁以内の 16 進数値で指定します。16 桁未満の値を指定したときは左詰めで設定され、残りは 16 桁になるまで 0x0 でパディングされます。
- 暗号化されたテキスト認証鍵
  show コマンドで表示される暗号化されたテキスト認証鍵を 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

- 暗号化テキスト認証鍵指定
  <key>に暗号化されたテキスト認証鍵を指定する場合に指定します。

[説明]

テキスト認証で使用する鍵を設定します。
show コマンドでは、暗号化されたテキスト認証鍵が encrypted と共に表示されます。

[未設定時]

テキスト認証鍵が設定されていないものとみなされます。

3.4.22　lan ip ospf auth md5key

[機能]

OSPF MD5 認証鍵情報の設定

[入力形式]

lan [<number>] ip ospf auth md5key <key_id> <key> [encrypted]

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<key_id>

- MD5 認証鍵 ID
  MD5 認証鍵 ID を、1～255 で指定します。
- 暗号化された MD5 認証鍵 ID
  show コマンドで表示される暗号化された MD5 認証鍵 ID 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。

<key>

- MD5 認証鍵
  MD5 認証鍵を、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。
- 暗号化された MD5 認証鍵
  show コマンドで表示される暗号化された MD5 認証鍵を 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 MD5 認証鍵情報指定
  <key_id>と<key>に暗号化された MD5 認証鍵 ID と MD5 認証鍵を指定する場合に指定します。

[説明]

MD5 認証で使用する鍵情報 (MD5 認証鍵 ID、MD5 認証鍵) を設定します。
show コマンドでは、暗号化された MD5 認証鍵 ID と MD5 認証鍵が encrypted と共に表示されます。

[未設定時]

MD5 認証で使用する鍵情報が設定されていないものとみなされます。

3.4.23 lan ip ospf passive

[機能]

OSPF パケット送信抑止の設定

[入力形式]

lan [<number>] ip ospf passive <interface_type>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<interface_type>

- on
  パケットの送信を抑止します。
- off
  パケットの送信を抑止しません。

[説明]

OSPF パケット送信の抑止を設定します。

[未設定時]

OSPF パケットの送信は抑止しないものとみなされます。

```
lan <number> ip ospf passive off
```

3.4.24　lan ip vrf use

[機能]

BGP / MPLS VPN 利用可否の設定

[入力形式]

lan [<number>] ip vrf use <mode> [<vrf_number>]

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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
  VRF を利用しません。
- on
  VRF を利用します。

<vrf_number>

- VRF 定義番号
  VRF を利用する場合は、VRF の定義番号を 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。

範囲	機種
0〜1	MR1000

[説明]

BGP / MPLS VPN を利用するかどうかを設定します。
利用する場合は、VRF の定義番号を設定します。

[未設定時]

BGP / MPLS VPN を使用しないものとみなされます。

```
lan <number> ip vrf use off
```

3.4.25 lan ip vrf route

[機能]

BGP / MPLS VPN 用 IPv4 スタティック経路情報の設定

[入力形式]

lan [<number>] ip vrf route <count> <address> / <mask> <next_hop>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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>

- スタティック経路情報定義番号
  スタティック経路情報の定義番号を、10 進数値で指定します。

範囲	機種
0〜63	MR1000

<address>/<mask>

- IPv4 アドレス / マスクビット数 (またはマスク値)
  あて先ネットワークを 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
  あて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。

<next_hop>

- 中継ルータ IPv4 アドレス
  あて先ネットワークへパケットを送信するときの中継ルータの IPv4 アドレスを指定します。

[説明]

BGP / MPLS VPN で使用する IPv4 スタティック経路情報を設定します。
本装置全体で以下の数まで定義できます。

最大定義数	機種
64	MR1000

[注意]

メトリック、優先度は設定できません。

[未設定時]

BGP / MPLS VPN 用 IPv4 スタティック経路を使用しないものとみなされます。

3.4.26 lan ip nat mode

[機能]

アドレス変換の設定

[入力形式]

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

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。
- static
  静的 NAT だけを使用します。

以下のパラメタは、<mode>に nat または multi または static を設定した場合に有効です。

<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 DHCP サーバから割り当てられた IP アドレスを使用します。

<addr_number>

- グローバル IP アドレスの個数
  動的アドレス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。
  <address>に any を指定した場合は、1 を指定してください。

<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) のどれかを指定します。
  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]

LAN インタフェース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。

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

3.4.27 lan ip nat static

[機能]

静的アドレス変換の設定

[入力形式]

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

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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、10 進数値で指定します。

範囲	機種
0〜199	MR1000

<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だけ指定可能です。
- 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]

LAN インタフェース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、本装置全体で以下の数まで定義できます。

最大定義数	機種
200	MR1000

[未設定時]

静的アドレス変換は設定されません。

3.4.28 lan ip nat static default

[機能]

テーブルに一致しないパケットの扱いの設定

[入力形式]

lan [<number>] ip nat static default <action>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<action>

すべての NAT テーブルにも一致しなかったパケットをどう扱うかを指定します。

- pass
  該当するパケットの IP アドレスやポート番号を変換しないで透過させます。
- reject
  該当するパケットを破棄します。

[説明]

すべての NAT テーブルに一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

すべての NAT テーブルにも一致しないパケットは破棄します。

```
lan <number> ip nat static default reject
```

3.4.29　lan ip nat rule

[機能]

アドレス変換ルールの設定

[入力形式]

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

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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 アドレスおよ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だけ有効となります。DNS の応答の UDP パケットのソース IP アドレスおよ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 アドレスおよ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 アドレスおよ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 アドレスおよびポート番号のチェックを行いません。

[説明]

LAN インタフェース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。

3.4.30　lan ip nat wellknown

[機能]

ポート番号変換の設定

[入力形式]

lan [<number>] ip nat wellknown <count> <port> <mode>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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>

ポート番号変換定義番号を、0～99 の 10 進数値で指定します。

<port>

- プライベートポート番号
  プライベートポート番号を、1～65535 の 10 進数値で指定します。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。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)
- any
  すべてのプライベートポート番号を対象とする場合に指定します。

<mode>

- on
  well-known ポート番号とみなし、変換を行いません。
- off
  well-known ポート番号とみなさず、変換を行います。

[説明]

プライベートポート番号の変換を行うかどうかの設定をします。プライベートポート番号がいずれの設定にもあてはまらない場合には、未設定時と同様にプライベートポート番号の変換を行います。ポート番号変換の設定は本装置全体で 100 個まで定義できます。

[未設定時]

以下のポート番号についてはポート番号の変換を行いません。
1～1024(本来の well-known ポート番号)
28800～28830(Microsoft Internet Gaming Zone)
1558(StreamWorks)
8000(StreamWorks)
118(Diablo)
116(Diablo)
6112(Battle.net)

6799(NETSTORM)
6800(NETSTORM)
9000(HEAVY GEAR)
7070(Real Player)
7000(VDO Live Video)
6667(IRC)
7648(CU-SeeMe)
7649(CU-SeeMe)
40027(SurfV)
40026(SurfV)
1638(DARK REIGN)

3.4.31　lan ip filter

[機能]

IP フィルタの設定

[入力形式]

lan [<number>] ip filter <count> <action> <src_addr>/<mask> <src_port> <dst_addr>/<mask> <dst_port> <protocol> <tcpconnect> [<tos> [<direction> [<icmptype> [<icmpcode>]]]]

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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、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すでに存在する場合は、既存の定義を変更します。

範囲	機種
0〜199	MR1000

<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。

<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あて先 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あて先 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
  すべてのあて先 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あて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あて先ポート番号を、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
  すべてのあて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、1〜255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。
- any
  すべてのプロトコル番号をフィルタリング対象とする場合に指定します。

<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。

<direction>

フィルタリングする方向を指定します。
省略した場合は、any を指定したものとみなされます。

- any
  入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。
- in
  入力パケットだけをフィルタリング対象とする場合に指定します。
- out
  出力パケットだけをフィルタリング対象とする場合に指定します。
- reverse
  入力パケットと出力パケットの両方をフィルタリング対象とします。
  ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。
  - 送信元 IP アドレス/マスクとあて先 IP アドレス/マスク
  - 送信元ポート番号とあて先ポート番号

<icmptype>

フィルタリング対象とする ICMP TYPE を指定します。

- ICMP TYPE
  フィルタリング対象とする送信元 ICMP TYPE を、0～255 の 10 進数値で指定します。複数の ICMP TYPE 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、「8-30」のように"-"(ハイフン) を使用して指定します。
  ICMP TYPE 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。
  - 0～255 の 10 進数値 (例: 8 = ICMP TYPE 8)
  - ICMP TYPE-ICMP TYPE (例: 2-8 = 2 から 8 までの ICMP TYPE)
  - ICMP TYPE- (例: 8- = 8 から 255 までの ICMP TYPE)

- -ICMP TYPE (例: -200 = 0 から 200 までの ICMP TYPE)
- ICMP TYPE,ICMP TYPE,… (例: 0,8,30- = 0 と 8 と 30 以降の ICMP TYPE)

- any
  すべての ICMP TYPE をフィルタリング対象とする場合に指定します。

<icmpcode>

フィルタリング対象とする ICMP CODE を指定します。

- ICMP CODE
  フィルタリング対象とする送信元 ICMP CODE を、0～255 の 10 進数値で指定します。複数の ICMP CODE 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、「8-30」のように"-"(ハイフン) を使用して指定します。
  ICMP CODE 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。
  - 0～255 の 10 進数値 (例: 8 = ICMP CODE 8)
  - ICMP CODE-ICMP CODE (例: 2-8 = 2 から 8 までの ICMP CODE)
  - ICMP CODE- (例: 8- = 8 から 255 までの ICMP CODE)
  - -ICMP CODE (例: -200 = 0 から 200 までの ICMP CODE)
  - ICMP CODE,ICMP CODE,… (例: 0,8,30- = 0 と 8 と 30 以降の ICMP CODE)

- any
  すべての ICMP CODE をフィルタリング対象とする場合に指定します。

[説明]

LAN インタフェースに対する 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 ICMP TYPE, ICMP CODE と一致するパケットを透過または遮断します。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 フィルタリング定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
200	MR1000

[注意]

<direction>に reverse を指定した場合には、入力パケットは IP アドレス/マスクとポート番号だけを逆転した条件でフィルタリングされます。このため、<tcpconnect>を有効にしている場合には、入力パケットに対しても、TCP プロトコルのコネクション接続要求がフィルタリング対象に含まれます。

[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。

3.4.32　lan ip filter move

[機能]

IP フィルタの優先順序の変更

[入力形式]

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

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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、10 進数値で指定します。
  すで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。

範囲	機種
0～199	MR1000

[説明]

IP フィルタの優先順序を変更します。

3.4.33 lan ip filter default

[機能]

いずれの IP フィルタテーブルにも不一致時の動作の設定

[入力形式]

lan [<number>] ip filter default <action> [<time>]

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<action>

いずれの IP フィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

- 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。
- spi
  該当するパケットに対して SPI を動作させます。

<time>

- 割当時間
  action に spi を指定したときに、接続に割り当てられた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) のどれかを指定します。
  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]

いずれの IP フィルタテーブルにも一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

いずれの IP フィルタテーブルにも一致しないパケットは透過します。

```
lan <number> ip filter default pass
```

3.4.34　lan ip tos

[機能]

TOS 値書き換え条件の設定

[入力形式]

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

[パラメタ]

<number>

- lan 定義番号

  lan 定義の通し番号を、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、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 値書き換え定義がすでに存在する場合は、既存定義の値を変更します。

範囲	機種
0〜99	MR1000

<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あて先 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あて先 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
  すべてのあて先 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あて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あて先ポート番号を、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>

TOS 値書き換え対象となるプロトコル番号を指定します。

- 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、1〜255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。
- any
  すべてのプロトコル番号を TOS 値書き換え対象とする場合に指定します。

<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 値書き換え定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
100	MR1000

[未設定時]

TOS 値書き換えを行わないものとみなされます。

3.4.35　lan ip tos move

[機能]

TOS 値書き換え条件の優先度の変更

[入力形式]

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

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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、10 進数値で指定します。
  すで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。

範囲	機種
0～99	MR1000

[説明]

TOS 値書き換え条件の優先度を変更します。

3.4.36　lan ip priority

[機能]

帯域制御の設定

[入力形式]

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

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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、10 進数値で指定します。

範囲	機種
0〜99	MR1000

<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あて先 IP アドレス、マスクビット数を指定します。

- あて先 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あて先 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あて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あて先ポート番号を、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>

帯域制御の対象となるプロトコル番号を指定します。

- 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、1～255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。
- any
  すべてのプロトコル番号を帯域制御の対象とする場合に指定します。

<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>

- express
  最優先データとして扱います。
- besteffort
  非優先 (ベストエフォート) として扱います。
- 帯域
  1～99 の 10 進数値で指定した場合、それぞれ指定した値の比で帯域を割り当てます。たとえば、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。「数字 + "kbps"(,"mbps")」で指定した場合、指定した帯域をそのまま割り当てます。1kbps～100000kbps または、1mbps～100mbps の範囲で指定します。全定義の帯域の合計が回線速度を超えた場合には、それぞれ指定した値の比で帯域を割り当てます。指定した値の合計値が回線速度に達しない場合、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。
  「"share" + 数字」で指定した場合、数字で指定した帯域制御定義番号で定義された帯域を共有します。この場合、指定する数字は自分自身の帯域制御定義番号より小さい、すでに定義されているものを指定しなければなりません。

[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、本装置全体で以下の数まで定義できます。

最大定義数	機種
100	MR1000

[注意]

IPv4,IPv6 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。
シェーピングを使用しない場合、帯域制御は有効に動作しません。

[未設定時]

帯域制御を行わないものとみなされます。

3.4.37 lan ip icmp redirect

[機能]

ICMP リダイレクトパケットの設定

[入力形式]

lan [<number>] ip icmp redirect <mode>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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>

ICMP リダイレクトパケットを送信するかどうかを指定します。

- on
  ICMP リダイレクトパケットを送信します。
- off
  ICMP リダイレクトパケットを送信しません。

[説明]

ICMP リダイレクトパケットを送信するかどうかを指定します。
<mode>に on が指定されている場合、ICMP リダイレクトパケットを送信します。
<mode>に off が指定されている場合、ICMP リダイレクトパケットを送信しません。

[未設定時]

ICMP リダイレクトパケットを送信するものとみなされます。

```
lan <number> ip icmp redirect on
```

3.4.38　lan ip multicast mode

[機能]

マルチキャストインタフェースの定義

[入力形式]

lan [<number>] ip multicast mode <mode>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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>

マルチキャスト定義の動作を指定します。

- off
  マルチキャストパケットを中継しません。
- static
  スタティックルーティングのみで動作します。
- pimdm
  PIM-DM として動作します。
- pimsm
  PIM-SM として動作します。

[説明]

<number>で指定したインタフェースのマルチキャスト・ルーティングプロトコルを有効化し、マルチキャストパケットを中継します。

[注意]

複数インタフェースで異なるプロトコルが選択された場合には、最初に見つかったインタフェースのプロトコルが有効になります。

[未設定時]

マルチキャストパケットを中継しません。

```
lan [<number>] ip multicast mode off
```

3.4.39 lan ip multicast ttl threshold

[機能]

マルチキャストインタフェースの TTL しきい値の定義

[入力形式]

lan [<number>] ip multicast ttl threshold <threshold>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<threshold>

- TTL しきい値
  マルチキャストパケットを中継するインタフェースの TTL のしきい値を 1～255 の 10 進数値で指定します。

[説明]

TTL が<threshold>で指定したしきい値以上のマルチキャストパケットだけ中継します。

[注意]

PIM-SM の PIM Register パケットによりカプセル化されるマルチキャスト・パケットは、出力先インタフェースの TTL しきい値の設定によらずに出力されます。

[未設定時]

1 になります。

```
lan [<number>] ip multicast ttl threshold 1
```

3.4.40　lan ip multicast pim preference

[機能]

マルチキャストインタフェースの PIM プリファレンス値の定義

[入力形式]

lan [<number>] ip multicast pim preference <preference>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<preference>

- プリファレンス値
  マルチキャストパケットを中継するインタフェースの PIM プリファレンス値を 1～65535 の 10 進数値で指定します。

[説明]

マルチキャスト・パケットの配送経路が重複した場合には、プリファレンス値の小さい経路で配送されます。

[注意]

PIM Assert 発行時には Assert 対象となるパケットの発信元へのユニキャスト経路を参照し、発信元へ向かうインタフェースのプリファレンス値を Assert メッセージに格納します。Assert メッセージが出力されるインタフェースのプリファレンス値が格納されるわけではありません。

[未設定時]

1024 になります。

```
lan [<number>] ip multicast pim preference 1024
```

3.4.41 lan ip multicast pim upstream type

[機能]

上流ルータの種類によるマルチキャストパケット転送許可設定

[入力形式]

lan [<number>] ip multicast pim upstream type <type>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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>

- pim
  上流ルータが PIM ルータのときのみ、マルチキャストパケットを転送します。
- any
  上流ルータが PIM ルータでない場合でも、マルチキャストパケットを転送します。

[説明]

本装置より上流にルータが存在し、そのルータを経由してマルチキャストパケットが転送されてくる場合、どの種類のルータからのマルチキャストパケットを転送するかを指定します。

上流ルータが PIM ルータでない場合 (マルチキャストパケットをスタティック経路によって転送するルータであった場合) に転送を許可したい場合は <type> に any を指定することで転送を可能にします。

[注意]

受信インタフェースと同一の IP セグメントから送信された (直接接続されたホストからの) マルチキャストパケットについては、本コマンドの指定に関わらず転送が行なわれます。

[未設定時]

上流ルータが PIM ルータのときのみ、マルチキャストパケットを転送します。

```
lan [<number>] ip multicast pim upstream type pim
```

3.4.42　lan ip arp cycle

[機能]

ARP 定期送信機能の設定

[入力形式]

lan [<number>] ip arp cycle <interval>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<interval>

- ARP 定期送信のインターバル
  ARP Request の送信間隔を、10 秒～20 分の範囲で指定します。
  単位は、m(分)、s(秒) のどれかを指定します。

[説明]

ARP 定期送信を利用する場合に、送信間隔を設定します。

[注意]

IP アドレスが設定されていないインタフェースでは、ARP 定期送信は動作しません。
定期送信のタイマは５秒刻みで動作するため、実際の送信間隔は５秒単位で繰り上げられます。たとえばインターバルを 21 秒に設定したときには、実際の送信間隔は 25 秒になります。

[未設定時]

ARP Request の定期送信を行いません。

3.5 IPv6 関連情報

3.5.1 lan ip6 use

[機能]

IPv6 機能の設定

[入力形式]

lan [<number>] ip6 use <mode>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

```
lan <number> ip6 use off
```

3.5.2　lan ip6 ifid

[機能]

IPv6 インタフェース ID の設定

[入力形式]

lan [<number>] ip6 ifid <interfaceID>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

```
lan <number> ip6 ifid auto
```

3.5.3 lan ip6 address

[機能]

IPv6 アドレスの設定

[入力形式]

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

[パラメタ]

<number>

- lan 定義番号

  lan 定義の通し番号を、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。

  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/プレフィックス長

  IPv6 アドレスとプレフィックス長を指定します。リンクローカルアドレスは指定できません。IPv6 DHCP クライアントが取得したプレフィックスを使用する場合は上位を"dhcp@インタフェース名"の形式で指定し，下位 80bit 分を IPv6 アドレス形式で指定します。インタフェース名には、rmt インタフェースを以下の範囲で指定します。

範囲	機種
rmt0〜rmt99	MR1000

例)rmt0 で動作する IPv6 DHCP クライアントが取得した IPv6 プレフィックスを使用する場合の設定例
dhcp@rmt0::/64
dhcp@rmt0::1:2:3:4/64
プレフィックス長には 64 を指定してください。

<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) のどれかを指定します。

  <address>/<prefixlen>に IPv6 DHCP クライアントが取得したプレフィックスを使用する指定をした場合は、IPv6 DHCP クライアントが取得した valid lifetime と比較して短い方が有効になります。

- 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) のどれかを指定します。

  <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。

  <address>/<prefixlen>に IPv6 DHCP クライアントが取得したプレフィックスを使用する指定をした場合は、IPv6 DHCP クライアントが取得した preferred lifetime と比較して短い方が有効になります。

- 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 0～ff の 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。

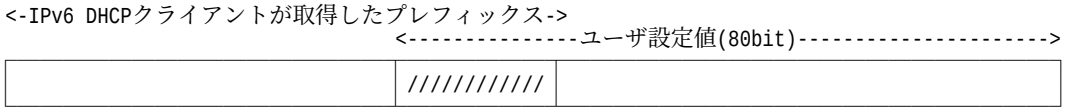
[説明]

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。

[注意]

IPv6 DHCP クライアントが取得したプレフィックスと設定値の重なる部分において，0 以外の値がある場合には，IPv6 アドレスは割り当てられません.



設定値が重なる部分

例）IPv6 DHCPクライアントが2001:db8:1000:5555::/64を取得した場合

設定内容	利用されるアドレス
dhcp@rmt0:0:100::1/64	2001:db8:1000:5555:100::1/64
dhcp@rmt0:100:200::1/64	無効

[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。

3.5.4 lan ip6 ra mode

[機能]

Router Advertisement の動作の設定

[入力形式]

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

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

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

3.5.5　lan ip6 ra interval

[機能]

Router Advertisement メッセージ送信間隔の設定

[入力形式]

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

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

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

3.5.6 lan 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]

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

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

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

3.5.7　lan 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]

lan [<number>] ip6 ra reachabletime <reachabletime>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<reachabletime>

- 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。

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

3.5.8 lan 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]

lan [<number>] ip6 ra retranstimer <retranstimer>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<retranstimer>

- 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。

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

3.5.9　lan 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]

lan [<number>] ip6 ra curhoplimit <curhoplimit>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

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

3.5.10 lan 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]

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

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

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

3.5.11　lan ip6 route

[機能]

IPv6 スタティック経路情報の設定

[入力形式]

lan [<number>] ip6 route <count> <address> / <prefixlen> <next_hop> [<metric> [<distance>]]

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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>

- スタティック経路情報定義番号
  スタティック経路情報の定義番号を、10 進数値で指定します。

範囲	機種
0〜255	MR1000

<address>/<prefixlen>

- IPv6 アドレス/プレフィックス
  あて先ネットワークを IPv6 アドレスとプレフィックスの組み合わせで指定します。
  リンクローカルアドレスは指定できません。
- default
  あて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。

<next_hop>

- 中継ルータ IPv6 アドレス
  あて先ネットワークへパケットを送信するときの中継ルータの IPv6 アドレスを指定します。
  ICMPv6redirect を正常に動作させるため、link-local address を指定してください。また、中継ルータが存在するネットワーク設定側に対して、適切にスタティック経路情報を設定してください。

<metric>

- RIP メトリック値
  このスタティック経路情報を RIP に再配布するときのメトリック値を、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。

<distance>

- 優先度
  このスタティック経路情報の優先度を、0〜254 の 10 進数値で指定します。
  優先度は数値の小さい方がより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]

IPv6 スタティック経路 (静的経路) 情報を設定します。

RIP メトリック値は、スタティック経路情報を RIP に再配布するときのメトリック値を設定します。RIP に再配布したときは、設定した RIP メトリック値+1 のメトリック値で RIP テーブルに登録されます。

優先度は、同じあて先への経路情報が複数ある場合、優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。各ダイナミックルーティングプロトコルの優先度については、routemanage ip6 distance コマンドを参照してください。

優先度に 0 が設定されているときは、routemanage interface floating コマンドでのフローティング設定に応じてフローティング動作が切り替わります。優先度に 1 以上が設定されているときは、常にフローティング動作します。

フローティング動作する場合、<next_hop>で指定した中継ルータと隣接しているインタフェースが通信可能な状態（リンクアップなど）であれば、スタティック経路情報をルーティングテーブルに追加します。通信不可能な状態（リンダウンなど）であれば、ルーティングテーブルから削除します。

フローティング動作しない場合は、インタフェースの状態にかかわらず常にスタティック経路情報をルーティングテーブルに追加します。

下記に、各設定値とフローティング動作の関係を示します。

<distance> 設定値	インタフェース経路の フローティング設定	スタティック経路の フローティング動作
0(省略値)	使用しない	しない
0(省略値)	使用する	する
1以上	使用しない	する
1以上	使用する	する

以下のような用途でスタティック経路情報を使用する場合、フローティング動作するとなるように設定してください。

- IP ルーティングおよびダイナミックルーティングでの広報において、スタティック経路の出口インタフェースで異常が発生した場合、ルーティングテーブルよりスタティック経路を削除する。
- あて先が同じ経路をダイナミックルーティングで受信した場合、優先度関係により経路を決定する。

IPv6 スタティック経路情報は、本装置全体で以下の数まで定義できます。

最大定義数	機種
256	MR1000

[注意]

同じあて先へのスタティック経路情報を複数設定する場合、以下の点に注意してください。

- 優先度が 0 のスタティック経路情報と、優先度が 0 または 1 以上のスタティック経路情報は同時に設定できません。
- 優先度が同じスタティック経路情報は同時に設定できません。

[未設定時]

IPv6 スタティック経路情報を使用しないものとみなされます。

3.5.12　lan ip6 rip use

[機能]

IPv6 RIP 基本情報の設定

[入力形式]

lan [<number>] ip6 rip use <send> <receive> [<metric>]

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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(IPv6) パケットを送信するかどうか指定します。

- on
  RIP(IPv6) パケットを送信します。
- off
  RIP(IPv6) パケットを送信しません。

<receive>

RIP(IPv6) パケットを受信するかどうか指定します。

- on
  RIP(IPv6) パケットを受信します。
- off
  RIP(IPv6) パケットを受信しません。

<metric>

- 加算メトリック値
  RIP(IPv6) パケット送信時の加算メトリック値を、0～16 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]

RIP(IPv6) の基本的な動作を設定します。<metric>は、RIP(IPv6) パケットを送信する際に加算するメトリック値を設定します。
RIP(IPv6) を使用するインタフェースは、本装置全体で以下の数まで定義できます。

最大定義数	機種
120	MR1000

[未設定時]

RIP(IPv6) 機能を使用しないものとみなされます。

```
lan <number> ip6 rip use off off 0
```

3.5.13 lan ip6 rip site-local

[機能]

IPv6 RIP site-local プレフィックス送受信の設定

[入力形式]

lan [<number>] ip6 rip site-local <mode>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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>

site-local プレフィックスを送受信するかどうかを指定します。

- on
  site-local プレフィックスを送受信します。
- off
  site-local プレフィックスを送受信しません。

[説明]

RIP(IPv6) で site-local プレフィックスを送受信するかどうかを設定します。

[未設定時]

site-local プレフィックスを送受信するものとみなされます。

```
lan <number> ip6 rip site-local on
```

3.5.14　lan ip6 rip aggregate

[機能]

IPv6 RIP における集約経路の設定

[入力形式]

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

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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
  集約経路のあて先ネットワークを 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
  集約経路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。

<rejectroute>

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

[説明]

RIP 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、実際に持たないあて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 reject 経路を設定することもできます。

同一 lan 定義内に同一の集約経路は設定できません。

[未設定時]

RIP(IPv6) で経路集約しないものとみなされます。

3.5.15 lan ip6 rip filter act

[機能]

IPv6 RIP フィルタ動作の設定

[入力形式]

lan [<number>] ip6 rip filter <count> act <action> <direction>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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定義番号を、10 進数値で指定します。優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜399	MR1000

<action>

フィルタリング条件に一致した場合の動作を指定します。

- pass
  該当する経路情報を透過します。
- reject
  該当する経路情報を遮断します。

<direction>

フィルタリングを行う方向を指定します。

- in
  受信時にフィルタリングを行います。
- out
  送信時にフィルタリングを行います。

[説明]

RIP(IPv6) での経路情報送受信時に、フィルタリング条件に一致した経路情報を通過 (pass) させるか遮断 (reject) させるかを設定します。フィルタリング条件は優先度順に検索し、条件に一致した経路情報があった時点でフィルタリングが行われ、それ以降の条件は参照されません。全条件に不一致の経路情報は遮断されます。

フィルタリング条件は、lan ip6 rip filter route コマンドを使用し経路情報を設定します。

<count>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号が既に存在する場合は、既存の定義が上書きされます。

RIP フィルタ (IPv6) は、本装置全体で以下の数まで定義できます。

最大定義数	機種
400	MR1000

[注意事項]

フィルタリング条件が設定されていない場合、本コマンドの設定は無効となります。

[未設定時]

RIP(IPv6) フィルタを使用しないものとみなされ、すべての RIP(IPv6) の経路情報が透過します。

3.5.16　lan ip6 rip filter move

[機能]

IPv6 RIP フィルタの優先順序の変更

[入力形式]

lan [<number>] ip6 rip filter move <count> <new_count>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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、10 進数値で指定します。
  すで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。

範囲	機種
0～399	MR1000

[説明]

RIP(IPv6) フィルタの優先順序を変更します。
<new_count>で、既存定義番号を指定した場合、その定義の前に挿入されます。また、
<new_count>は順番にソートされてリナンバリングされます。

3.5.17　lan ip6 rip filter route

[機能]

IPv6 RIP フィルタの経路情報設定

[入力形式]

lan [<number>] ip6 rip filter <count> route <address>/<prefixlen> [<prefix_match>]

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜399	MR1000

<address>/<prefixlen>

- 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経路情報を、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。
- any
  すべての経路情報をフィルタリング対象とする場合に指定します。
- default
  デフォルトルートをフィルタリング対象とする場合に指定します。

<prefix_match>

経路情報の検索条件を指定します。
省略した場合は、exact を指定したものとみなされます。
<address>/<prefixlen>に"any"または"default"を指定した場合は、<prefix_match>は指定できません。

- exact
  指定した<address>/<prefixlen>と経路情報の IPv6 アドレス/プレフィックス長を比較し、一致した場合に、フィルタリング対象とします。
- inexact
  指定した<address>と経路情報の IPv6 アドレスを比較し、<prefixlen>まで一致した場合、フィルタリング対象とします。

[説明]

フィルタリング条件として経路情報を設定します。

[未設定時]

フィルタリング条件が設定されていないものとみなされます。

3.5.18　lan ip6 rip filter set metric

[機能]

IPv6 RIP フィルタのメトリック設定

[入力形式]

lan [<number>] ip6 rip filter <count> set metric <metric>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0～399	MR1000

<metric>

- メトリック値
  メトリック値を、0～16 の 10 進数値で指定します。

[説明]

フィルタリング条件に一致した経路情報のメトリック値を変更します。<metric>に 1～16 を設定した場合、メトリック値は設定した値に変更されます。この場合、lan ip6 rip use コマンドで設定した加算メトリック値は加算されません。0 を指定した場合、メトリック値の変更は行われません。

[注意事項]

フィルタリング条件が設定されていない場合、本コマンドの設定は無効となります。
フィルタリング条件の"any"と一致した場合、本コマンドの設定は無効となります。

[未設定時]

フィルタリング条件に一致した経路情報のメトリック値を変更しないものとみなされます。

3.5.19　lan ip6 filter

[機能]

IPv6 フィルタの設定

[入力形式]

lan [<number>] ip6 filter <count> <action> <src_addr> / <prefixlen> <src_port> <dst_addr> / <prefixlen> <dst_port> <protocol> <tcpconnect> [<trafficclass> [<direction> [<icmptype> [<icmpcode>]]]]

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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、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。

範囲	機種
0〜199	MR1000

<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。

<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、0〜254 の 10 進数値で指定します。
- any
  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。

<trafficclass>

- フィルタリング対象 Traffic Class 値

  フィルタリング対象となる Traffic Class フィールドの値を 0-ff までの 16 進数値、または、"-"を使用して表現される 16 進数値の範囲を指定します。

  Traffic Class 値の指定は、"," を区切として 10 個まで設定可能です。

  複数の Traffic Class 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。

  Traffic Class 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 Traffic Class 値)
  - Traffic Class 値-Traffic Class 値 (例: 32-64 = 32 から 64 までの Traffic Class 値)
  - Traffic Class 値- (例: 80- = 80 から ff までの Traffic Class 値)
  - -Traffic Class 値 (例: -7f = 0 から 7f までの Traffic Class 値)
  - Traffic Class 値,Traffic Class 値,… (例: 10,20,30- = 10 と 20 と 30 以降の Traffic Class 値)

- any

  全ての Traffic Class 値をフィルタリング対象とします。省略された場合は any として扱われます。

<direction>

フィルタリングする方向を指定します。
省略した場合は、any を指定したものとみなされます。

- any

  入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。

- in

  入力パケットのみをフィルタリング対象とする場合に指定します。

- out

  出力パケットのみをフィルタリング対象とする場合に指定します。

- reverse

  入力パケットと出力パケットの両方をフィルタリング対象とします。ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。

  - 送信元 IP アドレス/プレフィックス長と宛先 IP アドレス/プレフィックス長
  - 送信元ポート番号と宛先ポート番号

<icmptype>

フィルタリングする ICMPv6 メッセージタイプ番号を指定します。

- フィルタリング対象 icmptype 値

  フィルタリング対象となる icmptype フィールドの値を 0-255 までの 10 進数値、または、"-"を使用して表現される 10 進数値の範囲を指定します。

  icmptype 値の指定は、"," を区切として 10 個まで設定可能です。

  記述形式は、<src_port>と同様です。

- any

  全ての icmptype 値をフィルタリング対象とします。省略された場合は any として扱われます。

<icmpcode>

フィルタリングする ICMPv6 メッセージコード番号を指定します。
icmpcode 指定時は、icmptype も指定する必要があります。

- フィルタリング対象 icmpcode 値
  フィルタリング対象となる icmpcode フィールドの値を 0-255 までの 10 進数値、または、"-"を使用して表現される 10 進数値の範囲を指定します。
  icmptype 値の指定は、"," を区切として 10 個まで設定可能です。
  記述形式は、<src_port>と同様です。
- any
  全ての icmpcode 値をフィルタリング対象とします。省略された場合は any として扱われます。

[説明]

このインタフェースに対する 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。
  - any 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 any 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。
- <icmptype>、<icmpcode>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 any を指定し、かつ<icmptype>、<icmpcode>を指定している場合、 ICMPv6 パケットの該当 type/code 番号を持つパケットのみが合致します。

- <protocol>に ICMPv6(58) を指定し、かつ<icmptype>、<icmpcode>を指定している場　合、指定プロトコルの該当 type/code 番号を持つパケットのみが合致します。
- <protocol>に ICMPv6(58) 以外を指定し、かつ<icmptype>、<icmpcode>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 フィルタリング定義は、本装置全体で次の数まで定義できます。

最大定義数	機種
200	MR1000

[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。

3.5.20　lan ip6 filter move

[機能]

IPv6 フィルタの優先順序の変更

[入力形式]

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

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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、10 進数値で指定します。
  すで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。

範囲	機種
0～199	MR1000

[説明]

IPv6 フィルタの優先順序を変更します。

3.5.21　lan ip6 filter default

[機能]

いずれの IP フィルタテーブルにも不一致時の動作の設定

[入力形式]

lan [<number>] ip6 filter default <action> [<time>]

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<action>

いずれの IPv6 フィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

- 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。
- spi
  該当するパケットに対して SPI を動作させます。

<time>

- 割当時間
  action に spi を指定したときに接続に割り当てられた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]

いずれの IPv6 フィルタテーブルにも一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

いずれの IPv6 フィルタテーブルにも一致しないパケットは透過します。

```
lan <number> ip6 filter default pass
```

3.5.22 lan ip6 trafficclass

[機能]

Traffic Class 値書き換え条件の設定

[入力形式]

lan [<number>] ip6 trafficclass <count> <src_addr>/<prefixlen> <src_port>
<dst_addr>/<prefixlen> <dst_port> <protocol> <trafficclass> <new_trafficclass>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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>

- Traffic Class 値書き換え定義番号
  Traffic Class 値書き換え条件の優先度を表す定義番号を、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 Traffic Class 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。

範囲	機種
0〜99	MR1000

<src_addr>/<prefixlen>

書き換え対象とする送信元 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
  書き換え対象とする送信元 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 アドレスを書き換え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>

書き換え対象とする送信元ポート番号を指定します。

- ポート番号
  書き換え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書き換え対象とする場合に指定します。

<dst_addr>/<prefixlen>

書き換え対象とする宛先 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
  書き換え対象とする宛先 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 アドレスを書き換え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>

書き換え対象とする宛先ポート番号を指定します。

- ポート番号
  書き換え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書き換え対象とする場合に指定します。

<protocol>

書き換え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
  書き換え対象とするプロトコル番号を、0〜254 の 10 進数値で指定します。
- any
  すべてのプロトコルを書き換え対象とします。

<trafficclass>

- Traffic Class 値
  書き換え対象となる Traffic Class フィールドの値を 0-ff までの 16 進数値、または、"-"を使用して表現される 16 進数値の範囲を指定します。
  Traffic Class 値の指定は、"," を区切として 10 個まで設定可能です。
  複数の Traffic Class 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。
  Traffic Class 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 Traffic Class 値)
  - Traffic Class 値-Traffic Class 値 (例: 32-64 = 32 から 64 までの Traffic Class 値)
  - Traffic Class 値- (例: 80- = 80 から ff までの Traffic Class 値)
  - -Traffic Class 値 (例: -7f = 0 から 7f までの Traffic Class 値)
  - Traffic Class 値,Traffic Class 値,… (例: 10,20,30- = 10 と 20 と 30 以降の Traffic Class 値)

- any
  すべての Traffic Class 値を書き換え対象とします。

<new_trafficclass>

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

[説明]

Traffic Class 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 Traffic Class 値を、指定した Traffic Class 値に書き換えます。
Traffic Class 値書き換え定義は、本装置全体で次の数まで定義できます。

最大定義数	機種
100	MR1000

[未設定時]

Traffic Class 値書き換えを行わないものとみなされます。

3.5.23　lan ip6 trafficclass move

[機能]

Traffic Class 値書き換え条件の優先度の変更

[入力形式]

lan [<number>] ip6 trafficclass move <count> <new_count>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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 Traffic Class 値書き換え定義番号
  優先順序を変更する前の Traffic Class 値書き換え定義番号を指定します。

<new_count>

- 移動先 Traffic Class 値書き換え定義番号
  <count>に対する新しい順序を、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。

範囲	機種
0〜99	MR1000

[説明]

Traffic Class 値書き換え条件の優先度を変更します。

3.5.24 lan ip6 priority

[機能]

IPv6 プロトコル帯域制御の設定

[入力形式]

lan [<number>] ip6 priority <count> <src_addr>/<prefixlen> <src_port> <dst_addr>/<prefixlen> <dst_port> <protocol> <trafficclass> <width>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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、10 進数値で指定します。

範囲	機種
0〜99	MR1000

<src_addr>/<prefixlen>

帯域制御の対象とする送信元 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
  帯域制御の対象とする送信元 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 アドレスを帯域制御の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>

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>/<prefixlen>

帯域制御の対象とする宛先 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
  帯域制御の対象とする宛先 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 アドレスを帯域制御の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>

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、0〜254 の 10 進数値で指定します
  (例: ICMPv6:58、TCP:6、UDP:17 など)。
- any
  すべてのプロトコル番号をフィルタリング対象とする場合に指定します。

<trafficclass>

- 帯域制御対象 Traffic Class 値
  帯域制御の対象となる Traffic Class フィールドの値を 0-ff までの 16 進数値、または、"-"を使用して表現される 16 進数値の範囲を指定します。Traffic Class 値の指定は、"," を区切として 10 個まで設定可能です。
  複数の Traffic Class 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。Traffic Class 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 Traffic Class 値)
  - Traffic Class 値-Traffic Class 値 (例: 32-64 = 32 から 64 までの Traffic Class 値)
  - Traffic Class 値- (例: 80- = 80 から ff までの Traffic Class 値)
  - -Traffic Class 値 (例: -7f = 0 から 7f までの Traffic Class 値)
  - Traffic Class 値,Traffic Class 値,… (例: 10,20,30- = 10 と 20 と 30 以降の Traffic Class 値)
- any
  すべての Traffic Class 値を、帯域制御の対象とします。省略された場合は any として扱われます。

<width>

- express
  最優先データとして扱います。
- besteffort
  非優先 (ベストエフォート) として扱います。

- 帯域

  1〜99 の 10 進数値で指定した場合、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。

  「数字 + "kbps"(,"mbps")」で指定した場合、指定した帯域をそのまま割り当てます。

  1kbps〜100000kbps または、1mbps〜100mbps の範囲で指定します。全定義の帯域の合計が回線速度を超えた場合には、それぞれ指定した値の比で帯域を割り当てます。指定した値の合計値が回線速度に達しない場合、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。

  「"share" + 数字」で指定した場合、数字で指定した帯域制御定義番号で定義された帯域を共有します。この場合、指定する数字は自分自身の帯域制御定義番号より小さい、すでに定義されているものを指定しなければなりません。

[説明]

IPv6 プロトコル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、トラフィッククラスを指定して、割り当てる帯域を指定します。

IPv6 プロトコル帯域制御は、本装置全体で次の数まで定義できます。

最大定義数	機種
100	MR1000

[注意]

IPv4,IPv6 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。シェーピングを使用しない場合、帯域制御は有効に動作しません。

[未設定時]

IPv6 プロトコル帯域制御を行わないものとみなされます。

3.6　ブリッジ関連情報

3.6.1　lan bridge use

[機能]

ブリッジ動作モード の設定

[入力形式]

lan [<number>] bridge use <mode>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

[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に設定してください。

[未設定時]

ブリッジを使用しないものとみなされます。

```
lan <number> bridge use off
```

3.6.2 lan bridge group

[機能]

ブリッジグループ識別子の設定

[入力形式]

lan [<number>] bridge group <group_id>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<group_id>

- グループ識別子
  グループ識別子を 10 進数値で指定します。

範囲	機種
0〜19	MR1000

[説明]

ブリッジのグループ識別子を設定します。

[未設定時]

グループ識別子に 0 を指定したものとみなされます。

```
lan <number> bridge group 0
```

3.6.3　lan bridge static

[機能]

静的学習テーブル情報の設定

[入力形式]

lan [<number>] bridge static <count> <mac>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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>

- 静的学習テーブル定義番号
  指定した定義番号と同じ値を持つ定義がすでに存在する場合は、既存の設定に対する修正とみなされます。

範囲	機種
0〜199	MR1000

<mac>

静的な定義として学習テーブルに追加する MAC アドレスを指定します。

[説明]

学習テーブルに指定された MAC アドレスを静的な学習テーブル情報として追加します。

3.6.4 lan bridge stp use

[機能]

STP 動作モード の設定

[入力形式]

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

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

[注意]

ブリッジグループ 0 以外のブリッジグループでは STP は動作しません。

[未設定時]

STP を使用しないものとみなされます。

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

3.6.5　lan bridge stp cost

[機能]

パスコストの設定

[入力形式]

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

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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>

LAN を経由する通信のパスコストを指定します。
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。

- 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	備考
Ethernet(100Mbps)		100	
Ethernet(10Mbps)		100	
HSD(64kbps)		15620	*：192kbps～1.5Mbpsは PRIの場合
HSD(128kbps)		7810	
HSD(192kbps)	*	1000	
HSD(256kbps)	*	1000	
HSD(384kbps)	*	1000	
HSD(512kbps)	*	1000	
HSD(768kbps)	*	1000	
HSD(1Mbps)	*	667	
HSD(1.5Mbps)	*	667	
FR(64kbps)		16000	
FR(128kbps)		8500	
FR(256kbps)	*	1100	
FR(384kbps)	*	1100	
FR(512kbps)	*	1100	
FR(768kbps)	*	1100	
FR(1Mbps)	*	680	
FR(1.5Mbps)	*	680	
ISDN(64kbps)		16000	
その他			
1Mbps>=速度		1000	
1.5Mbps>=速度>1Mbps		667	
4Mbps>=速度>1.5Mbps		250	
6Mbps>=速度>4Mbps		167	
10Mbps>=速度>6Mbps		100	
16Mbps>=速度>10Mbps		62	
20Mbps>=速度>16Mbps		50	
25Mbps>=速度>20Mbps		40	
40Mbps>=速度>25Mbps		25	
80Mbps>=速度>40Mbps		12	
速度>80Mbps		10	

- 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。

[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。

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

3.6.6　lan bridge stp priority

[機能]

インタフェース優先度の設定

[入力形式]

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

[パラメタ]

<number>

- lan 定義番号

  lan 定義の通し番号を、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。

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、定義番号のもっと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。

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

3.6.7 lan bridge filter

[機能]

MAC フィルタの設定

[入力形式]

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

[パラメタ]

<number>

- lan 定義番号

  lan 定義の通し番号を、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、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すでに存在する場合は、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。

範囲	機種
0〜255	MR1000

<action>

フィルタリング対象に該当するフレームを透過するかどうかを指定します。

- pass

  該当するフレームを透過します。

- reject

  該当するフレームを遮断します。

<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。

<dst_mac>

フィルタリング対象とするあて先 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 形式フレーム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 形式フレーム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
  すべてのフレームを対象とする場合に指定します。<value>は、指定不要です。

<vlan_analyze>

VLAN タグ付きフレームに対してタグの解析を行うかどうかを指定します。
<value>を指定したときだけ指定可能です。
省略した場合は、off を指定したものとみなされます。

- on
  VLAN タグ付きフレームの場合に VLAN タグを解析してフィルタリング処理を行います。VLAN タグ付きフレームの場合には、タグの長さ分ずれた位置にある LLC 形式
  フレームの LSAP や Ethernet 形式フレームのタイプに対してフィルタリング処理を行います。
- off
  VLAN タグ付きフレームの場合に VLAN タグを解析しないでフィルタリング処理を行います。VLAN タグ付きフレームの場合でもタグの長さ分ずらさすにそのままフィルタリング処理を行うため、VLAN タグの TPID が、<value>との比較対象になります。

[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フレームを、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、本装置全体で以下の数まで定義できます。

最大定義数	機種
256	MR1000

[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に設定してください。

[未設定時]

MAC フィルタを設定しないものとみなされ、すべてのフレームが透過します。

3.6.8　lan bridge filter move

[機能]

MAC フィルタの優先順序の変更

[入力形式]

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

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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、10 進数値で指定します。
  すで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。

範囲	機種
0～255	MR1000

[説明]

MAC フィルタの優先順序を変更します。

3.7 VRRP 関連情報

3.7.1 lan vrrp use

[機能]

VRRP 動作モード の設定

[入力形式]

lan [<number>] vrrp use <mode>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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>

VRRP 機能を使用するかどうかを指定します。

- on
  VRRP を使用する場合に指定します。
  <number>で指定した LAN インタフェースで VRRP が機能します。
- off
  VRRP を使用しない場合に指定します。
  <number>で指定した LAN インタフェースで VRRP は機能しません。

[説明]

この LAN インタフェースで、VRRP 機能を使用するかどうかを設定します。
VRRP 機能を使用しないと設定した場合、<number>で指定した LAN インタフェースでは VRRP 機能が動作しません。

[未設定時]

VRRP 機能を使用しないものとみなされます。

```
lan <number> vrrp use off
```

3.7.2　lan vrrp auth

[機能]

VRRP-AD の認証方法と認証パスワード の設定

[入力形式]

lan [<number>] vrrp auth <method> [<password>]

[パラメタ]

<number>

- lan 定義番号

  lan 定義の通し番号を、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。

<method>

認証方法について指定します。

- none

  <number>で指定した LAN インタフェースで VRRP-AD の認証を行いません。

- text

  <number>で指定した LAN インタフェースはテキスト パスワード を用いて VRRP-AD の認証を行います。

<password>

- 認証パスワード

  <method>に text を指定した場合、<number>で指定した LAN インタフェースで使用する VRRP-AD の認証パスワード を、0x21,0x23 ～ 0x7e の 8 桁以内の ASCII 文字列で指定します。

[説明]

この LAN インタフェースで VRRP-AD の認証に使用する認証方法と認証パスワード を設定します。

設定はこの LAN インタフェースに関係する VRRP グループのすべてに適用されます。

<method>に text を指定した場合は、パスワード を設定する必要があります。<method>に none を指定した場合、パスワード は指定できません。

[未設定時]

VRRP-AD の認証を使用しないものとみなされます。

```
lan <number> vrrp auth none
```

3.7.3 lan vrrp group id

[機能]

VRRP グループの設定

[入力形式]

lan [<number>] vrrp group <vrrp_number> id <vrid> <priority> [<virtual_ip#1> [<virtual_ip#2>]]

[パラメタ]

<number>

- lan 定義番号

  lan 定義の通し番号を、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。

<vrrp_number>

- VRRP グループ定義番号

  LAN インタフェースに対する VRRP グループ定義の通し番号を、0～1 の 10 進数値で指定します。

<vrid>

- VRID

  <vrrp_number>で定義した VRRP グループの保持する VRID を、1～255 の 10 進数値で指定します。

  VRID は装置内で一意でなければなりません。重複した VRID を指定した場合は<number>および<vrrp_number>の最小である設定だけが有効となり、他はすべて無効となります。

<priority>

- VRRP ルータの優先度

  VRRP ルータの優先度を、"master"、または 1～254 の 10 進数値で指定します。<priority>に"master"を指定した場合、VRRP グループは優先度 255 のマスタルータとして動作します。この場合、仮想ルータの IPv4 アドレスは<number>で指定した LAN インタフェースの実 IPv4 アドレスになります。

  lan <number> ip address <address> / <mask> <broadcast> で設定された<address>が実 IPv4 アドレスです。また、この場合には lan vrrp group preempt の指定は無効になり、プリエンプトモードは常に ON で動作します。

  それ以外の場合、VRRP グループは<priority>で指定した優先度のバックアップルータとして動作します。

  VRRP ルータの優先度は数値が大きいほど高くなります。

  トリガを使用する場合は優先度 1 の設定はさけてください。また、トリガを使用する場合は"master"を指定するとトリガが作動した場合に VRRP グループが設定された LAN が通信不能となります。トリガを使用する場合は"master"を指定しないでください。

<virtual_ip#X>

- 仮想ルータの IPv4 アドレス

  VRRP グループで使用する仮想ルータの IPv4 アドレスを指定します。

  指定可能な範囲は以下のとおりです。

  1.0.0.1 ～ 126.255.255.254

  128.0.0.1 ～ 191.255.255.254

  192.0.0.1 ～ 223.255.255.254

  <priority>に"master"を指定した場合は、仮想ルータの IPv4 アドレスは<number>で指定した LAN インタフェースの実 IPv4 アドレスとなるため、指定する事はできません。このときセカンダリ IPv4 アドレスが設定されている場合はセカンダリ IPv4 アドレスも仮想ルータの IPv4 アドレスとなります。

lan <number> ip alias <address> / <mask> <broadcast> で設定された<address>がセカンダリ IPv4 アドレスです。

それ以外の場合は、1 つ以上の仮想ルータの IPv4 アドレスを指定しなければなりません。また、その場合は VRRP グループ内で重複した仮想ルータの IPv4 アドレスを設定することはできません。仮想ルータの IPv4 アドレスに装置内のインタフェース実 IPv4 アドレスまたは、セカンダリ IPv4 アドレスを指定した場合は、この VRRP グループは無効となります。

[説明]

VRRP グループの VRID、優先度、仮想ルータの IPv4 アドレスを設定します。

マスタルータの設定は VRRP グループにつき 1 台の VRRP ルータにだけ行ってください。複数のマスタルータを設定した場合、仮想ルータを正しくバックアップすることができません。(VRRP グループで同一の仮想ルータの IPv4 アドレスが設定できないため。)

VRRP グループは VRID によって識別される同一 VRRP グループ内で優先度を競合し、マスタルータを決定します。

VRRP グループの仮想 MAC アドレスは VRID から自動的に生成されます。(00:00:5E:00:01:{VRID})

バックアップルータとして優先度を設定した場合でも、指定した優先度が同一 VRRP グループ内で最も高い優先度であればマスタルータとして動作します。また、VRRP ルータの優先度は VRRP グループ内で、できるだけ大きな差がつくように設定してください。近い優先度であった場合、マスタルータの切り替わりがスムーズに行われない場合があります。

VRRP 機能を使用する場合、本定義は必須定義であり未設定の場合は VRRP 機能が動作しません。

[未設定時]

VRRP グループの情報は設定されないものとみなされます。

3.7.4 lan vrrp group ad

[機能]

VRRP-AD の設定

[入力形式]

lan [<number>] vrrp group <vrrp_number> ad <interval>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<vrrp_number>

- VRRP グループ定義番号
  LAN インタフェースに対する VRRP グループ定義の通し番号を、0～1 の 10 進数値で指定します。

<interval>

- VRRP-AD 送出間隔
  VRRP-AD の送出間隔を、1 秒～255 秒の範囲で指定します。単位は、m(分)、s(秒) のどちらかを指定します。

[説明]

該当する自装置 VRRP グループが使用する VRRP-AD の送信間隔時間を設定します。
同一 VRRP グループ内では送出間隔時間を同じ値に設定してください。異なる値が設定された場合はスムーズにマスタルータの交代が行われなくなる可能性があります。

[未設定時]

VRRP-AD の送出間隔として 1 秒が設定されたものとみなされます。

```
lan <number> vrrp group <vrrp_number> ad 1s
```

3.7.5　lan vrrp group preempt

[機能]

プリエンプトモードの設定

[入力形式]

lan [<number>] vrrp group <vrrp_number> preempt <mode> [<time>]

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<vrrp_number>

- VRRP グループ定義番号
  LAN インタフェースに対する VRRP グループ定義の通し番号を、0～1 の 10 進数値で指定します。

<mode>

プリエンプトモードを指定します。

- on
  <vrrp_number>で指定した VRRP グループでプリエンプトモードを ON に設定します。
- off
  <vrrp_number>で指定した VRRP グループでプリエンプトモードを OFF に設定します。

<time>

- プリエンプトモード OFF への移行禁止時間
  VRRP が動作を開始してから、プリエンプトモード OFF へ移行するのを禁止する時間として 0 秒～900 秒の範囲で指定します。
  単位は、m(分)、s(秒) のどれかを指定します。
  省略した場合は、0 秒を指定したものとみなされます。
  なお、<mode>が off に設定されている場合にだけ有効であり、<mode>が on に設定される場合は指定できません。
  禁止時間内ではプリエンプトモードが ON に設定されたのと同様に動作します。この設定はシステム起動時に優先度の低いルータが先に動作を開始して、優先度の高いルータにマスタルータが渡されないようなことが発生する場合に有効です。

[説明]

VRRP グループのプリエンプトモードを設定します。

[未設定時]

プリエンプトモードに ON が設定されたものとみなされます。

```
lan <number> vrrp group <vrrp_number> preempt on
```

3.7.6 lan vrrp group trigger ifdown

[機能]

インタフェースダウントリガの設定

[入力形式]

lan [<number>] vrrp group <vrrp_number> trigger <trigger_no> ifdown <interface> [<priority>]

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<vrrp_number>

- VRRP グループ定義番号
  LAN インタフェースに対する VRRP グループ定義の通し番号を、0～1 の 10 進数値で指定します。

<trigger_no>

- トリガ定義番号
  VRRP グループに対するトリガ定義の通し番号を、10 進数値で指定します。

範囲	機種
0～127	MR1000

<interface>

トリガ対象インタフェースを指定します。

- インタフェース名
  lan または、rmt インタフェースを以下の範囲で指定します。

範囲	機種
lan0～lan19 rmt0～rmt99	MR1000

- any
  ループバックインタフェース以外すべてのパケット送出インタフェースをトリガ対象に含める場合に指定します。

<priority>

- 優先度
  変化させる優先度を、1～254 の 10 進数値で指定します。
  省略した場合は、254 を指定したものとみなされます。

[説明]

インタフェースダウントリガを設定します。

<interface>で指定したインタフェースがダウンした場合、トリガを適用します。

<interface>で指定したインタフェースが有効ではないインタフェースであった場合はトリガは動作しません。また、同一インタフェースに重複してトリガが設定された場合はすべてを適用します。

<interface>がリモートインタフェースである場合、ケーブル抜け、同期はずれ、または PVC 状態確認手順によって通信不可と判断された該当インタフェースに設定されたトリガを適用します。

トリガが適用された場合、VRRP グループの現在の優先度から<priority>で指定した値を減算した優先度の VRRP ルータとして動作します。

<priority>で優先度を減算すると 1 以下になる場合は、優先度 1 の VRRP ルータとして動作します。

[未設定時]

インタフェースダウントリガは設定されないものとみなされます。

3.7.7 lan vrrp group trigger route

[機能]

ルートダウントリガの設定

[入力形式]

lan [<number>] vrrp group <vrrp_number> trigger <trigger_no> route <dst_addr> <interface> [<priority>]

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<vrrp_number>

- VRRP グループ定義番号
  LAN インタフェースに対する VRRP グループ定義の通し番号を、0〜1 の 10 進数値で指定します。

<trigger_no>

- トリガ定義番号
  VRRP グループに対するトリガ定義の通し番号を、10 進数値で指定します。

範囲	機種
0〜127	MR1000

<dst_addr>

トリガを適用する経路を指定します。

- IPv4 アドレス / マスクビット数 (またはマスク値)
  あて先または中継先ネットワークの IPv4 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。
  - 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)

  設定値として、0.0.0.0 は指定できません。
- default
  経路としてデフォルトルートを指定します。

<interface>

トリガを適用する経路のパケット送出インタフェースを指定します。

- インタフェース名
  lan または、rmt インタフェースを以下の範囲で指定します。

範囲	機種
lan0〜lan19 rmt0〜rmt99	MR1000

- any
  パケット送出インタフェースを特定しない場合に指定します。

<priority>

- 優先度
  変化させる優先度を、1～254 の 10 進数値で指定します。
  省略した場合は、254 を指定したものとみなされます。

[説明]

ルートダウントリガを設定します。

<dst_addr>で指定したあて先のパケットを<interface>で指定したインタフェースに送出する経路がルーティングテーブルに存在しない場合、トリガを適用します。<interface>が any である場合は、送出先インタフェースに関係なくあて先の経路が存在していればトリガは適用となりません。

トリガが適用された場合、VRRP グループの現在の優先度から<priority>で指定した値を減算した優先度の VRRP ルータとして動作します。

<priority>で優先度を減算すると 1 以下になる場合は、優先度 1 の VRRP ルータとして動作します。

なお、VRRP グループが設定された LAN インタフェースがダウンした場合はこの限りではありません(自装置の VRRP グループは仮想ルータとして無効な状態となります)。

[未設定時]

ルートダウントリガは設定されないものとみなされます。

3.7.8 lan vrrp group trigger node

[機能]

ノードダウントリガの設定

[入力形式]

lan [<number>] vrrp group <vrrp_number> trigger <trigger_no> node <dst_addr> <interface> [<priority> [<resend_time> [<time_out> [<normal_interval> [error_interval>]]]]]

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<vrrp_number>

- VRRP グループ定義番号
  LAN インタフェースに対する VRRP グループ定義の通し番号を、
  0〜1 の 10 進数値で指定します。

<trigger_no>

- トリガ定義番号
  VRRP グループに対するトリガ定義の通し番号を、10 進数値で指定します。

範囲	機種
0〜127	MR1000

<dst_addr>

- ICMP ECHO パケットのあて先 IP アドレス
  ICMP ECHO パケットのあて先 IP アドレスを指定します。
  指定可能な範囲は以下のとおりです。
  1.0.0.1 〜 126.255.255.254
  128.0.0.1 〜 191.255.255.254
  192.0.0.1 〜 223.255.255.254

<interface>

ICMP ECHO パケットを送出するインタフェースを指定します。

- インタフェース名
  rmt インタフェースを以下の範囲で指定します。

範囲	機種
rmt0〜rmt99	MR1000

- any
  パケット送出インタフェースを特定しない場合に指定します。

<priority>

- 優先度

  変化させる優先度を、1～254 の 10 進数値で指定します。

  省略した場合は、254 を指定したものとみなされます。

<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) のどれかを指定します。

  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) のどれかを指定します。

  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) のどれかを指定します。

  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) のどれかを指定します。

  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]

ノードダウントリガを設定します。

<dst_addr>で指定したあて先に ICMP ECHO パケットを<interface>で指定したインタフェースから送出し、<time_out>時間応答がない場合、トリガを適用します。<interface>が any である場合、送出先インタフェースは経路情報に依存します。

トリガが適用された場合、VRRP グループの現在の優先度から<priority>で指定した値を減算した優先度の VRRP ルータとして動作します。

<priority>で優先度を減算すると 1 以下になる場合は、優先度 1 の VRRP ルータとして動作します。

なお、VRRP グループが設定された LAN インタフェースがダウンした場合はこの限りではありません(自装置の VRRP グループは仮想ルータとして無効な状態となります)。

[注意]

<dst_addr>にはブロードキャストアドレス、マルチキャストアドレスを指定しないでください。指定した場合は正常に動作しません。

優先度を"master"に設定した VRRP グループにノードダウントリガを設定した場合は正常に動作しません。ノードダウントリガを設定する場合は優先度を"master"以外にしてください。

ノードダウントリガで送信される ICMP ECHO パケットの送信元 IP アドレスは VRRP グループが設定された LAN のインタフェースアドレスとなりますので、ICMP ECHO 応答パケットの経路に注意してください。

ノードダウントリガでは定期的にパケットが送信されますので異常課金に注意してください。

[未設定時]

ノードダウントリガは設定されないものとみなされます。

3.8　MPLS 関連情報

3.8.1　lan mpls use

[機能]

MPLS 利用可否の設定

[入力形式]

lan [<number>] mpls use <mode>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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
  MPLS を利用します。
- off
  MPLS を利用しません。

[説明]

MPLS を利用するかどうかを設定します。

[未設定時]

off が選択されたものとして動作します。

```
lan <number> mpls use off
```

3.8.2 lan mpls distribution

[機能]

ラベル配布プロトコルの設定

[入力形式]

lan [<number>] mpls distribution <protocol>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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>

- ldp
  ラベル配布プロトコルに LDP を使用します。

[説明]

ラベル配布プロトコルを指定します。

[未設定時]

ldp が選択されたものとして動作します。

```
lan <number> mpls distribution ldp
```

3.8.3　lan mpls ldp hello-timers

[機能]

LDP Hello に関するタイマの設定

[入力形式]

lan [<number>] mpls ldp hello-timers <interval> <holdtime>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<interval>

- Hello 送信間隔のタイマ値
  Hello の送信間隔を、1 秒～65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。

<holdtime>

- HoldTime のタイマ値
  近隣関係の維持を判定するための HoldTime を、1 秒～65534 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
- infinity
  近隣関係の維持を判定するための HoldTime を infinity(0xffff:無限) とします。

[説明]

LDP 近隣関係の維持に用いられる Hello パケットの送信間隔と HoldTime を設定します。
HoldTime の値は interval の値より小さくすることはできません。
HoldTime の値は interval の値の 3 倍以上を設定することを推奨します。

[注意]

HoldTime は近隣関係にある LDP ルータとネゴシエーションし、値の小さい方が採用されますが、送信間隔はネゴシエーションしないため、相手 LSR のタイマ設定と自装置のタイマ設定を一致させておくことを推奨します。

[未設定時]

interval が 5 秒、HoldTime が 15 秒として動作します。

```
lan <number> mpls ldp hello-timers 5s 15s
```

3.8.4 lan mpls ldp keepalive-timers

[機能]

LDP KeepAlive に関するタイマの設定

[入力形式]

lan [<number>] mpls ldp keepalive-timers <interval> <timeout>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<interval>

- KeepAlive 送信間隔のタイマ値
  KeepAlive の送信間隔を、1 秒～65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。

<timeout>

- KeepAlive タイムアウトのタイマ値
  LDP セッションの維持を判定するためのタイムアウト時間を、1 秒～65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。

[説明]

LDP セッションの維持に用いられる KeepAlive メッセージの送信間隔とタイムアウトを設定します。
timeout の値は interval の値より小さくすることはできません。
timeout の値は interval の値の 3 倍以上を設定することを推奨します。

[注意]

タイムアウトは近隣関係にある LDP ルータとネゴシエーションし、値の小さい方が採用されますが、送信間隔はタイムアウトのネゴシエーション結果の 3 分の 1 の値とこのコマンドで設定された送信間隔とを比較し、値が小さい方が送信間隔として採用されます。

[未設定時]

interval が 1 分、timeout が 3 分として動作します。

```
lan <number> mpls ldp keepalive-timers 1m 3m
```

3.8.5　lan mpls ldp advertisement

[機能]

LDP ラベル広報方式の設定

[入力形式]

lan [<number>] mpls ldp advertisement <mode>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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>

- dod
  Downstream On Demand を使用します。
- du
  Downstream Unsolicited を使用します。

[説明]

LDP のラベル広報方式を指定します。

[未設定時]

du が選択されたものとして動作します。

```
lan <number> mpls ldp advertisement du
```

3.8.6 lan mpls ldp retention

[機能]

LDP ラベル保持方式の設定

[入力形式]

lan [<number>] mpls ldp retention <mode>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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>

- liberal
  Liberal Label Retention Mode を使用します。
- conservative
  Conservative Label Retention Mode を使用します。

[説明]

LDP のラベル保持方式を指定します。

[未設定時]

liberal が選択されたものとして動作します。

```
lan <number> mpls ldp retention liberal
```

3.8.7　lan mpls ldp interface-label

[機能]

PHP の無効化

[入力形式]

lan [<number>] mpls ldp interface-label <mode>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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
  インタフェースの IP アドレスにラベルを割り当てません。
- on
  インタフェースの IP アドレスにラベルを割り当てます。

[説明]

インタフェースの IP アドレスに対してラベルを割り当てるかどうかを指定します。
割り当てた場合は，インタフェース宛の LSP の PHP を無効にすることができます。

[注意]

MPLS トンネル接続機能を使用する場合、自側エンドポイントと IP アドレスが同一の時、本設定に依らず、PHP 機能は無効となります。

[未設定時]

off が選択されたものとして動作します。

```
lan <number> mpls ldp interface-label off
```

3.8.8 lan mpls ldp ip transport

[機能]

IPv4 Transport Address の設定

[入力形式]

lan [<number>] mpls ldp ip transport <address>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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>

- LDP セッションの送信元 IPv4 アドレス
  IPv4 アドレスを指定します。以下の範囲で指定してください。

  0.0.0.0
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

[説明]

インタフェース単位で LDP が相手との通信に用いる送信元 IPv4 アドレスを分ける必要がある場合に、本装置に設定された IPv4 アドレスを指定します。
0.0.0.0 を指定した場合は、MPLS 情報の設定の IPv4 Transport Address の設定に従います。

[未設定時]

MPLS 情報の設定の IPv4 Transport Address の設定に従います。

```
lan mpls ldp ip transport 0.0.0.0
```

[注意]

インタフェース単位で IPv4 Transport Address を設定する場合には、必ず本装置に存在するアドレスを指定してください。本装置に存在しないアドレスをインタフェースに指定した場合は、そのインタフェースでは LDP を使用できません。

3.8.9　lan mpls l2-circuit vc

[機能]

EoMPLS の VC 情報の設定

[入力形式]

lan [<number>] mpls l2-circuit vc <vc_id> <address> [<vc_type>]

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<vc_id>

- VC ID の設定
  lan 定義の VC ID を 1～4294967295 の 10 進数値で指定します。
  VC ID は装置内で一意でなければなりません。

<address>

- 相手装置の IPv4 アド レス
  指定可能な範囲は以下のとおりです。

  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

<vc_type>

- auto
  lan 定義から、ethernet か vlan かを自動的に識別します。
- ethernet
  lan 定義に関係なく VC Type を Ethernet に設定します。
- vlan
  lan 定義に関係なく VC Type を Ethernet VLAN に設定します。

省略時は auto を指定したものとみなされます。

[説明]

EoMPLS 通信の VC ID、相手装置のアド レス、VC Type の設定をします。

<vc_id> は EoMPLS 通信の相手装置と同じ値を指定します。本装置と相手装置で同じ VC ID を持つインタフェース同士を VC LSP で接続し、EoMPLS 通信を行います。VC ID 装置内で一意になるように設定する必要があります。

<address> は EoMPLS 通信の相手装置の IPv4 アド レスを指定します。相手装置にて指定した IPv4 Transport Address と同じ値を指定してください。EoMPLS 通信を行うためには相手装置のアド レスへの経路情報が必要となります。LDP ラベル広報経路情報の設定で、必要な経路情報を LDP で広報するように設定してください。

<vc_type> は、相手装置で同じ VC ID を持つインタフェースと同じ値を指定します。lan 定義と VC Type の設定の関係、および、EoMPLS 通信時のフレームの処理は以下のようになります。

本装置の設定		LDP の動作	EoMPLS 通信時のフレームの処理			
lan定義	<vc_type>の値	ラベル交換で使用するVC Type の値	lan定義のI/F側から タグなし受信	lan定義のI/F側から タグ付き受信	VC LSP側から タグなし受信	VC LSP側から タグ付き受信
VLAN定義していないlan定義	auto	Ethernet	そのまま転送	そのまま転送	そのまま転送	そのまま転送
	ethernet	Ethernet				
	vlan	Ethernet VLAN				
VLAN定義しているlan定義	auto	Ethernet VLAN	--	そのまま転送	タグを挿入して転送	タグを上書きして転送
	ethernet	Ethernet				
	vlan	Ethernet VLAN				

そのまま転送　　：フレームを加工せず、そのまま同じフレームを転送します。
タグを挿入して転送　：VC LSPから受信しlan定義に出力する際に、VLAN IDの設定、VLANのプライオリティ情報の設定で指定した VLAN タグをフレームに挿入します。
タグを上書きして転送：VC LSPから受信しlan定義に出力する際に、フレームに設定されている VLAN タグを、VLAN IDの設定、VLAN のプライオリティ情報の設定で指定した VLAN タグで上書きします。

[未設定時]

EoMPLS を使用しないものとみなされます。

[注意]

- 本設定で EoMPLS 通信の設定を行った LAN インタフェースでは、自装置宛の通信を含めて、すべての通信が EoMPLS 通信による転送の対象となります。
  このため本設定を行った lan 定義では以下の機能は使用できません。
  - IP 機能
  - IPv6 機能
  - ブリッジ機能 (STP、MAC 学習、MAC フィルタ機能を含みます)
  - VRRP 機能
  - MPLS 機能 (EoMPLS 機能は除きます)
- EoMPLS 通信の相手装置のアドレスが、MPLS LSP トンネルの REMOTE インタフェース設定のトンネルエンドポイントと同じである場合は、REMOTE インタフェースの設定で、MPLS を使用する、LDP Multicast Hello パケットを送信しない、と設定してください。
- EoMPLS 通信を行う場合は、MAC 学習や STP のサポートを行ないため、パケットのループが発生する構成は行わないでください。フレームがループし続け通信不可となります。EoMPLS 通信を用いて冗長構成を行う場合には、LAN インタフェース側に、STP 等を使用できるスイッチ装置を設置し、フレームがループしないようにしてください。
- VLAN タグが異なる VLAN インタフェース同士で EoMPLS 通信を行い、タグを上書きして転送する構成の場合は、STP パケットの VLAN タグも上書きされるため、STP が正常に動作しない可能性があります。VLAN インタフェース側で STP を使用する場合は、VLAN タグを本装置と相手装置で一致させてください。

3.8.10　lan mpls l2-circuit exp

[機能]

EoMPLS 通信時の Exp 値書き換えの設定

[入力形式]

lan [<number>] mpls l2-circuit exp {vlan|<exp>}

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

vlan

- VLAN タグのプライオリティを使用
  VLAN タグのプライオリティフィールドから値を取り出し、MPLS SHIM ヘッダの Exp フィールドにそのまま格納します。EoMPLS 通信で転送する
  フレームが VLAN でない場合は、Exp フィールドには 0 が格納されます。

<exp>

- 固定の Exp 値を使用
  書き換える Exp 値を、0〜7 の 10 進数値で設定します。

[説明]

EoMPLS 通信が用いる Exp 値を設定します。

[未設定時]

0 が設定されているものとみなされます。

```
lan mpls l2-circuit exp 0
```

[注意]

VC LSP と Tunnel LSP の両方で同じ Exp 値が格納されます。

3.9 VLAN 関連情報

3.9.1 lan vlan bind

[機能]

VLAN インタフェースの出力先の設定

[入力形式]

lan [<number>] vlan bind <master_number>

[パラメタ]

<number>

- lan 定義番号

  lan 定義の通し番号を、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。

<master_number>

出力先の物理 LAN インタフェースの定義番号を指定します。

[注意]

<master_number>に VLAN インタフェースを指定しても動作しません。

VLAN インタフェースの削除は通常の物理 LAN インタフェースと同様に delete lan コマンドによって行います。

lan vlan bind が設定されていない LAN インタフェースで VLAN の他の設定を行っても、無効となります。

[説明]

<master_number>で指定した物理 LAN インタフェースを出力先として、VLAN インタフェースとして動作します。lan vlan bind の定義がある LAN インタフェースは VLAN インタフェースとして動作し、lan vlan bind の定義がない LAN インタフェースは通常の物理 LAN インタフェースとして動作します。

VLAN インタフェースの IP アドレスは、lan ip address コマンドによって指定します。また VLAN 上で動作するサービスの定義は、通常の物理 LAN インタフェースと同様に lan コマンドで行います。

[未設定時]

VLAN として動作せず、通常の物理 LAN インタフェースとして動作します。

3.9.2　lan vlan tag vid

[機能]

VLAN ID の設定

[入力形式]

lan [<number>] vlan tag vid <vid>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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。

<vid>

VLAN ID を、1～4094 の 10 進数値で設定します。

[説明]

VLAN ID を設定します。

[未設定時]

<vid>に 1 が設定されたものとみなされます。

```
lan <number> vlan tag vid 1
```

3.9.3 lan vlan tag pri

[機能]

プライオリティ情報の設定

[入力形式]

lan [<number>] vlan tag pri <priority>

[パラメタ]

<number>

- lan 定義番号

  lan 定義の通し番号を、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。

<priority>

プライオリティを、0〜7 の 10 進数値で設定します。

[説明]

VLAN インタフェースのフレーム送出時に、VLAN タグのプライオリティフィールドに格納される値を設定します。

[未設定時]

<priority>に 0 が設定されたものとみなされます。

```
lan <number> vlan tag pri 0
```

3.9.4　lan vlan tag primap

[機能]

VLAN プライオリティマッピングの設定

[入力形式]

lan [<number>] vlan tag primap <count> <proto> <tos> <priority>

[パラメタ]

<number>

- lan 定義番号
  lan 定義の通し番号を、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>

- プライオリティマッピング定義番号
  プライオリティマッピング定義の通し番号を、10 進数値で指定します。

範囲	機種
0〜199	MR1000

<proto>

- ip
  IP パケットのプライオリティマッピングを定義します。
- ip6
  IPv6 パケットのプライオリティマッピングを定義します。

<tos>

マッピング対象とする ToS 値 (IP) または Traffic Class 値 (IPv6) を、0〜ff の 16 進数値、または"any"で指定します。複数の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 / Traffic Class 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。

- 0〜ff の 16 進数値 (例: ff = ff の TOS / Traffic Class 値)
- 16 進数値-16 進数値 (例: 32-64 = 32 から 64 までの TOS / Traffic Class 値)
- 16 進数値- (例: 80- = 80 から ff までの TOS / Traffic Class 値)
- -16 進数値 (例: -7f = 0 から 7f までの TOS / Traffic Class 値)
- 16 進数値,16 進数値,… (例: 10,20,30- = 10 と 20 と 30 以降の TOS / Traffic Class 値)

<priority>

プライオリティを、0〜7 の 10 進数値で設定します。

[説明]

IP の ToS 値、および IPv6 の Traffic Class 値から VLAN のプライオリティ値へのマッピングの設定をします。

VLAN プライオリティマッピング定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
200	MR1000

[未設定時]

VLAN プライオリティマッピング機能を使用しません。

第 4 章　相手情報の設定

- 相手定義番号の指定範囲

  本章のコマンド の [パラメタ] に記載されている<number>(相手定義番号) に指定する相手ネットワークの通し番号 (10 進数値) は、機種ごとに以下に示す範囲で指定してください。

範囲	機種
0〜99	MR1000

- 接続先定義番号の指定範囲

  “4.2 接続先情報” の [パラメタ] に記載されている<ap_number<(接続先定義番号) に指定する接続先の通し番号 (10 進数値) は、機種ごとに以下に示す範囲で指定してください。

範囲	機種
0〜99	MR1000

4.1 相手共通情報

4.1.1 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、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]

すで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。

4.1.2　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、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]

MR1000 の場合には以下に注意してください。
“1.2.7 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
```

4.1.3 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、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
```

4.1.4　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、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～100000k、または 1m～100m 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 または m 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。
  単位文字 m を付与した場合、単位は Mbps となります。
  1Kbps は 1000bps、1Mbps は 1000Kbps 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。

[注意]

使用する回線が LAN の場合、シェーピングを使用しないと帯域制御機能は有効に動作しません。

[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
```

4.2　接続先情報

4.2.1　remote ap name

[機能]

接続先の名称の設定

[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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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>

- 接続先名
  接続先名を、0x21,0x23～0x7e の 8 文字以内の ASCII 文字列で指定します。
  ただし、all は接続／切断コマンドで使う予約語であるため、使用しないでください。
  接続先名に all を指定した接続先のみを接続／切断することができなくなります。

[説明]

接続先名を設定します。

[注意]

接続先の情報をすべて未設定時の値で使用する場合には必ず接続先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接続先の情報は削除されます。

[未設定時]

接続先名を設定しないものとみなされます。

4.2.2　remote ap move

[機能]

接続先の優先順序の変更

[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、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>

- 対象接続先定義番号
  優先順序を変更する接続先定義番号を指定します。

<new_ap_number>

- 移動先接続先定義番号
  対象接続先を移動させる先の接続先定義番号を指定します。
  対象接続先は、ここで指定した接続先の前に移動されます。

[説明]

接続先の順序を変更します。

4.2.3 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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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 (“4.2.4 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。

回線種別	転送方式	MR1000
ISDN	PPP	○
HSD	PPP	○
FR	RFC2427方式	○
ATM	AAL5(RFC1483)	—
Ethernet	PPPoE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。
- overlap
  overlap ap として、別 IF からの出力とする場合に指定します。
- mpls
  MPLS LSP を使用する場合に指定します。
- discard
  この接続先利用時にはすべてのパケットが破棄されます。

[説明]

指定した接続先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
```

4.2.4 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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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。
- serial
  serial 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。できません)
- any
  ISDN を使用するように設定した、すべての wan 定義を指定したものとみなされます。

<conf_number>

wan 定義または lan 定義または serial 定義の定義番号を指定します。

- wan 定義の定義番号
  利用する wan 定義の定義番号を、10 進数値で指定します。

範囲	機種
0	MR1000

- lan 定義の定義番号
  利用する lan の定義番号を、10 進数値で指定します。

範囲	機種
0〜19	MR1000

- serial 定義の定義番号
  serial 定義の定義番号を、10 進数値で指定します。

範囲	機種
0	MR1000

[説明]

指定した接続先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、“4.2.3 remote ap datalink type” の<type>で physical を指定した場合にだけ有効です。

[未設定時]

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

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

4.2.5 remote ap recovery

[機能]

接続自動復旧モード の設定

[入力形式]

remote [<number>] ap [<ap_number>] recovery <mode> <startup>

[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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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>

- auto
  回線障害復旧時に接続を自動復旧します。
- manual
  回線障害発生時に自動的に接続先閉塞状態となり、回線障害が復旧した場合においてもオペレータ指示があるまで接続を復旧させません。

<startup>

- up
  装置起動時、および動的定義反映時は接続先閉塞していない状態で動作を開始します。
- down
  装置起動時、および動的定義反映時は接続先閉塞状態で動作を開始し、オペレータからの閉塞状態解除指示を待ちます。

[説明]

回線障害の復旧時に、接続回復の動作モード を設定します。

[未設定時]

装置起動時、および動的定義反映時に接続先閉塞していない状態で動作を開始し、回線障害発生時においても障害復旧後に接続を自動復旧します。

```
remote <number> ap <ap_number> recovery auto up
```

4.2.6　remote ap ip dns

[機能]

DNS サーバアドレスの設定

[入力形式]

remote [<number>] ap [<ap_number>] ip dns <dns>

[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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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。

<dns>

- DNS サーバアドレス
  接続先と接続するときに利用する DNS サーバのアドレスを指定します。
  ここでの指定によって、以下のように動作します。

  0.0.0.0　アドレスを自動取得するものとみなされます。

  255.255.255.255
  DNS サーバを使用しないものとみなされます。

  上記以外　設定したアドレスを、相手装置に通知します。
  この場合の設定可能な範囲は以下のとおりです。
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

[説明]

指定した接続先と接続するときに利用する DNS サーバアドレスを設定します。
本コマンドによる設定情報は、以下の 2 つの場合に利用されます。

- ProxyDNS からの利用
  ProxyDNS 機能と併用する場合、接続先と接続中のときは、<dns>で設定したアドレスに対して ProxyDNS から DNS 問い合わせを行います。本コマンドによる設定情報がない場合は、IPCP 機能によって相手ルータから DNS サーバアドレスを取得します。
- 通信相手への DNS サーバアドレス通知
  接続先から IPCP 機能を用いて DNS サーバアドレス通知要求を受けた場合に、<dns>で設定した IP アドレスを通知します。本コマンドによる設定がない場合は通知しません。

[未設定時]

アドレスを自動取得するものとみなされます。

```
remote <number> ap 0 ip dns 0.0.0.0
```

4.2.7　remote ap multiroute pattern

[機能]

マルチルーティングのパケット振り分けパターンの設定

[入力形式]

remote [<number>] ap [<ap_number>] multiroute pattern <count> <action> <src_addr>/<mask> <src_port> <dst_addr>/<mask> <dst_port> <protocol> [<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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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>

- パケット振り分けパターン定義番号
  パケット振り分けパターンの優先度を表す番号を、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、同じ値を持つ定義がすでに存在する場合は、既存の定義を変更します。

範囲	機種
0〜99	MR1000

<action>

該当するパケットの動作を設定します。

- use
  該当するパケットは、この ap 定義を利用して送信されます。
- unuse
  該当するパケットは、この ap 定義を利用して送信されません。
- backup
  以降の ap 定義で出力することができない場合に、この ap 定義を利用して送信されます。

<src_addr>/<mask>

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)
  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>

対象とする送信元ポート番号を指定します。

- ポート番号

  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対象とする場合に指定します。

<dst_addr>/<mask>

対象とするあて先 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)

  対象とするあて先 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

  すべてのあて先 IP アドレスを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>

対象とするあて先ポート番号を指定します。

- ポート番号

  対象とするあて先ポート番号を、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

  すべてのあて先ポート番号を対象とする場合に指定します。

<protocol>

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

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

- 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。

<tos>

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
  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]

マルチルーティング機能の接続先選択に対するパケットパターンを設定します。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
透過または遮断します。設定した優先度順に一致するか調べ、一致した時点で処理が判断され、それ以降の設定は参照されません。
本装置全体で以下の数まで定義できます。

最大定義数	機種
100	MR1000

[未設定時]

すべてのパケットがこの ap 定義を利用して送信可能とみなします。

4.2.8 remote ap multiroute pattern move

[機能]

マルチルーティングのパケット振り分けパターンの優先順序の変更

[入力形式]

remote [<number>] ap [<ap_number>] multiroute pattern 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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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>

- 対象ルール定義番号
  優先順序を変更するルール定義の番号を指定します。

<new_count>

- 移動先ルール定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すで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。

範囲	機種
0～99	MR1000

[説明]

マルチルーティングのパケット振り分けパターンの優先順序を変更します。

4.2.9　remote ap multiroute port add

[機能]

ポートルーティング情報の設定

[入力形式]

remote [<number>] ap [<ap_number>] multiroute port add <port> <server_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、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>

- 接続先定義番号

  相手ネットワーク内の接続先の通し番号を、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>

- サービスポート番号

  ポートルーティングの対象となるサービスポート番号を、1～65535 の 10 進数値で指定します。複数指定することはできません。

<server_name>

- サーバホスト名

  ポートルーティングサービスを提供するサーバホスト名を、0x21,0x23～0x7e のコードで構成される 80 文字以内の ASCII 文字列で指定します。

[説明]

ポートルーティングの対象とするポート番号を設定します。
本コマンドを実行した場合、条件に合致するパケットが指定した接続先に送信されます。
ポートルーティング情報は、本装置全体で 32 個まで定義できます。

[注意]

このコマンドは、V10 以前のソフトウェアの場合に使用します。
V11 以降は、remote ap multiroute pattern コマンドを利用して設定してください。また、remote ap multiroute port コマンドと remote ap multiroute pattern コマンドを混在して設定しないでください。

[未設定時]

ポートルーティング情報を定義しないものとみなされます。

4.2.10 remote ap limit charge

[機能]

課金累計制限の設定

[入力形式]

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

[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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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。

<charge>

- 課金累計上限
  課金累計の上限金額を、0～999999 の 10 進数値で指定します。
  0 を指定した場合は、上限を設定しません。

[説明]

指定した接続先に対する課金累計の上限値を設定します。
発信時に、接続先に対する課金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。次の優先度の接続先に対して処理を移します。

[未設定時]

課金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 charge 0
```

4.2.11　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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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)のどれかを指定します。0 秒を指定した場合は、上限を設定しません。

[説明]

指定した接続先に対する接続時間累計の上限値を設定します。
発信時に、この接続先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、この接続先に対する自動発信を行いません。次の優先度の接続先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
```

4.2.12 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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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 ppp auth type any
```

4.2.13　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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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。

<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]

指定した接続先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。

4.2.14 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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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。

<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。

4.2.15　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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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接続先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
```

4.2.16 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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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接続先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
```

4.2.17　remote ap pppoe acname

[機能]

アクセスコンセントレータ名 (AC-Name) の設定

[入力形式]

remote [<number>] ap [<ap_number>] pppoe acname <ac_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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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。

<ac_name>

- アクセスコンセントレータ名
  アクセスコンセントレータ名 (AC-Name) を、0x21,0x23～0x7e のコードで構成される 64 文字以内の ASCII 文字列で指定します。

[説明]

アクセスコンセントレータ名 (AC-Name) を設定します。

[未設定時]

アクセスコンセントレータ名 (AC-Name) を指定しないものとみなされます。

4.2.18 remote ap pppoe svname

[機能]

サービスネーム (Service-Name) の設定

[入力形式]

remote [<number>] ap [<ap_number>] pppoe svname <sv_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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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。

<sv_name>

- サービスネーム
  サービスネーム (Service-Name) を、0x21,0x23～0x7e のコードで構成される 64 文字以内の ASCII 文字列で指定します。

[説明]

サービスネーム (Service-Name) を設定します。

[未設定時]

サービスネーム (Service-Name) を指定しないものとみなされます。

4.2.19　remote ap dial number

[機能]

接続先の電話番号の設定

[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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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、以下のどれかを指定します。

- 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]

接続先の電話番号を設定します。

[注意]

MR1000 は PIAFS 接続に対応しています。PIAFS(64Kbps) 着信時は、<subaddress> で設定した相手サブアドレスは無視されます。

[未設定時]

接続先の電話番号を設定しないものとみなされます。

4.2.20 remote ap dial speed

[機能]

接続先の通信速度の設定

[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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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、以下のどれかを指定します。

- 0
- 1
- 2

<speed>

通信速度、通信手順を指定します。"PIAFS" および "PIAFS64K" は PIAFS 対応の MR1000 でだけ指定できます。

- 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]

接続先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
```

4.2.21 remote ap called accept

[機能]

接続先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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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]

指定した接続先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
```

4.2.22　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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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) “4.2.23 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、“4.2.19 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、指定した接続先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
```

4.2.23 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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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、"“4.2.19 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。

[注意]

MR1000 は PIAFS 接続に対応しています。PIAFS(64Kbps) 着信時には、<subaddress> で設定した相手サブアドレスは無視されます。

[未設定時]

着信時の CLID 相手判定に、"“4.2.19 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
```

4.2.24　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> [<direction>]

[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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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) のどれかを指定します。0 秒を指定した場合は、監視を行いません。

<direction>

- 省略
  送信パケット、および受信パケットを通信監視の対象とします。
- send
  送信パケットだけを通信監視の対象とします。受信パケットは監視対象とはなりません。
- receive
  受信パケットだけを通信監視の対象とします。送信パケットは監視対象とはなりません。

[説明]

指定した接続先と接続したときの無通信監視時間を設定します。
<time>で設定された間、監視対象となるパケットがない場合に、無通信として回線を切断します。

[未設定時]

無通信監視を行わないものとみなされます。

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

4.2.25 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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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。

4.2.26　remote ap step2

[機能]

夜間・休日時間帯の課金単位時間の設定

[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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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]

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。
この設定は、"“4.2.25 remote ap step”"を設定した場合にだけ有効です。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。

4.2.27 remote ap step3

[機能]

深夜時間帯の課金単位時間の設定

[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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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]

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。
この設定は、""4.2.25 remote ap step""を設定した場合にだけ有効です。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、""4.2.26 remote ap step2""で設定した値が使用されます。この設定もない場合には、""4.2.25 remote ap step""で設定した値が使用されます。

4.2.28　remote ap keep

[機能]

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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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。

- off
  回線接続を保持しません。
- on
  回線接続を保持します。
- 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
```

4.2.29 remote ap 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>] ap <ap_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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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。

4.2.30　remote ap 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>] ap <ap_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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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> ap <ap_number> fr cir 0
```

4.2.31 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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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。
- manual
  IPsec を手動鍵設定で使用します。
- ike
  IPsec 自動鍵交換を使用します。

[説明]

IPsec を使用するかどうかを設定します。
IPsec の自動鍵交換を使用する場合は、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 name remote
- remote ap ike release
- remote ap ike initial
- remote ap ike sessionwatch
- remote ap ike mode
- remote ap ike bind

手動鍵設定と自動鍵設定 (交換) の識別方法

<type>に、文字列"ike"を指定した場合、その定義を自動鍵設定 (交換) と判断します。
手動鍵設定を行う場合に、自動鍵設定 (交換) で使用する定義を行っても使用されません。
また、自動鍵設定 (交換) を行う場合に、手動鍵設定で使用する定義を行っても使用されません。

手動鍵設定の定義について

以下のコマンドは、手動鍵設定で使用される定義です。
remote <number> ap <ap_number> ipsec type manual と定義した場合に使用されます。

- remote ap ipsec send spi
- remote ap ipsec send protocol
- remote ap ipsec send range
- remote ap ipsec send encrypt
- remote ap ipsec send auth
- remote ap ipsec receive spi
- remote ap ipsec receive protocol
- remote ap ipsec receive range
- remote ap ipsec receive encrypt
- remote ap ipsec receive auth

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。

手動鍵設定の場合、自側の tunnel endpoint アドレスと相手側の tunnel endpoint アドレスの双方を指定してください。

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

相手側の tunnel endpoint アドレスが不定である場合:

- remote 0 ap 0 tunnel local 192.168.1.1

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

<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。

[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
```

4.2.32　remote ap ipsec send spi

[機能]

手動鍵送信用 IPsec 情報のセキュリティパラメタインデックスの設定

[入力形式]

remote [<number>] ap [<ap_number>] ipsec send spi <spi>

[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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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。

<spi>

- セキュリティパラメタインデックス
  手動鍵送信用 IPsec SA のセキュリティパラメタインデックスを、100～ffffffff の範囲の 16 進数値で指定します。

[説明]

手動鍵送信用 IPsec SA を認識する、セキュリティパラメタインデックスの設定を行います。

[注意]

手動鍵送信用 IPsec 情報の SPI 値は同一相手側 tunnel endpoint アドレスで同一の値を指定しないでください。
同一の SPI 値を指定した場合、通信できなくなることがあります。

[未設定時]

手動鍵送信用 IPsec 情報の SPI 設定は設定されません。

4.2.33 remote ap ipsec send protocol

[機能]

手動鍵送信用 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 send 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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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>

手動鍵送信用 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]

手動鍵送信用 IPsec SA の、セキュリティプロトコルの設定を行います。
認証/暗号アルゴリズム定義、セキュリティプロトコル定義と IPsec SA の関係

auth(認証)	encrypt(暗号)	セキュリティプロトコル	IPsec SA
―	―	esp(暗号)	×
―	―	ah(認証)	×
―	―	―	×
○	―	esp(暗号)	×
○	―	ah(認証)	◎
○	―	―	×
―	○	esp(暗号)	◎
―	○	ah(認証)	×
―	○	―	×
○	○	esp(暗号)	◎ESPinAuth(認証付暗号)
○	○	ah(認証)	◎
○	○	―	×

○:定義あり ―:定義なし ◎:SA作成可 ×:SA作成不可

[未設定時]

手動鍵送信用 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 send protocol none
```

4.2.34 remote ap ipsec send range

[機能]

手動鍵送信用 IPsec 情報の対象範囲の設定

[入力形式]

remote [<number>] ap [<ap_number>] ipsec send 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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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 対象となるあて先 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 対象となるあて先 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]

パケット送信時に 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 send range any4 any4
```

4.2.35　remote ap ipsec send encrypt

[機能]

手動鍵送信用 IPsec 情報の暗号情報の設定

[入力形式]

remote [<number>] ap [<ap_number>] ipsec send encrypt <enc_algo> [<kind> <enc_key> [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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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。

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

<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。

<enc_key>

暗号鍵を指定します。

- 暗号化されていない暗号鍵
  <enc_algo>で指定した暗号アルゴリズムが使用する鍵長未満の鍵を指定した場合は、16 進数鍵では鍵長になるまで 0x0 でパディングされます。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""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 暗号アルゴリズム	hex 16進数鍵	text 文字列鍵
des-cbc	1～16桁	8文字
3des-cbc	1～48桁	24文字
aes-cbc	1～32桁	16文字

- 暗号化された暗号鍵

  暗号化された暗号鍵を指定します。show コマンドで表示される暗号化された暗号鍵を 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>

- 暗号化暗号鍵指定

  <enc_key>に暗号化された暗号鍵を指定する場合に指定します。

[説明]

送信パケットを暗号化するための、暗号アルゴリズムと鍵の設定を行います。
show コマンドでは、暗号化された暗号鍵が encrypted と共に表示されます。
show remote [<number>] ap [<ap_number>] ipsec send encrypt を実行すると、暗号化されていない認証鍵が表示されます。

- 手動鍵設定としての暗号アルゴリズム

  暗号アルゴリズムが"null"および"none"の場合、暗号鍵は入力できません。

[注意]

- weak key

  手動鍵設定で指定する暗号鍵に、RFC2409 の Appendix A に記載されている weak key を設定した場合、コマンドエラーとなります。

  RFC2409 の Appendix A に記載されている weak key(DES, 3DES だけ)

```
0101010101010101, FEFEFEFEFEFEFEFE, 1F1F1F1FE0E0E0E0, E0E0E0E01F1F1F1F,
01FE01FE01FE01FE, FE01FE01FE01FE01, 1FE01FE00EF10EF1, E01FE01FF10EF10E,
01E001E001F101F1, E001E001F101F101, 1FFE1FFE0EFE0EFE, FE1FFE1FFE0EFE0E,
011F011F010E010E, 1F011F010E010E01, E0FEE0FEF1FEF1FE, FEE0FEE0FEF1FEF1
```

  3des-cbc の場合は、暗号鍵を 16 桁毎に 3 つの鍵に分割し、どれかの鍵が weak key となるような指定はできません。

[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 send encrypt none
```

4.2.36　remote ap ipsec send auth

[機能]

手動鍵送信用 IPsec 情報の認証情報の設定

[入力形式]

remote [<number>] ap [<ap_number>] ipsec send auth <auth_algo> [<kind> <auth_key> [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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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。

- hmac-md5
- hmac-sha1
- none

<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。

<auth_key>

認証鍵を指定します。

- 暗号化されていない認証鍵
  <auth_algo>で指定した認証アルゴリズムが使用する鍵長未満の鍵を指定した場合は、16 進数鍵では鍵長になるまで 0x0 でパディングされます。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""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 認証アルゴリズム	hex 16進数鍵	text 文字列鍵
hmac-md5 hmac-sha1	1～32桁 1～40桁	16文字 20文字

- 暗号化された認証鍵を指定します。
  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>

- 暗号化認証鍵指定
  <auth_key>に暗号化された認証鍵を指定する場合に指定します。

[説明]

送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。
show コマンドでは、暗号化された認証鍵が encrypted と共に表示されます。
show remote [<number>] ap [<ap_number>] ipsec send auth を実行すると、暗号化されていない認証鍵が表示されます。

- 手動鍵設定としての認証アルゴリズム
  認証アルゴリズムが"none"の場合、認証鍵は入力できません。

[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 send auth none
```

4.2.37　remote ap ipsec receive spi

[機能]

手動鍵受信用 IPsec 情報のセキュリティパラメタインデックスの設定

[入力形式]

remote [<number>] ap [<ap_number>] ipsec receive spi <spi>

[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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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。

<spi>

- セキュリティパラメタインデックス
  受信用 IPsec SA のセキュリティパラメタインデックスを、100～ffffffff の範囲の 16 進数値で指定します。

[説明]

手動鍵受信用 IPsec SA を認識する、セキュリティパラメタインデックスの設定を行います。

[注意]

手動鍵受信用 IPsec 情報の SPI 値は装置内で同一の値を指定しないでください。
同一の SPI 値を指定した場合、通信できなくなることがあります。

[未設定時]

手動鍵受信用 IPsec 情報の SPI 設定は設定されません。

4.2.38 remote ap ipsec receive protocol

[機能]

手動鍵受信用 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 receive 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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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>

手動鍵受信用 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]

手動鍵受信用 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]

手動鍵受信用 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 send protocol none
```

4.2.39　remote ap ipsec receive range

[機能]

手動鍵受信用 IPsec 情報の対象範囲の設定

[入力形式]

remote [<number>] ap [<ap_number>] ipsec receive range <dst_addr>/<mask> <src_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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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>/<mask>

IPsec 対象となる相手側 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 対象となる相手側 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。

<src_addr>/<mask>

IPsec 対象となる自側 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 対象となる自側 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]

パケット受信時に 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]

<dst_addr>,<src_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 receive range any4 any4
```

4.2.40 remote ap ipsec receive encrypt

[機能]

手動鍵受信用 IPsec 情報の暗号情報の設定

[入力形式]

remote [<number>] ap [<ap_number>] ipsec receive encrypt <enc_algo> [<kind> <enc_key> [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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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。

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

<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。

<enc_key>

暗号鍵を指定します。

- 暗号化されていない暗号鍵
  <enc_algo>で指定した暗号アルゴリズムが使用する鍵長未満の鍵を指定した場合は、16 進数鍵では鍵長になるまで 0x0 でパディングされます。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""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 暗号アルゴリズム	hex 16進数鍵	text 文字列鍵
des-cbc	1～16桁	8文字
3des-cbc	1～48桁	24文字
aes-cbc	1～32桁	16文字

- 暗号化された暗号鍵

  暗号化された暗号鍵を指定します。show コマンドで表示される暗号化された暗号鍵を 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>

- 暗号化暗号鍵指定

  <enc_key>に暗号化された暗号鍵を指定する場合に指定します。

[説明]

受信パケットを暗号化するための、暗号アルゴリズムと鍵の設定を行います。
show コマンドでは、暗号化された暗号鍵が encrypted と共に表示されます。
show remote [<number>] ap [<ap_number>] ipsec receive encrypt を実行すると、暗号化されていない認証鍵が表示されます。

- 手動鍵設定としての暗号アルゴリズム

  暗号アルゴリズムが"null"および"none"の場合、暗号鍵は入力できません。

[注意]

- weak key

  手動鍵設定で指定する暗号鍵に、RFC2409 の Appendix A に記載されている weak key を設定した場合、コマンドエラーとなります。

  RFC2409 の Appendix A に記載されている weak key(DES, 3DES だけ)

```
0101010101010101, FEFEFEFEFEFEFEFE, 1F1F1F1FE0E0E0E0, E0E0E0E01F1F1F1F,
01FE01FE01FE01FE, FE01FE01FE01FE01, 1FE01FE00EF10EF1, E01FE01FF10EF10E,
01E001E001F101F1, E001E001F101F101, 1FFE1FFE0EFE0EFE, FE1FFE1FFE0EFE0E,
011F011F010E010E, 1F011F010E010E01, E0FEE0FEF1FEF1FE, FEE0FEE0FEF1FEF1
```

  3des-cbc の場合は、暗号鍵を 16 桁毎に 3 つの鍵に分割し、どれかの鍵が weak key となるような指定はできません。

[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 receive encrypt none
```

4.2.41 remote ap ipsec receive auth

[機能]

手動鍵受信用 IPsec 情報の認証情報の設定

[入力形式]

remote [<number>] ap [<ap_number>] ipsec receive auth <auth_algo> [<kind> <auth_key> [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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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。

- hmac-md5
- hmac-sha1
- none

<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。

<auth_key>

認証鍵を指定します。

- 暗号化されていない認証鍵
  <auth_algo>で指定した認証アルゴリズムが使用する鍵長未満の鍵を指定した場合は、16 進数鍵では鍵長になるまで 0x0 でパディングされます。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""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 認証アルゴリズム	hex 16進数鍵	text 文字列鍵
hmac-md5 hmac-sha1	1～32桁 1～40桁	16文字 20文字

- 暗号化された認証鍵を指定します。
  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>

- 暗号化認証鍵指定

  <auth_key>に暗号化された認証鍵を指定する場合に指定します。

[説明]

送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。
show コマンドでは、暗号化された認証鍵が encrypted と共に表示されます。
show remote [<number>] ap [<ap_number>] ipsec send auth を実行すると、暗号化されていない認証鍵が表示されます。

- 手動鍵設定としての認証アルゴリズム

認証アルゴリズムが"none"の場合、認証鍵は入力できません。

[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 receive auth none
```

4.2.42 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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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
```

4.2.43　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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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
- aes-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) aes-cbc
2) 3des-cbc
3) des-cbc
4) 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
```

4.2.44 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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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、認証アルゴリズムの設定を行います。
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
```

4.2.45　remote ap ipsec ike pfs

[機能]

自動鍵交換用 IPsec 情報の PFS 使用時の DH(Diffie-Hellman) 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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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(グループ 1)
- modp1024
  Diffie-Hellman グループの MODP1024(グループ 2)
- modp1536
  Diffie-Hellman グループの MODP1536(グループ 5)
- 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 使用時の DH(Diffie-Hellman) 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
使用時の DH グループを設定してください。

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

4.2.46 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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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) のどれかを指定します。

[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
```

4.2.47　remote ap ipsec ike lifebyte

[機能]

自動鍵交換用 IPsec 情報の SA 有効パケット量の設定

[入力形式]

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

[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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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。

<lifebyte>

- SA 有効パケット量
  IPsec 用 Security Association(SA) 有効パケット量のバイト数を、0 または 2400k～108000m の範囲で指定します。
  単位は以下の 3 種類です。1k は 1024 バイトで計算されます。
  k: キロバイト (例: 2400k → 2400k)
  m: メガバイト (例: 4m → 4096k)
  g: ギガバイト (例: 1g → 1048576k)
  0 を指定した場合は、lifebyte による IPsec SA の更新を行いません。

[説明]

IPsec セッションの通信データを保護する、IPsec SA の SA 有効パケット量 (キロバイト) の設定を行います。

[未設定時]

SA 有効パケット量に 0 バイトを指定したものとみなされます。

```
remote <number> ap <ap_number> ipsec ike lifebyte 0
```

4.2.48 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 / 更新データ量) の設定

[入力形式]

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

[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、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>

- 接続先定義番号

  相手ネットワーク内の接続先の通し番号を、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) のどれかを指定します。

<byte>

- Initiator SA 更新データ量

  Initiator SA 更新データ量を、0 または 120kbyte～230400kbyte の範囲で指定します。

  単位は、k(キロバイト)、m(メガバイト) のどれかを指定します。

[説明]

自側が Initiator の場合に、IPsec SA の有効時間または SA 有効データ量が満了になる前に、IPsec SA の更新を行うための時間／データ量の設定を行います。

相手側の New SA Responder と同じ時間／データ量にならないように設定して下さい。

また、SA 有効データ量の設定を行い、更新データ量設定が 0 指定時には有効データ量満了した時点で SA 更新が行われます。

[未設定時]

Initiator SA 更新時間として 90s(90 秒)、データ量として 0k(0kbyte) 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 0
```

4.2.49　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 / 更新データ量) の設定

[入力形式]

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

[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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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) のどれかを指定します。
- off
  Responder 側からの SA 更新は行いません。

<byte>

- Responder SA 更新データ量
  Responder SA 更新データ量を、0 または 120kbyte～230400kbyte の範囲で指定します。
  単位は、k(キロバイト)、m(メガバイト) のどれかを指定します。

[説明]

自側が Responder の場合に、IPsec SA の有効時間または SA 有効データ量が満了になる前に、IPsec SA の更新を行うための時間／データ量の設定を行います。
相手側の New SA Initiator と同じ時間／データ量にならないように設定して下さい。
また、SA 有効データ量の設定を行い、更新データ量設定が 0 指定時には有効データ量満了した時点で SA 更新が行われます。更新時間設定が 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)、データ量として 0k(0kbyte) 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 0
```

4.2.50 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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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。
- any6
  すべての IPv6 アドレスを IPsec 対象に含めます。
  ::/0 と同意。

<dst_addr>/<mask>

IPsec 対象となるあて先 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 対象となるあて先 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。
- any6
  すべての IPv6 アドレスを IPsec 対象に含めます。
  ::/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
```

4.2.51 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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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
```

4.2.52　remote ap ike shared key

[機能]

IKE セッション確立時の共有鍵 (Pre-shared key) の設定

[入力形式]

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

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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>

共有鍵 (事前共有秘密鍵方式) を指定します。

- 暗号化されていない共有鍵を指定します。
  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
共有鍵	1～256桁	1～128文字

- 暗号化された共有鍵を指定します。
  show コマンドで表示される暗号化された共有鍵を 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

- 暗号化共有鍵指定
  <shared_key>に暗号化された共有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、共有鍵の設定を行います。

[未設定時]

共有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。

4.2.53 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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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>で指定した接続先情報の 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	認証(ハッシュ)情報	hmac-md5	0	...
c	DH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、DH グループ設定はすべて同じ値を設定してください。

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 情報の自装置識別情報を設定します。

4.2.54　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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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
- aes-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、必ず設定してください。
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。

4.2.55 remote ap ike proposal hash

[機能]

IKE セッション用認証 (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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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>

認証 (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]

認証のための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
```

4.2.56　remote ap ike proposal pfs

[機能]

IKE セッション用 DH(Diffie-Hellman) 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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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(グループ 1) の Diffie-Hellman グループ
- modp1024
  MODP1024(グループ 2) の Diffie-Hellman グループ
- modp1536
  MODP1536(グループ 5) 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、DH(Diffie-Hellman) グループの設定を行います。

[未設定時]

DH 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
```

4.2.57 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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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) のどれかを指定します。

[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
```

4.2.58　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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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) のどちらかを指定します。

<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
```

4.2.59 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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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送信 ID 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
```

4.2.60　remote ap ike name local

[機能]

IKE 情報の自装置識別情報の設定

[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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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>

- 自装置識別情報
  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。
  識別情報は、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。

[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識別情報の設定を行います。
ISAKMP SA のネゴシエーション交換モードについては、remote ap ike mode を参照して下さい。

[未設定時]

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

4.2.61 remote ap ike name remote

[機能]

IKE 情報の相手装置識別情報の設定

[入力形式]

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

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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>

- 相手装置識別情報
  相手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。

[説明]

IKE セッションを確立する、相手装置の IP アドレスが不定の場合に識別情報の設定を行います。
ISAKMP SA のネゴシエーション交換モードについては、remote ap ike mode を参照してください。

[未設定時]

IKE セッション用相手装置識別情報が設定されません。
装置識別情報により共有鍵認証を行う場合は、必ず設定してください。

4.2.62　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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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
- PPPoE を使用した時の切断時

[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
```

4.2.63 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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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
- PPPoE 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 の確立を行うものとみなされます。

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

4.2.64　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> [<timeout>]]]

[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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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 パケットのあて先 IP アドレス
  ICMP ECHO パケットのあて先 IP アドレスを指定します。
  IPsec 対象範囲に含まれる IP アドレスを以下の範囲で指定してください。
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254
  また、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) のどちらかを指定します。
  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) のどちらかを指定します。
  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。

<timeout>

- ICMP ECHO パケットのタイムアウト時間
  ICMP ECHO パケットのタイムアウト時間を、5 秒～180 秒 (3 分) の範囲で指定します。
  単位は、m(分)、s(秒) のどちらかを指定します。
  省略した場合は、5 秒を指定したものとみなされます。

[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。

指定したあて先 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。

あて先 IP アドレスは、IPv4 アドレスのみ指定可能です。

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。

ICMP ECHO パケットのタイムアウト時間は、回線品質が悪い時や高負荷状態により ICMP ECHO パケットの応答が遅延するような状況の時に有効です。

[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 5s
```

4.2.65　remote ap ike mode

[機能]

IKE 情報の交換モード の設定

[入力形式]

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

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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 ネゴシエーションの交換モード
  IKE ネゴシエーションの交換モードを指定します。

  auto ： IKE 情報の交換モードを tunnel endpoint address および IKE 情報装置識別情報の設定によって自動判別します。

  aggressive ：
  IKE 情報の交換モードとして Aggressive Mode を使用します。

  main ： IKE 情報の交換モードとして Main Mode を使用します。

[説明]

IKE セッションを確立する、IKE ネゴシエーション交換モード の設定を行います。
交換モード、tunnel endpoint address、装置識別情報の設定により、以下の表のように動作します。

tunnel endpoint addressの設定	nameの設定	modeの設定		
		aggressive	main	auto
tunnel local ○ tunnel remote ○	name local ○ name remote ×	Aggressive (Initiator)	Main	Main
	name local × name remote ○	Aggressive (Responder)	Main	Main
	name local ○ name remote ○	Aggressive*1	Main	Main
	name local × name remote ×	動作しない	Main	Main
tunnel local × tunnel remote ○	name local ○ name remote ×	Aggressive (Initiator)	動作しない	Aggressive (Initiator)
	name local × name remote ○	動作しない	動作しない	動作しない
	name local ○ name remote ○	Aggressive (Initiator)	動作しない	Aggressive (Initiator)
	name local × name remote ×	動作しない	動作しない	動作しない
tunnel local ○ tunnel remote ×	name local ○ name remote ×	動作しない	動作しない	動作しない
	name local × name remote ○	Aggressive (Responder)	動作しない	Aggressive (Responder)
	name local ○ name remote ○	Aggressive (Responder)	動作しない	Aggressive (Responder)
	name local × name remote ×	動作しない	動作しない	動作しない

○：設定有り　×：設定無し
※tunnel local/remoteが設定無しの場合は、name, modeの設定に関係なくすべて動作しません。
*1 初期動作としてInitiator、Responder両方の動作が可能です。

[未設定時]

IKE 情報の交換モードとして自動判別を行うものとみなされます。

```
remote <number> ap <ap_number> ike mode auto
```

4.2.66　remote ap ike bind

[機能]

利用 IKE 情報の設定

[入力形式]

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

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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>

- 利用する接続先定義番号指定の有無
  利用する IKE 情報が設定されている接続先定義番号を指定するかを決定します。

  self ：　同一接続先情報の IKE 定義を利用します。

  ap ：　<conf_number>で指定された接続先情報の IKE 定義を利用します。

<conf_number>

- 接続先情報定義番号
  利用する IKE 定義がされている接続先情報定義番号として 0 以上の 10 進数値を指定します。利用できる接続先情報は同一の相手情報定義内の接続先情報である必要があります。<kind>が self の場合には設定できません。

[説明]

利用する IKE 定義の接続先情報を設定します。
利用する IKE 定義に指定する接続先情報番号には、有効な IKE 定義が存在する必要があります。
有効な IKE 定義が存在しない場合、<ap_number>の接続先情報は利用できません。
利用する接続先情報の IKE 定義が有効な場合、利用する接続先情報定義は以下のとおりです。

- 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 name remote

- remote ap ike release
- remote ap ike initial
- remote ap ike sessionwatch
- remote ap tunnel local
- remote ap tunnel remote

[注意]

<conf_number>は、設定している接続先情報定義番号と同一の接続先情報定義番号は設定できません。

[未設定時]

利用する IKE 定義として同一接続先情報の IKE 定義を使用するとみなされます。

```
remote <remote_number> ap <ap_number> ike bind self
```

4.2.67　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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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 アドレスまたは IPv6 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。
  指定可能な範囲は以下のとおりです。

  IPv4: 1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  IPv6: ::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

  IPv6 DHCP クライアントが取得したプレフィックスを使用する場合は上位を"dhcp@インタフェース名"の形式で指定し，下位 80bit 分を IPv6 アドレス形式で指定します。インタフェース名には、rmt インタフェースを以下の範囲で指定します。

範囲	機種
rmt0～rmt99	MR1000

  例)rmt0 で動作する IPv6 DHCP クライアントが取得した IPv6 プレフィックスを使用する場合の設定例

  dhcp@rmt0::
  dhcp@rmt0::1:2:3:4

[説明]

指定した接続先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。

4.2.68 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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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 アドレスまたは IPv6 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  IPv4: 1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  IPv6: ::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

[説明]

指定した接続先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。

4.2.69　remote ap overlap to

[機能]

overlap ap の実際の送出先の設定

[入力形式]

remote [<number>] ap [<ap_number>] overlap to <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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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>

- lan
  実際の送出先を lan 定義とする場合に指定します。
- remote
  実際の送出先を remote 定義とする場合に指定します。

<conf_number>

lan 定義、remote 定義の定義番号を指定します。

- lan 定義の定義番号
  利用する lan の定義番号を、10 進数値で指定します。

範囲	機種
0～19	MR1000

- remote 定義の定義番号
  利用する remote の定義番号を、10 進数値で指定します。
  ただし、<number>と同じ値は指定できません。

範囲	機種
0～99	MR1000

[説明]

指定した接続先定義を利用してパケットを転送する場合の定義を設定します。
本コマンドは、remote ap datalink type の<type>で overlap を指定した場合にだけ有効です。

[未設定時]

パケット転送先を設定しないものとみなされます。

4.2.70 remote ap overlap nexthop

[機能]

overlap ap における転送先 IPv4 ルータの設定

[入力形式]

remote [<number>] ap [<ap_number>] overlap nexthop <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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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>

- 転送先となる IPv4 ルータの IP アドレスを指定します。
  以下の範囲で指定してください。

  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

[説明]

overlap ap 機能を利用して lan にパケットを転送する場合の、転送先 IPv4 ルータの IP アドレスを指定します。

本コマンドは、remote ap datalink type の<type>で overlap を指定し、remote ap overlap to の<kind>で lan を指定した場合にだけ有効です。

[未設定時]

IPv4 転送を行わないものとみなされます。

4.2.71　remote ap overlap nexthop6

[機能]

overlap ap における転送先 IPv6 ルータの設定

[入力形式]

remote [<number>] ap [<ap_number>] overlap nexthop6 <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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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>

- 転送先となる IPv6 ルータの IP アドレスを指定します。
  以下の範囲で指定してください。
  ::2 〜 feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

[説明]

overlap ap 機能を利用して lan にパケットを転送する場合の、転送先 IPv6 ルータの IP アドレスを指定します。

本コマンドは、remote ap datalink type の<type>で overlap を指定し、remote ap overlap to の<kind>で lan を指定した場合にだけ有効です。

[未設定時]

IPv6 転送を行わないものとみなされます。

4.2.72 remote ap sessionwatch

[機能]

接続先監視の設定

[入力形式]

remote [<number>] ap [<ap_number>] sessionwatch <source> <destination> <normal_interval> <abnormal_interval> <timeout> [<retry> [<send_ttl> [<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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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。

<source>

- ICMP ECHO パケットの送信元 IP アドレス
  ICMP ECHO パケットの送信元 IP アドレスを指定します。装置に設定されている自側 IPv4/IPv6 アドレスのどれかを指定してください。
  指定可能な範囲は以下のとおりです。

  IPv4: 1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  IPv6: ::2 ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<destination>

- ICMP ECHO パケットのあて先 IP アドレス
  監視対象となる IPv4/IPv6 アドレスを指定します。
  <source>と同じプロトコルアドレスで指定してください。
  指定可能な範囲は以下のとおりです。

  IPv4: 1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  IPv6: ::2 ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<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) のどちらかを指定します。

<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) のどちらかを指定します。

<timeout>

- 監視タイムアウト
  監視失敗とみなすまでのタイムアウト時間を、5 秒～180 秒 (3 分) の範囲で指定します。
  単位は、m(分)、s(秒) のどちらかを指定します。

<retry>

- ICMP ECHO パケットの再送間隔
  ICMP ECHO パケットの正常時送信に対して応答がない時の ICMP ECHO パケットの再送間隔を、1 秒～<timeout>-1 秒の範囲で指定します。
  単位は、m(分)、s(秒) のどちらかを指定します。
  省略時は、1s が指定されたものとして動作します。

<send_ttl>

- 送信 TTL / HopLimit 値
  ICMP ECHO パケットを送信する時の IPv4 TTL / IPv6 HopLimit 値を、1～255 の範囲で指定します。
  省略時は、255 が指定されたものとして動作します。

<mode>

監視方式を指定します。

- always
  常時監視を行ないます。
- idleonly
  無通信状態に限り監視を行ないます。

省略時は always が指定されたものとして動作します。

[説明]

接続先の生存確認を行うための動作情報を設定します。
指定したあて先 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、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、正常送信間隔での監視に戻ります。

[注意]

以下の場合においては、監視を行いません。

- ISDN 回線を利用する接続先で、常時接続機能を利用していない場合。
- PPPoE 回線を利用する接続先で、常時接続機能を利用していない場合。

また、IPsec / IKE を利用する接続先で、IKE セッション監視の設定 (remote ap ike sessionwatch) が同時に設定されている場合には、IKE セッション監視は動作せず、接続先監視機能だけが動作します。

[未設定時]

接続先監視機能を利用しないものとみなされます。

4.2.73 remote ap mpls to

[機能]

MPLS LSP の送出先の設定

[入力形式]

remote [<number>] ap [<ap_number>] mpls to <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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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>

- lan
  MPLS LSP の送出先を lan 定義とする場合に指定します。
- remote
  MPLS LSP の送出先を remote 定義とする場合に指定します。

<conf_number>

lan 定義、remote 定義の定義番号を指定します。

- lan 定義の定義番号
  利用する lan の定義番号を、10 進数値で指定します。

範囲	機種
0～19	MR1000

- remote 定義の定義番号
  利用する remote の定義番号を、10 進数値で指定します。
  ただし、<number>と同じ値は指定できません。

範囲	機種
0～99	MR1000

[説明]

指定した接続先定義を利用してパケットを転送する場合の定義を設定します。
本コマンドは、remote ap datalink type の<type>で mpls を指定した場合にだけ有効です。

[未設定時]

MPLS LSP を設定しないものとみなされます。

4.2.74　remote ap mpls nexthop

[機能]

MPLS LSP における次ホップのラベルスイッチルータの設定

[入力形式]

remote [<number>] ap [<ap_number>] mpls nexthop <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、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>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、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>

- 次ホップのラベルスイッチルータの IP アドレスを指定します。
  以下の範囲で指定してください。
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

[説明]

MPLS LSP を利用して lan にパケットを転送する場合の、次ホップのラベルスイッチルータの IP アドレスを指定します。

本コマンドは、remote ap datalink type の<type>で mpls を指定し、remote ap mpls to の<kind>で lan を指定した場合にだけ有効です。

[未設定時]

lan で MPLS LSP を使用しないものとみなされます。

4.3 PPP 関連情報

4.3.1 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、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 (“4.3.6 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
```

4.3.2　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、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
```

4.3.3 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、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
```

4.3.4　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、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) のどれかを指定します。

[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。

4.3.5 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、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) のどれかを指定します。

[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。

4.3.6　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、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
```

4.3.7 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、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、“4.3.6 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
```

4.3.8　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、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、“4.3.6 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
```

4.3.9 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、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、“4.3.6 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
```

4.4　IP 関連情報

4.4.1　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、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。
  自側 IP アドレスの指定可能な範囲は以下のとおりです。

  0.0.0.0
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  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。

4.4.2 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、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。
  相手側 IP アドレスの指定可能な範囲は以下のとおりです。

  0.0.0.0
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

  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。

4.4.3　remote ip route

[機能]

IPv4 スタティック経路情報の設定

[入力形式]

remote [<number>] ip route <count> <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、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>

- スタティック経路情報定義番号
  スタティック経路情報の定義番号を、10 進数値で指定します。

範囲	機種
0～255	MR1000

<address>/<mask>

- IPv4 アドレス / マスクビット数 (またはマスク値)
  あて先ネットワークを 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
  あて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
  このスタティック経路情報を RIP に再配布するときのメトリック値を、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。

<distance>

- 優先度
  このスタティック経路情報の優先度を、0～254 の 10 進数値で指定します。優先度は数値の小さい方がより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]

IPv4 スタティック経路 (静的経路) 情報を設定します。

RIP メトリック値は、スタティック経路情報を RIP に再配布するときのメトリック値を設定します。RIP に再配布したときは、設定した RIP メトリック値+1 のメトリック値で RIP テーブルに登録されます。

優先度は、同じあて先への経路情報が複数ある場合、優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。各ダイナミックルーティングプロトコルの優先度については、routemanage ip distance コマンドを参照してください。

優先度に 0 が設定されているときは、routemanage interface floating コマンドでのフローティング設定に応じてフローティング動作が切り替わります。優先度に 1 以上が設定されているときは、常にフローティング動作します。

フローティング動作する場合、remote インタフェースが通信可能な状態（リンクアップなど）であれば、スタティック経路情報をルーティングテーブルに追加します。通信不可能な状態（リンダウンなど）であれば、ルーティングテーブルから削除します。フローティング動作しない場合は、インタフェースの状態にかかわらず常にスタティック経路情報をルーティングテーブルに追加します。

下記に、各設定値とフローティング動作の関係を示します。

<distance> 設定値	インタフェース経路の フローティング設定	スタティック経路の フローティング動作
0(省略値)	使用しない	しない
0(省略値)	使用する	する
1以上	使用しない	する
1以上	使用する	する

以下のような用途でスタティック経路情報を使用する場合、フローティング動作するとなるように設定してください。

- IP ルーティングおよびダイナミックルーティングでの広報において、スタティック経路の出口インタフェースで異常が発生した場合、ルーティングテーブルよりスタティック経路を削除する。
- あて先が同じ経路をダイナミックルーティングで受信した場合、優先度関係により経路を決定する。

複数のスタティック経路情報で ECMP 機能を使用するときは、あて先、RIP メトリック値、優先度がそれぞれ同じとなるようにスタティック経路情報を設定します。また、ECMP 機能を使用する場合は、routemanage ip ecmp mode コマンドで ECMP を使用するように設定します。

ECMP となるスタティック経路情報は、同じあて先への経路情報ごとに装置全体で 4 個まで定義できます。

IPv4 スタティック経路情報は、本装置全体で以下の数まで定義できます。

最大定義数	機種
256	MR1000

[注意]

同じあて先へのスタティック経路情報を複数設定する場合、以下の点に注意してください。

- 優先度が 0 のスタティック経路情報と、優先度が 0 または 1 以上のスタティック経路情報は同時に設定できません。
- 優先度が同じで、RIP メトリック値が違うスタティック経路情報は同時に設定できません。

[未設定時]

IPv4 スタティック経路情報を使用しないものとみなされます。

4.4.4　remote ip rip use

[機能]

RIP 基本情報の設定

[入力形式]

remote [<number>] ip rip use <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、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 パケット送信時の加算メトリック値を、0～16 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。

<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]

RIP の基本的な動作を設定します。

<metric>は、RIP パケットを送信する際に加算するメトリック値を設定します。

RIP(IPv4) を使用するインタフェースは、本装置全体で以下の数まで定義できます。

最大定義数	機種
120	MR1000

[注意]

remote mtu コマンドを使用し、MTU 値を 576 よりも小さい値を設定すると、RIPv1(Broadcast), RIPv2(Broadcast) 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。

NAT との併用はできません。

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。

[未設定時]

RIP 機能を使用しないものとみなされます。

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

4.4.5　remote ip rip filter act

[機能]

RIP フィルタ動作の設定

[入力形式]

remote [<number>] ip rip filter <count> act <action> <direction>

[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、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定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜399	MR1000

<action>

フィルタリング条件に一致した場合の動作を指定します。

- pass
  該当する経路情報を透過します。
- reject
  該当する経路情報を遮断します。

<direction>

フィルタリングを行う方向を指定します。

- in
  受信時にフィルタリングを行います。
- out
  送信時にフィルタリングを行います。

[説明]

RIP での経路情報送受信時に、フィルタリング条件に一致した経路情報を通過 (pass) させるか遮断 (reject) させるかを設定します。フィルタリング条件は優先度順に検索し、条件に一致した経路情報があった時点でフィルタリングが行われ、それ以降の条件は参照されません。全条件に不一致の経路情報は遮断されます。

フィルタリング条件は、remote ip rip filter route コマンドを使用し経路情報を設定します。

<count>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号が既に存在する場合は、既存の定義が上書きされます。

RIP フィルタは、本装置全体で以下の数まで定義できます。

最大定義数	機種
400	MR1000

[注意事項]

フィルタリング条件が設定されていない場合、本コマンドの設定は無効となります。

[未設定時]

RIP フィルタを使用しないものとみなされ、すべての RIP の経路情報が透過します。

4.4.6　remote ip rip filter move

[機能]

RIP フィルタの優先順序の変更

[入力形式]

remote [<number>] ip rip 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、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、10 進数値で指定します。
  すで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。

範囲	機種
0～399	MR1000

[説明]

RIP フィルタの優先順序を変更します。
<new_count>で、既存定義番号を指定した場合、その定義の前に挿入されます。また、<new_count>は順番にソートされてリナンバリングされます。

4.4.7 remote ip rip filter route

[機能]

RIP フィルタの経路情報設定

[入力形式]

remote [<number>] ip rip filter <count> route <address> / <mask> [<prefix_match>]

[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、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定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜399	MR1000

<address>/<mask>/

- IPv4 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経路情報を、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)
- any
  すべての経路情報をフィルタリング対象とする場合に指定します。
- default
  デフォルトルート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。

<prefix_match>

経路情報 (IPv4 アドレス / マスク) の検索条件を指定します。
省略した場合は、exact を指定したものとみなされます。
<address> / <mask>に"any"または"default"を指定した場合は、<prefix_match>は指定できません。

- exact
  指定した<address> / <mask>と経路情報の IPv4 アドレス / マスクを比較し、一致した場合に、フィルタリング対象とします。
- inexact
  指定した<address>と経路情報の IPv4 アドレスを比較し、<mask>まで一致した場合、フィルタリング対象とします。

[説明]

フィルタリング条件として経路情報を設定します。

[未設定時]

フィルタリング条件が設定されていないものとみなされます。

4.4.8 remote ip rip filter set metric

[機能]

RIP フィルタのメトリック設定

[入力形式]

remote [<number>] ip rip filter <count> set metric <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、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定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0～399	MR1000

<metric>

- メトリック値
  メトリック値を、0～16 の 10 進数値で指定します。

[説明]

フィルタリング条件に一致した経路情報のメトリック値を変更します。
<metric>に 1～16 を設定した場合、メトリック値は設定した値に変更されます。また、この場合、remote ip rip use コマンドで設定した加算メトリック値は加算されません。0 を指定した場合、メトリック値の変更は行われません。

[注意事項]

フィルタリング条件が設定されていない場合、本コマンドの設定は無効となります。
フィルタリング条件の"any"と一致した場合、本コマンドの設定は無効となります。

[未設定時]

フィルタリング条件に一致した経路情報のメトリック値を変更しないものとみなされます。

4.4.9　remote ip ospf use

[機能]

OSPF 利用可否の設定

[入力形式]

remote [<number>] ip ospf use <mode> [<area_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、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
  OSPF を利用しません。
- on
  OSPF を利用します。

<area_number>

- エリア定義番号
  OSPF を利用する場合は、エリアの定義番号を指定します。
  省略した場合は、0 を指定したものとみなされます。

範囲	機種
0〜2	MR1000

[説明]

OSPF を利用するかどうかと、インタフェースが属するエリアの定義番号を設定します。
OSPF を使用するインタフェースは、本装置全体で以下の数まで定義できます。

最大定義数	機種
100	MR1000

[注意]

OSPF の利用は、"ospf ip area id"を設定した場合にだけ有効です。
Unnumbered インタフェースの場合、OSPF は動作しません。

[未設定時]

OSPF を使用しないものとみなされます。

```
remote <number> ip ospf use off
```

4.4.10 remote ip ospf cost

[機能]

OSPF 出力コストの設定

[入力形式]

remote [<number>] ip ospf cost <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、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。

<cost>

- 出力コスト
  出力コストを、1～65535 で指定します。

[説明]

OSPF 出力コストを設定します。

[未設定時]

OSPF 出力コストに 10 が設定されているものとみなされます。

```
remote <number> ip ospf cost 10
```

4.4.11　remote ip ospf hello

[機能]

OSPF Hello パケット送信間隔の設定

[入力形式]

remote [<number>] ip ospf hello <hello_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、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。

<hello_interval>

- Hello パケット送信間隔
  Hello パケットの送信間隔時間を、1 秒～65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、1s～65535s、1m～1092m、1h～18h です。

[説明]

OSPF 隣接関係の維持に用いられる Hello パケットの送信間隔を設定します。hello_interval の値は OSPF 隣接ルータ間で同じ値を設定します。

[注意]

OSPF 隣接ルータ間で異なる Hello パケットの送信間隔を設定した場合、ルーティングが行えません。

[未設定時]

Hello パケット送信間隔に 10 秒が設定されているものとみなされます。

```
remote <number> ip ospf hello 10s
```

4.4.12 remote ip ospf dead

[機能]

OSPF 隣接ルータ停止確認間隔の設定

[入力形式]

remote [<number>] ip ospf dead <dead_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、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。

<dead_interval>

- 隣接ルータ停止確認間隔
  隣接ルータ停止確認の間隔時間を、1 秒～65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、1s～65535s、1m～1092m、1h～18h です。

[説明]

OSPF 隣接関係の維持に用いられる隣接ルータ停止確認間隔を設定します。
隣接ルータ停止確認間隔の間に Hello パケットを受信しなかった場合は、そのルータとの隣接関係は解除されます。
dead_interval の値は OSPF 隣接ルータ間で同じ値を設定します。
dead_interval の値は Hello パケット送信間隔よりも大きな値を設定する必要があります。
Hello パケット送信間隔の 4 倍を設定することを推奨します。

[注意]

OSPF 隣接ルータ間で異なる隣接ルータ停止確認間隔を設定した場合、ルーティングが行えません。

[未設定時]

隣接ルータ停止確認間隔に 40 秒が設定されているものとみなされます。

```
remote <number> ip ospf dead 40s
```

4.4.13　remote ip ospf retrans

[機能]

OSPF パケット再送間隔の設定

[入力形式]

remote [<number>] ip ospf retrans <retransmit_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、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。

<retransmit_interval>

- パケット再送間隔
  パケットの再送間隔を、3 秒～65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、3s～65535s、1m～1092m、1h～18h です。

[説明]

OSPF パケットを再送する間隔を設定します。

[未設定時]

OSPF パケットの再送間隔に 5 秒が設定されているものとみなされます。

```
remote <number> ip ospf retrans 5s
```

4.4.14 remote ip ospf delay

[機能]

OSPF LSU パケット送信遅延時間の設定

[入力形式]

remote [<number>] ip ospf delay <transmit_delay>

[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、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。

<transmit_delay>

- LSU パケット送信遅延時間
  LSU パケットを送信する場合の遅延時間を、1 秒～65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、1s～65535s、1m～1092m、1h～18h です。

[説明]

LSU(Link State Update) パケットの送信遅延時間を設定します。LSU パケットでは、LSA(Link State Advertisement) を作成してからの経過時間に<transmit_delay>の値を加算して広報します。

[注意]

一般的な装置では、作成してからの経過時間が 1 時間となった LSA を破棄します。このため、LSU 送信遅延時間に 1 時間以上を設定した場合は、正しくルーティングできない場合があります。

[未設定時]

LSU パケット送信遅延時間に 1 秒が設定されているものとみなされます。

```
remote <number> ip ospf delay 1s
```

4.4.15　remote ip ospf auth type

[機能]

OSPF パケット認証方式の設定

[入力形式]

remote [<number>] ip ospf 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、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>

パケット認証方式を指定します。

- off
  認証を行いません。
- text
  テキスト認証を使用します。
- md5
  MD5 認証を使用します。

[説明]

OSPF パケットに対する認証方式を設定します。

[注意]

テキスト認証の使用は、"remote ip ospf auth textkey"を設定した場合にだけ有効です。MD5 認証の使用は、"remote ip ospf auth md5key"を設定した場合にだけ有効です。

[未設定時]

OSPF パケット認証を使用しないものとみなされます。

```
remote <number> ip ospf auth type off
```

4.4.16 remote ip ospf auth textkey

[機能]

OSPF テキスト認証鍵の設定

[入力形式]

remote [<number>] ip ospf auth textkey <kind> <key> [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、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。

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

<key>

- テキスト認証鍵
  文字列鍵の場合は、0x21,0x23～0x7e のコードで構成される 8 文字以内の ASCII 文字列で指定します。
  16 進数鍵の場合は、16 桁以内の 16 進数値で指定します。16 桁未満の値を指定したときは左詰めで設定され、残りは 16 桁になるまで 0x0 でパディングされます。
- 暗号化されたテキスト認証鍵
  show コマンドで表示される暗号化されたテキスト認証鍵を 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

- 暗号化テキスト認証鍵指定
  <key>に暗号化されたテキスト認証鍵を指定する場合に指定します。

[説明]

テキスト認証で使用する鍵を設定します。
show コマンドでは、暗号化されたテキスト認証鍵が encrypted と共に表示されます。

[未設定時]

テキスト認証鍵が設定されていないものとみなされます。

4.4.17　remote ip ospf auth md5key

[機能]

OSPF MD5 認証鍵情報の設定

[入力形式]

remote [<number>] ip ospf auth md5key <key_id> <key> [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、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。

<key_id>

- MD5 認証鍵 ID
  MD5 認証鍵 ID を、1～255 で指定します。
- 暗号化された MD5 認証鍵 ID
  show コマンドで表示される暗号化された MD5 認証鍵 ID 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。

<key>

- MD5 認証鍵
  MD5 認証鍵を、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。
- 暗号化された MD5 認証鍵
  show コマンドで表示される暗号化された MD5 認証鍵を 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 MD5 認証鍵情報指定
  <key_id>と<key>に暗号化された MD5 認証鍵 ID と MD5 認証鍵を指定する場合に指定します。

[説明]

MD5 認証で使用する鍵情報 (MD5 認証鍵 ID、MD5 認証鍵) を設定します。
show コマンドでは、暗号化された MD5 認証鍵 ID と MD5 認証鍵が encrypted と共に表示されます。

[未設定時]

MD5 認証で使用する鍵情報が設定されていないものとみなされます。

4.4.18 remote ip ospf passive

[機能]

OSPF パケット送信抑止の設定

[入力形式]

remote [<number>] ip ospf passive <interface_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、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。

<interface_type>

- on
  パケットの送信を抑止します。
- off
  パケットの送信を抑止しません。

[説明]

OSPF パケット送信の抑止を設定します。

[未設定時]

OSPF パケットの送信は抑止しないものとみなされます。

```
remote <number> ip ospf passive off
```

4.4.19　remote ip ospf multicast

[機能]

OSPF 送信方法の設定

[入力形式]

remote [<number>] ip ospf multicast <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、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>

OSPF パケットをマルチキャストで送信するかどうかを指定します。

- on
  マルチキャストで送信します。
- off
  ユニキャストで送信します。

[説明]

OSPF パケットは、通常はマルチキャストで送信します。マルチキャストでは受信できない相手装置と接続する場合、off を設定することでユニキャストで送信します。

[未設定時]

マルチキャストで送信するものとみなされます。

```
remote <number> ip ospf multicast on
```

4.4.20 remote ip ospf checkmtu

[機能]

OSPF パケットの MTU 値確認抑止の設定

[入力形式]

remote [<number>] ip ospf checkmtu <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、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>

OSPF パケットの MTU 値の確認を抑止するかどうかを指定します。

- on
  MTU 値の確認を行います。
- off
  MTU 値の確認を行いません。

[説明]

OSPF パケットの MTU 値は、通常、同一値であることを確認します。ただし、相手装置仕様により、MTU 値の不整合が回避できない場合、off を設定することで確認を抑止することができます。

[注意]

MTU 値の確認設定を off とする場合は、相手装置の送信するパケットの長さが自装置の MTU サイズ以下である必要があります。相手装置の仕様が確認できる場合だけご使用ください。

[未設定時]

OSPF パケットの MTU 値の確認を行うものとみなされます。

```
remote <number> ip ospf checkmtu on
```

4.4.21　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、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。
- static
  静的 NAT だけを使用します。

以下のパラメタは、<mode>に nat または multi または static を設定した場合に有効です。

<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
  動的アドレス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。
  <address>に any を指定した場合は、1 を指定してください。

<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) のどれかを指定します。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
```

4.4.22　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、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、10 進数値で指定します。

範囲	機種
0〜199	MR1000

<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だけ指定可能です。
- 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、本装置全体で以下の数まで定義できます。

最大定義数	機種
200	MR1000

[未設定時]

静的アドレス変換は設定されません。

4.4.23　remote ip nat static default

[機能]

テーブルに一致しないパケットの扱いの設定

[入力形式]

remote [<number>] ip nat static default <action>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通番として 0 以上の 10 進数値を指定する。省略時は 0 と認識する。

<action>

すべての NAT テーブルにも一致しなかったパケットをどう扱うかを指定します。

- pass
  該当するパケットの IP アドレスやポート番号を変換しないで透過させます。
- reject
  該当するパケットを破棄します。

[説明]

すべての NAT テーブルに一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

すべての NAT テーブルにも一致しないパケットは破棄します。

```
remote <number> ip nat static default reject
```

4.4.24 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、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 アドレスおよ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だけ有効となります。DNS の応答の UDP パケットのソース IP アドレスおよ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 アドレスおよ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 アドレスおよ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 アドレスおよ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。

4.4.25 remote ip nat wellknown

[機能]

ポート番号変換の設定

[入力形式]

remote [<number>] ip nat wellknown <count> <port> <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、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>

ポート番号変換定義番号を、0～99 の 10 進数値で指定します。

<port>

- プライベートポート番号
  プライベートポート番号を、1～65535 の 10 進数値で指定します。
  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。
  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)
- any
  すべてのプライベートポート番号を対象とする場合に指定します。

<mode>

- on
  well-known ポート番号とみなし、変換を行いません。
- off
  well-known ポート番号とみなさず、変換を行います。

[説明]

プライベートポート番号の変換を行うかどうかの設定をします。プライベートポート番号がいずれの設定にもあてはまらない場合には、未設定時と同様にプライベートポート番号の変換を行います。ポート番号変換の設定は本装置全体で 100 個まで定義できます。

[未設定時]

以下のポート番号についてはポート番号の変換を行いません。
1～1024(本来の well-known ポート番号)
28800～28830(Microsoft Internet Gaming Zone)
1558(StreamWorks)
8000(StreamWorks)
118(Diablo)

116(Diablo)
6112(Battle.net)
6799(NETSTORM)
6800(NETSTORM)
9000(HEAVY GEAR)
7070(Real Player)
7000(VDO Live Video)
6667(IRC)
7648(CU-SeeMe)
7649(CU-SeeMe)
40027(SurfV)
40026(SurfV)
1638(DARK REIGN)

4.4.26 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> [<direction> [<icmptype> [<icmpcode>]]]]

[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、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、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すでに存在する場合は、既存の定義を変更します。

範囲	機種
0〜199	MR1000

<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あて先 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あて先 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
  すべてのあて先 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あて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あて先ポート番号を、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
  すべてのあて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、1〜255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。
- any
  すべてのプロトコル番号をフィルタリング対象とする場合に指定します。

<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。

<direction>

フィルタリングする方向を指定します。
省略した場合は、any を指定したものとみなされます。

- any

  入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。

- in

  入力パケットだけをフィルタリング対象とする場合に指定します。

- out

  出力パケットだけをフィルタリング対象とする場合に指定します。

- reverse

  入力パケットと出力パケットの両方をフィルタリング対象とします。

  ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。

  - 送信元 IP アドレス/マスクとあて先 IP アドレス/マスク
  - 送信元ポート番号とあて先ポート番号

<icmptype>

フィルタリング対象とする ICMP TYPE を指定します。

- ICMP TYPE

  フィルタリング対象とする送信元 ICMP TYPE を、0〜255 の 10 進数値で指定します。複数の ICMP TYPE 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、「8-30」のように"-"(ハイフン) を使用して指定します。

  ICMP TYPE 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。

  - 0〜255 の 10 進数値 (例: 8 = ICMP TYPE 8)
  - ICMP TYPE-ICMP TYPE (例: 2-8 = 2 から 8 までの ICMP TYPE)
  - ICMP TYPE- (例: 8- = 8 から 255 までの ICMP TYPE)

- -ICMP TYPE (例: -200 = 0 から 200 までの ICMP TYPE)
- ICMP TYPE,ICMP TYPE,… (例: 0,8,30- = 0 と 8 と 30 以降の ICMP TYPE)

- any
  すべての ICMP TYPE をフィルタリング対象とする場合に指定します。

<icmpcode>

フィルタリング対象とする ICMP CODE を指定します。

- ICMP CODE
  フィルタリング対象とする送信元 ICMP CODE を、0～255 の 10 進数値で指定します。複数の ICMP CODE 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、「8-30」のように"-"(ハイフン) を使用して指定します。
  ICMP CODE 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。
  - 0～255 の 10 進数値 (例: 8 = ICMP CODE 8)
  - ICMP CODE-ICMP CODE (例: 2-8 = 2 から 8 までの ICMP CODE)
  - ICMP CODE- (例: 8- = 8 から 255 までの ICMP CODE)
  - -ICMP CODE (例: -200 = 0 から 200 までの ICMP CODE)
  - ICMP CODE,ICMP CODE,… (例: 0,8,30- = 0 と 8 と 30 以降の ICMP CODE)

- any
  すべての ICMP CODE 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 ICMP TYPE, ICMP CODE と一致するパケットを透過または遮断します。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 フィルタリング定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
200	MR1000

[注意]

<direction>に reverse を指定した場合には、入力パケットは IP アドレス/マスクとポート番号だけを逆転した条件でフィルタリングされます。このため、<tcpconnect>を有効にしている場合には、入力パケットに対しても、TCP プロトコルのコネクション接続要求がフィルタリング対象に含まれます。

[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。

4.4.27　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、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、10 進数値で指定します。
  すで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。

範囲	機種
0～199	MR1000

[説明]

IP フィルタの優先順序を変更します。

4.4.28　remote ip filter default

[機能]

いずれの IP フィルタテーブルにも不一致時の動作の設定

[入力形式]

remote [<number>] ip filter default <action> [<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、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。

<action>

いずれの IP フィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

- 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。
- spi
  該当するパケットに対して SPI を動作させます。

<time>

- 割当時間
  action に spi を指定したときに、接続に割り当てられた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) のどれかを指定します。
  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]

いずれの IP フィルタテーブルに一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

いずれの IP フィルタテーブルにも一致しないパケットは透過します。

```
remote <number> ip filter default pass
```

4.4.29 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、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、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 値書き換え定義がすでに存在する場合は、既存定義の値を変更します。

範囲	機種
0〜99	MR1000

<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あて先 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あて先 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
  すべてのあて先 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あて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あて先ポート番号を、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>

TOS 値書き換え対象となるプロトコル番号を指定します。

- 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、1～255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。
- any
  すべてのプロトコル番号を TOS 値書き換え対象とする場合に指定します。

<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 値書き換え定義は、本装置全体で以下の数まで定義できます。

最大定義数	機種
100	MR1000

[未設定時]

TOS 値書き換えを行わないものとみなされます。

4.4.30　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、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、10 進数値で指定します。
  すで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。

範囲	機種
0～99	MR1000

[説明]

TOS 値書き換え条件の優先度を変更します。

4.4.31 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、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、10 進数値で指定します。

範囲	機種
0〜99	MR1000

<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あて先 IP アドレス、マスクビット数を指定します。

- あて先 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あて先 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あて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あて先ポート番号を、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>

帯域制御の対象となるプロトコル番号を指定します。

- 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、1～255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。
- any
  すべてのプロトコル番号を帯域制御の対象とする場合に指定します。

<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>

- express
  最優先データとして扱います。
- besteffort
  非優先 (ベストエフォート) として扱います。
- 帯域
  1〜99 の 10 進数値で指定した場合、それぞれ指定した値の比で帯域を割り当てます。たとえば、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。
  「数字 + "kbps"(,"mbps")」で指定した場合、指定した帯域をそのまま割り当てます。
  1kbps〜100000kbps または、1mbps〜100mbps の範囲で指定します。全定義の帯域の合計が回線速度を超えた場合には、それぞれ指定した値の比で帯域を割り当てます。指定した値の合計値が回線速度に達しない場合、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。
  「"share" + 数字」で指定した場合、数字で指定した帯域制御定義番号で定義された帯域を共有します。この場合、指定する数字は自分自身の帯域制御定義番号より小さい、すでに定義されてあるもの指定しなければなりません。

[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、本装置全体で以下の数まで定義できます。

最大定義数	機種
100	MR1000

[注意]

IPv4,IPv6 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。
使用する回線が LAN の場合、シェーピングを使用しないと帯域制御機能は有効に動作しません。
使用する回線が ATM の場合、適切な VC 速度を設定しないと帯域制御機能は有効に動作しません。

[未設定時]

帯域制御を行わないものとみなされます。

4.4.32　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、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
```

4.4.33 remote ip multicast mode

[機能]

マルチキャストインタフェースの定義

[入力形式]

remote [<number>] ip multicast mode <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、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>

マルチキャスト定義の動作を指定します。

- off
  マルチキャストパケットを中継しません。
- static
  スタティックルーティングのみで動作します。
- pimdm
  PIM-DM として動作します。
- pimsm
  PIM-SM として動作します。

[説明]

<number>で指定したインタフェースのマルチキャスト・ルーティングプロトコルを有効化し、マルチキャストパケットを中継します。

[注意]

複数インタフェースで異なるプロトコルが選択された場合には、最初に見つかったインタフェースのプロトコルが有効になります。

[未設定時]

マルチキャストパケットを中継しません。

```
remote [<number>] ip multicast mode off
```

4.4.34　remote ip multicast ttl threshold

[機能]

マルチキャストインタフェースの TTL しきい値の定義

[入力形式]

remote [<number>] ip multicast ttl threshold <threshold>

[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、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。

<threshold>

- TTL しきい値
  マルチキャストパケットを中継するインタフェースの TTL のしきい値を 1～255 の 10 進数値で指定します。

[説明]

TTL が<threshold>で指定したしきい値以上のマルチキャストパケットだけ中継します。

[注意]

PIM-SM の PIM Register パケットによりカプセル化されるマルチキャスト・パケットは、出力先インタフェースの TTL しきい値の設定によらずに出力されます。

[未設定時]

1 になります。

```
remote [<number>] ip multicast ttl threshold 1
```

4.4.35 remote ip multicast pim preference

[機能]

マルチキャストインタフェースの PIM プリファレンス値の定義

[入力形式]

remote [<number>] ip multicast pim preference <preference>

[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、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。

<preference>

- プリファレンス値
  マルチキャストパケットを中継するインタフェースの PIM プリファレンス値を 1～65535 の 10 進数値で指定します。

[説明]

マルチキャスト・パケットの配送経路が重複したばあいには、プリファレンス値の小さい経路で配送されます。

[注意]

PIM Assert 発行時には Assert 対象となるパケットの発信元へのユニキャスト経路を参照し、発信元へ向かうインタフェースのプリファレンス値を Assert メッセージに格納します。Assert メッセージが出力されるインタフェースのプリファレンス値が格納されるわけではありません。

[未設定時]

1024 になります。

```
remote [<number>] ip multicast pim preference 1024
```

4.4.36　remote ip multicast pim upstream type

[機能]

上流ルータの種類によるマルチキャストパケット転送許可設定

[入力形式]

remote [<number>] ip multicast pim upstream 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、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>

- pim
  上流ルータが PIM ルータのときのみ、マルチキャストパケットを転送します。
- any
  上流ルータが PIM ルータでない場合でも、マルチキャストパケットを転送します。

[説明]

本装置より上流にルータが存在し、そのルータを経由してマルチキャストパケットが転送されてくる場合、どの種類のルータからのマルチキャストパケット転送を許可するかを指定します。

上流ルータが PIM ルータでない場合 (マルチキャストパケットをスタティック経路によって転送するルータであった場合) に転送を許可したい場合は <type> に any を指定することで転送を可能にします。

[注意]

受信インタフェースと同一の IP セグメントから送信された (直接接続されたホストからの) マルチキャストパケットについては、本コマンドの指定に関わらず転送が行なわれます。

[未設定時]

上流ルータが PIM ルータのときのみ、マルチキャストパケットを転送します。

```
remote [<number>] ip multicast pim upstream type pim
```

4.4.37 remote ip exp

[機能]

Exp 値書き換え条件の設定

[入力形式]

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

[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、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>

- Exp 書き換え条件定義番号

  Exp 書き換えの優先度を表す番号を、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 Exp 書き換え条件定義がすでに存在する場合は、既存の定義を変更します。

範囲	機種
0〜99	MR1000

<src_addr>/<mask>

Exp 値書き換え対象となる送信元 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)

  Exp 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 IP アドレスを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>

Exp 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

  Exp 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>

Exp 値書き換え対象となる送信先 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)
  Exp 値書き換え対象となる送信先 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>

Exp 値書き換え対象となる送信先ポート番号を指定します。

- ポート番号
  Exp 値書き換え対象となる送信先ポート番号を、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>

Exp 値書き換え対象となるプロトコル番号を指定します。

- プロトコル番号
  Exp 値書き換え対象となるプロトコル番号を、1〜255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。
- any
  すべてのプロトコル番号を Exp 値書き換え対象とする場合に指定します。

<tos>

Exp 値書き換え対象となる TOS 値を指定します。

- TOS 値
  Exp 値書き換え対象の 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、"-"(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 値を対象とする場合に指定します。

<exp>

- Exp 値
  書き換える Exp 値を、0～7 の 10 進数値で指定します。

[説明]

相手ネットワークに対する Exp 書き換え条件を設定します。
Exp 書き換え条件は、本装置全体で以下の数まで定義できます。

最大定義数	機種
100	MR1000

[注意]

remote ap datalink type mpls の ap を使用する場合にだけ有効です。

[未設定時]

Exp 値書き換えは行わないとみなされます。

4.4.38　remote ip exp move

[機能]

Exp 値書き換え条件優先順序の変更

[入力形式]

remote [<number>] ip exp 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、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 Exp 書き換え条件定義番号
  優先順序を変更する Exp 書き換え条件定義の番号を指定します。

<new_count>

- 移動先 Exp 書き換え条件定義番号
  <count>に対する新しい順序を、10 進数値で指定します。
  すで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。

範囲	機種
0～99	MR1000

[説明]

Exp 値を書き換えの条件優先順序を変更します。

4.5 IPv6 関連情報

4.5.1 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、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
```

4.5.2　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、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
```

4.5.3 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、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。

  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/プレフィックス長

  IPv6 アドレスとプレフィックス長を指定します。リンクローカルアドレスは指定できません。IPv6 DHCP クライアントが取得したプレフィックスを使用する場合は上位を"dhcp@インタフェース名"の形式で指定し，下位 80bit 分を IPv6 アドレス形式で指定します。インタフェース名には、rmt インタフェースを以下の範囲で指定します。

範囲	機種
rmt0〜rmt99	MR1000

例)rmt0で動作するIPv6 DHCPクライアントが取得したIPv6プレフィックスを使用する場合の設定例

```
dhcp@rmt0::/64
dhcp@rmt0::1:2:3:4/64
```

プレフィックス長には 64 を指定してください。

<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) のどれかを指定します。

  <address> / <prefixlen>に IPv6 DHCP クライアントが取得したプレフィックスを使用する指定をした場合は、IPv6 DHCP クライアントが取得した valid lifetime と比較して短い方が有効になります。

- 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) のどれかを指定します。<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。

  <address>/<prefixlen>に IPv6 DHCP クライアントが取得したプレフィックスを使用する指定をした場合は、IPv6 DHCP クライアントが取得した preferred lifetime と比較して短い方が有効になります。

- 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。

[注意]

IPv6 DHCP クライアントが取得したプレフィックスと設定値の重なる部分において，0 以外の値がある場合には，IPv6 アドレスは割り当てられません.

```
<-IPv6 DHCPクライアントが取得したプレフィックス->
                                <--------------ユーザ設定値(80bit)---------------------->
+-------------------------------+------------+-------------------------------------------+
|                               | //////////// |                                           |
+-------------------------------+------------+-------------------------------------------+
                                <------------>
                                 設定値が重なる部分
例）IPv6 DHCPクライアントが2001:db8:1000:5555::/64を取得した場合
    設定内容                    利用されるアドレス
    dhcp@rmt0:0:100::1/64       2001:db8:1000:5555:100::1/64
    dhcp@rmt0:100:200::1/64     無効
```

[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。

4.5.4 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、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
```

4.5.5　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、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
```

4.5.6 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、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
```

4.5.7　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、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
```

4.5.8 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、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
```

4.5.9　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、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
```

4.5.10 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、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
```

4.5.11　remote ip6 route

[機能]

IPv6 スタティック経路情報の設定

[入力形式]

remote [<number>] ip6 route <count> <address>/<prefixlen> [<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、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>

- スタティック経路情報定義番号
  スタティック経路情報の定義番号を、10 進数値で指定します。

範囲	機種
0〜255	MR1000

<address>/<prefixlen>

- IPv6 アドレス/プレフィックス
  あて先ネットワークを IPv6 アドレスとプレフィックスの組み合わせで指定します。
  リンクローカルアドレスは指定できません。
- default
  あて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
  このスタティック経路情報を RIP に再配布するときのメトリック値を、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。

<distance>

- 優先度
  このスタティック経路情報の優先度を、0〜254 の 10 進数値で指定します。
  優先度は数値の小さい方がより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]

IPv6 スタティック経路 (静的経路) 情報を設定します。
RIP メトリック値は、スタティック経路情報を RIP に再配布するときのメトリック値を設定します。RIP に再配布したときは、設定した RIP メトリック値+1 のメトリック値で RIP テーブルに登録されます。
優先度は、同じあて先への経路情報が複数ある場合、優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。各ダイナミックルーティングプロトコルの優先度については、routemanage ip6 distance コマンドを参照してください。

優先度に 0 が設定されているときは、routemanage interface floating コマンドでのフローティング設定に応じてフローティング動作が切り替わります。優先度に 1 以上が設定されているときは、常にフローティング動作します。

フローティング動作する場合、remote インタフェースが通信可能な状態（リンクアップなど）であれば、スタティック経路情報をルーティングテーブルに追加します。通信不可能な状態（リンダウンなど）であれば、ルーティングテーブルから削除します。フローティング動作しない場合は、インタフェースの状態にかかわらず常にスタティック経路情報をルーティングテーブルに追加します。

下記に、各設定値とフローティング動作の関係を示します。

<distance> 設定値	インタフェース経路の フローティング設定	スタティック経路の フローティング動作
0(省略値)	使用しない	しない
0(省略値)	使用する	する
1以上	使用しない	する
1以上	使用する	する

以下のような用途でスタティック経路情報を使用する場合、フローティング動作するとなるように設定してください。

- IP ルーティングおよびダイナミックルーティングでの広報において、スタティック経路の出口インタフェースで異常が発生した場合、ルーティングテーブルよりスタティック経路を削除する。
- あて先が同じ経路をダイナミックルーティングで受信した場合、優先度関係により経路を決定する。

IPv6 スタティック経路情報は、本装置全体で以下の数まで定義できます。

最大定義数	機種
256	MR1000

[注意]

同じあて先へのスタティック経路情報を複数設定する場合、以下の点に注意してください。

- 優先度が 0 のスタティック経路情報と、優先度が 0 または 1 以上のスタティック経路情報は同時に設定できません。
- 優先度が同じスタティック経路情報は同時に設定できません。

[未設定時]

IPv6 スタティック経路情報を使用しないものとみなされます。

4.5.12　remote ip6 rip use

[機能]

IPv6 RIP 基本情報の設定

[入力形式]

remote [<number>] ip6 rip use <send> <receive> [<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、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(IPv6) パケットを送信するかどうか指定します。

- on
  RIP(IPv6) パケットを送信します。
- off
  RIP(IPv6) パケットを送信しません。

<receive>

RIP(IPv6) パケットを受信するかどうか指定します。

- on
  RIP(IPv6) パケットを受信します。
- off
  RIP(IPv6) パケットを受信しません。

<metric>

- 加算メトリック値
  RIP(IPv6) パケット送信時の加算メトリック値を、0〜16 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]

RIP(IPv6) の基本的な動作を設定します。
<metric>は、RIP(IPv6) パケットを送信する際に加算するメトリック値を設定します。
RIP(IPv6) を使用するインタフェースは、本装置全体で以下の数まで定義できます。

最大定義数	機種
120	MR1000

[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。

[未設定時]

RIP(IPv6) 機能を使用しないものとみなされます。

```
remote <number> ip6 rip use off off 0
```

4.5.13　remote ip6 rip site-local

[機能]

IPv6 RIP site-local プレフィックス送受信の設定

[入力形式]

remote [<number>] ip6 rip site-local <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、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>

site-local プレフィックスを送受信するかどうかを指定します。

- on
  site-local プレフィックスを送受信します。
- off
  site-local プレフィックスを送受信しません。

[説明]

RIP(IPv6) で site-local プレフィックスを送受信するかどうかを設定します。

[未設定時]

site-local プレフィックスを送受信するものとみなされます。

```
remote <number> ip6 rip site-local on
```

4.5.14 remote ip6 rip aggregate

[機能]

IPv6 RIP における集約経路の設定

[入力形式]

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

[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、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
  集約経路のあて先ネットワークを 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
  集約経路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。

<rejectroute>

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

[説明]

RIP(IPv6) 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、実際に持たないあて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 reject 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]

RIP(IPv6) で経路集約しないものとみなされます。

4.5.15　remote ip6 rip filter act

[機能]

IPv6 RIP フィルタ動作の設定

[入力形式]

remote [<number>] ip6 rip filter <count> act <action> <direction>

[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、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定義番号を、10 進数値で指定します。優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜399	MR1000

<action>

フィルタリング条件に一致した場合の動作を指定します。

- pass
  該当する経路情報を透過します。
- reject
  該当する経路情報を遮断します。

<direction>

フィルタリングを行う方向を指定します。

- in
  受信時にフィルタリングを行います。
- out
  送信時にフィルタリングを行います。

[説明]

RIP(IPv6) での経路情報送受信時に、フィルタリング条件に一致した経路情報を通過 (pass) させるか遮断 (reject) させるかを設定します。フィルタリング条件は優先度順に検索し、条件に一致した経路情報があった時点でフィルタリングが行われ、それ以降の条件は参照されません。全条件に不一致の経路情報は遮断されます。

フィルタリング条件は、remote ip6 rip filter route コマンドを使用し経路情報を設定します。

<count>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号が既に存在する場合は、既存の定義が上書きされます。

RIP フィルタ (IPv6) は、本装置全体で以下の数まで定義できます。

最大定義数	機種
400	MR1000

[注意事項]

フィルタリング条件が設定されていない場合、本コマンドの設定は無効となります。

[未設定時]

RIP(IPv6) フィルタを使用しないものとみなされ、すべての RIP(IPv6) の経路情報が透過します。

4.5.16　remote ip6 rip filter move

[機能]

IPv6 RIP フィルタの優先順序の変更

[入力形式]

remote [<number>] ip6 rip 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、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、10 進数値で指定します。
  すで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。

範囲	機種
0～399	MR1000

[説明]

RIP(IPv6) フィルタの優先順序を変更します。
<new_count>で、既存定義番号を指定した場合、その定義の前に挿入されます。また、<new_count>は順番にソートされてリナンバリングされます。

4.5.17 remote ip6 rip filter route

[機能]

IPv6 RIP フィルタの経路情報設定

[入力形式]

remote [<number>] ip6 rip filter <count> route <address>/<prefixlen> [<prefix_match>]

[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、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定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜399	MR1000

<address>/<prefixlen>

- 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経路情報を、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。
- any
  すべての経路情報をフィルタリング対象とする場合に指定します。
- default
  デフォルトルートをフィルタリング対象とする場合に指定します。

<prefix_match>

経路情報の検索条件を指定します。
省略した場合は、exact を指定したものとみなされます。
<address>/<prefixlen>に"any"または"default"を指定した場合は、<prefix_match>は指定できません。

- exact
  指定した<address>/<prefixlen>と経路情報の IPv6 アドレス/プレフィックス長を比較し、一致した場合に、フィルタリング対象とします。
- inexact
  指定した<address>と経路情報の IPv6 アドレスを比較し、<prefixlen>まで一致した場合、フィルタリング対象とします。

[説明]

フィルタリング条件として経路情報を設定します。

[未設定時]

フィルタリング条件が設定されていないものとみなされます。

4.5.18　remote ip6 rip filter set metric

[機能]

IPv6 RIP フィルタのメトリック設定

[入力形式]

remote [<number>] ip6 rip filter <count> set metric <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、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定義番号を、10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

範囲	機種
0〜399	MR1000

<metric>

- メトリック値
  メトリック値を、0〜16 の 10 進数値で指定します。

[説明]

フィルタリング条件に一致した経路情報のメトリック値を変更します。
<metric>に 1〜16 を設定した場合、メトリック値は設定した値に変更されます。この場合、remote ip6 rip use コマンドで設定した加算メトリック値は加算されません。0 を指定した場合、メトリック値の変更は行われません。

[[注意事項]

フィルタリング条件が設定されていない場合、本コマンドの設定は無効となります。
フィルタリング条件の"any"と一致した場合、本コマンドの設定は無効となります。

[未設定時]

フィルタリング条件に一致した経路情報のメトリック値を変更しないものとみなされます。

4.5.19 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> [<trafficclass> [<direction> [<icmptype> [<icmpcode>]]]]

[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、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、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。

範囲	機種
0〜199	MR1000

<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、0〜254 の 10 進数値で指定します。

- any

  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。

<trafficclass>

- フィルタリング対象 Traffic Class 値

  フィルタリング対象となる Traffic Class フィールドの値を 0-ff までの 16 進数値、または、"-"を使用して表現される 16 進数値の範囲を指定します。

  Traffic Class 値の指定は、"," を区切として 10 個まで設定可能です。

  複数の Traffic Class 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。Traffic Class 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 Traffic Class 値)
  - Traffic Class 値-Traffic Class 値 (例: 32-64 = 32 から 64 までの Traffic Class 値)
  - Traffic Class 値- (例: 80- = 80 から ff までの Traffic Class 値)
  - -Traffic Class 値 (例: -7f = 0 から 7f までの Traffic Class 値)
  - Traffic Class 値,Traffic Class 値,… (例: 10,20,30- = 10 と 20 と 30 以降の Traffic Class 値)

- any

  全ての Traffic Class 値をフィルタリング対象とします。省略された場合は any として扱われます。

<direction>

フィルタリングする方向を指定します。
省略した場合は、any を指定したものとみなされます。

- any

  入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。

- in

  入力パケットのみをフィルタリング対象とする場合に指定します。

- out

  出力パケットのみをフィルタリング対象とする場合に指定します。

- reverse

  入力パケットと出力パケットの両方をフィルタリング対象とします。ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。

  - 送信元 IP アドレス/プレフィックス長と宛先 IP アドレス/プレフィックス長
  - 送信元ポート番号と宛先ポート番号

<icmptype>

フィルタリングする ICMPv6 メッセージタイプ番号を指定します。

- フィルタリング対象 icmptype 値

  フィルタリング対象となる icmptype フィールドの値を 0-255 までの 10 進数値、または、"-"を使用して表現される 10 進数値の範囲を指定します。

  icmptype 値の指定は、"," を区切として 10 個まで設定可能です。記述形式は、<src_port>と同様です。

- any

  全ての icmptype 値をフィルタリング対象とします。省略された場合は any として扱われます。

<icmpcode>

フィルタリングする ICMPv6 メッセージコード番号を指定します。
icmpcode 指定時は、icmptype も指定する必要があります。

- フィルタリング対象 icmpcode 値

  フィルタリング対象となる icmpcode フィールドの値を 0-255 までの 10 進数値、または、"-"を使用して表現される 10 進数値の範囲を指定します。

  icmptype 値の指定は、"," を区切として 10 個まで設定可能です。記述形式は、<src_port>と同様です。

- any

  全ての icmpcode 値をフィルタリング対象とします。省略された場合は any として扱われます。

[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。
  - any 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 any 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。
- <icmptype>、<icmpcode>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 any を指定し、かつ<icmptype>、<icmpcode>を指定している場合、　ICMPv6 パケットの該当 type/code 番号を持つパケットのみが合致します。
  - <protocol>に ICMPv6(58) を指定し、かつ<icmptype>、<icmpcode>を指定している場　合、指定プロトコルの該当 type/code 番号を持つパケットのみが合致します。

- <protocol>に ICMPv6(58) 以外を指定し、かつ<icmptype>、<icmpcode>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 フィルタリング定義は、本装置全体で次の数まで定義できます。

最大定義数	機種
200	MR1000

[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。

4.5.20　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、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、10 進数値で指定します。
  すで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。

範囲	機種
0〜199	MR1000

[説明]

IPv6 フィルタの優先順序を変更します。

4.5.21 remote ip6 filter default

[機能]

いずれの IP フィルタテーブルにも不一致時の動作の設定

[入力形式]

remote [<number>] ip6 filter default <action> [<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、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。

<action>

いずれの IPv6 フィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

- 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。
- spi
  該当するパケットに対して SPI を動作させます。

<time>

- 割当時間
  action に spi を指定したときに接続に割り当てられた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]

いずれの IPv6 フィルタテーブルにも一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

いずれの IPv6 フィルタテーブルにも一致しないパケットは透過します。

```
remote <number> ip6 filter default pass
```

4.5.22　remote ip6 trafficclass

[機能]

Traffic Class 値書き換え条件の設定

[入力形式]

remote [<number>] ip6 trafficclass <count> <src_addr>/<prefixlen> <src_port>
<dst_addr>/<prefixlen> <dst_port> <protocol> <trafficclass> <new_trafficclass>

[パラメタ]

<number>

- remote 定義番号
  remote 定義の通し番号を、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>

- Traffic Class 値書き換え定義番号
  Traffic Class 値書き換え条件の優先度を表す定義番号を、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 Traffic Class 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。

範囲	機種
0〜99	MR1000

<src_addr>/<prefixlen>

書き換え対象とする送信元 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
  書き換え対象とする送信元 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 アドレスを書き換え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>

書き換え対象とする送信元ポート番号を指定します。

- ポート番号
  書き換え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書き換え対象とする場合に指定します。

<dst_addr>/<prefixlen>
書き換え対象とする宛先 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
  書き換え対象とする宛先 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 アドレスを書き換え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>
書き換え対象とする宛先ポート番号を指定します。

- ポート番号
  書き換え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書き換え対象とする場合に指定します。

<protocol>
書き換え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
  書き換え対象とするプロトコル番号を、0〜254 の 10 進数値で指定します。
- any
  すべてのプロトコルを書き換え対象とします。

<trafficclass>

- Traffic Class 値
  書き換え対象となる Traffic Class フィールドの値を 0-ff までの 16 進数値、または、"-"を使用して表現される 16 進数値の範囲を指定します。
  Traffic Class 値の指定は、"," を区切として 10 個まで設定可能です。
  複数の Traffic Class 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。
  Traffic Class 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 Traffic Class 値)
  - Traffic Class 値-Traffic Class 値 (例: 32-64 = 32 から 64 までの Traffic Class 値)
  - Traffic Class 値- (例: 80- = 80 から ff までの Traffic Class 値)
  - -Traffic Class 値 (例: -7f = 0 から 7f までの Traffic Class 値)
  - Traffic Class 値,Traffic Class 値,… (例: 10,20,30- = 10 と 20 と 30 以降の Traffic Class 値)
- any
  すべての Traffic Class 値を書き換え対象とします。

<new_trafficclass>

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

[説明]

Traffic Class 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 Traffic Class 値を、指定した Traffic Class 値に書き換えます。
Traffic Class 値書き換え定義は、本装置全体で次の数まで定義できます。

最大定義数	機種
100	MR1000

[未設定時]

Traffic Class 値書き換えを行わないものとみなされます。

4.5.23 remote ip6 trafficclass move

[機能]

Traffic Class 値書き換え条件の優先度の変更

[入力形式]

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

[パラメタ]

<number>

- remote 定義番号
  remote 定義の通し番号を、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 Traffic Class 値書き換え定義番号
  優先順序を変更する前の Traffic Class 値書き換え定義番号を指定します。

<new_count>

- 移動先 Traffic Class 値書き換え定義番号
  <count>に対する新しい順序を、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。

範囲	機種
0～99	MR1000

[説明]

Traffic Class 値書き換え条件の優先度を変更します。

4.5.24　remote ip6 priority

[機能]

IPv6 プロトコル帯域制御の設定

[入力形式]

remote [<number>] ip6 priority <count> <src_addr> / <prefixlen> <src_port> <dst_addr> / <prefixlen> <dst_port> <protocol> <trafficclass> <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、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、10 進数値で指定します。

範囲	機種
0〜99	MR1000

<src_addr>/<prefixlen>

帯域制御の対象とする送信元 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
  帯域制御の対象とする送信元 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 アドレスを帯域制御の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>

帯域制御の対象とす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>/<prefixlen>

帯域制御の対象とする宛先 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
  帯域制御の対象とする宛先 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 アドレスを帯域制御の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>

帯域制御の対象とす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>

帯域制御の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
  帯域制御の対象となるプロトコル番号を、0～254 の 10 進数値で指定します (例: ICMPv6:58、TCP:6、UDP:17 など)。
- any
  すべてのプロトコル番号をフィルタリング対象とする場合に指定します。

<trafficclass>

- 帯域制御対象 Traffic Class 値
  帯域制御の対象となる Traffic Class フィールドの値を 0-ff までの 16 進数値、または、"-"を使用して表現される 16 進数値の範囲を指定します。
  Traffic Class 値の指定は、"," を区切として 10 個まで設定可能です。
  複数の Traffic Class 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。
  Traffic Class 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 Traffic Class 値)
  - Traffic Class 値-Traffic Class 値 (例: 32-64 = 32 から 64 までの Traffic Class 値)
  - Traffic Class 値- (例: 80- = 80 から ff までの Traffic Class 値)
  - -Traffic Class 値 (例: -7f = 0 から 7f までの Traffic Class 値)
  - Traffic Class 値,Traffic Class 値,… (例: 10,20,30- = 10 と 20 と 30 以降の Traffic Class 値)
- any
  すべての Traffic Class 値を、帯域制御の対象とします。省略された場合は any として扱われます。

<width>

- express
  最優先データとして扱います。
- besteffort
  非優先 (ベストエフォート) として扱います。
- 帯域
  1〜99 の 10 進数値で指定した場合、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。
  「数字 + "kbps"(,"mbps")」で指定した場合、指定した帯域をそのまま割り当てます。1kbps〜100000kbps または、1mbps〜100mbps の範囲で指定します。全定義の帯域の合計が回線速度を超えた場合には、それぞれ指定した値の比で帯域を割り当てます。指定した値の合計値が回線速度に達しない場合、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。
  「"share" + 数字」で指定した場合、数字で指定した帯域制御定義番号で定義された帯域を共有します。この場合、指定する数字は自分自身の帯域制御定義番号より小さい、既に定義されてあるもの指定しなければなりません。

[説明]

IPv6 プロトコル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、トラフィッククラスを指定して、割り当てる帯域を指定します。
IPv6 プロトコル帯域制御は、本装置全体で次の数まで定義できます。

最大定義数	機種
100	MR1000

[注意]

IPv4,IPv6 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。
使用する回線が LAN の場合、シェーピングを使用しないと帯域制御機能は有効に動作しません。
使用する回線が ATM の場合、適切な VC 速度を設定しないと帯域制御機能は有効に動作しません。

[未設定時]

IPv6 プロトコル帯域制御を行わないものとみなされます。

4.5.25 remote ip6 dhcp service

[機能]

IPv6 DHCP 機能の設定

[入力形式]

remote [<number>] ip6 dhcp service <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、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 DHCP 機能のモードを指定します。

- off
  IPv6 DHCP 機能を使用しません。
- client
  IPv6 DHCP クライアント機能を使用します。
- server
  IPv6 DHCP サーバ機能を使用します。

[説明]

IPv6 DHCP 機能情報を設定します。

[未設定時]

IPv6 DHCP 機能を使用しないものとみなされます。

```
remote <number> ip6 dhcp service off
```

4.5.26　remote ip6 dhcp duid

[機能]

IPv6 DHCP の DUID 設定

[入力形式]

remote [<number>] ip6 dhcp duid <kind> [<duid>]

[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、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>

- auto
  DUID を自動生成する場合に指定します。
- hex
  16 進数で DUID を指定します。
- text
  文字列で DUID を指定します。

<duid>

- DUID
  0x21,0x23～0x7e の 130 文字以内の ASCII 文字列、または 260 桁以内の 16 進数で指定します。
  <kind>が auto の場合は、指定できません。

[説明]

IPv6 DHCP サーバ／クライアントの DUID を指定します。

例)

```
remote ip6 dhcp duid auto
remote ip6 dhcp duid hex 2105afffe66437d
remote ip6 dhcp duid text omron
```

auto の場合は、DUID-LL フォーマットにより DUID を自動生成します。

[未設定時]

DUID を自動生成するものとみなされます。

```
remote <number> ip6 dhcp duid auto
```

4.5.27 remote ip6 dhcp client option pd

[機能]

IPv6 DHCP クライアントのプレフィックス要求の設定

[入力形式]

remote [<number>] ip6 dhcp client option pd <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、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
  プレフィックスを要求します。
- off
  プレフィックスを要求しません。
- troan
  draft-troan-dhcpv6-opt-prefix-delegation-01 に準拠した方式でプレフィックスを要求します。

[説明]

IPv6 DHCP クライアント機能を使用する場合に、サーバにプレフィックスを要求するかどうかを設定します。

<mode>に on を設定した場合は、RFC3315、3633 に準拠したオプション番号を使用します。

<mode>に troan に設定した場合は、DNS サーバオプションのオプション番号に 25 番を使用し、PD オプションのオプション番号に 30 番を使用してプレフィックスの要求を行います。

[未設定時]

プレフィックスを要求するものとみなされます。

```
remote <number> ip6 dhcp client option pd on
```

4.5.28　remote ip6 dhcp client option dns

[機能]

IPv6 DHCP クライアントの DNS サーバアドレス要求の設定

[入力形式]

remote [<number>] ip6 dhcp client option dns <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、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
  DNS サーバアドレスを要求します。
- off
  DNS サーバアドレスを要求しません。

[説明]

IPv6 DHCP クライアント機能を使用する場合に、サーバに DNS サーバアドレスを要求するかどうかを設定します。

[未設定時]

DNS サーバアドレスを要求するものとみなされます。

```
remote <number> ip6 dhcp client option dns on
```

4.5.29 remote ip6 dhcp client iaid

[機能]

IPv6 DHCP クライアントの IAID 設定

[入力形式]

remote [<number>] ip6 dhcp client iaid <iaid>

[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、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。

<iaid>

- auto
  IAID を自動生成する場合に指定します。
- IAID を指定
  IAID を指定する場合の設定可能範囲は、1〜4294967295 です。

[説明]

IPv6 DHCP クライアントの IAID を指定します。auto を指定した場合は、インタフェース番号が IAID として使用されます。

[未設定時]

IAID を自動生成するものとみなされます。

```
remote <number> ip6 client iaid auto
```

4.5.30　remote ip6 dhcp client route

[機能]

IPv6 DHCP クライアントのリジェクト経路設定

[入力形式]

remote [<number>] ip6 dhcp client route <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、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>

- blackhole
  DHCP クライアントで取得したプレフィックスを、リジェクト経路として登録します。
  リジェクト経路宛の送信者に対して、応答しません。
- reject
  DHCP クライアントで取得したプレフィックスを、リジェクト経路として登録します。
  リジェクト経路宛の送信者に対して、ICMP の unreach でエラー報告を行います。

[説明]

IPv6 DHCP クライアントで取得したプレフィックスをリジェクト経路として登録します。
<mode>が reject の場合は、リジェクト経路宛の送信者に対して、ICMP の unreach でエラー報告を行います。blackhole の場合は、応答しません。

[未設定時]

blackhole を設定するものとみなされます。

```
remote <number> ip6 dhcp client route blackhole
```

4.5.31 remote ip6 dhcp server preference

[機能]

IPv6 DHCP サーバのプリファレンス値設定

[入力形式]

remote [<number>] ip6 dhcp server preference <preference>

[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、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。

<preference>

- プリファレンス値
  IPv6 DHCP サーバの優先度を、0～255 の 10 進数値で指定します。

[説明]

IPv6 DHCP サーバのプリファレンス値を指定します。
プリファレンス値は、Advertise メッセージの Preference オプションで使用され、255 が最優先の値になります。

[未設定時]

プリファレンス値 0 を設定するものとみなされます。

```
remote <number> ip6 dhcp server preference 0
```

4.5.32　remote ip6 dhcp server info dns

[機能]

IPv6 DHCP サーバの DNS サーバアドレス配布情報設定

[入力形式]

remote [<number>] ip6 dhcp server info dns <dns1> [<dns2>]

[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、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。

<dns1>

- DNS サーバ IPv6 アドレス
  IPv6 DHCP クライアントに配布する、DNS サーバの IPv6 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  ::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<dns2>

- セカンダリ DNS サーバ IPv6 アドレス
  IPv6 DHCP クライアントに配布する、セカンダリ DNS サーバの IPv6 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  ::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

[説明]

IPv6 DHCP サーバ機能を使用する場合に、配布する DNS サーバアドレス情報の設定をします。

[未設定時]

なし

4.5.33 remote ip6 dhcp server info prefix

[機能]

IPv6 DHCP サーバのプレフィックス配布情報設定

[入力形式]

remote [<number>] ip6 dhcp server info prefix <prefix>/<prefixlen> <valid> <preferred> <routeset>

[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、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。

<prefix>/<prefixlen>

配布するプレフィックス、プレフィックス長を指定します。

- プレフィックス
  配布するプレフィックスを指定します。
  指定可能な範囲は以下のとおりです。

  ::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

- プレフィックス長
  配布プレフィックス長として、48～64 の範囲の 10 進数値を指定します。

<valid>

- valid lifetime
  このインタフェースから配布する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配布する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
  このインタフェースから配布する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配布するプレフィックスに対する preferred lifetime を無限とします。

<routeset>

- on
  配布プレフィックスへの経路を自動登録します。
- off
  配布プレフィックスへの経路を自動登録しません。

[説明]

IPv6 DHCP サーバ機能を使用する場合に、プレフィックス配布情報を設定します。

プレフィックスを配布する場合は、配布プレフィックス、プレフィックス長、Preferred Lifetime、Valid Lifetime、経路登録を指定して登録します。

<routeset>を on にした場合は、プレフィックス配布と同時にクライアントへの経路を追加します。

[未設定時]

なし

4.6 ブリッジ関連情報

4.6.1 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、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
```

4.6.2　remote bridge group

[機能]

ブリッジグループ識別子の設定

[入力形式]

remote [<number>] bridge group <group_id>

[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、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。

<group_id>

- グループ識別子
  グループ識別子を 10 進数値で指定します。

範囲	機種
0〜19	MR1000

[説明]

ブリッジのグループ識別子を設定します。

[未設定時]

グループ識別子に 0 を指定したものとみなされます。

```
remote <number> bridge group 0
```

4.6.3 remote bridge static

[機能]

静的学習テーブル情報の設定

[入力形式]

remote [<number>] bridge static <count> <mac>

[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、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>

- 静的学習テーブル定義番号
  指定した定義番号と同じ値を持つ定義がすでに存在する場合は、既存の設定に対する修正をみなされます。

範囲	機種
0〜199	MR1000

<mac>

静的な定義として学習テーブルに追加する MAC アドレスを指定します。

[説明]

学習テーブルに指定された MAC アドレスを静的な学習テーブル情報として追加します。

4.6.4　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、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。

[注意]

ブリッジグループ 0 以外のブリッジグループでは STP は動作しません。

[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
```

4.6.5 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、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。
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。

- 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	備考
Ethernet(100Mbps)		100	
Ethernet(10Mbps)		100	
HSD(64kbps)		15620	*：192kbps～1.5Mbpsは PRIの場合
HSD(128kbps)		7810	
HSD(192kbps)	*	1000	
HSD(256kbps)	*	1000	
HSD(384kbps)	*	1000	
HSD(512kbps)	*	1000	
HSD(768kbps)	*	1000	
HSD(1Mbps)	*	667	
HSD(1.5Mbps)	*	667	
FR(64kbps)		16000	
FR(128kbps)		8500	
FR(256kbps)	*	1100	
FR(384kbps)	*	1100	
FR(512kbps)	*	1100	
FR(768kbps)	*	1100	
FR(1Mbps)	*	680	
FR(1.5Mbps)	*	680	
ISDN(64kbps)		16000	
その他			
1Mbps>=速度		1000	
1.5Mbps>=速度>1Mbps		667	
4Mbps>=速度>1.5Mbps		250	
6Mbps>=速度>4Mbps		167	
10Mbps>=速度>6Mbps		100	
16Mbps>=速度>10Mbps		62	
20Mbps>=速度>16Mbps		50	
25Mbps>=速度>20Mbps		40	
40Mbps>=速度>25Mbps		25	
80Mbps>=速度>40Mbps		12	
速度>80Mbps		10	

- 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。

[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
```

4.6.6 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、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、定義番号のもっと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
```

4.6.7　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> [<vlan_analyze>]]

[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、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、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すでに存在する場合は、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。

範囲	機種
0〜255	MR1000

<action>

フィルタリング対象に該当するフレームを透過するかどうかを指定します。

- pass
  該当するフレームを透過します。
- reject
  該当するフレームを遮断します。
- restrict
  該当するフレームを、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あて先 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 形式フレーム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 形式フレーム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
  すべてのフレームを対象とする場合に指定します。<value>は、指定不要です。

<vlan_analyze>

VLAN タグ付きフレームに対してタグの解析を行うかどうかを指定します。<value>を指定したときだけ指定可能です。
省略した場合は、off を指定したものとみなされます。

- on
  VLAN タグ付きフレームの場合に VLAN タグを解析してフィルタリング処理を行います。VLAN タグ付きフレームの場合には、タグの長さ分ずれた位置にある LLC 形式
  フレームの LSAP や Ethernet 形式フレームのタイプに対してフィルタリング処理を行います。
- off
  VLAN タグ付きフレームの場合に VLAN タグを解析しないでフィルタリング処理を行います。VLAN タグ付きフレームの場合でもタグの長さ分ずらさすにそのままフィルタリング処理を行うため、VLAN タグの TPID が、<value>との比較対象になります。

[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フレームを、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、本装置全体で以下の数まで定義できます。

最大定義数	機種
256	MR1000

[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、すべてのフレームが透過します。

4.6.8 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、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、10 進数値で指定します。
  すで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。

範囲	機種
0～255	MR1000

[説明]

MAC フィルタの優先順序を変更します。

4.7　MPLS 関連情報

4.7.1　remote mpls use

[機能]

MPLS 機能の設定

[入力形式]

remote [<number>] mpls 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、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
  MPLS を利用します。
- off
  MPLS を利用しません。

[説明]

MPLS を利用するかどうかを設定します。

[未設定時]

off が選択されたものとして動作します。

```
remote <number> mpls use off
```

4.7.2 remote mpls distribution

[機能]

ラベル配布プロトコルの設定

[入力形式]

remote [<number>] mpls distribution <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、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>

- ldp
  ラベル配布プロトコルに LDP を使用します。

[説明]

ラベル配布プロトコルを指定します。

[未設定時]

ldp が選択されたものとして動作します。

```
remote <number> mpls distribution ldp
```

4.7.3　remote mpls ldp hello-timers

[機能]

LDP Hello に関するタイマの設定

[入力形式]

remote [<number>] mpls ldp hello-timers <interval> <holdtime>

[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、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。

<interval>

- Hello 送信間隔のタイマ値
  Hello の送信間隔を、1 秒～65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。

<holdtime>

- HoldTime のタイマ値
  近隣関係の維持を判定するための HoldTime を、1 秒～65534 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
- infinity
  近隣関係の維持を判定するための HoldTime を infinity(0xffff:無限) とします。

[説明]

LDP 近隣関係の維持に用いられる Hello パケットの送信間隔と HoldTime を設定します。
HoldTime の値は interval の値より小さくすることはできません。
HoldTime の値は interval の値の 3 倍以上を設定することを推奨します。

[注意]

HoldTime は近隣関係にある LDP ルータとネゴシエーションし、値の小さい方が採用されますが、送信間隔はネゴシエーションしないため、相手 LSR のタイマ設定と自装置のタイマ設定を一致させておくことを推奨します。

[未設定時]

interval が 5 秒、HoldTime が 15 秒として動作します。

```
remote <number> mpls ldp hello-timers 5s 15s
```

4.7.4 remote mpls ldp keepalive-timers

[機能]

LDP KeepAlive に関するタイマの設定

[入力形式]

remote [<number>] mpls ldp keepalive-timers <interval> <timeout>

[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、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。

<interval>

- KeepAlive 送信間隔のタイマ値
  KeepAlive の送信間隔を、1 秒～65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。

<timeout>

- KeepAlive タイムアウトのタイマ値
  LDP セッションの維持を判定するためのタイムアウト時間を、1 秒～65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。

[説明]

LDP セッションの維持に用いられる KeepAlive メッセージの送信間隔とタイムアウトを設定します。
timeout の値は interval の値より小さくすることはできません。
timeout の値は interval の値の 3 倍以上を設定することを推奨します。

[注意]

タイムアウトは近隣関係にある LDP ルータとネゴシエーションし、値の小さい方が採用されますが、送信間隔はタイムアウトのネゴシエーション結果の 3 分の 1 の値とこのコマンドで設定された送信間隔とを比較し、値が小さい方が送信間隔として採用されます。

[未設定時]

interval が 1 分、timeout が 3 分として動作します。

```
remote <number> mpls ldp keepalive-timers 1m 3m
```

4.7.5　remote mpls ldp advertisement

[機能]

LDP ラベル広報方式の設定

[入力形式]

remote [<number>] mpls ldp advertisement <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、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>

- dod
  Downstream On Demand を使用します。
- du
  Downstream Unsolicited を使用します。

[説明]

LDP のラベル広報方式を指定します。

[未設定時]

du が選択されたものとして動作します。

```
remote <number> mpls ldp advertisement du
```

4.7.6 remote mpls ldp retention

[機能]

LDP ラベル保持方式の設定

[入力形式]

remote [<number>] mpls ldp retention <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、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>

- liberal
  Liberal Label Retention Mode を使用します。
- conservative
  Conservative Label Retention Mode を使用します。

[説明]

LDP のラベル保持方式を指定します。

[未設定時]

liberal が選択されたものとして動作します。

```
remote <number> mpls ldp retention liberal
```

4.7.7　remote mpls ldp interface-label

[機能]

PHP の無効化

[入力形式]

remote [<number>] mpls ldp interface-label <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、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
  インタフェースの IP アドレスにラベルを割り当てません。
- on
  インタフェースの IP アドレスにラベルを割り当てます。

[説明]

インタフェースの IP アドレスに対してラベルを割り当てるかどうかを指定します。
割り当てた場合は，インタフェース宛の LSP の PHP を無効にすることができます。

[注意]

MPLS トンネル接続機能を使用する場合、自側エンドポイントと IP アドレスが同一の時、本設定に依らず、PHP 機能は無効となります。

[未設定時]

off が選択されたものとして動作します。

```
remote <number> mpls ldp interface-label off
```

4.7.8 remote mpls ldp ip transport

[機能]

IPv4 Transport Address の設定

[入力形式]

remote [<number>] mpls ldp ip transport <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、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>

- LDP セッションの送信元 IPv4 アドレス
  IPv4 アドレスを指定します。以下の範囲で指定してください。

  0.0.0.0
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

[説明]

インタフェース単位で LDP が相手装置との通信に用いる送信元 IPv4 アドレスを分ける必要がある場合に、本装置に設定された IPv4 アドレスを指定します。
0.0.0.0 を指定した場合は、MPLS 情報の設定の IPv4 Transport Address の設定に従います。

[未設定時]

MPLS 情報の設定の IPv4 Transport Address の設定に従います。

```
remote mpls ldp ip transport 0.0.0.0
```

[注意]

インタフェース単位で IPv4 Transport Address を設定する場合には、必ず本装置に存在するアドレスを指定してください。本装置に存在しないアドレスをインタフェースに指定した場合は、そのインタフェースでは LDP を使用できません。

4.7.9　remote mpls ldp multicast-hello

[機能]

Multicast Hello の設定

[入力形式]

remote [<number>] mpls ldp multicast-hello <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、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
  LDP Multicast Hello パケットを送信しません。
- on
  LDP Multicast Hello パケットを送信します。

[説明]

LDP Multicast Hello を送出するかしないかを設定します。off に設定すると、Multicast Hello を送出しません。

本設定は、MPLS LSP トンネルを使用する REMOTE インタフェースの設定において、トンネルエンドポイントに指定した装置が EoMPLS 通信の相手装置となる場合に off に設定します。

[未設定時]

on が設定されているものとみなされます。

```
remote mpls ldp multicast-hello on
```

[注意]

MPLS LSP トンネルを使用する REMOTE インタフェースのトンネルエンドポイントに指定した装置が EoMPLS 通信の相手装置となる場合には、本設定を必ず off に設定してください。

off に指定しない場合は、VC ラベルを交換できない通常の LDP セッションが確立してしまうため、EoMPLS 通信で用いる VC LSP ができず、EoMPLS 通信を行う事ができません。

それ以外の場合では必ず on に設定してください。off に設定した場合は LDP の隣接関係が構築できず、LDP のセッションが確立できなくなります。

第 5 章　着信デフォルト情報の設定

5.1　発信者番号 (CLID) で相手が判別できないときの着信動作情報

5.1.1　answer accept

[機能]

発信者番号非通知または発信者番号非登録相手からの着信動作の設定

[入力形式]

answer accept <mode>

[パラメタ]

<mode>

- enable
  着信を受け付けます。
- disable
  着信を受け付けません。

[説明]

発信者番号 (CLID) が通知されない着信、または “4.2.23 remote ap called number” で設定したいずれの番号とも一致しない着信について、着信を許可するかどうかを設定します。

[未設定時]

着信を受け付けないものとみなされます。

```
answer accept disable
```

5.1.2 answer ppp auth type

[機能]

着信認証方式の設定

[入力形式]

answer ppp auth type <authtype>

[パラメタ]

<authtype>

着信時の認証について指定します。

- off
  着信時の認証を行いません。
- pap
  着信時の認証プロトコルに PAP を使用します。
- chap_md5
  着信時の認証プロトコルに MD5-CHAP を使用します。
- any
  着信時の認証プロトコルに MD5-CHAP または PAP を使用します。

[説明]

着信時の認証方式を設定します。

[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。

```
answer ppp auth type any
```

5.1.3　answer ppp auth receive add

[機能]

受諾認証情報の設定

[入力形式]

answer ppp auth receive add <id> <password> [encrypted]

[パラメタ]

<id>

- 受諾認証 ID
  受諾認証 ID を、0x21,0x23～0x7e のコードで構成される 64 文字以内の ASCII 文字列で指定します。

<password>

- 受諾認証パスワード
  受諾認証パスワードを、0x21,0x23～0x7e のコードで構成される 64 文字以内の文字列で指定します。
- 暗号化された受諾認証パスワード
  show コマンドで表示される暗号化された受諾認証パスワードを 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>

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

[説明]

相手情報の設定に受諾認証情報の設定がない場合に利用される受諾認証情報を設定します。この情報は、発信者番号 (CLID) で相手が判別できた場合に利用されます。

[注意]

発信者番号 (CLID) で相手が判別できなかった場合には、この情報は利用されません。
show コマンドでは、暗号化された受諾認証パスワードが encrypted と共に表示されます。

[未設定時]

受諾認証 ID は定義されません。

5.1.4 answer ppp mp use

[機能]

着信時の MP 利用可否の設定

[入力形式]

answer ppp mp use <mode>

[パラメタ]

<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]

発信者番号 (CLID) で相手が判別できない着信について、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。

```
answer ppp mp use off
```

5.1.5　answer ppp mp bap use

[機能]

着信時の BAP/BACP 利用可否の設定

[入力形式]

answer ppp mp bap use <mode>

[パラメタ]

<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]

発信者番号 (CLID) で相手が判別できない着信について、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。

```
answer ppp mp bap use off
```

第 6 章　テンプレート情報の設定

- テンプレート定義番号の指定範囲
  本章のコマンドの [パラメタ] に記載されている<number>(テンプレート定義番号) に指定する通し番号 (10 進数値) は、機種ごとに以下に示す範囲で指定してください。

範囲	機種
0	MR1000

6.1　テンプレート共通情報

6.1.1　template name

[機能]

テンプレート名称の設定

[入力形式]

template [<number>] name <template_name>

[パラメタ]

<number>

- テンプレート定義番号

  テンプレート定義の通し番号を、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。

<template_name>

- テンプレート名

  テンプレート名を、0x21,0x23～0x7e の 8 文字以内の ASCII 文字列で指定します。ただし、all は切断コマンドで使う予約語であるため、使用しないでください。

  テンプレート名に all を指定したテンプレートのみを切断することができなくなります。

[説明]

テンプレート名を設定します。

[注意]

既に同一名称のテンプレートが登録されている場合は、異常終了します。

[未設定時]

テンプレート名を設定しないものとみなされます。

6.1.2 template mtu

[機能]

送信パケット最大長 (MTU 値) の設定

[入力形式]

template [<number>] mtu <mtu>

[パラメタ]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、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]

テンプレート着信で使用する rmt インタフェース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、rmt インタフェース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。

```
template <number> mtu 1500
```

6.1.3　template idle

[機能]

無通信監視タイマの設定

[入力形式]

template [<number>] idle <time> [<direction>]

[パラメタ]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、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。

<direction>

- 省略
  送信パケット、および受信パケットを通信監視の対象とします。
- send
  送信パケットのみを通信監視の対象とします。受信パケットは監視対象とはなりません。
- receive
  受信パケットのみを通信監視の対象とします。送信パケットは監視対象とはなりません。

[説明]

指定した接続先と接続したときの無通信監視時間を設定します。
<time>で設定された間、監視対象となるパケットがない場合に、無通信として回線を切断します。

[未設定時]

無通信監視を行わないものとみなされます。

```
template [<number>] idle 0d
```

6.1.4 template interface pool

[機能]

テンプレート着信で使用する rmt インタフェースの設定

[入力形式]

template [<number>] interface pool <start> <num>

[パラメタ]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、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。

<start>

- 開始 rmt インタフェース番号
  テンプレート着信で使用する開始 rmt インタフェース番号を 10 進数値で指定します。

範囲	機種
0〜99	MR1000

<num>

- インタフェース数
  テンプレート着信で使用する rmt インタフェース数を、10 進数値で指定します。

最大インタフェース数	機種
2	MR1000

[説明]

テンプレート着信で使用する rmt インタフェースを設定します。

[注意]

テンプレート着信用に予約した rmt インタフェース番号に該当する remote 定義番号には一切設定をしないでください。
定義が存在する場合には、該当する remote 定義を削除してから予約をおこなってください。
予約した範囲に該当する remote 定義が存在した場合には、テンプレート着信は無効になります。

[未設定時]

テンプレート着信で使用する rmt インタフェースが存在しないとみなされます。(テンプレート着信は機能しません。)

6.1.5　template aaa

[機能]

参照する AAA 情報の設定

[入力形式]

template [<number>] aaa <group_id>

[パラメタ]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、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。

<group_id>

- unuse
  AAA 情報を使用しません。
- AAA のグループ ID
  AAA のグループ ID を、10 進数値で指定します。

範囲	機種
0	MR1000

[説明]

テンプレート着信で認証および着信を行なう場合に参照する AAA のグループ ID を指定します。

[未設定時]

AAA 情報を参照しないものとみなされます。

6.1.6 template datalink bind

[機能]

テンプレート着信で使用する回線の設定

[入力形式]

template [<number>] datalink bind <kind> [<conf_number>]

[パラメタ]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、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。
- any
  ISDN を使用するように設定した、すべての wan 定義を指定したものとみなされます。

<conf_number>

wan 定義の定義番号を指定します。

- wan 定義の定義番号
  利用する wan 定義の定義番号を、10 進数値で指定します。

範囲	機種
0	MR1000

[説明]

テンプレート着信で使用する回線を設定します。

[未設定時]

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

```
template <number> datalink bind wan 0
```

6.2　PPP 関連情報

6.2.1　template ppp auth type

[機能]

認証方法の設定

[入力形式]

template [<number>] ppp auth type <authtype>

[パラメタ]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、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。

- 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]

着信時の認証方式を設定します。

[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。

```
template <number> ppp auth type any
```

6.2.2 template ppp compress

[機能]

データ圧縮機能の設定

[入力形式]

template [<number>] ppp compress <mode>

[パラメタ]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、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。

[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。

```
template <number> ppp compress off
```

6.2.3　template ppp ipcp vjcomp

[機能]

VJ-Compression の利用の有無の設定

[入力形式]

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

[パラメタ]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、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。

[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。

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

6.2.4 template ppp ipcp iphc

[機能]

IPv4 における IP ヘッダ圧縮 (IPHC) の設定

[入力形式]

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

[パラメタ]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、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。

[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。

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

6.2.5　template ppp ipv6cp iphc

[機能]

IPv6 における IP ヘッダ圧縮 (IPHC) の設定

[入力形式]

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

[パラメタ]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、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。

[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。

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

6.3 IPv4 関連情報

6.3.1 template ip dns

[機能]

DNS サーバアドレスの設定

[入力形式]

template [<number>] ip dns <dns>

[パラメタ]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、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。

<dns>

- DNS サーバアドレス
  接続先と接続するときに利用する DNS サーバのアドレスを指定します。
  ここで設定したアドレスを、相手装置に通知します。

  0.0.0.0 アドレスを相手装置に通知しません。

  上記以外 設定したアドレスを、相手装置に通知します。
  設定可能な範囲は以下のとおりです。
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

[説明]

指定した接続先と接続するときに利用する DNS サーバアドレスを設定します。
本コマンドによる設定情報は、以下の場合に利用されます。

- 通信相手への DNS サーバアドレス通知
  接続先から IPCP 機能を用いて DNS サーバアドレス通知要求を受けた場合に、<dns>で設定した IP アドレスを通知します。本コマンドによる設定がない場合は通知しません。

[未設定時]

DNS サーバアドレスがないものとみなされます。

```
template <number> ip dns 0.0.0.0
```

6.3.2　template ip address remote-pool

[機能]

相手に割り当てる IP アドレス範囲の設定

[入力形式]

template [<number>] ip address remote-pool <start> <num>

[パラメタ]

<start>

- 割り当て先頭アドレス
  割り当てる IP アドレスの先頭アドレスを指定します。
  指定可能な範囲は以下のとおりです。
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

<num>

- 割り当てアドレス数

最大アドレス数	機種
50	MR1000

[説明]

着信相手に対して、割り当てる IP アドレスの範囲を指定します。

[未設定時]

割り当てる IP アドレス範囲を設定しないものとみなされます。

6.3.3 template ip filter

[機能]

IP フィルタの設定

[入力形式]

template [<number>] ip filter <count> <action> <src_addr> / <mask> <src_port> <dst_addr> / <mask> <dst_port> <protocol> <tcpconnect> [<tos> [<direction> [<icmptype> [<icmpcode>]]]]

[パラメタ]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、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、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。

範囲	機種
0〜199	MR1000

<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。

<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、1〜255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。
- any
  すべてのプロトコル番号をフィルタリング対象とする場合に指定します。

<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。

<direction>

フィルタリングする方向を指定します。
省略した場合は、any を指定したものとみなされます。

- any
  入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。
- in
  入力パケットのみをフィルタリング対象とする場合に指定します。
- out
  出力パケットのみをフィルタリング対象とする場合に指定します。
- reverse
  入力パケットと出力パケットの両方をフィルタリング対象とします。
  ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。
  - 送信元 IP アドレス/マスクと宛先 IP アドレス/マスク
  - 送信元ポート番号と宛先ポート番号

<icmptype>

フィルタリング対象とする ICMP TYPE を指定します。

- ICMP TYPE
  フィルタリング対象とする送信元 ICMP TYPE を、0～255 の 10 進数値で指定します。
  複数の ICMP TYPE 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、「8-30」のように"-"(ハイフン) を使用して指定します。
  ICMP TYPE 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。
  - 0～255 の 10 進数値 (例: 8 = ICMP TYPE 8)
  - ICMP TYPE-ICMP TYPE (例: 2-8 = 2 から 8 までの ICMP TYPE)
  - ICMP TYPE- (例: 8- = 8 から 255 までの ICMP TYPE)

- -ICMP TYPE (例: -200 = 0 から 200 までの ICMP TYPE)
- ICMP TYPE,ICMP TYPE,… (例: 0,8,30- = 0 と 8 と 30 以降の ICMP TYPE)

- any
  すべての ICMP TYPE をフィルタリング対象とする場合に指定します。

<icmpcode>

フィルタリング対象とする ICMP CODE を指定します。

- ICMP CODE
  フィルタリング対象とする送信元 ICMP CODE を、0～255 の 10 進数値で指定します。複数の ICMP CODE 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、「8-30」のように"-"(ハイフン) を使用して指定します。
  ICMP CODE 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。
  - 0～255 の 10 進数値 (例: 8 = ICMP CODE 8)
  - ICMP CODE-ICMP CODE (例: 2-8 = 2 から 8 までの ICMP CODE)
  - ICMP CODE- (例: 8- = 8 から 255 までの ICMP CODE)
  - -ICMP CODE (例: -200 = 0 から 200 までの ICMP CODE)
  - ICMP CODE,ICMP CODE,… (例: 0,8,30- = 0 と 8 と 30 以降の ICMP CODE)

- any
  すべての ICMP CODE 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 ICMP TYPE, ICMP CODE 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 フィルタリング定義は、本装置全体で次の数まで定義できます。

最大定義数	機種
200	MR1000

[注意]

<direction>に reverse を指定した場合には、入力パケットは IP アドレス/マスクとポート番号のみを逆転した条件でフィルタリングされます。このため、<tcpconnect>を有効にしている場合には、入力パケットに対しても、TCP プロトコルのコネクション接続要求がフィルタリング対象に含まれます。

定義数の計算は「テンプレート情報で設定した定義数 x テンプレートで使用する rmt インタフェース数」で計算されますので、それを含めて装置最大定義数の範囲に収まるように定義してください。

装置最大定義数を越えた場合は資源不足により、該当機能が動作しない場合があります。

[未設定時]

IP フィルタを設定しないものとみなされます。

6.3.4 template ip filter move

[機能]

IP フィルタの優先順序の変更

[入力形式]

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

[パラメタ]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、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、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。

範囲	機種
0～199	MR1000

[説明]

IP フィルタの優先順序を変更します。

6.3.5　template ip filter default

[機能]

いずれの IP フィルタテーブルにも不一致時の動作の設定

[入力形式]

template [<number>] ip filter default <action> [<time>]

[パラメタ]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、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。

<action>

いずれの IP フィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

- 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。
- spi
  該当するパケットに対して SPI を動作させます。

<time>

- 割当時間
  action に spi を指定したときに、接続に割り当てられた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]

いずれの IP フィルタテーブルに一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

いずれの IP フィルタテーブルにも一致しないパケットは透過します。

```
template <number> ip filter default pass
```

6.3.6 template ip tos

[機能]

TOS 値書き換え条件の設定

[入力形式]

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

[パラメタ]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、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、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。

範囲	機種
0〜99	MR1000

<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>

TOS 値書き換え対象となるプロトコル番号を指定します。

- 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、1〜255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。
- any
  すべてのプロトコル番号を TOS 値書き換え対象とする場合に指定します。

<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 値書き換え定義は、本装置全体で次の数まで定義できます。

最大定義数	機種
100	MR1000

[注意]

定義数の計算は「テンプレート情報で設定した定義数 x テンプレートで使用する rmt インタフェース数」で計算されますので、それを含めて装置最大定義数の範囲に収まるように定義してください。
装置最大定義数を越えた場合は資源不足により、該当機能が動作しない場合があります。

[未設定時]

TOS 値書き換えを行わないものとみなされます。

6.3.7　template ip tos move

[機能]

TOS 値書き換え条件の優先度の変更

[入力形式]

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

[パラメタ]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、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、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。

範囲	機種
0～99	MR1000

[説明]

TOS 値書き換え条件の優先度を変更します。

6.3.8 template ip priority

[機能]

帯域制御の設定

[入力形式]

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

[パラメタ]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、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、10 進数値で指定します。

範囲	機種
0〜99	MR1000

<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>

帯域制御の対象となるプロトコル番号を指定します。

- 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、1～255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。
- any
  すべてのプロトコル番号を帯域制御の対象とする場合に指定します。

<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>

- express
  最優先データとして扱います。
- besteffort
  非優先 (ベストエフォート) として扱います。
- 帯域
  1〜99 の 10 進数値で指定した場合、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。
  「数字 + "kbps"(,"mbps")」で指定した場合、指定した帯域をそのまま割り当てます。1kbps〜100000kbps または、1mbps〜100mbps の範囲で指定します。全定義の帯域の合計が回線速度を超えた場合には、それぞれ指定した値の比で帯域を割り当てます。指定した値の合計値が回線速度に達しない場合、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。
  「"share" + 数字」で指定した場合、数字で指定した帯域制御定義番号で定義された帯域を共有します。この場合、指定する数字は自分自身の帯域制御定義番号より小さい、既に定義されてあるもの指定しなければなりません。

[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、本装置全体で次の数まで定義できます。

最大定義数	機種
100	MR1000

[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。
ISDN、専用線、フレームリレー以外の回線上で帯域制御機能を使用する場合には、シェーピングを使用しないと帯域制御は有効に動作しません。
定義数の計算は「テンプレート情報で設定した定義数 x テンプレートで使用する rmt インタフェース数」で計算されますので、それを含めて装置最大定義数の範囲に収まるように定義してください。
装置最大定義数を越えた場合は資源不足により、該当機能が動作しない場合があります。

[未設定時]

帯域制御を行わないものとみなされます。

6.3.9　template ip msschange

[機能]

MSS 書き換えの設定

[入力形式]

template [<number>] ip msschange <mss>

[パラメタ]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、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。

```
template <number> ip msschange 0
```

6.4 IPv6 関連情報

6.4.1 template ip6 use

[機能]

IPv6 機能の設定

[入力形式]

template [<number>] ip6 use <mode>

[パラメタ]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、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
  テンプレート着信で使用する rmt インタフェースで、IPv6 パケットの送受信を行います。
- off
  テンプレート着信で使用する rmt 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]

テンプレート着信で使用する rmt 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。

```
template <number> ip6 use off
```

6.4.2　template ip6 ifid

[機能]

IPv6 インタフェース ID の設定

[入力形式]

template [<number>] ip6 ifid <interfaceID>

[パラメタ]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、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>

テンプレート着信で使用する rmt 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
  rmt 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]

テンプレート着信で使用する rmt 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。

```
template <number> ip6 ifid auto
```

6.4.3 template ip6 filter

[機能]

IPv6 フィルタの設定

[入力形式]

template [<number>] ip6 filter <count> <action> <src_addr>/<prefixlen> <src_port> <dst_addr>/<prefixlen> <dst_port> <protocol> <tcpconnect> [<trafficclass> [<direction> [<icmptype> [<icmpcode>]]]]

[パラメタ]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、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、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。

範囲	機種
0〜199	MR1000

<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。

<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、0〜254 の 10 進数値で指定します。
- any
  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。

<trafficclass>

- フィルタリング対象 Traffic Class 値

  フィルタリング対象となる Traffic Class フィールドの値を 0-ff までの 16 進数値、または、"-"を使用して表現される 16 進数値の範囲を指定します。

  Traffic Class 値の指定は、"," を区切として 10 個まで設定可能です。

  複数の Traffic Class 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。

  Traffic Class 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 Traffic Class 値)
  - Traffic Class 値-Traffic Class 値 (例: 32-64 = 32 から 64 までの Traffic Class 値)
  - Traffic Class 値- (例: 80- = 80 から ff までの Traffic Class 値)
  - -Traffic Class 値 (例: -7f = 0 から 7f までの Traffic Class 値)
  - Traffic Class 値,Traffic Class 値,… (例: 10,20,30- = 10 と 20 と 30 以降の Traffic Class 値)

- any

  全ての Traffic Class 値をフィルタリング対象とします。省略された場合は any として扱われます。

<direction>

フィルタリングする方向を指定します。
省略した場合は、any を指定したものとみなされます。

- any

  入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。

- in

  入力パケットのみをフィルタリング対象とする場合に指定します。

- out

  出力パケットのみをフィルタリング対象とする場合に指定します。

- reverse

  入力パケットと出力パケットの両方をフィルタリング対象とします。

  ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。

  - 送信元 IP アドレス/プレフィックス長と宛先 IP アドレス/プレフィックス長
  - 送信元ポート番号と宛先ポート番号

<icmptype>

フィルタリングする ICMPv6 メッセージタイプ番号を指定します。

- フィルタリング対象 icmptype 値

  フィルタリング対象となる icmptype フィールドの値を 0-255 までの 10 進数値、または、"-"を使用して表現される 10 進数値の範囲を指定します。

  icmptype 値の指定は、"," を区切として 10 個まで設定可能です。

  記述形式は、<src_port>と同様です。

- any

  全ての icmptype 値をフィルタリング対象とします。省略された場合は any として扱われます。

<icmpcode>

フィルタリングする ICMPv6 メッセージコード番号を指定します。
icmpcode 指定時は、icmptype も指定する必要があります。

- フィルタリング対象 icmpcode 値
  フィルタリング対象となる icmpcode フィールドの値を 0-255 までの 10 進数値、または、"-"を使用して表現される 10 進数値の範囲を指定します。
  icmptype 値の指定は、"," を区切として 10 個まで設定可能です。
  記述形式は、<src_port>と同様です。
- any
  全ての icmpcode 値をフィルタリング対象とします。省略された場合は any として扱われます。

[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。
  - any 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 any 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。
- <icmptype>、<icmpcode>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 any を指定し、かつ<icmptype>、<icmpcode>を指定している場合、　ICMPv6 パケットの該当 type/code 番号を持つパケットのみが合致します。

- <protocol>に ICMPv6(58) を指定し、かつ<icmptype>、<icmpcode>を指定している場　合、指定プロトコルの該当 type/code 番号を持つパケットのみが合致します。
- <protocol>に ICMPv6(58) 以外を指定し、かつ<icmptype>、<icmpcode>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 フィルタリング定義は、本装置全体で次の数まで定義できます。

最大定義数	機種
200	MR1000

[注意]

定義数の計算は「テンプレート情報で設定した定義数 x テンプレートで使用する rmt インタフェース数」で計算されますので、それを含めて装置最大定義数の範囲に収まるように定義してください。
装置最大定義数を越えた場合は資源不足により、該当機能が動作しない場合があります。

[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。

6.4.4　template ip6 filter move

[機能]

IPv6 フィルタの優先順序の変更

[入力形式]

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

[パラメタ]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、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、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。

範囲	機種
0～199	MR1000

[説明]

IPv6 フィルタの優先順序を変更します。

6.4.5 template ip6 filter default

[機能]

いずれの IP フィルタテーブルにも不一致時の動作の設定

[入力形式]

template [<number>] ip6 filter default <action> [<time>]

[パラメタ]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、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。

<action>

いずれの IPv6 フィルタテーブルにも一致しなかったパケットをどう扱うかを指定します。

- 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。
- spi
  該当するパケットに対して SPI を動作させます。

<time>

- 割当時間
  action に spi を指定したときに接続に割り当てられた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]

いずれの IPv6 フィルタテーブルにも一致しなかったときにパケットをどう扱うかを設定します。

[未設定時]

いずれの IPv6 フィルタテーブルにも一致しないパケットは透過します。

```
template <number> ip6 filter default pass
```

6.4.6　template ip6 trafficclass

[機能]

トラフィッククラス値書き換え条件の設定

[入力形式]

template [<number>] ip6 trafficclass <count> <src_addr>/<prefixlen> <src_port> <dst_addr>/<prefixlen> <dst_port> <protocol> <trafficclass> <new_trafficclass>

[パラメタ]

<number>

- テンプレート定義番号

  テンプレート定義の通し番号を、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>

- Traffic Class 値書き換え定義番号

  Traffic Class 値書き換え条件の優先度を表す定義番号を、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 Traffic Class 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。

範囲	機種
0〜99	MR1000

<src_addr>/<prefixlen>

書き換え対象とする送信元 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

  書き換え対象とする送信元 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 アドレスを書き換え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>

書き換え対象とする送信元ポート番号を指定します。

- ポート番号

  書き換え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書き換え対象とする場合に指定します。

<dst_addr>/<prefixlen>

書き換え対象とする宛先 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
  書き換え対象とする宛先 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 アドレスを書き換え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>

書き換え対象とする宛先ポート番号を指定します。

- ポート番号
  書き換え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書き換え対象とする場合に指定します。

<protocol>

書き換え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
  書き換え対象とするプロトコル番号を、0〜254 の 10 進数値で指定します。
- any
  すべてのプロトコルを書き換え対象とします。

<trafficclass>

- Traffic Class 値
  書き換え対象となる Traffic Class フィールドの値を 0-ff までの 16 進数値、または、"-"を使用して表現される 16 進数値の範囲を指定します。
  Traffic Class 値の指定は、"," を区切として 10 個まで設定可能です。
  複数の Traffic Class 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。
  Traffic Class 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 Traffic Class 値)
  - Traffic Class 値-Traffic Class 値 (例: 32-64 = 32 から 64 までの Traffic Class 値)
  - Traffic Class 値- (例: 80- = 80 から ff までの Traffic Class 値)
  - -Traffic Class 値 (例: -7f = 0 から 7f までの Traffic Class 値)
  - Traffic Class 値,Traffic Class 値,… (例: 10,20,30- = 10 と 20 と 30 以降の Traffic Class 値)

- any
  すべての Traffic Class 値を書き換え対象とします。

<new_trafficclass>

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

[説明]

Traffic Class 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 Traffic Class 値を、指定した Traffic Class 値に書き換えます。
Traffic Class 値書き換え定義は、本装置全体で次の数まで定義できます。

最大定義数	機種
100	MR1000

[注意]

定義数の計算は「テンプレート情報で設定した定義数 x テンプレートで使用する rmt インタフェース数」で計算されますので、それを含めて装置最大定義数の範囲に収まるように定義してください。
装置最大定義数を越えた場合は資源不足により、該当機能が動作しない場合があります。

[未設定時]

Traffic Class 値書き換えを行わないものとみなされます。

6.4.7 template ip6 trafficclass move

[機能]

Traffic Class 値書き換え条件の優先度の変更

[入力形式]

template [<number>] ip6 trafficclass move <count> <new_count>

[パラメタ]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、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 Traffic Class 値書き換え定義番号
  優先順序を変更する前の Traffic Class 値書き換え定義番号を指定します。

<new_count>

- 移動先 Traffic Class 値書き換え定義番号
  <count>に対する新しい順序を、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。

範囲	機種
0～99	MR1000

[説明]

Traffic Class 値書き換え条件の優先度を変更します。

6.4.8　template ip6 priority

[機能]

IPv6 プロトコル帯域制御の設定

[入力形式]

template [<number>] ip6 priority <count> <src_addr> / <prefixlen> <src_port> <dst_addr> / <prefixlen> <dst_port> <protocol> <trafficclass> <width>

[パラメタ]

<number>

- テンプレート定義番号
  テンプレート定義の通し番号を、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、10 進数値で指定します。

範囲	機種
0〜99	MR1000

<src_addr>/<prefixlen>

帯域制御の対象とする送信元 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
  帯域制御の対象とする送信元 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 アドレスを帯域制御の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>

帯域制御の対象とす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>/<prefixlen>

帯域制御の対象とする宛先 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
  帯域制御の対象とする宛先 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 アドレスを帯域制御の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>

帯域制御の対象とす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>

帯域制御の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
  帯域制御の対象となるプロトコル番号を、0～254 の 10 進数値で指定します (例: TCP:6、UDP:17、ICMPv6:58 など)。
- any
  すべてのプロトコル番号をフィルタリング対象とする場合に指定します。

<trafficclass>

- 帯域制御対象 Traffic Class 値
  帯域制御の対象となる Traffic Class フィールドの値を 0-ff までの 16 進数値、または、"-"を使用して表現される 16 進数値の範囲を指定します。
  Traffic Class 値の指定は、"," を区切として 10 個まで設定可能です。
  複数の Traffic Class 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。
  Traffic Class 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 Traffic Class 値)
  - Traffic Class 値-Traffic Class 値 (例: 32-64 = 32 から 64 までの Traffic Class 値)
  - Traffic Class 値- (例: 80- = 80 から ff までの Traffic Class 値)
  - -Traffic Class 値 (例: -7f = 0 から 7f までの Traffic Class 値)
  - Traffic Class 値,Traffic Class 値,… (例: 10,20,30- = 10 と 20 と 30 以降の Traffic Class 値)
- any
  すべての Traffic Class 値を、帯域制御の対象とします。省略された場合は any として扱われます。

<width>

- express
  最優先データとして扱います。
- besteffort
  非優先 (ベストエフォート) として扱います。
- 帯域
  1～99 の 10 進数値で指定した場合、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。
  「数字 + "kbps"(,"mbps")」で指定した場合、指定した帯域をそのまま割り当てます。1kbps～100000kbps または、1mbps～100mbps の範囲で指定します。全定義の帯域の合計が回線速度を超えた場合には、それぞれ指定した値の比で帯域を割り当てます。
  指定した値の合計値が回線速度に達しない場合、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。
  「"share" + 数字」で指定した場合、数字で指定した帯域制御定義番号で定義された帯域を共有します。この場合、指定する数字は自分自身の帯域制御定義番号より小さい、既に定義されてあるもの指定しなければなりません。

[説明]

IPv6 プロトコル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、トラフィッククラスを指定して、割り当てる帯域を指定します。
IPv6 プロトコル帯域制御は、本装置全体で次の数まで定義できます。

最大定義数	機種
100	MR1000

[注意]

IPv4,IPv6 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。
ISDN、専用線、フレームリレー以外の回線上で帯域制御機能を使用する場合には、シェーピングを使用しないと帯域制御は有効に動作しません。
定義数の計算は「テンプレート情報で設定した定義数 x テンプレートで使用する rmt インタフェース数」で計算されますので、それを含めて装置最大定義数の範囲に収まるように定義してください。
装置最大定義数を越えた場合は資源不足により、該当機能が動作しない場合があります。

[未設定時]

IPv6 プロトコル帯域制御を行わないものとみなされます。

第 7 章　ルーティングプロトコル情報の設定

7.1　ルーティングマネージャ情報

7.1.1　routemanage ip distance

[機能]

IPv4 ルーティングプロトコル優先度の設定

[入力形式]

routemanage ip distance rip <rip_distance>
routemanage ip distance bgp <external_distance> [<internal_distance>]
routemanage ip distance ospf <ospf_distance>
routemanage ip distance dns <dns_distance>

[パラメタ]

<rip_distance>

- RIP 優先度
  RIP の優先度を、1～254 の 10 進数値で指定します。

<external_distance>

- EBGP 優先度
  EBGP の優先度を、1～254 の 10 進数値で指定します。

<internal_distance>

- IBGP 優先度
  IBGP の優先度を、1～254 の 10 進数値で指定します。
  省略した場合は 200 が指定されたものとみなされます。

<ospf_distance>

- OSPF 優先度
  OSPF の優先度を、1～254 の 10 進数値で指定します。

<dns_distance>

- DNS 優先度
  DNS の優先度を、1～254 の 10 進数値で指定します。

[説明]

IPv4 ルーティングプロトコルの優先度を設定します。
優先度は、同じあて先への経路情報が複数ある場合、優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。

[未設定時]

RIP の優先度を 120、EBGP の優先度を 20、IBGP の優先度を 200、OSPF の優先度を 110、DNS の優先度を 15 として優先経路選択を行うものとみなされます。

```
routemanage ip distance rip 120
routemanage ip distance bgp 20 200
routemanage ip distance ospf 110
routemanage ip distance dns 15
```

7.1.2 routemanage ip redist rip

[機能]

RIP 再配布経路の設定

[入力形式]

routemanage ip redist rip <redist_info> <mode> [<metric>]

[パラメタ]

<redist_info>

経路種別を指定します。

- static
  スタティック経路情報を示します。
- connected
  インタフェース経路情報を示します。
- bgp
  BGP 経路情報を示します。
- ospf
  OSPF 経路情報を示します。
- dns
  DNS 経路情報を示します。

<mode>

RIP に再配布するかどうかを指定します。

- off
  再配布しません。
- on
  再配布します。

<metric>

- RIP に再配布するメトリック値
  RIP に再配布する際のメトリック値を、0～16 の 10 進数値で指定します。
  BGP、OSPF、または DNS で受信した経路情報を RIP に再配布する場合に指定できます。
  RIP 広報メトリック値は、以下の計算値で決定されます。
  - RIP 広報値=インタフェースの加算メトリック値+1+<metric>

[説明]

RIP に再配布する経路情報を設定します。

[注意]

RIP を使用しているインタフェースの経路は、インタフェース経路情報の再配布設定にかかわらず再配布されます。

[未設定時]

スタティック経路情報とインタフェース経路情報だけを RIP に再配布するものとみなされます。

```
routemanage ip redist rip static on
routemanage ip redist rip connected on
routemanage ip redist rip bgp off 0
routemanage ip redist rip ospf off 0
routemanage ip redist rip dns off 0
```

7.1.3 routemanage ip redist bgp

[機能]

BGP 再配布経路の設定

[入力形式]

routemanage ip redist bgp <redist_info> <mode>
routemanage ip redist bgp vrf [<vrf_number>] <redist_info> <mode>

[パラメタ]

<redist_info>

経路種別を指定します。

- static
  スタティック経路情報を示します。
- connected
  インタフェース経路情報を示します。
- rip
  RIP 経路情報を示します。
  routemanage ip redist bgp vrf では指定できません。
- ospf
  OSPF 経路情報を示します。
  routemanage ip redist bgp vrf では指定できません。
- dns
  DNS 経路情報を示します。
  routemanage ip redist bgp vrf では指定できません。

<vrf_number>

- VRF 定義番号
  VRF の定義番号を、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。

範囲	機種
0〜1	MR1000

<mode>

BGP に再配布するかどうかを指定します。

- off
  再配布しません。
- on
  再配布します。

[説明]

BGP に再配布する経路情報を設定します。

[未設定時]

すべての経路種別を BGP に再配布しないものとみなされます。

```
routemanage ip redist bgp static off
routemanage ip redist bgp connected off
routemanage ip redist bgp rip off
routemanage ip redist bgp ospf off
routemanage ip redist bgp dns off
```

7.1.4 routemanage ip redist ospf

[機能]

OSPF 再配布経路の設定

[入力形式]

routemanage ip redist ospf <redist_info> <mode> [<metric> [<metric_type>]]

[パラメタ]

<redist_info>

経路種別を指定します。

- static
  スタティック経路情報を示します。
- connected
  インタフェース経路情報を示します。
- rip
  RIP 経路情報を示します。
- bgp
  BGP 経路情報を示します。
- dns
  DNS 経路情報を示します。

<mode>

OSPF に再配布するかどうかを指定します。

- off
  再配布しません。
- on
  再配布します。

<metric>

- メトリック値
  OSPF に再配布する際のメトリック値を、0～16777214 の 10 進数で指定します。
  省略した場合は、20 を指定したものとみなされます。

<metric_type>

外部経路のメトリックタイプを指定します。
省略した場合は、type2 を指定したものとみなされます。

- type1
  メトリックタイプを type1 とします。
- type2
  メトリックタイプを type2 とします。

[説明]

OSPF に再配布する経路情報を設定します。

[未設定時]

すべての経路種別を OSPF に再配布しないものとみなされます。

```
routemanage ip redist ospf static off 20 type2
routemanage ip redist ospf connected off 20 type2
routemanage ip redist ospf rip off 20 type2
routemanage ip redist ospf bgp off 20 type2
routemanage ip redist ospf dns off 20 type2
```

7.1.5 routemanage ip ecmp mode

[機能]

IPv4 ルーティングにおける ECMP の設定

[入力形式]

routemanage ip ecmp mode <mode>

[パラメタ]

<mode>

- off
  ECMP を使用しません。
- roundrobin
  ECMP を使用し、送出パス選択方式としてラウンドロビン方式を利用します。
- hash
  ECMP を使用し、送出パス選択方式としてハッシュ方式を使用します。

[説明]

IPv4 ルーティング機能における ECMP の使用の有無を設定します。なお、ECMP を使用する場合、以下の 2 種類の送出パス選択方式を選択します。

・ラウンドロビン方式

パケットごとに送出パスを順次切替える方式です。すべてのトラフィックがほぼ均等に分散される利点がある一方、通信の連続性 (個々の通信セッションが同じパスを利用するか) とパケットの到達順は送信時から保証されないという欠点があります。

・ハッシュ方式

送信元 IP アドレス、あて先 IP アドレスを元にハッシュ値を計算し、その値にしたがって送出パスを決定する方式です。通信の連続性および到達順はほぼ保証されますが、トラフィックが一部の通信パスにかたよる可能性があります。

[未設定時]

ECMP を利用しないものとみなされます。

```
routemanage ip ecmp mode off
```

7.1.6　routemanage ip ecmp ospf

[機能]

OSPF ルーティングプロトコルにおける最大 ECMP 数の設定

[入力形式]

routemanage ip ecmp ospf <max-multipath>

[パラメタ]

<max-multipath>

- 最大 ECMP 数
  最大 ECMP 数を、1～4 までの 10 進数値で指定します。
  1 を指定した場合、OSPF では ECMP 経路を扱いません。

[説明]

OSPF が生成した経路情報において、設定可能な ECMP 数を指定します。

[未設定時]

<max-multipath>に 1 を設定するものとみなされます。

```
routemanage ip ecmp ospf 1
```

7.1.7 routemanage ip redist ldp

[機能]

LDP ラベル広報経路情報の設定

[入力形式]

routemanage ip redist ldp <redist_info> <mode>

[パラメタ]

<redist_info>

- static
  本装置に設定されているスタティックルーティングの経路情報を示します。
- connected
  インタフェースが接続されているネットワークの経路情報を示します。
- rip
  RIP で受信した経路情報を示します。
- ospf
  OSPF で受信した経路情報を示します。
- bgp
  BGP で受信した経路情報を示します。

<mode>

- off
  <redist_info>で指定した経路情報をラベル広報しません。
- on
  <redist_info>で指定した経路情報をラベル広報します。

[説明]

LDP でラベル広報する経路情報の種別を選択します。

[未設定時]

以下の設定とみなされます。

- LDP で static を広報された経路をラベル広報しない
- LDP で connected の経路をラベル広報する
- LDP で rip で広報された経路をラベル広報する
- LDP で ospf で広報された経路をラベル広報する
- LDP で bgp で広報された経路をラベル広報しない

```
routemanage ip redist ldp static off
routemanage ip redist ldp connected on
routemanage ip redist ldp rip on
routemanage ip redist ldp ospf on
routemanage ip redist ldp bgp off
```

7.1.8　routemanage interface floating

[機能]

インタフェース経路のフローティング設定

[入力形式]

routemanage interface floating <mode>

[パラメタ]

<mode>

- off
  フローティング機能を使用しません。
- on
  フローティング機能を使用します。

[説明]

インタフェース経路のフローティング機能を設定します。<mode>が on の場合、インタフェースが通信可能（リンクアップなど）状態ならば、インタフェース経路をルーティングテーブルに追加します。通信不可能（リンクダウンなど）状態ならば、インタフェース経路をルーティングテーブルから削除します。
<mode>が off の場合、インタフェースの通信状態に関係なく、インタフェース経路をルーティングテーブルに追加します。
本設定は、IPv4 機能、IPv6 機能で共通となります。

[注意]

ルーティングプロトコル優先度<distance>が 0 のスタティックルーティングも、<mode>が on の場合、インタフェースの状態変動によって、ルーティングテーブルへの追加・削除を制御します。
<mode>が on の場合、インタフェースが利用不可能な状態の場合にはインタフェース経路がルーティングテーブルから削除されるとともに、インタフェースに設定された IP アドレスが通信に利用できなくなります。常に利用可能な IP アドレスが必要な場合には、loopback インタフェースに追加 IP アドレスを設定してください。
なお、以下のコマンドでは自装置の IP アドレスを指定します。これらのコマンドで常に利用可能な IP アドレスが必要な場合には、loopback インタフェースの追加 IP アドレスを使用してください。

- snmp agent address
- remote ap sessionwatch
- remote ap tunnel local

<mode>が on で自 IP アドレスを指定していない remote インタフェースから送信される場合、送信元 IP アドレスは以下の順番で選ばれます。
1.loopback インタフェース追加アドレス
2. 利用可能な lan の IP アドレス（定義番号の小さいものが優先）
3. 利用可能な remote の IP アドレス（定義番号の小さいものが優先）
常に同じアドレスが選択されるようにするためには、loopback インタフェースに追加 IP アドレスを設定してください。この設定がない場合、インタフェースの状態によって送信元 IP アドレスが変化する場合があります。
<mode>が on でマルチキャストで自装置が RP として動作している場合、RP として動作しているインタフェースの状態の変化により以下の動作になります。

- RP を自動選択にしている場合

  RP として動作しているインタフェースがダウンした場合、利用可能なインタフェースを自動検索し更新します。この場合、ネットワーク上にて RP が更新されるため、その RP を利用している通信は RP が更新されるまで一定時間停止します。また、インタフェース回線がふたたびアップすることで、RP が切り戻るため、やはりその RP を利用している通信は切り戻るまでの一定時間停止します。

  利用可能なインタフェースが検索できなかった場合には、RP としての動作を停止しますが、インタフェースがふたたびアップすることで復旧します。

- RP を手動選択にしている場合

  選択されているインタフェースがダウンした場合、RP としての動作を停止します。この場合、ネットワーク上にて RP が更新されるため、その RP を利用している通信が RP が更新されるまで一定時間停止します。

  また、インタフェースがふたたびアップすることで、RP は切り戻りますが、やはりその RP を利用している通信が切り戻るまでの一定時間停止します。

<mode>が on でマルチキャストで自装置が BSR として動作している場合、BSR として動作しているインタフェースの状態の変化により以下の動作になります。

- BSR を自動選択にしている場合

  RP として動作しているインタフェースがダウンした場合、利用可能なインタフェースを自動検索し更新します。この場合、ネットワーク上にて BSR が更新されるため、その BSR を利用している通信は BSR が更新されるまでの一定時間停止します。また、インタフェースがふたたび UP することで，BSR が切り戻るため、やはりその BSR を利用している通信は BSR が切り戻るまでの一定時間停止します。

  なお検索できなかった場合には、BSR としての動作を停止しますが、インタフェース回線がふたたびアップすることで復旧します。

- BSR を手動選択にしている場合

  選択されているインタフェースがダウンした場合には、BSR としての動作を停止します。この場合、ネットワーク上にて BSR が更新されるため，その BSR を利用している通信は BSR が更新されるまでの一定時間停止します.

  また、インタフェースがふたたびアップすることで BSR は切り戻りますが、やはりその BSR を利用している通信は切り戻るまでの一定時間停止します。

[未設定時]

インタフェースの通信状態に関係なく、常にインタフェース経路をルーティングテーブルに追加するものとみなされます。

```
routemanage interface floating off
```

7.1.9　routemanage ip6 distance

[機能]

IPv6 ルーティングプロトコル優先度の設定

[入力形式]

routemanage ip6 distance rip <rip_distance>
routemanage ip6 distance dns <dns_distance>
routemanage ip6 distance dhcp <dhcp_distance>

[パラメタ]

<rip_distance>

- RIP 優先度

  RIP の優先度を、1～254 の 10 進数値で指定します。

<dns_distance>

- DNS 優先度

  DNS の優先度を、1～254 の 10 進数値で指定します。

<dhcp_distance>

- DHCP 優先度

  DHCP の優先度を、1～254 の 10 進数値で指定します。

[説明]

IPv6 ルーティングプロトコルの優先度を設定します。優先度は、同じあて先への経路情報が複数ある場合、優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。
DHCP 経路情報の blackhole 経路、reject 経路の優先度は、DHCP 優先度の値となります。

[未設定時]

RIP の優先度を 120、DNS の優先度を 15、DHCP の優先度を 10 として優先経路選択を行うものとみなされます。

```
routemanage ip6 distance rip 120
        routemanage ip6 distance dns 15
        routemanage ip6 distance dhcp 10
```

7.1.10 routemanage ip6 redist rip

[機能]

IPv6 RIP 再配布経路の設定

[入力形式]

routemanage ip6 redist rip <redist_info> <mode> [<metric>]

[パラメタ]

<redist_info>

経路種別を指定します。

- static
  スタティック経路情報を示します。
- connected
  インタフェース経路情報を示します。
- dns
  DNS 経路情報を示します。
- dhcp
  DHCP 経路情報を示します。

<mode>

RIP に再配布するかどうかを指定します。

- off
  再配布しません。
- on
  再配布します。

<metric>

- RIP に再配布するメトリック値
  RIP に再配布する際のメトリック値を、0～16 の 10 進数値で指定します。
  DNS、または DHCP で受信した経路情報を RIP に再配布する場合に指定できます。
  RIP 広報メトリック値は、以下の計算値で決定されます。
  - RIP 広報値=インタフェースの加算メトリック値+1+<metric>

[説明]

RIP に再配布する経路情報を設定します。
DHCP 経路情報を再配布すると設定しても、DHCP 経路情報の blackhole 経路、reject 経路は、再配布できません。

[注意]

RIP を使用しているインタフェースの経路は、インタフェース経路情報の再配布設定にかかわらず再配布されます。

[未設定時]

スタティック経路情報とインタフェース経路情報を RIP に再配布するものとみなされます。

```
routemanage ip6 redist rip static on
routemanage ip6 redist rip connected on
routemanage ip6 redist rip dns off 0
routemanage ip6 redist rip dhcp off 0
```

7.2 RIP 情報

7.2.1 rip ip timers basic

[機能]

RIP タイマの設定

[入力形式]

rip ip timers basic <update> <timeout> <garbage>

[パラメタ]

<update>

- 定期広報タイマ値
  定期広報タイマ値を、10 秒～3600 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、10s～3600s、1m～60m、1h です。

<timeout>

- 有効期限タイマ値
  有効期限タイマ値を、10 秒～3600 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、10s～3600s、1m～60m、1h です。

<garbage>

- ガーベージタイマ値
  ガーベージタイマ値を、10 秒～3600 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、10s～3600s、1m～60m、1h です。

[説明]

RIP の基準となる定期広報タイマ値、有効期限タイマ値、ガーベージタイマ値を指定します。

<update>は、定期広報の送信間隔を設定します。なお、次に定期広報を行うまでの時間は、送信間隔に送信間隔の最大± 50%のゆらぎ幅の範囲で乱数により求められる値を加算した値が使用されます。ゆらぎ幅は、rip ip timers jitter コマンドで変更することができます。<timeout>は、隣接ルータから一定時間通知がない場合、その隣接ルータから受信していた経路を無効とするまでの時間を設定します。<garbage>では、無効となった経路情報を削除するまでの時間を設定します。無効となった経路は削除されるまでの間、定期広報でメトリック 16 として広報されます。

[未設定時]

定期広報タイマ値に 30 秒、有効期限タイマ値に 3 分、ガーベージタイマ値に 2 分が設定されているものとみなされます。

```
rip ip timers basic 30s 3m 2m
```

7.2.2　rip ip timers jitter

[機能]

RIP 定期広報ゆらぎ幅の設定

[入力形式]

rip ip timers jitter <jitter>

[パラメタ]

<jitter>

- ゆらぎ幅
  ゆらぎ幅 (%) を、0～50 の 10 進数値で指定します。

[説明]

RIP 定期広報のゆらぎ幅を設定します。次に定期広報を行うまでの時間は、定期広報の送信間隔にゆらぎ時間を加算した値が使用されます。ゆらぎ幅は、定期広報の送信間隔に対するゆらぎ時間の割合の±の最大値を設定します。ゆらぎ時間は、ゆらぎ幅の範囲で乱数により求められます。<jitter>に 0 が設定された場合、ゆらぎ時間は 0 秒となります。

[注意]

ゆらぎ幅に 0 が設定されている場合、隣接ルータとの間で RIP パケットの衝突が繰り返し発生し、RIP ルーティングは収束遅延する可能性があります。

[未設定時]

RIP 定期広報のゆらぎ幅に、50(%) が設定されているものとみなされます。

```
rip ip timers jitter 50
```

7.2.3 rip ip multipath

[機能]

RIP マルチパスの設定

[入力形式]

rip ip multipath <path_num>

[パラメタ]

<path_num>

- 同一パス数

  同一パス数を、1～2 までの 10 進数値で指定します。

[説明]

RIP テーブルに、同一パスの追加を有効とするかどうかを設定します。

<path_num>に 2 を指定した場合、同一パスの追加は有効となり、受信した RIP 経路や再配布経路が、RIP テーブルに追加可能となります。

同一パスの追加を有効とした場合、経路情報が無効状態となった時点で次の経路情報を瞬時に追加し、経路切替りの待ち時間を削減することができます。

同一パスを保持した場合、定期広報対象となる経路情報は、メトリックの小さい経路情報とします。

ただし、再配布経路と RIP 経路が混在した場合は、ルーティングプロトコル優先度の高い経路情報とします。

RIP 経路の同一パスをルーティングテーブルに追加する場合、メトリックの小さい経路を使用します。

同一メトリックの場合は、先に受信した RIP 経路を使用します。ただし、再配布経路と RIP 経路が混在した場合は、ルーティングプロトコル優先度の高い経路情報とします。

<path_num>に 1 を指定した場合、同一パスの追加はできません。

[注意]

<path_num>を超えた同一パスを RIP で受信した場合、追加済の RIP 経路情報とメトリックの比較を行い、メトリックの大きい RIP 経路情報は破棄されます。

[未設定時]

RIP テーブルに同一パスは、追加できないものとみなされます。

```
rip ip multipath 1
```

7.2.4　rip ip redist

[機能]

RIP 再配布フィルタの設定

[入力形式]

rip ip redist <number> <action> <address> / <mask> [<prefix_match>]

[パラメタ]

<number>

- 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定義番号を、0～49 の 10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

<action>

フィルタリング条件に一致した場合の動作を指定します。

- pass
  該当する経路情報を透過します。
- reject
  該当する経路情報を遮断します。

<address>/<mask>

フィルタリング対象とする経路情報を指定します。

- IPv4 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経路情報を、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)
- any
  すべての経路情報をフィルタリング対象とする場合に指定します。
- default
  デフォルトルート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。

<prefix_match>

経路情報 (IPv4 アドレス / マスク) の検索条件を指定します。
省略した場合は、exact を指定したものとみなされます。
<address> / <mask>に"any"または"default"を指定した場合は、<prefix_match>は指定できません。

- exact
  指定した<address> / <mask>と経路情報の IPv4 アドレス / マスクを比較し、一致した場合に、フィルタリング対象とします。
- inexact
  指定した<address>と経路情報の IPv4 アドレスを比較し、<mask>まで一致した場合、フィルタリング対象とします。

[説明]

RIP に再配布する経路情報に対するフィルタリング条件と動作を設定します。

IPv4 経路情報 (インタフェース経路、スタティック経路、BGP 経路、OSPF 経路）を RIP に再配布する場合、フィルタリング条件に一致した情報を再配布するかどうかを設定します。フィルタリング条件は優先順位で検索され、条件に一致した場合にフィルタリングの動作が行われ、それ以降の条件は参照されません。

すべてのフィルタリング条件に一致しない経路情報は RIP に再配布されません。

<number>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号が既に存在する場合は、既存の定義が上書きされます。

RIP 再配布フィルタは、本装置全体で 50 個まで定義できます。

[未設定時]

RIP 再配布フィルタが設定されていないものとみなされます。

7.2.5　rip ip redist move

[機能]

RIP 再配布フィルタの優先順序の変更

[入力形式]

rip ip redist move <number> <new_number>

[パラメタ]

<number>

- 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番号を指定します。

<new_number>

- 移動先フィルタリング定義番号
  <number>に対する新しい順序を、0～49 の 10 進数値で指定します。
  すで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]

RIP 再配布フィルタの優先順序を変更します。
<new_number>で、既存定義番号を指定した場合、その定義の前に挿入されます。また、
<new_number>は順番にソートされてリナンバリングされます。

7.2.6 rip ip neighbor

[機能]

RIP ユニキャスト送信の設定

[入力形式]

rip ip neighbor [<count>] <neighbor_address> <version>

[パラメタ]

<count>

- ユニキャスト送信相手の定義番号
  ユニキャスト送信相手の定義番号を、0〜29 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。

<neighbor_address>

RIP 経路をユニキャストで送信する相手ルータの IP アドレスを指定します。
指定可能な範囲は以下のとおりです。

1.0.0.1 〜 126.255.255.254
128.0.0.1 〜 191.255.255.254
192.0.0.1 〜 223.255.255.254

<version>

送信バージョンを指定します。

- v1
  RIPv1 で送信します。
- v2
  RIPv2 で送信します。

[説明]

特定の相手ルータに対して、RIP 経路をユニキャストで広報する場合に設定します。
<neighbor_address>には、LAN 側ネットワークに存在する RIP ルータを指定してください。
RIP 経路を広報する相手ルータは、本装置全体で 30 個まで定義できます。

[注意]

<neighbor_address>が属する LAN インタフェースで設定されている lan ip rip コマンドの<send>パラメタとは無関係に、ユニキャスト送信を行います。ただし、加算メトリックと認証機能については、lan ip rip で設定されている値を使用します。
自ネットワーク以外の相手ルータは指定できません。

[未設定時]

RIP ユニキャスト送信を設定しないものとみなします。

7.2.7　rip ip gwfilter

[機能]

RIP 相手フィルタの設定

[入力形式]

rip ip gwfilter <number> <action> <gateway_address>

[パラメタ]

<number>

- 相手フィルタリングの定義番号
  フィルタリングの優先度を表す定義番号を、0～29 の 10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

<action>

フィルタリング条件に一致した場合の動作を指定します。

- pass
  該当する相手ルータの RIP パケットを受信します。
- reject
  該当する相手ルータの RIP パケットを破棄します。

<gateway_address>

フィルタリング対象とする相手ルータ情報を指定します。

- IPv4 アドレス
  対象とする相手ルータの IPv4 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

- any
  すべての相手ルータを対象とする場合に指定します。

[説明]

特定の相手ルータから RIP 経路を受信する場合、フィルタリング条件に一致した相手ルータの RIP パケットを受信 (pass) させるか破棄 (reject) させるかを設定します。

フィルタリング条件は優先順位で検索し、条件に一致した相手ルータ情報があった時点でフィルタリングが行われ、それ以降の条件は参照されません。

すべてのフィルタリング条件に一致しない相手ルータ情報からの RIP パケットは破棄されます。

<number>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。

RIP 相手フィルタは、本装置全体で 30 個まで定義できます。

[未設定時]

RIP 相手フィルタを設定しないものとみなします。

7.2.8 rip ip gwfilter move

[機能]

RIP 相手フィルタの優先順序の変更

[入力形式]

rip ip gwfilter move <number> <new_number>

[パラメタ]

<number>

- 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番号を指定します。

<new_number>

- 移動先フィルタリング定義番号
  <number>に対する新しい順序を、0～29 の 10 進数値で指定します。
  すで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]

RIP 相手フィルタの優先順序を変更します。
<new_number>で、既存定義番号を指定した場合、その定義の前に挿入されます。また、
<new_number>は順番にソートされてリナンバリングされます。

7.2.9　rip ip6 timers basic

[機能]

IPv6 RIP タイマの設定

[入力形式]

rip ip6 timers basic <update> <timeout> <garbage>

[パラメタ]

<update>

- 定期広報タイマ値
  定期広報タイマ値を、10 秒～3600 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、10s～3600s、1m～60m、1h です。

<timeout>

- 有効期限タイマ値
  有効期限タイマ値を、10 秒～3600 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、10s～3600s、1m～60m、1h です。

<garbage>

- ガーベージタイマ値
  ガーベージタイマ値を、10 秒～3600 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、10s～3600s、1m～60m、1h です。

[説明]

RIP(IPv6) の基準となる定期広報タイマ値、有効期限タイマ値、ガーベージタイマ値を指定します。

<update>は、定期広報の送信間隔を設定します。なお、次に定期広報を行うまでの時間は、送信間隔に送信間隔の最大± 50%のゆらぎ幅の範囲で乱数により求められる値を加算した値が使用されます。

<timeout>は、隣接ルータから一定時間通知がない場合、その隣接ルータから受信していた経路を無効とするまでの時間を設定します。

<garbage>では、無効となった経路情報を削除するまでの時間を設定します。無効となった経路は削除されるまでの間、定期広報でメトリック 16 として広報されます。

[未設定時]

定期広報タイマ値に 30 秒、有効期限タイマ値に 3 分、ガーベージタイマ値に 2 分が設定されているものとみなされます。

```
rip ip6 timers basic 30s 3m 2m
```

7.2.10 rip ip6 multipath

[機能]

IPv6 RIP マルチパスの設定

[入力形式]

rip ip6 multipath <path_num>

[パラメタ]

<path_num>

- 同一パス数

  同一パス数を、1～2 までの 10 進数値で指定します。

[説明]

RIP テーブルに、同一パスの追加を有効とするかどうかを設定します。

<path_num>に 2 を指定した場合、同一パスの追加は有効となり、受信した RIP 経路や再配布経路が、RIP テーブルに追加可能となります。

同一パスの追加を有効とした場合、経路情報が無効状態となった時点で次の経路情報を瞬時に追加し、経路切替りの待ち時間を削減することができます。

同一パスを保持した場合、定期広報対象となる経路情報は、メトリックの小さい経路情報とします。ただし、再配布経路と RIP 経路が混在した場合は、ルーティングプロトコル優先度の高い経路情報とします。

RIP 経路の同一パスをルーティングテーブルに追加する場合、メトリックの小さい経路を使用します。

同一メトリックの場合は、先に受信した RIP 経路を使用します。ただし、再配布経路と RIP 経路が混在した場合は、ルーティングプロトコル優先度の高い経路情報とします。

<path_num>に 1 を指定した場合、同一パスの追加はできません。

[注意]

<path_num>を超えた同一パスを RIP で受信した場合、追加済の RIP 経路情報とメトリックの比較を行い、メトリックの大きい RIP 経路情報は破棄されます。

[未設定時]

RIP テーブルに同一パスは、追加できないものとみなされます。

```
rip ip6 multipath 1
```

7.2.11　rip ip6 redist

[機能]

IPv6 RIP 再配布フィルタの設定

[入力形式]

rip ip6 redist <number> <action> <address>/<prefixlen> [<prefix_match>]

[パラメタ]

<number>

- 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定義番号を、0～49 の 10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

<action>

フィルタリング条件に一致した場合の動作を指定します。

- pass
  該当する経路情報を透過します。
- reject
  該当する経路情報を遮断します。

<address>/<prefixlen>

フィルタリング対象とする経路情報を指定します。

- 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経路情報を、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。
- any
  すべての経路情報をフィルタリング対象とする場合に指定します。
- default
  デフォルトルート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。

<prefix_match>

経路情報 (IPv6 アドレス/プレフィックス長) の検索条件を指定します。省略した場合は、exact を指定したものとみなされます。<address>/<prefixlen>に"any"または"default"を指定した場合は、<prefix_match>は指定できません。

- exact
  指定した<address>/<mask>と経路情報の IPv6 アドレス/プレフィックス長を比較し、一致した場合に、フィルタリング対象とします。
- inexact
  指定した<address>と経路情報の IPv6 アドレスを比較し、<prefixlen>まで一致した場合、フィルタリング対象とします。

[説明]

RIP(IPv6) に再配布する経路情報に対するフィルタリング条件と動作を設定します。

IPv6 経路情報 (インタフェース経路、スタティック経路）を RIP(IPv6) に再配布する場合、フィルタリング条件に一致した情報を再配布するかどうかを設定します。

フィルタリング条件は優先順位で検索され、条件に一致した場合にフィルタリングの動作が行われ、それ以降の条件は参照されません。

すべてのフィルタリング条件に一致しない経路情報は RIP(IPv6) に再配布されません。

<number>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。

RIP(IPv6) 再配布フィルタは、本装置全体で 50 個まで定義できます。

[未設定時]

RIP(IPv6) 再配布フィルタが設定されていないものとみなされます。

7.2.12　rip ip6 redist move

[機能]

IPv6 RIP 再配布フィルタの優先順序の変更

[入力形式]

rip ip6 redist move <number> <new_number>

[パラメタ]

<number>

- 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番号を指定します。

<new_number>

- 移動先フィルタリング定義番号

  <number>に対する新しい順序を、0～49 の 10 進数値で指定します。すで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]

RIP(IPv6) 再配布フィルタの優先順序を変更します。<new_number>で、既存定義番号を指定した場合、その定義の前に挿入されます。また、<new_number>は順番にソートされてリナンバリングされます。

7.3 BGP 情報

7.3.1 bgp as

[機能]

BGP AS 番号の設定

[入力形式]

bgp as <as_number>

[パラメタ]

<as_number>

- 自装置の属する AS 番号
  自装置の属する AS 番号を、0～65535 の 10 進数値で指定します。
  0 を指定した場合、BGP の機能は動作しません。

[説明]

自装置の属する AS 番号を指定します。

[未設定時]

BGP を動作させないものとみなされます。

```
bgp as 0
```

7.3.2　bgp id

[機能]

BGP ID の設定

[入力形式]

bgp id <identifier>

[パラメタ]

<identifier>

- BGP の ID
  IPv4 アドレスを 0.0.0.0～255.255.255.255 のドット形式で指定します。

[説明]

BGP 接続において自装置を一意に示す ID を設定します。
ID は他のルータと重複しない値を指定し、一般的には自装置の IPv4 アドレスを使用します。
本コマンドを省略または 0.0.0.0 が設定されている場合は、以下のとおり ID を自動的に選択し使用します。

- loopback インタフェースに追加 IP アドレスが設定されている場合は、その IP アドレスを選択します。
- loopback インタフェースに追加 IP アドレスが設定されていない場合は、lan / remote インタフェースに設定されている IP アドレスの中からインタフェースの Up / Down の状態に関係なく最大のものを選択します。なお、remote インタフェースの相手側 IP アドレスおよび、lan インタフェースのセカンダリ IP アドレスは選択の対象となりません。

[未設定時]

自動的に選択された ID が使用されるものとみなされます。

```
bgp id 0.0.0.0
```

7.3.3 bgp vrf rd

[機能]

BGP / MPLS VPN ルート識別子の設定

[入力形式]

bgp vrf [<vrf_number>] rd <as_number> <id>

[パラメタ]

<vrf_number>

- VRF 定義番号
  VRF の定義番号を、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。

範囲	機種
0〜1	MR1000

<as_number>

- AS 番号
  AS 番号を、1〜65535 の 10 進数値で指定します。

<id>

- ID 番号
  VRF の ID を、0〜4294967295 の 10 進数値で指定します。

[説明]

BGP / MPLS VPN で使用するルート識別子を AS 番号と ID で設定します。
<as_number>は、自装置の属する AS 番号を設定します。
<id>は、VPN を一意に示す id を設定します。

[未設定時]

ルート識別子が設定されていないものとみなされます。

7.3.4　bgp mpls-resolution

[機能]

BGP MPLS 解決の設定

[入力形式]

bgp mpls-resolution <mode>

[パラメタ]

<mode>

MPLS 解決を行うかどうかを指定します。

- on
  MPLS 解決を行います。
- off
  MPLS 解決を行いません。

[説明]

BGP で受信した経路を MPLS で解決するかどうかを設定します。
<mode>が on の場合は、BGP で受信した経路を MPLS のラベルパスにマッピングします。off の場合は、マッピングしません。

[注意]

MPLS トンネル接続上で BGP を使用する場合は、本設定を off にしてください。

[未設定時]

MPLS 解決を行わないものとみなされます。

```
bgp mpls-resolution off
```

7.3.5 bgp network route

[機能]

BGP ネットワークの設定

[入力形式]

bgp network route [<count>] <address> / <mask>

[パラメタ]

<count>

- BGP ネットワークの定義番号
  BGP ネットワークの定義番号を、0〜15 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>

- BGP ネットワークアドレス / マスクビット数 (またはマスク値)
  BGP 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。
  - BGP ネットワークアドレス / マスクビット数 (例: 192.168.1.0 / 24)
  - BGP ネットワークアドレス / マスク値 (例: 192.168.1.0 / 255.255.255.0)

[説明]

BGP ネットワークを設定します。
本コマンドは、BGP テーブルにない経路情報を広報する場合に設定します。
bgp network igp コマンドで IGP 経路との同期が設定されている場合、設定された BGP ネットワークが IGP 経路として有効な場合に広報します。なお、IGP 経路の状態変更を認識するまで最大 15 秒かかります。
bgp network igp コマンドで IGP 経路との同期が設定されていない場合、IGP 経路が有効 / 無効のどちらの場合でも広報します。

[注意]

BGP / MPLS VPN で使用する IBGP では、本コマンドで設定した経路は広報されません。

[未設定時]

BGP ネットワークが設定されていないものとみなされます。

7.3.6　bgp network igp

[機能]

BGP ネットワークの IGP との同期設定

[入力形式]

bgp network igp <mode>

[パラメタ]

<mode>

IGP 経路と同期させるかどうかを指定します。

- on
  IGP 経路と同期させます。
- off
  IGP 経路と同期させません。

[説明]

BGP ネットワークを、IGP 経路と同期して広報するかどうかを設定します。
<mode>に on を設定した場合、IGP 経路が有効な場合にだけ広報し、無効な場合は広報しません。
<mode>に off を設定した場合、IGP 経路に関係なく広報します。

[未設定時]

BGP ネットワークを、IGP 経路と同期して広報するものとみなされます。

```
bgp network igp on
```

7.3.7 bgp aggregate

[機能]

BGP 集約経路の設定

[入力形式]

bgp aggregate [<count>] <address> / <mask> [<action>]

[パラメタ]

<count>

- BGP 集約経路の定義番号
  集約経路の定義番号を、0〜15 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>

- BGP 集約経路アドレス / マスクビット数 (またはマスク値)
  集約経路を 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。
  - BGP 集約経路アドレス / マスクビット数 (例: 192.168.1.0 / 24)
  - BGP 集約経路アドレス / マスク値 (例: 192.168.1.0 / 255.255.255.0)

  0.0.0.0 / 0, 0.0.0.0 / 0.0.0.0 は指定できません。

<action>

動作を指定します。

- summary-only
  BGP 集約経路だけを広報し、集約される個々の経路を広報しない場合に指定します。

[説明]

BGP 集約経路の設定を行います。
設定された集約経路に含まれる経路情報がある場合、集約経路情報を生成します。
<action>に summary-only が設定されていない場合は、集約経路と集約経路に含まれる個々の経路情報の両方が広報されます。summary-only が設定されている場合、集約経路に含まれる個々の経路情報はサプレス経路となり、集約経路だけを広報します。

[注意]

BGP / MPLS VPN で使用する IBGP では、本コマンドで経路を集約することはできません。

[未設定時]

BGP 集約経路が設定されていないものとみなされます。

7.3.8　bgp redist

[機能]

BGP 再配布フィルタの設定

[入力形式]

bgp redist <number> <action> <address> / <mask> [<prefix_match>]

[パラメタ]

<number>

- 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定義番号を、0～49 の 10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

<action>

フィルタリング条件に一致した場合の動作を指定します。

- pass
  該当する経路情報を透過します。
- reject
  該当する経路情報を遮断します。

<address>/<mask>

フィルタリング対象とする経路情報を指定します。

- IPv4 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経路情報を、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)
- any
  すべての経路情報をフィルタリング対象とする場合に指定します。
- default
  デフォルトルート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。

<prefix_match>

経路情報 (IPv4 アドレス / マスク) の検索条件を指定します。
省略した場合は、exact を指定したものとみなされます。
<address> / <mask>に"any"または"default"を指定した場合は、<prefix_match>は指定できません。

- exact
  指定した<address> / <mask>と経路情報の IPv4 アドレス / マスクを比較し、一致した場合に、フィルタリング対象とします。
- inexact
  指定した<address>と経路情報情報の IPv4 アドレスを比較し、<mask>まで一致した場合、フィルタリング対象とします。

[説明]

BGP に再配布する経路情報に対するフィルタリング条件と動作を設定します。

IPv4 経路情報 (インタフェース経路、スタティック経路、RIP 経路、OSPF 経路）を BGP に再配布する場合、フィルタリング条件に一致した情報を再配布するかどうかを設定します。フィルタリング条件は優先順位で検索され、条件に一致した場合にフィルタリングの動作が行われ、それ以降の条件は参照されません。

すべてのフィルタリング条件に一致しない経路情報は BGP に再配布されません。

<number>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。

BGP 再配布フィルタは、本装置全体で 50 個まで定義できます。

[未設定時]

BGP 再配布フィルタが設定されていないものとみなされます。

7.3.9　bgp redist move

[機能]

BGP 再配布フィルタの優先順序の変更

[入力形式]

bgp redist move <number> <new_number>

[パラメタ]

<number>

- 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番号を指定します。

<new_number>

- 移動先フィルタリング定義番号
  <number>に対する新しい順序を、0～49 の 10 進数値で指定します。
  すで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]

BGP 再配布フィルタの優先順序を変更します。
<new_number>で、既存定義番号を指定した場合、その定義の前に挿入されます。また、
<new_number>は順番にソートされてリナンバリングされます。

7.4 BGP 相手側情報

7.4.1 bgp neighbor address

[機能]

BGP 相手側 IP アドレスの設定

[入力形式]

bgp neighbor [<count>] address <address>

[パラメタ]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 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。

範囲	機種
0〜3	MR1000

<address>

- 相手装置の IPv4 アドレス
  指定可能な範囲は以下のとおりです。

  1.0.0.1 〜 126.255.255.254
  128.0.0.1 〜 191.255.255.254
  192.0.0.1 〜 223.255.255.254

[説明]

相手装置の定義番号および IPv4 アドレスを設定します。相手側情報の設定では、まず本コマンドを実行し、定義番号と IPv4 アドレスを設定しなければなりません。

[注意]

BGP / MPLS VPN 運用では、相手装置は 1 つだけ設定できます。

[未設定時]

相手側情報が設定されていないものとみなされます。

7.4.2　bgp neighbor as

[機能]

BGP 相手側 AS 番号の設定

[入力形式]

bgp neighbor [<count>] as <as_number>

[パラメタ]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 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。

範囲	機種
0～3	MR1000

<as_number>

- 相手側 AS 番号
  BGP 相手側 AS 番号を、1～65535 の 10 進数値で指定します。

[説明]

相手装置の属する AS 番号を設定します。
IP-VPN 接続を行う場合は、自装置の属する AS 番号とは異なる値を設定しなければなりません。
BGP / MPLS VPN を使用する場合は、本装置と同じ AS 番号を設定します。

[注意]

IP-VPN 接続と BGP / MPLS VPN 接続は同時に使用することはできません。

[未設定時]

相手装置の AS 番号が設定されていないものとみなされます。

7.4.3 bgp neighbor timers

[機能]

BGP 無通信監視タイマの設定

[入力形式]

bgp neighbor [<count>] timers <keepalive> <holdtime>

[パラメタ]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 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。

範囲	機種
0～3	MR1000

<keepalive>

- keepalive タイマ値
  keepalive タイマ値を、1 秒～65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、1s～65535s、1m～1092m、1h～18h です。

<holdtime>

- HoldTime のタイマ値 (秒)
  HoldTime のタイマ値を、3 秒～65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、3s～65535s、1m～1092m、1h～18h です。

[説明]

<keepalive>では、無通信状態において、相手装置との通信可否を確認するために送信する KEEPALIVE メッセージのタイマ値を設定します。相手装置の<holdtime>が自装置の<holdtime>よりも小さな値が設定されている場合、相手装置の<holdtime>の 3 分の 1 の値が使用されます。

<holdtime>では無通信状態で通信異常と判断する時間を設定します。本値は相手装置とネゴシエーションし、より小さな値をお互いの装置で使用します。

<keepalive>には<holdtime>よりも小さな値を指定してください。

<holdtime>と<keepalive>の設定値は、上位単位で表示可能な場合、上位単位で表示されます。

[未設定時]

<keepalive>に 30 秒、<holdtime>に 90 秒が設定されているものとみなされます。

```
bgp neighbor <count> timers 30s 90s
```

7.4.4　bgp neighbor medmetric

[機能]

BGP MED メトリックの設定

[入力形式]

bgp neighbor [<count>] medmetric <medmetric>

[パラメタ]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 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。

範囲	機種
0～3	MR1000

<medmetric>

- 相手装置に広報する MED メトリック値
  相手装置に広報する MED メトリック値を、0～4294967295 の 10 進数値で指定します。
  本パラメタ値は、小さい値がより高い優先度を示します。

[説明]

相手装置に EBGP で広報する MED メトリック値を指定します。<medmetric>に 0 以外を指定した場合、相手装置に広報する経路情報すべてに対して MED メトリック値を広報します。<medmetric>に 0 を指定した場合、MED メトリック値として 0 を広報します。

[注意]

BGP フィルタを設定している場合は、BGP フィルタでの MED メトリック値の設定が使用されます。

[未設定時]

MED メトリック値として 0 を広報するものとみなされます。

```
bgp neighbor <count> medmetric 0
```

7.4.5 bgp neighbor asprepend

[機能]

BGP AS パスプリペンド の設定

[入力形式]

bgp neighbor [<count>] asprepend <asprepend>

[パラメタ]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 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。

範囲	機種
0～3	MR1000

<asprepend>

- AS 番号の追加数
  AS 番号の追加数を、0～4 の 10 進数値で指定します。

[説明]

相手装置に EBGP で広報する AS 番号の個数を追加します。
<asprepend>で 0 を指定した場合は、広報される AS 番号は、自 AS 番号だけの 1 個として扱われます。

[注意]

BGP フィルタを設定している場合は、BGP フィルタでの AS 番号の追加数の設定が使用されます。

[未設定時]

広報する AS 番号の個数を追加しないとみなされます。

```
bgp neighbor <count> asprepend 0
```

7.4.6　bgp neighbor localpref

[機能]

BGP ローカル優先度の設定

[入力形式]

bgp neighbor [<count>] localpref <localpref>

[パラメタ]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 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。

範囲	機種
0～3	MR1000

<localpref>

- ローカル優先度
  ローカル優先度を、0～4294967295 の 10 進数値で指定します。

[説明]

EBGP で受信する経路情報のローカル優先度 (LOCAL_PREF 属性) を設定します。
ローカル優先度は、IBGP で広報され、同じ自律システム内での優先経路選択に使用されます。
ローカル優先度は、大きい値がより高い優先度を示します。

[注意]

BGP フィルタを設定している場合は、BGP フィルタでのローカル優先度の設定が使用されます。

[未設定時]

EBGP で受信する経路情報のローカル優先度として 100 が設定されているものとみなされます。

```
bgp neighbor <count> localpref 100
```

7.4.7 bgp neighbor ebgp-multihop

[機能]

EBGP マルチホップの設定

[入力形式]

bgp neighbor [<count>] ebgp-multihop <ttl>

[パラメタ]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 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。

範囲	機種
0～3	MR1000

<ttl>

- TTL 値
  TTL 値を、1～255 の 10 進数値で指定します。

[説明]

直接接続していない相手装置と EBGP 接続する場合に必要なホップ数 (IP パケットの TTL 値) を設定します。

[未設定時]

<ttl>に 1 が設定されているものとみなされます。

```
bgp neighbor <count> ebgp-multihop 1
```

7.4.8　bgp neighbor enforce-multihop

[機能]

BGP エンフォースマルチホップの設定

[入力形式]

bgp neighbor [<count>] enforce-multihop <mode>

[パラメタ]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 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。

範囲	機種
0～3	MR1000

<mode>

エンフォースマルチホップとして動作させるかどうかを指定します。

- on
  エンフォースマルチホップとして動作させます。
- off
  エンフォースマルチホップとして動作させません。

[説明]

エンフォースマルチホップとして動作させるかどうかを設定します。
<mode>に on が設定されている場合、EBGP のマルチホップ接続で EBGP マルチホップの TTL 値に 1 が設定されていても、受信した経路情報を破棄しません。off が設定されている場合は破棄します。

[未設定時]

エンフォースマルチホップとして動作しないものとみなされます。

```
bgp neighbor <count> enforce-multihop off
```

7.4.9 bgp neighbor default-originate

[機能]

BGP デフォルトルート広報可否の設定

[入力形式]

bgp neighbor [<count>] default-originate <mode>

[パラメタ]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 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。

範囲	機種
0〜3	MR1000

<mode>

- off
  デフォルトルートを広報しません。
- on
  デフォルトルートを広報します。

[説明]

デフォルトルートを広報するかどうかを設定します。
<mode>に on を設定した場合、広報する経路情報にデフオルトルートがあるときは広報します。
<mode>に off を設定した場合、広報する経路情報にデフオルトルートがあっても広報しません。

[未設定時]

デフォルトルートを広報しないものとみなされます。

```
bgp neighbor <count> default-originate off
```

7.4.10　bgp neighbor family

[機能]

BGP アドレスファミリの設定

[入力形式]

bgp neighbor [<count>] family <address_family>

[パラメタ]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 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。

範囲	機種
0～3	MR1000

<address_family>

- ipv4
  アドレスファミリとして IPv4 ユニキャストを使用します。
- vpnv4
  アドレスファミリとして VPN IPv4 ユニキャストを使用します。

[説明]

BGP で使用するアドレスファミリを設定します。
<address_family>で vpnv4 は、本装置全体で 1 つだけ設定できます。

[未設定時]

アドレスファミリとして IPv4 ユニキャストを使用するものとみなされます。

```
bgp neighbor <count> family ipv4
```

7.4.11 bgp neighbor source

[機能]

BGP 自側 IP アドレスの設定

[入力形式]

bgp neighbor [<count>] source <address>

[パラメタ]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 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。

範囲	機種
0〜3	MR1000

<address>

- 自インタフェースアドレス
  自装置のインタフェースのアドレスをドット形式で指定します。
  指定可能な範囲は以下のとおりです。

  1.0.0.1 〜 126.255.255.254
  128.0.0.1 〜 191.255.255.254
  192.0.0.1 〜 223.255.255.254

[説明]

BGP セッションで使用する自側 IP アドレスを設定します。
BGP / MPLS VPN を使用する場合には、loopback インタフェースのアドレスを指定します。

[未設定時]

BGP セッションの自側 IP アドレスを自動的に選択するものとみなされます。

7.4.12　bgp neighbor filter act

[機能]

BGP フィルタの動作設定

[入力形式]

bgp neighbor [<count>] filter <number> act <action> [<direction>]

[パラメタ]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 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。

範囲	機種
0〜3	MR1000

<number>

- フィルタの定義番号
  フィルタリングの優先度を表す定義番号を、0〜199 の 10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

<action>

フィルタリング条件に一致した場合の動作を指定します。

- pass
  該当する経路情報を透過します。
- reject
  該当する経路情報を遮断します。

<direction>

フィルタリングを行う方向を指定します。
省略時は out を指定したものとみなされます。

- in
  受信時にフィルタリングを行います。
- out
  送信時にフィルタリングを行います。

[説明]

BGP での経路情報送受信時に、フィルタリング条件に一致した経路情報を通過 (pass) させるか遮断 (reject) させるかを設定します。フィルタリング条件は優先度順に検索し、条件に一致した経路情報があった時点でフィルタリングが行われ、それ以降の条件は参照されません。全条件に不一致の経路情報は遮断されます。

フィルタリング条件は、bgp neighbor filter as コマンドを使用し AS 番号を、または、bgp neighbor filter route コマンドを使用し経路情報を設定します。

<number>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号が既に存在する場合は、既存の定義が上書きされます。

BGP フィルタは、本装置全体で 200 個まで定義できます。

[注意]

フィルタリング条件が設定されていない場合、本コマンドの設定は無効となります。
BGP/MPLS VPN 運用では、BGP フィルタを使用できません。

[未設定時]

BGP フィルタを使用しないものとみなされ、すべての BGP の経路情報が透過します。

7.4.13　bgp neighbor filter move

[機能]

BGP フィルタの優先順序の変更

[入力形式]

bgp neighbor [<count>] filter move <number> <new_number>

[パラメタ]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 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。

範囲	機種
0～3	MR1000

<number>

- 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番号を指定します。

<new_number>

- 移動先フィルタリング定義番号
  <number>に対する新しい順序を、0～199 の 10 進数値で指定します。
  すで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]

BGP フィルタの優先順序を変更します。
<new_number>で、既存定義番号を指定した場合、その定義の前に挿入されます。また、
<new_number>は順番にソートされてリナンバリングされます。

7.4.14 bgp neighbor filter as

[機能]

BGP フィルタの AS 番号設定

[入力形式]

bgp neighbor [<count>] filter <number> as <as_number>

[パラメタ]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 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。

範囲	機種
0～3	MR1000

<number>

- フィルタの定義番号
  フィルタリングの優先度を表す定義番号を、0～199 の 10 進数値で指定します。

<as_number>

- AS 番号
  AS 番号を、1～65535 の 10 進数で指定します。

[説明]

AS 番号をフィルタ条件として設定します。

[未設定時]

AS 番号をフィルタ条件としないものとみなされます。

7.4.15　bgp neighbor filter route

[機能]

BGP フィルタの経路情報設定

[入力形式]

bgp neighbor [<count>] filter <number> route <address> / <mask> [<prefix_match>]

[パラメタ]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 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。

範囲	機種
0～3	MR1000

<number>

- フィルタの定義番号
  フィルタリングの優先度を表す定義番号を、0～199 の 10 進数値で指定します。

<address>/<mask>

- IPv4 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ルーティング情報を指定します。
  フィルタリング対象とするルーティング情報を、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)
- any
  すべてのルーティング情報をフィルタリング対象とする場合に指定します。
- default
  デフォルトルート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。

<prefix_match>

ルーティング情報 (IPv4 アドレス / マスク) の検索条件を指定します。
省略した場合は、exact を指定したものとみなされます。
<address> / <mask>に"any"または"default"を指定した場合は、<prefix_match>は指定できません。

- exact
  指定した<address> / <mask>とルーティング情報の IPv4 アドレス / マスクを比較し、一致した場合に、フィルタリング対象とします。
- inexact
  指定した<address>とルーティング情報の IPv4 アドレスを比較し、<mask>まで一致した場合、フィルタリング対象とします。

[説明]

経路情報をフィルタ条件として設定します。

[注意]

同じフィルタ定義番号のフィルタ条件として AS 番号が設定されている場合、AS 番号がフィルタ条件となります。

[未設定時]

経路情報をフィルタ条件としないものとみなされます。

7.4.16　bgp neighbor filter set medmetric

[機能]

BGP フィルタの MED メトリック設定

[入力形式]

bgp neighbor [<count>] filter <number> set medmetric <medmetric>

[パラメタ]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 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。

範囲	機種
0～3	MR1000

<number>

- フィルタの定義番号
  フィルタリングの優先度を表す定義番号を、0～199 の 10 進数値で指定します。

<medmetric>

- MED メトリック値
  相手装置に広報する MED メトリック値を、0～4294967295 の範囲で設定します。

[説明]

相手装置に広報する MED メトリック値を設定します。
送信時のフィルタ条件に一致した場合、MED メトリック値に<medmetric>を設定して広報します。
受信時のフィルタに本設定を行っても、MED メトリック値の設定は行われません。

[注意事項]

フィルタリング条件が設定されていない場合、本コマンドの設定は無効となります。

[未設定時]

MED メトリック値を 0 として広報します。

7.4.17 bgp neighbor filter set asprepend

[機能]

BGP フィルタの AS パスプリペンド設定

[入力形式]

bgp neighbor [<count>] filter <number> set asprepend <asprepend>

[パラメタ]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 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。

範囲	機種
0～3	MR1000

<number>

- フィルタの定義番号
  フィルタリングの優先度を表す定義番号を、0～199 の 10 進数値で指定します。

<asprepend>

- AS 番号追加数
  相手装置に広報する AS 番号の追加数を、0～4 の 10 進数で指定します。

[説明]

相手装置に広報する AS 番号の追加数を設定します。
送信時のフィルタ条件に一致した場合、<asprepend>で設定した個数の AS 番号を追加して広報します。
受信時のフィルタに本設定を行っても、AS 番号の追加は行われません。

[注意事項]

フィルタリング条件が設定されていない場合、本コマンドの設定は無効となります。

[未設定時]

AS 番号の追加を行わないものとみなされます。

7.4.18　bgp neighbor filter set localpref

[機能]

BGP フィルタのローカル優先度設定

[入力形式]

bgp neighbor [<count>] filter <number> set localpref <localpref>

[パラメタ]

<count>

- 相手装置の定義番号
  相手装置の定義番号を 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。

範囲	機種
0～3	MR1000

<number>

- フィルタの定義番号
  フィルタリングの優先度を表す定義番号を、0～199 の 10 進数値で指定します。

<localpref>

- ローカル優先度
  ローカル優先度を、0～4294967295 の 10 進数値で指定します。

[説明]

EBGP で受信する経路情報のローカル優先度 (LOCAL_PREF 属性) を設定します。
EBGP 受信時のフィルタ条件に一致した場合、ローカル優先度に<localpref>を設定します。
IBGP 受信時のフィルタおよび、送信時のフィルタに本設定を行っても、ローカル優先度の設定は行われません。

[注意事項]

フィルタリング条件が設定されていない場合、本コマンドの設定は無効となります。

[未設定時]

EBGP で受信する経路情報のローカル優先度として 100 が設定されたものとみなされます。

7.5 OSPF 情報

7.5.1 ospf ip id

[機能]

OSPF ID の設定

[入力形式]

ospf ip id <identifier>

[パラメタ]

<identifier>

- OSPF の ID
  IPv4 アドレスを 0.0.0.0～255.255.255.255 のドット形式で指定します。

[説明]

OSPF 接続において自装置を一意に示す ID を設定します。
ID は他のルータと重複しない値を指定し、一般的には自装置の IPv4 アドレスを使用します。
本コマンドを省略または 0.0.0.0 が設定されている場合は、以下のとおり ID を自動的に選択し使用します。

- loopback インタフェースに追加 IP アドレスが設定されている場合は、その IP アドレスを選択します。
- loopback インタフェースに追加 IP アドレスが設定されていない場合は、lan/remote インタフェースに設定されている IP アドレスの中からインタフェースの Up/Down の状態に関係なく最大のものを選択します。なお、remote インタフェースの相手側 IP アドレスおよび、lan インタフェースのセカンダリ IP アドレスは選択の対象となりません。

[未設定時]

自動的に選択された ID が使用されるものとみなされます。

```
ospf ip id 0.0.0.0
```

7.6　OSPF エリア情報

7.6.1　ospf ip area id

[機能]

OSPF エリア ID の設定

[入力形式]

ospf ip area [<area_number>] id <area_id>

[パラメタ]

<area_number>

- エリア定義番号

  エリアの定義番号を指定します。

  省略した場合は、0 を指定したものとみなされます。

範囲	機種
0〜2	MR1000

<area_id>

- エリア ID

  エリア ID を IPv4 アドレス表記 (ドット形式) または 10 進数表記で指定します。

[説明]

エリア ID を設定します。同じエリア ID を複数設定することはできません。

[注意]

OSPF を利用する場合は、エリア ID を必ず設定してください。

[未設定時]

エリア ID が設定されていないものとみなされます。

7.6.2 ospf ip area type

[機能]

OSPF エリアタイプの設定

[入力形式]

ospf ip area [<area_number>] type <area_type>

[パラメタ]

<area_number>

- エリア定義番号
  エリアの定義番号を指定します。
  省略した場合は、0 を指定したものとみなされます。

範囲	機種
0〜2	MR1000

<area_type>

エリアタイプを指定します。

- transit
  通常エリア。
- stub
  スタブエリア。
- nssa
  準スタブエリア。

[説明]

バックボーンエリア以外のエリアに対し、エリアタイプを設定します。

[注意]

バックボーンエリアに stub または nssa を設定しても通常エリアとして動作します。

[未設定時]

エリアタイプとして通常エリアが設定されているものとみなされます。

```
ospf ip area <area_number> type transit
```

7.6.3　ospf ip area defcost

[機能]

OSPF スタブエリア用デフォルトルートコストの設定

[入力形式]

ospf ip area [<area_number>] defcost <cost>

[パラメタ]

<area_number>

- エリア定義番号
  エリアの定義番号を指定します。
  省略した場合は、0 を指定したものとみなされます。

範囲	機種
0～2	MR1000

<cost>

- デフォルトルートコスト
  デフォルトルートのコストを、0～16777215 で指定します。

[説明]

エリア境界ルータがスタブエリア、準スタブエリアに広報するデフォルトルートのコストを設定します。

[未設定時]

デフォルトルートのコストを 1 として広報するものとみなされます。

```
ospf ip area <area_number> defcost 1
```

7.6.4 ospf ip area range

[機能]

OSPF エリア内部集約経路の設定

[入力形式]

ospf ip area [<area_number>] range <range_number> <address> / <mask> [<cost>]

[パラメタ]

<area_number>

- エリア定義番号

  エリアの定義番号を指定します。

  省略した場合は、0 を指定したものとみなされます。

範囲	機種
0〜2	MR1000

<range_number>

- 集約経路定義番号

  集約経路の定義番号を指定します。

範囲	機種
0〜3	MR1000

<address>/<mask>

- IPv4 ネットワークアドレス / マスクビット数 (またはマスク値)

  集約経路を IPv4 ネットワークアドレスとマスクビット数の組み合わせで指定します。有効な記述形式は以下のとおりです。なお、ネットマスク値は最上位ビットから 1 で連続した値でなければなりません。

  IPv4 ネットワークアドレス / マスクビット数 (例: 192.168.1.0 / 24)

  IPv4 ネットワークアドレス / マスク値 (例: 192.168.1.0 / 255.255.255.0)

  0.0.0.0 / 0 は指定できません。

<cost>

- 集約経路のコスト

  集約経路のコストを、0〜16777215 の 10 進数値で指定します。

  省略、または 0 を指定した場合は、集約される経路の中でもっとも大きいコストの値が指定されたものとみなされます。

[説明]

エリア境界ルータでのエリア内部経路の集約を設定します。他のエリアには、集約した経路だけを広報します。集約された経路は広報されません。集約される経路がない場合は、集約経路を広報しません。

<cost>を設定した場合、集約される経路のコストに関係なく、設定された値をコストとして使用します。省略、または 0 が設定された場合は、集約される経路の中でもっとも大きいコストの値が使用されます。

<range_number>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。

[未設定時]

エリア内部経路を集約しないものとみなされます。

7.6.5 ospf ip area type3-lsa

[機能]

OSPF エリア間でのサマリ LSA 入出力可否の設定

[入力形式]

ospf ip area [<area_number>] type3-lsa <count> <action> <address> / <mask> <direction> [<prefix_match>]

[パラメタ]

<area_number>

- エリア定義番号

  エリアの定義番号を指定します。

  省略した場合は、0 を指定したものとみなされます。

範囲	機種
0〜2	MR1000

<count>

- サマリ LSA 入出力可否定義番号

  サマリ LSA 入出力可否の優先度を表す定義番号を、0〜29 の 10 進数値で指定します。優先度は数値の小さい方がより高い優先度を示します。

<action>

サマリ LSA 入出力可否条件と一致した場合の動作を指定します。

- pass

  該当するサマリ LSA を透過します。

- reject

  該当するサマリ LSA を遮断します。

<address>/<mask>

- IPv4 アドレス / マスクビット数 (またはマスク値)

  サマリ LSA 入出力可否の条件とする経路情報を、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)

- any

  すべての経路情報をサマリ LSA 入出力可否の条件とする場合に指定します。

<direction>

サマリ LSA 入出力の方向を示します。

- in

  他のエリアからのサマリ LSA の入力を示します。

- out

  他のエリアへのサマリ LSA の出力を示します。

<prefix_match>

経路情報 (IPv4 アドレス / マスク) の検索条件を指定します。
省略した場合は、exact を指定したものとみなされます。
<address> / <mask>に"any"を指定した場合は、<prefix_match>は指定できません。

- exact
  指定した<address> / <mask>と経路情報の IPv4 アドレス / マスクを比較し、一致した場合に、サマリ LSA 入出力可否の対象とします。
- inexact
  指定した<address>と経路情報の IPv4 アドレスを比較し、<mask>まで一致した場合に、サマリ LSA 入出力可否の対象とします。

[説明]

エリア境界ルータにおいて、エリア間で入出力するサマリ LSA を透過 (pass) するか、または遮断 (reject) するかを設定します。

他のエリアからサマリ LSA の入力があった場合は、優先度順に<direction>に in が設定されているサマリ LSA 入出力可否条件から一致する条件を検索します。一致する条件がない場合は、遮断されます。一致する条件があった場合は、その条件に設定されている<action>により動作が決定されます。pass が設定されている場合は、透過され、reject が設定されている場合は、遮断されます。<direction>に in が設定されている条件がない場合は、透過されます。

他のエリアへサマリ LSA を出力する場合は、優先度順に<direction>に out が設定されているサマリ LSA 入出力可否条件から一致する条件を検索します。一致する条件がない場合は、遮断されます。一致する条件があった場合は、その条件に設定されている<action>により動作が決定されます。pass が設定されている場合は、透過され、reject が設定されている場合は、遮断されます。<direction>に out が設定されている条件がない場合は、透過されます。

LSA 入出力可否条件に一致する条件があった場合、それ以降の条件は参照されません。

<count>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。

サマリ LSA 入出力可否は、本装置全体で 30 個まで定義できます。

[注意]

ospf ip area range コマンドを使用し集約経路を設定しているエリアにおいて、集約経路はサマリ LSA 入出力可否の対象となります。集約される経路は対象にならないことに注意してください。

また、以下の経路情報は、サマリ LSA 入出力可否の対象となりません。

- 各エリアの AS 境界ルータから注入された AS 外部経路
- スタブエリアおよび準スタブエリアのエリア境界ルータが注入するデフォルト経路

[未設定時]

エリア間でのサマリ LSA すべて透過するものとみなされます。

7.6.6 ospf ip area type3-lsa move

[機能]

OSPF エリア間でのサマリ LSA 入出力可否の優先順序の変更

[入力形式]

ospf ip area [<area_number>] type3-lsa move <count> <new_count>

[パラメタ]

<area_number>

- エリア定義番号

  エリアの定義番号を指定します。

  省略した場合は、0 を指定したものとみなされます。

範囲	機種
0～2	MR1000

<count>

- サマリ LSA 入出力可否定義番号

  優先順序を変更するサマリ LSA 入出力可否定義番号を指定します。

<new_count>

- 移動先サマリ LSA 入出力可否定義番号

  <count>に対する新しい順序を、0～29 の 10 進数値で指定します。すで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]

サマリ LSA 入出力可否定義の優先順序を変更します。<count>で、既存定義番号を指定した場合、その定義の前に挿入されます。また、<new_count>は順番にソートされてリナンバリングされます。

7.7　OSPF バーチャルリンク情報

7.7.1　ospf ip area vlink id

[機能]

OSPF バーチャルリンク接続先の設定

[入力形式]

ospf ip area [<area_number>] vlink [<vlink_number>] id <router_id>

[パラメタ]

<area_number>

- エリア定義番号
  エリアの定義番号を指定します。
  省略した場合は、0 を指定したものとみなされます。

範囲	機種
0～2	MR1000

<vlink_number>

- バーチャルリンク定義番号
  バーチャルリンクの定義番号を、0～1 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。

<router_id>

- 接続先 OSPF ルータ ID
  接続先ルータの OSPF ルータ ID を指定します。
  IPv4 アドレスをドット形式で指定します。0.0.0.0 は指定できません。

[説明]

バーチャルリンクの接続先を OSPF ルータ ID で設定します。

[注意]

バーチャルリンクは、スタブエリア、準スタブエリアでは使用できません。

[未設定時]

バーチャルリンクを使用しないものとみなされます。

7.7.2 ospf ip area vlink hello

[機能]

OSPF バーチャルリンク用 Hello パケット送信間隔の設定

[入力形式]

ospf ip area [<area_number>] vlink [<vlink_number>] hello <hello_interval>

[パラメタ]

<area_number>

- エリア定義番号
  エリアの定義番号を指定します。
  省略した場合は、0 を指定したものとみなされます。

範囲	機種
0～2	MR1000

<vlink_number>

- バーチャルリンク定義番号
  バーチャルリンクの定義番号を、0～1 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。

<hello_interval>

- Hello パケット送信間隔
  Hello パケットの送信間隔を、1 秒～65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、1s～65535s、1m～1092m、1h～18h です。

[説明]

バーチャルリンク接続先との OSPF 隣接関係の維持に用いられる Hello パケットの送信間隔を設定します。
hello_interval の値はバーチャルリンク接続先と同じ値を設定します。

[注意]

バーチャルリンク接続先と異なる Hello パケット送信間隔を設定した場合、ルーティングが行えません。

[未設定時]

バーチャルリンク用 Hello パケット送信間隔に 10 秒が設定されているものとみなされます。

```
ospf ip area <area_number> vlink <vlink_number> hello 10s
```

7.7.3　ospf ip area vlink dead

[機能]

OSPF バーチャルリンク用隣接ルータ停止確認間隔の設定

[入力形式]

ospf ip area [<area_number>] vlink [<vlink_number>] dead <dead_interval>

[パラメタ]

<area_number>

- エリア定義番号

  エリアの定義番号を指定します。

  省略した場合は、0 を指定したものとみなされます。

範囲	機種
0～2	MR1000

<vlink_number>

- バーチャルリンク定義番号

  バーチャルリンクの定義番号を、0～1 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。

<dead_interval>

- 隣接ルータ停止確認間隔

  隣接ルータ停止確認の間隔を、1 秒～65535 秒の範囲で指定します。

  単位は、h(時)、m(分)、s(秒) のどれかを指定します。

  各単位での設定可能範囲は、1s～65535s、1m～1092m、1h～18h です。

[説明]

バーチャルリンクでの OSPF 隣接関係の維持に用いられる隣接ルータ停止確認間隔を設定します。

隣接ルータ停止確認間隔の間に Hello パケットを受信しなかった場合は、バーチャルリンク接続先との隣接関係は解除されます。

dead_interval の値はバーチャルリンク接続先と同じ値を設定します。

dead_interval の値は Hello パケット送信間隔よりも大きな値を設定する必要があります。

Hello パケット送信間隔の 4 倍を設定することを推奨します。

[注意]

バーチャルリンク接続先と異なる隣接ルータ停止確認間隔を設定した場合、ルーティングが行えません。

[未設定時]

バーチャルリンク用隣接ルータ停止確認間隔に 40 秒が設定されているものとみなされます。

```
ospf ip area <area_number> vlink <vlink_number> dead 40s
```

7.7.4 ospf ip area vlink retrans

[機能]

OSPF バーチャルリンク用パケット再送間隔の設定

[入力形式]

ospf ip area [<area_number>] vlink [<vlink_number>] retrans <retransmit_interval>

[パラメタ]

<area_number>

- エリア定義番号
  エリアの定義番号を指定します。
  省略した場合は、0 を指定したものとみなされます。

範囲	機種
0〜2	MR1000

<vlink_number>

- バーチャルリンク定義番号
  バーチャルリンクの定義番号を、0〜1 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。

<retransmit_interval>

- パケット再送間隔
  パケットの再送間隔を、1 秒〜65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、1s〜65535s、1m〜1092m、1h〜18h です。

[説明]

バーチャルリンクで OSPF パケットを再送する間隔を設定します。

[未設定時]

バーチャルリンク用パケット再送間隔に 5 秒が設定されているものとみなされます。

```
ospf ip area <area_number> vlink <vlink_number> retrans 5s
```

7.7.5　ospf ip area vlink delay

[機能]

OSPF バーチャルリンク用 LSU パケット送信遅延時間の設定

[入力形式]

ospf ip area [<area_number>] vlink [<vlink_number>] delay <transmit_delay>

[パラメタ]

<area_number>

- エリア定義番号
  エリアの定義番号を指定します。
  省略した場合は、0 を指定したものとみなされます。

範囲	機種
0～2	MR1000

<vlink_number>

- バーチャルリンク定義番号
  バーチャルリンクの定義番号を、0～1 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。

<transmit_delay>

- LSU パケット送信遅延時間
  LSU パケットを送信する場合の遅延時間を、1 秒～65535 秒の範囲で指定します。
  単位は、h(時)、m(分)、s(秒) のどれかを指定します。
  各単位での設定可能範囲は、1s～65535s、1m～1092m、1h～18h です。

[説明]

LSU(Link State Update) パケットの送信遅延時間を設定します。LSU パケットでは、LSA(Link State Advertisement) を作成してからの経過時間に<transmit_delay>の値を加算して広報します。

[注意]

一般的な装置では、作成してからの経過時間が 1 時間となった LSA を破棄します。このため、LSU 送信遅延時間に 1 時間以上を設定した場合は、正しくルーティングできない場合があります。

[未設定時]

バーチャルリンク用 LSU パケット送信遅延時間に 1 秒が設定されているものとみなされます。

```
ospf ip area <area_number> vlink <vlink_number> delay 1s
```

7.7.6 ospf ip area vlink auth type

[機能]

OSPF バーチャルリンク用パケット認証方式の設定

[入力形式]

ospf ip area [<area_number>] vlink [<vlink_number>] auth type <authtype>

[パラメタ]

<area_number>

- エリア定義番号
  エリアの定義番号を指定します。
  省略した場合は、0 を指定したものとみなされます。

範囲	機種
0～2	MR1000

<vlink_number>

- バーチャルリンク定義番号
  バーチャルリンクの定義番号を、0～1 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>

パケット認証方式を指定します。

- off
  認証を行いません。
- text
  テキスト認証を使用します。
- md5
  MD5 認証を使用します。

[説明]

バーチャルリンクで OSPF パケットに対する認証方式を設定します。

[注意]

authtype で text を設定した場合は、テキスト認証鍵の設定が必要です。md5 を設定した場合は、MD5 認証鍵情報の設定が必要です。

[未設定時]

バーチャルリンクで OSPF パケット認証を使用しないものとみなされます。

```
ospf ip area <area_number> vlink <vlink_number> auth type off
```

7.7.7　ospf ip area vlink auth textkey

[機能]

OSPF バーチャルリンク用テキスト認証鍵の設定

[入力形式]

ospf ip area [<area_number>] vlink [<vlink_number>] auth textkey <kind> <key> [encrypted]

[パラメタ]

<area_number>

- エリア定義番号
  エリアの定義番号を指定します。
  省略した場合は、0 を指定したものとみなされます。

範囲	機種
0〜2	MR1000

<vlink_number>

- バーチャルリンク定義番号
  バーチャルリンクの定義番号を、0〜1 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。

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

<key>

- テキスト認証鍵
  文字列鍵の場合は、0x21,0x23〜0x7e のコードで構成される 8 文字以内の ASCII 文字列で指定します。
  16 進数鍵の場合は、16 桁以内の 16 進数値で指定します。16 桁未満の値を指定したときは左詰めで設定され、残りは 16 桁になるまで 0x0 でパディングされます。
- 暗号化されたテキスト認証鍵
  show コマンドで表示される暗号化されたテキスト認証鍵を 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

- 暗号化テキスト認証鍵指定
  <key>に暗号化されたテキスト認証鍵を指定する場合に指定します。

[説明]

バーチャルチンクのテキスト認証で使用する鍵を設定します。
show コマンドでは、暗号化されたテキスト認証鍵が encrypted と共に表示されます。

[未設定時]

バーチャルリンク用テキスト認証鍵が設定されていないものとみなされます。

7.7.8 ospf ip area vlink auth md5key

[機能]

OSPF バーチャルリンク用 MD5 認証鍵情報の設定

[入力形式]

ospf ip area [<area_number>] vlink [<vlink_number>] auth md5key <key_id> <key> [encrypted]

[パラメタ]

<area_number>

- エリア定義番号
  エリアの定義番号を指定します。
  省略した場合は、0 を指定したものとみなされます。

範囲	機種
0〜2	MR1000

<vlink_number>

- バーチャルリンク定義番号
  バーチャルリンクの定義番号を、0〜1 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。

<key_id>

- MD5 認証鍵 ID
  MD5 認証鍵 ID を、1〜255 で指定します。
- 暗号化された MD5 認証鍵 ID
  show コマンドで表示される暗号化された MD5 認証鍵 ID 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。

<key>

- MD5 認証鍵
  MD5 認証鍵を、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。
- 暗号化された MD5 認証鍵
  show コマンドで表示される暗号化された MD5 認証鍵を 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 MD5 認証鍵情報指定
  <key_id>と<key>に暗号化された MD5 認証鍵 ID と MD5 認証鍵を指定する場合に指定します。

[説明]

バーチャルリンクの MD5 認証で使用する鍵情報 (MD5 認証鍵 ID、MD5 認証鍵) を設定します。
show コマンドでは、暗号化された MD5 認証鍵 ID と MD5 認証鍵が encrypted と共に表示されます。

[未設定時]

バーチャルリンク用 MD5 認証鍵情報が設定されていないものとみなされます。

7.8　ASBR 情報

7.8.1　ospf ip definfo

[機能]

OSPF AS 境界ルータにおけるデフォルトルート広報の設定

[入力形式]

ospf ip definfo <mode> [<metric> [<metric_type>]]

[パラメタ]

<mode>

- off
  デフォルトルートを広報しません。
- always
  デフォルトルートを広報します。
- exist
  AS 外部経路にデフォルトルートが存在した場合だけ広報します。

<metric>

- メトリック値
  デフォルトルートのメトリック値を、0～16777214 で指定します。
  省略した場合は、10 を指定したものとみなされます。

<metric_type>

- type1
  外部メトリックタイプ 1 を指定します。
- type2
  外部メトリックタイプ 2 を指定します。
  省略した場合は、type2 を指定したものとみなされます。

[説明]

AS 境界ルータにおけるデフォルトルートの広報を設定します。

[注意]

本設定は、AS 境界ルータとして動作している場合にだけ有効となります。

[未設定時]

AS 境界ルータにおいてデフォルトルートを広報しないものとみなされます。

```
ospf ip definfo off
```

7.8.2 ospf ip summary

[機能]

OSPF AS 外部経路集約の設定

[入力形式]

ospf ip summary <summary_number> <address> / <mask>

[パラメタ]

<summary_number>

- 集約経路定義番号
  集約経路の定義番号を指定します。

範囲	機種
0～3	MR1000

<address>/<mask>

- IPv4 ネットワークアドレス / マスクビット数 (またはマスク値)
  集約経路の IPv4 ネットワークアドレスとマスクビット数の組み合わせを指定します。
  有効な記述形式は以下のとおりです。なお、ネットマスク値は最上位ビットから 1 で連続した値でなければなりません。
  IPv4 ネットワークアドレス / マスクビット数 (例: 10.10.0.0 / 16)
  IPv4 ネットワークアドレス / マスク値 (例: 10.10.0.0 / 255.255.0.0) 0.0.0.0 / 0 は指定できません。

[説明]

AS 境界ルータにおける AS 外部経路の集約を設定します。
AS 外部の経路を広報する場合は、集約した経路を広報します。
<summary_number>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。

[注意]

本設定は、AS 境界ルータとして動作している場合にだけ有効となります。

[未設定時]

AS 外部経路の集約を行わないものとみなされます。

7.8.3　ospf ip redist

[機能]

OSPF 再配布フィルタの設定

[入力形式]

ospf ip redist <number> <action> <address>/<mask> [<prefix_match> [<metric> <metric_type>]]

[パラメタ]

<number>

- 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定義番号を、0～49 の 10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

<action>

フィルタリング条件に一致した場合の動作を指定します。

- pass
  該当する経路情報を透過します。
- reject
  該当する経路情報を遮断します。

<address>/<mask>

フィルタリング対象とする経路情報を指定します。

- IPv4 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経路情報を、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)
- any
  すべての経路情報をフィルタリング対象とする場合に指定します。
- default
  デフォルトルート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。

<prefix_match>

経路情報 (IPv4 アドレス/マスク) の検索条件を指定します。
省略した場合は、exact を指定したものとみなされます。
<address>/<mask>に"any"または"default"を指定した場合は、<prefix_match>は指定できません。

- exact
  指定した<address>/<mask>と経路情報の IPv4 アドレス/マスクを比較し、一致した場合に、フィルタリング対象とします。
- inexact
  指定した<address>と経路情報の IPv4 アドレスを比較し、<mask>まで一致した場合、フィルタリング対象とします。

<metric>

再配布する経路情報のメトリック値を指定します。
省略した場合は、IPv4 ルーティングプロトコル再配布の設定で指定した値となります。
<action>に"reject"を指定した場合は、<metric>は指定できません。

- 再配布するメトリック値
  設定可能範囲は、0～16777214 です。

<metric_type>

再配布する経路情報のメトリックタイプを指定します。
省略した場合は、IPv4 ルーティングプロトコル再配布の設定で指定した値となります。
<action>に"reject"を指定した場合は、<metric_type>は指定できません。

- type1
  外部経路のメトリックタイプが type1
- type2
  外部経路のメトリックタイプが type2

[説明]

OSPF に再配布する経路に対するフィルタリング条件と動作を設定します。
IPv4 経路情報 (インタフェース経路, スタティック経路,RIP 経路,BGP 経路）を OSPF に再配布する場合、フィルタリング条件に一致した情報を再配布するかどうかを設定します。
フィルタリング条件は優先順位で検索され、条件に一致した場合にフィルタリングの動作が行われそれ以降の条件は参照されません。
すべてのフィルタリング条件に一致しない経路情報は再配布されません。
再配布する経路情報にメトリック値、およびメトリックタイプを指定できます。
<address>/<mask>に"any"を指定した場合、メトリック値、およびメトリックタイプは、IPv4 ルーティングプロトコル再配布の設定で指定した値となります。また、"default"を指定した場合は、
ospf ip definfo コマンドで指定した値となります。
<number>は、指定値が順番にソートされてリナンバリングされます。また、同値の定義番号がすでに存在する場合は、既存の定義が上書きされます。
OSPF 再配布フィルタは、本装置全体で 50 個まで定義できます。

[注意]

デフォルトルートを再配布する場合は、ospf definfo コマンドの設定も必要です。

[未設定時]

OSPF 再配布フィルタが設定されていないものとみなされます。

7.8.4　ospf ip redist move

[機能]

OSPF 再配布フィルタの優先順序の変更

[入力形式]

ospf ip redist move <number> <new_number>

[パラメタ]

<number>

- 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番号を指定します。

<new_number>

- 移動先フィルタリング定義番号
  <number>に対する新しい順序を、0～49 の 10 進数値で指定します。
  すで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]

OSPF 再配布フィルタの優先順序を変更します。
<new_number>で、既存定義番号を指定した場合、その定義の前に挿入されます。また、<new_number>は順番にソートされてリナンバリングされます。

第 8 章　ブリッジ情報の設定

8.1　ブリッジ情報

8.1.1　bridge age

[機能]

ブリッジ学習テーブルの生存時間の設定

[入力形式]

bridge [<group_id>] age <age_time>

[パラメタ]

<group_id>

- ブリッジグループ識別子
  ブリッジグループ識別子を 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。

範囲	機種
0〜19	MR1000

<age_time>

- 生存時間
  MAC アドレス学習によって学習した情報の生存時間を、10 秒〜1000000 秒の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。

[説明]

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。
アドレス学習テーブルの生存時間を設定します。
アドレス学習機能によって学習された MAC アドレステーブルを最後に使用してから削除されるまでの時間を設定します。

[注意]

ブリッジグループ 0 に設定された値がすべてのブリッジグループで使用され、ブリッジグループ 0 以外に設定された値は使用されません。

[未設定時]

アドレス学習テーブルの生存時間として 5 分を定義するものとみなされます。

```
bridge <group_id> age 5m
```

8.1.2 bridge stp priority

[機能]

ブリッジ優先度の設定

[入力形式]

bridge [<group_id>] stp priority <priority>

[パラメタ]

<group_id>

- ブリッジグループ識別子

  ブリッジグループ識別子を 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。

範囲	機種
0〜19	MR1000

<priority>

- 優先度

  ブリッジネットワーク内での本装置の優先度を、0〜65535 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。

[説明]

本コマンドは、STP を使用する場合にだけ有効です。

ルートブリッジ決定アルゴリズムで使用するブリッジの優先度を指定します。一般的なブリッジネットワークではルートブリッジにトラフィックが集中するため、バックボーンに近いブリッジが優先となるように設定してください。ルートブリッジにするブリッジには、最小の値を指定してください。

[注意]

ブリッジグループ 0 以外のブリッジグループでは STP は動作しません。

[未設定時]

優先度として 32768 を定義するものとみなされます。

```
bridge <group_id> stp priority 32768
```

8.1.3　bridge stp age

[機能]

Hello メッセージ待ち時間の設定

[入力形式]

bridge [<group_id>] stp age <max_age>

[パラメタ]

<group_id>

- ブリッジグループ識別子
  ブリッジグループ識別子を 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。

範囲	機種
0〜19	MR1000

<max_age>

- 待ち時間
  ルートブリッジから送出される構成情報 BPDU の待ち時間を、6 秒〜40 秒の範囲で指定します。
  単位は、s(秒) を指定します。

[説明]

本コマンドは、STP を使用する場合にだけ有効です。
ルートブリッジまたは代表ブリッジから送出される構成情報 BPDU の待ち時間を指定します。

[注意]

ブリッジグループ 0 以外のブリッジグループでは STP は動作しません。

[未設定時]

待ち時間に 20 秒を設定したものとみなされます。

```
bridge <group_id> stp age 20s
```

8.1.4 bridge stp hello

[機能]

Hello メッセージ送出間隔の設定

[入力形式]

bridge [<group_id>] stp hello <time>

[パラメタ]

<group_id>

- ブリッジグループ識別子
  ブリッジグループ識別子を 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。

範囲	機種
0〜19	MR1000

<time>

- 送出間隔
  ルートブリッジになったときに定期的に送出する構成情報 BPDU の送出間隔の時間を、1 秒〜10 秒の範囲で指定します。単位は、s(秒) を指定します。

[説明]

本コマンドは、STP を使用する場合にだけ有効です。
本装置がルートブリッジとなったときに送出する構成情報 BPDU の送出間隔を指定します。
STP を使用する場合でも、本装置がルートブリッジとならなかった場合は、設定が無効となります。

[注意]

ブリッジグループ 0 以外のブリッジグループでは STP は動作しません。

[未設定時]

送出間隔に 2 秒を設定したものとみなされます。

```
bridge <group_id> stp hello 2s
```

8.1.5　bridge stp delay

[機能]

最大中継遅延時間の設定

[入力形式]

bridge [<group_id>] stp delay <delay_time>

[パラメタ]

<group_id>

- ブリッジグループ識別子
  ブリッジグループ識別子を 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。

範囲	機種
0〜19	MR1000

<delay_time>

- 最大中継遅延時間
  最大中継遅延時間を、4 秒〜30 秒の範囲で指定します。単位は、s(秒) を指定します。

[説明]

本コマンド は、STP を使用する場合にだけ有効です。
最大中継遅延時間を設定します。
STP を使用する場合でも、本装置がルートブリッジとならなかった場合は、設定が無効となります。
STP で Listening 状態から Learning 状態に変化する場合、または Learning 状態から Forwarding 状態に変化するまでの時間 (ルートブリッジから広報される時間) を指定します。

[注意]

ブリッジグループ 0 以外のブリッジグループでは STP は動作しません。

[未設定時]

最大中継遅延時間に 15 秒を設定したものとみなされます。

```
bridge <group_id> stp delay 15s
```

8.1.6 bridge ip routing

[機能]

IPv4 ルーティングの設定

[入力形式]

bridge [<group_id>] ip routing <mode>

[パラメタ]

<group_id>

- ブリッジグループ識別子
  ブリッジグループ識別子を 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。

範囲	機種
0〜19	MR1000

<mode>

- on
  IPv4 ルーティングを有効にします。
- off
  IPv4 ルーティングを無効にし、IPv4 フレームをブリッジにより制御します。

[説明]

IPv4 ルーティングの設定します。
IPv4 ルーティングを無効とした場合、IPv4 フレームはブリッジにより制御されます。

[未設定時]

IPv4 をルーティングにより制御するものとみなされます。

```
bridge <group_id> ip routing on
```

8.1.7　bridge ip policy

[機能]

IPv4 転送ポリシの設定

[入力形式]

bridge [<group_id>] ip policy <mode>

[パラメタ]

<group_id>

- ブリッジグループ識別子
  ブリッジグループ識別子を 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。

範囲	機種
0〜19	MR1000

<mode>

- strict
  IPv4 ブリッジを行う場合に、グループ外からグループ内およびグループ内からグループ外へのルーティングによる転送を行いません。
- loose
  IPv4 ブリッジを行う場合に、グループ外からグループ内およびグループ内からグループ外へのルーティングによる転送を行います。

[説明]

本コマンドは、IPv4 をブリッジ対象とした場合にだけ有効です。
IPv4 ブリッジを行う場合に、グループ外からグループ内、およびグループ内からグループ外へのルーティングによる転送を行うかどうかを設定します。
IPv4 ブリッジ動作時にグループ内からグループ外へのルーティングによる転送が行われるのは以下の場合です。

- 受信フレームのあて先 MAC アドレスが受信インタフェース宛であるが、あて先 IP アドレスが受信インタフェース宛でない場合。

IPv4 ブリッジ動作時にグループ外からグループ内へのルーティングによる転送が行われるのは以下の場合です。

- IPv4 をルーティングするインタフェースで受信したパケットがルーティングにより IPv4 をブリッジするインタフェースへ出力される場合。

<mode>が strict の場合、これらの転送をブロックすることで、ブリッジ転送対象外のパケットに対してもグループ内に閉じた通信を行うことができます。

[未設定時]

グループ外からグループ内、およびグループ内からグループ外へのルーティングによる転送を行わないものとして動作します。

```
bridge <group_id> ip policy strict
```

8.1.8　bridge ip6 routing

[機能]

IPv6 ルーティングの設定

[入力形式]

bridge [<group_id>] ip6 routing <mode>

[パラメタ]

<group_id>

- ブリッジグループ識別子
  ブリッジグループ識別子を 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。

範囲	機種
0〜19	MR1000

<mode>

- on
  IPv6 ルーティングを有効にします。
- off
  IPv6 ルーティングを無効にし、IPv6 フレームをブリッジにより制御します。

[説明]

IPv6 ルーティングの設定します。
IPv6 ルーティングを無効とした場合、IPv6 フレームはブリッジにより制御されます。

[未設定時]

IPv6 をルーティングにより制御するものとみなされます。

```
bridge <group_id> ip6 routing
```

8.1.9 bridge ip6 policy

[機能]

IPv6 転送ポリシの設定

[入力形式]

bridge [<group_id>] ip6 policy <mode>

[パラメタ]

<group_id>

- ブリッジグループ識別子

  ブリッジグループ識別子を 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。

範囲	機種
0〜19	MR1000

<mode>

- strict

  IPv6 ブリッジを行う場合に、グループ外からグループ内およびグループ内からグループ外へのルーティングによる転送を行いません。

- loose

  IPv6 ブリッジを行う場合に、グループ外からグループ内およびグループ内からグループ外へのルーティングによる転送を行います。

[説明]

本コマンドは、IPv6 をブリッジ対象とした場合にだけ有効です。

IPv6 ブリッジを行う場合に、グループ外からグループ内、およびグループ内からグループ外へのルーティングによる転送を行うかどうかを設定します。

IPv6 ブリッジ動作時にグループ内からグループ外へのルーティングによる転送が行われるのは以下の場合です。

- 受信フレームのあて先 MAC アドレスが受信インタフェース宛であるが、あて先 IP アドレスが受信インタフェース宛でない場合。

IPv6 ブリッジ動作時にグループ外からグループ内へのルーティングによる転送が行われるのは以下の場合です。

- IPv6 をルーティングするインタフェースで受信したパケットがルーティングにより IPv6 をブリッジするインタフェースへ出力される場合。

<mode>が strict の場合、これらの転送をブロックすることで、ブリッジ転送対象外のパケットに対してもグループ内に閉じた通信を行うことができます。

[未設定時]

　グループ外からグループ内、およびグループ外からグループ内へのルーティングによる転送を行わないものとして動作します。

```
bridge <group_id> ip6 policy strict
```

8.1.10 bridge vlan tag transmit

[機能]

VLAN タグの転送方式の設定

[入力形式]

bridge [<group_id>] vlan tag transmit <mode>

[パラメタ]

<group_id>

- ブリッジグループ識別子
  ブリッジグループ識別子を 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。

範囲	機種
0〜19	MR1000

<mode>

- on
  VLAN タグをつけたまま透過ブリッジします。
- off
  VLAN タグを挿抜してブリッジします。

[説明]

VLAN インタフェースで受信した VLAN タグ付きフレームのタグを透過転送するかどうかを設定します。
VLAN タグを挿抜する設定の場合、VLAN インタフェースで受信してリモートインタフェースへ出力する際には VLAN タグを除去して転送し、リモートインタフェースで受信して VLAN インタフェースへ出力する際には VLAN タグを挿入して転送します。

[未設定時]

VLAN タグを挿抜してブリッジします。

```
bridge <group_id> vlan tag transmit off
```

8.1.11　bridge inter-remote

[機能]

リモートインタフェース間のブリッジ転送の設定

[入力形式]

bridge [<group_id>] inter-remote <mode>

[パラメタ]

<group_id>

- ブリッジグループ識別子
  ブリッジグループ識別子を 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。

範囲	機種
0〜19	MR1000

<mode>

- on
  リモートインタフェース間のブリッジ転送をおこないます。
- off
  リモートインタフェース間のブリッジ転送をおこないません。

[説明]

リモートインタフェース間でブリッジ転送をおこなうかおこなわないかを設定します。
リモートインタフェースと LAN インタフェースの間のブリッジだけを許し、あるリモートインタフェースから別のリモートインタフェースへのブリッジ転送をブロックしたい場合に<mode> に off を設定します。

[未設定時]

リモートインタフェース間でブリッジ転送をおこないます。

```
bridge <group_id> inter-remote on
```

第 9 章　MPLS 情報の設定

9.1　LDP 情報

9.1.1　mpls ldp router-id

[機能]

LDP ROUTER-ID の設定

[入力形式]

mpls ldp router-id <identifier>

[パラメタ]

<identifier>

- LDP を使用するルータを特定するための ID
  IPv4 アドレスで指定します。

[説明]

自装置を一意に示す ID を設定します。設定する ID は他のルータと重複しない ID を指定します。通信可能な自装置の IP アドレス (IPv4) を設定します。
0.0.0.0 を指定した場合、自動的にどれかの自装置の IP アドレス (IPv4) を使用します.

[未設定時]

0.0.0.0 が設定されているものとみなされ、router-id は自動的に設定されます。

```
mpls ldp router-id 0.0.0.0
```

9.1.2 mpls ldp control

[機能]

LDP 制御方式の設定

[入力形式]

mpls ldp control <mode>

[パラメタ]

<mode>

- ordered
  Ordered Label Distribution Control を使用します。
- independent
  Independent Label Distribution Control を使用します。

[説明]

LDP の制御方式を指定します。

[未設定時]

independent が選択されたものとして動作します。

```
mpls ldp control independent
```

9.1.3　mpls ldp ip transport

[機能]

IPv4 Transport Address の設定

[入力形式]

mpls ldp ip transport <address>

[パラメタ]

<address>

- LDP セッションの送信元 IPv4 アドレス
  IPv4 アドレスを指定します。以下の範囲で指定してください。

  0.0.0.0
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

[説明]

LDP がピアとの通信に用いる送信元 IPv4 アドレスを設定します。本装置に設定された IPv4 アドレスを指定します。

インタフェースの設定で IPv4 Transport Address を指定しない場合に、本設定が使用されます。本定義に 0.0.0.0 を指定した場合は、LDP が動作するインタフェースの IPv4 アドレスを IPv4 Transport Address として使用します。

[未設定時]

IPv4 Transport Address の設定を行わず、LDP が動作するインタフェースの IPv4 アドレスを送信元として使用します。

```
mpls ldp ip transport 0.0.0.0
```

[注意]

IPv4 Transport Address を指定する場合には、必ず本装置に存在するにアドレスを指定する必要があります。本装置に存在しないアドレスを指定した場合は、LDP を使用できません。

9.1.4 mpls ip propagate-ttl

[機能]

MPLS TTL 伝達の設定

[入力形式]

mpls ip propagate-ttl <mode>

[パラメタ]

<mode>

- on
  MPLS から IP または IP から MPLS にパケットを交換する際に、TTL の情報を伝達します。
- off
  MPLS から IP または IP から MPLS にパケットを交換する際に、TTL の情報を伝達しません。

[説明]

MPLS と IP の間での TTL の伝達方法を指定します。

mode が on の場合は。MPLS ラベル PUSH 時に IP パケットの TTL が伝達され、MPLS ラベル POP 時に IP パケットの TTL に書き戻されるため、MPLS ドメインを転送される IP パケットはドメインの hop 数分だけ TTL が減少します。

mode が off の場合は。MPLS ラベル PUSH 時に IP パケットの TTL が伝達されず、MPLS パケットの TTL は無条件で 255 となり、また MPLS ラベル POP 時にも IP パケットの TTL は書き戻されないため、MPLS ドメインを転送される IP パケットはドメインの hop 数を意識することがなく、ドメインを 1 つの仮想的なルータとして見るようになります。

[注意]

本設定は MPLS ドメイン中のすべてのルータで一致させる必要があります。

[未設定時]

on が選択されたものとして動作します。

```
mpls ip propagate-ttl on
```

9.1.5　mpls ldp targeted-hello ttl

[機能]

Targeted LDP の TTL 値の設定

[入力形式]

mpls ldp targeted-hello ttl <ttl>

[パラメタ]

<ttl>

- TTL 値
  Targeted Hello の TTL の値を 1～255 の 10 進数値で指定します。
  未設定時は 64 が指定されたものとして動作します。

[説明]

Targeted LDP で使用する Hello メッセージの TTL 値を指定します。

[未設定時]

64 が指定されたものとして動作します。

```
mpls ip targeted-hello ttl 64
```

第 10 章　マルチキャスト情報の設定

10.1　マルチキャスト情報

10.1.1　multicast ip pimsm candrp mode

[機能]

PIM-SM(IPv4) の RP の動作の指定。

[入力形式]

multicast ip pimsm candrp mode <mode>

[パラメタ]

<mode>

PIM-SM の RP としての動作モードを以下で指定します。

- off
  RP として動作しない
- on
  RP として動作する

[説明]

PIM-SM(IPv4) の RP としての動作モードを指定します。

[未設定時]

RP として動作しません。

```
multicast ip pimsm candrp mode off
```

10.1.2 multicast ip pimsm candrp address

[機能]

PIM-SM(IPv4) の RP のアドレスの設定

[入力形式]

multicast ip pimsm candrp address <address>

[パラメタ]

<address>

- RP アドレス
  PIM-SM(IPv4) の RP として動作するインタフェースのアドレスを指定します。
  0.0.0.0 を指定すると利用できるアドレスを自動で検索します。
  指定可能な範囲は以下のとおりです。
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

[説明]

RP として動作するインタフェースのアドレスを指定します。

[未設定時]

利用できるアドレスを自動で検索します。

```
multicast ip pimsm candrp address 0.0.0.0
```

10.1.3　multicast ip pimsm candrp priority

[機能]

PIM-SM(IPv4) の RP としての動作時のプライオリティ

[入力形式]

multicast ip pimsm candrp priority <priority>

[パラメタ]

<priority>

- プライオリティ
  PIM-SM(IPv4) の RP としての動作時のプライオリティを 0～255 の 10 進数値で設定します。

[説明]

RP としての動作時のプライオリティを設定します。

[注意]

指定した値が小さいほど、優先順位が高くなります。

[未設定時]

0(最高) が指定されたものとみなされます。

```
multicast ip pimsm candrp priority 0
```

10.1.4 multicast ip pimsm candbsr mode

[機能]

PIM-SM(IPv4) の BSR の動作の指定

[入力形式]

multicast ip pimsm candbsr mode <mode>

[パラメタ]

<mode>

PIM-SM(IPv4) の BSR としての動作モードを以下で指定します。

- off
  BSR として動作しない
- on
  BSR として動作する

[説明]

PIM-SM の BSR としての動作モードを指定します。

[未設定時]

BSR として動作しません。

```
multicast ip pimsm candbsr mode off
```

10.1.5　multicast ip pimsm candbsr address

[機能]

PIM-SM(IPv4) の BSR のアドレスの設定

[入力形式]

multicast ip pimsm candbsr address <address>

[パラメタ]

<address>

- BSR アドレス
  PIM-SM(IPv4) の BSR として動作するインタフェースのアドレスを指定します。
  0.0.0.0 を指定すると利用できるアドレスを自動で検索します。
  指定可能な範囲は以下のとおりです。
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

[説明]

BSR として動作するインタフェースのアドレスを指定します。

[未設定時]

利用できるアドレスを自動で検索します。

```
multicast ip pimsm candbsr address 0.0.0.0
```

10.1.6 multicast ip pimsm candbsr priority

[機能]

PIM-SM(IPv4) の BSR のプライオリティの設定

[入力形式]

multicast ip pimsm candbsr priority <priority>

[パラメタ]

<priority>

- プライオリティ
  PIM-SM(IPv4) の BSR としての動作時のプライオリティを 0〜255 の 10 進数値で設定します。

[説明]

BSR としての動作時のプライオリティを設定します。

[注意]

指定した値が大きいほど、優先順位が高くなります。

[未設定時]

0(最低) が設定されたものとみなされます。

```
multicast ip pimsm candbsr priority 0
```

10.1.7　multicast ip pimsm spt mode

[機能]

PIM-SM(IPv4) の SPT への経路変更の動作の指定

[入力形式]

multicast ip pimsm spt mode <mode>

[パラメタ]

<mode>

PIM-SM(IPv4) の SPT への経路変更の動作モードを以下で指定します。

- on
  経路変更を行う
- off
  経路変更を行わない

[説明]

PIM-SM(IPv4) の SPT への経路変更の動作モードを指定します。

[注意]

SPT への切り替えは、マルチキャスト・パケットの受信者の直前のルータ (lasthop router) が行います。SPT の設定は、lasthop router 上で行います。

[未設定時]

経路変更を行います。

```
multicast ip pimsm spt mode on
```

10.1.8 multicast ip pimsm spt rate

[機能]

PIM-SM(IPv4) の SPT への経路変更のしきい値

[入力形式]

multicast ip pimsm spt rate <rate>

[パラメタ]

<rate>

- データ転送速度
  PIM-SM(IPv4) の SPT への経路変更のしきい値となる
  データ転送速度を、1k～100000k、または 1m～100m 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 または m 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。
  単位文字 m を付与した場合、単位は Mbps となります。
  1Kbps は 1000bps、1Mbps は 1000Kbps です。
  0 の場合、経路変更を即座に行います。

[説明]

SPT への経路変更のしきい値をデータ転送速度で設定します。

[注意]

経路変更が行われるまで、最大で 5 秒のタイムラグが発生する場合があります。

[未設定時]

即座に SPT への経路変更を行います。

```
multicast ip pimsm spt rate 0
```

10.1.9　multicast ip pimsm register checksum

[機能]

PIM-SM(IPv4) の Register パケットの送信時のチェックサムの計算方法

[入力形式]

multicast ip pimsm register checksum <checksum>

[パラメタ]

<checksum>

PIM-SM(IPv4) の Register パケットの送信時のチェックサムの計算方法を以下で指定します。

- header
  ヘッダ部だけで計算する
- full
  パケット全体で計算する

[説明]

PIM-SM(IPv4) の Register パケットの送信時のチェックサムの計算方法を設定します。

[注意]

PIM Register パケットは、RFC2362 ではヘッダ部だけで計算するように定義されていますが、
一部のルータはパケット全体で計算します。このようなルータが RP を行う場合には、
PIM Register パケットが受信されない可能性があるため、チェックサムの計算範囲を「パケット全体」に変更する必要があります。
本装置は PIM Register パケットの受信時には、ヘッダ部 (RC2362 準拠) とパケット全体の 2 通りの方法で計算するため、本装置が RP を行う場合には、どちらの計算方法のパケットを受信しても問題はありません。

[未設定時]

ヘッダ部だけで計算します。

```
multicast ip pimsm register checksum header
```

10.1.10 multicast ip route

[機能]

IPv4 マルチキャスト・スタティックルーティング情報の設定

[入力形式]

multicast ip route <count> <src_address> <group_address> <incoming> <outgoing>

[パラメタ]

<count>

- スタティックルーティング定義番号
  スタティックルーティング定義番号を、0〜19 の 10 進数値で指定します。

<src_address>

- 配送元ホストアドレス
  配送元ホストを IPv4 アドレスで指定します。
  指定可能な範囲は以下のとおりです。
  1.0.0.1 〜 126.255.255.254
  128.0.0.1 〜 191.255.255.254
  192.0.0.1 〜 223.255.255.254

<group_address>

- マルチキャスト・グループアドレス
  マルチキャスト・グループアドレスを以下の範囲の IPv4 アドレスで指定します。

  224.0.1.0 〜 239.255.255.255

<incoming>

- 入力インタフェース
  入力インタフェースとして lan または、rmt インタフェースを指定します。

<outgoing>

- 出力インタフェース
  出力インタフェースとして lan または、rmt インタフェースを指定します。
  複数指定する場合は、","(カンマ) で区切ります。また、範囲指定する場合は、「rmt1-rmt4」のように"-"(ハイフン) を使用して指定します。

最大出力インタフェース数	機種
5	MR1000

[説明]

IPv4 マルチキャスト・スタティックルーティング情報を設定します。
入力インタフェースおよび出力インタフェースの指定は以下の範囲で指定します。

範囲	機種
lan0〜lan19 rmt0〜rmt99	MR1000

[未設定時]

IPv4 マルチキャスト・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。

第 11 章　UPnP 情報の設定

11.1　UPnP 情報

11.1.1　upnp use

[機能]

VoIP NAT トラバーサル機能の設定

[入力形式]

upnp use <mode>

[パラメタ]

<mode>

- off
  VoIP NAT トラバーサル機能を使用しません。
- on
  VoIP NAT トラバーサル機能を使用します。

[説明]

VoIP NAT トラバーサル機能を使用するかどうかを設定します。
VoIP NAT トラバーサル機能は、NAT 機能を使用すると通信できない VoIP アダプタを通信できるようにします。ただし、VoIP アダプタが UPnP(Universal Plug and Play) に対応していなければ通信できません。
同様に、UPnP に対応したアプリケーションプログラム (UPnP クライアント) も通信できるようになることがあります。
VoIP アダプタ (UPnP クライアント) および通信相手は、以下に示すインタフェースに接続してください。

- VoIP アダプタ (UPnP クライアント)
  NAT 機能を使用しない lan インタフェースに接続してください。
  ない場合、VoIP NAT トラバーサル機能は動作しません。
- 通信相手
  NAT を使用する定義番号が一番小さい lan インタフェースに接続してください。
  ない場合、NAT を使用する定義番号が一番小さい remote インタフェースに接続してください。
  いずれもない場合、VoIP アダプタ (UPnP クライアント) は通信できません。

[注意]

VoIP アダプタ (UPnP クライアント) との通信に、以下のポート番号を使用します。
そのため、これらのポートを IP フィルタリングで遮断しないでください。

プロトコル	ポート番号
UDP TCP	1900 5432

UPnP クライアントは通常の NAT 変換も併用することがあります。NAT の割当時間が短いと通信が切断されることがありますので、NAT の定義で必要十分な割当時間を設定してください。
NAT の定義でグローバル IP アドレスの個数には 1 を指定してください。2 以上を指定すると UPnP が正しく動作しないことがあります。

[未設定時]

VoIP NAT トラバーサル機能を使用しないものとみなされます。

```
upnp use off
```

11.1.2　upnp portmapping lease

[機能]

ポートマッピング有効期限の設定

[入力形式]

upnp portmapping lease <time>

[パラメタ]

<time>

- ポートマッピング有効期限

  UPnP クライアントがポートマッピングを無期限で設定しようとしたときに、強制的に設定する有効期限を指定します。

  有効期限は、60 秒 (1 分)～86400 秒 (1 日) の範囲で、数字と単位をつなげて指定します。

  単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。

[説明]

UPnP クライアントがポートマッピングを無期限で設定しようとしたときに、強制的に設定する有効期限を設定します。設定したポートマッピングが使用されなくなってから有効期限を過ぎたとき、そのポートマッピングを強制的に削除します。本設定がなく、UPnP クライアントがポートマッピングを無期限で登録した場合、

UPnP クライアントがポートマッピングを削除するまでポートマッピングが設定されたままになります。

[注意]

本設定によってポートマッピングが強制的に削除された場合、そのポートマッピングを設定した UPnP クライアントが通信できなくなります。その場合、その UPnP クライアントを再起動してください。

[未設定時]

ポートマッピング有効期限を設定しないものとみなされ、ポートマッピングを強制的に削除しません。

第 12 章　AAA 情報の設定

- グループ ID の指定範囲
  各コマンドの [パラメタ] に記載されている [<group_id>](グループ ID) に指定するグループの通し番号 (10 進数値) は、機種ごとに以下に示す範囲で指定してください。

範囲	機種
0〜9	MR1000

- AAA ユーザ情報定義番号の指定範囲
  各コマンドの [パラメタ] に記載されている [<number>](AAA ユーザ情報定義番号) に指定するグループ内の通し番号 (10 進数値) は、機種ごとに以下に示す範囲で指定してください。

範囲	機種
0〜999	MR1000

12.1　グループ ID 情報

12.1.1　aaa name

[機能]

グループ名称の設定

[入力形式]

aaa [<group_id>] name <group_name>

[パラメタ]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略した場合は、0 を指定したものとみなされます。

<group_name>

- グループ名
  グループ名を、0x21,0x23～0x7e の 32 文字以内の ASCII 文字列で指定します。

[説明]

グループ名を設定します。

[注意]

既に同一名称のグループが登録されている場合は、異常終了します。

[未設定時]

グループ名を設定しないものとみなされます。

12.1.2 AAA ユーザ情報

12.1.2.1 認証情報

12.1.2.1.1 aaa user id

[機能]

認証情報の設定 (ユーザ ID)

[入力形式]

aaa [<group_id>] user [<number>] id <id>

[パラメタ]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略した場合は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
  グループ内での通し番号を、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>

- ユーザ ID
  ユーザ 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。

[説明]

認証プロトコルに使用する、認証情報 (ユーザ ID) を設定します。

[未設定時]

認証情報 (ユーザ ID) を設定しないものとみなされます。

12.1.2.1.2　aaa user password

[機能]

認証情報の設定 (パスワード)

[入力形式]

aaa [<group_id>] user [<number>] password <password> [encrypted]

[パラメタ]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略した場合は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
  グループ内での通し番号を、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。

<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]

認証プロトコルに使用する、認証情報 (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]

認証情報 (パスワード) を設定しないものとみなされます。

12.1.2.1.3 aaa user called number

[機能]

CLID の設定

[入力形式]

aaa [<group_id>] user [<number>] called number <called_number> [<subaddress>]

[パラメタ]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略した場合は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
  グループ内での通し番号を、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]

CLID 相手判定で、チェックする番号を設定します。

[注意]

MR1000 は PIAFS 接続に対応しています。PIAFS(64Kbps) 着信時には、<subaddress> で設定した相手サブアドレスは無視されますので、設定しないでください。

[未設定時]

CLID 相手判定を行わないものとみなします。

12.1.2.2　IP 関連情報

12.1.2.2.1　aaa user ip address local

[機能]

自側 IP アドレスの設定

[入力形式]

aaa [<group_id>] user [<number>] ip address local <address>

[パラメタ]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略した場合は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
  グループ内での通し番号を、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
  自側 IP アドレスを指定します。
  指定可能な範囲は以下のとおりです。
  0.0.0.0
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254
  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。

12.1.2.2.2 aaa user ip address remote

[機能]

相手側 IP アドレスの設定

[入力形式]

aaa [<group_id>] user [<number>] ip address remote <address>

[パラメタ]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略した場合は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
  グループ内での通し番号を、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
  相手側 IP アドレスを指定します。
  指定可能な範囲は以下のとおりです。
  0.0.0.0
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254
  0.0.0.0 を指定した場合は、設定を IP アドレスなし (unnumbered) として動作します。
- depend-template
  テンプレート定義による設定を適用する場合に指定します。

[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]

テンプレート定義による設定を適用します。

12.1.2.2.3　aaa user ip route

[機能]

IPv4 スタティック経路情報の設定

[入力形式]

aaa [<group_id>] user [<number>] ip route <count> <address> / <mask> <metric> <distance>

[パラメタ]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。省略した場合は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
  グループ内での通し番号を、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>

- スタティック経路情報定義番号
  スタティック経路情報定義番号を、10 進数値で指定します。

範囲	機種
0〜255	MR1000

<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
  このスタティック経路情報を RIP に再配布するときのメトリック値を、1〜15 の 10 進数値で指定します。
- RIP メトリック値
  このスタティック経路情報を 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。
  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

  このスタティック経路情報の優先度を、1〜254 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。

[説明]

IPv4 スタティック経路 (静的経路) 情報を設定します。

RIP メトリック値は、スタティック経路情報を RIP に再配布するときのメトリック値を設定します。RIP に再配布したときは、設定した RIP メトリック値+1 のメトリック値で RIP テーブルに登録されます。

優先度は、同じあて先への経路情報が複数ある場合、優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。各ダイナミックルーティングプロトコルの優先度については、routemanage ip distance コマンドを参照してください。

優先度の設定値に関わらず、常にフローティング動作します。

remote インタフェースが通信可能な状態（リンクアップなど）であれば、スタティック経路情報をルーティングテーブルに追加します。通信不可能な状態（リンダウンなど）であれば、ルーティングテーブルから削除します。

複数のスタティック経路情報で ECMP 機能を使用するときは、あて先、RIP メトリック値、優先度がそれぞれ同じとなるようにスタティック経路情報を設定します。また、ECMP 機能を使用する場合は、routemanage ip ecmp mode コマンドで ECMP を使用するように設定します。ECMP となるスタティック経路情報は、同じあて先への経路情報ごとに装置全体で 4 個まで定義できます。

IPv4 スタティック経路情報は、本装置全体で次の数まで定義できます。

最大定義数	機種
256	MR1000

[注意]

同じあて先へのスタティック経路情報を複数設定する場合、以下の点に注意してください。

- 優先度が同じで、RIP メトリック値が違うスタティック経路情報は同時に設定できません。

[未設定時]

IPv4 スタティック経路情報を設定しないものとみなされます。

12.1.2.3　IPv6 関連情報

12.1.2.3.1　aaa user ip6 ifid

[機能]

IPv6 インタフェース ID の設定

[入力形式]

aaa [<group_id>] user [<number>] ip6 ifid <interfaceID>

[パラメタ]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略した場合は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
  グループ内での通し番号を、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)。
- depend-template
  テンプレート定義による設定を適用する場合に指定します。

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]

インタフェース ID を設定します。

[未設定時]

テンプレート定義による設定が適用されます。

12.1.2.3.2 aaa user ip6 route

[機能]

IPv6 スタティック経路情報の設定

[入力形式]

aaa [<group_id>] user [<number>] ip6 route <count> <address>/<prefixlen> <metric> <distance>

[パラメタ]

<group_id>

- グループ ID
  各グループを示す ID を 10 進数値の通し番号で指定します。
  省略した場合は、0 を指定したものとみなされます。

<number>

- AAA ユーザ情報定義番号
  グループ内での通し番号を、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>

- スタティック経路情報定義番号
  スタティック経路情報定義番号を、10 進数値で指定します。

範囲	機種
0〜255	MR1000

<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
  このスタティック経路情報を 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。
  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>

<distance>

- 優先度
  このスタティック経路情報の優先度を、1〜254 の 10 進数値で指定します。
  優先度は数値の小さい方がより高い優先度を示します。

[説明]

IPv6 スタティック経路 (静的経路) 情報を設定します。

RIP メトリック値は、スタティック経路情報を RIP に再配布するときのメトリック値を設定します。

RIP に再配布したときは、設定した RIP メトリック値+1 のメトリック値で RIP テーブルに登録されます。

優先度は、同じあて先への経路情報が複数ある場合、優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。各ダイナミックルーティングプロトコルの優先度については、routemanage ip6 distance コマンドを参照してください。

優先度の設定値に関わらず、常にフローティング動作します。

remote インタフェースが通信可能な状態（リンクアップなど）であれば、スタティック経路情報をルーティングテーブルに追加します。通信不可能な状態（リンダウンなど）であれば、ルーティングテーブルから削除します。

IPv6 スタティック経路情報は、本装置全体で次の数まで定義できます。

最大定義数	機種
256	MR1000

[注意]

同じあて先へのスタティック経路情報を複数設定する場合、以下の点に注意してください。

- 優先度が同じスタティック経路情報は同時に設定できません。

[未設定時]

IPv6 スタティック経路情報を設定しないものとみなされます。

第 13 章　装置情報の設定

13.1　SNMP 情報

13.1.1　snmp service

[機能]

SNMP エージェント機能および SNMP トラップ機能の設定

[入力形式]

snmp service <mode>

[パラメタ]

<mode>

- on
  SNMP エージェント機能および SNMP トラップ機能を有効にします。
- off
  SNMP エージェント機能および SNMP トラップ機能を停止します。

[説明]

SNMP エージェント機能および SNMP トラップ機能を有効にするかどうかを設定します。

[未設定時]

SNMP エージェント機能を停止するとみなされます。

```
snmp service off
```

13.1.2 snmp agent contact

[機能]

SNMP エージェント機能でのルータ管理者の設定

[入力形式]

snmp agent contact <syscontact>

[パラメタ]

<syscontact>

- ルータ管理者 (sysContact 値)
  本装置の管理者を表す MIB 変数 sysContact を、40 文字以内で指定します。

[説明]

SNMP エージェント機能でのルータ管理者を設定します。

[未設定時]

ルータ管理者を設定しないものとみなされます。

13.1.3　snmp agent sysname

[機能]

SNMP エージェント機能での機器名称の設定

[入力形式]

snmp agent sysname <sysname>

[パラメタ]

<sysname>

- 機器名称 (sysName 値)
  本装置の機器名称を表す MIB 変数 sysName を、32 文字以内で指定します。

[説明]

SNMP エージェント機能での機器名称を設定します。

[未設定時]

機器名称を設定しないものとみなされます。

13.1.4 snmp agent location

[機能]

SNMP エージェント機能での機器設置場所の設定

[入力形式]

snmp agent location <syslocation>

[パラメタ]

<syslocation>

- 機器設置場所 (sysLocation 値)
  本装置の管理者を表す MIB 変数 sysLocation を、72 文字以内で指定します。

[説明]

SNMP エージェント機能での機器設置場所を設定します。

[未設定時]

機器設置場所を設定しないものとみなされます。

13.1.5　snmp agent address

[機能]

SNMP エージェントアドレスの設定

[入力形式]

snmp agent address <address>

[パラメタ]

<address>

- エージェントアドレス
  本装置のエージェントアドレスを設定します。
  0.0.0.0 を指定した場合は、SNMP エージェントアドレスを削除します。
  指定可能な範囲は以下のとおりです。
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

[説明]

SNMP エージェントのアドレスを設定します。本設定は TRAP 送信時の自局アドレスにも使用されます。SNMP エージェント機能を使用する場合は必ず設定してください。

[未設定時]

エージェントアドレスを設定しないものとみなされます。その場合、TRAP パケットの自局 IP アドレスは不定となります。

13.1.6 snmp manager

[機能]

SNMP ホスト情報の設定

[入力形式]

snmp manager <manager_number> <address> <community> <trap> [<write>]

[パラメタ]

<manager_number>

- SNMP ホスト定義番号
  SNMP ホスト定義の通し番号を、0〜7 の 10 進数値で指定します。

<address>

- アクセス許可 / トラップ送信アドレス
  アクセス許可およびトラップを送信するあて先 IP アドレスを、XXX.XXX.XXX.XXX(XXX は 3 桁の 10 進数値) の形式で指定します。
  0.0.0.0 を指定すると、すべてのホストからのアクセスを許可し、trap 送信は行いません。
  指定可能な範囲は以下のとおりです。
  1.0.0.1 〜 126.255.255.254
  128.0.0.1 〜 191.255.255.254
  192.0.0.1 〜 223.255.255.254

<community>

コミュニティ名を指定します。

- コミュニティ名
  トラップを送信するときのコミュニティ名を、1〜32 文字で指定します。
- public
  任意の SNMP マネージャと通信する場合に指定します。

<trap>

トラップ送信するかどうかを指定します。

- on
  トラップ送信する場合に指定します。
- off
  トラップ送信しない場合に指定します。

<write>

SNMP マネージャからの書き込みを許可するかどうか指定します。

- enable
  SNMP マネージャからの書き込みを許可する場合に指定します。
- disable
  SNMP マネージャからの書き込みを許可しない場合に指定します。

省略した場合は、disable を指定したものとみなされます。

[説明]

SNMP ホストの情報を設定します。

[未設定時]

SNMP ホストの情報を設定しないものとみなされます。

13.2 システムログ情報

13.2.1 syslog server

[機能]

システムログ情報の受信サーバの設定

[入力形式]

syslog server <address>

[パラメタ]

<address>

- IP アドレス
  システムログ情報 (メッセージ) を受信するサーバの IP アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

[説明]

システムログ情報 (メッセージ) を受信するサーバを設定します。
以下に、システムログ情報の出力方法を示します。

1) “syslog server <address>” で設定した IP アドレスのホストに送信する。
2) dsplog コマンドで表示する。

[未設定時]

システムログ情報を受信するサーバを指定しないものとみなされます。

13.2.2　syslog pri

[機能]

システムログ情報の出力対象プライオリティの設定

[入力形式]

syslog pri <mode>

[パラメタ]

<mode>

- プライオリティ

  システムログ情報を出力する対象となるプライオリティを、以下の中から指定します。複数指定する場合は、","(カンマ) で区切ります。

  error　プライオリティLOG_ERROR を対象とする場合に指定します。

  warn　プライオリティLOG_WARNING を対象とする場合に指定します。

  notice　プライオリティLOG_NOTICE を対象とする場合に指定します。

  info　プライオリティLOG_INFO を対象とする場合に指定します。

[説明]

システムログ情報を出力する対象となるプライオリティを指定します。

[未設定時]

何も指定しないものとみなされ、システムログ情報は収集されません。

13.2.3 syslog facility

[機能]

システムログ情報のファシリティの設定

[入力形式]

syslog facility <num>

[パラメタ]

<num>

- ファシリティ
  システムログ情報のファシリティを、0〜23 の 10 進数値で設定します。

[説明]

システムログ情報のファシリティを指定します。

[未設定時]

0 を指定したものとみなされます。

```
syslog facility 0
```

13.2.4　syslog security

[機能]

システムログ情報の出力対象セキュリティの設定

[入力形式]

syslog security <securetype>

[パラメタ]

<securetype>

- セキュリティ対象
  セキュリティログ情報の出力対象を、以下の中から指定します。
  複数指定する場合は、","(カンマ) で区切ります。

  ipfilter　IP filter モジュールを対象とする場合に指定します。

  nat　NAT モジュールを対象とする場合に指定します。

  ppp　PPP モジュールを対象とする場合に指定します。

  dhcp　DHCP モジュールを対象とする場合に指定します。

  proxydns
  ProxyDNS モジュールを対象とする場合に指定します。

  none　すべてのモジュールを対象外とする場合に指定します。

[説明]

システムログ情報を出力する対象となるセキュリティを指定します。

[未設定時]

すべてを指定したものとみなされます。

```
syslog security ipfilter,nat,ppp,dhcp,proxydns
```

13.2.5 syslog dupcut

[機能]

システムログ情報の重複メッセージ出力の設定

[入力形式]

syslog dupcut <cut>

[パラメタ]

<cut>

- yes
  直前に出力されたメッセージが重複した場合、出力しません。
- no
  重複チェックを行わず、すべてのメッセージを出力します。

[説明]

システムログにメッセージを出力する際、直前に出力したメッセージと重複した場合に出力するかどうかを指定します。

[未設定時]

重複チェックを行わないものとみなされます。

```
syslog dupcut no
```

13.3　自動時刻設定情報

13.3.1　time auto server

[機能]

時刻情報の提供サーバの設定

[入力形式]

time auto server <address> <protocol>

[パラメタ]

<address>

- IPv4 アドレス
  時刻情報を提供しているサーバの IPv4 アドレスを指定します。
  DHCP サーバが広報する時刻提供サーバに従う場合は、0.0.0.0 を指定します。
  指定可能な範囲は以下のとおりです。

  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

- IPv6 アドレス
  時刻情報を提供しているサーバの IPv6 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  ::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<protocol>

使用するプロトコルを指定します。

- time
  TIME プロトコル (TCP) を使用する場合に指定します。
- sntp
  簡易 NTP プロトコル (UDP) を使用する場合に指定します。
- dhcp
  DHCP サーバから広報される TIME プロトコルまたは簡易 NTP に従います。

[説明]

時刻提供サーバの情報を設定します。
time auto server の<address>で指定した時刻提供サーバから、<protocol>で指定したプロトコルを使用して、自動的に時刻を設定します。
本装置のインタフェースが DHCP クライアントとして動作している場合に限り、<protocol>で dhcp を指定することができます。この場合、DHCP サーバが広報する時刻提供サーバから指定されたプロトコルを使用して設定します。また、TIME プロトコルと SNTP が同時に広報された場合には、SNTP を優先します。

[未設定時]

自動時刻設定を行わないものとみなされます。

13.3.2 time auto interval

[機能]

時刻情報の自動設定間隔の設定

[入力形式]

time auto interval <time>

[パラメタ]

<time>

時刻情報を設定する間隔を指定します。

- start
  電源投入時またはリセット時に一度だけ、時刻情報を設定する場合に指定します。
- 間隔
  時刻情報を設定する間隔を、0 秒～最大 10 日の範囲で指定します。単位は、d(日)、h(時)、m(分)、s(秒) のどれかを指定します。

[説明]

自動時刻を設定する間隔を設定します。

[未設定時]

時刻提供サーバを使用する場合だけ、電源投入時またはリセット時に一度だけ時刻情報設定するものとみなされます。

```
time auto interval start
```

13.3.3　time zone

[機能]

時刻情報のタイムゾーンの設定

[入力形式]

time zone <offset>

[パラメタ]

<offset>

- 差分
  本装置が使用するタイムゾーンを指定します。
  GMT(グリニッジ標準時間) からの時差を指定します。日本で使用する場合は、0900 を指定してください。

[説明]

タイムゾーンを設定します。

[未設定時]

```
time zone 0
```

13.4 ProxyDNS 情報

13.4.1 proxydns domain

[機能]

プロキシ DNS の順引き動作条件の設定

[入力形式]

proxydns domain <count> <qtype> <qname> <address>/<mask> reject (転送要求の破棄)
proxydns domain <count> <qtype> <qname> <address>/<mask> static <ipaddress> (固定 DNS サーバ指定)
proxydns domain <count> <qtype> <qname> <address>/<mask> to <remote_number> (相手ネットワークの DNS サーバ指定)
proxydns domain <count> <qtype> <qname> <address>/<mask> on <remote_number> [<route>] (相手ネットワーク指定)

[パラメタ]

<count>

- 転送先定義番号

  転送先定義番号として、0〜31 の 10 進数値を指定します。

  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転送先定義番号が存在する場合は、既存定義の前に挿入されます。

<qtype>

- 問い合わせタイプ番号

  1〜11、または 13〜65535 の 10 進数値を指定します。

  以下に、問い合わせタイプの一部分を示します。

名称	番号	説　明
A	1	ホスト・アドレス
NS	2	ドメインに対して認証されたネーム・サーバ
CNAME	5	別名(Alias名、ドメイン名)
SOA	6	ゾーン管理開始
PTR	12	ドメイン名空間の他の部分へのポインタ
HINFO	13	ホストが使用するCPUとOS
MX	15	ドメインに対するメール交換
SRV	33	サービス

- any

  PTR(12) を除くすべてのタイプを対象する場合に指定します。

<qname>

- ホスト名

  条件となるホスト名を、80 文字以内で指定します。

  ホスト名には、以下のワイルドカードを使用できます。

  - *(アスタリスク)

    0 文字以上の任意の文字列とみなされます。

  - ?(クェスチョンマーク)

    任意の一文字とみなされます。

以下に、ワイルドカードを使用したホスト名の記述例および一致例を示します。

www.*.com

以下のどの文字列とも一致するとみなされます。

・www.testa.com

・www.test1.test.com

test 以下のどの文字列とも一致するとみなされます。

・www.test.com

・test.com

・test.co.jp

www.test?.com

以下のどの文字列とも一致するとみなされます。

・www.test1.com

・www.test2.com

・www.testA.com

なお、ホスト名をチェックするときに、大文字と小文字の区別はされません。

<address>/<mask>

対象となる送信元 IPv4 アドレス / マスクビット数または送信元 IPv6 アドレス / プレフィックス長を指定します。

- 送信元 IPv4 アドレス / マスクビット数 (またはマスク値)
  対象となる送信元 IPv4 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。
- 送信元 IPv6 アドレス / プレフィックス長
  対象となる送信元 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
  すべてのアドレスを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) または 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。

<ipaddress>

- DNS サーバ IP アドレス
  要求を転送する DNS サーバの IPv4 アドレスまたは IPv6 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

IPv4: 1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

IPv6: ::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<remote_number>

- 転送先相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。

範囲	機種
0～99	MR1000

<route>

DNS 問い合わせにより経路を設定するかどうかを設定します。

- on
  経路を設定します。
- off
  経路を設定しません。

省略した場合は、off を指定したものとみなされます。

[説明]

プロキシ DNS の順引き動作条件を設定します。
各コマンドについて説明します。

転送要求の破棄

proxydns domain <count> <qtype> <qname> <address>/<mask> reject

指定した DNS 要求の転送を無効にするフィルタを設定します。

<qname>で指定するホスト名は、DNS データベースに登録されていても、そのホスト (群) へのアクセスを制限する場合に使用します。条件と一致した場合は破棄されます。

固定 DNS サーバの指定

proxydns domain <count> <qtype> <qname> <address>/<mask> static <ipaddress>

指定した DNS 要求の転送先 IP アドレスを指定します。
以下の場合に有効です。

- 専用線に接続する場合
- LAN 側に DNS サーバが存在する場合
- リモート側の DNS サーバを固定にする場合

相手ネットワークの DNS サーバ指定

proxydns domain <count> <qtype> <qname> <address>/<mask> to <remote_number>

回線から通知された DNS サーバを使用します。

相手情報でマルチルーティングを定義している場合は、その設定に従います。回線切断中は、接続先情報の接続優先順位に従います。

相手ネットワークの指定

proxydns domain <count> <qtype> <qname> <address>/<mask> on <remote_number> [<route>]

回線から通知された DNS サーバへ指定のネットワークを使用して DNS 要求を転送します。回線切断中は、接続先情報の接続優先順位に従います。

<route>に on を指定すると DNS 要求を転送した相手ネットワークへの経路を動的に設定します。

[未設定時]

プロキシ DNS の順引き動作条件を設定しないものとみなされます。

13.4.2　proxydns domain move

[機能]

プロキシ DNS の順引き動作条件の順序の変更

[入力形式]

proxydns domain move <count> <new_count>

[パラメタ]

<count>

- 変更前転送先定義番号
  順序を変更する転送先定義番号を指定します。

<new_count>

- 新しい転送先定義番号
  <count>に対して、新しい順序を指定します。
  すで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]

プロキシ DNS の順引き動作条件の順序を変更します。
すでに存在する転送先定義番号と同じ番号を指定した場合には、指定した定義の前に挿入されます。

13.4.3 proxydns address

[機能]

プロキシ DNS の逆引き動作条件の設定

[入力形式]

proxydns address <count> <address>/<mask> reject (転送要求の破棄)
proxydns address <count> <address>/<mask> static <ipaddress> (固定 DNS サーバ指定)
proxydns address <count> <address>/<mask> to <remote_number> (相手ネットワークの DNS サーバ指定)
proxydns address <count> <address>/<mask> on <remote_number> [<route>] (相手ネットワーク指定)

[パラメタ]

<count>

- 転送先定義番号
  転送先定義番号として、0〜31 の 10 進数値を指定します。
  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転送先定義番号が存在する場合は、既存定義の前に挿入されます。

<address>/<mask>

逆引き対象 IPv4 アドレス/マスクビット数または IPv6 アドレス/プレフィックス長を指定します。

- 逆引き対象 IPv4 アドレス/マスクビット数 (またはマスク値)
  逆引き対象 IPv4 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。
- 逆引き対象 IPv6 アドレス/プレフィックス長
  逆引き対象 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。
- any4
  IPv4 アドレスの逆引きのすべてを対象とする場合に指定します。
- any6
  IPv6 アドレスの逆引きのすべてを対象とする場合に指定します。
- any
  すべてのアドレスの逆引きを対象とする場合に指定します。

<ipaddress>

- DNS サーバ IP アドレス
  要求を転送する DNS サーバの IPv4 アドレスまたは IPv6 アドレスを指定します。
  指定可能な範囲は以下のとおりです。

  IPv4: 1.0.0.1 〜 126.255.255.254
  128.0.0.1 〜 191.255.255.254
  192.0.0.1 〜 223.255.255.254

  IPv6: ::2 〜 fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: 〜 feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

<remote_number>

- 転送先相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。

範囲	機種
0～99	MR1000

<route>

DNS 問い合わせにより経路を設定するかどうかを設定します。

- on
  経路を設定します。
- off
  経路を設定しません。

省略した場合は、off を指定したものとみなされます。

[説明]

プロキシ DNS の逆引き動作条件を設定します。
各コマンドについて説明します。

転送要求の破棄

proxydns address <count> <address>/<mask> reject
指定した DNS 要求の転送を無効にするフィルタを設定します。
<qname>で指定するホスト名は、DNS データベースに登録されていても、そのホスト (群) へのアクセスを制限する場合に使用します。条件と一致した場合は破棄されます。

固定 DNS サーバの指定

proxydns address <count> <address>/<mask> static <ipaddress>
指定した DNS 要求の転送先 IP アドレスを指定します。転送先への経路は、IP ルーティングにしたがって決められます。
以下の場合に有効です。

- 専用線に接続する場合
- LAN 側に DNS サーバが存在する場合
- リモート側の DNS サーバを固定にする場合

相手ネットワークの DNS サーバ指定

proxydns address <count> <address>/<mask> to <remote_number>
回線から通知された DNS サーバを使用します。
相手情報でマルチルーティングを定義している場合は、その設定に従います。回線切断中は、接続先情報の接続優先順位に従います。

相手ネットワークの指定

proxydns address <count> <address>/<mask> on <remote_number> [<route>]
回線から通知された DNS サーバへ指定のネットワークを使用して DNS 要求を転送します。
回線切断中は、接続先情報の接続優先順位に従います。
<route>に on を指定すると DNS 要求を転送した相手ネットワークへの経路を動的に設定します。

[未設定時]

プロキシ DNS の逆引き動作条件を設定しないものとみなされます。

13.4.4 proxydns address move

[機能]

プロキシ DNS の逆引き動作条件の順序の変更

[入力形式]

proxydns address move <count> <new_count>

[パラメタ]

<count>

- 変更前転送先定義番号
  順序を変更する転送先定義番号を指定します。

<new_count>

- 新しい転送先定義番号
  <count>に対して、新しい順序を指定します。
  すで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]

プロキシ DNS の逆引き動作条件の順序を変更します。
すでに存在する転送先定義番号と同じ番号を指定した場合には、指定した定義の前に挿入されます。

13.4.5　proxydns unicode

[機能]

プロキシ DNS の問い合わせパケットの透過の可否の設定

[入力形式]

proxydns unicode <action>

[パラメタ]

<action>

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する場合に指定します。
- reject
  該当するパケットを破棄する場合に指定します。

[説明]

プロキシ DNS の問い合わせ名 (QNAME) に非表示文字が含まれる場合に、その問い合わせのパケットを透過するかどうかを設定します。

[未設定時]

該当パケットを破棄するものとみなされます。

```
proxydns unicode reject
```

13.5 ホストデータベース情報

13.5.1 host name

[機能]

ホストデータベース情報のホスト名の設定

[入力形式]

host <number> name <name>

[パラメタ]

<number>

- 定義番号

  ホストデータベース情報の定義番号を、0～63 の 10 進数値で指定します。

<name>

- ホスト名

  ホスト名を、英数字、"-"(ハイフン)、"."(ピリオド) で構成される 80 文字以内の ASCII 文字列で指定します。

[説明]

本装置配下に接続されたホストのホスト名をホストデータベースに設定します。

本コマンドは、簡易 DNS サーバ機能、DHCP スタティック機能、リモートパワーオン機能から利用されます。

以下に、各機能とパラメタの関係を示します。

パラメタ / 機能	name	ip_address	ip6_address	mac_address	rpon
簡易DNSサーバ	○	○	○	－	－
DHCPスタティック	－	○	－	○	－
リモートパワーオン (手動/schedule)	－	－	－	○	○

○:有効、－:無効

[未設定時]

ホストデータベースを設定しないものとみなされます。

13.5.2　host ip address

[機能]

ホストデータベース情報の IP アドレスの設定

[入力形式]

host <number> ip address <ip_address>

[パラメタ]

<number>

- 定義番号

  ホストデータベース情報の定義番号を、0～63 の 10 進数値で指定します。

<ip_address>

- IP アドレス

  ホストの IP アドレスを指定します。

[説明]

本装置配下に接続されたホストの IP アドレスをホストデータベースに設定します。

本コマンドは、簡易 DNS サーバ機能、DHCP スタティック機能、リモートパワーオン機能から利用されます。

以下に、各機能とパラメタの関係を示します。

パラメタ / 機能	name	ip_address	ip6_address	mac_address	rpon
簡易DNSサーバ	○	○	○	－	－
DHCPスタティック	－	○	－	○	－
リモートパワーオン (手動/schedule)	－	－	－	○	○

○:有効、－:無効

[未設定時]

ホストデータベースを設定しないものとみなされます。

13.5.3 host ip6 address

[機能]

ホストデータベース情報の IPv6 アドレスの設定

[入力形式]

host <number> ip6 address <ip6_address>

[パラメタ]

<number>

- 定義番号

  ホストデータベース情報の定義番号を、0～63 の 10 進数値で指定します。

<ip6_address>

- IPv6 アドレス

  ホストの IPv6 アドレスを指定します。

[説明]

本装置配下に接続されたホストの IPv6 アドレスをホストデータベースに設定します。
本コマンドは、簡易 DNS サーバ機能から利用されます。
以下に、各機能とパラメタの関係を示します。

パラメタ / 機能	name	ip_address	ip6_address	mac_address	rpon
簡易DNSサーバ	○	○	○	―	―
DHCPスタティック	―	○	―	○	―
リモートパワーオン (手動/schedule)	―	―	―	○	○

○:有効、―:無効

[未設定時]

ホストデータベースを設定しないものとみなされます。

13.5.4　host mac

[機能]

ホストデータベース情報の MAC アドレスの設定

[入力形式]

host <number> mac <mac_address>

[パラメタ]

<number>

- 定義番号

  ホストデータベース情報の定義番号を、0～63 の 10 進数値で指定します。

<mac_address>

- MAC アドレス

  ホストの 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。

[説明]

本装置配下に接続されたホストの MAC アドレスをホストデータベースに設定します。

本コマンドは、簡易 DNS サーバ機能、DHCP スタティック機能、リモートパワーオン機能から利用されます。

以下に、各機能とパラメタの関係を示します。

パラメタ / 機能	name	ip_address	ip6_address	mac_address	rpon
簡易DNSサーバ	○	○	○	－	－
DHCPスタティック	－	○	－	○	－
リモートパワーオン (手動/schedule)	－	－	－	○	○

○:有効、－:無効

[未設定時]

ホストデータベースを設定しないものとみなされます。

13.5.5 host rpon

[機能]

ホストデータベース情報のリモートパワーオン対象の設定

[入力形式]

host <number> rpon <rpon>

[パラメタ]

<number>

- 定義番号

  ホストデータベース情報の定義番号を、0～63 の 10 進数値で指定します。

<rpon>

リモートパワーオンの対象にするかどうかを設定します。

- off

  リモートパワーオンの対象にしません。

[説明]

本装置配下に接続されたホストのリモートパワーオン情報をホストデータベースに設定します。

本コマンドは、簡易 DNS サーバ機能、DHCP スタティック機能、リモートパワーオン機能から利用されます。

以下に、各機能とパラメタの関係を示します。

パラメタ / 機能	name	ip_address	ip6_address	mac_address	rpon
簡易DNSサーバ	○	○	○	―	―
DHCPスタティック	―	○	―	○	―
リモートパワーオン (手動/schedule)	―	―	―	○	○

○:有効、―:無効

[未設定時]

リモートパワーオンの対象にするものとみなされます。

13.6　パスワード情報

13.6.1　password set

[機能]

管理者パスワードの設定

[入力形式]

password set <password> [encrypted] [<mode>]

[パラメタ]

<password>

- パスワード
  パスワードの文字列を、0x21,0x23～0x7e の 16 文字以内の ASCII 文字で指定します。
- 暗号化されたパスワード
  show コマンドで表示される暗号化されたパスワードを 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

- 暗号化パスワード指定
  <password>に暗号化されたパスワードを指定する場合に指定します。

<mode>

- パスワード問い合わせモード
  WWW ブラウザを使用して本装置の操作、表示、保守を行う場合に、処理メニュー毎にパスワードを問い合わせるかどうかを設定できます。
  パスワードの問い合わせモードを、以下の数値から選んで論理和し、0～7 の 8 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。

  4　「操作メニュー」でパスワードを問い合わせます。
  2　「表示メニュー」でパスワードを問い合わせます。
  1　「保守メニュー」でパスワードを問い合わせます。

[説明]

本装置に管理者がログオンするためのパスワードを設定します。
本パスワードでログオンすると、すべてのコマンドとメニューが使用できます。
パスワードは、本コマンドで設定した直後に有効となります。

[注意]

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

[未設定時]

管理者パスワードは設定されていません。

13.6.2 password user set

[機能]

ユーザパスワードの設定

[入力形式]

password user set <password> [encrypted] [<mode>]

[パラメタ]

<password>

- パスワード
  パスワードの文字列を、0x21,0x23～0x7e の 16 文字以内の ASCII 文字で指定します。
- 暗号化されたパスワード
  show コマンドで表示される暗号化されたパスワードを 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

- 暗号化パスワード指定
  <password>に暗号化されたパスワードを指定する場合に指定します。

<mode>

- パスワード有効モード
  ユーザパスワードで使用できるモードを、以下の数値から選んで論理和し、1～7 の 8 進数値で指定します。省略した場合は、7 を指定したものとみなされ、設定コマンドおよび設定メニュー以外が使用できます。

  4 操作コマンドおよび操作メニューが使用できます。

  2 表示コマンドおよび表示メニューが使用できます。

  1 保守コマンドおよび保守メニューが使用できます。

[説明]

本装置にユーザがログオンするためのパスワードを設定します。
ユーザパスワードでログオンすると、設定コマンドおよび設定メニューは使用できません。また、<mode>で無効にしたコマンドおよびメニューも使用できません。
パスワードは、本コマンドで設定した直後に有効となります。

[注意]

ftp 接続時には、ユーザパスワードは使用できません。
ユーザパスワードを設定する場合、管理者パスワードも設定してください。管理者パスワードを設定しない場合、パスワードなしで使用できます。また、管理者パスワードの<mode>でパスワードを問い合わせないようにしているモードは、ユーザパスワードの<mode>の設定に関わらず、パスワードなしでメニューが使用できます。
ユーザパスワードでログオンした場合、env コマンドで環境変数を設定できますが、設定した内容は保存されず、ログアウトすると設定した内容は破棄されます。
また、history コマンドは管理者が実行したコマンドは表示されず、履歴番号は非連続になります。
show コマンドでは、暗号化されたパスワードが encrypted と共に表示されます。

[例]

```
# password set foo       (設定メニュー以外はパスワード入力不要)
# password user set bar  (設定コマンド以外は使用可能)
```

- コンソール、telnet の場合

  ログオンパスワードに foo を入力すると、すべてのコマンドを実行できます。

  ログオンパスワードに bar を入力すると、操作、表示および保守コマンドを実行できます。設定コマンドは実行できず、エラーが表示されます。

- WWW ブラウザの場合

  設定メニューを選択すると、パスワードが問い合わせられます。

  foo を入力すると、設定メニューの内容が表示されます。

  bar を入力しても、設定メニューの内容は表示されません。

  操作メニュー、表示メニュー、保守メニューの内容はパスワードなしで表示されます。

```
# password set foo 7       (すべてのメニューでパスワードが必要)
# password user set bar 2  (表示コマンドのみ使用可)
```

- コンソール、telnet の場合

  ログオンパスワードに foo を入力すると、すべてのコマンドを実行できます。

  ログオンパスワードに bar を入力すると、表示コマンドは実行できますが、設定、操作および保守コマンドは実行できず、エラーが表示されます。

- WWW ブラウザの場合

  設定、操作、保守メニューを選択すると、パスワードが問い合わせられます。

  foo を入力すると、いずれのメニューも内容が表示されます。

  bar を入力すると、表示メニューの内容は表示されますが、設定、操作および保守メニューの内容は表示されず、再びパスワードが問い合わせられます。

13.7　スケジュール情報

13.7.1　schedule at

[機能]

システムスケジュールの日時指定コマンドの設定

[入力形式]

schedule <number> at <day> <time> <command>

[パラメタ]

<number>

スケジュール定義を指定します。

- スケジュール定義番号
  スケジュール定義番号を、0～15 の 10 進数値で指定します。
- any
  スケジュール定義番号を省略する場合に指定します。

<day>

- 日
  スケジュールの実行日または開始日を、1～31 の 10 進数値で指定します。
- 曜日
  スケジュールの実行曜日または開始曜日を、以下の中から指定します。

sun	日曜日
mon	月曜日
tue	火曜日
wed	水曜日
thu	木曜日
fri	金曜日
sat	土曜日

  複数の曜日を指定する場合は、","(カンマ) で区切って指定します。
- any
  スケジュールの実行日または開始日を毎日とする場合に指定します。
  電源投入時または再起動時は、本パラメタを指定してください。

<time>

- 実行時間
  実行する時、分を、0～9 の 4 桁の 10 進数値で指定します (例: 0635 = 午前 6 時 35 分、2330 = 午後 11 時 30 分)。
- pwon
  電源投入時に実行する場合に指定します。
- rset
  システム再起動時、または電源投入時に実行する場合に指定します。

<command>

実行するコマンド 文字列を指定します。

- isdnstat -drc
  課金情報をクリアする場合に指定します。
- mdmstat -drc
  モデム統計情報をクリアする場合に指定します。
- disconnect all
  強制切断する場合に指定します。
- rpon all
  リモートパワーオンを実行する場合に指定します。

[説明]

システムスケジュールを設定します。
このスケジュールに従って、指定した時刻にコマンド を実行します。

[未設定時]

スケジュール情報を設定しないものとみなされます。

13.7.2 schedule in

[機能]

システムスケジュールの期間指定動作の設定

[入力形式]

schedule <number> in <day> <time> <action>

[パラメタ]

<number>

スケジュール定義を指定します。

- スケジュール定義番号
  スケジュール定義番号を、0～15 の 10 進数値で指定します。
- any
  スケジュール定義番号を省略する場合に指定します。

<day>

- 日
  スケジュールの実行日または開始日を、1～31 の 10 進数値で指定します。
- 曜日
  スケジュールの実行曜日または開始曜日を、以下の中から指定します。

sun	日曜日
mon	月曜日
tue	火曜日
wed	水曜日
thu	木曜日
fri	金曜日
sat	土曜日

  複数の曜日を指定する場合は、","(カンマ) で区切って指定します。
- any
  スケジュールの実行日または開始日を毎日とする場合に指定します。
  電源投入時または再起動時は、本パラメタを指定してください。

<time>

- 開始時刻～終了時刻
  開始時刻～終了時刻を、0～9 の 4 桁の 10 進数値で指定します。開始時刻と終了時刻の間は、"-"(ハイフン) でつなぎます (例: 0900-1700 = 午前 9 時から午後 5 時まで、2300-0800 = 午後 11 時から翌午前 8 時まで)。

<action>

動作を指定します。

- diallock
  <time>で指定した時刻の間、自動発信を抑止します。
- dialreject
  <time>で指定した時刻の間、自動着信を抑止します。
- timerctl
  <time>で指定した時間の間、無通信監視タイマによる切断を行いません。ただし、相手情報の接続保持情報が設定が無効 (off) の場合は対象になりません。

[説明]

システムスケジュールを設定します。
このスケジュールに従って、指定した時刻の間、ある状態を維持することができます。

[未設定時]

スケジュール情報を設定しないものとみなされます。

13.7.3 schedule syslog

[機能]

システムスケジュールのシステムログ出力可否の設定

[入力形式]

schedule <number> syslog <syslog>

[パラメタ]

<number>

スケジュール定義を指定します。

- スケジュール定義番号
  スケジュール定義番号を、0～15 の 10 進数値で指定します。
- any
  スケジュール定義番号を省略する場合に指定します。

<syslog>

- yes
  コマンド実行時の出力をシステムログで行う場合に指定します。
- no
  コマンド実行時の出力をシステムログで行わない場合に指定します。

[説明]

スケジュールによって起動されたコマンドが出力するメッセージを、システムログに出力するかどうかを指定します。

スケジュールで起動するコマンドが指定されている場合にだけ有効です。

[未設定時]

コマンド実行時の出力をシステムログに出力しないものとみなされます。

```
schedule <number> syslog no
```

13.8　電話番号変更予約情報

13.8.1　dnconvinfo date

[機能]

電話番号変更予約の日時の設定

[入力形式]

dnconvinfo <index> date <date>

[パラメタ]

<index>

- 登録番号
  電話番号変更予約情報の登録番号を、0～3 の 10 進数値で指定します。

<date>

- 変更日時
  変更日時を、yymmddHHMM の形式で指定します。

yy	西暦の下 2 桁を指定します。西暦 2036 年まで指定できます。
mm	月を、1～12 の 10 進数値で指定します。
dd	日付を、1～31 の 10 進数値で指定します。
HH	時間を、0～23 の 10 進数値で指定します。
MM	分を、0～59 の 10 進数値で指定します。

[説明]

すべての構成定義情報の電話番号を一括変更する場合に必要となる、電話番号変更日時を設定します。
変更処理は、以下の 2 つの方法によって行われます。

- 時刻指定によって、スケジュール機能から自動的に実施します。
  なお、スケジュール機能によって実施した場合は、定義情報が保存され、システムがリセットされます。
- 時刻指定によらずに、コマンドで実施します。

[注意]

以下に、スケジュール機能によって電話番号変更を実施する場合の注意事項を示します。

- 装置の時刻を正しく設定してください。
- 実施時刻に、装置の電源を投入しておいてください。

[例]

以下に、構成定義情報に定義されている電話番号 123456789 を、1999 年 1 月 1 日午前 2 時にすべて 999999999 へ変更する場合の設定例を示します。

```
# dnconvinfo 0 date 9901010200
# dnconvinfo 0 dial 0 123456789 99999999
# show dnconvinfo
0 date 9901010200
0 dial 0 123456789 99999999
#
```

[未設定時]

電話番号変更予約情報を設定しないものとみなされます。

13.8.2　dnconvinfo dial

[機能]

電話番号変更予約の電話番号の設定

[入力形式]

dnconvinfo <index> dial <count> <src_number> <dst_number>

[パラメタ]

<index>

- 登録番号
  電話番号変更予約情報の登録番号を、0～3 の 10 進数値で指定します。

<count>

- 電話番号情報定義番号
  電話番号情報の定義番号を、0～3 の 10 進数値で指定します。

<src_number>

- 変更前電話番号
  変更対象の電話番号を、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。

<dst_number>

- 変更後電話番号
  変更後の電話番号を、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。

[説明]

すべての構成定義情報の電話番号を一括変更する場合に必要となる、変更電話番号を設定します。
変更処理は、以下の 2 つの方法によって行われます。

- 時刻指定によって、スケジュール機能から自動的に実施します。
  なお、スケジュール機能によって実施した場合は、定義情報が保存され、システムがリセットされます。
- 時刻指定によらずに、コマンドで実施します。

[注意]

以下に、スケジュール機能によって電話番号変更を実施する場合の注意事項を示します。

- 装置の時刻を正しく設定してください。
- 実施時刻に、装置の電源を投入しておいてください。

[例]

以下に、構成定義情報に定義されている電話番号 123456789 を、1999 年 1 月 1 日午前 2 時にすべて 999999999 へ変更する場合の設定例を示します。

```
# dnconvinfo 0 date 9901010200
# dnconvinfo 0 dial 0 123456789 to 99999999
# show dnconvinfo
0 date 9901010200
0 dial 0 123456789 to 99999999
#
```

[未設定時]

電話番号変更予約情報を設定しないものとみなされます。

13.9　ファームウェア更新情報

13.9.1　updateinfo

[機能]

ファームウェア更新情報の設定

[入力形式]

updateinfo <host> <user> <password> <pathname>

[パラメタ]

<host>

更新するファームウェアの転送元ホスト (ftp サーバ) を、以下の形式で指定します。ホスト名を指定する場合は、ホストデータベース情報に該当するホスト名が登録されているか、または本装置が DNS サーバを使用できる状態でなければなりません。

- ホスト名
  ホスト名を、0x21,0x23～0x7e の 128 文字以内の ASCII 文字列で指定します。
- IPv4 アドレス
  指定可能な範囲は以下のとおりです。

  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

- IPv6 アドレス
  指定可能な範囲は以下のとおりです。

  ::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

  リンクローカルアドレスを指定する場合、アドレスに続けて"%<interface>" を指定して、どのインタフェースを使用するのか指定してください。たとえば、"fe80::1%lan0"のように指定します。

<user>

- ユーザ名
  ftp ユーザ名を、0x21,0x23～0x7e の 16 文字以内の ASCII 文字列で指定します。

<password>

- パスワード
  ftp パスワードを、0x21,0x23～0x7e の 32 文字以内の ASCII 文字列で指定します。anonymous FTP サーバの場合は、管理者のメールアドレスを指定します。

<pathname>

- パス名
  更新するファームウェアの ftp サーバ上のパス名を、0x21,0x23～0x7e の 80 文字以内の ASCII 文字列で指定します。

[説明]

ファームウェアを更新するための情報を設定します。
update コマンドで ftp サーバ上のファームウェアを取得する場合は、必ず本コマンドを実行してください。

[未設定時]

ファームウェア更新情報を設定しないものとみなされます。

13.10　その他

13.10.1　addact

[機能]

コマンド実行予約の設定

[入力形式]

addact <index> <date> <command>

[パラメタ]

<index>

- 登録番号
  コマンド実行予約情報の登録番号を指定します。必ず 0 を指定してください。

<date>

- 実行日時
  コマンド実行日時を、yymmddHHMM の形式で指定します。

yy	西暦の下 2 桁を指定します。西暦 2036 年まで指定できます。
mm	月を、1〜12 の 10 進数値で指定します。
dd	日付を、1〜31 の 10 進数値で指定します。
HH	時間を、0〜23 の 10 進数値で指定します。
MM	分を、0〜59 の 10 進数値で指定します。

<command>

実行するコマンド文字列を指定します。

- reset config1
  構成定義 1 に切替えて再起動する場合に指定します。
- reset config2
  構成定義 2 に切替えて再起動する場合に指定します。

上記以外のコマンドを指定した場合の動作は保証されません。

[説明]

コマンド実行予約を設定します。

[注意]

以下に、スケジュール機能によってコマンドを実行する場合の注意事項を示します。

- 装置の時刻を正しく設定してください。
- 実施時刻に、装置の電源を投入しておいてください。

[例]

以下に、1999 年 1 月 1 日 午前 2 時 に構成定義 2 に切替えて再起動する場合の設定例を示します。

```
# addact 0 9901010200 reset config2
# show addact
0 9901010200 reset config2
#
```

[未設定時]

コマンドの実行予約を行わないものとみなされます。

13.10.2　watchdog service

[機能]

ウォッチドッグリセットの設定

[入力形式]

watchdog service <mode>

[パラメタ]

<mode>

- on
  ウォッチドッグリセット機能を起動する場合に指定します。
- off
  ウォッチドッグリセット機能を停止する場合に指定します。

[説明]

ウォッチドッグリセット機能の起動または停止を設定します。
<mode>に"on"を指定した場合、本装置がハングアップすると 16～48 秒以内にリセットがかかり再起動します。
<mode>に"off"を指定した場合、本装置がハングアップしてもリセットがかかりません。
本設定は構成定義を保存した後、本装置のリセットまたは電源の再投入を行うことによって反映されます。

[未設定時]

ウォッチドッグリセット機能は起動とみなされます。

```
watchdog service on
```

13.10.3 consoleinfo

[機能]

シリアルコンソール接続サービスの設定

[入力形式]

consoleinfo autologout <time>

[パラメタ]

<time>

- 強制ログアウト時間

  シリアルコンソールでログインしたままコマンド実行が行われない状態が続いたときに強制ログアウトさせる時間を、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) のどれかを指定します。

  0 秒を指定した場合には、強制ログアウトしません。

[説明]

シリアルコンソールでログインしたまま<time>で指定した時間内にコマンド実行されなかった場合、強制的にログアウトさせるように設定します。

[未設定時]

強制ログアウトさせないものとみなされます。

```
consoleinfo autologout 0s
```

13.10.4　telnetinfo

[機能]

TELNET 接続サービスの設定

[入力形式]

telnetinfo autologout <time>

[パラメタ]

<time>

- 自動切断時間

  telnet 接続したクライアントからコマンド入出力が行われない状態で自動切断するまでの時間を、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) のどれかを指定します。

[説明]

TELNET コネクションの入出力がない場合にコネクションを切断するまでの時間を設定します。

[未設定時]

TELNET コネクションの入出力の監視を行わないものとみなされます。

```
telnetinfo autologout 0s
```

13.10.5 sysdown harderr thermal

[機能]

温度異常時の動作の設定

[入力形式]

sysdown harderr thermal <mode>

[パラメタ]

<mode>

- yes
  システムダウンさせる場合に指定します。
- no
  運用を継続する場合に指定します。

[説明]

温度異常時の動作を設定します。

[未設定時]

温度異常時に運用を継続するものとみなされます。

```
sysdown harderr thermal no
```

13.10.6　page

[機能]

画面単位表示モード の設定

[入力形式]

page <mode>

[パラメタ]

<mode>

- on
  画面単位表示モード にします。
- off
  画面単位表示モード を解除します。

[説明]

画面単位表示モード にするかどうかを指定します。
画面単位表示モード にすると、コマンド 実行時に暗黙的に more コマンド を使うようになり、コマンド の出力を画面単位に進めたり戻したりできるようになります。
画面単位表示モード を解除した場合には、コマンド の出力は通常どおり止まること無く表示されます。画面単位表示モード を解除していても、more コマンド を使うことによりコマンド の出力を画面単位に表示できます。
本コマンド の設定は、本コマンド を実行した直後から有効になります。enable コマンド を実行する必要はありません。

[注意]

画面単位表示は、画面サイズが 24 行 80 桁であるものとして動作します。画面サイズが 24 行 80 桁以外の場合には、env コマンド で環境変数 LINES と COLUMNS に行数と桁数を設定してください。設定しない場合には表示が乱れます。詳しくは more コマンド および env コマンド を参照してください。

[未設定時]

画面単位表示モード を解除するものとみなされます。

```
page off
```

13.10.7 mflag

[機能]

CE 保守ログインの可否の設定

[入力形式]

mflag <mode>

[パラメタ]

<mode>

- on
  CE 専用パスワードによるログインを許可する場合に指定します。
- off
  CE 専用パスワードによるログインを拒否する場合に指定します。

[説明]

CE 保守ログインを許可するかどうかを設定します。

[未設定時]

CE 専用パスワードによるログインを拒否するものとみなされます。

```
mflag off
```

13.10.8　sysname

[機能]

本装置の名称の設定

[入力形式]

sysname <name>

[パラメタ]

<name>

- ルータ名称
  本装置の名称を、0x21,0x23～0x7e の 32 文字以内の ASCII 文字列で指定します。

[説明]

本装置の名称を設定します。
ここで設定した名称は、DHCP クライアント機能で DHCP サーバに対して広報されます。
本コマンドで設定する名称は、SNMP で使用する MIB 変数 sysName としても使用することができます。その場合、snmp agent sysname コマンドで設定している sysName を削除しておくことで本コマンドで設定したホスト名が sysName として使用されます。
本コマンドと snmp agent sysname コマンドとはネットワーク動作として直接の関連性はありませんが、ネットワークの管理上、同じ名称に統一するべきです。

[未設定時]

本装置の名称を設定しないものとみなされます。

13.10.9 loopback ip address

[機能]

loopback インタフェース追加 IP アドレスの設定

[入力形式]

loopback ip address [<number>] <address>

[パラメタ]

<number>

- 追加 IP アドレス定義番号

  追加 IP アドレス定義番号として 0 を指定します。

  省略した場合は、0 とを指定したものとみなされます。

<address>

- IP アドレス

  loopback インタフェースに割り当てる IP アドレスを指定します。IP アドレスに 0.0.0.0 を指定するとその定義番号を持った IP アドレスを無効にします。

  loopback インタフェースに割り当てた IP アドレスを通信に使う場合には、以下の範囲で通信可能なアドレスを設定してください。

  1.0.0.1 ～ 126.255.255.254

  128.0.0.1 ～ 191.255.255.254

  192.0.0.1 ～ 223.255.255.254

[説明]

loopback インタフェースに追加 IP アドレスを設定します。なお、loopback インタフェースの IP アドレスとしてはすでに 127.0.0.1 が設定されています。

[注意]

loopback インタフェースにはホストアドレスだけ設定可能であり、ネットマスク長は 32 固定です。
他のインタフェースと違うネットワークの IP アドレスを設定する必要があります。

[未設定時]

追加 IP アドレスなしとしてみなします。

```
loopback ip address <number> 0.0.0.0
```

13.10.10　loopback ip ospf use

[機能]

OSPF 利用可否の設定

[入力形式]

loopback ip ospf use <mode> [<area_number>]

[パラメタ]

<mode>

- off
  OSPF を利用しません。
- on
  OSPF を利用します。

<area_number>

- エリア定義番号
  OSPF を利用する場合は、エリアの定義番号を指定します。
  省略した場合は、0 を指定したものとみなされます。

範囲	機種
0～2	MR1000

[説明]

loopback インタフェースで OSPF を利用するかどうかと、属するエリアの定義番号を設定します。
<mode>で on を設定した場合でも、127.0.0.1 の IP アドレスは OSPF の対象外となります。
OSPF は、本装置全体で以下の数まで定義できます。

最大定義数	機種
100	MR1000

[注意]

OSPF の利用は、"ospf ip area id"を設定した場合にだけ有効です。

[未設定時]

OSPF を使用しないものとみなされます。

```
loopback ip ospf use off
```

13.10.11 loopback mpls ldp interface-label

[機能]

PHP の無効化

[入力形式]

loopback mpls ldp interface-label <mode>

[パラメタ]

<mode>

- off
  インタフェースの IP アドレスにラベルを割り当てません。
- on
  インタフェースの IP アドレスにラベルを割り当てます。

[説明]

インタフェースの IP アドレスに対してラベルを割り当てるかどうかを指定します。割り当てた場合は, インタフェース宛の LSP の PHP を無効にすることができます。

[注意]

MPLS トンネル接続機能を使用する場合、自側エンドポイントと IP アドレスが同一の時、本設定に依らず、PHP 機能は無効となります。

[未設定時]

off が選択されたものとして動作します。

```
loopback mpls ldp interface-label off
```

13.10.12　serverinfo ftp

[機能]

FTP サーバ機能の設定

[入力形式]

serverinfo ftp ip <mode>

[パラメタ]

<mode>

- on
  FTP サーバ機能を有効にします。
- off
  FTP サーバ機能を停止します。

[説明]

FTP サーバ機能を有効にするかどうかを設定します。

[未設定時]

FTP サーバ機能を有効にするとみなされます。

```
serverinfo ftp ip on
```

13.10.13 serverinfo ftp ip6

[機能]

FTP サーバ機能の IPv6 の設定

[入力形式]

serverinfo ftp ip6 <mode>

[パラメタ]

<mode>

- on
  FTP サーバ機能を有効にします。
- off
  FTP サーバ機能を停止します。

[説明]

FTP サーバ機能の IPv6 を有効にするかどうかを設定します。

[未設定時]

FTP サーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo ftp ip6 on
```

13.10.14　serverinfo sftp

[機能]

SSH FTP サーバ機能の設定

[入力形式]

serverinfo sftp ip <mode>

[パラメタ]

<mode>

- on
  SSH FTP サーバ機能を有効にします。
- off
  SSH FTP サーバ機能を停止します。

[説明]

SSH FTP サーバ機能を有効にするかどうかを設定します。
本設定が off、かつ、serverinfo ssh ip コマンドの設定が off の場合、sftp クライアントからの IPv4 アドレスでの接続要求は拒否されます。
本設定が off、かつ、serverinfo ssh ip コマンドの設定が on の場合、sftp クライアントからの IPv4 アドレスでの接続要求は一旦接続されてすぐに切断されます。

[注意]

本設定を有効にすると、本装置電源投入時および reset コマンド実行時に ssh ホスト認証鍵を生成するようになり、数十秒～数分の処理時間を要します。
ssh ホスト認証鍵の生成が完了した後に ssh 接続できるようになります。

[未設定時]

SSH FTP サーバ機能を有効にするとみなされます。

```
serverinfo sftp ip on
```

13.10.15 serverinfo sftp ip6

[機能]

SSH FTP サーバ機能の IPv6 の設定

[入力形式]

serverinfo sftp ip6 <mode>

[パラメタ]

<mode>

- on
  SSH FTP サーバ機能の IPv6 を有効にします。
- off
  SSH FTP サーバ機能の IPv6 を停止します。

[説明]

SSH FTP サーバ機能の IPv6 を有効にするかどうかを設定します。
本設定が off、かつ、serverinfo ssh ip6 コマンドの設定が off の場合、sftp クライアントからの IPv6 アドレスでの接続要求は拒否されます。
本設定が off、かつ、serverinfo ssh ip6 コマンドの設定が on の場合、sftp クライアントからの IPv6 アドレスでの接続要求は一旦接続されてすぐに切断されます。

[注意]

本設定を有効にすると、本装置電源投入時および reset コマンド実行時に ssh ホスト認証鍵を生成するようになり、数十秒～数分の処理時間を要します。
ssh ホスト認証鍵の生成が完了した後に ssh 接続できるようになります。

[未設定時]

SSH FTP サーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo sftp ip6 on
```

13.10.16　serverinfo telnet

[機能]

TELNET サーバ機能の設定

[入力形式]

serverinfo telnet ip <mode>

[パラメタ]

<mode>

- on
  TELNET サーバ機能を有効にします。
- off
  TELNET サーバ機能を停止します。

[説明]

TELNET サーバ機能を有効にするかどうかを設定します。

[未設定時]

TELNET サーバ機能を有効にするとみなされます。

```
serverinfo telnet ip on
```

13.10.17　serverinfo telnet ip6

[機能]

TELNET サーバ機能の IPv6 の設定

[入力形式]

serverinfo telnet ip6 <mode>

[パラメタ]

<mode>

- on
  TELNET サーバ機能を有効にします。
- off
  TELNET サーバ機能を停止します。

[説明]

TELNET サーバ機能の IPv6 を有効にするかどうかを設定します。

[未設定時]

TELNET サーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo telnet ip6 on
```

13.10.18　serverinfo ssh

[機能]

SSH ログインサーバ機能の設定

[入力形式]

serverinfo ssh ip <mode>

[パラメタ]

<mode>

- on
  SSH ログインサーバ機能を有効にします。
- off
  SSH ログインサーバ機能を停止します。

[説明]

SSH ログインサーバ機能を有効にするかどうかを設定します。
本設定が off、かつ、serverinfo sftp ip コマンドの設定が off の場合、ssh クライアントからの IPv4 アドレスでの接続要求は拒否されます。
本設定が off、かつ、serverinfo sftp ip コマンドの設定が on の場合、ssh クライアントからの IPv4 アドレスでの接続要求は一旦接続されてすぐに切断されます。

[注意]

本設定を有効にすると、本装置電源投入時および reset コマンド実行時に ssh ホスト認証鍵を生成するようになり、数十秒～数分の処理時間を要します。
ssh ホスト認証鍵の生成が完了した後に ssh 接続できるようになります。

[未設定時]

SSH ログインサーバ機能を有効にするとみなされます。

```
serverinfo ssh ip on
```

13.10.19 serverinfo ssh ip6

[機能]

SSH ログインサーバ機能の IPv6 の設定

[入力形式]

serverinfo ssh ip6 <mode>

[パラメタ]

<mode>

- on
  SSH ログインサーバ機能の IPv6 を有効にします。
- off
  SSH ログインサーバ機能の IPv6 を停止します。

[説明]

SSH ログインサーバ機能の IPv6 を有効にするかどうかを設定します。
本設定が off、かつ、serverinfo sftp ip6 コマンドの設定が off の場合、ssh クライアントからの IPv6 アドレスでの接続要求は拒否されます。
本設定が off、かつ、serverinfo sftp ip6 コマンドの設定が on の場合、ssh クライアントからの IPv6 アドレスでの接続要求は一旦接続されてすぐに切断されます。

[注意]

本設定を有効にすると、本装置電源投入時および reset コマンド実行時に ssh ホスト認証鍵を生成するようになり、数十秒～数分の処理時間を要します。
ssh ホスト認証鍵の生成が完了した後に ssh 接続できるようになります。

[未設定時]

SSH ログインサーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo ssh ip6 on
```

13.10.20　serverinfo http

[機能]

HTTP サーバ機能の設定

[入力形式]

serverinfo http ip <mode>

[パラメタ]

<mode>

- on
  HTTP サーバ機能を有効にします。
- off
  HTTP サーバ機能を停止します。

[説明]

HTTP サーバ機能を有効にするかどうかを設定します。

[未設定時]

HTTP サーバ機能を有効にするとみなされます。

```
serverinfo http ip on
```

13.10.21 serverinfo http ip6

[機能]

HTTP サーバ機能の IPv6 の設定

[入力形式]

serverinfo http ip6 <mode>

[パラメタ]

<mode>

- on
  HTTP サーバ機能を有効にします。
- off
  HTTP サーバ機能を停止します。

[説明]

HTTP サーバ機能の IPv6 を有効にするかどうかを設定します。

[未設定時]

HTTP サーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo http ip6 on
```

13.10.22　serverinfo dns

[機能]

DNS サーバ機能の設定

[入力形式]

serverinfo dns ip <mode>

[パラメタ]

<mode>

- on
  DNS サーバ機能を有効にします。
- off
  DNS サーバ機能を停止します。

[説明]

DNS サーバ（スタティック）機能および ProxyDNS 機能を有効にするかどうかを設定します。

[未設定時]

DNS サーバ機能を有効にするとみなされます。

```
serverinfo dns ip on
```

13.10.23 serverinfo dns ip6

[機能]

DNS サーバ機能の IPv6 の設定

[入力形式]

serverinfo dns ip6 <mode>

[パラメタ]

<mode>

- on
  DNS サーバ機能を有効にします。
- off
  DNS サーバ機能を停止します。

[説明]

DNS サーバ（スタティック）機能および ProxyDNS 機能の IPv6 を有効にするかどうかを設定します。

[未設定時]

DNS サーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo dns ip6 on
```

13.10.24　serverinfo sntp

[機能]

SNTP サーバ機能の設定

[入力形式]

serverinfo sntp ip <mode>

[パラメタ]

<mode>

- on
  SNTP サーバ機能を有効にします。
- off
  SNTP サーバ機能を停止します。

[説明]

SNTP サーバ機能を有効にするかどうかを設定します。

[未設定時]

SNTP サーバ機能を有効にするとみなされます。

```
serverinfo sntp ip on
```

13.10.25 serverinfo sntp ip6

[機能]

SNTP サーバ機能の IPv6 の設定

[入力形式]

serverinfo sntp ip6 <mode>

[パラメタ]

<mode>

- on
  SNTP サーバ機能を有効にします。
- off
  SNTP サーバ機能を停止します。

[説明]

SNTP サーバ機能の IPv6 を有効にするかどうかを設定します。

[未設定時]

SNTP サーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo sntp ip6 on
```

13.10.26　serverinfo time ip tcp

[機能]

TCP による TIME サーバ機能の設定

[入力形式]

serverinfo time ip tcp <mode>

[パラメタ]

<mode>

- on
  TCP による TIME サーバ機能を有効にします。
- off
  TCP による TIME サーバ機能を停止します。

[説明]

TCP による TIME サーバ機能を有効にするかどうかを設定します。

[未設定時]

TCP による TIME サーバ機能を有効にするとみなされます。

```
serverinfo time ip tcp on
```

13.10.27 serverinfo time ip6 tcp

[機能]

TCP による TIME サーバ機能の IPv6 の設定

[入力形式]

serverinfo time ip6 tcp <mode>

[パラメタ]

<mode>

- on
  TCP による TIME サーバ機能を有効にします。
- off
  TCP による TIME サーバ機能を停止します。

[説明]

TCP による TIME サーバ機能の IPv6 を有効にするかどうかを設定します。

[未設定時]

TCP による TIME サーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo time ip6 tcp on
```

13.10.28　serverinfo time ip udp

[機能]

UDP による TIME サーバ機能の設定

[入力形式]

serverinfo time ip udp <mode>

[パラメタ]

<mode>

- on
  UDP による TIME サーバ機能を有効にします。
- off
  UDP による TIME サーバ機能を停止します。

[説明]

UDP による TIME サーバ機能を有効にするかどうかを設定します。

[未設定時]

UDP による TIME サーバ機能を有効にするとみなされます。

```
serverinfo time ip udp on
```

13.10.29 serverinfo time ip6 udp

[機能]

UDP による TIME サーバ機能の IPv6 の設定

[入力形式]

serverinfo time ip6 udp <mode>

[パラメタ]

<mode>

- on
  UDP による TIME サーバ機能を有効にします。
- off
  UDP による TIME サーバ機能を停止します。

[説明]

UDP による TIME サーバ機能の IPv6 を有効にするかどうかを設定します。

[未設定時]

UDP による TIME サーバ機能の IPv6 を有効にするとみなされます。

```
serverinfo time ip6 udp on
```

第 14 章　制御コマンド

14.1 装置の制御

14.1.1 logon

[機能]

コマンドの使用開始の宣言

[入力形式]

logon

[オプション]

なし

[パラメタ]

なし

[説明]

コマンドの使用開始を宣言します。
本コマンドは、シリアルポートに接続されたコンソールから実行できます。

[注意]

シリアルポートに接続されたコンソールから logon している最中に、他のプログラムからコマンドを実行することはできません。他のプログラムからコマンドを実行する場合は、“14.1.2 exit” を実行して、コンソールでのコマンド使用を終了してください。
本コマンド実行直後、以下のメッセージが表示されて処理を待たされることがあります。
本装置内で他の処理が行なわれているためで、処理が終了するまでしばらくお待ちください。
なお、本メッセージは他のコマンドの使用の際にも表示されることがあります。

```
Waiting for completion of the other operation...
```

[例]

以下に、実行例を示します。

```
> logon
Password:
#
```

14.1.2　exit

[機能]

コマンドの使用終了

[入力形式]

exit

[オプション]

なし

[パラメタ]

なし

[説明]

コンソールからのコマンド操作を終了します。
telnet でリモート端末から使用している場合は、telnet コネクションを切断します。

[例]

以下に、実行例を示します。

```
# exit
>
```

14.1.3 save

[機能]

構成定義情報の保存

[入力形式]

save [<config>]

[オプション]

なし

[パラメタ]

<config>
以下のどちらかの保存先構成定義を指定します。省略時は、動作中の構成定義に保存します。

- config1
  不揮発性メモリの構成定義 1 に保存する。
- config2
  不揮発性メモリの構成定義 2 に保存する。

[説明]

構成定義情報を保存します。
構成定義コマンドによって設定または変更した構成定義情報を、FLASH メモリに格納します。
格納する構成定義情報のサイズが、FLASH メモリ上の構成定義保存領域のサイズを超えていた場合は、以下のエラーメッセージを出力します。また、FLASH メモリへの格納は行われません。

```
save failed: config too big
```

また、ハードエラーを検出し、システムダウンペンディング状態では、以下のメッセージを出力し、異常終了します。

```
detected HARD ERROR, cannot execute
```

本装置の通信負荷が高い状態などでは、以下のメッセージを出力し、異常終了することがあります。
この場合には通信負荷を停止して再度本コマンドを実行してください。

```
save failed: config write error
```

[例]

以下に、実行例を示します。

```
# save
```

14.1.4　clear statistics

[機能]

統計情報のクリア

[入力形式]

clear statistics

[オプション]

なし

[パラメタ]

なし

[説明]

全ての統計情報をクリアします。

[例]

```
# clear statistics
#
```

14.1.5 load

[機能]

構成定義の読み込み

[入力形式]

load <config>

[オプション]

なし。

[パラメタ]

<config>

以下のどれかを指定します。

- config1
  FLASH メモリの構成定義 1 を読み込む
- config2
  FLASH メモリの構成定義 2 を読み込む
- running
  動作中の構成定義を読み込む

[説明]

指定の構成定義を読み込みます。
設定中の内容は、すべて無効になります。
本装置の通信負荷が高い状態などでは、以下のメッセージを出力し、異常終了することがあります。
この場合には通信負荷を停止して再度本コマンドを実行してください。

```
load failed: config read error
```

[操作例]

```
# load config1
#
```

14.1.6　delete

[機能]

構成定義情報の削除

[入力形式]

delete <コマンド 名>

[オプション]

なし

[パラメタ]

<コマンド 名>

削除したい構成定義のコマンド 名を指定します。指定したコマンド 名に続く構成定義情報が削除されます。

[説明]

構成定義情報を削除します。

[例]

以下に、削除の操作例を示します。

1)　remote の情報をすべて削除する場合

```
# delete remote
```

2)　remote 0 の情報をすべて削除する場合

```
# delete remote 0
```

3)　remote 0 ap 0 の情報をすべて削除する場合

```
# delete remote 0 ap 0
```

4)　remote 0 ap 0 name の情報を削除する場合

```
# delete remote 0 ap 0 name
```

14.1.7 enable

[機能]

構成定義情報の動的変更

[入力形式]

enable [all]

[オプション]

なし

[パラメタ]

- all
  動的定義変更に対応していないコマンド の変更も含めて、すべての構成定義情報を有効にします。

[説明]

各コマンド で設定または変更した構成定義情報を、装置の再起動を行わずに有効にします。
以下の構成定義情報を追加または変更した場合には、以下のエラーメッセージを表示し、動的定義変更はできません。reset で再起動してください。

- watchdog service

```
enable: need reset
```

追加または変更した構成定義情報がない場合には、以下のメッセージが表示されます。

```
enable : system configuration is not changed.
```

また、動的定義変更に対応していないコマンド を変更し、all を指定しないで enable コマンド を実行した場合には、以下のメッセージに続いて、有効になっていないコマンド が表示されます。すべての変更を有効にしたい場合には、all を指定して enable コマンド を再度、実行するか、または、save コマンド を実行後に reset コマンド を実行してください。

```
enable : following system configuration is not applied.
```

[注意]

enable コマンド を実行した場合、構成定義情報の変更内容によっては装置内部のアド レス情報などを再設定するために、一旦、通信インタフェースをダウンさせます。そのため、enable コマンド 実行時に通信が途切れますのでご注意ください。(参照：付録 B enable コマンド 実行時の影響について) また、複数インタフェースを変更するなど、一度に大量のコマンド を投入して enable コマンド を実行した場合、enable コマンド の完了まで時間がかかる場合があります。目安としては、1 つの remote や lan など、1 インタフェース分程度の変更を行なうごとに enable コマンド を実行するようにして、一度に大量の変更を行なわないようにしてください。

[例]

以下に、実行例を示します。

```
# enable
```

14.1.8 reset

[機能]

装置の再起動

[入力形式]

reset [<mode>]

[オプション]

なし

[パラメタ]

<mode>

再起動のモードを指定します。

- clear
  設定をご購入時の状態に戻し、装置を再起動します。
- config1
  構成定義 1 に切替えて、装置を再起動します。
- config2
  構成定義 2 に切替えて、装置を再起動します。

[説明]

装置を再起動します。
構成定義情報を変更した場合は、本コマンドを実行して装置を再起動してください。変更した内容は、再起動後に有効となります。
装置を再起動しないで変更した内容を有効にしたい場合は、“14.1.7 enable” を実行します。
本装置の通信負荷が高い状態などでは、以下のメッセージを出力し、異常終了することがあります。
この場合には通信負荷を停止して再度本コマンドを実行してください。

```
reset: default configuration change error
```

```
reset: configuration change error
```

[例]

以下に、実行例を示します。

```
# reset
```

14.1.9　update

[機能]

ファームウェアの更新

[入力形式]

update

[オプション]

なし

[パラメタ]

なし

[説明]

ファームウェア更新情報にしたがって他システムからファームウェアを読み込み、FLASH メモリの内容を書き替えます。

以下に、ファームウェア更新手順の概要を示します。

1) ファームウェア更新情報を設定します。(""“13.9.1 updateinfo”"参照)

   # updateinfo ....

   # save

   # enable

2) ファームウェアを更新します。

   # update

3) 装置を再起動します。

   # reset

また、ハード エラーを検出し、システムダウンペンディング状態では、以下のメッセージを出力し、異常終了します。

```
detected HARD ERROR, cannot execute
```

[例]

以下に、実行例を示します。

```
> logon
Password:
# updateinfo 192.168.1.2 mr mr-passwd /MR/MRSOFT.ftp
# save
# enable
# update
    --ファイル転送(FTP)--
    --ファイルチェック(md5)--
    --バージョンチェック(ファームウェア種別とバージョン)--
    --FLASHメモリへの書き込み--
# reset
    --更新したファームウェアでシステムを再起動--
>
```

14.1.10 date

[機能]

絶対時間の設定/表示

[入力形式]

date [<yymmddHHMMSS>]

[オプション]

なし

[パラメタ]

<yymmddHHMMSS>

日付および時刻を指定します。

yy 西暦の下 2 桁を指定します。00～36 を指定した場合は、西暦 2000 年以降とみなされます。

mm 月を、1～12 の 10 進数値で指定します。

dd 日付を、1～31 の 10 進数値で指定します。

HH 時間を、0～23 の 10 進数値で指定します。

MM 分を、0～59 の 10 進数値で指定します。

SS 秒を、0～59 の 10 進数値で指定します。

指定した日付と時間は、ローカルタイムで処理されます。

[説明]

絶対時間を設定します。

パラメタなしで本コマンドを実行した場合は、現在の日付と時刻を表示します。

本コマンドをパラメタなしで実行すると、"Fri Jun 27 18:36:53 2001"の形式で現在の日付と時刻が表示されます。

コマンド実行時にパラメタで日付と時刻を指定した場合、その情報を絶対時間として設定します。

[例]

以下に、実行例を示します。

- 現在の日付と時刻を設定する場合

```
# date 010716155300
#
```

- 現在の日付と時刻を表示する場合

```
# date
Mon Jun 30 15:53:01 2001
#
```

[注意]

構成定義情報にタイムゾーン (time zone <offset>) が指定されていない状態では GMT (グリニッジ標準時間) として表示/設定されます。

14.1.11　rdate

[機能]

リモートホストの時刻を本装置の絶対時間に設定

[入力形式]

rdate

[オプション]

なし

[パラメタ]

なし

[説明]

タイムサーバから現在時刻を取得し、本装置の絶対時間として設定します。
“13.3.1 time auto server” で指定したサーバから、現在時刻を取得します。

[例]

以下に、サーバから現在時刻を取得する場合の実行例を示します。

```
# rdate
Mon Jun 30 10:30:00 2001
#
```

14.1.12 dnconv

[機能]

電話番号変更処理の実施

[入力形式]

dnconv <index>

[オプション]

なし

[パラメタ]

<index>

一括変更処理の対象とする、電話番号変更予約情報を指定します。

- 0～3
  電話番号変更予約情報 (dnconvinfo) の登録番号を指定します。
- all
  登録されている電話番号変更情報 (dnconvinfo) すべてを対象とする場合に指定します。

[説明]

電話番号変更予約情報に従って、構成定義情報に登録されている電話番号を一括変更します。

[注意]

本コマンドでは、電話番号一括変更処理後の構成定義情報の保存 (save)、およびシステムのリセット (reset) は行いません。

[例]

以下に、実行例を示します。

- 特定の電話番号変更予約情報の一括変更処理

```
# dnconv 1
 ....
# dnconv 3
 ....
# save
# reset
>
```

- すべての電話番号変更予約情報の一括変更処理

```
# dnconv all
 ....
# save
# reset
>
```

14.1.13　upnpctl

[機能]

UPnP の制御

[入力形式]

upnpctl clear portmapping

[オプション]

なし

[パラメタ]

clear portmapping

ポートマッピング情報を強制的に削除します。

[説明]

UPnP のポートマッピング情報を強制的に削除します。

ポートマッピングを設定した UPnP クライアントを使用している場合、UPnP クライアントを再起動する必要があります。

14.1.14 vrrpctl

[機能]

VRRP 機能の制御

[入力形式]

vrrpctl preempt on {<lan_number>|all} [{<vrid>|all} [<interval>]]

[オプション]

なし

[パラメタ]

<lan_number>

コマンド適用対象の LAN インタフェースを指定します。

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。

範囲	機種
0〜19	MR1000

- all
  すべての LAN インタフェースを適用対象とする場合に指定します。

<vrid>

コマンド適用対象の VRRP グループを指定します。

- VRID
  対象の LAN インタフェースに設定されている VRRP グループの VRID を、1〜255 の 10 進数値で指定します。
- all
  対象の LAN インタフェースに設定されているすべての VRRP グループを適用対象とする場合に指定します。

<interval>

- プリエンプトモード ON 時間
  プリエンプトモードを ON にする時間を、1〜900 の範囲で指定します。単位は秒です。
  省略した場合は、VRRP グループに設定された VRRP-AD 送信間隔の 3 倍+5 秒の時間を指定したものとみなされます。
  また、VRRP-AD 送信間隔の 3 倍+5 より小さい値を指定しても VRRP-AD 送信間隔の 3 倍+5 秒を指定されたものとして動作します。

[説明]

VRRP グループの動作を、一時的にプリエンプトモードが ON に設定されたものとして動作させます。
これにより、プリエンプトモードが OFF に設定された自装置 VRRP グループが現在のマスタルータより優先度の高いバックアップルータである場合、マスタルータに状態を切り戻すことができます。
コマンドが正常に実行された場合は以下のメッセージを出力します。

```
vrrpctl: command accepted vrid<vrid>
```

<vrid>　コマンドが適用された VRRP グループを示します。

指定された自装置 VRRP グループのプリエンプトモードが ON であったり、現在のマスタルータの優先度のほうが高い場合、要求は無視され以下のエラーメッセージを出力します。なお、VRID が指定されなかった場合はエラーメッセージは出力されません。

```
vrrpctl: not command accept vrid<vrid>
```

<vrid>　コマンドが適用されなかった VRRP グループを示します。

また、有効ではない VRRP グループが指定された場合は以下のエラーメッセージを出力します。

```
vrrpctl: Bad vrid<vrid> provided
```

<vrid>　有効ではない VRRP グループを示します。

[例]

以下に、現在はマスタルータとして動作している待機設定ルータで lan0 の VRID が 10 の VRRP グループを、優先度の高い仮想ルータへきり戻しを行う場合の実行例を示します。

```
# vrrpctl preempt on 0 10
vrrpctl: command accepted vrid10
#
```

14.1.15 arp

[機能]

システムの ARP 情報表示
システムの ARP 情報の追加/削除

[入力形式]

表示: arp [<address> | -a]

削除: arp -d {<address> | all | -a }

[オプション]

-a すべてのエントリを表示します。

-d 指定された IP アドレスの ARP エントリを削除します。all または -a が指定された場合にはすべてのエントリを削除します。

[パラメタ]

<address>

- IP アドレス
  IP アドレスを指定します。

[説明]

ARP 情報の表示および削除を行います。

14.2　リモートパワーオンの制御

14.2.1　rpon

[機能]

リモートパワーオン機能のための MagicPacket の送信

[入力形式]

rpon <host_number>

[オプション]

なし

[パラメタ]

<host_number>

- ホストデータベース定義番号
  MagicPacket 送出先のホストデータベース定義番号を指定します。
- all
  ホストデータベースに登録されたリモートパワーオン対象の全ホスト。

[説明]

ホストデータベース定義番号により指定されたホストに対して、MagicPacket を送出します。<host_number>が指定されないか、有効範囲から外れているか、またはそのホスト情報に MAC アドレスが設定されていない場合にはなにもしません。<hosts_number>に all が指定されている場合は、MAC アドレスが設定されておりリモートパワーオン非対象ホストではない全ホストに対して MagicPacket を送出します。

[例]

以下に、実行例を示します。

```
# rpon 2
#
```

14.3 LAN の制御

14.3.1 open

[機能]

LAN の閉塞状態解除の指示

[入力形式]

open <lan_number>

[オプション]

なし

[パラメタ]

<lan_number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。

範囲	機種
0～19	MR1000

- all
  すべての LAN の閉塞状態解除を行います。

[説明]

LAN の閉塞状態の解除を行います。

[注意]

閉塞状態で、かつ LAN ポートがリンクを確立できない状態で open コマンドを実行した場合には、再度閉塞状態にはならずに、リンクランプが消灯から橙点滅に変化します。この際には、次回リンクが確立したときに通信が可能となります。

[例]

以下に、lan 0 の閉塞を解除する場合の実行例を示します。

```
# open 0
#
```

14.3.2　close

[機能]

LAN の閉塞状態移行の指示

[入力形式]

close <lan_number>

[オプション]

なし

[パラメタ]

<lan_number>

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。

範囲	機種
0～19	MR1000

- all
  すべての LAN の閉塞状態への移行を行います。

[説明]

LAN を閉塞状態へ移行します。

[注意]

閉塞状態では、リンクランプは消灯します。
閉塞状態では、LAN 定義が無い場合と同じ状態になります。ランプ表示もそれに準じたものになります。
閉塞状態に移行すると、当該の LAN ポートではパケットを受信できなくなります。このため当該の LAN ポートで TCP による通信を行なっている場合には、無応答になります。telnet による操作時、ブラウザからの操作時には注意してください。

[例]

以下に、lan 0 を閉塞状態に移行する場合の実行例を示します。

```
# close 0
#
```

14.4 回線の制御

14.4.1 connect

[機能]

回線の接続、または閉塞状態解除の指示

[入力形式]

connect <remote_number> <ap_number> [<id> <password>]
connect <ap_name>

[オプション]

なし

[パラメタ]

<remote_number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。

範囲	機種
0～99	MR1000

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。

範囲	機種
0～99	MR1000

<ap_name>

- 接続先名
  接続または閉塞状態を解除する接続先を指定します。
- all
  すべての接続先の閉塞状態を解除します。

<id>

- 送信認証 ID(最大 64 文字)

<password>

- 送信認証パスワード (最大 64 文字)

[説明]

回線接続、または閉塞状態の解除を行います。
指定した接続先に ISDN / PPPoE を利用して通信する場合には接続処理を行います。また、常時接続機能を使用する場合 ("remote ap keep connect"を設定した場合) には、閉塞状態を解除します。
<ap_name>を指定する場合には、同じ接続先名が複数定義されていると一番小さい定義番号の接続先に対してだけ動作します。
接続ごとに認証 ID、認証パスワードを変更する場合には、<id>、<password>を指定します。

[注意]

閉塞状態で、かつ回線が接続不可能な状態で connect コマンドを実行した場合には、再度閉塞状態になります。

この場合、閉塞状態を解除するには、再度 connect コマンドを実行する必要があります。

[例]

以下に、tokyo という名前の接続先と接続する場合の実行例を示します。

```
# connect tokyo
#
```

14.4.2 addlink

[機能]

MP 使用時のチャネル数増加

[入力形式]

addlink <remote_number> <ap_number>
addlink <ap_name>

[オプション]

なし

[パラメタ]

<remote_number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。

範囲	機種
0～99	MR1000

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。

範囲	機種
0～99	MR1000

<ap_name>

- 接続先名
  接続先の名前を指定します。

[説明]

MP で 1B 使用時に、チャネル数増加を設定します。

[例]

以下に、実行例を示します。

```
# addlink 0 0
#
```

14.4.3　disconnect

[機能]

回線の切断、または閉塞状態移行の指示

[入力形式]

接続先指定の切断
disconnect <remote_number> <ap_number>
disconnect <ap_name>
テンプレート着信での接続に対する切断
disconnect template <ifname>
disconnect template <template_number> [<user_id>]

[パラメタ]

<remote_number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。

範囲	機種
0〜99	MR1000

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。

範囲	機種
0〜99	MR1000

<ap_name>

切断、または閉塞状態に移行させる接続先を指定します。

- 接続先名
  接続先の名前を指定します。
- all
  すべての接続先の切断および閉塞状態への移行を行います。(テンプレート着信での接続も切断されます。)

<ifname>

- 切断するインタフェース名
  切断するインタフェースのインタフェース名 (例:rmt0) を指定します。

<temp_number>

切断するテンプレート定義番号を指定します。

- テンプレート定義番号
  テンプレート定義の通し番号を、10 進数値で指定します。

範囲	機種
0	MR1000

<user_id>

特定ユーザの接続を切断する場合にユーザ ID を指定します。

[説明]

回線切断、または閉塞状態への移行を行います。

指定した接続先に ISDN / PPPoE を利用して通信する場合には切断処理を行います。また、常時接続機能を使用する場合 ("remote ap keep connect"を設定した場合) には、閉塞状態への移行を行います。all を指定した場合には、すべての接続先の切断および閉塞状態への移行を行います。(テンプレート着信による接続も含まれます。)

[例]

以下に、tokyo という名前の接続先と切断する場合の実行例を示します。

```
# disconnect tokyo
#
```

14.4.4　dellink

[機能]

MP 使用時のチャネル数削減

[入力形式]

dellink <remote_number> <ap_number>
dellink <ap_name>

[オプション]

なし

[パラメタ]

<remote_number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。

範囲	機種
0～99	MR1000

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先の通し番号を、10 進数値で指定します。

範囲	機種
0～99	MR1000

<ap_name>

- 接続先名
  接続先の名前を指定します。

[説明]

MP で 2B 使用時に、チャネル数を削減します。

[例]

以下に、実行例を示します。

```
# dellink 0 0
#
```

14.4.5 timerctl start

[機能]

回線接続保持タイマの起動

[入力形式]

timerctl start [<time>]

[オプション]

なし

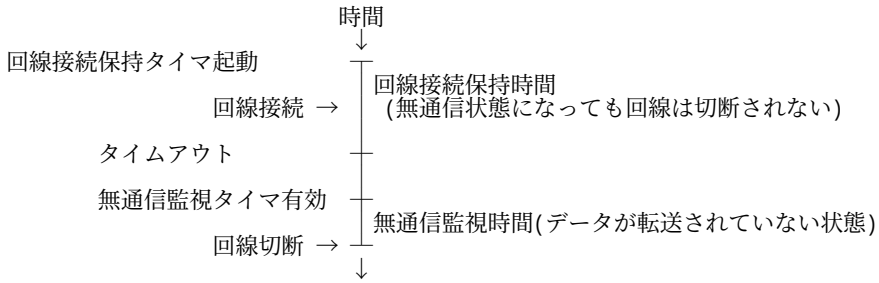
[パラメタ]

<time>

- 回線接続保持時間
  回線接続保持時間を、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) のどれかを指定します。

[説明]

回線接続保持タイマを起動します。
本コマンドは、回線が接続されているかどうかに限らず実行できます。
回線接続保持タイマは、本コマンドの実行によって起動し、タイムアウトまたは timerctl stop コマンド (“14.4.6 timerctl stop” を参照) の実行によって停止します。
time を省略した場合には、装置起動 / 再起動 / 設定反映の時点から最初の実行時については wan isdn keep time で設定した値を利用します。それ以外の実行時には前回利用した値が設定されたものとみなされます。
停止後は、無通信監視タイマによる接続時間の監視を再開します。
本コマンドは、回線が接続されているかどうかに限らず実行できます。以下に、回線の未接続時に本コマンドを実行した場合の流れを示します。



[注意]

回線接続保持タイマを起動すると、指定した接続保持時間内は無通信監視タイマによる切断を行いません。ただし、以下の場合には、回線接続を保持することができません。

- “14.4.3 disconnect” で、手動切断した場合
- 相手側から切断された場合
- “4.2.28 remote ap keep” で、「回線接続を保持しない」が設定されている場合 (例: remote 0 ap 0 keep off)

[例]

以下に、回線接続保持時間を 8 時間とする場合の実行例を示します。

```
# timerctl start 8h
#
```

14.4.6 timerctl stop

[機能]

回線接続保持タイマの停止

[入力形式]

timerctl stop

[オプション]

なし

[パラメタ]

なし

[説明]

回線接続保持タイマを停止します。

回線接続保持タイマは、“14.4.5 timerctl start” の実行によって起動され、タイムアウトまたは本コマンドの実行によって停止します。

停止後は、無通信監視タイマによる接続時間の監視を再開します。

[例]

以下に実行例を示します。

```
# timerctl stop
#
```

14.4.7　timerctl remain

[機能]

回線接続保持タイマの残り時間の表示

[入力形式]

timerctl remain

[オプション]

なし

[パラメタ]

なし

[説明]

回線接続保持タイマの残り時間を表示します。

回線接続保持タイマ起動中に本コマンドを実行すると、接続保持時間の残り時間が表示されます。回線接続保持タイマの停止中に本コマンドを実行した場合は、0 が表示されます。

[例]

以下に、回線接続保持タイマの起動中に本コマンドを実行した場合の実行例を示します。

```
# timerctl start 8h
# timerctl remain
7h
#
```

14.5 他装置の制御

14.5.1 telnet

[機能]

telnet サーバへの接続

[入力形式]

telnet [{-e <escape_char>|-E}] [-S <src_addr>] [-T <tos>] [{-4|-6}] <host> [<port>]

[オプション]

-e <escape_char>

エスケープ文字を指定します。

telnet 接続中にエスケープ文字キーに続けて"q"キーを入力すると、telnet 接続を強制的に切断することができます。

エスケープ文字としてコントロール文字を指定する場合、"^"に続けて文字を指定します。たとえば、CTRL+A であれば"^A"を指定します。

文字を複数指定した場合、最初の文字だけが有効となります。

省略時は、"^]"(CTRL+]) を指定したものとみなされます。

-E

エスケープ文字を無効にします。

-e オプションと共に指定してもエラーにはなりませんが、後から指定した方が有効になります。

-S <src_addr>

ソースアドレス (本ルータのアドレス) を、以下の形式で指定します。

- IPv4 アドレス
- IPv6 アドレス

<host>で指定するアドレスと同じバージョンおよび同じスコープ (範囲) のアドレスを指定してください。

省略時は、適切なアドレスが設定されます。

-T <tos>

TOS 値を 0～ff の範囲の 16 進数で指定します。

<host>が IPv6 アドレスの場合には指定できません。

省略時は、0 を指定したものとみなされます。

-4

<host>の IPv4 アドレスに telnet 接続する場合に指定します。

-6

<host>の IPv6 アドレスに telnet 接続する場合に指定します。

[パラメタ]

<host>

接続先ホスト (telnet サーバ) を、以下の形式で指定します。

- ホスト名
- IPv4 アドレス
- IPv6 アドレス

  リンクローカルアドレスを指定する場合、アドレスに続けて"%<interface>" を指定して、どのインタフェースを使用するのか指定してください。たとえば、"fe80::1%lan0"のように指定します。

<port>

ポート番号を 1～65535 の範囲の 10 進数で指定します。
省略時は、telnet ポート番号である 23 を指定したものとみなされます。

[説明]

telnet サーバが動作しているホストやルータに接続して、遠隔操作することができます。
telnet サーバから以下の情報を求められた場合には、本装置の情報 (括弧内の値) を通知します。

- 端末タイプ (VT100)
- 通信速度 (9600bps)
- 画面サイズ (画面行数、画面桁数)

[例]

以下に、実行例を示します。

```
# telnet 192.168.1.2                    他ルータにtelnet接続
Trying 192.168.1.2...                   接続手続き中
Connected to 192.168.1.2.               接続完了
Escape character is '^]'                エスケープ文字表示
login passwd:                           他ルータのパスワード入力
login OK.                               他ルータにログイン成功
# exit                                  他ルータのプロンプト表示、exit実行
Connection closed by foreign host.      切断
#                                       本ルータのプロンプト表示
```

14.6 その他の制御

14.6.1 ping

[機能]

ICMP エコー要求パケットの送信

[入力形式]

ping [-{r|v|rv}] [-S <src_addr>] [-T <ttl>] <host> [<timeout>]
ping -s [-{r|v|rv}] [-S <src_addr>] [-T <ttl>] <host> [<packetsize> [<count>]]

[オプション]

-s

1 秒間隔で ICMP ECHO_REQUEST を送信します。

-r

ルーティング制御を行わずに ICMP ECHO_REQUEST を送信します。

-v

冗長出力を有効にします。

-S <src_addr>

ソース IP アドレスを指定します。装置に定義されていないアドレスは指定できません。

-T <ttl>

TTL を 1～255 の範囲で指定します。

[パラメタ]

<host>

エコーテストの対象とする IP アドレスまたはホスト名を指定します。

ホスト名を指定する場合は、ホストデータベース情報に該当するホスト名が登録されているか、または本装置が DNS サーバを使用できる状態でなければなりません。

<timeout>

- タイムアウト時間

  ICMP ECHO_RESPONSE の応答待ち時間を、0 以上の 10 進数値 (単位:秒) で指定します。

  省略した場合は、20 秒を指定したものとみなされます。

<packetsize>

- パケットサイズ

  ICMP ECHO_REQUEST のパケットサイズを、0～5000 の 10 進数値 (単位:バイト) で指定します。

  省略した場合は、64 バイトを指定したものとみなされます。

<count>

- パケット送信回数

  ICMP ECHO_REQUEST の送信回数を、1 以上の 10 進数値で指定します。

  省略または 0 を指定した場合は、Ctrl+C を入力するまで無限となります。

[説明]

指定したホスト (IP アドレスまたはホスト名) に対して、ICMP ECHO_REQUEST を送信し、ICMP ECHO_RESPONSE の受信を確認します。

[例]

以下に、実行例を示します。

実行例 1　ping コマンドをオプションなしで実行した場合の実行例を示します。

```
# ping 192.168.1.1
192.168.1.1 is alive
#
```

実行例 2　ping コマンドの-s オプションで実行した場合の実行例を示します (1 秒間隔で 56 バイトの request を 5 回送信)。

```
# ping -s 192.168.1.1 56 5
PING 192.168.1.1: 56 data bytes.
64 bytes from 192.168.1.1 : icmp_seq=0. ttl=253. time=13.104 ms
64 bytes from 192.168.1.1 : icmp_seq=1. ttl=253. time=10.704 ms
64 bytes from 192.168.1.1 : icmp_seq=2. ttl=253. time=10.560 ms
64 bytes from 192.168.1.1 : icmp_seq=3. ttl=253. time= 9.888 ms
64 bytes from 192.168.1.1 : icmp_seq=4. ttl=253. time=13.056 ms

----192.168.1.1 PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms)  min/ave/max = 9.888/11.462/13.104
#
```

14.6.2 ping6

[機能]

ICMPv6 エコー要求パケットの送信

[入力形式]

ping6 <address>[%<interface>]

[オプション]

なし

[パラメタ]

<address>

- 送信先 IPv6 アドレス

  ICMPv6 送信先の IPv6 アドレスを指定します。

<interface>

- 送信先インタフェース名

  送信先 IPv6 アドレスが link-local scope の場合に、出力先インタフェースを指定します。link-local scope 以外の IPv6 アドレス指定時に指定した場合はエラーとなります。

[説明]

指定したホストに対して ICMPv6 ECHO_REQUEST を送信し、ICMPv6 ECHO_RESPONSE の受信を確認します。ホスト名での指定はできません。

[注意]

- ping6 の動作を途中で中断することはできません。
- ping6 の動作中に、CTRL-C を入力しないでください。

[例]

以下に実行例を示します。

```
# ping6 fe80::200:eff:fef1:dc%lan0
ping6 (56=40+8+8 bytes) fe80::200:eff:fef1:efa%lan0 --> fe80::200:eff:fef1:dc%lan0
16 bytes from fe80::200:eff:fef1:efa%lan0 icmp_seq=0 hlim=64 time=0.768ms
16 bytes from fe80::200:eff:fef1:efa%lan0 icmp_seq=0 hlim=64 time=0.691ms
16 bytes from fe80::200:eff:fef1:efa%lan0 icmp_seq=0 hlim=64 time=0.788ms
16 bytes from fe80::200:eff:fef1:efa%lan0 icmp_seq=0 hlim=64 time=0.732ms
16 bytes from fe80::200:eff:fef1:efa%lan0 icmp_seq=0 hlim=64 time=0.715ms
```

14.6.3　traceroute

[機能]

ネットワーク経路の表示

[入力形式]

traceroute [-S <src_addr>] [-M] <host> [<data_size>]

[オプション]

-S <src_addr>

ソース IP アドレスを指定します。装置に定義されていないアドレスは指定できません。

-M

応答に MPLS のラベル情報が含まれる場合に，情報を表示します.

[パラメタ]

<host>

- あて先ホスト

  あて先ホストの IP アドレス、またはホスト名を指定します。

  ホスト名を指定した場合は、ホストデータベース情報に該当ホスト名が登録されているか、本装置が DNS サーバを使用可能な状態でなければなりません。

<data_size>

- データサイズ

  送信するパケットに付加するデータサイズを、0〜9959 の 10 進数値 (単位:バイト) で指定します。

  省略した場合は、0 バイトを指定したものとみなされます。

[説明]

ネットワーク経路を表示します。

指定した host(IP アドレスまたはホスト名) に対して、IP データグラムヘッダの生存時間 (TTL) の値を 1 から 1 つずつ単調に増加させながら試験パケットを送信し、時間超過またはあて先到達不能の ICMP パケット受信によって、host までの経路情報を表示します。

[例]

以下に、実行例を示します。

実行例 1　host から応答がある場合の実行例を示します。

```
# traceroute 192.168.1.1
traceroute to 192.168.1.1 (192.168.1.1), 30 hops max, 40 byte packets
 1  192.168.5.1 (192.168.5.1)  20 ms  20 ms  20 ms
 2  192.168.1.1 (192.168.1.1)  41 ms  41 ms  41 ms
#
```

実行例 2　host から応答がない場合の実行例を示します。

```
# traceroute 192.168.1.1
traceroute to 192.168.1.1 (192.168.1.1), 30 hops max, 40 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
    :
30  * * *
#
```

実行例 3　応答に MPLS のラベル情報が含まれる場合の実行例を示します。

```
# traceroute -M 10.1.101.2
traceroute to 10.1.101.2 (10.1.101.2), 30 hops max, 40 byte packets
 1  10.1.201.1 (10.1.201.1)  1 ms  1 ms  1 ms Label1=17 ExpBits1=0
 2  10.4.1.1 (10.4.1.1)  1 ms  1 ms  2 ms Label1=29 ExpBits1=0
 3  10.5.1.1 (10.5.1.1)  2 ms  1 ms  2 ms Label1=16 ExpBits1=0
 4  10.1.101.2 (10.1.101.2)  2 ms  2 ms  2 ms Label1=18 ExpBits1=0
#
```

第 15 章　表示コマンド

15.1 画面単位の表示

15.1.1 more

[機能]

コマンドの出力を画面単位に表示します。

[入力形式]

more <command>

[オプション]

なし

[パラメタ]

<command>

実行するコマンド名およびオプションやパラメタを指定します。

[説明]

パラメタで指定したコマンドを実行し、その出力結果を画面単位に表示します。

本コマンドは、画面サイズが 24 行 80 桁であるものとして動作します。画面サイズが 24 行 80 桁以外の場合には、env コマンドで環境変数 LINES と COLUMNS に行数と桁数を設定してください。設定しない場合には表示が乱れます。詳しくは env コマンドを参照してください。なお、telnet でログインしていて、telnet クライアントに画面の行数桁数を通知する機能がある場合には、環境変数を設定しなくとも乱れることなく表示されます。

コマンドの出力を一画面分表示すると、プロンプトが表示され、キー入力待ちになります。

コマンドの出力が一画面に満たない場合、プロンプト表示およびキー入力待ちは行われず、more コマンドを指定しなかったのと同じ動作になります。

コマンドの出力を最後まで表示すると more コマンドは終了します。

キー入力待ちのとき、以下のようなプロンプトが表示されます。

more(xx%):

(xx は全体バイト数に対する表示済バイト数の割合)

キー入力時のキーと動作の一覧を以下に示します。^x は CTRL キーを押しながら x キーを押すことを、M-x は ESC キーを押してから x キーを押すことを表しています。

キー	動作
1 2 3 4 5 6 7 8 9 0	行数、行番号、回数指定(以下のキーを入力する前に指定)
f ^F ^V SPACE	一画面または指定行数前進(途中の行は省略)
b ^B M-v BS	一画面または指定行数後退(途中の行は省略)
z	一画面の行数を指定行数に変更し一画面前進
w	一画面の行数を指定行数に変更し一画面後退
j ^J e ^E ^N ↓ RETURN	一行または指定行数前進(すべての行を表示)
k ^K y ^Y ^P ↑	一行または指定行数後退(すべての行を表示)
d ^D	半画面の行数を指定行数に変更し半画面前進
u ^U	半画面の行数を指定行数に変更し半画面後退
g <	先頭画面または指定行番号以降表示
G >	最終画面または指定行番号以降表示
/検索パターン	順検索(指定数回)
?検索パターン	逆検索(指定数回)
n	同方向に再検索
N	逆方向に再検索
M-x	x(任意コマンド)を実行し、最後まで表示しても終了しない
r ^R ^L	画面再表示
^G	情報表示(行数、バイト数、割合)
h H	ヘルプ表示(キーバインド一覧)
q Q ^C	終了

行番号を指定する場合、画面上での行番号を指定します。コマンドが一行分として画面桁数以上出力した場合、画面上では複数の行として扱われます。先頭行番号は 1 です。

検索時にはプロンプトとしてスラッシュ(/) またはクエスチョン (?) が表示され、検索パターンを入力できるようになります。検索パターンは 76 文字まで入力できます。画面桁数が 80 桁未満の場合、画面桁数以上の検索パターンを入力すると画面表示が乱れますので、画面再表示を行ってください。

検索パターンで使用できる特殊文字を以下に示します。それ以外はその文字自身を検索します。

特殊文字	検索対象
.	任意の一文字
^	行頭
$	行末
\<	単語開始
\>	単語終了
\x	x (xは < > 以外の文字)

検索で見つかった場合には、見つかった文字列が反転表示されます。

検索で見つからなかった場合には、以下のプロンプトが表示されるので、RETURN キーを入力してください。CTRL+C を入力した場合には、more コマンドが終了します。

```
more: pattern not found (press RETURN)
```

情報表示した場合には、以下のようなプロンプトが表示されます。

```
more(line 1-22/515 lines, 1428/33473 bytes, 4%):
          - -- ---        ---- -----        -
          a b  c          d    e           f
```

意味:

a: 画面最上行番号

b: 画面最下行番号

c: 全体行数

d: 表示バイト数

e: 全体バイト数

f: 表示バイト数に対する全体バイト数の割合 (d ÷ e × 100)

ヘルプ表示時には、ヘルプ表示後、以下のプロンプトが表示されるので、RETURN キーを入力してください。CTRL+C を入力した場合には、more コマンドが終了します。

```
more: help (press RETURN)
```

page コマンドで、コマンド実行時には暗黙的に常に more コマンドを使うように設定できます。

[例]

以下に、表示例を示します。

構成定義情報を画面単位に表示する場合

```
# more show
remote 0 ...
lan 0 ...
:
more(50%): (SPACEキー入力)
:
syslog ...
more(99%): (qキー入力)
#
```

page コマンドを使用して構成定義情報を画面単位に表示する場合

```
# page on
# show
remote 0 ...
lan 0 ...
:
more(50%): (SPACEキー入力)
:
syslog ...
more(99%): (qキー入力)
#
```

15.2　構成定義の表示

15.2.1　show

[機能]

構成定義情報の表示

[入力形式]

show [-a] [-r] [<コマンド名>]

[オプション]

-a　未設定時の値を含むすべての構成定義情報を表示します。本オプションを指定しない場合、未設定時と同じ値については表示されません。

-r　現在動作中の構成定義情報を表示します。本オプションを指定しない場合、編集中の構成定義情報が表示されます。

[パラメタ]

<コマンド名>

表示したい構成定義のコマンド名を指定します。指定したコマンド名に続く構成定義情報が表示されます。省略した場合は、すべての構成定義情報が表示されます。

[説明]

構成定義情報を表示します。

オプション未指定の場合は、編集中の構成定義情報を表示します。この時コマンド名を省略すると未設定時値を除くすべての構成定義情報が表示されます。未設定時の値を含むすべての構成定義情報を表示したい場合には、-a オプションを指定します。また、表示したいパラメタの直前までをコマンド名として指定した場合には、必ずパラメタの内容が表示されます。

-r オプションを指定した場合は、現在の動作情報として使用中の構成定義情報が表示されます。

-r オプションと-a オプションを同時に指定することもできます。

[例]

以下に、表示例を示します。

構成定義情報全体を表示する場合 (オプション未指定)

```
# show
lan 0 ip address 192.168.1.1/24 3
syslog pri error,warn,info
syslog facility 23
telnetinfo autologout 5m
time zone 0900
consoleinfo autologout 8h
env KANJI=SJIS
#
```

lan 0 インタフェースの IP アド レスを表示する場合

```
# show lan 0 ip address
192.168.1.1/24 3
#
```

動作中の構成定義情報を表示する場合 (-r オプションを指定)

```
# show -r
lan 0 mode auto
lan 0 ip address 192.168.1.1/24 3
syslog pri error,warn,notice,info
telnetinfo autologout 5m
time zone 0900
env KANJI=SJIS
```

動作中の構成定義情報すべてを表示する場合 (-a と-r オプションを指定)

```
# show -ar
lan 0 bind mb 0
lan 0 mode auto
lan 0 mdi auto
lan 0 flowctl on
lan 0 mtu 1500
lan 0 shaping off
lan 0 backup mode master
lan 0 recovery auto up
lan 0 ip address 192.168.1.1/24 3
lan 0 ip dhcp service off
lan 0 ip dhcp info time 0d
lan 0 ip proxyarp on
lan 0 ip localproxyarp off
lan 0 ip rip use off off 0 off
lan 0 ip ospf use off
lan 0 ip ospf cost 10
lan 0 ip ospf hello 10s
lan 0 ip ospf dead 40s
lan 0 ip ospf retrans 5s
lan 0 ip ospf delay 1s
lan 0 ip ospf priority 1
lan 0 ip ospf auth type off
lan 0 ip ospf passive off
lan 0 ip multicast mode off
lan 0 ip multicast pim preference 1024
lan 0 ip multicast pim upstream type pim
lan 0 ip multicast ttl threshold 1
lan 0 ip vrf use off
lan 0 ip nat mode off
lan 0 ip nat static default reject
lan 0 ip filter default pass
lan 0 ip icmp redirect on
lan 0 ip6 use off
lan 0 ip6 ifid auto
lan 0 ip6 ra mode off
lan 0 ip6 ra interval 600 200 1800
lan 0 ip6 ra mtu 0
lan 0 ip6 ra reachabletime 0
lan 0 ip6 ra retranstimer 0
lan 0 ip6 ra curhoplimit 64
lan 0 ip6 ra flags 00
lan 0 ip6 rip use off off 0
lan 0 ip6 rip site-local on
lan 0 ip6 filter default pass
```

(続く)

```
lan 0 bridge use off
lan 0 bridge stp use off
lan 0 bridge stp cost auto
lan 0 bridge stp priority 128
lan 0 bridge group 0
lan 0 vrrp use off
lan 0 vrrp auth none
lan 0 vrrp group 0 ad 1s
lan 0 vrrp group 0 preempt on
lan 0 vrrp group 1 ad 1s
lan 0 vrrp group 1 preempt on
lan 0 mpls use off
lan 0 mpls distribution ldp
lan 0 mpls ldp hello-timers 5s 15s
lan 0 mpls ldp keepalive-timers 1m 3m
lan 0 mpls ldp retention liberal
lan 0 mpls ldp advertisement du
lan 0 mpls ldp interface-label off
lan 0 mpls ldp ip transport 0.0.0.0
lan 0 mpls l2-circuit exp 0
lan 0 vlan tag vid 1
lan 0 vlan tag pri 0
answer accept disable
answer ppp auth type any
answer ppp mp use off
answer ppp mp bap use off
snmp service off
upnp use off
upnp portmapping lease 0d
multicast ip pimsm candrp mode off
multicast ip pimsm candrp address 0.0.0.0
multicast ip pimsm candrp priority 0
multicast ip pimsm candbsr mode off
multicast ip pimsm candbsr address 0.0.0.0
multicast ip pimsm candbsr priority 0
multicast ip pimsm spt mode on
multicast ip pimsm spt rate 0
multicast ip pimsm register checksum header
syslog pri error,warn,info
syslog facility 23
syslog dupcut no
syslog security ipfilter,nat,ppp,dhcp,proxydns
mflag off
telnetinfo autologout 5m
time zone 0900
consoleinfo autologout 8h
proxydns unicode reject
bridge 0 age 5m
bridge 0 stp priority 32768
bridge 0 stp age 20s
bridge 0 stp hello 2s
bridge 0 stp delay 15s
bridge 0 ip routing on
bridge 0 ip policy strict
bridge 0 ip6 routing on
bridge 0 ip6 policy strict
bridge 0 vlan tag transmit off
bridge 0 inter-remote on
        :
bridge 19 age 5m
bridge 19 stp priority 32768
bridge 19 stp age 20s
bridge 19 stp hello 2s
bridge 19 stp delay 15s
bridge 19 ip routing on
bridge 19 ip policy strict
bridge 19 ip6 routing on
bridge 19 ip6 policy strict
bridge 19 vlan tag transmit off
bridge 19 inter-remote on
```

(続く)

```
routemanage ip distance rip 120
routemanage ip distance bgp 20 200
routemanage ip distance ospf 110
routemanage ip distance dns 15
routemanage ip redist rip static on
routemanage ip redist rip connected on
routemanage ip redist rip bgp off 0
routemanage ip redist rip ospf off 0
routemanage ip redist rip dns off 0
routemanage ip redist bgp static off
routemanage ip redist bgp connected off
routemanage ip redist bgp rip off
routemanage ip redist bgp ospf off
routemanage ip redist bgp dns off
routemanage ip redist ospf static off 20 type2
routemanage ip redist ospf connected off 20 type2
routemanage ip redist ospf rip off 20 type2
routemanage ip redist ospf bgp off 20 type2
routemanage ip redist ospf dns off 20 type2
routemanage ip redist ldp static off
routemanage ip redist ldp connected on
routemanage ip redist ldp rip on
routemanage ip redist ldp bgp off
routemanage ip redist ldp ospf on
routemanage ip ecmp mode off
routemanage ip ecmp ospf 1
routemanage ip6 distance rip 120
routemanage ip6 distance dns 15
routemanage ip6 distance dhcp 10
routemanage ip6 redist rip static on
routemanage ip6 redist rip connected on
routemanage ip6 redist rip dns off 0
routemanage ip6 redist rip dhcp off 0
routemanage interface floating off
rip ip timers basic 30s 3m 2m
rip ip timers jitter 50
rip ip multipath 1
rip ip6 timers basic 30s 3m 2m
rip ip6 multipath 1
bgp as 0
bgp id 0.0.0.0
bgp mpls-resolution off
bgp network igp on
ospf ip id 0.0.0.0
ospf ip definfo off 10 type2
mpls ldp router-id 0.0.0.0
mpls ldp control independent
mpls ldp ip transport 0.0.0.0
mpls ldp targeted-hello ttl 64
mpls ip propagate-ttl on
loopback ip ospf use off
loopback mpls ldp interface-label off
watchdog service on
sysdown harderr fan no
sysdown harderr thermal no
serverinfo ftp ip on
serverinfo ftp ip6 on
serverinfo telnet ip on
serverinfo telnet ip6 on
serverinfo http ip on
serverinfo http ip6 on
serverinfo dns ip on
serverinfo dns ip6 on
serverinfo sntp ip on
serverinfo sntp ip6 on
serverinfo time ip tcp on
serverinfo time ip udp on
serverinfo time ip6 tcp on
serverinfo time ip6 udp on
page off
env KANJI=SJIS
#
```

(続き)

15.2.2　diff

[機能]

構成定義情報の差分の表示

[入力形式]

diff <config1> <config2>

[オプション]

なし

[パラメタ]

<config1>, <config2>

比較したい構成定義種別を指定します。

- work
  設定中の構成定義
- running
  動作中の構成定義
- config1
  FLASH メモリの構成定義 1
- config2
  FLASH メモリの構成定義 2
- config
  FLASH メモリの構成定義

[説明]

指定の構成定義の差分を表示します。<config1>にだけ定義されていいる情報の先頭には"< "を、<config2>にだけ定義されている情報には"> "を付加して表示します。

[例]

以下に、表示例を示します。

```
# diff running work
===
> remote 0 name rmt0
> remote 1 name rmt1
===
< remote 3 name rmt3
< remote 4 name rmt4
< remote 5 name rmt5
< remote 6 name rmt6
---
> remote 3 name inter3
===
< remote 8 name rmt8
< remote 9 name rmt9
< remote 10 name rmt10
< syslog server 192.168.33.63
===
> env kanji=EUC
#
```

15.3 ネットワーク状態の表示

15.3.1 netstat

[機能]

ネットワーク状態の表示

[入力形式]

netstat (ソケット状態表示)
netstat -a (全ソケット状態表示)
netstat -A (PCB アドレスを含んだプロトコル表示)
netstat [-A] [-a] -f <address_family> (指定アドレスファミリソケット状態表示)
netstat -i [-b] [-d] [-I <interface>] (インタフェース統計表示)
netstat -r [-f <address_family>] (ルーティングテーブル表示)
netstat -g (マルチキャストルーティングテーブル表示)
netstat -s [-p <protocol>] (プロトコル統計情報表示)
netstat -r -s [-f <address_family>] (ルーティングテーブル統計情報表示)
netstat -g -s (マルチキャストルーティングテーブル統計情報表示)
netstat -e [-f <address_family>] (ECMP 状態表示)
netstat clear (すべての統計情報のクリア)
netstat clear -i (インタフェース統計情報のクリア)
netstat clear -g (マルチキャストルーティングテーブルのカウンタのクリア)
netstat clear -s (プロトコル統計情報のクリア)
netstat clear -r -s (ルーティングテーブル統計情報のクリア)
netstat clear -g -s (マルチキャストルーティングテーブル統計情報のクリア)
netstat clear -e (ECMP のカウンタのクリア)

[オプション]

-A

ソケットと関係する全プロトコル制御ブロック (PCB) アドレスを含めて、ソケット状態を表示します。

-a

サーバプロセスで利用されているソケットも含めて、すべてのソケットを表示します。なお、通常、サーバプロセスで使用されているソケットは表示されません。

-b

-i と併用して指定する場合に、入出力 byte 数を表示します。

-d

-i と併用して指定する場合に、プロトコル処理部で送信時に欠落したパケット数を合わせて表示します。

-f <address_family>

指定した<address_family>に関する情報だけを表示します。
指定できる<address_family>は、inet(IPv4) と inet6(IPv6) です。
省略した場合は、inet と inet6 の両方を指定したものとみなされます。

-I <interface>

指定した<interface>についての統計情報を表示します。

-i

インタフェース情報を表示します。

-p <protocol>

指定した<protocol>の統計情報を表示します。

指定できる<protocol>は、tcp、udp、ip、icmp、igmp、ipsec、pim、tcp6、udp6、ip6、icmp6、ipsec6 です。

-s

各プロトコルの統計情報を表示します。-r と併用して指定する場合は、ルーティングテーブルに関する統計情報を表示します。

-g と併用して指定する場合は、マルチキャストルーティングテーブルに関する統計情報を表示します。

-r

ルーティングテーブルを表示します。-s と併用して指定する場合は、ルーティングテーブルに関する統計情報を表示します。

-g

マルチキャストルーティングテーブルを表示します。-s と併用して指定する場合は、マルチキャストルーティングテーブルに関する統計情報を表示します。

-e

ECMP 対象になっているルーティングテーブルの情報を表示します。

[パラメタ]

clear

統計情報をクリアします。clear の後にオプションがある場合には、指定された統計情報のみがクリアされます。

[説明]

ソケット状態、ネットワークインタフェース情報、ルーティングテーブル、または統計情報を表示します。

[例]

以下に、表示例および表示内容を示します。

全ソケット状態

```
# netstat -a
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address      Foreign Address      (state)
----- ------ ------  -------------      ---------------      -------
 (1)   (2)    (3)         (4)                (5)              (6)

tcp        0      3  10.232.78.147.23   10.232.77.39.32824   ESTABLISHED
tcp        0      0  *.37               *.0                  LISTEN
tcp        0      0  *.1723             *.0                  LISTEN
tcp        0      0  *.21               *.0                  LISTEN
tcp        0      0  *.80               *.0                  LISTEN
tcp        0      0  *.23               *.0                  LISTEN
udp        0      0  *.0                *.0
udp        0      0  *.37               *.0
udp        0      0  *.520              *.0
udp        0      0  127.0.0.1.7501     *.0
udp        0      0  *.1813             *.0
udp        0      0  127.0.0.1.7500     *.0
udp        0      0  *.1812             *.0
udp        0      0  *.69               *.0
udp        0      0  *.50000            *.0
udp        0      0  *.161              *.0
udp        0      0  *.8900             *.0
udp        0      0  *.53               *.0
udp        0      0  *.123              *.0
udp        0      0  *.67               *.0
udp        0      0  *.0                *.0
udp        0      0  *.59000            *.0
udp        0      0  *.9069             *.0
Active Internet6 connections (including servers)
Proto Recv-Q Send-Q  Local Address      Foreign Address      (state)
tcp6       0      0  *.23               *.0                  LISTEN
udp6       0      0  *.521              *.0
```

1) プロトコル
2) 受信待ち行列長
3) 送信待ち行列長
4) ローカルアドレス
5) リモートアドレス
6) プロトコル内部状態

インタフェース情報表示

```
# netstat -i
Name    Mtu   Network          Address                     Ipkts Ierrs    Opkts Oerrs
----    ---   -------          -------                     ----- -----    ----- -----
(1)(2)  (3)     (4)              (5)                        (6)   (7)      (8)   (9)
lan0    1500  <Link#1>         00:00:0e:f1:00:60           487     0       67     0
lan0    1500  10.232.78/24     10.232.78.147               487     0       67     0
lan0    1500  fe80::/64        fe80::200:eff:fef1:60       487     0        8     0
lo0     16384 <Link#54>                                      0     0        0     0
lo0     16384 fe80::/64        fe80::1                       0     0        0     0
lo0     16384 ::1/128          ::1                           0     0        0     0
lo0     16384 127              127.0.0.1                     0     0        0     0
```

1) 名前
2) ステータス
   名前の後に*がついているものは down、それ以外は up です。
3) MTU 長
4) ネットワークおよびサブネットマスク
5) リモートアドレス
6) 入力パケット数
7) 入力エラーパケット数
8) 出力パケット数
9) 出力エラーパケット数

ルーティングテーブル表示

```
# netstat -r
Routing tables

Internet:
Destination              Gateway               Flags      Netif Expire
-----------              -------               -----      ----- ------
   (1)                     (2)                  (3)        (4)   (5)

default                  10.232.78.129         UGSc        lan0
10.232.78/24             link#1                UC          lan0
10.232.78.129            0:a0:c9:78:d8:60      UHLW        lan0   1178
127.0.0.1                127.0.0.1             UH           lo0
Total Routing Tables  0 ---(6)
Total ARP Tables  1 ---(7)

Internet6:
Destination              Gateway               Flags      Netif Expire
::1                      ::1                   UH           lo0
fe80::%lan0/64           link#1                UC          lan0
fe80::%lo0/64            fe80::1%lo0           Uc           lo0
ff01::/32                ::1                   U            lo0
ff02::%lan0/32           link#1                UC          lan0
ff02::%lo0/32            fe80::1%lo0           UC           lo0
Total Routing Tables  0 ---(6)
Total NDP Tables  0 ---(8)
```

1) ネットワークまたはホストのあて先 IP アドレス
2) あて先ゲートウェイ IP アドレス
3) ルーティング情報を得た手段などを示すフラグ
   フラグの詳細を以下に示します。

   1　　ルーティングフラグ#1 にて特定されるプロトコル

   2　　ルーティングフラグ#2 にて特定されるプロトコル

3 ルーティングフラグ#3 にて特定されるプロトコル

B 破棄されるパケット

b ブロードキャストアドレスを表現する経路

C 新しい経路を生成する

c 使用時に、プロトコル専用の新しい経路を生成する

D リダイレクトによって動的に生成された経路

G ゲートウェイなどによる中継を必要としている到達先

H ホストエントリ (これ以外はネットワーク)

L アドレス変換を連動させられる正当なアドレス

M リダイレクトによって動的に変更される

R 到達不可能なホストまたはネットワーク

S スタティックルート

U 使用可能経路

W クローンした結果として作成された経路

X 外部の daemon がプロトコルからリンクアドレス変換を行う

4) 経由インタフェース

5) 当経路破棄までの残時間 (単位:秒)

6) ルーティングテーブルエントリ数

7) ARP テーブルエントリ数

8) NDP テーブルエントリ数

IPv6 の Neigbor Cache エントリの最大値を以下に示します。ただし、通信のための内部管理情報として利用されるエントリが含まれます。そのため、LAN で直接接続できる端末数は最大値より少なくなる場合があります。

1024

最大値	機種
2000	MR1000

マルチキャスト ルーティングテーブル表示

```
# netstat -g

Virtual Interface Table
 VIF Netif    Thresh Local-Address     Pkts-In   Pkts-Out
   0  lan0         1 192.168.1.1             0          0
   1  lan1         1 192.168.2.1             0          0
   2 register      1 192.168.1.1             0          0
 --- -------- ------ -------------     -------   --------
 (1)    (2)     (3)       (4)            (5)        (6)

Total Virtual Interface Tables  3   --- (7)

Multicast Forwarding Cache
 Origin          Group             Packets In-VIF  Out-VIFs
 192.168.2.2     239.255.30.1            7    1    0
 192.168.2.2     239.255.30.2            5    1    0
 192.168.2.2     239.255.30.3            3    1    0
 ------------    ------------      ------- ------  --------
      (8)             (9)            (10)   (11)     (12)

Total Multicast Routing Tables  3   --- (13)
#
```

インタフェース情報

1) VIF(Virtual Interface) 番号
2) VIF に対応する実際のインタフェース。register は PIM-SM 使用時の PIM Register パケットの送受信用の仮想インタフェース
3) TTL しきい値
4) インタフェースの IP アドレス
5) 入力パケット数
6) 出力パケット数
7) VIF の総数

マルチキャスト・ルーティングテーブル情報

8) マルチキャスト・パケットの送信元のアドレス
9) マルチキャスト・グループ
10) パケット数
11) 入力 VIF

    マルチキャスト・ルーティングテーブルは、マルチキャスト・パケットの到達時に一時的に作成されます。この際、入力 VIF は空欄となっています。

    そのあと、マルチキャスト・ルーティングテーブルは入力インタフェースと出力インタフェースの決定後に有効になり、マルチキャスト・パケットの転送に利用されますが、転送に利用されない場合には、そのまま削除されます。
12) 出力先 VIF
13) マルチキャスト・ルーティングテーブルの総数

ECMP 状態表示

```
# netstat -e
ECMP information

Internet:
Destination          Gateway               Packets Netif   Since
-----------          -------               ------- -----   ------
   (1)                 (2)                   (3)    (4)      (5)
192.168.10           192.168.1.2                0  lan0   Nov  9 19:03:13 2002
                     192.168.2.2                0  lan1
#
```

1) ネットワークまたはホストのあて先 IP アドレス
2) あて先ゲートウェイ IP アドレス
3) ECMP 経路が変更されてからの出力パケット数※ ECMP 経路が変更されたときに 0 になります
4) 経由インタフェース
5) ECMP 経路の変更がされた時刻

統計情報

```
# netstat -s
tcp: ---(1)
        95 packets sent
                90 data packets (16322 bytes)
                0 data packets (0 bytes) retransmitted
                0 resends initiated by MTU discovery
                4 ack-only packets (1 delayed)
                0 URG only packets
                0 window probe packets
                0 window update packets
                1 control packet
        156 packets received
                87 acks (for 16322 bytes)
                1 duplicate ack
                0 acks for unsent data
                72 packets (103 bytes) received in-sequence
                0 completely duplicate packets (0 bytes)
                0 old duplicate packets
                0 packets with some dup. data (0 bytes duped)
                1 out-of-order packet (0 bytes)
                0 packets (0 bytes) of data after window
                0 window probes
                0 window update packets
                0 packets received after close
                0 discarded for bad checksums
                0 discarded for bad header offset fields
                0 discarded because packet too short
        0 connection requests
        2 connection accepts
        0 bad connection attempts
        0 listen queue overflows
        2 connections established (including accepts)
        1 connection closed (including 0 drops)
                1 connection updated cached RTT on close
                1 connection updated cached RTT variance on close
                0 connections updated cached ssthresh on close
        0 embryonic connections dropped
        87 segments updated rtt (of 88 attempts)
        0 retransmit timeouts
                0 connections dropped by rexmit timeout
        0 persist timeouts
                0 connections dropped by persist timeout
        0 keepalive timeouts
                0 keepalive probes sent
                0 connections dropped by keepalive
        76 correct ACK header predictions
        66 correct data packet header predictions

udp: ---(2)
        151 datagrams received
        0 with incomplete header
        0 with bad data length field
        0 with bad checksum
        0 dropped due to no socket
        74 broadcast/multicast datagrams dropped due to no socket
        0 dropped due to full socket buffers
        0 not for hashed pcb
        77 delivered
        0 datagrams output

ip: ---(3)
        307 total packets received
        0 bad header checksums
        0 with size smaller than minimum
        0 with data size < data length
        0 with ip length > max ip packet size
        0 with header length < data size
        0 with data length < header length
        0 with bad options
        0 with incorrect version number
```

(続く)

```
        0 fragments received
        0 fragments dropped (dup or out of space)
        0 fragments dropped after timeout
        0 packets reassembled ok
        307 packets for this host
        0 packets for unknown/unsupported protocol
        0 packets forwarded
        0 packets not forwardable
        0 redirects sent
        95 packets sent from this host
        0 packets sent with fabricated ip header
        0 output packets dropped due to no bufs, etc.
        0 output packets discarded due to no route
        0 output datagrams fragmented
        0 fragments created
        0 datagrams that can't be fragmented
        0 tunneling packets that can't find gif

icmp: ---(4)
        0 calls to icmp_error
        0 errors not generated 'cuz old message was icmp
        0 messages with bad code fields
        0 messages < minimum length
        0 bad checksums
        0 messages with bad length
        0 message responses generated

igmp: ---(5)
        480 messages received
        0 messages received with too few bytes
        0 messages received with bad checksum
        35 membership queries received
        0 membership queries received with invalid field(s)
        185 membership reports received
        0 membership reports received with invalid field(s)
        7 membership reports received for groups to which we belong
        139 membership reports sent

ipsec: ---(6)
        0 inbound packets processed successfully
        0 inbound packets violated process security policy
        0 inbound packets with no SA available
        0 invalid inbound packets
        0 discard inbound packets by interface down
        0 inbound packets failed due to insufficient memory
        0 inbound packets failed getting SPI
        0 inbound packets failed on AH replay check
        0 inbound packets failed on ESP replay check
        0 inbound packets considered authentic
        0 inbound packets failed on authentication
        0 inbound packets considered authentic(ESPinAuth)
        0 inbound packets failed on authentication(ESPinAuth)
        0 outbound packets processed successfully
        0 outbound packets violated process security policy
        0 outbound packets with no SA available
        0 invalid outbound packets
        0 outbound packets failed due to insufficient memory
        0 outbound packets with no route
        0 ipsec queue overflows

pim: ---(7)
        36 messages received
        432 bytes received
        0 messages received with too few bytes
        0 messages received with bad checksum
        0 messages received with bad version
        0 data register messages received
        0 data register bytes received
        0 data register messages received on wrong iif
        0 bad registers received
        0 full checksum registers received
        0 data register messages sent
        0 data register bytes sent
```

(続く)

```
ip6: ---(8)
        0 total packets received
        0 with size smaller than minimum
        0 with data size < data length
        0 with bad options
        0 with incorrect version number
        0 fragments received
        0 fragments dropped (dup or out of space)
        0 fragments dropped after timeout
        0 fragments that exceeded limit
        0 packets reassembled ok
        0 packets for this host
        0 packets forwarded
        0 packets not forwardable
        0 redirects sent
        6 packets sent from this host
        0 packets sent with fabricated ip header
        0 output packets dropped due to no bufs, etc.
        0 output packets discarded due to no route
        0 output datagrams fragmented
        0 fragments created
        0 datagrams that can't be fragmented
        0 packets that violated scope rules
        0 multicast packets which we don't join
        Mbuf statistics:
                0 one mbuf
                0 one ext mbuf
                0 two or more ext mbuf
        0 packets whose headers are not continuous
        0 tunneling packets that can't find gif
        0 packets discarded due to too many headers
        0 failures of source address selection
        0 forward cache hit
        0 forward cache miss

icmp6: ---(9)
        0 calls to icmp6_error
        0 errors not generated because old message was icmp6 error or so
        0 errors not generated because rate limitation
        Output histogram:
                multicast listener report: 5
                neighbor solicitation: 1
        0 messages with bad code fields
        0 messages < minimum length
        0 bad checksums
        0 messages with bad length
        Histogram of error messages to be generated:
                0 no route
                0 administratively prohibited
                0 beyond scope
                0 address unreachable
                0 port unreachable
                0 packet too big
                0 time exceed transit
                0 time exceed reassembly
                0 erroneous header field
                0 unrecognized next header
                0 unrecognized option
                0 redirect
                0 unknown
        0 message responses generated
        0 messages with too many ND options

tcp6: ---(10)
        0 packets sent
                0 data packets (0 bytes)
                0 data packets (0 bytes) retransmitted
                0 ack-only packets (0 delayed)
                0 URG only packets
                0 window probe packets
                0 window update packets
                0 control packets
```

(続く)

```
        0 packets received
                0 acks (for 0 bytes)
                0 duplicate acks
                0 acks for unsent data
                0 packets (0 bytes) received in-sequence
                0 completely duplicate packets (0 bytes)
                0 old duplicate packets
                0 packets with some dup. data (0 bytes duped)
                0 out-of-order packets (0 bytes)
                0 packets (0 bytes) of data after window
                0 window probes
                0 window update packets
                0 packets received after close
                0 discarded for bad checksums
                0 discarded for bad header offset fields
                0 discarded because packet too short
        0 connection requests
        0 connection accepts
        0 bad connection attempts
        0 connections established (including accepts)
        0 connections closed (including 0 drops)
        0 embryonic connections dropped
        0 segments updated rtt (of 0 attempts)
        0 retransmit timeouts
                0 connections dropped by rexmit timeout
        0 persist timeouts
        0 connections timed out in persist
        0 keepalive timeouts
                0 keepalive probes sent
                0 connections dropped by keepalive
        0 correct ACK header predictions
        0 correct data packet header predictions
        0 PCB cache misses

udp6: ---(11)
        0 datagrams received
        0 with incomplete header
        0 with bad data length field
        0 with bad checksum
        0 with no checksum
        0 dropped due to no socket
        0 multicast datagrams dropped due to no socket
        0 dropped due to full socket buffers
        0 delivered
        0 datagrams output

ipsec6: ---(12)
        0 inbound packets processed successfully
        0 inbound packets violated process security policy
        0 inbound packets with no SA available
        0 invalid inbound packets
        0 discard inbound packets by interface down
        0 inbound packets failed due to insufficient memory
        0 inbound packets failed getting SPI
        0 inbound packets failed on AH replay check
        0 inbound packets failed on ESP replay check
        0 inbound packets considered authentic
        0 inbound packets failed on authentication
        0 inbound packets considered authentic(ESPinAuth)
        0 inbound packets failed on authentication(ESPinAuth)
        0 outbound packets processed successfully
        0 outbound packets violated process security policy
        0 outbound packets with no SA available
        0 invalid outbound packets
        0 outbound packets failed due to insufficient memory
        0 outbound packets with no route
        0 ipsec queue overflows
```

(続き)

1) TCP 統計情報

2) UDP 統計情報

3) IP 統計情報

4) ICMP 統計情報

5) IGMP 統計情報

6) IPSEC 統計情報

7) PIM 統計情報

8) IP6 統計情報

9) ICMP6 統計情報

10) TCP6 統計情報

11) UDP6 統計情報

12) IPSEC6 統計情報

マルチキャスト・ルーティングテーブル統計情報

```
# netstat -sg
multicast forwarding: ---(1)
          0 multicast forwarding cache lookups
          0 multicast forwarding cache misses
          0 upcalls to multicast daemon
          0 upcall queue overflows
          0 upcalls dropped due to full socket buffer
          0 cache cleanups
          0 datagrams with no route for origin
          0 datagrams arrived with bad tunneling
          0 datagrams could not be tunneled
          0 datagrams arrived on wrong interface
          0 datagrams selectively dropped
          0 datagrams dropped due to queue overflow
          0 datagrams dropped for being too large
```

1) マルチキャスト・ルーティングテーブル統計情報

15.3.2　dhcpstat

[機能]

DHCP 運用状況の表示

[入力形式]

dhcpstat [-f <address_family>] [-I <interface>]

[オプション]

-f <address_family>

指定した address_family に関する情報のみを表示します。

本装置は inet(IPv4), inet6(IPv6) のみサポート します。未指定時には inet, inet6 の両方が指定されたものとして動作します。

-I <interface>

指定したインタフェースについての DHCP 運用状況を表示します。

[パラメタ]

なし

[説明]

DHCP の以下の機能の運用状況を表示します。

IPv4 DHCP サーバの運用状況表示

リース可能アド レスレンジ、リース中のアド レスとリース先情報およびリース期間を表示します。

IPv4 DHCP リレーエージェント の運用状況表示

中継先 DHCP サーバアド レスを表示します。

IPv4 DHCP クライアント の運用状況表示

クライアント状態、リース開始時刻／終了時刻、サーバから獲得したオプション情報を表示します。

IPv6 DHCP サーバの運用状況表示

配布プレフィックス情報、リース中のプレフィックス情報とリース先情報およびリース期間を表示します。

IPv6 DHCP クライアント の運用状況表示

IPv6 DHCP クライアント状態、リース開始時刻／終了時刻、サーバから獲得したオプション情報を表示します。

また、指定されたインタフェースで IPv4 DHCP サーバ、リレーエージェント、クライアント、IPv6 DHCP サーバ、クライアントのいずれも動作していない場合は何も表示されません。

また、インタフェースの指定がない場合は、全てのインタフェースの DHCP 情報が表示されます。

[例]

以下に、表示例を示します。

IPv4 DHCP サーバの場合

```
# dhcpstat -f inet -I lan0

[lan0] IPv4 DHCP Server Informations

Lease IP Address          : 192.168.1.2  [Range: 253] --- (1)
Subnet Mask               : 255.255.255.0 --- (2)
Default Router Address    : 192.168.1.1 --- (3)
DNS Server Address        : 192.168.1.1 --- (4)
Domain Name               : omron.co.jp --- (5)
Lease Time                : 0001.00:00:00 --- (6)

Active Client List:
No. IP address          MAC address       Lease remain
--- ----------          -----------       ------------
(7) (8)                 (9)               (10)
001 192.168.1.2         00:00:00:00:00:00 0000.23:59:00
002 192.168.1.3         00:00:00:00:00:00 0000.23:59:00
003 192.168.1.4         00:00:00:00:00:00 0000.23:59:00
004 192.168.1.5         00:00:00:00:00:00 0000.23:59:00
005 192.168.1.6         00:00:00:00:00:00 0000.23:59:00
:

#
```

1) 配布 IP アドレス先頭 [配布アドレス数]
2) 配布サブネットマスク
3) 配布デフォルトルータアドレス
4) 配布 DNS サーバアドレス
5) 配布ドメイン名
6) リース時間
7) 通番
8) IP アドレス
9) MAC アドレス
10) 残りリース時間

IPv4 DHCP リレーエージェントの場合

```
# dhcpstat

[lan0] IPv4 DHCP Relay Agent Information

Forwarding DHCP Server: 192.168.3.1 --- (1)

#
```

1) DHCP サーバアドレス

IPv4 DHCP クライアント の場合

```
# dhcpstat

[lan0] IPv4 DHCP Client Informations

Leased IP Address         : 192.168.1.2 --- (1)
Subnet Mask               : 255.255.255.0 --- (2)
Default Router Address    : 192.168.1.1 --- (3)
DHCP Server Address       : 192.168.1.1 --- (4)
TIME Server Address       : 192.168.1.X --- (5)
NTP Server Address        : 192.168.1.X --- (6)
DNS Server Address        : 192.168.1.1 --- (7)
Domain Name               : omron.co.jp --- (8)
Lease Time                : 0001.00:00:00 --- (9)
Renewal Time              : 0000.12:00:00 --- (10)
Rebinding Time            : 0000.18:00:00 --- (11)
Lease Expire              : Tue Dec  1 14:00:13 1998 --- (12)
Client Status             : BOUND --- (13)

#
```

1) 獲得 IP アドレス
2) 獲得サブネットマスク
3) 獲得デフォルトルータアドレス
4) 獲得 DHCP サーバアドレス
5) 獲得タイムサーバアドレス
6) 獲得 NTP サーバアドレス
7) 獲得 DNS サーバアドレス
8) 獲得ドメイン名
9) リース時間
10) リース更新時間 (T1)
11) リース更新時間 (T2)
12) リース有効期限
13) DHCP クライアント状態

IPv6 DHCP サーバの場合

```
# dhcpstat

[rmt0] IPv6 DHCP Server Informations

Server DUID               : 0003 0001 0200 0eff fe58 a00b       .. .. .. .. .X .. ---(1)
Server Preference         : 0 ---(2)
DNS Server Address        : 2001:db8::1 ---(3)
                            2001:db8::3 ---(4)
Active Client
------------------------------------------------------------------------------
Client DUID             : ffff                                 .. ---(5)
IAID                    : 2 ---(6)
Prefix/Prefixlen        : 2001:db8::/48 ---(7)
Preferred Lifetime      : infinity ---(8)
Valid Lifetime          : infinity ---(9)
Delegated Time          : Wed May 26 09:56:28 2004 ---(10)
Lease remain            : infinity ---(11)
#
```

1) サーバ DUID
2) サーバプリファレンス値

3) 配布 DNS サーバアドレス
4) 配布セカンダリ DNS サーバアドレス
5) クライアント DUID
6) IAID
7) 配布プレフィックス
8) Preferred Lifetime
9) Valid Lifetime
10) 配布時間
11) リース有効期限

IPv6 DHCP クライアントの場合

```
# dhcpstat
[rmt0] IPv6 DHCP Client Informations

Client Status             : ACTIVE ---(1)
IAID                      : 2 ---(2)
Client DUID               : ffff                                  .. ---(3)
Server DUID               : 0003 0001 0200 0eff fe58 a00b         .. .. .. .. .X .. ---(4)
Server Preference         : 0 ---(5)
DNS Server Address        : 2001:db8::1 ---(6)
                            2001:db8::3 ---(7)
Delegated Time            : Wed May 26 09:56:28 2004 ---(8)
Uptime                    : 0000.00:00:41 ---(9)
T1 (Renewal Time)         : infinity ---(10)
T2 (Rebind Time)          : infinity ---(11)
Preferred Lifetime        : infinity ---(12)
Valid Lifetime            : infinity ---(13)
Prefix/Prefixlen          : 2001:db8::/48 ---(14)

Assign Interface List
------------------------------------------------------------------------------
I/F Name                  Prefix/Prefixlen
rmt1                      2001:db8:0:1::/64 ---(15)
rmt2                      2001:db8:0:2::/64
rmt3                      2001:db8:0:2::/64
#
```

1) クライアント状態
2) IAID
3) クライアント DUID
4) サーバ DUID
5) サーバプリファレンス値
6) 獲得 DNS サーバアドレス
7) 獲得セカンダリ DNS サーバアドレス
8) 獲得時間
9) 経過時間
10) T1 時間
11) T2 時間
12) Preferred Lifetime
13) Valid Lifetime
14) 獲得プレフィックス
15) 割り当てプレフィックス情報

15.4　ルーティングプロト コル情報の表示

15.4.1　routestat ip route

[機能]

ルーティングマネージャ情報の表示

[入力形式]

- 経路情報表示
  routestat ip route
  routestat ip route <route-type>
  routestat ip route <address>/<mask> [inexact]
- 経路情報数表示
  routestat ip route summary
- VRF 経路情報表示
  routestat ip route vrf [<vrf_number>]

[オプション]

なし

[パラメタ]

<route-type>

経路情報の種別を指定します。

- connected
  インタフェース経路情報を示します。
- static
  スタティック経路情報を示します。
- rip
  RIP 経路情報を示します。
- bgp
  BGP 経路情報を示します。
- ospf
  OSPF 経路情報を示します。
- dns
  DNS 経路情報を示します。

<address>/<mask> [inexact]

経路情報を<address>/<mask>で指定します。デフォルトルートを表示するときは、"default"と指定することができます。

inexact を指定することにより、指定した<address>と IPv4 ルーティング情報のアドレスを比較し、<mask>まで一致した経路情報を表示することができます。

<vrf_number>

VRF 番号の定義番号を、10 進数値で指定します。

範囲	機種
0〜1	MR1000

[説明]

routestat ip route

すべての経路情報を表示します。

routestat ip route <route-type>

指定した種別の経路情報を表示します。

routestat ip route <address>/<mask>

指定した経路情報を表示します。inexact を指定することにより、指定した指定した経路情報に含まれる経路情報をすべて表示することができます。

routestat ip route summary

経路情報種別ごとの経路情報数とその合計を表示します。

routestat ip route vrf

すべての VRF 経路情報を表示します。<vrf_number>を指定することにより、特定の VRF 定義番号の情報を表示することができます。

[例]

以下に、表示例および表示内容を示します。

全経路情報表示の場合

```
# routestat ip route
Codes: C - Connected, S - Static, R - RIP, B - BGP, O - OSPF, DN - DNS,
       > - selected route, * - FIB route

C > * 192.168.10.0/24 is directly connected, lan0
C > * 192.168.20.0/24 is directly connected, lan1
C > * 192.168.30.1/32 is directly connected, rmt0
C > * 192.168.30.2/32 is directly connected, rmt0
R > * 192.168.80.0/24 [120/2] via 192.168.10.50, lan0, 00:11:35
R > * 192.168.81.0/24 [120/3] via 192.168.10.50, lan0, 00:11:35
R > * 192.168.82.0/24 [120/3] via 192.168.10.50, lan0, 00:11:34
(1)    (2)          (3)       (4)            (5)    (6)
Total Routing Tables  3   (7)
```

1) ルーティングプロトコル種別 (Codes)

以下のどれかが表示されます。

C : インタフェース経路

S : スタティック経路

R : RIP 経路

B : BGP 経路

O : OSPF 経路

DN: DNS 経路

> : 同一経路の中で優先される経路

*** :** IP ルーティングで使用される有効経路

2) 経路のネットワークアドレス/マスクビット数

インタフェース経路で、かつ、remote 側に IP アドレスが割り振られていない場合、"unnumbered"が表示されます。デフォルトルート (0.0.0.0/0) の場合は、"default"が表示されます。

3) 優先度/メトリック値 ([distance/metric])

インタフェース経路のときは表示されません。

4) 経路情報送信元 IPv4 アドレス
以下のどれかが表示されます。

"**via IPv4address**"
送信元の IPv4 アドレスが表示されます。

"**is directly connected**"
インタフェース経路、または、送信元 IPv4 アドレスが存在しないスタティック経路のときに表示されます。

5) インタフェース名
インタフェースを表示します。状態により以下のどれかが表示される場合があります。

"**inactive**"
使用不可能状態

"**(recursive via IPv4address)**"
BGP 使用時、リカーシブ (経由ネットワークとして IPv4 アドレスを使用) の場合に表示されます。

"**(recursive is directly connected)**"
BGP 使用時、リカーシブ (経由ネットワークとしてインタフェース経路を使用) の場合に表示されます。

6) 時間
経路情報を更新してから経過した時間が表示されます。
RIP 経路、BGP 経路または OSPF 経路の場合に表示されます。

7) ルーティングテーブルエントリ数
スタティック経路とダイナミックルーティング経路の合計を表示します。インタフェース経路の数は含まれません。

経路情報を指定して表示する場合

```
#routestat ip route 192.168.4.0/24
  Routing entry for 192.168.4.0/24 (1)
  Known via "rip", distance 120, metric 3, best
             (2)                          (3)
  Last update 00:02:43 ago (4)
  * 192.168.3.55, via lan0
 (5)        (6)       (7)
```

1) 経路のネットワークアドレス/マスクビット数
インタフェース経路で、かつ、remote 側に IP アドレスが割り振られていない場合、"unnumbered"が表示されます。デフォルトルート (0.0.0.0/0) の場合は、"default"が表示されます。

2) ルーティングプロトコル種別
以下のどれかが表示されます。

"**connected**"
インタフェース経路

"**static**"　スタティック経路

"**rip**"　RIP 経路

"**bgp**"　BGP 経路

"**ospf**"　OSPF 経路

"**dns**"　DNS 経路

3) 優先経路 (best)
同一経路の中で優先される経路の場合、"best"が表示されます。

4) 時間
経路情報を更新してから経過した時間が表示されます。RIP 経路、BGP 経路または OSPF 経路の場合に表示されます。

5) 有効経路
IP ルーティングで使用される有効経路の場合は、"*"が表示されます。

6) 経路情報送信元 IPv4 アドレス
以下のどれかが表示されます。

"**IPv4address**"
送信元の IPv4 アドレスが表示されます。

"**directly connected**"
インタフェース経路、または、送信元 IPv4 アドレスが存在しないスタティック経路のときに表示されます。

7) インタフェース名
インタフェースを表示します。状態により以下のどれかが表示される場合があります。

"**inactive**"
使用不可能状態

"**(recursive via IPv4address)**"
BGP 使用時、リカーシブ (経由ネットワークとして IPv4 アドレスを使用) の場合に表示されます。

"**(recursive is directly connected)**"
BGP 使用時、リカーシブ (経由ネットワークとしてインタフェース経路を使用) の場合に表示されます。

経路情報数表示の場合

```
# routestat ip route summary
 RouteSource(1)  Networks(2)     FIB(3)
 connected              4          4
 static                 1          1
 rip                    0          0
 bgp                    0          0
 ospf                   0          0
 dns                    0          0
 Total                  5          5
```

1) ルーティングプロトコル種別 (RouteSource)
以下のどれかが表示されます。

"**connected**"
インタフェース経路

"**static**"　スタティック経路

"**rip**"　RIP 経路

"**bgp**"　BGP 経路

"**ospf**"　OSPF 経路

"**dns**"　　DNS 経路

2) エントリ数 (Networks)
登録されている経路エントリ数が表示されます。

3) 有効経路数 (FIB)
登録されている経路エントリ数において、IPv4 ルーティングテーブルに設定されている有効経路数が表示されます。

VRF 経路情報表示の場合

```
# routestat ip route vrf 0
[VRF 0]
Codes: C - Connected, S - Static, B - BGP,
       > - selected route, * - FIB route

C > * 192.168.10.0/24 is directly connected, lan1
S >   60.60.60.0/24 [1/0] via 192.168.10.100, lan1
B >   192.168.40.0/24 [200/0] MPLS nexthop 10.1.1.4 (recursive via 172.16.1.2), 00:51:17
(1)     (2)           (3)             (4)                          (5)            (6)

Total VRF Tables  2   (7)
```

1) ルーティングプロトコル種別 (Codes)
以下のどれかが表示されます。

C :　　インタフェース経路

S :　　スタティック経路

B :　　BGP 経路

> :　　同一経路の中で優先 / 採用される経路

*** :**　　IPv4 ルーティング情報のインタフェース経路

2) 経路のネットワークアドレス / マスクビット数
デフォルトルート (0.0.0.0 / 0) の場合は、"default"が表示されます。

3) 優先度 / メトリック値 ([distance / metric])
インタフェース経路のときは表示されません。

4) ネクストホップ
以下のどれかが表示されます。

"**via IPv4address**"
送信元の IPv4 アドレスが表示されます。

"**is directly connected**"
インタフェース経路のときに表示されます。

"**MPLS nexthop**"
MPLS を中継するときに表示されます。

5) インタフェース名
インタフェースを表示します。状態により以下のどれかが表示される場合があります。

"**inactive**"
使用不可能状態

"**(recursive via IPv4address)**"
BGP 使用時、リカーシブ (経由ネットワークとして IPv4 アドレスを使用) の場合に表示されます。

"**(recursive is directly connected)**"

BGP 使用時、リカーシブ (経由ネットワークとしてインタフェース経路を使用) の場合に表示されます。

6) 時間

経路情報を更新してから経過した時間が表示されます。

BGP 経路の場合に表示されます。

7) ルーティングテーブルエントリ数

スタティック経路とダイナミックルーティング経路の合計を表示します。インタフェース経路の数は含まれません。

15.4.2　routestat ip rip

[機能]

RIP 情報の表示

[入力形式]

- RIP 経路情報表示
  routestat ip rip
- RIP プロトコル情報表示
  routestat ip rip proto

[オプション]

なし

[パラメタ]

なし

[説明]

RIP に関する情報を表示します。

routestat ip rip

RIP が管理している経路情報を表示します。

routestat ip rip proto

RIP プロトコルの情報を表示します。

[例]

以下に、表示例および表示内容を示します。

RIP 経路情報表示の場合

```
# routestat ip rip
Codes: R - RIP, C - Connected, S - Static, O - OSPF, B - BGP, DN - DNS,
       > - best

   Network            Next Hop         Metric From          Interface  Time
(1)   (2)               (3)             (4)    (5)                      (6)
B > 11.11.10.0/24      192.168.20.30         1                    lan1
B > 40.40.40.0/24      192.168.20.30         1                    lan1
C > 192.168.10.0/24                          1                    lan0
C > 192.168.20.0/24                          1                    lan1
S > 192.168.30.0/24    192.168.10.11         2                    lan0
R > 192.168.40.0/24    192.168.10.10         3 192.168.10.10      lan0  02:49
R                      192.168.10.12         4 192.168.10.12      lan0  02:31
R > 192.168.41.0/24    192.168.10.50         3 192.168.10.50      lan0  02:55
```

1) ルーティングプロトコル種別 (Codes)
   以下のどれかが表示されます。

   R :　RIP 経路

   C :　インタフェース経路

   S :　スタティック経路

   O :　OSPF 経路

   B :　BGP 経路

DN: DNS 経路

> : ベストパス

2) 経路のネットワークアドレス/マスクビット数 (Network)
デフォルトルート (0.0.0.0/0) の場合は、"default"が表示されます。

3) ネクストホップルータの IP アドレス (Next Hop)

4) メトリック値 (Metric)
このメトリック値がネットワーク上に広報されます。
ただし、加算メトリックが設定されている場合は、この Metric 値+加算メトリック値が広報されます。

5) 送信元 IPv4 アドレス (From)
RIP 経路の場合、送信元 IPv4 アドレスが表示されます。

6) 時間 (Time)
有効期限タイマの残り時間を表示します。0:00 になると、この経路に関しては、メトリック値が 16 で広報されることを意味します。
メトリック値が 16 の場合、ガーベージタイマの残り時間を表示します。

RIP プロトコル情報表示の場合

```
#routestat ip rip proto
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 24 seconds   (1)
  Timeout after 180 seconds, garbage collect after 120 seconds           (2)
  Default redistribution metric is 1                                      (3)
  Redistributing: static connected                                        (4)
  Routing network:                                                        (5)
    Interface        Send  Recv   Add-Metric  Ignore  Passwd
    lan0             v2m   v2             0     off
    rmt0             v2m   v2             5     off
  Routing Information Sources:
    Gateway          BadPackets BadRoutes  Distance Last Update          (6)
    192.168.10.10             0         0       120   00:00:07
    192.168.30.10             0         0       120   00:00:24
    192.168.10.50             0         0       120   00:00:13
  Distance: (default is 120)                                              (7)
  Entries: 6                                                              (8)
```

1) Sending updates every 30 seconds with +/-50%, next due in 24 seconds
RIP 定期広報に関する情報を表示します。
この表示例の場合、定期広報タイマ値は 30 秒であり、ゆらぎは± 50%(15 秒のゆらぎ) であることを意味します。また、次の定期広報は、約 24 秒後であることを意味します。

2) Timeout after 180 seconds, garbage collect after 120 seconds
RIP のタイムアウトに関する情報を表示します。
この表示例の場合、RIP 有効期限タイマ値は、180 秒であり、ガーベージタイマ値は、120 秒であることを意味します。

3) Default redistribution metric is 1
RIP に再配布した経路種別に対するメトリックは、1 加算して処理することを意味します。

4) Redistributing:
RIP に再配布したプロトコルに関する情報を表示します。

5) Routing network:
自装置側で設定されている RIP の構成定義に関する情報を表示します。

Interface :

構成定義で設定したインタフェース名

Send :　送信モードを表示します。

Off :　RIP パケットを送信しない

v1 :　RIPv1 で送信

v2 :　RIPv2(ブロードキャスト) で送信

v2m :　RIPv2(マルチキャスト) で送信

Recv :　受信モードを表示します。

Off :　RIP パケットを受信しない

v1 :　RIPv1 だけ受信

v2 :　RIPv1,RIPv2(ブロードキャスト / マルチキャスト) で受信

Add-Metric:

加算メトリック値を表示します。

Ignore :　RIPv2 認証つきパケットを受信した場合の動作

Off :　RIPv2 パケットを受信した場合、破棄しません。

On :　RIPv2 パケットを受信した場合、破棄します。

Passwd :　RIPv2 で認証機能を使用する場合のパスワードを表示します。

6) Routing Information Sources:

RIP の通信を行っている相手ルーターの情報を表示します。

Gateway :

相手ルーターの IP アドレスを表示します。

BadPackets:

RIP パケット内の異常パケット数の累積数を表示します。

BadRoutes :

RIP パケット内の経路情報に関する異常経路数の累積数を表示します。

Distance :

相手ルーターの優先度を表示します。現状は 120 固定で表示されます。

Update :　相手ルーターとの接続時間を表示します。

7) Distance:

自装置の RIP の優先度を表示します。

8) Entries:

保持している RIP エントリ数を表示します。インタフェース経路数は含まれません。

15.4.3 routestat bgp

[機能]

BGP 情報の表示

[入力形式]

- BGP 経路情報表示
  routestat bgp [<address>/<mask> [inexact]]
- BGP 情報サマリ表示
  routestat bgp summary
- BGP 相手装置情報表示
  routestat bgp nbr [<neighbor>]
- BGP VRF 経路情報表示
  routestat bgp vrf [<vrf_number>]

[オプション]

なし

[パラメタ]

<address>/<mask> [inexact]

経路情報を<address>/<mask>で指定します。デフォルトルートを表示するときは、"default"と指定することができます。

inexact を指定することにより、指定した<address>と IPv4 ルーティング情報のアドレスを比較し、<mask>まで一致した経路情報を表示することができます。

<neighbor>

BGP 相手装置の IP アドレスを指定します。

<vrf_number>

VRF 番号の定義番号を、10 進数値で指定します。

範囲	機種
0〜1	MR1000

[説明]

BGP の情報を表示します。

routestat bgp

すべての経路情報を表示します。<address>/<mask>で経路情報を指定することにより、特定の経路情報だけを表示することができます。経路情報を表示したときは、inexact を指定することにより、指定した経路情報に含まれる経路情報をすべて表示することができます。

routestat bgp summary

エントリ数や相手装置情報のサマリを表示します。

routestat bgp nbr

BGP 相手装置の情報を表示します。<neighbor>を指定することにより特定の相手装置の情報だけを表示することができます。

routestat bgp vrf

すべての VRF 経路情報を表示します。<vrf_number>を指定することにより、特定の VRF 番号経路情報だけを表示することができます。

[例]

以下に、表示例および表示内容を示します。

BGP 経路情報表示の場合

```
# routestat bgp
BGP local router ID is 192.168.40.2
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop         Metric     LocPrf Path
(1)  (2)              (3)             (4)        (5)   (6)
*> 20.0.0.0         0.0.0.0                              i
*> 30.30.30.0/24    172.16.10.30                         ?
*> 50.50.50.0/24    192.168.1.20          0        100  50 65000 i
*> 172.16.10.0/24   0.0.0.0                              ?
*> 172.16.20.0/24   0.0.0.0                              ?
*> 192.168.1.10/32  0.0.0.0                              ?
*> 192.168.1.20/32  0.0.0.0                              ?

Total number of prefixes 7   (7)
```

1) 状態 (Status)
   以下のどれかが表示されます。

   s :　他経路に集約されている経路

   *** :**　有効経路

   > :　ベストパス

   i :　IBGP で受信した経路

2) 経路のネットワークアドレス/マスクビット数 (Network)
   デフォルトルートの場合は 0.0.0.0/0 と表示されます。

3) ネクストホップ (Next Hop)
   bgp network コマンドで設定した経路やインタフェース経路は 0.0.0.0 と表示されます。

4) メトリック値 (Metric)

5) ローカル優先度 (LocPrf)

6) パス、オリジン (Path)
   経由した AS 番号とオリジンが表示されます。オリジンは以下のどれかが表示されます。

   i :　AS 内部で生成した経路

   e :　EGP を通して受信した経路

   ? :　BGP で学習したスタティック経路、RIP 経路、OSPF 経路およびインタフェース経路

7) BGP 経路の総数

BGP 経路情報表示（経路情報指定）の場合

```
# routestat bgp 100.1.1.0/24
BGP routing table entry for 100.1.1.0/24                                    (1)
Paths: (1 available, best #1, table Default-IP-Routing-Table)               (2)
  Advertised to non peer-group peers:                                       (3)
  192.168.1.2
  40                                                                        (4)
    10.1.1.4 from 10.1.1.4 (1.1.1.2)                                        (5)
      Origin incomplete, metric 0, valid, external, best                    (6)
      Last update: Thu Mar 13 14:39:40 2003                                 (7)
```

1) BGP routing table entry for 100.1.1.0/24
   指定した経路情報が表示されます。デフォルトルートの場合は、0.0.0.0/0 と表示されます。

2) Paths: (1 available, best #1, table Default-IP-Routing-Table)

   available：
   有効な経路数が表示されます。

   best： ベストパスが何番目かが表示されます。

   table: 使用しているテーブルが表示されます。

   no best path:
   ベストパスがない場合に表示されます。

   not advertised to any peer:
   COMMUNITY 属性 (NO_ADVERTISE) により、この経路を他の BGP 装置に広報しない場合に表示されます。

   not advertised to EBGP peer:
   COMMUNITY 属性 (NO_EXPORT) により、この経路を他の EBGP 装置に広報しない場合に表示されます。

   Advertisements suppressed by an aggregate.：
   AGGREGATOR 属性が設定されている場合に表示されます。

3) Advertised to non peer-group peers:
   この経路情報を他の BGP 装置に広報している場合は、その BGP 装置の IP アドレスとともに表示されます。広報していない場合は、"Not advertised to any peer"と表示されます。

4) 40
   AS パス属性が表示されます。自装置の経路の場合は LOCAL と表示されます。
   AGGREGATOR 属性が設定されている場合は、"aggregated by"に続き経路集約を行った BGP 装置の AS 番号と BGP ID が表示されます。

5) 10.1.1.4 from 10.1.1.4 (1.1.1.2)
   ネクストホップアドレスと、送信元 IPv4 アドレス（BGP ID）が表示されます。
   インタフェース経路の場合、ネクストホップアドレスと送信元 IPv4 アドレスは 0.0.0.0 と表示されます。
   スタティック経路の場合、送信元 IPv4 アドレスは 0.0.0.0 と表示されます。
   EBGP マルチホップ接続でリカーシブ経路が無効な場合は、"inaccessible"と表示されます。

6) Origin incomplete, metric 0, valid, external, best

   Origin： ORIGIN 属性が表示されます。"IGP"、"EGP"または、"incomplete"のどれかが表示されます。

   metric： Med メトリックが表示されます。

localpref:

ローカル優先度が表示されます。

valid:　経路情報が有効なことを示します。

external：

EBGP 接続の場合に表示されます。

aggregated, local:

集約された経路の場合に表示されます。

sourced:　インタフェース経路、スタティック経路、RIP、OSPF 経路の場合に表示されます。

sourced, local:

network コマンドで作成した経路の場合に表示されます。

atomic-aggregate:

ATOMIC_AGGREGATE 属性が設定されている場合に表示されます。

best:　ベストパスの場合に表示されます。

Community:

COMMUNITY 属性が設定されている場合に表示されます。"no-export" または、"no-advertise"のどれかが表示されます。

7) Last update: Thu Mar 13 14:39:40 2003

最後に更新された日時が表示されます。

構成定義情報にタイムゾーン (time zone <offset>) が指定されていない状態では GMT(グリニッジ標準時間) として表示されます。

BGP 情報サマリ表示の場合

```
# routestat bgp summary
BGP router identifier 10.1.1.1, local AS number 10                          (1)
4 BGP entries                                                               (2)
1 BGP AS-PATH entries                                                       (3)
0 BGP community entries                                                     (4)

(5)            (6) (7) (8)     (9)       (10) (11) (12)     (13)
Neighbor        V   AS MsgRcvd MsgSent    InQ OutQ Up/Down  State/PfxRcd
10.1.1.4        4   10     6       7       0    0 00:00:24        0

Total number of neighbors 1                                                (14)
#
```

1) 自装置の BGP ID と AS 番号
2) IPv4Unicast エントリ数
3) BGP 通信を行っている自律システム (AS) 数
4) 受信したコミュニティ属性の数
5) 相手装置の IP アドレス
6) 自装置の BGP 版数
7) 相手装置の AS 番号
8) 相手装置から受信したメッセージの累積数
9) 相手装置に送信したメッセージの累積数
10) 相手装置から受信し、処理待ち状態となっているメッセージ数
11) 相手装置への送信処理待ち状態となっているメッセージ数

12) 現在の状態になってからの経過時間

13) 状態または受信エントリ数

Established 状態の場合は受信エントリ数が表示されます。それ以外の場合は現在の状態が表示されます。

14) 相手装置数

BGP VRF 経路情報表示の場合

```
# routestat bgp vrf 0
[VRF 0]
BGP local router ID is 192.168.1.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf Path
(1)  (2)              (3)                (4)        (5)   (6)
*>i100.0.0.0        192.168.1.2                         100  ?
*> 192.168.1.0      0.0.0.0                                  ?

Total number of prefixes 2   (7)
```

1) 状態を表示します。以下のどれかが表示されます。

***** : 有効経路

> : ベストパス

i : IBGP で受信した経路

2) 経路のネットワークアドレス/マスクビット数 (Network)

デフォルトルートの場合は 0.0.0.0/0 と表示されます。

3) ネクストホップ (Next Hop)

インタフェース経路は 0.0.0.0 と表示されます。

4) メトリック値 (Metric)

5) ローカル優先度 (LocPrf)

6) パス、オリジン (Path)

オリジンは以下のどれかが表示されます。

i : AS 内部で生成した経路

e : EGP を通して受信した経路

? : BGP で学習したスタティック経路およびインタフェース経路

7) BGP VRF 経路の総数

BGP 相手装置情報表示の場合

```
# routestat bgp nbr
BGP neighbor is 192.168.40.1, remote AS 1234, local AS 5678, external link (1)
  BGP version 4, remote router ID 192.168.40.1                              (2)
  BGP state = Established, up for 00:00:24                                  (3)
  Last read 00:00:23, hold time is 90, keepalive interval is 30 seconds     (4)
  Configured hold time is 90, keepalive interval is 30 seconds              (5)
  Neighbor capabilities:                                                    (6)
    Route refresh: advertised and received(old and new)
    Address family IPv4 Unicast: advertised and received
  Received 3 messages, 0 notifications, 0 in queue                          (7)
  Sent 4 messages, 0 notifications, 0 in queue                              (8)
  Route refresh request: received 0, sent 0                                 (9)
  Minimum time between advertisement runs is 30 seconds                    (10)
  Update source is 10.1.1.1                                                (11)

 For address family: IPv4 Unicast                                          (12)
  NEXT_HOP is always this router                                           (13)
  1 accepted prefixes                                                      (14)
  2 announced prefixes                                                     (15)

  Connections established 1; dropped 0                                     (16)
Local host: 192.168.40.2, Local port: 1038                                 (17)
Foreign host: 192.168.40.1, Foreign port: 179                              (18)
Nexthop: 192.168.40.2                                                      (19)
Read thread: on  Write thread: off                                         (20)
```

1) BGP neighbor is 192.168.40.1, remote AS 1234, local AS 5678, external link
   相手装置の IP アドレス、相手装置の属する AS 番号, 自装置の属する AS 番号を示します。
   "external link"は BGP 接続形態が EBGP であることを示します。IBGP の場合は"internal link"と表示されます。

2) BGP version 4, remote router ID 192.168.40.1
   自装置の BGP 版数と相手装置の router-ID を示します。

3) BGP state = Established, up for 00:00:24
   BGP 状態と BGP 接続が確立してからの経過時間を示します。
   BGP 状態には以下があります。

   Idle :　アイドル状態

   Connect :
   接続中状態

   Active :　アクティブ状態

   OpenSent :
   OPEN メッセージ待ち状態

   OpenConfirm:
   BGP 接続確立のための KEEPALIVE メッセージ待ち状態

   Established:
   BGP 接続が確立した状態

4) Last read 00:00:23, hold time is 90, keepalive interval is 30 seconds
   相手装置から最後にメッセージ受信してからの経過時間、Holdtime タイマの値、Keepalive タイマの値を示します。

5) Configured hold time is 90, keepalive interval is 30 seconds
   自装置での Holdtime タイマの設定値、自装置での Keepalive タイマの設定値を示します。

6) Neighbor capabilities:
   相手装置とネゴシエートしたケイパビリティを以下の情報で表示します。

- Route refresh: advertised and received(old and new)
  Route refresh capability(OLD,NEW) を示します。
- Address family IPv4 Unicast: advertised and received
  Multiprotocol extension capability(IPv4 unicast) を示します。
- Address family VPNv4 Unicast: advertised and received
  Multiprotocol extension capability(VPNv4 unicast) を示します。

7) Received 3 messages, 0 notifications, 0 in queue
   受信したメッセージ数、受信した NOTIFICATION 数、未処理の受信メッセージ数を示します。
8) Sent 4 messages, 0 notifications, 0 in queue
   送信したメッセージ数、送信した NOTIFICATION 数、未処理の送信メッセージ数を示します。
9) Route refresh request: received 0, sent 0
   ROUTE_REFRESH メッセージの送受信メッセージ数を示します。
10) Minimum time between advertisement runs is 30 seconds
    アドバタイズメントタイマ値を示します。EBGP では 30 秒、IBGP では 5 秒が表示されます。
11) Update source is 10.1.1.1
    BGP セッションの自側に設定されている IP アドレスを示します。
12) For address family: IPv4 Unicast
    アドレスファミリを示します。
    "IPv4 Unicast"または、"VPNv4 unicast"が表示されます。
13) NEXT_HOP is always this router
    NEXTHOP を常に自装置のアドレスとして広報することを示します。
14) 1 accepted prefixes
    相手装置から受信した経路情報の数を示します。
15) 2 announced prefixes
    自装置から広報した経路情報の数を示します。
16) Connections established 1; dropped 0
    Established 状態となった回数、および、Established 状態で BGP 接続を終了した回数を示します。
17) Local host: 192.168.40.2, Local port: 1038
    BGP 接続に使用している自装置の IP アドレスとポート番号を示します。
18) Foreign host: 192.168.40.1, Foreign port: 179
    BGP 接続に使用している相手装置の IP アドレスとポート番号を示します。
19) Nexthop: 192.168.40.2
    NEXTHOP として使用する IP アドレスを示します。
20) Read thread: on Write thread: off
    受信 / 送信処理状況を示します。
    受信可能状態の場合は "Read thread: on"が表示され、受信不可状態の場合は"Read thread: off"が表示されます。
    送信処理中の場合は "Write thread: on"が表示され、送信処理を行っていない場合は"Write thread: off"が表示されます。

15.4.4　routestat ip ospf

[機能]

OSPF 情報の表示

[入力形式]

- OSPF プロトコル情報表示
  routestat ip ospf proto
- OSPF ルーティングテーブル表示
  routestat ip ospf
- LSA ヘッダ情報表示
  routestat ip ospf lsa
  routestat ip ospf lsa self
- ルータリンク情報表示
  routestat ip ospf lsa router
  routestat ip ospf lsa router <link_id>
  routestat ip ospf lsa router self
- ネットワークリンク情報表示
  routestat ip ospf lsa net
  routestat ip ospf lsa net <link_id>
  routestat ip ospf lsa net <link_id> adv <router_id>
  routestat ip ospf lsa net <link_id> self
  routestat ip ospf lsa net adv <router_id>
  routestat ip ospf lsa net self
- サマリリンク情報表示
  routestat ip ospf lsa sum
  routestat ip ospf lsa sum <link_id>
  routestat ip ospf lsa sum <link_id> adv <router_id>
  routestat ip ospf lsa sum <link_id> self
  routestat ip ospf lsa sum adv <router_id>
  routestat ip ospf lsa sum self
- ASBR サマリリンク情報表示
  routestat ip ospf lsa asbr
  routestat ip ospf lsa asbr <link_id>
  routestat ip ospf lsa asbr <link_id> adv <router_id>
  routestat ip ospf lsa asbr <link_id> self
  routestat ip ospf lsa asbr adv <router_id>
  routestat ip ospf lsa asbr self
- 外部ネットワークリンク情報表示
  routestat ip ospf lsa asex
  routestat ip ospf lsa asex <link_id>
  routestat ip ospf lsa asex <link_id> adv <router_id>
  routestat ip ospf lsa asex <link_id> self
  routestat ip ospf lsa asex adv <router_id>
  routestat ip ospf lsa asex self

- NSSA 外部ネットワークリンク情報表示
  routestat ip ospf lsa nssa
  routestat ip ospf lsa nssa <link_id>
  routestat ip ospf lsa nssa <link_id> adv <router_id>
  routestat ip ospf lsa nssa <link_id> self
  routestat ip ospf lsa nssa adv <router_id>
  routestat ip ospf lsa nssa self
- OSPF インタフェース情報表示
  routestat ip ospf if
- OSPF 隣接ルータ情報表示
  routestat ip ospf nbr
  routestat ip ospf nbr <router_id>
- OSPF 隣接ルータ情報詳細表示
  routestat ip ospf nbr detail

[オプション]

なし

[パラメタ]

<link_id>
リンク ID を、IPv4 アドレスをドット形式で指定します。

<router_id>
接続先ルータの OSPF ルータ ID を、IPv4 アドレスをドット形式で指定します。

[説明]

routestat ip ospf proto
OSPF プロトコルの一般的な情報を表示します。

routestat ip ospf
OSPF リンクステートデータベース情報の表示を行います。

routestat ip ospf lsa
LSA のヘッダ情報を一覧表示します。

routestat ip ospf lsa self
本装置が生成した LSA のヘッダ情報を一覧表示します。

routestat ip ospf lsa router
ルータリンク情報を表示します。

routestat ip ospf lsa router <link_id>
ルータリンク情報の中で、指定したルータ LSA を表示します。
<link_id>には、IPv4 アドレス形式でルータ ID を指定します。

routestat ip ospf lsa router self
本装置が生成したルータ LSA を表示します。

routestat ip ospf lsa net
ネットワークリンク情報を表示します。

routestat ip ospf lsa net <link_id>

ネットワークリンク情報の中で、指定したネットワークアドレスの LSA を表示します。
<link_id>には、ネットワークアドレスを指定します。

routestat ip ospf lsa net <link_id> adv <router_id>

ネットワークンク情報内の指定したネットワークアドレスの中で、指定したルータが広報した LSA を表示します。
<link_id>には、ネットワークアドレスを指定します。
<router_id>には、IPv4 アドレス形式で広報ルータ ID を指定します。

routestat ip ospf lsa net <link_id> self

ネットワークリンク情報内の指定したネットワークアドレスの中で、本装置が生成した LSA を表示します。
<link_id>には、ネットワークアドレスを指定します。

routestat ip ospf lsa net adv <router_id>

ネットワークリンク情報の中で、指定したルータが広報した LSA を表示します。
<router_id>には、IPv4 アドレス形式で広報ルータ ID を指定します。

routestat ip ospf lsa net self

本装置が生成したネットワークリンク情報を表示します。

routestat ip ospf lsa sum

サマリリンク情報を表示します。

routestat ip ospf lsa sum <link_id>

サマリリンク情報の中で、指定したエリア外ネットワークアドレスの LSA を表示します。
<link_id>には、エリア外ネットワークアドレスを指定します。

routestat ip ospf lsa sum <link_id> adv <router_id>

サマリリンク情報内の指定したエリア外ネットワークアドレスの中で、指定したルータが広報した LSA を表示します。
<link_id>には、エリア外ネットワークアドレスを指定します。
<router_id>には、IPv4 アドレス形式で広報ルータ ID を指定します。

routestat ip ospf lsa sum <link_id> self

サマリリンク情報内の指定したエリア外ネットワークアドレスの中で、本装置が生成した LSA を表示します。
<link_id>には、IPv4 アドレス形式でエリア外ネットワークアドレスを指定します。

routestat ip ospf lsa sum adv <router_id>

サマリリンク情報の中で、指定したルータが広報した LSA を表示します。
<router_id>には、IPv4 アドレス形式で広報ルータ ID を指定します。

routestat ip ospf lsa sum self

本装置が生成したサマリリンク情報を表示します。

routestat ip ospf lsa asbr

ASBR サマリリンク情報を表示します。

routestat ip ospf lsa asbr <link_id>

ASBR サマリリンク情報の中で、指定した AS 境界ルータの LSA を表示します。
<link_id>には、IPv4 アドレス形式で AS 境界ルータのルータ ID を指定します。

routestat ip ospf lsa asbr <link_id> adv <router_id>

ASBR サマリリンク情報内の指定した AS 境界ルータの中で、指定したルータが広報した LSA を表示します。
<link_id>には、IPv4 アドレス形式で AS 境界ルータのルータ ID を指定します。
<router_id>には、IPv4 アドレス形式で広報ルータ ID を指定します。

routestat ip ospf lsa asbr <link_id> self

ASBR サマリリンク情報内の指定した AS 境界ルータの中で、本装置が生成した LSA を表示します。
<link_id>には、IPv4 アドレス形式で AS 境界ルータのルータ ID を指定します。

routestat ip ospf lsa asbr adv <router_id>

ASBR サマリリンク情報の中で、指定したルータが広報した LSA を表示します。
<router_id>には、IPv4 アドレス形式で広報ルータ ID を指定します。

routestat ip ospf lsa asbr self

本装置が生成した ASBR サマリリンク情報を表示します。

routestat ip ospf lsa asex

外部ネットワークリンク情報を表示します。

routestat ip ospf lsa asex <link_id>

外部ネットワークリンク情報の中で、指定した外部ネットワークアドレスの LSA を表示します。
<link_id>には、外部ネットワークアドレスを指定します。

routestat ip ospf lsa asex <link_id> adv <router_id>

外部ネッワーク情報内の指定した外部ネットワークアドレスの中で、指定したルータが広報した LSA を表示します。
<link_id>には、外部ネットワークアドレスを指定します。
<router_id>には、IPv4 アドレス形式で広報ルータ ID を指定します。

routestat ip ospf lsa asex <link_id> self

外部ネットワーク情報内の指定した外部ネットワークアドレスの中で、本装置が生成した LSA を表示します。
<link_id>には、外部ネットワークアドレスを指定します。

routestat ip ospf lsa asex adv <router_id>

外部ネットワークリンク情報の中で、指定したルータが広報した LSA を表示します。
<router_id>には、IPv4 アドレス形式で広報ルータ ID を指定します。

routestat ip ospf lsa asex self

本装置が生成した外部ネットワークリンク情報を表示します。

routestat ip ospf lsa nssa

NSSA 外部ネットワークリンク情報を表示します。

routestat ip ospf lsa nssa <link_id>

NSSA 外部ネットワークリンク情報の中で、指定した NSSA 外部ネットワークアドレスの LSA を表示します。
<link_id>には、NSSA 外部ネットワークアドレスを指定します。

routestat ip ospf lsa nssa <link_id> adv <router_id>

NSSA 外部ネッワーク情報内の指定した NSSA 外部ネットワークアドレスの中で、指定したルータが広報した LSA を表示します。
<link_id>には、NSSA 外部ネットワークアドレスを指定します。
<router_id>には、IPv4 アドレス形式で広報ルータ ID を指定します。

routestat ip ospf lsa nssa <link_id> self

NSSA 外部ネットワーク情報内の指定した NSSA 外部ネットワークアドレスの中で、本装置が生成した LSA を表示します。
<link_id>には、NSSA 外部ネットワークアドレスを指定します。

routestat ip ospf lsa nssa adv <router_id>

NSSA 外部ネットワークリンク情報の中で、指定したルータが広報した LSA を表示します。
<router_id>には、IPv4 アドレス形式で広報ルータ ID を指定します。

routestat ip ospf lsa nssa self

本装置が生成した外部ネットワークリンク情報を表示します。

routestat ip ospf if

インタフェース特有の OSPF 関連情報を表示します。

一覧には LAN 情報または相手情報で、lan / remote ip ospf use on の設定したインタフェースだけが表示されます。

routestat ip ospf nbr

OSPF 隣接ルータに関する情報を表示します。

routestat ip ospf nbr <router_id>

OSPF 隣接ルータに関する情報の中で、指定した OSPF 隣接ルータの詳細情報を表示します。

<router_id>には、IPv4 アドレス形式で OSPF 隣接ルータ ID を指定します。

routestat ip ospf nbr detail

OSPF 隣接ルータに関する情報の詳細を一覧表示します。

[例]

OSPF プロトコル情報表示の場合

```
# routestat ip ospf proto
 OSPF Router ID: 3.3.3.3                                          (1)
 Supports only single TOS (TOS0) routes
 This implementation conforms to RFC2328
 RFC1583Compatibility flag is enabled                             (2)
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs    (3)
 Refresh timer 10 secs                                            (4)
 This router is an ABR, ABR type is: Standard (RFC2328)           (5)
 Number of external LSA 1                                         (6)
 Number of LSA 5                                                  (7)
 Number of areas attached to this router: 2                       (8)

 Area ID: 0.0.0.0 (Backbone)                                      (9)
   Number of interfaces in this area: Total: 1, Active: 1         (10)
   Number of fully adjacent neighbors in this area: 1             (11)
   SPF algorithm executed 14 times                                (12)
   Number of LSA 5                                                (13)

 Area ID: 0.0.0.3
   Number of interfaces in this area: Total: 1, Active: 1
   Number of fully adjacent neighbors in this area: 1
   Number of full virtual adjacencies going through this area: 0  (14)
   SPF algorithm executed 14 times
   Number of LSA 5
```

1) Router ID: 3.3.3.3

   ルータ ID を示します。

2) RFC1583Compatibility flag is enabled

   RFC1583 互換機能の有効 / 無効を示します。本装置では、常に enabled が表示されます。

3) SPF schedule delay 5 secs, Hold time between two SPFs 10 secs

   spf-delay タイマ値と spf-holdtime タイマ値を示します。

4) Refresh timer

   LSA リフレッシュタイマ値を示します。

5) This router is an

   本ルータがエリア境界ルータ / AS 境界ルータであることを示します。

6) Number of external LSA

   外部リンク情報の数を示します。

7) Number of LSA
LSA データベースに登録されている LSA 数を示します。

8) Number of areas attached to this router:
本ルータが接続しているエリア数を示します。

9) Area ID:
本ルータが接続しているエリアの ID およびエリア種別を表示します。

10) Number of interfaces in this area: Total: , Active:
本エリア内のインタフェース数合計および稼動中のインタフェース数を示します。

11) Number of fully adjacent neighbors in this area:
本エリア内で FULL 状態にあるルータの数を示します。

12) SPF algorithm executed
SPF 計算アルゴリズムの実行回数を示します。

13) Number of LSA
リンクステート情報数を示します。

14) Number of full virtual adjacencies going through this area:
エリアを経由しているバーチャルリンク数を示します。

OSPF ルーティングテーブル表示の場合

```
# routestat ip ospf
OSPF :
============ OSPF network routing table ============
(1)  (2)                  (3)        (4)
N    192.168.2.0/24       [10] area: 0.0.0.0
                          directly connected, lan0     (5)
N IA 192.168.3.0/24       [20] area: 0.0.0.0
                          via 192.168.2.3, lan0        (6)
N    192.168.12.1/32      [10] area: 0.0.0.0
                          directly connected, rmt0

============ OSPF router routing table =============
R    3.3.3.3              [10] area: 0.0.0.0, ABR
                          via 192.168.2.3, lan0
R    4.4.4.4           IA [20] area: 0.0.0.0, ASBR
                          via 192.168.2.3, lan0

============ OSPF external routing table ===========
N E2 0.0.0.0/0            [20/20] tag: 0
                          via 192.168.2.3, lan0
```

1) 経路の種別を示します。

N : ネットワーク経路を示します。

N IA : 他のエリアの経路であることを示します。(Inter Area)

R : 境界ルータの経路を示します。

N E1 : タイプ 1 外部経路を示します。

N E2 : タイプ 2 外部経路を示します。

2) ネットワークおよびマスク長を示します。

3) ネットワークまでのコストを示します。
タイプ 2 外部経路の場合は、OSPF コストと外部メトリック値を示します。

4) エリア ID を示します。

5) directly connected, lan0
ネットワークが当ルータに直接接続されていることを示します。

6) via 192.168.2.3, lan0
ネクストホップのルータアドレスおよび出力インタフェースを示します。

LSA ヘッダ情報表示の場合

```
# routestat ip ospf lsa

       OSPF Router ID (3.3.3.3)                                    (1)

               Router Link States (Area 0.0.0.0)                   (2)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
2.2.2.2         2.2.2.2           15 0x80000091 0x033a 2
3.3.3.3         3.3.3.3         1674 0x8000000c 0xa7a1 1

               Net Link States (Area 0.0.0.0)                      (3)

Link ID         ADV Router      Age  Seq#       CkSum
192.168.2.3     3.3.3.3         1674 0x80000004 0x16b2

               Summary Link States (Area 0.0.0.0)                  (4)

Link ID         ADV Router      Age  Seq#       CkSum  Route
192.168.3.0     3.3.3.3          647 0x80000006 0x983d 192.168.3.0/24

               ASBR-Summary Link States (Area 0.0.0.0)             (5)

Link ID         ADV Router      Age  Seq#       CkSum
4.4.4.4         3.3.3.3         1418 0x80000005 0xa68b

               Router Link States (Area 0.0.0.3)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
3.3.3.3         3.3.3.3           59 0x80000007 0xd179 1
4.4.4.4         4.4.4.4           66 0x80000008 0x94ab 1

               Net Link States (Area 0.0.0.3)

Link ID         ADV Router      Age  Seq#       CkSum
192.168.3.4     4.4.4.4           66 0x80000006 0x3385

               Summary Link States (Area 0.0.0.3)

Link ID         ADV Router      Age  Seq#       CkSum  Route
192.168.2.0     3.3.3.3          938 0x80000005 0xa532 192.168.2.0/24
192.168.12.1    3.3.3.3         1358 0x80000004 0x9330 192.168.12.1/32
```

```
               NSSA-external Link States (Area 0.0.0.1 [NSSA])     (6)

Link ID         ADV Router      Age  Seq#       CkSum  Route
0.0.0.0         3.3.3.3          829 0x80000001 0x9431 E2 0.0.0.0/0 [0x0]
192.168.2.0     11.11.11.11       90 0x80000006 0xefb4 E2 192.168.2.0/24 [0x0]
```

```
               AS External Link States                             (7)

Link ID         ADV Router      Age  Seq#       CkSum  Route
0.0.0.0         4.4.4.4          920 0x80000005 0x2b7f E2 0.0.0.0/0 [0x0]
```

1) OSPF Router ID (3.3.3.3)
   ルータ ID を表示します。
2) Router Link States (Area 0.0.0.0) ルータリンク情報を表示するエリア ID を示します。
3) Net Link States (Area 0.0.0.0) ネットワークリンク情報を表示するエリア ID を示します。
4) Summary Link States (Area 0.0.0.0) サマリリンク情報を表示するエリア ID を示します。
5) ASBR-Summary Link States (Area 0.0.0.0) ASBR サマリリンク情報を表示するエリア ID を示します。
6) NSSA-external Link States (Area 0.0.0.1 [NSSA]) NSSA 外部リンク情報を表示するエリア ID を示します。

7) AS External Link States 外部ネットワークリンク情報を示します。

ルータリンク情報表示の場合

```
# routestat ip ospf lsa router

       OSPF Router ID (3.3.3.3)


               Router Link States (Area 0.0.0.0)

  LS age: 37                                                    ┐ (1)
  Options: 0x2 (*|-|-|-|-|-|E|-)                                │
  Flags: 0x0                                                    │
  LS Type: router-LSA                                           │
  Link State ID: 2.2.2.2                                        │
  Advertising Router: 2.2.2.2                                   │
  LS Seq Number: 80000098                                       │
  Checksum: 0xf441                                              │
  Length: 48                                                    ┘
   Number of Links: 2                                             (2)

    Link connected to: a Transit Network                        ┐ (3)
     (Link ID) Designated Router address: 192.168.2.3           │
     (Link Data) Router Interface address: 192.168.2.2          │
      Number of TOS metrics: 0                                  │
       TOS 0 Metric: 10                                         │
                                                                │
    Link connected to: Stub Network                             │
     (Link ID) Network/subnet number: 192.168.12.1              │
     (Link Data) Network Mask: 255.255.255.255                  │
      Number of TOS metrics: 0                                  │
       TOS 0 Metric: 10                                         ┘
```

1) LS age: ～ Length: 48

   LSA ヘッダ情報を示します。

2) Number of Links: 2

   リンク数を示します。

3) Link connected to ～

   ルータリンク情報を示します。

ネットワークリンク情報表示の場合

```
# routestat ip ospf lsa net

       OSPF Router ID (3.3.3.3)


               Net Link States (Area 0.0.0.0)

  LS age: 235                                                   ┐ (1)
  Options: 0x2 (*|-|-|-|-|-|E|-)                                │
  LS Type: network-LSA                                          │
  Link State ID: 192.168.2.3 (address of Designated Router)     │
  Advertising Router: 3.3.3.3                                   │
  LS Seq Number: 80000005                                       │
  Checksum: 0x14b3                                              │
  Length: 32                                                    ┘
  Network Mask: /24                                             ┐ (2)
        Attached Router: 2.2.2.2                                │
        Attached Router: 3.3.3.3                                ┘
```

1) LS age: ～ Length: 32

   LSA ヘッダ情報を示します。

2) Network Mask: /24 ～

   ネットワークリンク情報を示します。

サマリリンク情報表示の場合

```
# routestat ip ospf lsa sum

       OSPF Router ID (3.3.3.3)


               Summary Link States (Area 0.0.0.0)

  LS age: 1161                                                          ┐ (1)
  Options: 0x2 (*|-|-|-|-|-|E|-)                                        │
  LS Type: summary-LSA                                                  │
  Link State ID: 192.168.3.0 (summary Network Number)                   │
  Advertising Router: 3.3.3.3                                           │
  LS Seq Number: 80000006                                               │
  Checksum: 0x983d                                                      │
  Length: 28                                                            ┘
  Network Mask: /24                                                     ┐ (2)
        TOS: 0  Metric: 10                                              ┘
```

1) LS age: 〜 Length: 28

   LSA ヘッダ情報を示します。

2) Network Mask: /24 〜

   サマリリンク情報を示します。

ASBR サマリリンク情報表示の場合

```
# routestat ip ospf lsa asbr

       OSPF Router ID (3.3.3.3)


               ASBR-Summary Link States (Area 0.0.0.0)

  LS age: 1609                                                          ┐ (1)
  Options: 0x2 (*|-|-|-|-|-|E|-)                                        │
  LS Type: ASBR-summary-LSA                                             │
  Link State ID: 4.4.4.4 (AS Boundary Router address)                   │
  Advertising Router: 3.3.3.3                                           │
  LS Seq Number: 80000005                                               │
  Checksum: 0xa68b                                                      │
  Length: 28                                                            ┘
  Network Mask: /0                                                      ┐ (2)
        TOS: 0  Metric: 10                                              ┘
```

1) LS age: 〜 Length: 28

   LSA ヘッダ情報を示します。

2) Network Mask: /0 〜

   ASBR サマリリンク情報を示します。

外部ネットワークリンク情報表示の場合

```
# routestat ip ospf lsa asex

       OSPF Router ID (3.3.3.3)

                AS External Link States

  LS age: 1196                                                    ┐ (1)
  Options: 0x2 (*|-|-|-|-|-|E|-)                                  │
  LS Type: AS-external-LSA                                        │
  Link State ID: 0.0.0.0 (External Network Number)                │
  Advertising Router: 4.4.4.4                                     │
  LS Seq Number: 80000005                                         │
  Checksum: 0x2b7f                                                │
  Length: 36                                                      ┘
  Network Mask: /0                                                ┐ (2)
        Metric Type: 2 (Larger than any link state path)          │
        TOS: 0                                                    │
        Metric: 20                                                │
        Forward Address: 0.0.0.0                                  │
        External Route Tag: 0                                     ┘
```

1) LS age: ～ Length: 36

   LSA ヘッダ情報を示します。

2) Network Mask: /0 ～

   外部ネットワークリンク情報を示します。

NSSA 外部ネットワークリンク情報表示の場合

```
# routestat ip ospf lsa nssa

       OSPF Router ID (11.11.11.11)


                NSSA-external Link States (Area 0.0.0.1 [NSSA])

  LS age: 906                                                     ┐ (1)
  Options: 0x0 (*|-|-|-|-|-|-|-)                                  │
  LS Type: AS-NSSA-LSA                                            │
  Link State ID: 0.0.0.0 (External Network Number For NSSA)       │
  Advertising Router: 3.3.3.3                                     │
  LS Seq Number: 80000001                                         │
  Checksum: 0x9431                                                │
  Length: 36                                                      ┘
  Network Mask: /0                                                ┐ (2)
        Metric Type: 2 (Larger than any link state path)          │
        TOS: 0                                                    │
        Metric: 1                                                 │
        NSSA: Forward Address: 0.0.0.0                            │
        External Route Tag: 0                                     ┘

  LS age: 46
  Options: 0x8 (*|-|-|-|N/P|-|-|-)
  LS Type: AS-NSSA-LSA
  Link State ID: 192.168.2.0 (External Network Number For NSSA)
  Advertising Router: 11.11.11.11
  LS Seq Number: 80000007
  Checksum: 0xedb5
  Length: 36
  Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        NSSA: Forward Address: 192.168.1.11
        External Route Tag: 0
```

1) LS age: ～ Length: 36

   LSA ヘッダ情報を示します。

2) Network Mask: ～

NSSA 外部ネットワークリンク情報を示します。

OSPF インタフェース情報表示の場合

```
# routestat ip ospf if
lan0 is up, line protocol is up                                          (1)
  Internet Address 192.168.3.4/24, Area 0.0.0.3                          (2)
    Router ID 4.4.4.4, Network Type BROADCAST, Cost: 10                  (3)
    Transmit Delay is 1 sec, State DR, Priority 1                        (4)
    Designated Router (ID) 4.4.4.4, Interface Address 192.168.3.4        (5)
    Backup Designated Router (ID) 3.3.3.3, Interface Address 192.168.3.3 (6)
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 (7)
      Hello due in 00:00:02                                              (8)
    Neighbor Count is 1, Adjacent neighbor count is 1                    (9)
    Crypt Sequence Number is 0                                          (10)
lan1 is down, line protocol is down
  OSPF not enabled on this interface
rmt0 is up, line protocol is up
  OSPF not enabled on this interface
rmt1 is down, line protocol is down
  OSPF not enabled on this interface
```

1) lan0 is up, line protocol is up

回線の状態を示します。

2) Internet Address 192.168.3.4 / 24, Area 0.0.0.3

インタフェースのアドレス、ネットワークマスク長およびエリア ID を示します。

3) Router ID 4.4.4.4, Network Type BROADCAST, Cost: 10

ルータ ID、ネットワークタイプおよびそのネットワークまでの出力コストを示します。

4) Transmit Delay is 1 sec, State DR, Priority 1

LSU パケット送信遅延時間、状態および指定ルータ優先度を示します。

5) Designated Router (ID) 4.4.4.4, Interface Address 192.168.3.4

指定ルータのルータ ID および IP アドレスを示します。

6) Backup Designated Router (ID) 3.3.3.3, Interface Address 192.168.3.3

副指定ルータのルータ ID および IP アドレスを示します。

7) Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

以下のタイマに関する情報を示します。

Hello :　Hello パケット送信間隔

Dead :　隣接ルータ停止確認間隔の時間

Wait :　指定ルータを認識するまでの時間

Retransmit :

パケット再送間隔

8) Hello due in 00:00:02

Hello パケットが再送されるまでの時間を示します。

9) Neighbor Count is 1, Adjacent neighbor count is 1

隣接関係にあるルータの数および FULL 状態にあるルータの数を示します。

10) Crypt Sequence Number is 0

送信する OSPF パケットの Crypt Sequence Number を示します。

MD5 認証を行わない場合には 0 が表示されます。

OSPF 隣接ルータ情報の表示の場合

```
# routestat ip ospf nbr
OSPF :
(1)            (2)   (3)            (4)         (5)            (6)
Neighbor ID    Pri   State          Dead Time   Address        Interface
4.4.4.4          1   Full/DR        00:00:33    192.168.3.4    lan0:192.168.3.3
2.2.2.2          1   Full/Backup    00:00:33    192.168.2.2    lan1:192.168.2.3
```

1) Neighbor ID

   隣接ルータの ID を示します。

2) Pri

   隣接ルータのプライオリティを示します。

3) State

   隣接ルータとの状態を示します。

4) Dead Time

   隣接ルータの停止を検出するまでの残り時間を示します。

5) Address

   隣接ルータの IP アドレスを示します。

6) Interface

   隣接ルータに接続する当ルータのインタフェース名、および IP アドレスを示します。

OSPF 隣接ルータ情報の詳細表示の場合

```
# routestat ip ospf nbr detail
 Neighbor 5.5.5.5, interface address 192.168.1.5              (1)
    In the area 0.0.0.0 via interface lan0                    (2)
    Neighbor priority is 1, State is Full, 11 state changes   (3)
    DR is 192.168.1.1, BDR is 192.168.1.5                     (4)
    Options is 0x02 (*|-|-|-|-|-|E|-)                         (5)
    Dead timer due in 00:00:36                                (6)
    Neighbor is up for 00:03:40                               (7)
    Database Summary List 0                                   (8)
    Link State Request List 0                                 (9)
    Link State Retransmission List 0                         (10)
```

1) Neighbor 5.5.5.5, interface address 192.168.1.5

   隣接ルータのルータ ID とアドレスを示します。

2) In the area 0.0.0.0 via interface lan0

   接続しているエリアとインタフェース名を示します。

3) Neighbor priority is 1, State is Full, 11 state changes

   隣接ルータの指定ルータ優先度、状態および状態の遷移回数を示します。

4) DR is 192.168.1.1, BDR is 192.168.1.5

   指定ルータおよび副指定ルータのアドレスを示します。

5) Hello パケットに設定されたオプションを示します。

   0x02 (*|-|-|-|-|-|E|-) :

   通常エリア

   0x00 (*|-|-|-|-|-|-|-) :

   スタブエリア

   0x08 (*|-|-|-|N/P|-|-|-) :

   準スタブエリア (nssa)

6) Dead timer due
隣接ルータの停止を検出するまでの残り時間を示します。

7) Neighbor is up for
隣接ルータと Hello パケットの交換を開始してからの経過時間を示します。

8) Database Summary List
データベースサマリリスト中の LSA 数を示します。

9) Link State Request List
リンクステート要求リスト中の LSA 数を示します。

10) Link State Retransmission List
リンクステート再送リスト中の LSA 数を示します。

15.4.5 routestat ip6 route

[機能]

ルーティングマネージャ情報の表示 (IPv6)

[入力形式]

- IPv6 経路情報表示
  routestat ip6 route
  routestat ip6 route <route-type>
  routestat ip6 route <prefix> / <prefixlen> [inexact]
- IPv6 経路情報数表示
  routestat ip6 route summary

[オプション]

なし

[パラメタ]

<route-type>

経路情報の種別を指定します。

- connected
  インタフェース経路情報を示します。
- static
  スタティック経路情報を示します。
- rip
  RIP 経路情報を示します。
- dns
  DNS 経路情報を示します。
- dhcp
  DHCP 経路情報を示します。

<prefix>/<prefixlen> [inexact]

経路情報を<prefix> / <prefixlen>で指定します。デフォルトルートを表示するときは、"default"と指定することができます。

inexact を指定することにより、指定した<prefix>と IPv6 ルーティング情報のプレフィックスを比較し、<prefixlenk>まで一致した経路情報を表示することができます。

[説明]

routestat ip6 route

すべての経路情報を表示します。

routestat ip6 route <route-type>

指定した種別の経路情報を表示します。

routestat ip6 route <prefix>/<prefixlen> [inexact]

指定した経路情報を表示します。inexact を指定することにより、指定した指定した経路情報に含まれる経路情報をすべて表示することができます。

routestat ip6 route summary

経路情報種別ごとの経路情報数とその合計を表示します。

[例]

以下に、表示例および表示内容を示します。

IPv6 全経路情報表示の場合

```
# routestat ip6 route
Codes: C - Connected, S - Static, R - RIP, DN - DNS, DH - DHCP,
       > - selected route, * - FIB route
 (1)       (2)                     (3)

C > * 2001:db8:10::/64 is directly connected, lan0
S > * 2001:db8:20::/64 [0/1] via fe80::1, lan0
R > * 2001:db8:30::/64 [120/2] via fe80::207:50ff:fee6:8e61, lan0, 01:08:41
R   * 2001:db8:40::/64 [120/0] via ::1(reject), lo0, 00:53:10
S     2001:db8:50::/64 [0/1] via fe80::2, lan1 inactive
          (4)

Total Routing Tables 4
```

1) 経路情報種別／優先経路／有効経路情報 (Codes)

経路情報の種別とベストパス、および、有効経路情報であることを示す記号が表示されます。

C :　インタフェース経路情報

S :　スタティック経路情報

R :　RIP 経路情報

DN:　DNS 経路情報

DH:　DHCP 経路情報

> :　ベストパス

*** :**　有効経路情報

2) あて先

経路情報のあて先がプレフィックス／プレフィックス長で表示されます。リンクローカルアドレスは表示されません。

デフォルトルート (::/0) は、"default"として表示されます。

3) 付加情報

経路情報の付加情報が表示されます。

"is directly connected, lan0"は、その経路情報が lan0 のインタフェース経路情報であることを示しています。

"[0/1]"は、優先度が 0 で、RIP メトリック値が 1 であることを示しています。

"via fe80::1, lan0 inactive"は、中継ルータアドレスとして lan0 を使用する fe80::1 が設定されていることを示しており、inactive は、現在、そのインタフェースが使用不可状態であることを示しています。

"via fe80::207:50ff:fee6:8e61, lan0, 01:08:41"は、中継ルータアドレスとして lan0 を使用する fe80::207:50ff:fee6:8e61 が設定されており、この経路情報が登録されてから 1 時間 8 分 41 秒が経過したことを示しています。

"(reject)"は、reject 経路情報であることを示しています。blackhole 経路情報のときは、"(blockhole)"と表示されます。reject 経路情報,blackhole 経路情報は、ループバックインタフェース lo0 を使用します。

4) 有効経路情報数

インタフェース経路情報を除く有効経路情報数が表示されます。なお、reject 経路情報数、blockhole 経路情報数も含まれます。

IPv6 経路情報数表示の場合

```
# routestat ip6 route summary
RouteSource   Networks        FIB
    (1)           (2)         (3)
connected            2          2
static               4          4
rip                  0          0
dns                  0          0
dhcp                 0          0
Total                6          6
```

1) 経路情報種別 (RouteSource)
   経路情報の種別が表示されます。
2) 経路情報総数 (Networks)
   経路情報の総数として有効な経路情報数、無効な経路情報数の合計が表示されます。
3) 有効経路情報数 (FIB)
   有効な経路情報としてルーティングテーブルに登録されている経路情報数が表示されます。

15.4.6　routestat ip6 rip

[機能]

RIP 情報の表示 (IPv6)

[入力形式]

- IPv6 RIP 経路情報表示
  routestat ip6 rip
- IPv6 RIP プロトコル情報表示
  routestat ip6 rip proto

[オプション]

なし

[パラメタ]

なし

[説明]

RIP(IPv6) に関する情報を表示します。

routestat ip6 rip

IPv6 RIP 経路情報に関連した情報を表示します。

routestat ip6 rip proto

IPv6 RIP プロトコルに関連した情報を表示します。

[例]

以下に、表示例および表示内容を示します。

IPv6 RIP 経路情報表示の場合

```
# routestat ip6 rip
Codes: R - RIP, C - Connected, S - Static, DN - DNS, DH - DHCP,
       > - best
   Network                    Next Hop             Interface  Metric  Time
(1)  (2)                       (3)                      (4)     (5)    (6)
S >  default                                          lan0       1
R >  100::/64                  fe80::1:0:0:20         lan1       2  02:54
R                              fe80::1:0:0:30         lan2       3  02:34
R >  200::1:0:0:0:0/64         fe80::1:0:0:30         lan2      16  01:23
C >  2001:db8:1:/64                                   lan0       1
```

1) 経路情報種別／優先経路 (Codes)
   経路情報の種別とベストパスであることを示す記号が表示されます。

   C :　インタフェース経路情報

   S :　スタティック経路情報

   R :　RIP 経路情報

   DN:　DNS 経路情報

   DH:　DHCP 経路情報

   > :　ベストパス

2) 経路情報 (Network)
経路情報がプレフィックス／プレフィックス長で表示されます。
デフォルトルート (::/0) は、"default"として表示されます。

3) ネクストホップ (Next Hop)
ネクストホップの IP アドレスが表示されます。
インタフェース経路情報、スタティック経路情報の場合は、空白となります。

4) インタフェース名
経路情報がネクストホップとして使用するインタフェース名が表示されます。

5) メトリック値 (Metric)
経路情報のメトリック値が表示されます。

6) 時間 (Time)
経路情報の有効期限までの残り時間が表示されます。メトリック値が 16 のときは、ガーベージ状態が終了するまでの残り時間が表示されます。

IPv6 RIP プロトコル情報表示の場合

```
# routestat ip6 rip proto
Routing Protocol is "ripng"
  Sending updates every 60 seconds with +/-50%, next due in 32 seconds       (1)
  Timeout after 180 seconds, garbage collect after 120 seconds               (2)
  Default redistribute metric is 1                                           (3)
  Redistributing: connected static dns dhcp                                  (4)
  Distance: (default is 120)                                                 (5)
  Entries: 6                                                                 (6)
```

1) 定期広報情報
定期広報タイマ値、ゆらぎ幅、および定期広報までの残り時間が表示されます。
"Sending updates every 60 seconds with +/-50%"は、定期広報タイマが 60 秒でゆらぎ幅が± 50%であることを示しています。
"next due in 32 seconds"は、次の定期広報が 32 秒後に行われることを示しています。

2) 有効期限タイマ/ガーベージタイマ情報
有効期限タイマ値、ガーベージタイマ値が表示されます。
"Timeout after 180 seconds"は有効期限タイマ値を示しています。
"garbage collect after 120 seconds"はガーベージタイマ値を示しています。

3) 再配布時メトリック値
RIP に再配布する経路情報のメトリック値が表示されます。

4) 再配布経路種別
RIP に再配布するように設定されている経路種別が表示されます。

Connected :
インタフェース経路情報

Static : スタティック経路情報

DNS : DNS 経路情報

DHCP : DHCP 経路情報

5) 優先度
RIP の優先度が表示されます。

6) エントリ数
RIP テーブルのエントリ数が表示されます。

15.4.7　routestat clear

[機能]

ルーティングプロトコル情報の統計情報クリア

[入力形式]

routestat clear

[オプション]

なし

[パラメタ]

なし

[説明]

ルーティングプロトコル (IPv4 / IPv6) の統計情報をクリアします。

15.4.8 routestat info

[機能]

ルーティングプロトコル主要情報表示 (IPv4)

[入力形式]

routestat info

[オプション]

なし

[パラメタ]

なし

[説明]

ルーティングプロトコル (IPv4) の主要な情報として、以下のコマンドの結果を表示します。
routestat ip route
routestat ip rip
routestat ip rip proto
routestat bgp
routestat bgp nbr
routestat ip ospf proto

15.5　回線状態の表示

15.5.1　laninfo

[機能]

LAN インタフェース情報の表示

[入力形式]

laninfo [<number>]

[オプション]

なし

[パラメタ]

<number>

- LAN インタフェース番号
  インタフェースの通番を、10 進数値で指定します。
  省略した場合は、すべての LAN インタフェースを指定したものとみなされます。

範囲	機種
0～19	MR1000

[説明]

LAN インタフェースの情報を表示します。

[例]

以下に、表示例を示します。

```
# laninfo
lan0                                                          --- (1)
  status        : up                                          --- (2)
    since       : Mar  6 20:59:30 2003                        --- (3)
  type          : normal                                      --- (4)
  * master port : mb, line0     (LinkUp, 100Mbps, FullDuplex)
 -- -----------   ---------     --------------------------------
 (5)    (6)          (7)                        (8)
      since     : Mar  6 20:59:30 2003                        --- (9)

lan1
  status        : up
    since       : Mar  6 20:59:29 2003
  type          : normal        (vlan bound from: lan3)
                                ----------------------
                                          (10)
  * master port : mb, line1     (LinkUp, 10Mbps, HalfDuplex)
      since     : Mar  6 20:59:29 2003
    backup port : slot0, line0  (LinkUp, 100Mbps, FullDuplex)  --- (11)
      since     : Mar  6 20:59:29 2003

lan3
  status        : up
    since       : Mar  6 20:59:29 2003
  type          : vlan  (VID=1, Priority=0)
                        -------------------
                                (12)
  * master port : lan1  (LinkUp)
      since     : Mar  6 20:59:29 2003

lan4
  status        : not attached

#
```

1) LAN 番号

2) LAN の状態

以下のどれかが表示されます。

up 動作中

down 未動作

not attached

構成定義不備により、動作していない

3) 通状態遷移時刻

「status」が現在の状態に変化した時刻を表示します。

4) LAN の種類

以下のどれかが表示されます。

normal 通常の LAN インタフェース

vlan VLAN インタフェース

5) 動作中のポート

動作中のポートを＊記号で示します。LAN ポートバックアップ機能を使用しない場合には、常に master ポートを指すことになります。

6) ポート名

以下を表示します。

master port

master ポートです。

backup port

backup ポートです。LAN ポートバックアップ機能を使用する場合だけ表示されます。

7) 利用する物理回線

利用する物理回線を表示します。VLAN インタフェースの場合には、出力先の LAN インタフェース名を表示します。

8) 回線の状態

VLAN インタフェースの場合には、出力先の物理インタフェースの LinkUp / LinkDown 状態だけを表示します。

9) 状態遷移時刻

回線の LinkUp / LinkDown 状態が、現在の状態に変化した時刻を表示します。

10) VLAN 情報

VLAN の出力先として選択されている物理 LAN インタフェースの場合には、どの VLAN インタフェースから出力先に選択されているかを表示します。

11) LAN バックアップ情報

バックアップポートの情報です。LAN ポートバックアップ機能の使用時だけ表示されます。

12) VLAN 情報

VLAN として定義されているインタフェースの場合には、VLAN ID、プライオリティを表示します。

15.5.2 lineis

[機能]

回線の状態表示

[入力形式]

lineis

[オプション]

なし

[パラメタ]

なし

[説明]

WAN 回線の接続状況を表示します。

[例]

以下に、各回線種別の表示例および表示内容を示します。

回線種別が専用線の場合

```
# lineis
line status             : connected                     --- (1)
communicated time       : 0000.00:30:03                 --- (2)
IPCP                    : opened                        --- (3)
negotiated IP address   : 192.168.1.1 -> 192.168.2.1    --- (4)
IPV6CP                  : opened                        --- (5)
BCP                     : opened                        --- (6)
MPLSCP                  : opened                        --- (7)
```

1) 回線状態

以下のどれかが表示されます。

enabling 同期確立中

synchronization failed

同期外れ状態

connected

通信中

disconnected

利用者指示による停止中

idle 回線未使用

以下の情報は、通信中 (「line status」が connected) の場合だけ表示されます。

2) 通信時間

通信時間が以下の形式で表示されます。

dddd.hh:mm:ss (日. 時:分:秒)

3) IPCP 状態

以下のどれかが表示されます。

opened　IPv4 利用可能

negotiating

IPCP ネゴシエーション中

closed　IPv4 利用不可能

4) 自側 IP アドレス→相手側 IP アドレス

IPCP のアドレスネゴシエーション結果が表示されます。アドレスネゴシエーションなしで接続した場合は、255.255.255.255 となります。

5) IPV6CP 状態

以下のどれかが表示されます。

opened　IPv6 利用可能

negotiating

IPv6CP ネゴシエーション中

closed　IPv6 利用不可能

6) BCP 状態

以下のどれかが表示されます。

opened　Bridge 利用可能

negotiating

BCP ネゴシエーション中

closed　Bridge 利用不可能

7) MPLSCP 状態

以下のどれかが表示されます。

opened　MPLS 利用可能

negotiating

MPLSCP ネゴシエーション中

closed　MPLS 利用不可能

回線種別が ISDN 回線の場合

```
# lineis
[SLOT0]                                                  --- (1)
line type             : ISDN                             --- (2)
dial no 0             : *                                --- (3)
dial no 1             : *                                --- (4)
<B1ch>
channel status        : connected(MP)                    --- (5)
call status           : call-out                         --- (6)
remote target         : tokyo.ap1 [remote 0 ap 0]        --- (7)
remote TEL no         : 4588*                            --- (8)
line speed            : 64000 bps                        --- (9)
communicated time     : 0000.00:00:01                    --- (10)
IPCP                  : opened                           --- (11)
negotiated IP address : 192.168.1.1 -> 255.255.255.255   --- (12)
DNS server address    : 255.255.255.255                  --- (13)
IPV6CP                : opened                           --- (14)
BCP                   : opened                           --- (15)
MPLSCP                : opened                           --- (16)
send/receive traffic  : 0%/0%                            --- (17)
<B2ch>
channel status        : connected(MP)
call status           : call-out
remote target         :  [remote 0 ap 0]
remote TEL no         : 4588*
line speed            : 64000 bps
communicated time     : 0000.00:00:04
IPCP                  : opened
negotiated IP address : 192.168.1.1 -> 255.255.255.255
DNS server address    : 255.255.255.255
IPV6CP                : opened
BCP                   : opened
MPLSCP                : opened
send/receive traffic  : 0%/0%
```

1) スロット番号

   スロット番号が表示されます。MR1000 では必ず [MB] (基本ボード) が表示されます。

2) 回線種別

   ISDN(ISDN 回線利用中) が表示されます。

3) 自局番号 0

   設定済みの自局番号 0 が表示されます。「*」以降はサブアドレスです。

4) 自局番号 1

   設定済みの自局番号 1 が表示されます。「*」以降はサブアドレスです。

5) 回線状態

   以下のどれかが表示されます。

   enabling 同期確立中

   synchronization failed

   同期外れ状態

   idle チャネル未使用

   disconnecting

   切断中

   connected

   通信中

   connected(MP)

   MP で通信中

   callin 着信処理中

alerting　相手呼出中

以下の情報は、通信中 (「channel status」が connected) の場合だけ表示されます。

6) 接続方向
以下のどれかが表示されます。

call-out　発信によって接続

call-in　着信によって接続

7) 相手ネットワーク名、接続先名 (テンプレート着信の場合はテンプレート番号、ユーザ ID)
接続中の相手ネットワーク名と接続先名が表示されます。
テンプレート着信による接続の場合には、テンプレート番号とユーザ ID が表示されます。

8) 接続先電話番号
接続先の電話番号が表示されます。

9) 回線速度
接続中の回線の回線速度が表示されます。

10) 通信時間
通信時間が以下の形式で表示されます。
dddd.hh:mm:ss (日. 時:分:秒)

11) IPCP 状態
以下のどれかが表示されます。

opened　IPv4 利用可能

negotiating
IPCP ネゴシエーション中

closed　IPv4 利用不可能

12) 自側 IP アドレス→相手側 IP アドレス
IPCP のアドレスネゴシエーション結果が表示されます。アドレスネゴシエーションなしで接続した場合は、255.255.255.255 となります。

13) DNS サーバアドレス
IPCP の DNS サーバアドレスネゴシエーション結果が表示されます。DNS サーバアドレスネゴシエーションなしで接続した場合は、255.255.255.255 となります。

14) IPV6CP 状態
以下のどれかが表示されます。

opened　IPv6 利用可能

negotiating
IPv6CP ネゴシエーション中

closed　IPv6 利用不可能

15) BCP 状態
以下のどれかが表示されます。

opened　Bridge 利用可能

negotiating
BCP ネゴシエーション中

closed　Bridge 利用不可能

16) MPLS 状態

以下のどれかが表示されます。

opened　MPLS 利用可能

negotiating

MPLSCP ネゴシエーション中

closed　MPLS 利用不可能

17) 送信回線使用率 / 受信回線使用率

データ送受信における回線使用率が表示されます。

回線種別がフレームリレーの場合

```
# lineis
[SLOT0]
line type             : FR 128Kbps                    ---(1)
<DLCI: 17>
channel status        : synchronization failed        ---(2)
communicated time     : 0000.00:00:00                 ---(3)
remote target         : rmt0.ap0 [remote 0 ap 0]      ---(4)
remote DLCI           : 0                             ---(5)
remote IP address     : 192.168.100.2                 ---(6)
local IP address      : 192.168.100.1                 ---(7)
CIR                   : 0                             ---(8)
send/receive traffic  : 0%/0%                         ---(9)
```

1) 回線種別

回線種別 (FR) と回線速度が表示されます。

FR 64Kbps

フレームリレー (64Kbps)

FR 128Kbps

フレームリレー (128Kbps)

FR 192Kbps

フレームリレー (192Kbps)

FR 256Kbps

フレームリレー (256Kbps)

FR 384Kbps

フレームリレー (384Kbps)

FR 512Kbps

フレームリレー (512Kbps)

FR 768Kbps

フレームリレー (768Kbps)

FR 1152Kbps

フレームリレー (1Mbps)

FR 1536Kbps

フレームリレー (1.5Mbps)

以下は定義された DLCI 単位に表示されます。

2) チャネル状態

以下のどれかが表示されます。

enabling　同期確立中

synchronization failed

同期外れ状態

connected

通信中

disconnected

利用者指示による停止中

3) 通信時間

通信時間が以下の形式で表示されます。

dddd.hh:mm:ss (日. 時:分:秒)

4) 相手ネットワーク名、接続先名

接続中の相手ネットワーク名と接続先名が表示されます。

5) 相手 DLCI

相手 DLCI が表示されます。

6) 相手 IP アドレス

相手 IP アドレスが表示されます。

7) 自 IP アドレス

自 IP アドレスが表示されます。

8) CIR

定義した CIR(認定情報速度) が表示されます。

9) 送信回線使用率 / 受信回線使用率

データ送受信における回線使用率が表示されます。

モデム接続の場合

```
# lineis
[COM]
line type             : MODEM                              --- (1)
line status           : connected                          --- (2)
call status           : call-out                           --- (3)
remote target         : rmt0.ap0 [remote 0 ap 0]           --- (4)
remote TEL no         : 1002*                              --- (5)
line speed            : 28800 bps                          --- (6)
communicated time     : 0000.00:00:41                      --- (7)
IPCP                  : opened                             --- (8)
negotiated IP address : 192.168.2.1 -> 255.255.255.255    --- (9)
DNS server address    : 255.255.255.255                    --- (10)
IPV6CP                : closed                             --- (11)
BCP                   : closed                             --- (12)
send/receive traffic  : 0%/0%                              --- (13)
```

1) 回線種別

MODEM が表示されます。

2) 回線状態

以下のどれかが表示されます。

enabling　同期確立中

synchronization failed
同期外れ状態

idle 回線未使用

disconnecting
切断中

connected
通信中

callin 着信処理中

alerting 相手呼出中

以下の情報は、通信中 (「line status」が connected) の場合だけ表示されます。

3) 接続方向
以下のどれかが表示されます。

call-out 発信によって接続

call-in 着信によって接続

4) 相手ネットワーク名、接続先名
接続中の相手ネットワーク名と接続先名が表示されます。

5) 接続先電話番号
接続先の電話番号が表示されます。

6) 回線速度
接続中の回線の回線速度が表示されます。

7) 通信時間
通信時間が以下の形式で表示されます。
dddd.hh:mm:ss (日. 時:分:秒)

8) IPCP 状態
以下のどれかが表示されます。

opened IPv4 利用可能

negotiating
IPCP ネゴシエーション中

closed IPv4 利用不可能

9) 自側 IP アドレス→相手側 IP アドレス
IPCP のアドレスネゴシエーション結果が表示されます。アドレスネゴシエーションなしで接続した場合は、255.255.255.255 となります。

10) DNS サーバアドレス
IPCP の DNS サーバアドレスネゴシエーション結果が表示されます。DNS サーバアドレスネゴシエーションなしで接続した場合は、255.255.255.255 となります。

11) IPV6CP 状態
以下のどれかが表示されます。

opened IPv6 利用可能

negotiating
IPv6CP ネゴシエーション中

closed　IPv6 利用不可能

12) BCP 状態
以下のどれかが表示されます。

opened　Bridge 利用可能

negotiating
BCP ネゴシエーション中

closed　Bridge 利用不可能

13) 送信回線使用率 / 受信回線使用率
データ送受信における回線使用率が表示されます。

15.5.3 isdnstat

[機能]

ISDN 関連の統計情報の表示

[入力形式]

isdnstat -{D | d | r} [<index>]
isdnstat clear -{D | d | r} [<index>]

[オプション]

-D

データ通信の発着信統計情報を一覧表示します。以下の情報が表示されます。

- 発信回数
- 相手ビジーによる発信失敗回数
- 他の網理由によるエラーによる発信失敗回数
- 着信回数
- 着信拒否回数

-d

データ通信としての課金および時間の統計情報を一覧表示します。以下の情報が表示されます。

- 発信での通信総時間
- 総課金
- 1 回あたりの最長時間、そのときの課金、および接続先
- 1 回あたりの最高課金、そのときの時間、および接続先
- 最終接続の時間、課金、および接続先

-r

課金および時間の統計情報を一覧表示します。以下の情報が表示されます。

- 接続先定義ごとの、通信総時間および総課金

clear

統計情報をクリアします。対象となるデータを表示するオプションと同時に指定すると該当する統計情報のみクリアします。

[パラメタ]

<index>

対象とする wan 定義番号を指定します。
省略した場合は、すべての wan 定義が対象となります。

[説明]

ISDN 接続関連の統計情報を表示します。

[例]

以下に、各オプションの表示例および表示内容を示します。

発着信統計情報を表示する場合 (-D 指定時)

```
# isdnstat -D
[wan 0]
call setup count    = 2  --- (1)
call busy count     = 0  --- (2)
call error count    = 0  --- (3)
called accept count = 0  --- (4)
called reject count = 0  --- (5)
```

1) 発信の回数
2) 着ユーザビジーによって発信失敗した回数
3) 着ユーザビジー以外の網理由で発信失敗した回数
4) 着信の回数
5) 着信を拒否した回数

課金統計情報を表示する場合 (-d 指定時)

```
# isdnstat -d
[wan 0]
total time for callout  = 0000.00:03:04      --- (1)
total charge            = 10                 --- (2)
peek time   remote      = internet.ISP-1     --- (3)
            time        = 0000.00:02:57      --- (4)
            charge      = 10                 --- (5)
peek charge remote      = internet.ISP-1     --- (6)
            time        = 0000.00:02:57      --- (7)
            charge      = 10                 --- (8)
last        remote      = intranet.OFFICE-I  --- (9)
            time        = 0000.00:00:07      --- (10)
            charge      = 0                  --- (11)
```

1) 発信接続の総通信時間
2) 総課金額
3) 最長接続時の相手名
4) 最長接続時の接続時間
5) 最長接続時の課金額
6) 最高課金時の相手名
7) 最高課金時の接続時間
8) 最高課金時の課金額
9) 最終接続時の相手名
10) 最終接続時の接続時間
11) 最終接続時の課金額

相手ごとのデータ通信課金統計情報を表示する場合 (-r 指定時)

```
# isdnstat -r
remote  ap    charge  time
------  --    ------  ----
 (1)    (2)    (3)     (4)

     0   0        10  0000.00:02:57
     1   0         0  0000.00:00:07
```

1) 相手定義番号

2) 接続先定義番号

3) 課金の合計金額

4) 接続の合計時間

15.5.4　frstat

[機能]

フレームリレーの PVC 状態、および統計情報の表示

[入力形式]

frstat [<dlci>]
frstat clear

[オプション]

なし

[パラメタ]

<dlci>

- DLCI 番号
  表示する DLCI の番号を、16～991 の 10 進数値で指定します。
  省略した場合は、すべての DLCI を指定したものとみなされます。

clear

統計情報をクリアします。

[説明]

フレームリレーの PVC 状態および統計情報を表示します。

[例]

以下に、表示例を示します。

```
# frstat

[DLCI: 16]    --- (1)
  CIR                   : 0           --- (2)
  trans state           : active      --- (3)
  load state            : send(min)   --- (4)
  possible send bytes   : 819         --- (5)
  max send bytes        : 819         --- (6)
  max send bytes(lower) : 819         --- (7)
  max send bytes(upper) : 819         --- (8)
  max send bytes(CIR)   : 819         --- (9)
  sending bytes         : 0           --- (10)
  send throughput       : 0 bytes/s   --- (11)
  waiting send packets  : 0           --- (12)
  fecn received         : 0           --- (13)
  becn received         : 0           --- (14)
  send errors           : 0           --- (15)
  receive errors        : 0           --- (16)
  send bytes            : 37141       --- (17)
  receive bytes         : 1426753     --- (18)

[DLCI: 17]
  CIR                   : 0
  trans state           : active
  load state            : send(min)
  possible send bytes   : 819
  max send bytes        : 819
  max send bytes(lower) : 819
  max send bytes(upper) : 819
  max send bytes(CIR)   : 819
  sending bytes         : 0
  send throughput       : 0 bytes/s
  waiting send packets  : 0
  fecn received         : 0
  becn received         : 0
  send errors           : 0
  receive errors        : 0
  send bytes            : 0
  receive bytes         : 0

#
```

以下に表示内容を示します。

1) DLCI 番号

2) CIR 値

3) 伝送制御状態

- **disable**

  enable 指示待ち

- **inactive**

  enable 状態 (inactive)

- **active**　enable 状態 (active)

4) 輻輳制御状態

- **stop**　停止状態

- **send(min)**

  下限値で送信中

- **send(min..cir)**

  下限から CIR で送信中

- **send(cir)**

  CIR で送信中

- **send(cir..max)**

  CIR から上限で送信中

- **send(max)**

  上限値で送信中

5) 送出可能データ量 (byte)
6) Tc(100ms) 時間内に送出できる最大データ長 (byte)
7) Tc(100ms) 時間内に送出できる最大データ長の下限値 (byte)
8) Tc(100ms) 時間内に送出できる最大データ長の上限値 (byte)
9) Tc(100ms) 時間内に送出できる最大データ長に CIR 値適用 (byte)
10) 送信中バイト数 (残り)
11) 送信スループット (byte/s)
12) 送信待ちパケット数
13) 1 時間毎の FECN ON フレーム受信回数
14) 1 時間毎の BECN ON フレーム受信回数
15) 送信フレーム破棄回数 (合計)
16) 受信フレーム破棄回数 (合計)
17) 送信バイト数 (合計)
18) 受信バイト数 (合計)

15.5.5 mdmstat

[機能]

モデム関連の統計情報の表示

[入力形式]

mdmstat -{D|d|r}
mdmstat clear [-{D|d|r}]

[オプション]

-D

データ通信の発着信統計情報を一覧表示します。以下の情報が表示されます。

- 発信回数
- 相手ビジーによる発信失敗回数
- 他の網理由によるエラーによる発信失敗回数
- 着信回数
- 着信拒否回数

-d

データ通信としての時間の統計情報を一覧表示します。以下の情報が表示されます。

- 発信での通信総時間
- 1 回あたりの最長時間、および接続先
- 最終接続の時間、および接続先

-r

時間の統計情報を一覧表示します。以下の情報が表示されます。

- 接続先定義ごとの、通信総時間

clear

統計情報をクリアします。対象となるデータを表示するオプションと同時に指定すると該当する統計情報のみクリアします。

[説明]

モデム接続関連の統計情報を表示します。

[例]

以下に、各オプションの表示例および表示内容を示します。

発着信統計情報を表示する場合 (-D 指定時)

```
# mdmstat -D
[COM]
call count          = 2  --- (1)
call busy count     = 0  --- (2)
call error count    = 0  --- (3)
called accept count = 0  --- (4)
called reject count = 0  --- (5)
```

1) 発信の回数
2) 着ユーザビジーによって発信失敗した回数

3)　着ユーザビジー以外の網理由で発信失敗した回数

4)　着信の回数

5)　着信を拒否した回数

接続時間統計情報を表示する場合 (-d 指定時)

```
# mdmstat -d
[COM]
total time for callout  = 0000.00:03:04      --- (1)
peek time   remote      = internet.ISP-1     --- (2)
            time        = 0000.00:02:57      --- (3)
last        remote      = intranet.OFFICE-I  --- (4)
            time        = 0000.00:00:07      --- (5)
```

1)　発信接続の総通信時間

2)　最長接続時の相手名

3)　最長接続時の接続時間

4)　最終接続時の相手名

5)　最終接続時の接続時間

相手ごとのデータ通信統計情報を表示する場合 (-r 指定時)

```
# mdmstat -r
remote  ap      time
------  --      ----
 (1)    (2)      (3)

     0   0      0000.00:02:57
     1   0      0000.00:00:07
```

1)　相手定義番号

2)　接続先定義番号

3)　接続の合計時間

15.5.6 tempstat

[機能]

テンプレート着信の通信状態、および統計情報の表示

[入力形式]

tempstat
tempstat -i [-I <interface>] [-t <temp_no>]
tempstat -s [-t <temp_no>]
tempstat clear [-t <temp_no>]

[オプション]

オプションを指定しなかった場合は、-i -s を指定したものとみなされます。

-i

インタフェースごとの通信状態を表示します。

-s

統計情報を表示します。

[パラメタ]

-I <interface>

表示するインタフェースを指定します。

-t <temp_no>

表示するテンプレート定義番号を指定します。
省略した場合には、すべてのテンプレートを順にソートして表示します。

clear

統計情報をクリアします。

[説明]

テンプレート着信で接続した相手との通信状態やテンプレート着信の統計情報を表示します。

[例]

以下に表示例と、その内容を示します。

インタフェースごとの通信状態を表示する場合 (-i 指定時)

```
# tempstat -i
[Template 0]
status                : active                                    --- (1)
Number of interfaces  :  Active: 1, Free: 9                       --- (2)

rmt30(user id:kawagoe-1)                                          --- (3)
  status              : connected                                 --- (4)
    detail            : connected                                 --- (5)
    since             : Aug 26 10:52:46 2004                      --- (6)
    communicated time : 0000.00:30:03                             --- (7)
  speed               : 128000 bps                                --- (8)
    send traffic      : 1432 byte/s                               --- (9)
    receive traffic   : 10.4K byte/s                              --- (10)
  type                : ISDN                                      --- (11)
    IPCP              : opened                                    --- (12)
      local address   :   192.168.1.1                             --- (13)
      DNS server      :   192.168.2.5                             --- (14)
    IPV6CP            : opened                                    --- (15)

[Template 1]
status                : active                                    --- (1)
Number of interfaces  :  Active: 1, Free: 7                       --- (2)

rmt40(user id:sayama-5)                                           --- (3)
  status              : connected                                 --- (4)
    detail            : connected                                 --- (5)
    since             : Aug 26 10:52:16 2004                      --- (6)
    communicated time : 0000.00:29:33                             --- (7)
  speed               : 128000 bps                                --- (8)
    send traffic      : 1032 byte/s                               --- (9)
    receive traffic   : 10.2K byte/s                              --- (10)
  type                : ISDN                                      --- (11)
    IPCP              : opened                                    --- (12)
      local address   :   192.168.1.2                             --- (13)
      DNS server      :   192.168.2.6                             --- (14)
    IPV6CP            : opened                                    --- (15)
```

1) テンプレート動作状態が表示されます。以下のいずれかが表示されます。

   - active
     動作
   - inactive
     非動作

2) テンプレートで予約されたインタフェースの使用状況が表示されます。

3) 定義内容
   インタフェース名および着信した接続先のユーザ ID が表示されます。(認証せずに着信した場合にはユーザ ID に unknown が表示されます。)

4) 接続状態
   現在の接続状態を表示します。以下のいずれかが表示されます。

   - connected
     接続状態

5) 接続詳細状態
   接続状態の詳細がある場合に表示されます。

   - 通信手段が ISDN の場合
     チャネルの詳細状態が表示されます。

     ◇ disc-to-sync
       接続中に同期外れを検出し、切断処理中

◇ disc-to-idle
切断処理中

◇ connected
接続状態

6) 状態遷移時刻
「status」が現在の状態に変化した時刻を表示します。

7) 通信時間
dddd.hh:mm:ss の形式で通信時間を表示します。dddd=日数、hh=時間、mm=分、ss=秒を示します。
ISDN の場合、「status」が connected の場合にのみ表示されます。

8) 伝送速度
現在の伝送速度を表示します。MP の場合は合計速度が表示されます。

9) 送信レート
最新のデータ送信レートを表示します。

10) 受信レート
最新のデータ受信レートを表示します。

11) 通信手段
相手システムとの通信手段を表示します。以下のいずれかが表示されます。

- ISDN
  ISDN 回線

以下の情報は PPP を利用して通信する場合に限り表示されます。

12) IPCP 状態
IPv4 通信の状態を表示します。以下のいずれかが表示されます。

- opened
  通信可能
- negotiating
  ネゴシエーション中
- closed
  通信不可

13) IPv4 アドレス
IPCP ネゴシエーションにより決定された自側 IPv4 アドレスが、表示されます。アドレスネゴシエーションが行えなかった場合には 255.255.255.255 となります。

14) DNS サーバアドレス
IPCP ネゴシエーションにより決定された DNS サーバアドレスを表示します。DNS サーバアドレスネゴシエーションが行えなかった場合には、255.255.255.255 となります。

15) IPV6CP 状態
IPv6 通信の状態を表示します。以下のいずれかが表示されます。

- opened
  通信可能
- negotiating
  ネゴシエーション中
- closed
  通信不可

テンプレート着信の統計情報を表示する場合 (-s 指定時)

```
# tempstat -s
[Template 0]
pooled interface      = rmt30-rmt39        --- (1)
accept count          = 2                  --- (2)
reject count          = 1                  --- (3)
total time            = 0000.00:13:04      --- (4)
peek time             = 0000.00:12:57      --- (5)
last time             = 0000.00:00:07      --- (6)

[Template 1]
pooled interface      = rmt40-rmt37        --- (1)
accept count          = 5                  --- (2)
reject count          = 2                  --- (3)
total time            = 0000.00:19:14      --- (4)
peek time             = 0000.00:10:17      --- (5)
last time             = 0000.00:00:13      --- (6)
```

1) テンプレート着信で使用する予約インタフェース
2) 着信成功回数
3) 着信拒否回数
4) 接続時間の総和
5) 最長接続時の接続時間
6) 最終接続時の接続時間

15.6　接続状態の表示

15.6.1　apstat

[機能]

通信状態の表示

[入力形式]

apstat
apstat <remote_number> [<ap_number>]
apstat <ap_name>

[オプション]

なし

[パラメタ]

<remote_number>

- 相手定義番号
  相手ネットワークの通し番号を、10 進数値で指定します。

範囲	機種
0～99	MR1000

<ap_number>

- 接続先定義番号
  相手ネットワーク内の接続先定義番号を、10 進数値で指定します。

範囲	機種
0～99	MR1000

<ap_name>

- 接続先名
  接続先の名前を指定します。

[説明]

指定した相手との通信状態を表示します。
相手定義番号と接続先定義番号の両方を指定した場合、または接続先名を指定した場合には、指定した接続先情報の接続状態が表示されます。
相手定義番号だけを指定した場合には、指定したネットワーク情報のすべての接続先情報の接続状態が表示されます。
相手情報が指定されなかった場合には、すべてのネットワーク情報のすべての接続先情報の接続状態が表示されます。

[例]

以下に表示例と、その内容を示します。

```
# apstat
remote 0 ap 0         : Internet.isp                                  --- (1)
  status              : connected                                     --- (2)
    detail            : connected                                     --- (3)
    since             : Aug 26 10:52:46 2002                          --- (4)
    communicated time : 0000.00:30:03                                 --- (5)
  speed               : 128000 bps                                    --- (6)
    send traffic      : 1432 byte/s                                   --- (7)
    receive traffic   : 10.4K byte/s                                  --- (8)
  type                : ISDN                                          --- (9)
    IPCP              : opened                                        --- (10)
      local address   :   192.168.1.1                                 --- (11)
      DNS server      :   192.168.2.5                                 --- (12)
    IPV6CP            : opened                                        --- (13)
    BCP               : opened                                        --- (14)
    MPLSCP            : opened                                        --- (15)

remote 1 ap 0         : yokohama.fr0
  status              : connected
    since             : Aug 26 10:52:46 2002
  speed               : 64000 bps
    send traffic      : 2245 byte/s
    receive traffic   : 42 byte/s
  type                : FR

remote 2 ap 0         : kawasaki.vpn
  status              : connected
    since             : Aug 26 10:52:46 2002
  speed               : not available
    send traffic      : not available
    receive traffic   : not available
  type                : IPsec/IKE
     exchange type    : aggressive                                    --- (16)
     IKE SA           : established                                   --- (17)
     IPsec SA         : established                                   --- (18)
```

1) 定義内容

構成定義で設定された相手ネットワーク名および接続先名が表示されます。

2) 接続状態

現在の接続状態を表示します。以下のどれかが表示されます。

- not attached

  構成定義矛盾などにより利用不可

- linkoff

  利用する回線がダウン

- connectable

  未接続状態

- connected

  接続状態

- force down

  閉塞状態

- watch failed

  接続先監視による通信障害検出状態

3) 接続詳細状態

接続状態の詳細がある場合に表示されます。

- 通信手段が ISDN の場合
  チャネルの詳細状態が表示されます。
  - ◇ disc-to-sync
    接続中に同期外れを検出し、切断処理中
  - ◇ disc-to-idle
    切断処理中
  - ◇ connected
    接続状態
  - ◇ callin
    着信処理中
  - ◇ alerting
    相手呼出中
- 通信手段が PPPoE の場合
  PPPoE の詳細状態が表示されます。
  - ◇ waitPADO
    PADO 受信待ち
  - ◇ waitPADS
    PADS 受信待ち
  - ◇ connected
    接続状態
- 通信手段が MODEM の場合
  - ◇ disc-to-sync
    接続中に同期外れを検出し、切断処理中
  - ◇ disc-to-idle
    切断処理中
  - ◇ connected
    接続状態
  - ◇ callin
    着信処理中
  - ◇ alerting
    相手呼出中

4) 状態遷移時刻
   「status」が現在の状態に変化した時刻を表示します。
5) 通信時間
   dddd.hh:mm:ss の形式で通信時間を表示します。dddd=日数、hh=時間、mm=分、ss=秒を示します。
   「Type」が ISDN または PPPoE または MODEM の場合にだけ表示されます。
   ISDN または PPPoE の場合、「status」が connected の場合にだけ表示されます。
   MODEM の場合、「detail」が alerting、connected、disc-to-idle、disc-to-sync の場合だけ表示されます。
6) 伝送速度
   現在の伝送速度を表示します。MP の場合は合計速度が表示されます。

7) 送信レート
最新のデータ送信レートを表示します。

8) 受信レート
最新のデータ受信レートを表示します。

9) 通信手段
相手システムとの通信手段を表示します。以下のどれかが表示されます。

- HSD
  専用線
- ISDN
  ISDN 回線
- FR
  FrameRelay 回線
- IPv4
  IPv6-over-IPv4 tunnel
- PPPoE
  PPPoE
- IPsec
  IPsec(手動設定鍵を利用)
- IPsec/IKE
  IPsec(IKE による鍵交換を利用)
- overlap
  overlap ap 機能を利用
- mpls
  MPLS LSP
- MODEM
  モデム

以下の情報は PPP を利用して通信する場合に限り表示されます。

10) IPCP 状態
IPv4 通信の状態を表示します。以下のどれかが表示されます。

- opened
  通信可能
- negotiating
  ネゴシエーション中
- closed
  通信不可

11) IPv4 アドレス
IPCP ネゴシエーションにより決定された自側 IPv4 アドレスが、表示されます。アドレスネゴシエーションが行えなかった場合には 255.255.255.255 となります。

12) DNS サーバアドレス
IPCP ネゴシエーションにより決定された DNS サーバアドレスを表示します。DNS サーバアドレスネゴシエーションが行えなかった場合には、255.255.255.255 となります。

13) IPV6CP 状態
IPv6 通信の状態を表示します。以下のどれかが表示されます。

- opened
  通信可能
- negotiating
  ネゴシエーション中
- closed
  通信不可

14) BCP 状態
ブリッジ通信の状態を表示します。以下のどれかが表示されます。

- opened
  通信可能
- negotiating
  ネゴシエーション中
- closed
  通信不可

15) MPLSCP 状態
MPLS 通信の状態を表示します。以下のどれかが表示されます。

- opened
  通信可能
- negotiating
  ネゴシエーション中
- closed
  通信不可

以下の情報は IPsec / IKE を利用して通信する場合に限り表示されます。
IPsec 手動鍵設定を利用する場合は表示されません。

16) 鍵交換モード
IKE における鍵交換モード を表示します。以下のどれかが表示されます。

- main
  Main モード を利用
- aggressive
  Aggressive モード を利用

17) IKE SA 状態
IKE SA の状態を表示します。以下のどれかが表示されます。

- established
  確立済み
- negotiating
  確立中
- expired
  削除待ち

- none
  未確立

18) IPsec SA 状態

IPsec SA の状態を表示します。以下のどれかが表示されます。

- established
  確立済み
- negotiating
  確立中
- expired
  削除待ち
- none
  未確立

15.7　統計情報の表示

15.7.1　stlan

[機能]

LANドライバの統計情報の表示

[入力形式]

stlan [<slot> [<port>]]
stlan clear

[パラメタ]

<slot>

- mb
  必ず"mb"(基本ボード) を指定してください。

<port>

ポート番号を指定します。

clear

LANドライバの統計情報を全てクリアします。

[説明]

LANドライバの統計情報を表示します。
<port>を省略した場合は、対象<slot>上に搭載される全ポートの情報が表示されます。
<port> および <slot>を省略した場合は、本装置に搭載されるすべてのポートの情報が表示されます。
clear パラメタを指定する場合は、LANドライバの統計情報のクリアを行うのみで、統計情報表示は行いません。

[注意]

統計情報は、本装置を再起動するとクリアされます。

[例]

以下に、表示例および表示内容を示します。

表示例

```
# stlan

[LAN PORT-0 STATUS]
interface status          : auto 100M Full       ---(1)
since                     : Oct  2 17:31:26 2002 ---(2)
[LAN LOG INFORMATION]
Input packets             : 7388 --- (3)
Input error packets       : 0    --- (4)
 long frame               : 0    --- (5)
 bad alignment frame      : 0    --- (6)
 short frame              : 0    --- (7)
 CRC error                : 0    --- (8)
 overrun                  : 0    --- (9)
 late collision           : 0    --- (10)
Output packets            : 7388 --- (11)
Output error packets      : 0    --- (12)
 late collision           : 0    --- (13)
 too many collision       : 0    --- (14)
 underrun                 : 0    --- (15)
 loss of carrier          : 0    --- (16)

[LAN PORT-1 STATUS]
interface status          : 100M Full
since                     : Oct  2 17:31:26 2002
[LAN LOG INFORMATION]
Input packets             : 599
Input error packets       : 0
 long frame               : 0
 bad alignment frame      : 0
 short frame              : 0
 CRC error                : 0
 overrun                  : 0
 late collision           : 0
Output packets            : 599
Output error packets      : 0
 late collision           : 0
 too many collision       : 0
 underrun                 : 0
 loss of carrier          : 0
```

1) インタフェース状態
   伝送路が自動でネゴシエーションされた場合には auto が表示されます。
   接続完了時に速度は 10M、100M のどれかが表示されます。
   接続完了時に伝送路状態として、Half、Full のどれかが表示されます。
2) 状態遷移時刻
   インタフェース状態が現在の状態に変化した時刻を表示します。
3) 受信フレーム数
4) 受信エラーフレーム数
5) 最大フレーム長オーバー検出回数
6) アライメントエラー検出回数
7) ショートフレーム検出回数
8) CRC エラー検出回数
9) オーバーラン検出回数
10) レイトコリジョン検出回数
11) 送信フレーム数
12) 送信エラーフレーム数
13) レイトコリジョン検出回数

14) リジョン発生による送信リトライアウト検出回数

15) アンダーラン検出回数

16) キャリアセンスロスト検出回数

15.7.2　stins

[機能]

ISDN 統計情報の表示

[入力形式]

stins [<slot> [<line> [<channel>]]]
stins clear

[パラメタ]

<slot>

スロット番号
MR1000 では、必ず"mb"(基本ボード) を指定してください。

<line>

ライン番号

- 0
  コネクタ 0

<channel>

チャネル番号

- d
  Dch
- bx
  (BRI の ISDN 回線の場合) x=1,2 :B1ch,B2ch

clear

ISDN 統計情報を全てクリアします。

[説明]

ISDN 統計情報を表示します。
<slot>を省略した場合は、対象のボードを搭載する全スロット・コネクタの d,b1,b2 の順に全チャネルの情報を表示します。
<line>を省略した場合は、対象スロットの d,b1,b2 の順に全チャネルの情報を表示します。
<channel>を省略した場合は、対象スロット・コネクタの d,b1,b2 の順に全チャネルの情報を表示します。なお、回線種別が"fr","hsd"の場合、b2 チャネルの情報は表示されません。
clear パラメタを指定した場合は、ISDN 統計情報のクリアを行なうのみで統計情報の表示は行ないません。

[注意]

統計情報は再起動によりクリアされます。

[例]

以下に表示例および表示内容を示します。

表示例 (BRI ISDN)

```
# stins mb 0 d
[LINE STATUS]
date                    : Oct 14 16:00:40 2002 --- (1)
channel                 : [MB][CNCT0][D] --- (2)
 speed                  : 16k              --- (3)
 status                 : wait sync        --- (4)
 since                  : Oct 14 16:00:24 2002 ---(5)
 func                   : Q921             --- (6)
[D CHANNEL INFORMATION]
received frame          : 0  --- (7)
         bytes          : 0  --- (8)
sent     frame          : 0  --- (9)
         bytes          : 0  --- (10)
Input frame dropped
  busy                  : 0  --- (11)
  CRC error             : 0  --- (12)
  abort frame           : 0  --- (13)
  bad length            : 0  --- (14)
  bad octet             : 0  --- (15)
Output frame dropped
  underrun              : 0  --- (16)
Collision count         : 0  --- (17)
SYNC    count           : 0  --- (18)
        time            : 0  --- (19)
OUTSYNC count           : 0  --- (20)
        time            : 53 --- (21)
```

```
# stins mb 0 b1
[LINE STATUS]
date                    : Oct 14 16:00:40 2002
channel                 : [MB][CNCT0][B1]
 speed                  : 64k
 status                 : wait setline
 since                  : Oct 14 16:00:24 2002
 func                   : HDLC
[LINE LOG INFORMATION]
received frame          : 0
         bytes          : 0
sent     frame          : 0
         bytes          : 0
Input frame dropped
  busy                  : 0
  CRC error             : 0
  abort frame           : 0
  bad length            : 0
  bad octet             : 0
Output frame dropped
  underrun              : 0
Flow control
  limit                 : 0      --- (22)
  count                 : 0      --- (23)
  condition             : XON    --- (24)
Flag send/monitor mode  : yes/no --- (25)
  flag recv             : 0      --- (26)
  idle recv             : 0      --- (27)
  flag received count   : 0      --- (28)
                time    : 0      --- (29)
  idle received count   : 0      --- (30)
                time    : 0      --- (31)
```

表示例 (BRI フレームリレー/専用線)

```
# stins
[LINE STATUS]
date                        : Oct 14 16:00:40 2002
channel                     : [SLOT0][CNCT0][-]
 speed                      :
 status                     : data
 since                      : Oct 14 16:00:24 2002
 func                       :
[LAYER1 INFORMATION]
SYNC    count               : 4
        time                : 35099
OUTSYNC count               : 3
        time                : 6

[LINE STATUS]
date                        : Oct 14 16:00:40 2002
channel                     : [SLOT0][CNCT0][-]
 speed                      : 128k
 status                     : data
 since                      : Oct 14 16:00:24 2002
 func                       : HDLC
[LINE LOG INFORMATION]
received frame              : 0
         bytes              : 0
sent     frame              : 0
         bytes              : 0
Input frame dropped
  busy                      : 0
  CRC error                 : 0
  abort frame               : 0
  bad length                : 0
  bad octet                 : 0
Output frame dropped
  underrun                  : 0
Flow control
  limit                     : 0
  count                     : 0
  condition                 : XON
Flag send/monitor mode      : no/no
  flag recv                 : 0
  idle recv                 : 0
  flag received count       : 0
                time        : 0
  idle received count       : 0
                time        : 0
```

表示例 (BRI フレームリレー/専用線)

```
# stins
[LINE STATUS]
date                      : Oct 14 16:00:40 2002
channel                   : [SLOT0][CNCT0][-]
 speed                    :
 status                   : data
 since                    : Oct 14 16:00:24 2002
 func                     :
[LAYER1 INFORMATION]
SYNC    count             : 4
        time              : 35099
OUTSYNC count             : 3
        time              : 6

[LINE STATUS]
date                      : Oct 14 16:00:40 2002
channel                   : [SLOT0][CNCT0][-]
 speed                    : 128k
 status                   : data
 since                    : Oct 14 16:00:24 2002
 func                     : HDLC
[LINE LOG INFORMATION]
received frame            : 0
         bytes            : 0
sent     frame            : 0
         bytes            : 0
Input frame dropped
  busy                    : 0
  CRC error               : 0
  abort frame             : 0
  bad length              : 0
  bad octet               : 0
Output frame dropped
  underrun                : 0
Flow control
  limit                   : 0
  count                   : 0
  condition               : XON
Flag send/monitor mode    : no/no
  flag recv               : 0
  idle recv               : 0
  flag received count     : 0
                time      : 0
  idle received count     : 0
                time      : 0
```

表示内容の説明 (D/B チャネル表示)

1) コマンド投入時刻

   stins コマンドが入力された時刻を表示します。

2) チャネル種別

   回線が ISDN の場合はスロット番号、ライン番号、D、B1、B2 のどれかが表示されます。

   回線がフレームリレー、専用線の場合は、スロット番号、ライン番号が表示されます。

3) 通信速度

   通信速度が kbps 単位で表示されます。

4) チャネル状態

   以下のどれかが表示されます。

   Init : 初期化中状態

   Wait Setline :

   チャネル未使用状態

   Wait Enable :

   チャネル使用開始待ち状態

Wait Sync :

同期確立待ち状態

Wait Call :

発着信待ち状態 (呼毎起動)

Wait Sync_s :

発信時同期確立待ち状態 (呼毎起動)

Outsync :

同期はずれ検出状態

Wait Enable_con :

チャネル起動中状態

Data :　データ送受信可能状態

Wait Disable :

チャネル停止指示待ち状態

Wait Disable_con:

チャネル停止完了待ち状態

Wait Flag :

フラグ受信待ち状態

Recv IDLE :

アイドル受信検出状態

5) 状態遷移時刻
チャネル状態が現在の状態に変化した時刻を表示します。

6) 通信種別
以下のどれかが表示されます。

Q921　D チャネルの場合に表示されます

Q921(per-call)

呼毎起動指定時の D チャネルの場合に表示されます

HDLC　HDLC プロトコル使用時に表示されます

PIAFS　PIAFS プロトコル使用時に表示されます

TRANSPARENT

トランスペアレント使用時に表示されます

7) 受信フレーム数
8) 受信バイト数
9) 送信フレーム数
10) 送信バイト数
11) 受信バッファビジー検出回数
12) 受信 CRC エラー検出回数
13) 受信アボートエラー検出回数
14) 受信フレーム長違反検出回数
15) 受信非オクテットフレーム検出回数
16) 送信アンダーラン検出回数

17) 衝突検出回数
18) 同期確立通知回数
19) 同期確立時間 (100ms 単位)
20) 同期外れ通知回数
21) 同期外れ時間 (100ms 単位)
22) フロー制御しきい値
23) 総送信要求バイト数
24) フロー制御状態
25) フラグ送信・監視モード状態
26) フラグ受信検出回数
27) フラグ断検出回数
28) フラグ受信通知回数
29) フラグ受信時間 (100ms 単位)
30) フラグ断通知回数
31) フラグ断時間 (100ms 単位)

15.7.3　stpiafs

[機能]

PIAFS 統計情報の表示

[入力形式]

stpiafs
stpiafs clear

[オプション]

なし。

[パラメタ]

clear

統計情報をクリアします。

[説明]

PIAFS 統計情報を表示します。

[例]

以下に表示例および表示内容を示します。

```
# stpiafs
[LINE LOG INFORMATION]
channel                  : [MB][CNCT0][B1] --- (1)
received frame           : 548             --- (2)
received byte            : 41648           --- (3)
 bad CRC                 : 45              --- (4)
 buffer full             : 0               --- (5)
sent frame               : 727             --- (6)
sent byte                : 55252           --- (7)
 sent idle data          : 1               --- (8)
[PIAFS LOG INFORMATION]
 duplicate frame         : 89  --- (9)
 bad FCS                 : 45  --- (10)
 other error             : 0   --- (11)
 send retry (over RTF)   : 1   --- (12)
 re-synchronization      : 0   --- (13)
 t010 timeout            : 1   --- (14)
 t011 timeout            : 0   --- (15)
 t012 timeout            : 0   --- (16)
 resync by Xbit          : 0   --- (17)
 sync 32k                : 1   --- (18)
 sync 64k                : 0   --- (19)
 t001 timeout            : 0   --- (20)
 t002 timeout            : 0   --- (21)
 t003 timeout            : 0   --- (22)
 t101 timeout            : 0   --- (23)
 output NEGO
   request               : 4   --- (24)
   accept                : 1   --- (25)
   reject                : 0   --- (26)
   reject cause          : 0   --- (27)
 output PARAM
   request               : 0   --- (28)
```

```
   accept                : 8   --- (29)
   reject                : 0   --- (30)
   reject cause          : 0   --- (31)
 output SYNC
   request               : 0   --- (32)
   accept                : 0   --- (33)
   reject                : 0   --- (34)
   reject cause          : 0   --- (35)
 output ARQ
   request               : 0   --- (36)
   accept                : 0   --- (37)
   reject                : 0   --- (38)
   reject cause          : 0   --- (39)
 output REL
   request               : 0   --- (40)
   accept                : 6   --- (41)
   reject                : 0   --- (42)
   request cause         : 0   --- (43)
   reject cause          : 0   --- (44)
 input NEGO
   request               : 7   --- (45)
   accept                : 0   --- (46)
   reject                : 0   --- (47)
   reject cause          : 0   --- (48)
 input PARAM
   request               : 8   --- (49)
   accept                : 0   --- (50)
   reject                : 0   --- (51)
   reject cause          : 0   --- (52)
 input SYNC
   request               : 0   --- (53)
   accept                : 0   --- (54)
   reject                : 0   --- (55)
   reject cause          : 0   --- (56)
 input ARQ
   request               : 0   --- (57)
   accept                : 0   --- (58)
   reject                : 0   --- (59)
   reject cause          : 0   --- (60)
 input REL
   request               : 6   --- (61)
   accept                : 0   --- (62)
   reject                : 0   --- (63)
   request cause         : 17  --- (64)
   reject cause          : 0   --- (65)
 input unknown           : 0   --- (66)
 input nop               : 0   --- (67)
 input nop2              : 0   --- (68)

[PIAFS CONTROL INFORMATION]
 protocol                : 4   --- (69)
 negotiated param
   data protocol         : 1   --- (70)
   control protocol      : 2   --- (71)
   rtf                   : 9   --- (72)
   compress              : 0   --- (73)
   p1                    : 0   --- (74)
   p2                    : 0   --- (75)
   frame length          : 80  --- (76)
   M                     : 63  --- (77)
   fi format             : 1   --- (78)
   sync format           : 1   --- (79)

[LINE LOG INFORMATION]
channel                  : [MB][CNCT0][B2]
              :
              :
```

1) チャネル種別

   スロット番号、ライン番号、チェネル種別が表示されます。

2) 受信フレーム数

3) 受信バイト数

4) 受信 CRC エラー検出回数
5) 受信バッファビジー検出回数
6) 送信フレーム数
7) 送信バイト数
8) 空フレーム送出回数
   以降の情報は接続時に一旦クリアされます。
9) データ二重受信
10) FCS エラー発生回数
11) FCS エラー以外発生回数
12) データフレーム再送回数
13) 再同期発生回数
14) 送受信速度切替タイマ A(T010) タイムアウト発生回数
15) 送受信速度切替タイマ B(T011) タイムアウト発生回数
16) 送受信速度切替タイマ C(T012) タイムアウト発生回数
17) 対応伝送速度切替通知による速度切替発生回数
18) 32Kbps 同期回数
19) 64Kbps 同期回数
20) 同期受付待ちタイマ (T001) タイムアウト発生回数
21) 同期受付送出後タイマ (T002) タイムアウト発生回数
22) 同期要求待ちタイマ (T003) タイムアウト発生回数
23) 制御送信確認待ちタイマ (T101) タイムアウト発生回数
24) ネゴ同期要求送信回数
25) ネゴ同期受付送信回数
26) ネゴ同期拒否送信回数
27) ネゴ同期拒否理由
28) 通信パラメタ設定要求送信回数
29) 通信パラメタ設定受付送信回数
30) 通信パラメタ設定拒否送信回数
31) 通信パラメタ設定拒否理由
32) 同期要求送信回数
33) 同期受付送信回数
34) 同期拒否送信回数
35) 同期拒否理由
36) ARQ パラメタ設定要求送信回数
37) ARQ パラメタ設定受付送信回数
38) ARQ パラメタ設定拒否送信回数
39) ARQ パラメタ設定拒否理由
40) データリンク解放要求送信回数
41) データリンク解放受付送信回数

42) データリンク解放拒否送信回数
43) データリンク解放要求理由
44) データリンク解放拒否理由
45) ネゴ同期要求受信回数
46) ネゴ同期受付受信回数
47) ネゴ同期拒否受信回数
48) ネゴ同期拒否理由
49) 通信パラメタ設定要求受信回数
50) 通信パラメタ設定受付受信回数
51) 通信パラメタ設定拒否受信回数
52) 通信パラメタ設定拒否理由
53) 同期要求受信回数
54) 同期受付受信回数
55) 同期拒否受信回数
56) 同期拒否理由
57) ARQ パラメタ設定要求受信回数
58) ARQ パラメタ設定受付受信回数
59) ARQ パラメタ設定拒否受信回数
60) ARQ パラメタ設定拒否理由
61) データリンク解放要求受信回数
62) データリンク解放受付受信回数
63) データリンク解放拒否受信回数
64) データリンク解放要求理由
65) データリンク解放拒否理由
66) 未定義フレーム受信回数
67) 受信破棄フレーム数
68) 受信破棄フレーム数 2
69) プロトコル種別
70) ARQ データ伝送プロトコルバージョン
71) ARQ 制御情報伝送プロトコルバージョン
72) 測定 RTF 値
73) データ圧縮方式識別子
74) 符号語総数 (P1)
75) 最大文字列長 (P2)
76) フレーム長
77) 最大フレーム番号 (M)
78) FI 構造識別子
79) 同期フレーム構造識別子

15.7.4　bridgestat

[機能]

ブリッジに関する状態および統計情報の表示

[入力形式]

bridgestat -i [-I <interface>] [-g [<group_id>]] (入出力パケット数表示)
bridgestat -l [-I <interface>] [-g [<group_id>]] (学習テーブル情報表示)
bridgestat -t (学習テーブル割り当て状況表示)
bridgestat -s [-I <interface>] (STP 状態表示)
bridgestat clear [-I <interface>] (ブリッジ統計情報のクリア)

[オプション]

オプションを指定しなかった場合は、-l を指定したものとみなされます。また、STP が有効なときは、-s を指定したものとみなされます。

-i

インタフェースごとの入出力パケット数を表示します。

-l

学習テーブルの情報を表示します。

-t

学習テーブルの割り当て状況を表示します。

-s

STP の状態を表示します。

[パラメタ]

-I <interface>

表示するインタフェースを指定します。

-g [<group_id>]

表示するブリッジグループを指定します。
group_id を省略した場合には、すべてのグループをグループ順にソートして表示します。

範囲	機種
0〜19	MR1000

ただし、-I と -g は同時に指定できません。

clear

ブリッジの統計情報 (入出力パケット数) をクリアします。

[説明]

ブリッジに関する状態、または統計情報を表示します。

[例]

以下に、表示例および表示内容を示します。

インタフェースごとの入出力パケット数を表示する場合 (-i 指定時)

```
# bridgestat -i
Name    Group   Status  IPv4     IPv6     D_if   STP              In     Out
----    -----   ------  ----     ----     ---    ---              --     ---
(1)     (2)      (3)    (4)      (5)      (6)    (7)              (8)    (9)

lan0    0       valid   Bridge   Routing  *      not use           0       2
lan1    0       valid   Bridge   Routing         not use           0       1
lan2    1       valid   Bridge   Routing  *      not use           0       0
lan3    1       valid   Bridge   Routing         not use           0       0
rmt0    1       valid   Bridge   Routing         not use           0       0
```

1) インタフェース名
   lan、または rmt インタフェース名が表示されます。
2) グループ識別子
3) ブリッジの状態
   以下のどれかが表示されます。

   valid ブリッジは有効

   invalid ブリッジは無効

4) IPv4 転送方式
   以下のどれかが表示されます。

   Bridge ブリッジで転送

   Routing ルーティングで転送

5) IPv6 転送方式
   以下のどれかが表示されます。

   Bridge ブリッジで転送

   Routing ルーティングで転送

6) 代表インタフェース
   レイヤ 3 代表インタフェースには * が表示されます。
7) STP の状態
   以下のどれかが表示されます。

   not use STP は無効

   Listening
   Listening 状態

   Learning Learning 状態

   Forwarding
   Forwarding 状態

8) 入力パケット数
9) 出力パケット数

インタフェースごとの入出力パケット数をグループ毎に表示する場合 (-i -g 指定時)

```
# bridgestat -i -g
[Group:0]
Name    Group   Status  IPv4     IPv6     D_if   STP             In     Out
----    -----   ------  ----     ----     ---    ---             --     ---
(1)     (2)      (3)    (4)      (5)      (6)    (7)             (8)    (9)

lan0    0       valid   Bridge   Routing  *      not use          0       2
lan1    0       valid   Bridge   Routing         not use          0       1

[Group:1]
----    -----   ------  ----     ----     ---    ---             --     ---
(1)     (2)      (3)    (4)      (5)      (6)    (7)             (8)    (9)

lan2    1       valid   Bridge   Routing  *      not use          0       0
lan3    1       valid   Bridge   Routing         not use          0       0
rmt0    1       valid   Bridge   Routing         not use          0       0
```

1) インタフェース名

   lan、または rmt インタフェース名が表示されます。

2) グループ識別子

3) ブリッジの状態

   以下のどれかが表示されます。

   valid　　ブリッジは有効

   invalid　ブリッジは無効

4) IPv4 転送方式

   以下のどれかが表示されます。

   Bridge　　ブリッジで転送

   Routing　ルーティングで転送

5) IPv6 転送方式

   以下のどれかが表示されます。

   Bridge　　ブリッジで転送

   Routing　ルーティングで転送

6) 代表インタフェース

   レイヤ 3 代表インタフェースには * が表示されます。

7) STP の状態

   以下のどれかが表示されます。

   not use　STP は無効

   Listening

   Listening 状態

   Learning　Learning 状態

   Forwarding

   Forwarding 状態

8) 入力パケット数

9) 出力パケット数

学習テーブルの情報を表示する場合 (-l 指定時)

```
# bridgestat -l
HashNo.  MAC address        Name    PortNo.  Status   Age  Group
-------  -----------        ----    -------  ------   ---  -----
  (1)        (2)             (3)      (4)     (5)     (6)   (7)

11       00:a0:c9:67:e1:4b  lan0    1        Used     297  0
```

1) 学習テーブルが登録されている Hash 番号
2) 学習テーブルに登録されている MAC アドレス
3) エントリされた端末が存在するインタフェース名
4) ポート番号
5) 学習テーブルの状態
   以下のどれかが表示されます。

   Used 使用中

   Static 静的学習テーブル

   unUsed 解放済み
6) 残り生存時間 (秒)
7) グループ識別子

学習テーブルの情報をグループ毎に表示する場合 (-l -g 指定時)

```
# bridgestat -l -g
[Group:0]
HashNo.  MAC address        Name    PortNo.  Status   Age  Group
-------  -----------        ----    -------  ------   ---  -----
  (1)        (2)             (3)      (4)     (5)     (6)   (7)

11       00:a0:c9:67:e1:4b  lan0    1        Used     297  0

[Group:1]
HashNo.  MAC address        Name    PortNo.  Status   Age  Group
-------  -----------        ----    -------  ------   ---  -----
  (1)        (2)             (3)      (4)     (5)     (6)   (7)

18       00:0e:c7:61:11:41  lan1    2        Used     257  1
```

1) 学習テーブルが登録されている Hash 番号
2) 学習テーブルに登録されている MAC アドレス
3) エントリされた端末が存在するインタフェース名
4) ポート番号
5) 学習テーブルの状態
   以下のどれかが表示されます。

   Used 使用中

   Static 静的学習テーブル

   unUsed 解放済み
6) 残り生存時間 (秒)
7) グループ識別子

学習テーブルの割り当て状況を表示する場合 (-t 指定時)

```
# bridgestat -t
use        free       max alloc  learn      delete     expire
---        ----       ---------  -----      ------     ------
(1)        (2)           (3)      (4)        (5)        (6)

6          1021       6          6          0          0
```

1) 使用中の学習テーブル数
2) 未使用の学習テーブル数
3) 過去に割り当てられた学習テーブルの最大値
4) 学習テーブルにエントリした回数
5) 学習テーブルに空きがないために削除された学習テーブル数
6) 寿命によって削除された学習テーブル数

STP 情報を表示する場合 (-s 指定時)

```
# bridgestat -s
[lan0]
status             : Forwarding --- (1)
Root ID            : 8000-00:00:0e:58:00:6e --- (2)
Designated bridge  : 8000-00:00:0e:58:00:6e --- (3)
Path cost          : 00000000 --- (4)
Max age            : 20       --- (5)
Message age        : 0        --- (6)
Hello time         : 2        --- (7)
Forward delay      : 15       --- (8)

[rmt0]
status             : Forwarding --- (1)
Root ID            : 8000-00:00:0e:58:00:6e --- (2)
Designated bridge  : 8000-00:00:0e:58:00:6e --- (3)
Path cost          : 00000000 --- (4)
Max age            : 20       --- (5)
Message age        : 0        --- (6)
Hello time         : 2        --- (7)
Forward delay      : 15       --- (8)

[rmt2]
status             : not use  --- (1)
```

1) STP の状態
   以下のどれかが表示されます。

   not use　STP は無効

   Listening
   Listening 状態

   Learning　Learning 状態

   Forwarding
   Forwarding 状態

2) ルートブリッジ ID
   ルートブリッジの ID が、「優先度-MAC アドレス」の形式で表示されます。
3) 代表ブリッジ ID
   代表ブリッジの ID が、「優先度-MAC アドレス」の形式で表示されます。
4) パスコスト値
   ルートブリッジまでのパスコスト値が表示されます。

5) 最大待ち合わせ時間 (秒)
構成情報 BPDU の最大待ち合わせ時間 (秒) が表示されます。

6) 経過時間 (秒)
ルートブリッジが送出した構成情報 BPDU が自装置に届くまでの経過時間 (秒) が表示されます。

7) 送出間隔 (秒)
構成情報 BPDU の送出間隔 (秒) が表示されます。

8) 最大中継遅延時間 (秒)
最大中継遅延時間 (秒) が表示されます。

15.7.5　natstat

[機能]

NAT 状態と統計情報の表示

[入力形式]

natstat
natstat -s
natstat -t [<interface>]
natstat clear

[オプション]

-s

NAT の統計情報を表示します。以下の情報が表示されます。

- プライベート→グローバル変換回数
- グローバル→プライベート変換回数
- プライベート→グローバルエラー発生回数
- グローバル→プライベートエラー発生回数
- フラグメントパケットの正常変換回数
- フラグメントパケットのエラー発生回数
- 現在使用中の NAT 変換テーブル個数
- NAT 変換テーブルのピークホールド個数 (NAT モジュールで確保した NAT 変換テーブル個数)
- メモリ枯渇回数
- 変換テーブルにないパケットの受信回数
- 異常に短いパケットの受信回数
- その他のエラー回数

-t

NAT 変換テーブルを一覧表示します。以下の情報が表示されます。

- インタフェース名
- 変換テーブル数
- 変換テーブル通番
- グローバル IP アドレス
- グローバルポート番号
- グローバル ICMP_ID
- プライベート IP アドレス
- プライベートポート番号
- プライベート ICMP_ID
- 相手側 IP アドレス
- 相手側ポート番号
- テーブル解放残時間 [*10 秒]

[パラメタ]

<interface>

インタフェース名を指定します。

clear

統計情報をクリアします。

[説明]

NAT 統計情報または変換テーブルを表示します。
オプション指定がない場合は、-s を指定したものとみなされます。

[例]

以下に、表示例および表示内容を示します。

統計情報

```
# natstat -s
*** NAT stat information ***
           to Global   to Private
translate          85 ---(1)    63 ---(2)
error               0 ---(3)     0 ---(4)

            fragment
translate           0 ---(5)
error               0 ---(6)

             current         peak
nat table         12 ---(7)    12 ---(8)

error accounting
  lack of memory                0 ---(9)
  table not found               0 ---(10)
  too small packet              0 ---(11)
  other reason                  0 ---(12)
```

1) プライベート→グローバル変換回数
2) グローバル→プライベート変換回数
3) プライベート→グローバルエラー発生回数
4) グローバル→プライベートエラー発生回数
5) フラグメントパケットの正常変換回数
6) フラグメントパケットのエラー発生回数
7) 現在使用中の NAT 変換テーブル個数
8) NAT 変換テーブルのピークホールド個数 (NAT モジュールで確保した NAT 変換テーブル個数)
9) メモリ枯渇回数
10) 変換テーブルにないパケットの受信回数
11) 異常に短いパケットの受信回数
12) その他のエラー回数

変換テーブル表示

```
# natstat -t
*** NAT table information ***
I/F : rmt0  ---(1)
ap 0: ap-001
-(2)- -(3)--
dynamic NAT table queue
[NAT table]   tblnum:12  ---(4)
index  GlobalAddr/Port       PrivateAddr/Port      DestAddr/Port         remain
       GlobalAddr:Icmp_Id    PrivateAddr:Icmp_Id   DestAddr
[   0] 10.36.195.136/10031   192.168.1.2/1055      10.36.195.1/80             2
-(5)-- ------(6)------ -(7)- ----(8)---- -(9)-     -----(10)----- -(11)-  -(12)-
[   1] 10.36.195.136/10030   192.168.1.2/1054      10.36.195.1/80             2
[   2] 10.36.195.136/10029   192.168.1.2/1053      10.36.195.1/80             2
[   3] 10.36.195.136/10028   192.168.1.2/1052      10.36.195.1/80             2
[   4] 10.36.195.136/10027   192.168.1.2/1051      10.36.195.1/80             2
[   5] 10.36.195.136/10026   192.168.1.2/1050      10.36.195.1/80             2
[   6] 10.36.195.136/10025   192.168.1.2/1049      10.36.195.1/80             2
[   7] 10.36.195.136/10024   192.168.1.2/1048      10.36.195.1/80             2
[   8] 10.36.195.136/10023   192.168.1.2/1047      10.36.195.1/80             2
[   9] 10.36.195.136/10022   192.168.1.2/1046      10.36.195.1/80             2
[  10] 10.36.195.136/10021   192.168.1.2/1045      10.36.195.1/80             2
[  11] 10.36.195.136/10020   192.168.1.2/1044      10.36.195.1/80             2
[  12] 10.36.195.136/10019   192.168.1.2/1043      10.36.195.1/80             2
[  13] 10.36.195.136/10018   192.168.1.2/1042      10.36.195.1/80             2
[  14] 10.36.195.136/10017   192.168.1.2/1041      10.36.195.1/80             2
[  15] 10.36.195.136/10016   192.168.1.2/1040      10.36.195.1/80             2
[  16] 10.36.195.136/10015   192.168.1.2/1039      10.36.195.1/80             2
[  17] 10.36.195.136/10014   192.168.1.2/1038      10.36.195.1/80             2
[  18] 10.36.195.136/10013   192.168.1.2/1037      10.36.195.1/80             2

application table queue
[NAT table]   tblnum:1
index  GlobalAddr/Port       PrivateAddr/Port      DestAddr/Port         remain
[   0] 10.36.195.136/10010   192.168.1.2/1034      10.36.195.28/49167        30

static NAT table queue
[NAT table]   tblnum:3
index  GlobalAddr/Port       PrivateAddr/Port      DestAddr/Port         remain
       GlobalAddr:Icmp_Id    PrivateAddr:Icmp_Id   DestAddr
[   0] 10.36.195.255/0       10.36.195.255/0       0.0.0.0/0                  0
[   1] 10.36.195.0/0         10.36.195.0/0         0.0.0.0/0                  0
[   2] 10.36.195.136:0       10.36.195.136:0       0.0.0.0                    0

address table queue
[NAT table]   tblnum:1
index  GlobalAddr            PrivateAddr           DestAddr              remain
[   0] 10.36.195.136         192.168.1.2           0.0.0.0                   30
```

1) インタフェース名
2) 接続先定義番号
3) 接続先名
4) 変換テーブル数
5) 変換テーブル通番
6) グローバル IP アドレス
7) グローバルポート番号、またはグローバル ICMP_ID
8) プライベート IP アドレス
9) プライベートポート番号、またはプライベート ICMP_ID
10) 相手側 IP アドレス
11) 相手側ポート番号
12) テーブル解放残時間 [*10 秒]

15.7.6 upnpstat

[機能]

UPnP 情報の表示

[入力形式]

upnpstat UPnP 情報の全表示
upnpstat statistic UPnP 統計情報の表示
upnpstat portmapping UPnP ポートマッピング情報の表示
upnpstat clear UPnP 統計情報の初期化

[オプション]

なし

[パラメタ]

なし

UPnP に関するすべての情報 (UPnP 統計情報および UPnP ポートマッピング情報) を表示します。

statistic

UPnP 変数名と現在値、および、UPnP 制御名と UPnP クライアントからの要求回数を表示します。

portmapping

UPnP クライアントによって設定されたポートマッピング情報を表示します。

clear

UPnP 制御の要求回数を 0 に初期化します。
UPnP 変数の現在値や UPnP ポートマッピング情報は初期化されません。

[説明]

UPnP に関する情報を表示します。
または、UPnP 統計情報を初期化します。

[例]

以下に、UPnP 統計情報の表示例を示します。

```
# upnpstat statistic
[lan0]                                                              (1)

Variable:                   Value                                   (2)
DefaultConnectionService
WANAccessType               Ethernet
Layer1UpstreamMaxBitRate    100000000
Layer1DownstreamMaxBitRate  100000000
PhysicalLinkStatus          Up
ConnectionType              IP_ROUTED
PossibleConnectionTypes     IP_ROUTED
ConnectionStatus            Connected
Uptime                      1234
LastConnectionError         ERROR_NONE
RSIPAvailable               FALSE
NATEnabled                  TRUE
ExternalIPAddress           123.45.67.89
PortMappingNumberOfEntries  3
PortMappingEnabled          TRUE

Action:                     Requested                               (3)
SetDefaultConnectionService  0
GetDefaultConnectionService  0
GetCommonLinkProperties      0
SetConnectionType            0
GetConnectionTypeInfo        0
RequestConnection            0
ForceTermination             0
GetStatusInfo                1
GetNATRSIPStatus             1
GetGenericPortMappingEntry   0
GetSpecificPortMappingEntry  0
AddPortMapping               4
DeletePortMapping            4
GetExternalIPAddress         7
```

1) 外部インタフェース名

2) UPnP 変数名、現在値

DefaultConnectionService

初期値は空白 (UPnP クライアントが設定)

WANAccessType

常に Ethernet

Layer1UpstreamMaxBitRate

上り回線速度 (bps)

Layer1DownstreamMaxBitRate

下り回線速度

PhysicalLinkStatus

物理リンク状態 (Up:接続、Down:切断)

ConnectionType

常に IP_ROUTED

PossibleConnectionTypes

常に IP_ROUTED

ConnectionStatus

接続状態 (Connected:接続、Disconnected:切断)

Uptime　接続経過時間 (秒)

LastConnectionError

接続異常要因

RSIPAvailable

常に FALSE

NATEnabled

常に TRUE

ExternalIPAddress

外部 IP アドレス

PortMappingNumberOfEntries

ポートマッピング登録数 (※)

PortMappingEnabled

常に TRUE

3) UPnP 制御名、UPnP クライアントからの要求回数

SetDefaultConnectionService

DefaultConnectionService 設定

GetDefaultConnectionService

DefaultConnectionService 取得

GetCommonLinkProperties

WANAccessType,Layer1Up / DownstreamMaxBitRate,PhysicalLinkStatus 取得

SetConnectionType

ConnectionType 設定

GetConnectionTypeInfo

ConnectionType,PossibleConnectionTypes 取得

RequestConnection

接続要求 (非サポート)

ForceTermination

切断要求 (非サポート)

GetStatusInfo

ConnectionStatus,LastConnectionError,Uptime 取得

GetNATRSIPStatus

NATRSIPAvailable,NATEnabled 取得

GetGenericPortMappingEntry

PortMapping 取得 (番号指定)

GetSpecificPortMappingEntry

PortMapping 取得 (条件指定)

AddPortMapping

PortMapping 登録 (※)

DeletePortMapping

PortMapping 削除 (※)

GetExternalIPAddress

ExternalIPAddress 取得

※ AddPortMapping と DeletePortMapping の差が PortMappingNumberOfEntries の数になるとは限りません。同じ内容を再登録したり、存在しない内容を削除することがあるためです。

以下に、UPnP ポートマッピング情報の表示例を示します。

```
# upnpstat portmapping
[lan0]                                                                    (1)

date  time     external      internal     protocol lease description
(2)              (3)           (4)           (5)   (6) (7)
09/20 17:35:18 0.0.0.0:5091  192.168.0.2:5091  UDP     0 VoIP (192.168.0.2:5091)
09/20 17:35:20 0.0.0.0:5090  192.168.0.2:5090  UDP     0 VoIP (192.168.0.2:5090)
09/20 17:35:22 0.0.0.0:5060  192.168.0.2:5060  UDP     0 VoIP (192.168.0.2:5060)
```

1) 外部インタフェース名
2) 作成日時
3) 外部アド レス:外部ポート
4) 内部アド レス:内部ポート
5) プロトコル種別 (TCP か UDP)
6) 有効期間 (秒)
7) 説明

15.7.7 filterstat

[機能]

IP フィルタ状態と統計情報の表示

[入力形式]

filterstat [-s] [-t] [-f <address_family>] [<interface>]
filterstat clear

[オプション]

-s

IP フィルタの統計情報を表示します。以下の情報が表示されます。

- インタフェース名
- 処理したパケット数
- 透過したパケット数
- 遮断したパケット数

<interface>を指定しない場合には、さらに以下の情報が表示されます。

- 装置全体の静的フィルタテーブル数
- 装置全体の動的フィルタテーブル数
- 装置全体の SPI フィルタテーブル数
- メモリ不足で SPI フィルタテーブルを確保できなかった回数
- テーブル数が最大値に達していて SPI フィルタテーブルを確保できなかった回数

-t

IP フィルタテーブルを一覧表示します。以下の情報が表示されます。

- インタフェース名
- いずれの IP フィルタテーブルにも不一致時の動作
- IP フィルタテーブル数
- ソース IP アドレス
- ソース IP のマスク長
- ディスティネーション IP アドレス
- ソース IP のマスク長
- プロトコル番号
- TCP 接続要求を受け入れるか否か
- 入出力方向
- フィルタ動作
- TOS 値
- ICMP TYPE
- ICMP CODE
- Traffic Class 値
- テーブルタイマ

-f <address_family>

指定した<address_family>に関する情報だけを表示します。
指定できる<address_family>は、inet(IPv4) と inet6(IPv6) です。
省略した場合は、inet と inet6 の両方を指定したものとみなされます。

[パラメタ]

<interface>

インタフェース名を指定します。

clear

統計情報をクリアします。

[説明]

IP フィルタ統計情報もしくは、IP フィルタテーブルを表示します。
オプション指定がない場合は、-s を指定したものとみなされます。

[例]

以下に、表示例および表示内容を示します。

統計情報

```
# filterstat
[lan0]---(1)
IPv4 filter
  static table                          1---(2)
  dynamic table                         0---(3)
  SPI table                             1---(4)

  packet                 in          out
  pass(static)          358---(5)      2---(6)
  pass(dynamic)           0---(7)      0---(8)
  pass(SPI)               1---(9)      1---(10)
  reject                  0---(11)     0---(12)
  total                 359---(13)     3---(14)

IPv6 filter
  static table                          1---(2)
  dynamic table                         0---(3)
  SPI table                             1---(4)

  packet                 in          out
  pass(static)          358---(5)      2---(6)
  pass(dynamic)           0---(7)      0---(8)
  pass(SPI)               1---(9)      1---(10)
  reject                  0---(11)     0---(12)
  total                 359---(13)     3---(14)

[all]
IPv4 filter
  static table                          1---(15)
  dynamic table                         0---(16)
  SPI table                             1---(17)

  lack of memory                        0---(18)
  SPI table limit over                  0---(19)

IPv6 filter
  static table                          1---(15)
  dynamic table                         0---(16)
  SPI table                             1---(17)

  lack of memory                        0---(18)
  SPI table limit over                  0---(19)
```

1)　インタフェース名

2) 静的フィルタテーブル数
3) 動的フィルタテーブル数
4) SPI フィルタテーブル数
5) 入力側で静的フィルタで透過したパケット数
6) 出力側で静的フィルタで透過したパケット数
7) 入力側で動的フィルタで透過したパケット数
8) 出力側で動的フィルタで透過したパケット数
9) 入力側で SPI フィルタで透過したパケット数
10) 出力側で SPI フィルタで透過したパケット数
11) 入力側で遮断したパケット数
12) 出力側で遮断したパケット数
13) 入力側で処理したパケット数
14) 出力側で処理したパケット数
15) 装置全体の静的フィルタテーブル数
16) 装置全体の動的フィルタテーブル数
17) 装置全体の SPI フィルタテーブル数
18) メモリ不足で SPI フィルタテーブルを確保できなかった回数
19) テーブル数が最大値に達していて SPI フィルタテーブルを確保できなかった回数

IP フィルタテーブル表示

```
# filterstat -t
[lan0]---(1)
IPv4 filter
 default:spi---(2)

 static table:3---(3)
       src IP/mask:port         dst IP/mask:port         proto SYN  dir  action
                                                          tos  type code
 [  0] any:any                  any:21                     6   Y   any    pass
                                                         any  any  any
 [  1] any:21                   any:any                    6   N   any    pass
                                                         any  any  any
 [  2] 10.0.0.0/8:5000          192.168.1.0/24:6000       17   Y   out    pass
  (4)  (5)     (6)(7)           (8)       (9) (10)      (11) (12) (13)   (14)
                                                         any  any  any
                                                         (15) (16) (17)

 dynamic table:1---(18)
       src(dst) IP/mask:port    dst(src) IP/mask:port    proto SYN action remain
 [  0] 192.168.1.2/32:any       10.36.195.28/32:54063      6   Y    pass     30
                                                                          (19)

 SPI table:1---(20)
       src(dst) IP/mask:port    dst(src) IP/mask:port    proto SYN action remain
 [  0] 192.168.1.2/32:any       10.36.195.28/32:any        1   -    pass     30

IPv6 filter
 default:spi---(2)

 static table:3---(3)
       src IP/prefixlen:port    dst IP/prefixlen:port    proto SYN  dir  action
                                                         class type code
 [  0] any:any                  any:21                     6   Y   out   pass
                                                         any  any  any
 [  1] any:21                   any:any                    6   N    in   pass
                                                        0-10 any  any
 [  2] 2001:200:1::/64:any      2001:200:2::/64:6000      58   Y   rev   pass
  (4)  (5)         (6) (7)      (8)         (9) (10)     (11) (12) (13)  (14)
                                                         any  1-10   0
                                                         (21) (16) (17)

 dynamic table:1---(18)
       src IP/prefixlen:port    dst IP/prefixlen:port    proto SYN action remain
 [  0] 2001:200:1::88/128:49165 2001:200:2::27/128:21512   6   Y   pass    30
                                                                          (19)

 SPI table:1---(20)
       src IP/prefixlen:port    dst IP/prefixlen:port    proto SYN action remain
 [  0] 2001:200:1::88/128:22    2001:200:2::27/128:12431   1   -   pass    30
```

1) インタフェース名
2) いずれの IP フィルタテーブルにも不一致時の動作
3) 静的フィルタテーブル数
4) フィルタ通番
5) フィルタ送信元 IP アドレス
6) フィルタ送信元 IP アドレスマスク
7) フィルタ送信元ポート番号
8) フィルタ送信先 IP アドレス
9) フィルタ送信先 IP アドレスマスク
10) フィルタ送信先ポート番号
11) フィルタプロトコル番号
12) フィルタ TCP 接続要求を含むか否か

13) パケットの入出力方向

any: 入力パケットと出力パケットの両方に対してフィルタ動作を行います。

in: 入力パケットに対してだけフィルタ動作を行います。

out: 出力パケットに対してだけフィルタ動作を行います。

rev: 入力パケットと出力パケットの両方に対してフィルタ動作を行います。ただし、入力パケットについては、以下のものを逆転した条件でフィルタ動作をします。

- 送信元 IP アドレス/マスクと宛先 IP アドレス/マスク
- 送信元ポート番号と宛先ポート番号

14) フィルタ動作

15) TOS 値

16) ICMP TYPE

17) ICMP CODE

18) 動的フィルタテーブル数

19) フィルタテーブルタイマ [*10 秒]

20) SPI フィルタテーブル数

21) Traffic Class 値

15.7.8　ipsecstat

[機能]

システムの IPsec / IKE 情報の表示

[入力形式]

ipsecstat [<protocol>]

[オプション]

なし

[パラメタ]

<protocol>

isakmp　ISAKMP SA 情報の表示

ipsec　IPsec SA および SPD 情報の一括表示

[説明]

(1) オプションなし

```
# ipsecstat
[IPsec SA Information]
[1]     Remote Name(ISP-0), rmt0, ap0
        Side(Initiator), Gateway(192.168.2.1, 192.168.1.1), OUT
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=171237444(0x0a34e044)
        Created(Apr 26 17:59:03 2004), NewSA(23040secs, 3276Kbyte)
        Lifetime(28800secs), Current(332secs), Remain(28468secs)
        Lifebyte(4096Kbyte), Current(2528Kbytes), Remain(1568Kbyte)

[2]     Remote Name(ISP-0), rmt0, ap0
        Side(Initiator), Gateway(192.168.1.1, 192.168.2.1), IN
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=181913669(0x0ad7c845)
        Created(Apr 26 17:59:03 2004), NewSA(23040secs, 3276Kbyte)
        Lifetime(28800secs), Current(332secs), Remain(28468secs)
        Lifebyte(4096Kbyte), Current(2528Kbytes), Remain(1568Kbyte)

[3]     Remote Name(ISP-1), rmt1, ap0
        Side(Initiator), Gateway(2001:db8:1111:2::66, 2001:db8:1111:1::66), OUT
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=171237446(0x0a34e046)
        Created(Apr 26 17:59:03 2004), NewSA(23040secs, 3276Kbyte)
        Lifetime(28800secs), Current(332secs), Remain(28468secs)
        Lifebyte(4096Kbyte), Current(2528Kbytes), Remain(1568Kbyte)

[4]     Remote Name(ISP-1), rmt1, ap0
        Side(Initiator), Gateway(2001:db8:1111:1::66, 2001:db8:1111:2::66), IN
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=181913671(0x0ad7c847)
        Created(Apr 26 17:59:03 2004), NewSA(23040secs, 3276Kbyte)
        Lifetime(28800secs), Current(332secs), Remain(28468secs)
        Lifebyte(4096Kbyte), Current(2528Kbytes), Remain(1568Kbyte)

[IKE SA Information]
[1]     Destination(192.168.1.1.500), Source(192.168.2.1.500), rmt0
        Cookies(2ee33635dcc2a837:ece2a45bc12889ef)
        Side(Initiator), Status(ESTABLISHED), Exchangetype(AGGRESSIVE)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        Created(Apr 26 17:59:03 2004)
        Lifetime(86400secs), Current(10secs), Remain(86390secs)

[2]     Destination(2001:db8:1111:1::66.500), Source(2001:db8:1111:2::66.500), rmt1
        Cookies(6ee33635dcc2a837:dce2a45bc12889ef)
        Side(Initiator), Status(ESTABLISHED), Exchangetype(AGGRESSIVE)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        Created(Apr 26 17:59:03 2004)
        Lifetime(86400secs), Current(10secs), Remain(86390secs)
```

(2) isakmp オプション指定

```
# ipsecstat isakmp
[1]     Destination(192.168.1.1.500), Source(192.168.2.1.500), rmt0
        Cookies(2ee33635dcc2a837:ece2a45bc12889ef)
        Side(Initiator), Status(ESTABLISHED), Exchangetype(AGGRESSIVE)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        Created(Apr 26 17:59:03 2004)
        Lifetime(86400secs), Current(10secs), Remain(86390secs)

[2]     Destination(fec0:1::66.500), Source(fec0:2::66.500), rmt1
        Cookies(6ee33635dcc2a837:dce2a45bc12889ef)
        Side(Initiator), Status(ESTABLISHED), Exchangetype(AGGRESSIVE)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        Created(Apr 26 17:59:03 2004)
        Lifetime(86400secs), Current(10secs), Remain(86390secs)
```

(3) ipsec オプション指定

```
# ipsecstat ipsec
[1]     Remote Name(ISP-0), rmt0, ap0
        Side(Initiator), Gateway(192.168.2.1, 192.168.1.1), OUT
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=171237444(0x0a34e044)
        Created(Apr 26 17:59:03 2004), NewSA(23040secs, 3276Kbyte)
        Lifetime(28800secs), Current(332secs), Remain(28468secs)
        Lifebyte(4096Kbyte), Current(2528Kbytes), Remain(1568Kbyte)

[2]     Remote Name(ISP-0), rmt0, ap0
        Side(Initiator), Gateway(192.168.1.1, 192.168.2.1), IN
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=181913669(0x0ad7c845)
        Created(Apr 26 17:59:03 2004), NewSA(23040secs, 3276Kbyte)
        Lifetime(28800secs), Current(332secs), Remain(28468secs)
        Lifebyte(4096Kbyte), Current(2528Kbytes), Remain(1568Kbyte)

[3]     Remote Name(ISP-1), rmt1, ap0
        Side(Initiator), Gateway(fec0:2::66, fec0:1::66), OUT
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=171237446(0x0a34e046)
        Created(Apr 26 17:59:03 2004), NewSA(23040secs, 3276Kbyte)
        Lifetime(28800secs), Current(332secs), Remain(28468secs)
        Lifebyte(4096Kbyte), Current(2528Kbytes), Remain(1568Kbyte)

[4]     Remote Name(ISP-1), rmt1, ap0
        Side(Initiator), Gateway(fec0:1::66, fec0:2::66), IN
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=181913671(0x0ad7c847)
        Created(Apr 26 17:59:03 2004), NewSA(23040secs, 3276Kbyte)
        Lifetime(28800secs), Current(332secs), Remain(28468secs)
        Lifebyte(4096Kbyte), Current(2528Kbytes), Remain(1568Kbyte)
```

IPsec SA/SPD 情報

```
[1]     Remote Name(ISP-0), rmt0, ap0
 *1     *2                  *5    *6
[1]     Destination(192.168.2.20/24), Source(192.168.1.10/24), rmt0, ap0
 *1     *3                      *4                          *5    *6
        Side(Initiator), Gateway(192.168.2.1, 192.168.1.1), OUT
        *7               *8                                 *9
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        *10            *11               *12                *13
        Status(mature), Spi=171237444(0x0a34e044)
        *14             *15
        Created(Apr 26 17:59:03 2004), NewSA(23040secs, 3276Kbyte)
        *16                        *17
        Lifetime(28800secs), Current(332secs), Remain(28468secs)
        *18                  *19               *20
        Lifebyte(4096Kbyte), Current(2528Kbytes), Remain(1568Kbyte)
        *21                  *22                 *23
```

***1 :**　IPsec SA / SPD 表示番号

***2 :**　IPsec 対象区間のネットワーク名 (IPsec 対象範囲が any4 または any6 の場合)

***3 :**　IPsec 対象あて先 IP アドレス (IPsec 対象範囲の指定がある場合)

***4 :**　IPsec 対象送信元 IP アドレス (IPsec 対象範囲の指定がある場合)

***5 :**　IPsec 対象区間のインタフェース名

***6 :**　IPsec 対象区間の接続先定義番号

***7 :**　ネゴシエーションサイド

Initiator:　イニシエータ

Responder:

レスポンダ

Manual : 手動鍵設定 (*13 / *17 / *18 / *20 / *21 / *23 は、—で表示されます)

***8 :** IPsec 対象パケットをセキュア / アンセキュア化する送信元 IP アドレスおよびあて先 IP アドレス (IKE セッション)

***9 :** ポリシの方向

OUT: 出力用ポリシ

IN : 入力用ポリシ

***10:** 使用するセキュリティプロトコル

***11:** 暗号アルゴリズム

***12:** 認証アルゴリズム

***13:** PFS 使用時の DH(Diffie-Hellman) グループ

***14:** IPsec SA の状態

larval: IPsec SA 作成中状態 (ネゴシエーション中の状態)

mature: IPsec SA 作成完了状態 (ネゴシエーションが完了し、IPsec SA が作成された状態)

dying : SA の更新時間 (softtime) に到達した状態

※ IPsec 通信に使用されるのは、mature または dying の状態の IPsec SA となります。

***15:** SPI 値

***16:** IPsec SA 作成時間 (秒)

***17:** IPsec SA の更新を開始する時間 (秒) および有効パケット量 (キロバイト)

***18:** IPsec SA 有効時間 (秒)

***19:** IPsec SA 作成からの経過時間 (秒)

***20:** IPsec SA 削除までの残存時間 (秒)

***21:** IPsec SA 有効パケット量 (キロバイト)

***22:** IPsec SA 作成からの転送バイト数 (キロバイト)

出力時: 暗号化 / 認証後のパケット長の累計

入力時: 復号化 / 認証前のパケット長の累計

***23:** IPsec SA 削除までの残バイト数 (キロバイト)

ISAKMP SA 情報

```
[1]     Destination(192.168.1.1.500), Source(192.168.2.1.500), rmt0
*1      *2                            *3                        *4
        Cookies(2ee33635dcc2a837:ece2a45bc12889ef)
        *5
        Side(Initiator), Status(ESTABLISHED), Exchangetype(AGGRESSIVE)
        *6               *7                   *8
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        *9               *10                   *11
        Created(Apr 26 17:59:03 2004)
        *12
        Lifetime(86400secs), Current(10secs), Remain(86390secs)
        *13                  *14              *15
```

***1 :** ISAKMP SA 表示番号

***2 :**　ISAKMP あて先 IP アドレス

***3 :**　ISAKMP 送信元 IP アドレス

***4 :**　IPsec 対象区間のインタフェース名

***5 :**　クッキー (Initiator:Responder)

***6 :**　ネゴシエーションサイド

Initiator:　イニシエータ

Responder:
レスポンダ

***7 :**　ISAKMP SA のネゴシエーション状態
MSG1RECEIVED
MSG1SENT
MSG2RECEIVED
MSG2SENT
MSG3RECEIVED
MSG3SENT
MSG4RECEIVED
ESTABLISHED
EXPIRED

※　ESTABLISHED は、Phase1 のネゴシエーションが完了した状態を意味します。
EXPIRED は、ISAKMP SA 情報の削除待ちを意味します。
その他は、Phase1 のネゴシエーション中の状態を意味します。

***8 :**　交換モード

BASE:　Base モード (未サポート)

MAIN:　Main モード

AUTH ONLY:
Authentication Only モード (未サポート)

AGGRESSIVE:
Aggressive モード

***9 :**　暗号アルゴリズム

***10:**　認証アルゴリズム

***11:**　PFS グループ

***12:**　ISAKMP SA 作成時間

***13:**　ISAKMP SA 有効時間 (秒)

***14:**　ISAKMP SA 作成からの経過時間 (秒)

***15:**　ISAKMP SA 削除までの残存時間 (秒)

15.7.9 ikestat

[機能]

IKE 統計情報表示

[入力形式]

ikestat [-i [<interface>]]
ikestat [<mode>]

[オプション]

-i

リモート・インタフェースについての IKE 統計情報を簡易表示します。

[パラメタ]

<interface>

インタフェース名を指定します。

<mode>

clear
IKE ネゴシエーションパケットに統計情報をクリアします。

[説明]

IKE ネゴシエーションパケットの統計情報を表示します。

[例]

表示例 (IKE ネゴシエーションパケットの統計情報の表示)

```
# ikestat
received isakmp packet:
 0 isakmp packet received error --- (1)
 0 total isakmp packet received --- (2)
       0 invalid IP address --- (3)
       0 invalid ISAKMP header --- (4)
       0 invalid ISAKMP packet --- (5)
       0 possible attack --- (6)
received isakmp packet exchange type:
       0 Base Exchange --- (7)
       0 Identity Protection Exchange --- (8)
       0 Authentication Only Exchange --- (9)
       0 Aggressive Exchange --- (10)
               0 invalid Security Association --- (11)
               0 invalid Key Exchange --- (12)
               0 invalid Identification --- (13)
               0 invalid Certificate --- (14)
               0 invalid Certificate Request --- (15)
               0 invalid Hash --- (16)
               0 invalid Signature --- (17)
               0 invalid Nonce --- (18)
               0 invalid Notification --- (19)
               0 invalid Delete --- (20)
               0 invalid Vendor ID --- (21)
               0 invalid Next Payload type --- (22)
       0 Informational Exchange --- (23)
               0 Notification --- (24)
                       0 No Proposal Chosen --- (25)
                       0 Initial Contact --- (26)
                       0 others Notify Message --- (27)
                       0 invalid Notify Message type --- (28)
               0 there is no valid ISAKMP-SA --- (29)
               0 invalid Security Association
               0 invalid Key Exchange
               0 invalid Identification
               0 invalid Certificate
               0 invalid Certificate Request
               0 invalid Hash
               0 invalid Signature
               0 invalid Nonce
               0 invalid Notification
               0 invalid Delete
                       0 invalid received delete message --- (30)
               0 invalid Vendor ID
               0 invalid Next Payload type
       0 Quick Mode Exchange --- (31)
               0 there is no valid ISAKMP-SA --- (32)
               0 invalid Security Association
               0 invalid Key Exchange
               0 invalid Identification
               0 invalid Certificate
               0 invalid Certificate Request
               0 invalid Hash
               0 invalid Signature
               0 invalid Nonce
               0 invalid Notification
               0 invalid Delete
               0 invalid Vendor ID
               0 invalid Next Payload type
       0 New group  Exchange --- (33)
       0 Acknowledged Informational Exchange --- (34)
       0 invalid Exchange type --- (35)
sent isakmp packet:
 0 isakmp packet send error --- (36)
 0 total isakmp packet sent --- (37)
sent isakmp packet phase1:
       0 isakmp phase1 packet resent --- (38)
       0 phase1 give up --- (39)
sent isakmp packet phase2:
       0 isakmp phase2 packet resent --- (40)
       0 phase2 give up --- (41)
```

続く

```
sent isakmp packet information:
       0 No Proposal Chosen --- (42)
       0 Initial Contact --- (43)
       0 others Notify Message --- (44)
others:
       0 phase1 count > phase1_max --- (45)
       0 encrypting failed --- (46)
       0 decrypting failed --- (47)
       0 failed to create inbound IPsec SA --- (48)
       0 failed to create outbound IPsec SA --- (49)
       0 IKE SA information no entry --- (50)
       0 IPsec SA information no entry --- (51)
       0 shared key no entry --- (52)
       0 IPsec remote interface Down --- (53)
       0 invalid remote address --- (54)
       0 invalid local address --- (55)
       0 failed to allocate buffer --- (56)
       0 other --- (57)
```

続き

1) パケット受信エラー数
2) 受信パケットの合計数
3) 無効な IP アドレス受信数
4) 無効な ISAKMP ヘッダ受信数
5) 無効な ISAKMP パケット受信数
6) 自装置に対して攻撃していると思われるパケットの受信数
7) Base 交換受信数
8) Identity 交換受信数
9) Authentication Only 交換受信数
10) Aggressive 交換受信数
11) SA ペイロード受信失敗数
12) 鍵交換ペイロード受信失敗数
13) ID ペイロード受信失敗数
14) 証明書ペイロード受信失敗数
15) 証明書要求ペイロード受信失敗数
16) ハッシュペイロード受信失敗数
17) 署名ペイロード受信失敗数
18) Nonce ペイロード受信失敗数
19) 通知ペイロード受信失敗数
20) 削除ペイロード受信失敗数
21) ベンダ ID ペイロード受信失敗数
22) 無効なペイロードタイプ受信数
23) Informational 交換受信数
24) 通知ペイロード受信数
25) SA Proposal が受け入れられない通知メッセージ受信数
26) 初めての SA 確立通知メッセージ受信数
27) その他の通知メッセージ受信数
28) 無効な通知メッセージの受信数

29) ISAKMP SA がない Informational 受信数
30) 無効な削除メッセージ受信数
31) Quick Mode 受信数
32) ISAKMP SA がない Quick Mode 受信数
33) New group Mode 受信数
34) Acknowledged Informational 受信数
35) 無効な交換タイプ受信数
36) パケット送信エラー数
37) 送信パケットの合計数
38) Phase1 パケット再送数
39) Phase1 ネゴシエーション失敗数
40) Phase2 パケット再送数
41) Phase2 ネゴシエーション失敗数
42) SA Proposal が受け入れられない通知メッセージ送信数
43) 始めての SA 確立通知メッセージ送信数
44) その他の通知メッセージ送信数
45) 装置内での ISAKMP SA 最大数超過数
46) ISAKMP パケット暗号化失敗数
47) ISAKMP パケット復号化失敗数
48) 受信用 IPsec SA 作成失敗数
48) 送信用 IPsec SA 作成失敗数
49) IKE SA 情報検索失敗数
50) IPsec SA 情報検索失敗数
51) 共有鍵検索失敗
52) IPsec 用相手情報アクセスポイント回線閉塞時
53) ネゴシエーション中止数
54) 相手側アドレス不正数
55) 自側アドレス不正数
56) 領域獲得失敗数
57) その他のエラー数

表示例 (リモート・インタフェース IKE 統計情報簡易表示)

```
# ikestat -i
[rmt0]: --- (1)
 0 total Phase1 packet received --- (2)
       0 invalid Payload --- (3)
 0 total Phase1 packet sent --- (4)
       0 isakmp phase1 packet resent --- (5)
       0 phase1 give up --- (6)
 0 total Phase2 packet received --- (7)
       0 invalid Payload --- (8)
 0 total Phase2 packet sent --- (9)
       0 isakmp phase2 packet resent --- (10)
       0 phase2 give up --- (11)
 0 total Informational packet received --- (12)
       0 invalid Payload --- (13)
 0 total Informational packet sent --- (14)
[rmt1]:
 0 total Phase1 packet received
       0 invalid Payload
 0 total Phase1 packet sent
       0 isakmp phase1 packet resent
       0 phase1 give up
 0 total Phase2 packet received
       0 invalid Payload
 0 total Phase2 packet sent
       0 isakmp phase2 packet resent
       0 phase2 give up
 0 total Informational packet received
       0 invalid Payload
 0 total Informational packet sent
[rmt2]:
 0 total Phase1 packet received
       0 invalid Payload
 0 total Phase1 packet sent
       0 isakmp phase1 packet resent
       0 phase1 give up
 0 total Phase2 packet received
       0 invalid Payload
 0 total Phase2 packet sent
       0 isakmp phase2 packet resent
       0 phase2 give up
 0 total Informational packet received
       0 invalid Payload
 0 total Informational packet sent
```

1) 表示 Remote インタフェース
2) Phase1 受信合計数
3) Phase1 無効ペイロード 受信数
4) Phase1 送信合計数
5) Phase1 再送数
6) Phase1 ネゴシエーション失敗数
7) Phase2 受信合計数
8) Phase2 無効ペイロード 受信数
9) Phase2 送信合計数
10) Phase2 再送数
11) Phase2 ネゴシエーション失敗数
12) 通知メッセージ受信合計数
13) 通知メッセージ無効ペイロード 受信数
14) 通知メッセージ送信合計数

15.7.10　vrrpstat

[機能]

VRRP 機能における各種情報の表示

[入力形式]

vrrpstat [[-g] [<lan_number> [<vrid>]]]
vrrpstat -G <lan_number> <vrid>
vrrpstat clear

[オプション]

-g

グループ簡易情報を表示

-G

グループ簡易情報を表示 (ヘッダなし)

[パラメタ]

<lan_number>

コマンド適用対象の LAN インタフェースを指定します。

- lan 定義番号
  lan 定義の通し番号を、10 進数値で指定します。

範囲	機種
0〜19	MR1000

<vrid>

コマンド適用対象の VRRP グループを指定します。

- VRID
  VRRP グループの VRID を、1〜255 の 10 進数値で指定します。

clear

VRRP 統計情報を全てクリアします。

[説明]

オプションなしの場合は、VRRP グループの詳細情報を表示します。
<lan_number>と<vrid>の両方を指定した場合は、指定 LAN インタフェースの指定 VRRP グループ詳細情報を表示します。
<lan_number>だけを指定した場合は、指定 LAN インタフェースに設定されたすべての VRRP グループ詳細情報を表示します。
<lan_number>と<vrid>の両方を指定しない場合は、全 VRRP グループの詳細情報を表示します。
-g オプションを指定することによって、VRRP グループ簡易情報を表示します。
-g オプションだけ指定した場合は、全 VRRP グループの簡易情報を表示します。
<lan_number>と<vrid>の両方を指定した場合は指定 LAN インタフェースの指定 VRRP グループ簡易情報を表示します。
<lan_number>だけ指定した場合は、指定した LAN インタフェースに設定されたすべての VRRP グループ簡易情報を表示します。

-G オプションを指定することによって、VRRP グループ簡易情報を表示します。

-G オプションを指定した場合、<lan_number>と<vrid>を指定しなくてはなりません。指定 LAN インタフェースの指定 VRRP グループ状態だけを表示します。

clear を指定することによって、詳細情報にて表示される全 VRRP グループの統計情報カウンタを 0 で初期化することができます。

[例]

-g オプション

VRRP グループに関する簡易情報を表示します。

定義されている VRID の一覧とそのグループの状態を表示します。グループの状態として、Master / Backup / Initialize があります。

- Master :

  マスタルータとして仮想ルータの IPv4 アドレス宛のパケットをフォワーディングしている状態。

- Backup :

  バックアップルータとしてマスタルータのダウンに備えている状態。

- Initialize :

  マスタルータまたはバックアップルータになることができない状態。

```
# vrrpstat -g
<LAN 0>
  VRID  Status
    10  Master
    20  Backup

<LAN 1>
  VRID  Status
    25  Backup
    40  Initialize

#
```

-G オプション

VRRP グループに関する情報を表示します。

指定した VRRP グループの状態を表示します。グループの状態として Master / Backup / Initialize があります。

```
# vrrpstat -G 0 10
    10  Master

#
```

オプションなし

オプションが指定されない場合は、VRRP グループについての詳細情報を表示します。

```
# vrrpstat
<LAN 0>
  State              : OK
  Authentication Type: Text
  Authentication Pass: "omron"
  Interface statistics information:
      0          Bad checksum packets
      0          VRRP Version illegal packets
      0          VRID illegal packets

  VRID 10
    Master(PRI 255 now 255/PREEMPT ON)
    Now Master : Me
    Virtual MAC Address : 00:00:5E:00:01:0A
    Virtual Router IP Address:
        10.124.2.126
        10.124.2.224
    VRRP advertisement interval 1
    Shutdown interface trigger:
        lan1  reduce 200  OFF
        rmt11 reduce 100  OFF
    Shutdown route trigger:
        default            lan0  reduce 255  OFF
        10.232.79.200/32   rmt1  reduce 100  OFF
    Shutdown node trigger:
        192.168.100.100 lan0  reduce 255  OFF
        10.232.79.193   rmt1  reduce 100  OFF
    Group statistics information:
        1          become master-router
        0          received VRRP advertisement packets
        0          VRRP advertisement interval configuration mismatched packets
        0          Authentication failed packets
        0          TTL illegal packets
        0          received priority 0 advertisement packets
        0          sent priority 0 advertisement packets
        0          VRRP type illegal packets
        0          Virtual router IP address configuration mismatched packets
        0          Authentication type illegal packets
        0          Authentication type mismatch packets
        0          Length illegal packets

  VRID 20
    Backup(PRI 100 now 50/PREEMPT OFF)
    Now Master : 10.124.2.100 Priority 255
    Virtual MAC Address : 00:00:5E:00:01:14
    Virtual Router IP Address:
        10.124.2.138
        10.124.2.139
    VRRP advertisement interval 1
    Shutdown interface trigger:
        rmt3  reduce  50  ON
    Group statistics information:
        0          become master-router
        6130       received VRRP advertisement packets
        0          VRRP advertisement interval configuration mismatched packets
        0          Authentication failed packets
        0          TTL illegal packets
        0          received priority 0 advertisement packets
        0          sent priority 0 advertisement packets
        0          VRRP type illegal packets
        0          Virtual router IP address configuration mismatched packets
        0          Authentication type illegal packets
        0          Authentication type mismatch packets
        0          Length illegal packets

```

2　　情報を表示する LAN インタフェースの番号

3　　LAN インタフェースの状態 : OK / NG

4　　LAN インタフェースの VRRP パケット認証方法

5　　LAN インタフェースの VRRP パケット認証パスワード

7　　受信 VRRP パケットチェックサム異常数

8	受信 VRRP パケット VRRP バージョン異常数
9	受信 VRRP パケット VRID 異常数
11	VRID
12	VRRP グループ状態 (設定優先度、現在の優先度 / プリエンプトモード) VRRP グループ状態 : 現在の VRRP グループの状態 (Master / Backup / Initialize) 設定優先度 : 構成定義で設定された優先度 現在の優先度 : トリガイベントの減算値を含めた現在の優先度 プリエンプトモード : 構成定義で設定されたプリエンプトモード (ON / OFF)
13	現在のマスタルータの実 IPv4 アドレスと優先度 (自装置がマスタルータである場合は"Me" を表示)
14	仮想 MAC アドレス
15-17	仮想ルータの IPv4 アドレス
18	VRRP-AD の送信間隔
19-21	インタフェースダウントリガと適用状態
22-24	ルートダウントリガと適用状態
25-27	ノードダウントリガと適用状態
29	マスタルータになった回数
30	VRRP-AD 総受信数
31	受信 VRRP-AD 送信間隔異常数
32	受信 VRRP-AD 認証パスワード異常数
33	受信 VRRP-AD TTL 異常数
34	優先度 0 の VRRP-AD 総受信数
35	優先度 0 の VRRP-AD 総送信数
36	受信 VRRP パケットタイプ異常数
37	受信 VRRP-AD バックアップ IPv4 アドレス構成異常数
38	受信 VRRP-AD 認証タイプ異常数
39	受信 VRRP-AD 認証タイプ不一致数
40	受信 VRRP-AD ヘッダ長異常数

15.7.11　ldpstat

[機能]

LDP 情報の表示

[入力形式]

ldpstat [status]
ldpstat adjacency
ldpstat fec
ldpstat interface [{<interface> | detail}]
ldpstat session [{<address> | detail}]
ldpstat vc

[オプション]

なし。

[パラメタ]

status

LDP の動作状況を表示します.

adjacency

LDP 近隣関係にある相手 LSR の情報を表示します。

fec

FEC テーブルの情報を表示します。

interface

すべてのインタフェースの LDP 情報をリストで表示します。

interface <interface>

指定したインタフェースの LDP 情報を詳細に表示します。

interface detail

すべてのインタフェースの LDP 情報を詳細に表示します。

session

すべての LDP セッションの情報をリストで表示します。

session <address>

指定した相手 LSR に関連した LDP セッションの情報を詳細に表示します。
<address>には、相手 LSR を IPv4 アドレスで指定します。

session detail

すべての LDP セッションの情報を詳細に表示します。

vc

すべての VC の情報をリストで表示します。

[説明]

LDP に関する情報を表示します。
パラメタを省略すると，ldpstat status, ldpstat interface detail, ldpstat session detail, ldpstat vc detail をまとめて表示します.

[例]

以下に表示例および表示内容を示します。

・LDP の状態を表示する場合 (status 指定時)

```
# ldpstat status
Router ID               : 10.1.201.2                              (1)
LDP Version             : 1                                       (2)
Label Control Mode      : Independent                             (3)
Request Retry           : On                                      (4)
Transport Address data  : 10.1.201.2 (platform wide)              (5)
Import routes           : connected, RIP, OSPF                    (6)
```

1) 装置の ROUTER-ID
2) LDP のバージョン (常に 1)
3) LDP 配布制御方式
   以下のどれかが表示されます。

   Independent :
   Independent Label Distribution Control

   Ordered :
   Ordered Label Distribution Control

4) Label Request の再送 (常に On)
5) トランスポートアドレス
6) 経路の使用の有無
   以下のどれかが 1 つ以上表示されます。

   connected :
   conencted 経路を用いてラベル広報を行う

   static : static 経路を用いてラベル広報を行う

   RIP : RIP 経路を用いてラベル広報を行う

   OSPF : OSPF 経路を用いてラベル広報を行う

   BGP : BGP 経路を用いてラベル広報を行う

   none : 経路を用いてラベル広報を行いません

・LDP 近隣関係にある相手 LSR の情報を表示する場合 (adjacency 指定時)

```
# ldpstat adjacency
IP Address              Name  Holdtime        LDP ID
----------              ----  --------        ------
   (1)                   (2)   (3)             (4)
192.168.2.2             lan0  15              192.168.1.1:0
192.168.3.1             lan1  15              192.168.3.1:0
```

1) 近隣関係にある相手 LSR の IP アドレス
2) インタフェース名
3) Holdtime (秒)
4) 相手 LSR の LDP-ID(LDP ROUTER-ID:LABEL-SPACE)

・FEC テーブルの情報を表示する場合 (fec 指定時)

```
# ldpstat fec
Codes  Prefix            Session           Out Label         Nexthop Addr
-----  ------            -------           ----------        ------------
  (1)    (2)               (3)               (4)               (5)
NL>    192.168.1.0/24    192.168.2.2       18                192.168.2.2
E >    192.168.2.0/24    non-existent      none              none
E >    192.168.3.0/24    non-existent      none              none
NL>    192.168.4.0/24    192.168.3.1       23                192.168.3.1

Total/MAX FEC Entries : 4 / 362
                       ---  ---
                       (6)  (7)
```

1) コード

   以下のどれかが表示されます。

   E :　この FEC の出口 (Egress)

   N :　この FEC の出口ではない (Non-Egress)

   L :　この FEC に対しラベルで受信

   > :　この FEC に対しこのルートを使用

2) プレフィックス
3) LDP セッションの相手 LSR の IP アドレス
4) 出力ラベル
5) 次ホップアドレス
6) 現在 FEC 数の合計
7) 装置の最大 FEC 数

・インタフェースの LDP 情報を表示する場合 (interface 指定時)

```
# ldpstat interface
Name       LDP Identifier  Label-switching
----       -------------   ---------------
(1)              (2)           (3)
lan0       192.168.2.1:0   Enabled
lan1       192.168.2.1:0   Enabled
```

1) インタフェース名
2) LDP-ID(LDP ROUTER-ID:LABEL-SPACE)
3) MPLS の有効 / 無効

・インタフェースの LDP 情報を表示する場合 (interface で特定の interface を指定した時)

```
#ldpstat interface lan0
Status                 : Enabled                 (1)
Primary IP Address     : 10.1.201.2              (2)
Interface Type         : Ethernet                (3)
Hello Interval         : 5                       (4)
Hold Time              : 15                      (5)
Keepalive Interval     : 60                      (6)
Keepalive Timeout      : 180                     (7)
Advertisement Mode     : Downstream Unsolicited  (8)
Label Retention Mode   : Liberal                 (9)
```

1) LDP の動作状態

2) インタフェースの IP アドレス

3) インタフェース種別
以下のどれかが表示されます。

Ethernet :
Ethernet MPLS mode

ATM SHIM :
RFC3031 / 3032 ATM MPLS mode

PPP : PPP MPLS mode

4) Hello の送信インターバルの値 (秒)

5) Hello のホールドタイマーの値 (秒)
ホールドタイマーが無限秒である場合は infinity と表示されます。

6) KeepAlive の送信インターバルの値 (秒)

7) KeepAlive タイムアウトの値 (秒)

8) ラベル広報モード (Advertise)
以下のどれかが表示されます。

Downstream Unsolicited :
Downstream Unsolicited Label advertisement mode

Downstream on Demand :
Downstream on Demand Label advertisement mode

9) ラベル保持モード (Retention)
以下が表示されます。

Liberal : Liberal Label retention mode

Conservative :
Conservative Label retention mode

・LDP セッションの情報を表示する場合 (session 指定時)

```
# ldpstat session
IP Address      Name       Role    State           KeepAlive    Retention/Advertise
----------      ----       ----    -----           ---------    -------------------
  (1)            (2)       (3)      (4)            (5)          (6)
192.168.2.2      lan0      Passive OPERATIONAL     180          Liberal/DU
192.168.3.1      lan1      Active  OPERATIONAL     180          Conservative/DoD
```

1) LDP セッションを確立している相手 LSR の IP アドレス

2) インタフェース名

3) ロール
以下のどれかが表示されます。

Active : アクティブロール

Passive : パッシブロール

4) LDP セッションの状態
以下のどれかが表示されます。

NON_EXISTENT

INITIALIZED

OPENSENT

OPENREC

OPERATIONAL

5) KeepAlive タイムアウトの値 (秒)

6) ラベル保持モード / ラベル広報モード

ラベル保持モード (Retention)

以下のどれかが表示されます。

Liberal : Liberal Label retention mode

Conservative :

Conservative Label retention mode

ラベル広報モード (Advertise)

以下のどれかが表示されます。

DU : Downstream Unsolicited Label advertisement mode

DoD : Downstream on Demand Label advertisement mode

・LDP セッションの情報を表示する場合 (session で特定の address を指定した時)

```
# ldpstat session 10.1.201.1
 Session state         : OPERATIONAL                                    (1)
 Session role          : Active                                         (2)
 TCP Connection        : Established                                    (3)
 IP Address for TCP    : 10.1.201.1                                     (4)
 Interface being used  : lan0                                           (5)
 Peer LDP ID           : 10.4.1.2:0                                     (6)
 Adjacencies           : 10.1.201.1                                     (7)
 Advertisement mode    : Downstream Unsolicited                         (8)
 Label retention mode  : Liberal                                        (9)
 Keepalive Timeout     : 180                                            (10)
 Reconnect Interval    : 15                                             (11)
 Address List received : 10.1.201.1                                    (12)
 Received Labels :       Fec              Label          Maps To       (13)
                 IPV4:10.0.0.6/32         19             16
                 IPV4:10.1.101.2/32       20             18
 Sent Labels :   Fec                      Label          Maps To       (14)
                 IPV4:10.0.0.6/32         16             19
                 IPV4:10.0.0.201/32       17             none
                 IPV4:10.1.101.2/32       18             20
                 IPV4:10.1.201.0/24       impl-null      none
                 IPV4:10.1.201.2/32       19             none
                 IPV4:192.168.201.0/24    impl-null      none
```

1) LDP セッションの状態

以下のどれかが表示されます。

NON_EXISTENT

INITIALIZED

OPENSENT

OPENREC

OPERATIONAL

2) ロール

以下のどれかが表示されます。

Active : アクティブロール

Passive : パッシブロール

3) TCP コネクションの状態
以下のどれかが表示されます。

Established

Not Established

4) TCP で使用する相手 LSR の IP アドレス
5) インタフェース名
6) 相手 LSR の LDP-ID(LDP ROUTER-ID:LABEL-SPACE)
7) 近隣関係にある相手 LSR の IP アドレス
8) ラベル広報モード (Advertise)
以下のどれかが表示されます。

Downstream Unsolicited :
Downstream Unsolicited Label advertisement mode

Downstream on Demand :
Downstream on Demand Label advertisement mode

9) ラベル保持モード (Retention)
以下が表示されます。

Liberal : Liberal Label retention mode

Conservative :
Conservative Label retention mode

10) KeepAlive タイムアウトの値 (秒)
11) 再接続のインターバルの値 (秒)
12) 受信した Address List の値
13) セッションで受信した FEC とラベル値とラベルマッピングしたラベル値
14) セッションで送信した FEC とラベル値とラベルマッピングしたラベル値

・VC の情報を表示する場合 (vc 指定時)

```
# ldpstat vc
Transport Client     VC     VC       Local       Remote      Destination
VC ID     I/F        State  Type     VC Label    VC Label    Address
--------  ----       ----   -----    ---------   ---------   -----------
 (1)      (2)       (3)     (4)        (5)         (6)         (7)
1         lan1       UP     ethernet 16          17          10.1.201.2
2         lan2       UP     ethernet 17          18          10.1.201.2
```

1) VC ID
2) VC インタフェース名
3) VC の状態
以下のどれかが表示されます。

UP : VC インタフェース UP

DOWN : VC インタフェース DOWN

4) VC Type
   VC ラベル交換に使用したインタフェースの種類を表示します。
   以下のどれかが表示されます。

   ethernet :
   Ethernet

   vlan : Ethernet VLAN

5) 自側 VC ラベル (受信用)
6) 相手側 VC ラベル (送信用)
7) VC 相手の IP アド レス

・**LDP の各情報をまとめて表示する場合**

```
# ldpstat
[LDP Status]
Router ID               : 10.1.201.2
LDP Version             : 1
Label Control Mode      : Independent
Request Retry           : On
Transport Address data  : 10.1.201.2 (platform wide)
Import routes           : connected, RIP, OSPF

[LDP Interface Information]
[Interface lan0]
Status                  : Enabled
Primary IP Address      : 10.1.201.2
Interface Type          : Ethernet
Hello Interval          : 5
Hold Time               : 15
Keepalive Interval      : 60
Keepalive Timeout       : 180
Advertisement Mode      : Downstream Unsolicited
Label Retention Mode    : Conservative

[Interface lan1]
Status                  : Disabled

[Interface lo0]
Status                  : Disabled

[LDP Session Information]
[Session peer address 10.1.201.1]
Session state         : OPERATIONAL
Session role          : Active
TCP Connection        : Established
IP Address for TCP    : 10.1.201.1
Interface being used  : lan0
Peer LDP ID           : 10.4.1.2:0
Adjacencies           : 10.1.201.1
Advertisement mode    : Downstream Unsolicited
Label retention mode  : Conservative
Keepalive Timeout     : 180
Reconnect Interval    : 15
Address List received : 10.1.201.1
Received Labels :       Fec             Label           Maps To
                IPV4:10.0.0.6/32        19              16
                IPV4:10.1.101.2/32      20              18
Sent Labels :   Fec                     Label           Maps To
                IPV4:10.0.0.6/32        16              19
                IPV4:10.0.0.201/32      17              none
                IPV4:10.1.101.2/32      18              20
                IPV4:10.1.201.0/24      impl-null       none
                IPV4:10.1.201.2/32      19              none
                IPV4:192.168.201.0/24   impl-null       none
[Session peer address 10.1.201.2]
Session state         : OPERATIONAL
Session role          : Passive
TCP Connection        : Established
IP Address for TCP    : 10.1.201.2
Interface being used  : lan0
Peer LDP ID           : 10.0.0.201:0
Adjacencies           : 10.1.201.2
Advertisement mode    : Downstream Unsolicited
Label retention mode  : Liberal
Keepalive Timeout     : 180
Reconnect Interval    : 15
Address List received : 10.0.0.201
                        10.1.201.2
Received Labels :       Fec             Label           Maps To
                VC:1                    16
                VC:2                    17
Sent Labels :   Fec                     Label           Maps To
                VC:1                    17
                VC:2                    18

[LDP VC Information]
Transport Client     VC     VC       Local       Remote      Destination
VC ID     I/F        State  Type     VC Label    VC Label    Address
1         lan1       UP     ethernet 16          17          10.1.201.2
2         lan2       UP     ethernet 17          18          10.1.201.2
```

15.7.12　mplsstat

[機能]

MPLS テーブル情報の表示

[入力形式]

mplsstat status
mplsstat ftn [<address>[/<mask>]] [detail]
mplsstat ilm [<address>[/<mask>]] [detail]
mplsstat vrf [<vrf_number>] [<address>[/<mask>]] [detail]
mplsstat interface [{<interface> | detail}]
mplsstat vc [{<vc_id> | <interface>}] [detail]
mplsstat clear ftn [<address>[/<mask>]]
mplsstat clear ilm [<address>[/<mask>]]
mplsstat clear vrf [<vrf_number>] [<address>[/<mask>]]
mplsstat clear interface [<interface>]
mplsstat clear vc [{<vc_id> | <interface>}] mplsstat clear

[オプション]

なし

[パラメタ]

status

MPLS の状態を表示します。

ftn

FTN テーブルのすべての情報を表示します。

ftn detail

FTN テーブルのすべての情報を統計情報を含めて表示します。

ftn <address>/<mask>

指定した IPv4 ネットワークアドレスにマッチする FTN テーブルの情報を表示します。
<address>/<mask>には、IPv4 アドレスとマスクビット数またはマスク値の組み合わせを指定します。
/<mask> を省略した場合は，ホストアドレスとみなします。

ftn <address>/<mask> detail

指定した IPv4 ネットワークアドレスにマッチする FTN テーブルの情報を統計情報を含めて表示します。
<address>/<mask>には、IPv4 アドレスとマスクビット数またはマスク値の組み合わせを指定します。
/<mask> を省略した場合は，ホストアドレスとみなします.

ilm

ILM テーブルのすべての情報を表示します。

ilm detail

ILM テーブルのすべての情報を統計情報を含めて表示します。

ilm <address>/<mask>

指定した IPv4 ネットワークアドレスにマッチする ILM テーブルの情報を表示します。
<address>/<mask>には、IPv4 アドレスとマスクビット数またはマスク値の組み合わせを指定します。
/<mask> を省略した場合は，ホストアドレスとみなします.

ilm <address>/<mask> detail

指定した IPv4 ネットワークアドレスにマッチする ILM テーブルの情報を統計情報を含めて表示します。
<address>/<mask>には、IPv4 アドレスとマスクビット数またはマスク値の組み合わせを指定します。
/<mask> を省略した場合は，ホストアドレスとみなします.

vrf

すべての VRF 定義番号のすべての VRF テーブルの情報を表示します。

vrf detail

すべての VRF 定義番号のすべての VRF テーブルの情報を統計情報を含めて表示します。

vrf <vrf_number>

指定した VRF 定義番号のすべての VRF テーブルの情報を表示します。

vrf <vrf_number> detail

指定した VRF 定義番号のすべての VRF テーブルの情報を統計情報を含めて表示します。

vrf <address>/<mask>

すべての VRF 定義番号の VRF テーブルの中から，指定した IPv4 ネットワークアドレスにマッチする VRF テーブルの情報を表示します。
<address>/<mask>には、IPv4 アドレスとマスクビット数またはマスク値の組み合わせを指定します。

vrf <address>/<mask> detail

すべての VRF 定義番号の VRF テーブルの中から，指定した IPv4 ネットワークアドレスにマッチする VRF テーブルの情報を統計情報を含めて表示します。
<address>/<mask>には、IPv4 アドレスとマスクビット数またはマスク値の組み合わせを指定します。
/<mask> を省略した場合は，ホストアドレスとみなします.

vrf <vrf_number> <address>/<mask>

指定した VRF 定義番号の VRF テーブルの中から，指定した IPv4 ネットワークアドレスにマッチする情報を表示します。
<address>/<mask>には、IPv4 アドレスとマスクビット数またはマスク値の組み合わせを指定します。
/<mask> を省略した場合は，ホストアドレスとみなします.

vrf <vrf_number> <address>/<mask> detail

指定した VRF 定義番号の VRF テーブルの中から，指定した IPv4 ネットワークアドレスにマッチする情報を統計情報を含めて表示します。
<address>/<mask>には、IPv4 アドレスとマスクビット数またはマスク値の組み合わせを指定します。
/<mask> を省略した場合は，ホストアドレスとみなします.

interface

すべてのインタフェースの統計情報をリストで表示します。

interface detail

すべてのインタフェースの統計情報を詳細に表示します。

interface <interface>

指定したインタフェースの統計情報を詳細に表示します。

vc

すべての VC 情報を表示します。

vc detail

すべての VC 情報を詳細に表示します。

vc <vc_id>

指定した VC ID の VC 情報を詳細に表示します。

vc <interface>

指定したインタフェースの VC 情報を詳細に表示します。

clear ftn

すべての FTN テーブルの統計情報をクリアします。

clear ftn <address>/<mask>

指定した IPv4 ネットワークアドレスにマッチする FTN テーブルの統計情報をクリアします。
<address>/<mask>には、IPv4 アドレスとマスクビット数またはマスク値の組み合わせを指定します。
/<mask> を省略した場合は，ホストアドレスとみなします.

clear ilm

すべての ILM テーブルの統計情報をクリアします。

clear ilm <address>/<mask>

指定した IPv4 ネットワークアドレスにマッチする ILM テーブルの統計情報をクリアします。
<address>/<mask>には、IPv4 アドレスとマスクビット数またはマスク値の組み合わせを指定します。
/<mask> を省略した場合は，ホストアドレスとみなします.

clear vrf

すべての VRF 定義番号のすべての VRF テーブルの統計情報をクリアします。

clear vrf <vrf_number>

指定した VRF 定義番号のすべての VRF テーブルの統計情報をクリアします。

clear vrf <address>/<mask>

すべての VRF 定義番号の指定した IPv4 ネットワークアドレスにマッチする VRF テーブルの統計情報をクリアします。
<address>/<mask>には、IPv4 アドレスとマスクビット数またはマスク値の組み合わせを指定します。
/<mask> を省略した場合は，ホストアドレスとみなします.

clear vrf <vrf_number> <address>/<mask>

指定した VRF 定義番号の指定した IPv4 ネットワークアドレスにマッチする VRF テーブルの統計情報をクリアします。
<address>/<mask>には、IPv4 アドレスとマスクビット数またはマスク値の組み合わせを指定します。
/<mask> を省略した場合は，ホストアドレスとみなします.

clear interface

すべてのインタフェースの統計情報をクリアします。

clear interface <interface>

指定したインタフェースの統計情報をクリアします。

clear vc

すべての VC 統計情報をクリアします。

clear vc <vc_id>

指定した VC ID の VC 統計情報をクリアします。

clear vc <interface>

指定した VC ID の VC 統計情報をクリアします。

clear

FTN テーブル, ILM テーブル, VRF テーブル, インタフェース, VC の統計情報をクリアします。

[説明]

MPLS のテーブル情報を表示します。
パラメタを指定しない場合は，mplsstat status, mplsstat ftn detail,
mplsstat ilm detail, mplsstat vrf detail, mplsstat interface detail, mplsstat vc detail をまとめて表示します.

[例]

以下に、表示例および表示内容を示します。

MPLS の状態を表示する場合 (status 指定)

```
# mplsstat status
[Status of MPLS Forwarder]
MPLS Forwarder           : Enabled          (1)
Number of Interface      : 2                (2)
Number of Entry          :
  FTN                    : 6                (3)
  ILM                    : 8                (4)
  VRF                    : 2                (5)
IP Propagate TTL         : Off              (6)
```

1) MPLS の有効／無効

   Enabled の場合に有効，Disabled の場合に無効であることを表します。

2) インタフェース数

   MPLS で使用するインタフェース数を表示します。

3) FTN エントリ数

   MPLS 中の FTN のエントリ数を表示します。

4) ILM エントリ数

   MPLS 中の ILM のエントリ数を表示します。

5) VRF エントリ数

   MPLS 中の VRF のエントリ数を表示します。

6) TTL 継承動作

   On の場合に継承する，Off の場合に継承しないことを表します。

FTN テーブルの情報を表示する場合 (ftn 指定時)

- エントリが存在する場合

```
# mplsstat ftn
[Data for FTN Table]
PREFIX              NH ADDR          OUT I/F      LABEL   OPCODE
------              -------          -------      ------  ------
 (1)                 (2)              (3)          (4)     (5)
100.232.1.0/24      100.232.2.1      rmt0         19      PUSH
192.168.3.0/24      192.168.5.1      lan1         18      PUSH
192.168.4.0/24      192.168.2.1      lan0         17      PUSH
```

- エントリが存在しない場合

```
# mplsstat ftn
[Data for FTN Table]
No Entry.
```

- detail を指定した場合

```
# mplsstat ftn detail
[Data for FTN Table]
PREFIX              NH ADDR          OUT I/F      LABEL   OPCODE      PACKETS    OCTETS
------              -------          -------      -----   ------      -------    ------
 (1)                  (2)              (3)         (4)     (5)          (6)         (7)
100.232.1.0/24      100.232.2.1      rmt0         19      PUSH              0          0
192.168.3.0/24      192.168.5.1      lan1         18      PUSH             29       2162
192.168.4.0/24      192.168.2.1      lan0         17      PUSH              0          0
```

1) プレフィックス
   ftn を指定した場合はプレフィックス順に表示します。
2) 次ホップアドレス
   インタフェース経路は 0.0.0.0 と表示されます。
3) 出力インタフェース名
4) 出力ラベル (出力ラベル値がない場合は '-'を表示)
5) ラベルオペレーションコード
   以下のどれかが表示されます。

   PUSH : プレフィックスに該当する IP パケットに出力ラベルを PUSH して出力インタフェース名のインタフェースに出力します。

   DLVR-VPN :
   プレフィックスに該当する IP パケットを出力インタフェース名のインタフェースにそのまま出力します。

6) エントリを使用して送出したパケット数
7) エントリを使用して送出したオクテット数

ILM テーブルの情報を表示する場合 (ilm 指定時)

- エントリが存在する場合

```
# mplsstat ilm
[Data for ILM Table]
PREFIX              IN-LABEL  OUT-LABEL  NH ADDR          OUT I/F      OPCODE
------              --------  ---------  -------          -------      ------
 (1)                 (2)       (3)       (4)              (5)          (6)
192.168.4.0/24      17        -         192.168.3.1      lan1         POP
192.168.1.0/24      18        -         192.168.2.2      lan0         POP
```

- エントリが存在しない場合

```
# mplsstat ilm
[Data for ILM Table]
No Entry.
```

- detail を指定した場合

```
# mplsstat ilm detail
[Data for ILM Table]
PREFIX              IN-LABEL  OUT-LABEL  NH ADDR          OUT I/F  OPCODE    PACKETS    OCTETS
------              --------  ---------  -------          -------  ------    -------    ------
 (1)                 (2)       (3)       (4)              (5)      (6)       (7)        (8)
192.168.4.0/24      17        -         192.168.3.1      lan1     POP             0          0
192.168.1.0/24      18        -         192.168.2.2      lan0     POP           211      15613
```

1) プレフィックス
2) 入力ラベル
   ilm を指定した場合は入力ラベル順に表示します。
3) 出力ラベル (出力ラベル値がない場合は '-'を表示)
4) 次ホップアドレス
   インタフェース経路は 0.0.0.0 と表示されます。

5) 出力インタフェース名

6) ラベルオペレーションコード
以下のどれかが表示されます。

POP : 入力ラベルに該当する MPLS パケットからラベルを POP して出力インタフェース名のインタフェースに出力します。

SWAP : 入力ラベルに該当する MPLS パケットのラベルを出力ラベルに SWAP して出力インタフェース名のインタフェースに出力します。

POP-VPN :
入力ラベルに該当する MPLS パケットから VPN ラベルを POP して出力インタフェースの VRF インタフェースに出力します。

7) エントリを使用して送出したパケット数

8) エントリを使用して送出したオクテット数

VRF テーブルの情報を表示する場合 (vrf 指定時)

- エントリが存在する場合

```
# mplsstat vrf
[Data for VRF Table # 2 ]
                     ---
                     (1)
PREFIX              NH ADDR          OUT I/F      LABEL   OPCODE
------              -------          -------      ------  ------
 (2)                 (3)              (4)          (5)     (6)
192.168.100.0/24    10.56.11.21      16/lan0      21      PUSH AND LOOKUP
192.168.130.0/24    10.56.11.77      17/lan0      22      PUSH AND LOOKUP
192.168.160.0/24    192.168.2.1      lan1         -       DELIVER TO IP FOR VPN
                                          :
[Data for VRF Table # 1 ]
PREFIX              NH ADDR          OUT I/F      LABEL   OPCODE
192.168.120.0/24    10.56.11.21      16/lan0      25      PUSH AND LOOKUP
```

- エントリが存在しない場合

```
# mplsstat vrf
[Data for VRF Table # 2 ]
No Entry.
                                          :
[Data for VRF Table # 1 ]
No Entry.
```

- detail を指定した場合

```
# mplsstat vrf detail
[Data for VRF Table # 2 ]
                     ---
                     (1)
PREFIX              NH ADDR          OUT I/F      LABEL   OPCODE      PACKETS    OCTETS
------              -------          -------      ------  ------      -------    ------
 (2)                 (3)              (4)          (5)     (6)          (7)        (8)
192.168.100.0/24    10.56.11.21      16/lan0      21      PUSH-VPN         13      1104
192.168.130.0/24    10.56.11.77      17/lan0      22      PUSH-VPN         26      2006
192.168.160.0/24    192.168.2.1      lan1         -       DLVR-VPN          0         0
                                          :
[Data for VRF Table # 1 ]
PREFIX              NH ADDR          OUT I/F      LABEL   OPCODE      PACKETS    OCTETS
192.168.120.0/24    10.56.11.21      16/lan0      25      PUSH-VPN          0         0
192.168.4.0/24      192.168.2.1      lan0         17      PUSH              0         0
```

1) VRF 定義番号
2) プレフィックス
   vrf を指定した場合はプレフィックス順に表示します。
3) 次ホップアドレス
   インタフェース経路は 0.0.0.0 と表示されます。
4) 出力インタフェース名
   LSP に送出する場合は LSP ラベル / インタフェース名 の形式で，それ以外の場合はインタフェース名だけ表示されます。
5) 出力ラベル (出力ラベル値がない場合は ‘-‘を表示)
6) ラベルオペレーションコード
   以下のどれかが表示されます。

   PUSH : プレフィックスに該当する IP パケットに出力ラベルを PUSH して出力インタフェース名のインタフェースに出力します。

   PUSH-VPN :
   プレフィックスに該当する IP パケットに VPN ラベルを PUSH して次ホップアドレスに該当する FTN エントリを再検索し，FTN エントリの内容に従って出力します。

   DLVR-VPN :
   プレフィックスに該当する IP パケットを出力インタフェース名のインタフェースにそのまま出力します。
7) エントリを使用して送出したパケット数
8) エントリを使用して送出したオクテット数

MPLS を使用するすべてのインタフェースの統計情報を表示する場合

(interface 指定時で <interface> を省略)

```
# mplsstat interface
[Data for Interface Table]
I/F     USE      IN-PACKET  OUT-PACKET   Error (   TTL  LABEL  SHORT  ENTRY)
---     ---      ---------  ----------   -----     ---  -----  -----  ------
(1)     (2)         (3)        (4)        (5)      (6)   (7)    (8)    (9)
lan0    Enabled      11136       11123      13 (     6      4      0      8)
lan1    Disabled         0           0       0 (     0      0      0      0)
rmt0    Enabled      28748       98983      16 (     2      4      6      3)
```

1) インタフェース名
2) MPLS の有効／無効
3) 入力 MPLS パケット数
4) 出力 MPLS パケット数
5) エラー破棄パケット総数
6) TTL Expire 検出数
7) 不正ラベル検出数
8) 不正長のパケット検出数
9) ILM 未登録検出数

特定のインタフェースの統計情報を表示する場合 (interface 指定時で <interface> を指定)

```
# mplsstat interface lan0
[Data for Interface Table]
Interface                : lan0              (1)
Use for MPLS Forwarder   : Enabled           (2)
PACKET RESULT            :
  in packet              : 11136             (3)
  out packet             : 11123             (4)
ERROR and DROP PACKET    : 13                (5)
  TTL Expire             : 6                 (6)
  illegal label packet   : 4                 (7)
  too short MPLS packet  : 0                 (8)
  ILM no entry           : 3                 (9)
```

1) インタフェース名
2) MPLS の有効／無効
3) 入力 MPLS パケット数
4) 出力 MPLS パケット数
5) エラー破棄パケット総数
6) TTL Expire 検出数
7) 不正ラベル検出数
8) 不正長のパケット検出数
9) ILM 未登録検出数

すべての VC 情報を表示する場合 (vc 指定時で <vc_id> または <interface> を省略)

- エントリが存在する場合

```
# mplsstat vc
[Data for VC]

VC I/F  VC ID    NH ADDR           OUT I/F       OUTLABEL  INLABEL
------  -------  ---------------   -----------   --------  --------
 (1)     (2)         (3)              (4)          (5)      (6)
lan1    1        10.56.11.21       16/lan0       21        22
lan2    2        10.56.11.21       16/lan0       22        23
```

- エントリが存在しない場合

```
# mplsstat vc
[Data for VC]
No Entry.
                                        :
```

特定のインタフェースの VC 情報を表示する場合 (vc 指定時で <interface> を指定)

```
# mplsstat vc lan1
[Data for VC]
VC Interface             : lan1              (1)
Virtual Circuit ID       : 1                 (2)
In Label                 : 22                (3)
Nexthop Address          : 10.56.11.21       (4)
Out Interface            : 16/lan0           (5)
Out Label                : 21                (6)
PACKET RESULT            :
  in packet              : 450               (7)
  in octet               : 17622             (8)
  out packet             : 28                (9)
  out octet              : 2134              (10)
```

1) VC 識別子

2) VC インタフェース名
3) 入力ラベル
   VC LSP が確立できていなく、入力ラベルが存在しない場合は N / A と表示されます。
4) 次ホップアド レス
   インタフェース経路は 0.0.0.0 と表示されます。
5) 出力インタフェース名
   LSP に送出する場合は LSP ラベル / インタフェース名 の形式で，それ以外の場合はインタフェース名だけ表示されます。
6) 出力ラベル
   VC LSP が確立できていなく、出力ラベルが存在しない場合は N / A と表示されます。
7) VC で受信したパケット数
8) VC で受信したオクテット数
9) VC で送出したパケット数
10) VC で送出したオクテット数

15.7.13 mcstat

[機能]

マルチキャスト情報の表示

[入力形式]

mcstat [<parameter>]

[オプション]

なし

[パラメタ]

<parameter>

- protocol
  マルチキャスト・ルーティングプロトコル情報の表示
- group
  グループ情報の表示
- interface
  インタフェース情報の表示
- route
  マルチキャスト・ルーティングテーブル情報の表示
- rp
  BSR/RP 情報の表示

[説明]

マルチキャスト情報を一覧表示します。パラメタ無しで実行すると、全情報を表示します。以下の情報が表示されます。

[例]

以下に、表示例を示します。

```
# mcstat
Multicast Protocol: PIM-SM   ---(1)

Multicast Groups
 VIF Querier           Uptime        QTimer Expire Flags
   0 me                0000.00:00:00     45      0 QUERIER
 --- -------           ------------ ------ ------ -------
 (2)    (3)               (4)        (5)    (6)    (7)
     Group             Reporter          Uptime
     239.255.255.10    192.168.1.100     0000.00:03:27
     239.255.255.11    192.168.1.100     0000.00:01:24
     ----------        ----------        -------------
         (8)               (9)               (10)
 VIF Querier           Uptime        QTimer Expire Flags
   1 192.168.2.2       0000.00:01:23     55    160
     Group             Reporter          Uptime
     239.255.255.12    192.168.2.100     0000.00:00:21
Total Multicast Groups: 3   ---(11)

Virtual Interface Table
 VIF Netif    Thresh Local-Address     Subnet           Flags       Neighbors
   0 lan0          1 192.168.1.1       192.168.1        PIM         192.168.1.2
   1 lan1          1 192.168.2.1       192.168.2        DR NO-NBR
   2 register      1 192.168.1.1
 --- -------- ------ -------------     ---------        ---------   -----------
 (12)   (13)   (14)      (15)             (16)             (17)         (18)
Total Virtual Interface Tables: 3   ---(19)
Total Neighbors: 1   ---(20)

Multicast Routing Table
--------------------------(*,G)----------------------------
 Source          Group           RP-addr         Flags
 INADDR_ANY      239.255.20.1    192.168.2.1     WC RP
 ----------      ------------    -----------     -----
    (21)            (22)            (23)         (24)
                  012   ---(25)
    Joined   oifs: ...   ---(26)
    Pruned   oifs: ...   ---(27)
    Leaves   oifs: .l.   ---(28)
    Asserted oifs: ...   ---(29)
    Outgoing oifs: .o.   ---(30)
    Incoming     : ..I   ---(31)
    Upstream nbr : 192.168.1.1     ---(32)
    Preference   : 0 (0x00000000)  ---(33)
    Metric       : 0 (0x00000000)  ---(34)
    Entry Timer  :    200    ---(35)
    J/P Timer    :     30    ---(36)
    RegSup Timer :      0    ---(37)
    Assert Timer :      0    ---(38)
    Join Timers  :   vif0   vif1   vif2
                        0      0      0
                     -----------------
                           (39)
    Prune Timers :   vif0   vif1   vif2
                        0      0      0
                     -----------------
                           (40)
--------------------------(S,G)----------------------------
 Source          Group           RP-addr         Flags
 192.168.3.2     239.255.20.1    192.168.2.1     RP CACHE SG
                   012
    Joined   oifs: ...
    Pruned   oifs: p..
    Leaves   oifs: .l.
    Asserted oifs: ...
    Outgoing oifs: .o.
    Incoming     : ..I
    Upstream nbr : 192.168.1.1
    Preference   : 1024 (0x00000400)
    Metric       : 1024 (0x00000400)
    Entry Timer  :    210
    J/P Timer    :     40
    RegSup Timer :      0
    Assert Timer :      0
    Join Timers  :   vif0   vif1   vif2
                        0      0      0
```

続く

```
Number of Groups: 1                 ---(41)
Number of Cache MIRRORs: 1          ---(42)
Total Multicast Routing Tables: 2   ---(43)

--------------------------RP-Set---------------------------
Current BSR address: 192.168.1.1   ---(44)
RP-address      Incoming   Group prefix   Priority   Holdtime
192.168.1.1     2          224/4          0          95
-----------     --------   ------------   --------   --------
    (45)          (46)         (47)         (48)       (49)
Total RPs: 1   ---(50)

#
```

続き

マルチキャスト・ルーティングプロトコル情報

1) 動作中のマルチキャスト・ルーティングプロトコル
   グループ情報
2) VIF(Virtual Interface) 番号
3) IGMP General Query の送信者 (自分自身の場合には me と表示)
4) IGMP Query を受け取ってからの経過時間 (自身が Querier の場合には常に 0)
5) IGMP General Query 発行用のタイマ
6) Other Querier Present Interval のタイムアウトまでの時間
7) フラグ情報
   フラグの内容を以下に説明します。

   QUERIER
   IGMP Querier である

8) グループアドレス
   224.0.0.0/24 のグループはローカル・ネットワーク用に予約されているため、マルチキャスト・パケット転送の対象外になります。
9) IGMP Membership Report の送信者
10) IGMP Membership Report を受信してからの経過時間
11) IGMP で管理されているグループの総数
    インタフェース情報
12) VIF(Virtual Interface) 番号
13) VIF に対応する実際のインタフェース。register は PIM-SM 使用時の
    PIM Register パケットの送受信用の仮想インタフェース
14) TTL しきい値
15) インタフェースの IP アドレス
16) インタフェースのサブネットワークアドレス
17) フラグ情報
    フラグの内容を以下に説明します。

    DISABLED
    非動作状態

    DOWN インタフェースダウン

    DR 代表ルータ (DR:Designated Router) として動作

PIM　PIM プロトコルが動作中

P2P　Point-to-Point インタフェース

NO-NBR

隣接ルータが存在しない

18) 隣接ルータ

19) VIF の総数

20) 隣接ルータの総数

マルチキャスト・ルーティングテーブル情報

21) マルチキャスト・パケットの送信元アドレス

(*,G) エントリの場合には INADDR_ANY となります。

22) マルチキャスト・グループ

23) RP アドレス (PIM-SM だけ)

24) フラグ情報

フラグの内容を以下に説明します。

SPT　SPT への経路

SPT フラグが立つのは、RP 経由のツリーと SPT の分岐点となるルータです。分岐点が最終ホップのルータよりも上流にある場合には、最終ホップのルータは SPT への切り替えが行われたことを知る手段がないため、SPT フラグは立ちません。

WC　ワイルド・カードを含むエントリ

RP　RP への経路

CACHE　カーネルにルーティングテーブルが登録されている

ASSERTED

Assert タイマが動作している冗長なネットワーク構成により複数の転送経路が存在する場合には、PIM Assert メッセージにより片側の経路が刈り取られます。この際、転送経路が変わる場合があるため、下流のルータは上流側のネットワーク上で発生した PIM Assert を追随してアップストリーム・ルータを切り替え、Assert タイマを動作させます。Assert タイマの満了時には、アップストリーム・ルータを再びもとに戻します。

SG　(S,G) エントリ

25) VIF の番号の下１桁

26) インタフェース情報 (Join 状態フラグ、PIM-SM だけ)

インタフェース情報は、左から vif0、vif1、vif2 の状態を表します。

たとえば .j. のように表示されているのならば、vif1 だけが Join 状態にあり、vif0、vif2 は Join 状態でないことを示します。

27) インタフェース情報 (Prune 状態フラグ)

28) インタフェース情報 (グループ参加者の存在フラグ)

29) インタフェース情報 (Assert 状態フラグ)

30) 出力先インタフェース

31) 入力インタフェース

32) アップストリーム・ルータ

上流側のパケットの転送者となっているルータです。

33) プリファレンス値

34) メトリック値

35) ルーティングテーブルの生存時間

36) Join/Prune タイマ (PIM-SM だけ)

37) Register-Suppression タイマ (PIM-SM だけ)

38) Assert タイマ

39) VIF ごとの Join タイマ (PIM-SM だけ)

40) VIF ごとの Prune タイマ (PIM-DM だけ)

41) マルチキャスト・ルーティングを行っているグループの総数
(*,G) または (S,G) エントリが存在しているグループの総数です。

42) CACHE フラグが立っているマルチキャスト・ルーティングテーブルの総数

43) (*,G)、(S,G) エントリの総数
BSR/RP 情報 (PIM-SM だけ)

44) BSR アドレス

45) RP アドレス

46) 入力インタフェース

47) マルチキャスト・グループ

48) プライオリティ

49) 生存時間

50) RP の総数

15.8　ログ、トレースの表示

15.8.1　elog

[機能]

エラーログの表示

[入力形式]

elog

[オプション]

なし

[パラメタ]

なし

[説明]

ROM または I/O ドライバによるハード診断エラー、およびシステムダウンのエラーログ情報を表示します。

[注意]

"Logging time:"で表示する時刻は、構成定義情報にタイムゾーン (time zone <offset>) が指定されていない状態では GMT(グリニッジ標準時間) での表示となります。

[例]

以下に、表示例を示します。

表示例

```
# elog
[0] Error Log:
flag=80,mode=00,unit=80,regsp=0028b490
Firm information:
MR1000  V21.00 PTF:NY0001
System down information:
down code [81010015:00000001]
Logging time:
Sun Jul 22 12:35:27 2001
Register:
    srr0   [00085c18] srr1   [00001030] lr     [001dbaf8] dar    [00000000]
    dsisr  [00000000] sivec  [00000000] simr_h [20422d00] simr_l [24002058]
    dmiss  [0028b570] imiss  [00005c18] tescr1 [00393980] ltescr1[0028b590]
    gpr00  [00010000] gpr01  [0028b570] gpr02  [00000016] gpr03  [81010015]
    gpr04  [00000001] gpr05  [0028b490] gpr06  [00000001] gpr07  [00000000]
    gpr08  [00000004] gpr09  [00000001] gpr10  [f0011b30] gpr11  [f0011b30]
    gpr12  [28000000] gpr13  [00000000] gpr14  [0074e754] gpr15  [00235b24]
    gpr16  [00000020] gpr17  [f0010c1c] gpr18  [0028b610] gpr19  [00280000]
    gpr20  [0028b608] gpr21  [0074e754] gpr22  [00000000] gpr23  [00000000]
    gpr24  [0028b608] gpr25  [0028b610] gpr26  [0090d7f4] gpr27  [08000800]
    gpr28  [00235b48] gpr29  [0090d704] gpr30  [00000001] gpr31  [00000001]
Configuration Register:
    pcisr  [----0000] errdr1 [------00] ipbesr [------00] errdr2 [------00]
    pcibesr[------00] ppear  [00000000]
#
```

15.8.2 dsplog

[機能]

syslog メッセージの表示

[入力形式]

dsplog

[オプション]

なし

[パラメタ]

なし

[説明]

syslog メッセージの履歴を表示します。最新のメッセージからさかのぼって、1024 件以上表示できます。

[注意]

本装置を再起動すると、syslog メッセージはクリアされます。

[例]

以下に、表示例を示します。

```
Nov 11 08:31:06 init: system startup now.
Nov 11 08:31:06 protocol: [mb/0] lan port link down
Nov 11 08:31:06 protocol: [mb/0] lan port link up
```

15.8.3　ppptrace

[機能]

PPP フレームトレースの表示

[入力形式]

ppptrace

[オプション]

なし

[パラメタ]

なし

[説明]

PPP フレームトレース情報を表示します。

[注意]

PPP フレームトレース情報は、本装置を再起動するとクリアされます。

[例]

以下に、表示例および表示内容を示します。

表示例 (PPPoE 接続の場合)

```
# ppptrace

[001] internet.ISP     : PPP session start                02.08.07 09:55:01.697
-(1)- ----(2)-----       ------(3)--------                ----------(4)--------
        port=slot:mb, line:0 (lan0)
             ---------(5)----------

[002] internet.ISP     : Send LCP       Configure-Request 02.08.07 09:55:01.697
                        -(6)- -(7)-     -------(8)-------
        port=slot:mb, line:0 (lan0)
        data=c021 0100 000a 0506 f01e 028e
             -----------(9)--------------

[003] internet.ISP     : Recv LCP       Configure-Request 02.08.07 09:55:02.116
        port=slot:mb, line:0 (lan0)
        data=c021 0101 001c 0802 0702 0206 0000 0000
             0104 05ae 0506 b104 7cbb 0304 c023

[004] internet.ISP     : Send LCP       Configure-Reject  02.08.07 09:55:02.116
        port=slot:mb, line:0 (lan0)
        data=c021 0401 000e 0802 0702 0206 0000 0000

[005] internet.ISP     : Recv LCP       Configure-Nak     02.08.07 09:55:02.116
        port=slot:mb, line:0 (lan0)
        data=c021 0300 0008 0104 05ae
```

```
[006] internet.ISP     : Send LCP       Configure-Request 02.08.07 09:55:02.116
        port=slot:mb, line:0 (lan0)
        data=c021 0101 000e 0104 05ae 0506 f01e 028e

[007] internet.ISP     : Recv LCP       unknown code(0c)  02.08.07 09:55:02.121
        port=slot:mb, line:0 (lan0)
        data=c021 0c00 002a b104 7cbb 7573 6572 2d70
             7070 2032 2e33 2e33 2028 6275 696c 7420
             4a61 6e20 3238 2032 3030 3229

[008] internet.ISP     : Send LCP       Code-Reject       02.08.07 09:55:02.121
        port=slot:mb, line:0 (lan0)
        data=c021 0701 002e 0c00 002a b104 7cbb 7573
             6572 2d70 7070 2032 2e33 2e33 2028 6275
             696c 7420 4a61 6e20 3238 2032 3030 3229

[009] internet.ISP     : Recv LCP       Configure-Request 02.08.07 09:55:02.121
        port=slot:mb, line:0 (lan0)
        data=c021 0102 0012 0104 05ae 0506 b104 7cbb
             0304 c023

[010] internet.ISP     : Send LCP       Configure-Ack     02.08.07 09:55:02.121
        port=slot:mb, line:0 (lan0)
        data=c021 0202 0012 0104 05ae 0506 b104 7cbb
             0304 c023

[011] internet.ISP     : Recv LCP       Configure-Ack     02.08.07 09:55:02.121
        port=slot:mb, line:0 (lan0)
        data=c021 0201 000e 0104 05ae 0506 f01e 028e

[012] internet.ISP     : Send PAP       Authenticate-Req  02.08.07 09:55:02.121
        port=slot:mb, line:0 (lan0)
        data=c023 0101 000e 0474 6573 7404 7465 7374

[013] internet.ISP     : Recv LCP       unknown code(0c)  02.08.07 09:55:02.150
        port=slot:mb, line:0 (lan0)
        data=c021 0c01 002a b104 7cbb 7573 6572 2d70
             7070 2032 2e33 2e33 2028 6275 696c 7420
             4a61 6e20 3238 2032 3030 3229

[014] internet.ISP     : Send LCP       Code-Reject       02.08.07 09:55:02.150
        port=slot:mb, line:0 (lan0)
        data=c021 0702 002e 0c01 002a b104 7cbb 7573
             6572 2d70 7070 2032 2e33 2e33 2028 6275
             696c 7420 4a61 6e20 3238 2032 3030 3229

[015] internet.ISP     : Recv PAP       Authenticate-Ack  02.08.07 09:55:02.150
        port=slot:mb, line:0 (lan0)
        data=c023 0201 0010 0b47 7265 6574 696e 6773
             2121

[016] internet.ISP     : Send IPCP      Configure-Request 02.08.07 09:55:02.151
        port=slot:mb, line:0 (lan0)
        data=8021 0100 0010 0306 0000 0000 8106 0000
             0000

[017] internet.ISP     : Recv CCP       Configure-Request 02.08.07 09:55:02.151
        port=slot:mb, line:0 (lan0)
        data=80fd 0101 000a 1a04 7800 0102

[018] internet.ISP     : Send LCP       Protocol-Reject   02.08.07 09:55:02.151
        port=slot:mb, line:0 (lan0)
        data=c021 0803 0010 80fd 0101 000a 1a04 7800
             0102

[019] internet.ISP     : Recv IPCP      Configure-Request 02.08.07 09:55:02.151
        port=slot:mb, line:0 (lan0)
        data=8021 0101 0010 0306 b40a 0101 0206 002d
             0f01

[020] internet.ISP     : Send IPCP      Configure-Reject  02.08.07 09:55:02.151
        port=slot:mb, line:0 (lan0)
        data=8021 0401 000a 0206 002d 0f01
```

```
[021] internet.ISP     : Recv IPCP      Configure-Nak     02.08.07 09:55:02.153
        port=slot:mb, line:0 (lan0)
        data=8021 0300 0010 0306 b40a 0164 8106 b40a
             010a

[022] internet.ISP     : Send IPCP      Configure-Request 02.08.07 09:55:02.153
        port=slot:mb, line:0 (lan0)
        data=8021 0101 0010 0306 b40a 0164 8106 b40a
             010a

[023] internet.ISP     : Recv LCP       unknown code(0c)  02.08.07 09:55:02.157
        port=slot:mb, line:0 (lan0)
        data=c021 0c02 002a b104 7cbb 7573 6572 2d70
             7070 2032 2e33 2e33 2028 6275 696c 7420
             4a61 6e20 3238 2032 3030 3229

[024] internet.ISP     : Send LCP       Code-Reject       02.08.07 09:55:02.157
        port=slot:mb, line:0 (lan0)
        data=c021 0703 002e 0c02 002a b104 7cbb 7573
             6572 2d70 7070 2032 2e33 2e33 2028 6275
             696c 7420 4a61 6e20 3238 2032 3030 3229

[025] internet.ISP     : Recv IPCP      Configure-Request 02.08.07 09:55:02.157
        port=slot:mb, line:0 (lan0)
        data=8021 0102 000a 0306 b40a 0101

[026] internet.ISP     : Send IPCP      Configure-Ack     02.08.07 09:55:02.157
        port=slot:mb, line:0 (lan0)
        data=8021 0202 000a 0306 b40a 0101

[027] internet.ISP     : Recv IPCP      Configure-Ack     02.08.07 09:55:02.157
        port=slot:mb, line:0 (lan0)
        data=8021 0201 0010 0306 b40a 0164 8106 b40a
             010a

[028] internet.ISP     : Send LCP       Echo-Request      02.08.07 09:56:02.216
        port=slot:mb, line:0 (lan0)
        data=c021 0904 0008 f01e 028e

[029] internet.ISP     : Recv LCP       Echo-Reply        02.08.07 09:56:02.217
        port=slot:mb, line:0 (lan0)
        data=c021 0a04 0008 b104 7cbb
#
```

1) ログ番号

   ログ番号が、001～999 の 10 進数値で表示されます。

2) 接続先名

   この PPP セッションが利用した接続先名が<ネットワーク名>.<接続先名>の形式で表示されます。

3) ネゴシエーション開始

   ネゴシエーション開始時に表示されます。

4) 採取時間

   情報を採取した時間が表示されます。

5) 回線識別子

   以下の形式で通信に利用した回線が表示されます。

   slot:<slot 番号> line:<line 番号> (<回線固有情報>)

<slot 番号>

通信に利用した物理回線のスロット番号が表示されます。

(※ MR1000 では必ず"mb"(基本ボード) が表示されます。)

<line 番号>

通信に利用した物理回線の回線番号が表示されます。

回線固有情報 :

利用する回線に応じた内容が表示されます。

- HSD の場合
  表示されません。
- ISDN の場合
  チャネル名が表示されます。
- PPPoE の場合
  利用した lan 定義が表示されます。

6) 送受信
   以下のどれかが表示されます。

   - Send
   - Recv

7) プロトコル種別
   PPP のプロトコル種別として、以下のプロトコルが表示されます。
   プロトコル種別の前に「MP:」が付加されている場合、そのパケットが MP によってカプセル化されていることを示します。
   (※ CCP,ICCP,BAP,BACP,BCP,MPLSCP は未サポートです。)

```
Oxc021  LCP     : Link Control Protocol
Oxc023  PAP     : Password Authentication Protocol
Oxc223  CHAP    : Challenge-Handshake Authentication Protocol
Ox8021  IPCP    : Internet Protocol Control Protocol
Ox8031  BCP     : Bridge Control Protocol
Ox8057  IPV6CP  : IPv6 Control Protocol
Ox80fd  CCP     : Compression Control Protocol
Ox80fb  ICCP    : Individual Compression Control Protocol
Oxc02d  BAP     : Bandwidth Allocation Protocol
Oxc02b  BACP    : Bandwidth Allocation Control Protocol
Oxc029  CBCP    : Callback Control Protocol
0x8281  MPLSCP  : MPLS Control Protocol
```

8) コード種別
   各プロトコルにおけるコードの内容が以下の文字列で表示されます。

   - プロトコル種別が LCP、CCP、ICCP、IPCP、IPV6CP、BCP、MPLSCP の場合

```
Ox01    Configure-Request
Ox02    Configure-Ack
Ox03    Configure-Nak
Ox04    Configure-Reject
Ox05    Terminate-Request
Ox06    Terminate-Ack
Ox07    Code-Reject
```

   - プロトコル種別が LCP の場合

```
Ox08    Protocol-Reject
Ox09    Echo-Request
Ox0a    Echo-Reply
Ox0b    Discard-Request
```

   - プロトコル種別が CCP、ICCP の場合

```
Ox0e    Reset-Request
Ox0f    Reset-Act
```

   - プロトコル種別が PAP の場合

```
Ox01    Authenticate-Request
Ox02    Authenticate-Ack
Ox03    Authenticate-Nak
```

- プロトコル種別が CHAP の場合

```
Ox01    Challenge
Ox02    Response
Ox03    Success
Ox04    Failure
```

- プロトコル種別が BAP の場合

```
Ox01    Call-Request
Ox02    Call-Response
Ox03    Callback-Request
Ox04    Callback-Response
Ox05    Link-Drop-Request
Ox06    Link-Drop-Response
Ox07    Call-Status-Ind
Ox08    Call-Status-Rsp
```

- プロトコル種別が CBCP の場合

```
Ox01    Callback-Request
Ox02    Callback-Response
Ox03    Callback-Ack
```

9) data=

送受信したパケットの内容が、16 進数値で表示されます。最大 108 バイト分までが表示され、それより後は表示されません。

15.8.4 pppoetrace

[機能]

PPPoE フレームトレースの表示

[入力形式]

pppoetrace

[オプション]

なし

[パラメタ]

なし

[説明]

PPPoE のフレームトレースを表示します。

[注意]

PPPoE フレームトレース情報は、本装置を再起動するとクリアされます。

[例]

以下に表示例および表示内容を示します。

```
# pppoetrace
[01] Internet.ISP      : PPPoE Discovery Stage start      00.01.02 09:19:54.225
---- ------------        -------------------------      --------------------
(1)     (2)                 (3)                                   (4)

[02] Internet.ISP      : Send PADI                len=35  00.01.02 09:19:54.275
                         ---- ----                ------
                         (5)  (6)                   (7)

       data=ffff ffff ffff 0000 0eaa 010c 8863 1109 --- (8)
            0000 000f 0101 0000 0103 0007 0000 0eaa
            010c 01

[03] Internet.ISP      : Recv PADO                len=62  00.01.02 09:19:54.325
       data=0000 0eaa 010c 0003 e48a 0c1c 8863 1107
            0000 002a 0101 0000 0103 0007 0000 0eaa
            010c 0101 0200 0372 6173 0104 0010 4c3b
            69dc e7d6 949a 90d6 86b5 8bdf 5ce5

[04] Internet.ISP      : Send PADR                len=62  00.01.02 09:19:54.445
       data=0003 e48a 0c1c 0000 0eaa 010c 8863 1119
            0000 002a 0101 0000 0103 0007 0000 0eaa
            010c 0101 0200 0372 6173 0104 0010 4c3b
            69dc e7d6 949a 90d6 86b5 8bdf 5ce5

[05] Internet.ISP      : Recv PADS                len=62  00.01.02 09:19:54.495
       data=0000 0eaa 010c 0003 e48a 0c1c 8863 1165
            0003 002a 0101 0000 0103 0007 0000 0eaa
            010c 0101 0200 0372 6173 0104 0010 4c3b
            69dc e7d6 949a 90d6 86b5 8bdf 5ce5

[06] Internet.ISP      : Send PADT                len=20  00.01.02 09:21:16.099
       data=0003 e48a 0c1c 0000 0eaa 010c 8863 11a7
            0003 0000
```

1) ログ番号
   ログ番号が 01～99 の 10 進数値で表示されます。
2) 接続先名
   この PPPoE セッションが利用した接続先名が<ネットワーク名>.<接続先名>の形式で表示されます。
3) ネゴシエーション開始
   ネゴシエーション開始時に表示されます。
4) pppoetrace 採取時刻
   pppoetrace 採取時刻が表示されます。
5) 送受信
   以下のどれかが表示されます。
   - Send
   - Recv
6) コード種別
   PPPoE フレームのコードの内容として、以下のコードが表示されます。
   - PADI
     PPPoE Active Discovery Initiation
   - PADO
     PPPoE Active Discovery Offer
   - PADR
     PPPoE Active Discovery Request
   - PADS
     PPPoE Active Discovery Session-confirmation
   - PADT
     PPPoE Active Discovery Terminate
   - SESS
     Session Stage
7) フレーム長
   送受信したフレーム長が 10 進数値で表示されます。
8) data=
   送受信したフレームの内容を 16 進数値で表示します。最大 128 バイト分まで表示され、それより後は表示されません。

15.8.5 mdmtrace

[機能]

モデム制御トレースの表示

[入力形式]

mdmtrace

[オプション]

なし

[パラメタ]

なし。

[説明]

発着呼のトレースデータを表示する。

[注意]

モデム制御トレース情報は、本装置を再起動するとクリアされます。

[例]

以下に、表示例および表示内容を示します。

```
# mdmtrace

[01]  Send                                          03.08.02 09:08:33.951
(1)-  (2)-                                          ----------(3)--------
        sig_on=(CS,ER,RS)
        -------(4)-------
        data=4154 0d                                AT.
        ----(5)-----                                -(6)-

[02]  Recv                                          03.08.02 09:08:33.960
        sig_on=(CS,ER,RS)
        data=0d0a 4f4b 0d0a                         ..OK..

[03]  Send                                          03.08.02 09:08:33.961
        sig_on=(CS,ER,RS)
        data=4154 2646 0d                           AT&F.

[04]  Recv                                          03.08.02 09:08:33.978
        sig_on=(CS,ER,RS)
        data=0d0a 4f4b 0d0a                         ..OK..

[05]  Send                                          03.08.02 09:08:33.979
        sig_on=(CS,ER,RS)
        data=4154 4530 5631 5337 353d 3053 3935 3d34   ATE0V1S75=0S95=4
             350d                                   5.

[06]  Recv                                          03.08.02 09:08:33.991
        sig_on=(CS,ER,RS)
        data=4154 4530 5631 5337 353d 3053 3935 3d34   ATE0V1S75=0S95=4
             350d 0d0a 4f4b 0d0a                    5...OK..

[07]  Send                                          03.08.02 09:08:33.992
        sig_on=(CS,ER,RS)
        data=4154 5631 0d                           ATV1.

[08]  Recv                                          03.08.02 09:08:34.001
        sig_on=(CS,ER,RS)
        data=0d0a 4f4b 0d0a                         ..OK..

[09]  Send                                          03.08.02 09:08:34.002
        sig_on=(CS,ER,RS)
        data=4154 4530 0d                           ATE0.

[10]  Recv                                          03.08.02 09:08:34.012
        sig_on=(CS,ER,RS)
        data=0d0a 4f4b 0d0a                         ..OK..

[11]  Send                                          03.08.02 09:08:34.013
        sig_on=(CS,ER,RS)
        data=4154 264b 330d                         AT&K3.

[12]  Recv                                          03.08.02 09:08:34.022
        sig_on=(CS,ER,RS)
        data=0d0a 4f4b 0d0a                         ..OK..

[13]  Send                                          03.08.02 09:08:34.023
        sig_on=(CS,ER,RS)
        data=4154 5834 0d0a 00                      ATX4...

[14]  Recv                                          03.08.02 09:08:34.032
        sig_on=(CS,ER,RS)
        data=0d0a 4f4b 0d0a                         ..OK..

[15]  Send                                          03.08.02 09:08:34.034
        sig_on=(CS,ER,RS)
        data=4154 4d31 0d0a 00                      ATM1...

[16]  Recv                                          03.08.02 09:08:34.043
        sig_on=(CS,ER,RS)
        data=0d0a 4f4b 0d0a                         ..OK..

[17]  Send                                          03.08.02 09:08:34.044
        sig_on=(CS,ER,RS)
        data=4154 4c32 0d0a 00                      ATL2...

[18]  Recv                                          03.08.02 09:08:34.053
        sig_on=(CS,ER,RS)
        data=0d0a 4f4b 0d0a                         ..OK..
#
```

1) ログ番号
ログ番号が、01～99 の 10 進数値で表示されます。

2) 送受信
以下のどれかが表示されます。

Send ルータがモデムへデータを送信したことを示します。

Recv ルータがモデムからデータを受信したことを示します。

Change Signal
RS-232C インタフェース信号が変更されたことを示します。

3) 採取時間
情報を採取した時間が表示されます。

4) 信号状態
RS-232C インタフェース信号が ON の信号が表示されます。
信号の内容を以下に説明します。

CS モデムがデータ受信可能であることを示します。

ER ルータが通信可能であることを示します。

RS ルータがデータ受信可能であることを示します。または、ルータがデータ送信を要求していることを示します。

CI 着信を検出したことを示します。

CD キャリアが検出され、接続状態であることを示します。

DR モデムが送受信可能であることを示します。

5) data=
送受信したデータの内容が、16 進数値で表示されます。最大 128 バイト分までが表示され、それより後は表示されません。

6) ASCII 表示
5) のデータが ASCII 文字で表示されます。

15.8.6　iketrace

[機能]

IKE トレース情報表示

[入力形式]

iketrace [<mode>]

[パラメタ]

<mode>

- clear
  取得した IKE トレース情報を消去します。

[説明]

IKE ネゴシエーションパケットのトレース情報を表示します。
以下に機種ごとのトレース表示最大数を示します。

表示最大数	機種
30	MR1000

[注意]

IKE フレームトレース情報は、本装置を再起動するとクリアされます。

[例]

以下に表示例および表示内容を示します。

```
# iketrace
[1]  ISAKMP Send                                Aug  7 10:26:26 2002
---  -----------                                --------------------
(1)     (2)                                            (3)
        Cookies:(22f2b428fb243bba:0000000000000000)
                 --------------------------------
                              (4)
        Exchange Type: Aggressive          Len:215(0xd7)
                       ----------           --------
                           (5)                 (6)
        data=22f2 b428 fb24 3bba 0000 0000 0000 0000 --- (7)
             0110 0400 0000 0000 0000 00d7 0400 0038
             0000 0001 0000 0001 0000 002c 0101 0001
             0000 0024 0101 0000 8001 0001 8002 0001
             8003 0001 8004 0001 800b 0001 000c 0004
             0001 5180 0a00 0064 1d9b dedd 0bd7 55bf
             d1d1 0ba1 3595 fa9e 421e 790e 4e9b c95c
             dc1e 07bc e220 2179 095c 11f8 4138 a44a


[2]  ISAKMP Receive                             Aug  7 10:26:27 2002
        Cookies:(22f2b428fb243bba:5b504feebef8c495)
        Exchange Type: Aggressive          Len:255(0xff)
        data=22f2 b428 fb24 3bba 5b50 4fee bef8 c495
             0110 0400 0000 0000 0000 00ff 0400 0038
             0000 0001 0000 0001 0000 002c 0101 0001
             0000 0024 0101 0000 8001 0001 8002 0001
             8003 0001 8004 0001 800b 0001 000c 0004
             0001 5180 0a00 0064 05ab 21eb 7d9c 2261
             80b8 ca00 9647 fdc1 ea94 1d0b 1740 ba33
             5f64 a095 fb90 ac52 e533 e820 7da5 ceca


[3]  ISAKMP Send                                Aug  7 10:26:27 2002
        Cookies:(22f2b428fb243bba:5b504feebef8c495)
        Exchange Type: Aggressive          Len:48(0x30)
        data=22f2 b428 fb24 3bba 5b50 4fee bef8 c495
             0810 0400 0000 0000 0000 0030 0000 0014
             0d89 bb75 240e 3028 294d 41af 7c86 0d15


[4]  ISAKMP Send(Before Encrypt)                Aug  7 10:26:27 2002
        Cookies:(22f2b428fb243bba:5b504feebef8c495)
        Exchange Type: Informational       Len:76(0x4c)
        data=22f2 b428 fb24 3bba 5b50 4fee bef8 c495
             0810 0501 774d 2a19 0000 004c 0b00 0014
             81de 9a99 455f a72d 9b54 c631 2909 3d1b
             0000 001c 0000 0001 0110 6002 22f2 b428
             fb24 3bba 5b50 4fee bef8 c495


[5]  ISAKMP Send                                Aug  7 10:26:27 2002
        Cookies:(22f2b428fb243bba:5b504feebef8c495)
        Exchange Type: Informational       Len:84(0x54)
        data=22f2 b428 fb24 3bba 5b50 4fee bef8 c495
             0810 0501 774d 2a19 0000 0054 ebbb fd4a
             474c 9cf7 6a1f daaa c622 7389 5d0d 2787
             d87b ca80 af88 338f 2dca 3147 c9d2 5656
             2602 59c8 f6e1 6c61 d8a3 0ae3 4d79 7ffa
             ac57 7db9


[6]  ISAKMP Send(Before Encrypt)                Aug  7 10:26:27 2002
        Cookies:(22f2b428fb243bba:5b504feebef8c495)
        Exchange Type: Quick               Len:148(0x94)
        data=22f2 b428 fb24 3bba 5b50 4fee bef8 c495
             0810 2001 4730 70fb 0000 0094 0100 0014
             fd3b 2b24 f778 8e08 a7c8 bbb2 b7bc 0914
             0a00 0030 0000 0001 0000 0001 0000 0024
             0103 0401 03ff 7c4b 0000 0018 0102 0000
             8001 0001 8002 7080 8004 0001 8005 0001
             0500 0014 f7c2 d1ab d5c6 d3e4 5929 38ae
             91f9 5354 0500 0010 0400 0000 0000 0000
```

続く

```
[7]  ISAKMP Send                              Aug  7 10:26:27 2002
       Cookies:(22f2b428fb243bba:5b504feebef8c495)
       Exchange Type: Quick               Len:156(0x9c)
       data=22f2 b428 fb24 3bba 5b50 4fee bef8 c495
            0810 2001 4730 70fb 0000 009c 789e 35b5
            fb49 2b8a 3ebd 5663 81ab 4c78 e4cf 864c
            b968 1d8e 6238 d076 b095 0b17 af03 33e0
            2735 f9ba 13dd 2000 3efb bc65 1e8b b482
            3be8 48ac ebab 6548 3394 512e 6a27 5f37
            c16a 97a8 4a65 40fa 06b1 3eef 1ea2 8e0d
            9a87 b933 6bed 117b ec8b 0b35 e227 32c4


[8]  ISAKMP Receive                           Aug  7 10:26:27 2002
       Cookies:(22f2b428fb243bba:5b504feebef8c495)
       Exchange Type: Quick               Len:156(0x9c)
       data=22f2 b428 fb24 3bba 5b50 4fee bef8 c495
            0810 2001 4730 70fb 0000 009c f14e ecb1
            938f 88aa bafe 127d dea8 0a24 5a45 2d47
            c50e 36dc f77e dccc 6d20 4395 c1f1 574d
            76c0 a67c 53e3 b7e8 9a6b 276a aea5 585d
            87f0 6db3 9a77 227c 8696 4105 296b 83e9
            e0fc f516 3ead f907 96a4 2910 c2a9 0ca7
            fa1e 92a5 ce82 3af0 16e0 9ee1 cea3 4f2d


[9]  ISAKMP Receive(After Decrypt)            Aug  7 10:26:27 2002
       Cookies:(22f2b428fb243bba:5b504feebef8c495)
       Exchange Type: Quick               Len:156(0x9c)
       data=22f2 b428 fb24 3bba 5b50 4fee bef8 c495
            0810 2001 4730 70fb 0000 009c 0100 0014
            d4d3 5742 a8e3 f18a 76c4 94f7 d080 e877
            0a00 0030 0000 0001 0000 0001 0000 0024
            0103 0401 0efd a61d 0000 0018 0102 0000
            8001 0001 8002 7080 8004 0001 8005 0001
            0500 0014 c538 a8b4 8271 1754 da9e 84c4
            fcb6 d999 0500 0010 0400 0000 0000 0000


[10]  ISAKMP Send(Before Encrypt)             Aug  7 10:26:27 2002
       Cookies:(22f2b428fb243bba:5b504feebef8c495)
       Exchange Type: Quick               Len:48(0x30)
       data=22f2 b428 fb24 3bba 5b50 4fee bef8 c495
            0810 2001 4730 70fb 0000 0030 0000 0014
            9b63 756e 00c2 1d9c e7f0 94ef b608 5817


[11]  ISAKMP Send                             Aug  7 10:26:27 2002
       Cookies:(22f2b428fb243bba:5b504feebef8c495)
       Exchange Type: Quick               Len:52(0x34)
       data=22f2 b428 fb24 3bba 5b50 4fee bef8 c495
            0810 2001 4730 70fb 0000 0034 6062 6bca
            2665 5bd9 f8d6 4f97 4245 3ea1 939d 0665
            1259 cdca
```

続き

1) ログ番号

   ログ番号が、1～30 の 10 進数で表示されます。

2) 送受信

   以下のどれかが表示されます。

   - ISAKMP Send

     送信フレーム

   - ISAKMP Receive

     受信フレーム

   - ISAKMP Send(Before Encrypt)

     暗号化前の送信フレーム

- ISAKMP Receive(After Decrypt)
  復号化後の受信フレーム

3) IKE トレース採取時間
   IKE トレース採取時間が表示されます。
4) Cookie
   Cookie を (Initiator 側 Cookie:Responder 側 Cookie) の形式で表示されます。
5) Exchange Type
   以下の Exchange Type が表示されます。

   - NONE
     交換なし
   - Base
     Base モード
   - Identity Protection
     Identity Protection モード
   - Authentication Only
     Authentication Only モード
   - Aggressive
     Aggressive モード
   - Informational
     Informational モード
   - Quick
     Quick モード
   - New group
     New group モード
   - Acknowledged Informational
     Acknowledged Informational モード

6) Len
   ISAKMP パケット長が表示されます。
7) data=
   送受信したパケットの内容が、16 進数で表示されます。最大 320 バイトまでが表示されます。

15.9　装置情報の表示

15.9.1　uptime

[機能]

システム起動時からの経過時間の表示

[入力形式]

uptime

[オプション]

なし

[パラメタ]

なし

[説明]

システム起動時からの経過時間を表示します。

[例]

以下に、表示例を示します。

```
# uptime
0000.01:20:22
#
```

15.9.2 idinfo

[機能]

ファームウェアのバージョン情報の表示

[入力形式]

idinfo [-c]

[オプション]

-c

動作中の構成定義番号もあわせて表示されます。

[パラメタ]

なし

[説明]

ファームウェアの製品情報を表示します。
製品名、MAC アドレス、ROM 版数、ファーム版数が、順番に表示されます。

[例]

以下に、表示例および表示内容を示します。

表示例 (MR1000 基本ソフトウェアの場合)

```
# idinfo
MR1000  --- (1)
00000ef16014-00000ef16017 --- (2)
ROM:3.2 --- (3)
FIRM:V21.00 --- (4)
```

1) 製品名
製品名が表示されます。

MR1000：
MR1000 基本ソフトウェア

2) MAC アドレス
MAC アドレスが 12 桁の 16 進数値で表示されます。

3) ROM 版数
ROM 版数が xx.yy の形式で出力されます。xx.yy は 10 進数値で表示されます。

4) ファーム版数
ファームウェア版数が Vxx.yy の形式で表示されます。
xx.yy は 2 桁の 10 進数値で表示されます。

表示例 (MR1000 基本ソフトウェアの場合)

```
# idinfo -c
TYPE    : MR1000                        ---(1)
SN      : 00000005                      ---(2)
MAC     : 00000ef16014-00000ef16017     ---(3)
ROM     : 3.2                           ---(4)
FIRM    : V21.00                        ---(5)
CURRENT : config1                       ---(6)
```

1) TYPE

製品名が表示されます。

MR1000 ：

MR1000 基本ソフトウェア

2) SN

本装置のシリアル番号が 8 桁の 10 進数値で表示されます。

3) MAC

MAC アド レスが 12 桁の 16 進数値で表示されます。

4) ROM

ROM 版数が xx.yy の形式で出力されます。xx.yy は 10 進数値で表示されます。

5) FIRM

ファームウェア版数が Vxx.yy の形式で表示されます。

xx.yy は 2 桁の 10 進数値で表示されます。

6) CURRENT

現在動作中の構成定義番号が表示されます。

15.9.3 sysinfo

[機能]

ハードウェアの状態の表示

[入力形式]

sysinfo

[オプション]

なし

[パラメタ]

なし

[説明]

ハードウェア状態を表示します。

[例]

表示例

```
# sysinfo
[Board information]
  Mother board  : MR1000     (Normal)                 --------- (1)

[Memory information]
  ECC single bit correction count: 0                  --------- (2)

[Hardware monitor information]
  Thermal       : 27 celsius (Normal)                 --------- (3)
```

1) 製品名を表示します。
() 内は、本装置の状態を表します。

(Normal) 正常状態

(Hard Error)

ハードエラー状態

2) 内蔵メモリの ECC(Error checking and correction) single bit 訂正回数

3) 装置内温度を表示します。
() 内は、温度状態を表します。

(Normal) 正常状態

(Warning)

温度異常検出

(Hard Error)

温度異常 (Warning 状態が、一定時間連続した場合)

15.10　その他の表示

15.10.1　help

[機能]

制御コマンド、表示コマンド の HELP 表示

[入力形式]

help [<command>]

[オプション]

なし

[パラメタ]

<command>

- コマンド 名

  制御コマンド 名、または表示コマンド 名を指定します。

  省略した場合は、使用可能なコマンド 一覧が表示されます。

[説明]

制御コマンド、表示コマンド のヘルプを表示します。

[例]

以下に、使用可能なコマンド 一覧を表示する場合の表示例を示します。

表示例

```
# help
*** control ***
  /logon        /exit         /reset        /save         /enable
  /delete       /open         /close        /connect      /disconnect
  /addlink      /dellink      /timerctl     /update       /ping
  /traceroute   /telnet       /date         /rdate        /rpon
  /clear        /dnconv       /ping6        /vrrpctl      /load
  /arp

*** display ***
  /uptime       /show         /more         /netstat      /dhcpstat
  /natstat      /lineis       /isdnstat     /frstat       /apstat
  /tempstat     /elog         /ppptrace     /pppoetrace   /dsplog
  /stlan        /stins        /stpiafs      /help         /history
  /bridgestat   /ipsecstat    /iketrace     /ikestat      /routestat
  /ldpstat      /mplsstat     /sysinfo      /filterstat   /vrrpstat
  /laninfo      /mcstat       /upnpstat     /diff         /idinfo
  /tech-support
```

15.10.2 tech-support

[機能]

解析情報の一括表示

[入力形式]

tech-support [-c <count>] [-i <time>]

[オプション]

-c <count>

統計情報の表示回数を 1～100 の 10 進数で指定します。
省略した場合は、2 回を指定したものとみなされます。

-i <time>

統計情報の表示間隔を 0～3600 の 10 進数 (単位:秒) で指定します。
省略した場合は、1 秒を指定したものとみなされます。

[パラメタ]

なし。

[説明]

本装置の設定情報や各種ステータスなど解析に必要な情報が一括で表示されます。ターミナルソフトウェアの出力キャプチャ機能を使用して、本コマンド実行時の出力内容を保存してください。

[注意]

画面単位表示モード (page on を設定した状態)、または more コマンドを使用して本コマンドの出力を画面単位に表示することはできません。

第 16 章　シェル関連コマンド

16.1 env

[機能]

環境変数の表示/設定/削除

[入力形式]

env (表示)
env <name>=<value> (設定)
env -u <name> (削除)

[オプション]

-u

環境変数を削除する場合に指定します。

[パラメタ]

<name>

環境変数名を指定します。

<value>

環境変数値を指定します。

[説明]

環境変数を表示、設定、または削除します。
環境変数名と環境変数値の説明を以下に示します。

- PROMPT

  プロンプト文字列を指定します。

  文字列に空白が含まれる場合は、ダブルクォーテーション (") で囲みます。また、プロンプト文字列中にバックスラッシュで始まる特殊文字を含めると、以下のように展開した文字列に置き換わります。

特殊文字	展開文字列
\!	履歴番号
\p	標準プロンプト文字列(空白文字含む)
\$	標準プロンプト文字(1文字)
\c	構成定義番号が2の場合は「config2」
\C	構成定義番号
\u	環境変数USERの値(ログオン前は無効)
\U	環境変数USERの値(ログオン前も有効)
\h	環境変数HOSTNAMEまたはsysnameの値(.の手前まで)
\H	環境変数HOSTNAMEまたはsysnameの値(すべて)
\d	日付(月/日 形式)
\t	時刻(時:分:秒 形式、24時間制)
\T	時刻(時:分:秒 形式、12時間制)
\@	時刻(時:分NN 形式、12時間制、NN:amかpm)
\\	バックスラッシュ(\)1個

  以下に、標準プロンプトを示します。

状　態	標準プロンプト
シリアルコンソール ログオン前	>
シリアルコンソール ログオン後	#
telnet ログオン後	#

特殊文字 (\p, \$, \U を除く) は、ログオン前には表示されません。
特殊文字が表示されない場合、それに続く空白一つも表示されません。
環境変数 USER がない場合、"\u"および"\U"とそれに続く空白 1 つが表示されません。
環境変数 HOSTNAME および sysname がない場合、"\h"および"\H"とその直前の"@"またはそれに続く空白 1 つが表示されません。
以下に、設定例を示します。

```
env PROMPT="\u@\h \! \p"
```

- PROMPT0
  ログオンする前のプロンプト文字列を指定します。
  指定する文字列は、環境変数 PROMPT と同じです。
  本環境変数がない場合、環境変数 PROMPT と同じ文字列を指定したものとみなされます。
- COLUMNS
  画面桁数を 10 進数値で指定します。1 以上を指定した場合に、設定が有効になります。
  実際の画面の桁数と異なる値を指定すると、コマンド入力時や画面単位表示時に表示やカーソル位置が乱れます。また、80 桁以下の場合、画面単位表示時に表示が乱れることがあります。
  なお、telnet でログインしている場合、画面サイズを通知する telnet クライアントを使用している場合には、通知された桁数に従って表示するため、本環境変数を設定する必要はありません。本環境変数を設定した場合、設定直後は設定値に従いますが、画面サイズを変更したりログインしなおした場合には、再び telnet クライアントから通知された値に従って表示します。画面サイズを通知しない telnet クライアントを使用している場合には、本環境変数を設定する必要があります。
- LINES
  画面行数を 10 進数値で指定します。1 以上を指定した場合に、設定が有効となります。
  実際の画面の行数と異なる値を指定すると、コマンド入力時や画面単位表示時に表示やカーソル位置が乱れます。また、13 行以下の場合、コマンド入力時に画面行数以上の入力を行うと表示が乱れ、3 行以下の場合、画面単位表示時に表示が乱れます。
  なお、telnet でログインしている場合、画面サイズを通知する telnet クライアントを使用している場合には、通知された行数に従って表示するため、本環境変数を設定する必要はありません。本環境変数を設定した場合、設定直後は設定値に従いますが、画面サイズを変更したりログインしなおした場合には、再び telnet クライアントから通知された値に従って表示します。画面サイズを通知しない telnet クライアントを使用している場合には、本環境変数を設定する必要があります。
- KANJI
  漢字コードを指定します。コマンド引数補完時の引数説明が指定した漢字コードで表示されます。
  環境変数値と漢字コードの対応を以下に示します。

環境変数値	漢字コード
SJIS	ShiftJIS
EUC	EUC
その他/なし	EUC

- USER
  ユーザ名を文字列で指定します。環境変数 PROMPT の"\u"や"\U"で使用されます。
- HOSTNAME
  ホスト名を文字列で指定します。環境変数 PROMPT の"\h"や"\H"で使用されます。

- TIMESTAMP
  コマンドを実行する際にコマンド実行日時を表示するかどうかを指定します。
  コマンド実行日時を表示するようにした場合、以下の形式で日時を表示してからコマンドを実行します。
  ― 曜日 月 日 時:分:秒 年 ―
  または
  ― 曜日 月 日 時:分:秒 タイムゾーン 年 ―
  環境変数値とコマンド実行日時表示動作の対応を以下に示します。

環境変数値	動　作
yes on その他/なし	表示する 表示する 表示しない

- NOBELL
  シェルは、以下の場合にベルを鳴らします。
  - 最大文字数 (1022 文字) を超えて入力しようとした場合
  - 最大文字数 (1022 文字) を超える貼付けを行った場合
  - 補完候補がない場合

  以下の値によってベルの動作を指定できます。

環境変数値	動　作
yes on その他/なし	鳴らさない 鳴らさない 鳴らす

- HISTSIZE
  履歴行数を 0～100 の 10 進数値で指定します。100 以上を指定しても、100 を指定したものとみなされます。0 を指定すると、履歴を残しません。
  行数を変更した場合、履歴番号や履歴内容は引き継がれますが、0 から増やした場合には履歴番号が 1 からになります。
  削除したり無効な値を指定すると、前の履歴行数のままとなります。
- SAVEENV
  環境変数は、“14.1.3 save” で構成定義情報と共に保存できます。環境変数 SAVEENV では、save コマンドで環境変数も保存するかどうかを指定します。

環境変数値	動　作
no off その他/なし	保存しない 保存しない 保存する

[注意]

環境変数を保存する場合、上記以外の環境変数はできるだけ設定しないでください。
PROMPT に空となるような文字列を指定すると、プロンプトが表示されず、入力できない状態のように見えますが、入力してコマンド実行することができます。
ユーザパスワードでログオンしている場合、exit したときに本コマンドで設定した内容は破棄されます。

[未設定時]

以下に示すように環境変数が設定されているものとみなされます。

```
env PROMPT="\u\c\p"
env -u PROMPT0
env COLUMNS=80
env LINES=24
env KANJI=EUC
env -u USER
env -u HOSTNAME
env TIMESTAMP=no
env NOBELL=no
env HISTSIZE=24
env SAVEENV=yes
```

16.2 history

[機能]

コマンド履歴の表示/消去

[入力形式]

history [-t] (表示)
history clear (消去)

[オプション]

-t

- 時刻表示
  履歴表示時に各履歴の先頭にコマンドを実行した時刻を表示します。

[パラメタ]

なし

- 履歴表示
  全履歴を表示します。

clear

- 履歴削除
  全履歴を消去します。

[説明]

コマンド履歴を表示または削除します。
履歴を表示すると、履歴番号と履歴内容が一覧表示されます。履歴を編集中で実行していない行には、履歴番号のあとに"*"が表示されます。"*"が表示されている場合は、以下のどれかの方法で"*"を消すことができます。

- Ctrl+P キーまたは↑キーでその行を表示し、改行キーを押してコマンドを実行する。
- Ctrl+P キーまたは↑キーでその行を表示し、Ctrl+C を押して入力内容を破棄する。
- Ctrl+P キーまたは↑キーでその行を表示し、Ctrl+U を押して空行にして他の履歴に移動する。

履歴を消去すると、履歴番号は 1 からふり直されます。
履歴行数は、環境変数 HISTSIZE で変更できます。環境変数については、env を参照してください。

[注意]

履歴番号が 32767 を超えると、適当な小さい履歴番号にふり直されます。
ユーザパスワードでログインしている場合、管理者が実行したコマンドは表示されず、履歴番号は非連続になります。

第 17 章　enable コマンド 実行時の影響について

　各構成定義コマンド で構成定義を変更後に enable コマンド を実行した時の影響について以下に示します。なお、各構成定義コマンド の変更／追加／削除のそれぞれについて、影響は同じです。

種別	コマンド名	enable実行時影響
WAN情報	wan	(3)
LAN情報	lan bind	(3)-1
	lan mode	(3)
	lan mdi	(3)
	lan mtu	(2)
	lan shaping	(2)
	lan backup	(3)
	lan recovery	(3)
	lan ip address	(2)
	lan ip alias	(2)
	lan ip dhcp service	(5)
	lan ip dhcp info	(1)
	lan ip proxyarp	(1)
	lan ip route	(1)
	lan ip rip use	(1)-1
	lan ip rip filter	(1)-1 ※1
	lan ip ospf use	(1)-1
	lan ip ospf cost	(1)
	lan ip ospf hello	(1)
	lan ip ospf dead	(1)
	lan ip ospf retrans	(1)
	lan ip ospf delay	(1)
	lan ip ospf priority	(1)
	lan ip ospf auth	(1)
	lan ip ospf passive	(1)
	lan ip vrf	(5) ※6
	lan ip nat	(1)
	lan ip filter	(1)
	lan ip tos	(1)
	lan ip priority	(1)
	lan ip icmp	(1)
	lan ip multicast	(1)
	lan ip arp	(3)
	lan ip6 use	(2)
	lan ip6 ifid	(2)
	lan ip6 address	(2)
	lan ip6 ra	(1)
	lan ip6 route	(1)
	lan ip6 rip use	(1)-1
	lan ip6 rip site-local	(1)-1 ※1
	lan ip6 rip aggregate	(1)-1 ※1
	lan ip6 rip filter	(1)-1 ※1
	lan bridge use	(3)
	lan bridge group	(1)
	lan bridge static	(1)
	lan bridge stp	(1)
	lan bridge filter	(1)
	lan vrrp use	(3)
	lan vrrp auth	(1)
	lan vrrp group id	(3)
	lan vrrp group ad	(1)
	lan vrrp group preempt	(1)
	lan vrrp group trigger	(1)
	lan mpls	(1)
	lan vlan bind	(2)-3
	lan vlan tag	(2)

相手情報	remote name	(2)
	remote autodial	(2)
	remote mtu	(2)
	remote shaping	(2)
	remote ap name	(2)
	remote ap move	(2)
	remote ap datalink	(3)
	remote ap ip	(2)
	remote ap multiroute	(2)
	remote ap limit	(2)
	remote ap ppp	(2)
	remote ap dial	(2)
	remote ap called	(2)
	remote ap idle	(2)
	remote ap step	(2)
	remote ap step2	(2)
	remote ap step3	(2)
	remote ap keep	(2)
	remote ap fr	(2)
	remote ap ipsec	(2)
	remote ap ike	(2)
	remote ap tunnel	(2)
	remote ap overlap	(2)
	remote ap sessionwatch	(1)
	remote ap mpls	(2)
	remote ppp	(2)
	remote ip address	(2)
	remote ip route	(1)
	remote ip rip use	(1)-1
	remote ip rip filter	(1)-1 ※1
	remote ip ospf use	(1)-1
	remote ip ospf cost	(1)
	remote ip ospf hello	(1)
	remote ip ospf dead	(1)
	remote ip ospf retrans	(1)
	remote ip ospf delay	(1)
	remote ip ospf auth	(1)
	remote ip ospf passive	(1)
	remote ip ospf multicast	(1)
	remote ip ospf checkmtu	(1)
	remote ip nat	(1)
	remote ip filter	(1)
	remote ip tos	(1)
	remote ip priority	(1)
	remote ip msschange	(1)
	remote ip multicast	(1)
	remote ip exp	(1)
	remote ip6 use	(2)
	remote ip6 ifid	(2)
	remote ip6 address	(2)
	remote ip6 ra	(1)
	remote ip6 route	(1)
	remote ip6 rip use	(1)-1
	remote ip6 rip site-local	(1)-1 ※1
	remote ip6 rip aggregate	(1)-1 ※1
	remote ip6 rip filter	(1)-1 ※1
	remote bridge use	(2)
	remote bridge group	(1)
	remote bridge static	(1)
	remote bridge stp use	(2)
	remote bridge stp cost	(1)
	remote bridge stp priority	(1)
	remote bridge filter	(1)
	remote mpls	(1)

SERIAL情報	serial	(3)
着信デフォルト情報	answer	(2)-2
テンプレート情報	template name	(6)
	template mtu	(7)
	template idle	(7)
	template interface pool	(8)
	template aaa	(6)
	template datalink bind	(6)
	template ppp	(7)
	template ip dns	(7)
	template ip address remote pool	(8)
	template ip filter	(1)
	template ip tos	(1)
	template ip priority	(1)
	template ip msschange	(1)
	template ip6 use	(7)
	template ip6 ifid	(7)
	template ip6 filter	(1)
	template ip6 priority	(1)
	template ip6 trafficclass	(1)
AAA情報	aaa	(1)
ルーティング プロトコル情報	routemanage ip distance	(5)
	routemanage ip redist rip	(1)
	routemanage ip redist bgp	(1)
	routemanage ip redist bgp vrf	(5) ※7
	routemanage ip redist ospf	(1)
	routemanage ip ecmp	(5)
	routemanage interface	(5)
	routemanage ip6 distance	(5)
	routemanage ip6 redist rip	(1)
	bgp as	(4)
	bgp id	(4)
	bgp vrf	(5) ※7
	bgp mpls-resolution	(5) ※7
	bgp network route	(1)
	bgp network igp	(1)-1 ※2
	bgp aggregate	(1)
	bgp redist	(1)
	bgp neighbor address	(1)-1 ※3
	bgp neighbor as	(1)-1 ※3
	bgp neighbor timers	(1)-1 ※3
	bgp neighbor medmetric	(1)-1 ※3
	bgp neighbor asprepend	(1)-1 ※3
	bgp neighbor localpref	(1)-1 ※3
	bgp neighbor nexthopself	(1)-1 ※3
	bgp neighbor ebgp-multihop	(1)-1 ※3
	bgp neighbor enforce-multihop	(5) ※7
	bgp neighbor default-originate	(1)-1 ※3
	bgp neighbor family	(5) ※7
	bgp neighbor source	(1)-1 ※3
	bgp neighbor filter	(1)-1 ※3
	ospf ip id	(4)
	ospf ip area id	(1)-1 ※4
	ospf ip area type	(1)-1 ※4
	ospf ip area defcost	(1)
	ospf ip area range	(1)-1
	ospf ip area type3-lsa	(1)
	ospf ip area vlink id	(1)-1 ※4
	ospf ip area vlink hello	(1)
	ospf ip area vlink dead	(1)
	ospf ip area vlink retrans	(1)
	ospf ip area vlink delay	(1)
	ospf ip area vlink auth	(1)
	ospf ip definfo	(1)
	ospf ip summary	(1)-1
	ospf ip redist	(1)-1

ルーティング プロトコル情報	rip ip timers rip ip multipath rip ip redist rip ip neighbor rip ip gwfilter rip ip6 timers rip ip6 multipath rip ip6 redist	(1) (1) (1)-1 (1)-1 (1)-1 (1) (1) (1)-1
ブリッジ情報	bridge age bridge stp bridge ip routing bridge ip policy bridge ip6 routing bridge ip6 policy bridge vlan bridge inter-remote	(1) (1) (2)-1 (1) (2)-1 (1) (1) (1)
MPLS情報	mpls	(1)
マルチキャスト情報	multicast	(1)
装置情報	snmp syslog time proxydns host password set schedule dncnvinfo updateinfo addact watchdog service consoleinfo telnetinfo sysdown page mflag sysname loopback ip address loopback ip ospf loopback mpls serverinfo	(1) (1) (1) (1) (1) (0) (1) (1) (1) (1) ※5 (1) (1) (1) (0) (1) (5) (5) (1)-1 (1) (1)
シェル関連コマンド	env	(0)

(0)　コマンドを実行すると、その直後から有効になります。

(1)　該当箇所の該当機能だけ停止／再開になります。

(1)-1　(1) に加え、該当経路の追加・削除が行われるため、本装置や隣接ルータにおいて経路変更が伴います。

(2)　該当論理インタフェースでの通信が中断されます。

(2)-1　(2) で該当論理インタフェースとはブリッジが有効で PPP で接続されているインタフェースです。

(2)-2　(2) で該当論理インタフェースとはすべての ISDN のインタフェースです。

(2)-3　通常は (2) ですが、IPv6 使用時は (5) になります。

(3)　該当物理回線が切断されます。

(3)-1　通常は (3) ですが、IPv6 使用時は (5) になります。

(4)　該当ルーティングプロトコルが再起動されます。

(5)　enable コマンドのパラメタに all が必要となります。この場合、全ての回線が切断され、すべてのルーティングプロトコルが再起動されます。

(6) 該当テンプレートで着信した接続が全て切断されます。

(7) 現在接続中の回線は設定変更前のままの定義で接続が保持されます。
設定変更後の新しい設定は定義変更後に着信した接続から有効になります。

(8) 設定範囲の先頭を変更した場合には該当テンプレートで着信した接続が全て切断されます。
設定範囲を縮小した場合には、該当テンプレートて着信した接続が全て切断されます。
設定範囲の先頭を変更しなかった場合で、設定範囲を拡大したときのみ接続が維持されます。

※ 1 設定以前の送受信経路に対しては適用されません。

※ 2 BGP ネットワークで設定されている経路が一時的に削除される場合があります。

※ 3 設定変更時、該当する BGP セッションが一時的に切断されます。

※ 4 設定変更時、該当するエリア全体の経路の変更を伴うため、その間通信に影響します。

※ 5 enable コマンドでは変更内容は反映されません。装置のリセットが必要です。

※ 6 本設定が行われている LAN インタフェースでは、IP アドレス設定など lan コマンドによる設定変更を行った場合に enable コマンドのパラメタに all が必要となります。

※ 7 本設定が行われている状態では、"routemanage ip redist bgp"または、bgp コマンドによる設定変更を行った場合に enable コマンドのパラメタに all が必要となります。

MR1000　コマンドリファレンス

発行日　　2005年1月

第1版　　K1N-D-04167A

発行責任　　オムロン株式会社

Printed in Japan