YAMAHA

ISDN

Network Equipment

コマンドリファレンス

Rev.6.03.34, Rev.7.00.30, Rev.7.01.53
Rev.8.01.27, Rev.8.02.43, Rev.8.03.76
Rev.9.00.37, Rev.10.00.38, Rev.10.01.01

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

※ イーサネットは富士ゼロックス株式会社の登録商標です。
※ Microsoft、Windows は米国 Microsoft 社の米国およびその他の国における登録商標です。
※ NetWare は米国 Novell,Inc. の登録商標です。
※ Stac LZS は米国 Hi/fn 社の登録商標です。
※ FOMA、mopera、mopera U は株式会社 NTT ドコモの登録商標です。
※ microSDHC ロゴは商標です。

目次

1. コマンドリファレンスの見方 28
1.1 対応するプログラムのリビジョン 28
1.2 コマンドリファレンスの見方 28
1.3 インタフェース名について 28
1.4 no で始まるコマンドの入力形式について 29
1.5 コマンドの入力文字数とエスケープシーケンスについて 29
1.6 相手先情報番号のモデルによる違いについて 29
1.7 工場出荷設定値について 29

2. コマンドの使い方 30
2.1 コンソールについて 30
2.1.1 コンソールによる設定手順 31
2.1.2 CONSOLE または SERIAL ポートからの設定 32
2.1.3 TELNET による設定 34
2.1.4 リモートセットアップ 35
2.2 SSH サーバーについて 36
2.2.1 使用に当たっての注意事項 36
2.2.2 SSH サーバーの設定 36
2.3 TFTP について 36
2.3.1 TFTP による設定手順 37
2.3.2 設定ファイルの読み出し 37
2.3.3 設定ファイルの書き込み 38
2.4 コンソール使用時のキーボード操作について 38
2.5 「show」で始まるコマンド 39
2.5.1 show コマンドの表示内容から検索パターンに一致する内容だけを抜き出す 39
2.5.2 show コマンドの表示内容を見やすくする 40
2.5.3 外部メモリへのリダイレクト機能 41

3. ヘルプ 42
3.1 コンソールに対する簡易説明の表示 42
3.2 コマンド一覧の表示 42

4. 機器の設定 43
4.1 ログインパスワードの設定 43
4.2 ログインパスワードの暗号化保存 43
4.3 管理パスワードの設定 43
4.4 管理パスワードの暗号化保存 43
4.5 ログインユーザ名とログインパスワードの設定 44
4.6 ユーザの属性を設定 44
4.7 他のユーザの接続の強制切断 46
4.8 セキュリティクラスの設定 46
4.9 タイムゾーンの設定 47
4.10 現在の日付けの設定 47
4.11 現在の時刻の設定 47
4.12 リモートホストによる時計の設定 47
4.13 NTP による時計の設定 47
4.14 コンソールのプロンプト表示の設定 48
4.15 コンソールの言語とコードの設定 48
4.16 コンソールの表示文字数の設定 48
4.17 コンソールの表示行数の設定 48
4.18 コンソールにシステムメッセージを表示するか否かの設定 49
4.19 SYSLOG を受けるホストの IP アドレスの設定 49
4.20 SYSLOG ファシリティの設定 49
4.21 NOTICE タイプの SYSLOG を出力するか否かの設定 49
4.22 INFO タイプの SYSLOG を出力するか否かの設定 50
4.23 DEBUG タイプの SYSLOG を出力するか否かの設定 50

4.24 SYSLOG を送信する時の始点 IP アドレスの設定 50
4.25 SYSLOG パケットの始点ポート番号の設定 50
4.26 SYSLOG に実行コマンドを出力するか否かの設定 51
4.27 電源の設定 51
4.28 TELNET サーバー機能の ON/OFF の設定 51
4.29 TELNET サーバー機能の listen ポートの設定 51
4.30 TELNET サーバーへアクセスできるホストの IP アドレスの設定 52
4.31 TELNET サーバーへ同時に接続できるユーザ数の設定 52
4.32 マスタクロック用インタフェースの設定 52
4.33 温度監視の閾値の設定 53
4.34 ファストパス機能の設定 53
4.35 LAN インタフェースの動作設定 53
4.36 ポートミラーリング機能の設定 53
4.37 LAN インタフェースの動作タイプの設定 54
4.38 LAN インタフェースの受信パケットバッファサイズの設定 57
4.39 ログインタイマの設定 57
4.40 TFTP によりアクセスできるホストの IP アドレスの設定 57
4.41 Magic Packet を LAN に中継するか否かの設定 58
4.42 インタフェースまたはシステムの説明の設定 58
4.43 TCP のコネクションレベルの syslog を出力するか否かの設定 59
4.44 HTTP リビジョンアップ実行を許可するか否かの設定 60
4.45 HTTP リビジョンアップ用 URL の設定 60
4.46 HTTP リビジョンアップ用 Proxy サーバーの設定 60
4.47 HTTP リビジョンアップ処理のタイムアウトの設定 61
4.48 リビジョンダウンを許可するか否かの設定 61
4.49 DOWNLOAD ボタンによるリビジョンアップ操作を許可するか否かの設定 61
4.50 SSH サーバー機能の ON/OFF の設定 61
4.51 SSH サーバー機能の listen ポートの設定 62
4.52 SSH サーバーへアクセスできるホストの IP アドレスの設定 62
4.53 SSH サーバーへ同時に接続できるユーザ数の設定 62
4.54 SSH サーバー ホスト鍵の設定 62
4.55 SSH クライアントの生存確認 63
4.56 パケットバッファのパラメータの変更 63
4.57 有効になっているアラーム音を鳴らすか全く鳴らさないかの設定 64
4.58 USB ホスト機能に関連するアラーム音を鳴らすか否かの設定 64
4.59 microSD 機能に関連するアラームを鳴らすか否かの設定 65
4.60 起動時のアラーム音を鳴らすか否かの設定 65
4.61 HTTP リビジョンアップ機能に関連するアラームを鳴らすか否かの設定 65
4.62 LED の輝度を調整する 65

5. ISDN 関連の設定 66

5.1 共通の設定 66
5.1.1 BRI 回線の種類の指定 66
5.1.2 自分の ISDN 番号の設定 66
5.1.3 内蔵 DSU 使用の可否の設定 67
5.1.4 終端抵抗の設定 67
5.1.5 PP で使用するインタフェースの設定 67
5.1.6 課金額による発信制限の設定 68
5.1.7 PIAFS の着信を許可するか否かの設定 68
5.1.8 PIAFS 接続時の起動側の指定 69
5.1.9 PIAFS の発信方式の設定 69
5.1.10 専用線がダウンした時にバックアップする相手先情報番号の設定 69
5.2 相手側の設定 70
5.2.1 常時接続の設定 70
5.2.2 相手 ISDN 番号の設定 70
5.2.3 自動接続の設定 70
5.2.4 相手への発信順序の設定 71
5.2.5 着信許可の設定 71
5.2.6 発信許可の設定 71

5.2.7 再発信抑制タイマの設定 . . . 72
5.2.8 エラー切断後の再発信禁止タイマの設定 . . . 72
5.2.9 相手にコールバック要求を行うか否かの設定 . . . 72
5.2.10 相手からのコールバック要求に応じるか否かの設定 . . . 72
5.2.11 コールバック要求タイプの設定 . . . 73
5.2.12 コールバック受け入れタイプの設定 . . . 73
5.2.13 MS コールバックでユーザからの番号指定を許可するか否かの設定 . . . 73
5.2.14 コールバックタイマの設定 . . . 73
5.2.15 コールバック待機タイマの設定 . . . 74
5.2.16 ISDN 回線を切断するタイマ方式の指定 . . . 74
5.2.17 切断タイマの設定 (ノーマル) . . . 74
5.2.18 切断タイマの設定 (ファスト) . . . 75
5.2.19 切断タイマの設定 (強制) . . . 75
5.2.20 入力切断タイマの設定 (ノーマル) . . . 75
5.2.21 出力切断タイマの設定 (ノーマル) . . . 76
5.2.22 課金単位時間方式での課金単位時間と監視時間の設定 . . . 76

6. フレームリレー関連の設定 . . . 77
6.1 カプセル化の種類の設定 . . . 77
6.2 DLCI の設定 . . . 78
6.3 DLCI ごとのパラメータの設定 . . . 78
6.4 PVC 状態確認手順の設定 . . . 78
6.5 InARP 使用の設定 . . . 79
6.6 フレームリレーダウン時にバックアップする相手先情報番号の設定 . . . 79
6.7 FR 圧縮機能の設定 . . . 79
6.8 輻輳制御をするか否かの設定 . . . 80
6.9 回線に対する送信順序方式の設定 . . . 80
6.10 指定パケットに DE ビットを立てるか否かの設定 . . . 80

7. PRI 関連の設定 . . . 81
7.1 PRI 回線の種類の設定 . . . 82
7.2 情報チャネルとタイムスロットの設定 . . . 82
7.3 PP で使用するインタフェースの設定 . . . 82

8. IP の設定 . . . 83
8.1 インタフェース共通の設定 . . . 83
8.1.1 IP パケットを扱うか否かの設定 . . . 83
8.1.2 IP アドレスの設定 . . . 83
8.1.3 セカンダリ IP アドレスの設定 . . . 84
8.1.4 インタフェースの MTU の設定 . . . 84
8.1.5 echo, discard, time サービスを動作させるか否かの設定 . . . 84
8.1.6 IP の静的経路情報の設定 . . . 85
8.1.7 IP パケットのフィルタの設定 . . . 86
8.1.8 フィルタセットの定義 . . . 88
8.1.9 Source-route オプション付き IP パケットをフィルタアウトするか否かの設定 . . . 88
8.1.10 ディレクテッドブロードキャストパケットをフィルタアウトするか否かの設定 . . . 88
8.1.11 動的フィルタの定義 . . . 88
8.1.12 動的フィルタのタイムアウトの設定 . . . 89
8.1.13 侵入検知機能の動作の設定 . . . 90
8.1.14 1 秒間に侵入検知情報を通知する頻度の設定 . . . 90
8.1.15 重複する侵入検知情報の通知抑制の設定 . . . 91
8.1.16 侵入検知情報の最大表示件数の設定 . . . 91
8.1.17 侵入検知で用いる閾値の設定 . . . 91
8.1.18 TCP セッションの MSS 制限の設定 . . . 92
8.1.19 IPv4 の経路情報に変化があった時にログに記録するか否かの設定 . . . 92
8.1.20 フィルタリングによるセキュリティの設定 . . . 93
8.1.21 フィルタに一致する IP パケットの DF ビットを 0 に書き換えるか否かの設定 . . . 94
8.1.22 IP パケットの TOS フィールドの書き換えの設定 . . . 94
8.1.23 代理 ARP の設定 . . . 94

8.1.24 ARP エントリの寿命の設定 . . . 95
8.1.25 静的 ARP エントリの設定 . . . 95
8.1.26 ARP が解決されるまでの間に送信を保留しておくパケットの数を制御する . . . 95
8.2 PP 側の設定 . . . 96
8.2.1 PP 側 IP アドレスの設定 . . . 96
8.2.2 リモート IP アドレスプールの設定 . . . 96
8.2.3 PP 経由のキープアライブの時間間隔の設定 . . . 97
8.2.4 PP 経由のキープアライブを使用するか否かの設定 . . . 97
8.2.5 PP 経由のキープアライブのログをとるか否かの設定 . . . 98
8.2.6 専用線ダウン検出時の動作の設定 . . . 98
8.3 RIP の設定 . . . 98
8.3.1 RIP を使用するか否かの設定 . . . 98
8.3.2 RIP に関して信用できるゲートウェイの設定 . . . 99
8.3.3 RIP による経路の優先度の設定 . . . 99
8.3.4 RIP パケットの送信に関する設定 . . . 99
8.3.5 RIP パケットの受信に関する設定 . . . 100
8.3.6 RIP のフィルタリングの設定 . . . 100
8.3.7 RIP で加算するホップ数の設定 . . . 100
8.3.8 RIP2 での認証の設定 . . . 101
8.3.9 RIP2 での認証キーの設定 . . . 101
8.3.10 回線切断時の経路保持の設定 . . . 101
8.3.11 回線接続時の PP 側の RIP の動作の設定 . . . 102
8.3.12 回線接続時の PP 側の RIP 送出の時間間隔の設定 . . . 102
8.3.13 回線切断時の PP 側の RIP の動作の設定 . . . 102
8.3.14 回線切断時の PP 側の RIP 送出の時間間隔の設定 . . . 102
8.3.15 バックアップ時の RIP の送信元インタフェース切り替えの設定 . . . 103
8.3.16 RIP で強制的に経路を広告する . . . 103
8.3.17 RIP2 でのフィルタの比較方法 . . . 104
8.3.18 RIP のタイマーを調整する . . . 104
8.4 VRRP の設定 . . . 105
8.4.1 インタフェース毎の VRRP の設定 . . . 105
8.4.2 シャットダウントリガの設定 . . . 105
8.5 バックアップの設定 . . . 106
8.5.1 プロバイダ接続がダウンした時に PP バックアップする接続先の指定 . . . 106
8.5.2 バックアップからの復帰待ち時間の設定 . . . 106
8.5.3 LAN 経由でのプロバイダ接続がダウンした時にバックアップする接続先の指定 . . . 107
8.5.4 バックアップからの復帰待ち時間の設定 . . . 107
8.5.5 LAN 経由のキープアライブを使用するか否かの設定 . . . 107
8.5.6 LAN 経由のキープアライブの時間間隔の設定 . . . 108
8.5.7 LAN 経由のキープアライブのログをとるか否かの設定 . . . 108
8.5.8 ネットワーク監視機能の設定 . . . 109
8.6 IGMP の設定 . . . 110
8.6.1 インタフェースごとの IGMP の設定 . . . 110
8.6.2 静的な IGMP の設定 . . . 110
8.7 PIM-SM の設定 . . . 111
8.7.1 インタフェースごとの PIM-SM の設定 . . . 111
8.7.2 静的な RP のグループの設定 . . . 111
8.7.3 PIM-SM に関する詳細なログ出力の設定 . . . 112
8.7.4 register の checksum 計算方法の設定 . . . 112
8.7.5 PIM JOIN/PRUNE メッセージの宛先の設定 . . . 112
8.7.6 PIM の Join(*,G) メッセージ送信時に Periodic Prune メッセージを含ませるかどうかの設定 . . . 112
8.7.7 implicit 経路の優先度の設定 . . . 113
8.7.8 フローテーブルの各エントリの寿命を設定する . . . 113
8.8 受信パケット統計情報の設定 . . . 114
8.8.1 受信パケットの統計情報を記録するか否かの設定 . . . 114
8.8.2 受信したパケットの統計情報のクリア . . . 114
8.8.3 受信したパケットの統計情報の表示 . . . 115
8.8.4 統計情報を記録する受信パケットの分類数の設定 . . . 115

8.9 パケット転送フィルターの設定 . . . 116
8.9.1 パケット転送フィルターの定義 . . . 116
8.9.2 インタフェースへのパケット転送フィルターの適用 . . . 116

9. IPX の設定 . . . 117
9.1 インタフェース共通の設定 . . . 117
9.1.1 IPX パケットを扱うか否かの設定 . . . 117
9.1.2 静的な SAP テーブルの設定 . . . 117
9.1.3 IPX SAP Get Nearest Server Request に応答するか否かの設定 . . . 117
9.1.4 IPX パケットのフィルタの設定 . . . 118
9.2 LAN 側の設定 . . . 119
9.2.1 イーサネットフレームタイプの設定 . . . 119
9.2.2 LAN 側の IPX ネットワーク番号の設定 . . . 119
9.2.3 LAN 側でのフィルタリングによるセキュリティの設定 . . . 119
9.2.4 LAN 側の RIP/SAP ブロードキャストの設定 . . . 120
9.2.5 経路情報の追加 . . . 120
9.3 PP 側相手毎の IPX の設定 . . . 120
9.3.1 IPX ルーティング許可の設定 . . . 120
9.3.2 PP 側 IPX ネットワーク番号の設定 . . . 120
9.3.3 経路情報の追加 . . . 121
9.3.4 IPXWAN 使用の設定 . . . 121
9.3.5 IPXWAN プライマリネットワーク番号の設定 . . . 121
9.3.6 回線接続時の PP 側の RIP/SAP の動作の設定 . . . 121
9.3.7 回線接続時の PP 側の RIP/SAP 送出の時間間隔の設定 . . . 122
9.3.8 回線切断時の PP 側の RIP/SAP の動作の設定 . . . 122
9.3.9 回線切断時の PP 側の RIP/SAP 送出の時間間隔の設定 . . . 122
9.3.10 回線切断時に RIP/SAP 情報を保持するか否かの設定 . . . 122
9.3.11 Timer/Information Request の再送間隔と最大再送回数の設定 . . . 123
9.3.12 Watchdog パケットに対する代理応答の設定 . . . 123
9.3.13 Watchdog 代理応答の時間間隔の設定 . . . 123
9.3.14 SPX キープアライブ代理応答のタイマの設定 . . . 123
9.3.15 SPX キープアライブ代理応答を行うか否かの設定 . . . 124
9.3.16 IPX シリアライゼーションパケットをフィルタアウトするか否かの設定 . . . 124
9.3.17 PP 側でのフィルタリングによるセキュリティの設定 . . . 124

10. ブリッジの設定 . . . 125
10.1 インタフェース共通の設定 . . . 125
10.1.1 ブリッジ使用許可の設定 . . . 125
10.1.2 ブリッジするインタフェースの設定 . . . 125
10.1.3 MAC アドレスのラーニングを行うか否かの設定 . . . 125
10.1.4 ラーニング情報消去タイマの設定 . . . 126
10.1.5 ブリッジのフィルタの設定 . . . 126
10.2 LAN 側の設定 . . . 126
10.2.1 静的なラーニング情報の設定 . . . 126
10.2.2 LAN 側でのブリッジのフィルタリングの設定 . . . 127
10.3 PP 側相手毎のブリッジの設定 . . . 127
10.3.1 ラーニング情報の設定 . . . 127
10.3.2 PP 側でのブリッジのフィルタリングの設定 . . . 127

11. イーサネットフィルタの設定 . . . 128
11.1 フィルタ定義の設定 . . . 128
11.2 インタフェースへの適用の設定 . . . 129

12. 入力遮断フィルタの設定 . . . 130
12.1 フィルタ定義の設定 . . . 130
12.2 適用の設定 . . . 131

13. ポリシーフィルタの設定 . . . 132
13.1 サービスの定義 . . . 132
13.2 インタフェースグループの定義 . . . 132

13.3 アドレスグループの定義 133
13.4 サービスグループの定義 133
13.5 ポリシーフィルタの定義 134
13.6 ポリシーセットの定義 135
13.7 ポリシーセットの有効化 135
13.8 ポリシーセットの自動切り替え 136
13.9 タイマーの設定 137

14. URL フィルタの設定 138
14.1 フィルタ定義の設定 138
14.2 URL フィルタのインタフェースへの適用 138
14.3 URL フィルタでチェックを行う HTTP のポート番号の設定 139
14.4 URL フィルターを使用するか否かの設定 139
14.5 URL フィルタで破棄するパケットの送信元に HTTP レスポンスを返す動作の設定 139
14.6 フィルタにマッチした際にログを出力するか否かの設定 140

15. PPP の設定 141
15.1 相手の名前とパスワードの設定 141
15.2 受け入れる認証タイプの設定 141
15.3 要求する認証タイプの設定 142
15.4 自分の名前とパスワードの設定 142
15.5 同一 username を持つ相手からの二重接続を禁止するか否かの設定 142
15.6 LCP 関連の設定 143
15.6.1 Address and Control Field Compression オプション使用の設定 143
15.6.2 Magic Number オプション使用の設定 143
15.6.3 Maximum Receive Unit オプション使用の設定 143
15.6.4 Protocol Field Compression オプション使用の設定 144
15.6.5 lcp-restart パラメータの設定 144
15.6.6 lcp-max-terminate パラメータの設定 144
15.6.7 lcp-max-configure パラメータの設定 144
15.6.8 lcp-max-failure パラメータの設定 144
15.6.9 Configure-Request をすぐに送信するか否かの設定 145
15.7 PAP 関連の設定 145
15.7.1 pap-restart パラメータの設定 145
15.7.2 pap-max-authreq パラメータの設定 145
15.8 CHAP 関連の設定 145
15.8.1 chap-restart パラメータの設定 145
15.8.2 chap-max-challenge パラメータの設定 145
15.9 IPCP 関連の設定 146
15.9.1 Van Jacobson Compressed TCP/IP 使用の設定 146
15.9.2 PP 側 IP アドレスのネゴシエーションの設定 146
15.9.3 ipcp-restart パラメータの設定 146
15.9.4 ipcp-max-terminate パラメータの設定 146
15.9.5 ipcp-max-configure パラメータの設定 147
15.9.6 ipcp-max-failure パラメータの設定 147
15.9.7 WINS サーバーの IP アドレスの設定 147
15.9.8 IPCP の MS 拡張オプションを使うか否かの設定 147
15.9.9 ホスト経路が存在する相手側 IP アドレスを受け入れるか否かの設定 148
15.10 IPXCP 関連の設定 148
15.10.1 ipxcp-restart パラメータの設定 148
15.10.2 ipxcp-max-terminate パラメータの設定 148
15.10.3 ipxcp-max-configure パラメータの設定 148
15.10.4 ipxcp-max-failure パラメータの設定 148
15.11 BCP 関連の設定 149
15.11.1 LAN Identification 使用の設定 149
15.11.2 Tinygram compression 使用の設定 149
15.11.3 bcp-restart パラメータの設定 149
15.11.4 bcp-max-terminate パラメータの設定 149
15.11.5 bcp-max-configure パラメータの設定 149
15.11.6 bcp-max-failure パラメータの設定 150

15.12 MSCBCP関連の設定 . . . 150
15.12.1 mscbcp-restart パラメータの設定 . . . 150
15.12.2 mscbcp-maxretry パラメータの設定 . . . 150
15.13 CCP関連の設定 . . . 151
15.13.1 全パケットの圧縮タイプの設定 . . . 151
15.13.2 ccp-restart パラメータの設定 . . . 151
15.13.3 ccp-max-terminate パラメータの設定 . . . 151
15.13.4 ccp-max-configure パラメータの設定 . . . 152
15.13.5 ccp-max-failure パラメータの設定 . . . 152
15.14 IPV6CP関連の設定 . . . 152
15.14.1 IPV6CP を使用するか否かの設定 . . . 152
15.15 MP関連の設定 . . . 152
15.15.1 MP を使用するか否かの設定 . . . 152
15.15.2 MP の制御方法の設定 . . . 153
15.15.3 MP のための負荷閾値の設定 . . . 153
15.15.4 MP の最大リンク数の設定 . . . 153
15.15.5 MP の最小リンク数の設定 . . . 153
15.15.6 MP のための負荷計測間隔の設定 . . . 154
15.15.7 MP のパケットを分割するか否かの設定 . . . 154
15.16 BACP関連の設定 . . . 154
15.16.1 bacp-restart パラメータの設定 . . . 154
15.16.2 bacp-max-terminate パラメータの設定 . . . 154
15.16.3 bacp-max-configure パラメータの設定 . . . 155
15.16.4 bacp-max-failure パラメータの設定 . . . 155
15.17 BAP関連の設定 . . . 155
15.17.1 bap-restart パラメータの設定 . . . 155
15.17.2 bap-max-retry パラメータの設定 . . . 155
15.18 PPPoE関連の設定 . . . 155
15.18.1 PPPoE で使用する LAN インタフェースの指定 . . . 155
15.18.2 アクセスコンセントレータ名の設定 . . . 156
15.18.3 セッションの自動接続の設定 . . . 156
15.18.4 セッションの自動切断の設定 . . . 156
15.18.5 PADI パケットの最大再送回数の設定 . . . 156
15.18.6 PADI パケットの再送時間の設定 . . . 156
15.18.7 PADR パケットの最大再送回数の設定 . . . 157
15.18.8 PADR パケットの再送時間の設定 . . . 157
15.18.9 PPPoE セッションの切断タイマの設定 . . . 157
15.18.10サービス名の指定 . . . 157
15.18.11TCP パケットの MSS の制限の有無とサイズの指定 . . . 158
15.18.12ルーター側には存在しない PPPoE セッションを強制的に切断するか否かの設定 . . . 158

16. DHCPの設定 . . . 159
16.1 DHCPサーバー・リレーエージェント機能 . . . 159
16.1.1 DHCP の動作の設定 . . . 159
16.1.2 RFC2131 対応動作の設定 . . . 160
16.1.3 リースする IP アドレスの重複をチェックするか否かの設定 . . . 160
16.1.4 DHCP スコープの定義 . . . 161
16.1.5 DHCP 予約アドレスの設定 . . . 161
16.1.6 DHCP アドレス割り当て動作の設定 . . . 163
16.1.7 DHCP 割り当て情報を元にした予約設定の生成 . . . 164
16.1.8 DHCP オプションの設定 . . . 165
16.1.9 DHCP リース情報の手動追加 . . . 165
16.1.10 DHCP リース情報の手動削除 . . . 166
16.1.11 DHCP サーバーの指定の設定 . . . 166
16.1.12 DHCP サーバーの選択方法の設定 . . . 166
16.1.13 DHCP BOOTREQUESTパケットの中継基準の設定 . . . 166
16.2 DHCPクライアント機能 . . . 167
16.2.1 DHCP クライアントのホスト名の設定 . . . 167
16.2.2 DNS サーバーアドレスを取得する LAN インタフェースの設定 . . . 167
16.2.3 要求する IP アドレスリース期間の設定 . . . 168

16.2.4 IP アドレス取得要求の再送回数と間隔の設定 168
16.2.5 DHCP クライアント ID オプションの設定 168
16.2.6 DHCP クライアントが DHCP サーバーへ送るメッセージ中に格納するオプションの設定 169

17. ICMP の設定 170
17.1 IPv4 の設定 170
17.1.1 ICMP Echo Reply を送信するか否かの設定 170
17.1.2 ICMP Echo Reply をリンクダウン時に送信するか否かの設定 170
17.1.3 ICMP Mask Reply を送信するか否かの設定 170
17.1.4 ICMP Parameter Problem を送信するか否かの設定 170
17.1.5 ICMP Redirect を送信するか否かの設定 171
17.1.6 ICMP Redirect 受信時の処理の設定 171
17.1.7 ICMP Time Exceeded を送信するか否かの設定 171
17.1.8 ICMP Timestamp Reply を送信するか否かの設定 171
17.1.9 ICMP Destination Unreachable を送信するか否かの設定 172
17.1.10 IPsec で復号したパケットに対して ICMP エラーを送るか否かの設定 172
17.1.11 受信した ICMP のログを記録するか否かの設定 172
17.1.12 ステルス機能の設定 172
17.1.13 ARP による MTU 探索を行うか否かの設定 173
17.1.14 切り詰められたパケットに対して、ICMP Destination Unreachable を送信するか否かの設定 173
17.2 IPv6 の設定 174
17.2.1 ICMP Echo Reply を送信するか否かの設定 174
17.2.2 ICMP Echo Reply をリンクダウン時に送信するか否かの設定 174
17.2.3 ICMP Parameter Problem を送信するか否かの設定 174
17.2.4 ICMP Redirect を送信するか否かの設定 174
17.2.5 ICMP Redirect 受信時の処理の設定 175
17.2.6 ICMP Time Exceeded を送信するか否かの設定 175
17.2.7 ICMP Destination Unreachable を送信するか否かの設定 175
17.2.8 受信した ICMP のログを記録するか否かの設定 175
17.2.9 ICMP Packet-Too-Big を送信するか否かの設定 176
17.2.10 IPsec で復号したパケットに対して ICMP エラーを送るか否かの設定 176
17.2.11 ステルス機能の設定 176
17.2.12 サイズエラーで切り詰められたフレームに対して、ICMP エラー (Packet Too Big) を送信するか否かの設定 177

18. トンネリング 178
18.1 トンネルインタフェースの使用許可の設定 178
18.2 トンネルインタフェースの使用不許可の設定 178
18.3 トンネルインタフェースの種別の設定 178
18.4 トンネルインタフェースの IPv4 アドレスの設定 178
18.5 トンネルインタフェースの相手側の IPv4 アドレスの設定 179
18.6 トンネルインタフェースの端点 IP アドレスの設定 179

19. IPsec の設定 180
19.1 IPsec の動作の設定 181
19.2 事前共有鍵の登録 181
19.3 IKE の鍵交換を始動するか否かの設定 181
19.4 設定が異なる場合に鍵交換を拒否するか否かの設定 182
19.5 IKE の鍵交換に失敗したときに鍵交換を休止せずに継続するか否かの設定 182
19.6 鍵交換の再送回数と間隔の設定 183
19.7 相手側のセキュリティ・ゲートウェイの名前の設定 183
19.8 相手側セキュリティ・ゲートウェイの IP アドレスの設定 183
19.9 相手側の ID の設定 184
19.10 自分側のセキュリティ・ゲートウェイの名前の設定 184
19.11 自分側セキュリティ・ゲートウェイの IP アドレスの設定 184
19.12 自分側の ID の設定 185
19.13 IKE キープアライブ機能の設定 185
19.14 IKE キープアライブに関する SYSLOG を出力するか否かの設定 186
19.15 IKE が用いる暗号アルゴリズムの設定 186

19.16 受信したIKEパケットを蓄積するキューの長さの設定 . . . 186
19.17 IKEが用いるグループの設定 . . . 187
19.18 IKEが用いるハッシュアルゴリズムの設定 . . . 187
19.19 受信したパケットのSPI値が無効な値の場合にログに出力するか否かの設定 . . . 187
19.20 IKEペイロードのタイプの設定 . . . 188
19.21 IKEの情報ペイロードを送信するか否かの設定 . . . 188
19.22 PFSを用いるか否かの設定 . . . 188
19.23 XAUTHの設定 . . . 188
19.24 XAUTH認証に使用するユーザIDの設定 . . . 189
19.25 XAUTH認証に使用するユーザIDの属性の設定 . . . 189
19.26 XAUTH認証に使用するユーザグループの設定 . . . 189
19.27 XAUTH認証に使用するユーザグループの属性の設定 . . . 190
19.28 XAUTHによるユーザ認証の設定 . . . 190
19.29 内部IPアドレスプールの設定 . . . 191
19.30 IPsecクライアントに割り当てる内部IPアドレスプールの設定 . . . 191
19.31 IKEのログの種類の設定 . . . 191
19.32 ESPをUDPでカプセル化して送受信するか否かの設定 . . . 192
19.33 SA関連の設定 . . . 192
19.33.1 SAの寿命の設定 . . . 192
19.33.2 SAのポリシーの定義 . . . 193
19.33.3 SAの手動更新 . . . 193
19.33.4 ダングリングSAの動作の設定 . . . 194
19.33.5 IPsec NATトラバーサルを利用するための設定 . . . 195
19.33.6 SAの削除 . . . 195
19.34 トンネルインタフェース関連の設定 . . . 196
19.34.1 IPsecトンネルの外側のIPv4パケットに対するDFビットの制御の設定 . . . 196
19.34.2 使用するSAのポリシーの設定 . . . 196
19.34.3 IPCompによるデータ圧縮の設定 . . . 196
19.34.4 トンネルバックアップの設定 . . . 197
19.34.5 トンネルテンプレートの設定 . . . 198
19.35 トランスポートモード関連の設定 . . . 199
19.35.1 トランスポートモードの定義 . . . 199

20. PPTP機能の設定 . . . 200

20.1 共通の設定 . . . 200
20.1.1 PPTPサーバーを動作させるか否かの設定 . . . 200
20.1.2 相手先情報番号にバインドされるトンネルインタフェースの設定 . . . 200
20.1.3 PPTPの動作タイプの設定 . . . 200
20.1.4 PPTPホスト名の設定 . . . 201
20.1.5 PPTPパケットのウィンドウサイズの設定 . . . 201
20.1.6 PPTPの動作モードの設定 . . . 201
20.1.7 PPTP暗号鍵生成のための要求する認証方式の設定 . . . 201
20.1.8 PPTP暗号鍵生成のための受け入れ可能な認証方式の設定 . . . 202
20.1.9 PPTPのコネクション制御のsyslogを出力するか否かの設定 . . . 202
20.2 リモートアクセスVPN機能 . . . 202
20.2.1 PPTPトンネルの切断タイマの設定 . . . 202
20.2.2 PPTPトンネルの端点の名前の設定 . . . 202
20.2.3 PPTPキープアライブの設定 . . . 203
20.2.4 PPTPキープアライブのログ設定 . . . 203
20.2.5 PPTPキープアライブを出すインターバルとカウントの設定 . . . 203
20.2.6 PPTP接続において暗号化の有無により接続を許可するか否かの設定 . . . 203

21. SNMPの設定 . . . 204

21.1 SNMPによるアクセスを許可するホストの設定 . . . 204
21.2 SNMP送信パケットの始点アドレスの設定 . . . 204
21.3 読み出し専用のコミュニティ名の設定 . . . 205
21.4 読み書き可能なコミュニティ名の設定 . . . 205
21.5 sysContactの設定 . . . 205
21.6 sysLocationの設定 . . . 205

21.7 sysName の設定 206
21.8 SNMP トラップを送信するか否かの設定 206
21.9 SNMP の linkDown トラップの送信制御の設定 206
21.10 SNMP トラップのコミュニティ名の設定 207
21.11 SNMP トラップの送信先の設定 207
21.12 PP インタフェースの情報を MIB2 の範囲で表示するか否かの設定 207
21.13 トンネルインタフェースの情報を MIB2 の範囲で表示するか否かの設定 207
21.14 PP インタフェースのアドレスの強制表示の設定 208
21.15 LAN インタフェースの各ポートのリンクが up/down したときにトラップを送信するか否かの設定 . . 208

22. RADIUS の設定 209
22.1 RADIUS による認証を使用するか否かの設定 209
22.2 RADIUS によるアカウントを使用するか否かの設定 209
22.3 RADIUS サーバーの指定 209
22.4 RADIUS 認証サーバーの指定 210
22.5 RADIUS アカウントサーバーの指定 210
22.6 RADIUS 認証サーバーの UDP ポートの設定 210
22.7 RADIUS アカウントサーバーの UDP ポートの設定 210
22.8 RADIUS シークレットの設定 211
22.9 RADIUS 再送信パラメータの設定 211

23. NAT 機能 212
23.1 インタフェースへの NAT ディスクリプタ適用の設定 212
23.2 NAT ディスクリプタの動作タイプの設定 212
23.3 NAT 処理の外側 IP アドレスの設定 213
23.4 NAT 処理の内側 IP アドレスの設定 213
23.5 静的 NAT エントリの設定 213
23.6 IP マスカレード使用時に rlogin,rcp と ssh を使用するか否かの設定 214
23.7 静的 IP マスカレードエントリの設定 214
23.8 NAT の IP アドレスマップの消去タイマの設定 215
23.9 IP マスカレードテーブルの TTL 処理方式の設定 215
23.10 外側から受信したパケットに該当する変換テーブルが存在しないときの動作の設定 216
23.11 IP マスカレードで利用するポートの範囲の設定 216
23.12 FTP として認識するポート番号の設定 216
23.13 IP マスカレードで変換しないポート番号の範囲の設定 217
23.14 NAT のアドレス割当をログに記録するか否かの設定 217
23.15 SIP メッセージに含まれる IP アドレスを書き換えるか否かの設定 217
23.16 IP マスカレード変換時に DF ビットを削除するか否かの設定 218
23.17 IP マスカレードで変換するセッション数の設定 218

24. DNS の設定 219
24.1 DNS を利用するか否かの設定 219
24.2 DNS サーバーの IP アドレスの設定 219
24.3 DNS ドメイン名の設定 219
24.4 DNS サーバーを通知してもらう相手先情報番号の設定 220
24.5 DHCP/IPCP MS 拡張で DNS サーバーを通知する順序の設定 220
24.6 プライベートアドレスに対する問い合わせを処理するか否かの設定 220
24.7 SYSLOG 表示で DNS により名前解決するか否かの設定 221
24.8 DNS 問い合わせの内容に応じた DNS サーバーの選択 221
24.9 静的 DNS レコードの登録 222
24.10 DNS 問い合わせパケットの始点ポート番号の設定 222
24.11 DNS サーバーへアクセスできるホストの IP アドレス設定 223
24.12 DNS キャッシュを使用するか否かの設定 223
24.13 DNS キャッシュの最大エントリ数の設定 223

25. 優先制御／帯域制御 224
25.1 インタフェース速度の設定 224
25.2 クラス分けのためのフィルタ設定 224
25.3 キューイングアルゴリズムタイプの選択 227

25.4 MP インタリーブの設定 . . . 227
25.5 クラス分けフィルタの適用 . . . 228
25.6 クラス毎のキュー長の設定 . . . 228
25.7 第 2 階層クラスのキュー長の設定 . . . 229
25.8 デフォルトクラスの設定 . . . 229
25.9 第 2 階層のデフォルトクラスの設定 . . . 229
25.10 クラスの属性の設定 . . . 230
25.11 動的なクラス変更 (Dynamic Class Control) の設定 . . . 231

26. 連携機能 . . . 233
26.1 連携動作を行うか否かの設定 . . . 233
26.2 連携動作で使用するポート番号の設定 . . . 233
26.3 帯域測定で連携動作を行う相手毎の動作の設定 . . . 233
26.4 負荷監視通知で連携動作を行う相手毎の動作の設定 . . . 235
26.5 負荷監視サーバーとしての動作トリガの設定 . . . 236
26.6 負荷監視クライアントとしての動作の設定 . . . 237
26.7 連携動作の手動実行 . . . 237

27. OSPF . . . 238
27.1 OSPF の有効設定 . . . 238
27.2 OSPF の使用設定 . . . 238
27.3 OSPF による経路の優先度設定 . . . 238
27.4 OSPF のルーター ID 設定 . . . 238
27.5 OSPF で受け取った経路をルーティングテーブルに反映させるか否かの設定 . . . 239
27.6 外部プロトコルによる経路導入 . . . 239
27.7 OSPF で受け取った経路をどう扱うかのフィルタの設定 . . . 240
27.8 外部経路導入に適用するフィルタ定義 . . . 241
27.9 OSPF エリア設定 . . . 242
27.10 エリアへの経路広告 . . . 242
27.11 スタブ的接続の広告 . . . 242
27.12 仮想リンク設定 . . . 243
27.13 指定インタフェースの OSPF エリア設定 . . . 244
27.14 非ブロードキャスト型ネットワークに接続されている OSPF ルーターの指定 . . . 246
27.15 スタブが存在する時のネットワーク経路の扱いの設定 . . . 246
27.16 OSPF の状態遷移とパケットの送受信をログに記録するか否かの設定 . . . 246

28. BGP . . . 247
28.1 BGP の起動の設定 . . . 247
28.2 経路の集約の設定 . . . 247
28.3 経路を集約するためのフィルタの設定 . . . 247
28.4 AS 番号の設定 . . . 248
28.5 ルーター ID の設定 . . . 248
28.6 BGP による経路の優先度の設定 . . . 248
28.7 BGP で受信した経路に対するフィルタの適用 . . . 248
28.8 BGP で受信する経路に適用するフィルタの設定 . . . 249
28.9 BGP に導入する経路に対するフィルタの適用 . . . 250
28.10 BGP の設定の有効化 . . . 250
28.11 BGP に導入する経路に適用するフィルタの設定 . . . 250
28.12 BGP による接続先の設定 . . . 251
28.13 BGP のログの設定 . . . 251

29. IPv6 . . . 252
29.1 共通の設定 . . . 252
29.1.1 IPv6 パケットを扱うか否かの設定 . . . 252
29.1.2 IPv6 インタフェースのリンク MTU の設定 . . . 252
29.1.3 TCP セッションの MSS 制限の設定 . . . 252
29.1.4 タイプ 0 のルーティングヘッダ付き IPv6 パケットを破棄するか否かの設定 . . . 253
29.1.5 IPv6 ファストパス機能の設定 . . . 253

29.2 IPv6 アドレスの管理 253
29.2.1 インタフェースの IPv6 アドレスの設定 253
29.2.2 インタフェースのプレフィックスに基づく IPv6 アドレスの設定 254
29.2.3 DAD(Duplicate Address Detection) の送信回数の設定 254
29.2.4 自動的に設定される IPv6 アドレスの最大数の設定 255
29.2.5 始点 IPv6 アドレスを選択する規則の設定 255
29.3 近隣探索 255
29.3.1 ルーター広告で配布するプレフィックスの定義 255
29.3.2 ルーター広告の送信の制御 256
29.4 経路制御 257
29.4.1 IPv6 の経路情報の追加 257
29.5 RIPng 257
29.5.1 RIPng の使用の設定 257
29.5.2 インタフェースにおける RIPng の送信ポリシーの設定 257
29.5.3 インタフェースにおける RIPng の受信ポリシーの設定 258
29.5.4 RIPng の加算ホップ数の設定 258
29.5.5 インタフェースにおける信頼できる RIPng ゲートウェイの設定 258
29.5.6 RIPng で送受信する経路に対するフィルタリングの設定 259
29.5.7 回線接続時の PP 側の RIPng の動作の設定 259
29.5.8 回線接続時の PP 側の RIPng 送出の時間間隔の設定 259
29.5.9 回線切断時の PP 側の RIPng の動作の設定 260
29.5.10 回線切断時の PP 側の RIPng 送出の時間間隔の設定 260
29.5.11 RIPng による経路を回線切断時に保持するか否かの設定 260
29.5.12 RIPng による経路の優先度の設定 260
29.6 フィルタの設定 261
29.6.1 IPv6 フィルタの定義 261
29.6.2 IPv6 フィルタの適用 261
29.6.3 IPv6 動的フィルタの定義 262
29.7 IPv6 マルチキャストパケットの転送の設定 263
29.7.1 MLD の動作の設定 263
29.7.2 MLD の静的な設定 264
29.7.3 IPv6 マルチキャストの転送モードの設定 264
29.8 近隣要請 265
29.8.1 アドレス重複チェックをトリガに近隣要請を行うか否かの設定 265

30. OSPFv3 266
30.1 OSPFv3 の有効設定 266
30.2 OSPFv3 の使用設定 266
30.3 OSPFv3 のルーター ID 設定 266
30.4 OSPFv3 エリア設定 267
30.5 エリアへの経路広告 267
30.6 指定インタフェースの OSPFv3 エリア設定 267
30.7 仮想リンク設定 269
30.8 OSPFv3 による経路の優先度設定 270
30.9 OSPFv3 で受け取った経路をルーティングテーブルに反映させるか否かの設定 270
30.10 OSPFv3 で受け取った経路をどう扱うかのフィルタの設定 271
30.11 外部プロトコルによる経路導入 272
30.12 外部経路導入に適用するフィルタ定義 272
30.13 OSPFv3 のログ出力設定 273

31. 状態メール通知機能 274
31.1 状態メール通知機能の動作の設定 274
31.2 メールサーバーの設定 274
31.3 送信元のメールアドレスの設定 274
31.4 送信先メールアドレスの設定 274
31.5 サブジェクトの設定 275
31.6 送信タイムアウトの設定 275
31.7 通知内容の設定 275
31.8 状態メール通知の実行 275

32. トリガによるメール通知機能 276
32.1 メール設定識別名の設定 276
32.2 SMTP メールサーバーの設定 276
32.3 POP メールサーバーの設定 277
32.4 メール処理のタイムアウト値の設定 277
32.5 メールの送信時に使用するテンプレートの設定 277
32.6 メール通知のトリガの設定 278

33. HTTP サーバー機能 280
33.1 共通の設定 280
33.1.1 HTTP サーバー機能の有無の設定 280
33.1.2 HTTP サーバーへアクセスできるホストの IP アドレス設定 280
33.1.3 HTTP サーバーのセッションタイムアウト時間の設定 280
33.1.4 HTTP サーバー機能の listen ポートの設定 281
33.1.5 PP インタフェースとトンネルインタフェースの名前の設定 281
33.2 かんたん設定ページ用の設定 281
33.2.1 プロバイダ接続タイプの設定 281
33.2.2 プロバイダ情報の PP との関連付けと名前の設定 282
33.2.3 プロバイダ接続設定 282
33.2.4 プロバイダの DNS サーバーのアドレス設定 282
33.2.5 LAN インタフェースの DNS サーバーのアドレスの設定 282
33.2.6 DNS サーバーを通知してくれる相手の相手先情報番号の設定 283
33.2.7 フィルタ型ルーティングの形式の設定 283
33.2.8 LAN 側のプロバイダ名称の設定 283
33.2.9 NTP サーバーの設定 283
33.2.10 プロバイダの NTP サーバーのアドレス設定 284
33.2.11 かんたん設定ページの切断ボタンを押した後に自動接続するか否かの設定 284
33.2.12 かんたん設定ページで IPv6 接続を行うか否かの設定 284

34. ネットボランチ DNS サービスの設定 285
34.1 ネットボランチ DNS サービスの使用の可否 285
34.2 ネットボランチ DNS サーバーへの手動更新 285
34.3 ネットボランチ DNS サーバーからの削除 285
34.4 ネットボランチ DNS サービスで使用するポート番号の設定 286
34.5 ネットボランチ DNS サーバーに登録済みのホスト名一覧を取得 286
34.6 ホスト名の登録 286
34.7 通信タイムアウトの設定 286
34.8 ホスト名を自動生成するか否かの設定 287
34.9 ネットボランチ DNS サーバーの設定 287
34.10 自動更新に失敗した場合のリトライ間隔と回数の設定 287

35. UPnP の設定 288
35.1 UPnP を使用するか否かの設定 288
35.2 UPnP に使用する IP アドレスを取得するインタフェースの設定 288
35.3 UPnP のポートマッピング用消去タイマのタイプの設定 288
35.4 UPnP のポートマッピングの消去タイマの設定 289
35.5 UPnP の syslog を出力するか否かの設定 289

36. USB の設定 290
36.1 USB ホスト機能を使うか否かの設定 290
36.2 USB メモリに保存する SYSLOG ファイル名の指定 290
36.3 統計情報を書き出すファイル名のプレフィックスの設定 291
36.4 USB ボタンと DOWNLOAD ボタン同時押下による設定ファイル、ファームウェアファイルのコピー操作を許可するか否かの設定 291
36.5 USB ボタンと DOWNLOAD ボタン同時押下によりコピーする設定ファイル名の指定 292
36.6 USB ボタンと DOWNLOAD ボタン同時押下によりコピーするファームウェアファイル名の指定 292
36.7 USB ポートに接続した機器の初期化に使う AT コマンドの設定 292
36.8 USB ポートに接続した機器のフロー制御を行うか否かの設定 293

37. スケジュール 294
37.1 スケジュールの設定 294

38. VLAN の設定 295
38.1 VLAN ID の設定 295
38.2 スイッチングハブのポートが所属する VLAN の設定 295

39. 生存通知機能 296
39.1 生存通知の共有鍵の設定 296
39.2 生存通知を受信するか否かの設定 296
39.3 生存通知の実行 296

40. SNTP サーバー機能 297
40.1 SNTP サーバー機能を有効にするか否かの設定 297
40.2 SNTP サーバーへのアクセスを許可するホストの設定 297

41. 外部メモリ機能 298
41.1 microSD カードスロットを使うか否かの設定 298
41.2 外部メモリに保存する統計情報のファイル名のプレフィックスの設定 299
41.3 外部メモリに保存する SYSLOG ファイル名の指定 300
41.4 外部メモリボタンと DOWNLOAD ボタンの同時押下による設定ファイル、ファームウェアファイルのコピー操作を許可するか否かの設定 300
41.5 外部メモリ内のファイルからの起動を許可するか否かの設定 301
41.6 起動時、あるいは外部メモリボタンと DOWNLOAD ボタン同時押下により読み込まれる、ファームウェアファイル名の指定 301
41.7 起動時、あるいは外部メモリボタンと DOWNLOAD ボタン同時押下により読み込まれる、設定ファイル名の指定 302
41.8 ファイル検索時のタイムアウトを設定する 302
41.9 バッチファイルを実行する 303
41.10 バッチファイルと実行結果ファイルの設定 303
41.11 DOWNLOAD ボタンを押した時に実行する機能の設定 303
41.12 DOWNLOAD ボタンによるバッチファイルの実行を許可するか否かの設定 304

42. HTTP アップロード機能 305
42.1 HTTP アップロードするファイルの設定 305
42.2 HTTP アップロード先 URL の設定 305
42.3 HTTP アップロードを許可するか否かの設定 306
42.4 HTTP アップロードのタイムアウト時間の設定 306
42.5 HTTP アップロードのリトライの間隔と回数の設定 306
42.6 HTTP アップロードで使用するプロキシサーバーの設定 306
42.7 HTTP アップロードの実行 307
42.8 HTTP アップロード機能に関連するアラーム音を鳴らすか否かの設定 307

43. モバイルインターネット接続機能 308
43.1 携帯端末を使用するか否かの設定 308
43.2 携帯端末の種別設定 308
43.3 携帯端末に直接コマンドを発行する 309
43.4 指定した相手に対して発信制限を解除する 309
43.5 PP で使用するインタフェースの設定 309
43.6 携帯端末からの自動発信設定 309
43.7 携帯端末を切断するタイマの設定 310
43.8 携帯端末を入力がないときに切断するタイマの設定 310
43.9 携帯端末を出力がないときに切断するタイマの設定 310
43.10 発信先アクセスポイントの設定 310
43.11 パケット通信量制限の設定 311
43.12 パケット通信時間制限の設定 311
43.13 同じ発信先に対して連続して認証に失敗できる回数の設定 311
43.14 LCP の Async Control Character Map オプション使用の設定 312
43.15 発信者番号通知 (186) を付加するかどうかの設定 312

43.16 詳細な SYSLOG を出力するか否かの設定 312
43.17 携帯端末が接続状態になったときにアラーム音を鳴らすかどうかの設定 312

44. ブリッジインタフェース (ブリッジ機能) 313
44.1 ブリッジインタフェースに収容する実インタフェースを設定する 313
44.2 自動的なラーニングを行うか否かの設定 314
44.3 ブリッジがラーニングした情報の消去タイマーの設定 314
44.4 静的なラーニング情報の設定 314

45. 操作 315
45.1 相手先情報番号の選択 315
45.2 トンネルインタフェース番号の選択 315
45.3 設定に関する操作 315
45.3.1 管理ユーザへの移行 315
45.3.2 終了 315
45.3.3 設定内容の保存 316
45.3.4 設定ファイルの複製 316
45.3.5 ファームウェアファイルを内蔵フラッシュ ROM にコピー 317
45.3.6 設定ファイルの削除 317
45.3.7 実行形式ファームウェアファイルの削除 318
45.3.8 デフォルト設定ファイルの設定 318
45.3.9 デフォルトファームウェアファイルの設定 318
45.3.10 設定の初期化 318
45.3.11 遠隔地のルーターの設定 318
45.3.12 遠隔地のルーターからの設定に対する制限 319
45.4 動的情報のクリア操作 319
45.4.1 アカウントのクリア 319
45.4.2 ARP テーブルのクリア 319
45.4.3 IP の動的経路情報のクリア 319
45.4.4 IPX の動的経路情報のクリア 319
45.4.5 IPX の動的 SAP 情報のクリア 320
45.4.6 ブリッジのラーニング情報のクリア 320
45.4.7 ログのクリア 320
45.4.8 InARP のクリア 320
45.4.9 DNS キャッシュのクリア 320
45.4.10 PRI のステータス情報のクリア 320
45.4.11 NAT アドレステーブルのクリア 321
45.4.12 インタフェースの NAT アドレステーブルのクリア 321
45.4.13 IPv6 の動的経路情報の消去 321
45.4.14 近隣キャッシュの消去 321
45.5 その他の操作 321
45.5.1 相手先の使用許可の設定 321
45.5.2 相手先の使用不許可の設定 322
45.5.3 再起動 322
45.5.4 インタフェースの再起動 322
45.5.5 PP インタフェースの再起動 323
45.5.6 発信 323
45.5.7 切断 323
45.5.8 ping 323
45.5.9 ping6 の実行 324
45.5.10 traceroute 324
45.5.11 traceroute6 の実行 324
45.5.12 nslookup 324
45.5.13 IPv4 動的フィルタのコネクション管理情報の削除 324
45.5.14 TELNET クライアント 325
45.5.15 IPv6 動的フィルタのコネクション管理情報の削除 325
45.5.16 スイッチングハブ MAC アドレステーブルの消去 325
45.5.17 PRI のループバックの実行 326
45.5.18 PRI のループバック待ち受けの設定 326

45.5.19 Magic Packet の送信 327
45.5.20 HTTP を利用したファームウェアのチェックおよびリビジョンアップの実行 327
45.5.21 入力遮断フィルタの状態のクリア 328
45.5.22 ポリシーフィルタの状態のクリア 328
45.5.23 URL フィルタの統計情報のクリア 328
45.5.24 状態メール通知の実行 328

46. 設定の表示 329
46.1 機器設定の表示 329
46.2 すべての設定内容の表示 329
46.3 指定した PP の設定内容の表示 329
46.4 指定したトンネルの設定内容の表示 329
46.5 設定ファイルの一覧 330
46.6 ファイル情報の一覧の表示 330
46.7 インタフェースに付与されている IPv6 アドレスの表示 330
46.8 マスタクロックを得ている回線の表示 330
46.9 SSH サーバー公開鍵の表示 330
46.10 指定したインタフェースのフィルタ内容の表示 331
46.11 ファームウェアファイルの一覧 331

47. 状態の表示 332
47.1 ARP テーブルの表示 332
47.2 インタフェースの状態の表示 332
47.3 各相手先の状態の表示 332
47.4 DLCI の表示 332
47.5 IP の経路情報テーブルの表示 333
47.6 RIP で得られた経路情報の表示 333
47.7 IPv6 の経路情報の表示 333
47.8 IPv6 の RIP テーブルの表示 334
47.9 近隣キャッシュの表示 334
47.10 IPXWAN の状態の表示 334
47.11 SAP テーブルの表示 334
47.12 IPX の経路情報テーブルの表示 334
47.13 ブリッジのラーニング情報の表示 334
47.14 IPsec の SA の表示 335
47.15 VRRP の情報の表示 335
47.16 動的 NAT ディスクリプタのアドレスマップの表示 335
47.17 動作中の NAT ディスクリプタの適用リストの表示 335
47.18 LAN インタフェースの NAT ディスクリプタのアドレスマップの表示 336
47.19 IP マスカレードで使用しているポート番号の個数の表示 336
47.20 PPTP の状態の表示 336
47.21 OSPF 情報の表示 336
47.22 BGP の状態の表示 336
47.23 DHCP サーバーの状態の表示 337
47.24 DHCP クライアントの状態の表示 337
47.25 バックアップ状態の表示 337
47.26 動的フィルタによって管理されているコネクションの表示 338
47.27 IPv6 の動的フィルタによって管理されているコネクションの表示 338
47.28 ネットワーク監視機能の状態の表示 338
47.29 侵入情報の履歴の表示 339
47.30 相手先ごとの接続時間情報の表示 339
47.31 ネットボランチ DNS サービスに関する設定の表示 339
47.32 スイッチングハブ MAC アドレステーブルの表示 339
47.33 UPnP に関するステータス情報の表示 340
47.34 トンネルインタフェースの状態の表示 340
47.35 VLAN インタフェースの状態の表示 340
47.36 トリガによるメール通知機能の状態の表示 340
47.37 マルチキャストの経路情報の表示 340
47.38 IGMP のグループ管理情報の表示 341

47.39 PIM-SM によって管理される情報の表示 341
47.40 MLD のグループ管理情報の表示 341
47.41 IPv6 マルチキャストの経路情報の表示 341
47.42 ログインしているユーザ情報の表示 342
47.43 パケットバッファの状態の表示 342
47.44 QoS ステータスの表示 342
47.45 連携動作の状態の表示 343
47.46 OSPFv3 情報の表示 343
47.47 入力遮断フィルタの状態表示 343
47.48 ポリシーフィルタの状態表示 344
47.49 ポリシーフィルタの制御対象サービスの表示 344
47.50 URL フィルタの情報の表示 344
47.51 生存通知の状態の表示 344
47.52 USB ホスト機能の動作状態を表示 345
47.53 リモートセットアップ機能に関する接続情報の表示 345
47.54 技術情報の表示 345
47.55 microSD スロットの動作状態を表示 345
47.56 外部メモリの動作状態を表示 345

48. ロギング 346
48.1 ログの表示 346
48.2 アカウントの表示 346
48.3 通信履歴の表示 346

49. 診断 347
49.1 ポートの開閉状態の診断 347
49.2 ポートへ到達可能なアクセス範囲の診断 347
49.3 ポートの開閉状態の診断で検出可能な通過パケットの最大数の設定 348
49.4 ポートの開閉状態の診断結果の履歴数の設定 348
49.5 ポートの開閉状態の診断結果の表示 348
49.6 ポートへ到達可能なアクセス範囲の診断結果の表示 348
49.7 ポートの開閉状態の診断結果の消去 348

50. 統計 349
50.1 統計機能を有効にするか否かの設定 349

コマンド索引

A

account threshold . . . 68
account threshold pp . . . 68
administrator . . . 31, 315
administrator password . . . 43
administrator password encrypted . . . 43
alarm entire . . . 64
alarm http revision-up . . . 65
alarm http upload . . . 307
alarm mobile . . . 312
alarm sd . . . 65
alarm startup . . . 65
alarm usbhost . . . 64
auth user . . . 189
auth user attribute . . . 189
auth user group . . . 189
auth user group attribute . . . 190

B

bgp aggregate . . . 247
bgp aggregate filter . . . 247
bgp autonomous-system . . . 248
bgp configure refresh . . . 250
bgp export . . . 248
bgp export aspath . . . 248
bgp export filter . . . 249
bgp import . . . 250
bgp import filter . . . 250
bgp log . . . 251
bgp neighbor . . . 251
bgp preference . . . 248
bgp router id . . . 248
bgp use . . . 247
bridge filter . . . 126
bridge group . . . 125
bridge interface filter . . . 127
bridge interface learning . . . 126
bridge learning . . . 125, 314
bridge learning expire . . . 126
bridge member . . . 313
bridge pp filter . . . 127
bridge pp learning . . . 127
bridge use . . . 125

C

clear account . . . 319
clear account pp . . . 319
clear arp . . . 319
clear bridge learning . . . 320
clear diagnosis config port . . . 348
clear dns cache . . . 320
clear inarp . . . 320
clear ip dynamic routing . . . 319
clear ip inbound filter . . . 328
clear ip policy filter . . . 328
clear ip traffic list . . . 114
clear ip traffic list pp . . . 114
clear ip traffic list tunnel . . . 114
clear ipv6 dynamic routing . . . 321
clear ipv6 inbound filter . . . 328
clear ipv6 neighbor cache . . . 321
clear ipv6 policy filter . . . 328
clear ipx dynamic routing . . . 319
clear ipx dynamic sap . . . 320
clear log . . . 320
clear mobile access limitation . . . 309
clear mobile access limitation pp . . . 309
clear nat descriptor dynamic . . . 321
clear nat descriptor interface dynamic . . . 321
clear nat descriptor interface dynamic pp . . . 321
clear nat descriptor interface dynamic tunnel . . . 321
clear pri status . . . 320
clear switching-hub macaddress . . . 325
clear url filter . . . 328
clear url filter pp . . . 328
clear url filter tunnel . . . 328
cold start . . . 318
connect . . . 323
console character . . . 31, 48
console columns . . . 48
console info . . . 49
console lines . . . 48
console prompt . . . 48
cooperation . . . 233, 237
cooperation bandwidth-measuring remote . . . 233
cooperation load-watch control . . . 237
cooperation load-watch remote . . . 235
cooperation load-watch trigger . . . 236
cooperation port . . . 233
copy config . . . 316
copy exec . . . 317

D

date . . . 47
delete config . . . 317
delete exec . . . 318
description . . . 58
dhcp client client-identifier . . . 168
dhcp client client-identifier pool . . . 168
dhcp client client-identifier pp . . . 168
dhcp client hostname . . . 167
dhcp client hostname pool . . . 167
dhcp client hostname pp . . . 167
dhcp client option . . . 169
dhcp client option pool . . . 169
dhcp client option pp . . . 169
dhcp convert lease to bind . . . 164
dhcp duplicate check . . . 160
dhcp manual lease . . . 165
dhcp manual release . . . 166
dhcp relay select . . . 166
dhcp relay server . . . 166
dhcp relay threshold . . . 166
dhcp scope . . . 161
dhcp scope bind . . . 161
dhcp scope lease type . . . 163
dhcp scope option . . . 165
dhcp server rfc2131 compliant . . . 160
dhcp service . . . 159
diagnose config port access . . . 347
diagnose config port map . . . 347
diagnosis config port history-num . . . 348
diagnosis config port max-detect . . . 348
disconnect . . . 31, 323

disconnect ip connection 324
disconnect ipv6 connection 325
disconnect user 46
dns cache max entry 223
dns cache use 223
dns domain 219
dns host 223
dns notice order 220
dns private address spoof 220
dns server 219
dns server dhcp 167
dns server pp 220
dns server select 221
dns service 219
dns srcport 222
dns static 222
dns syslog resolv 221

E

ethernet filter 128
ethernet interface filter 129
execute at-command 309
execute batch 303
exit 315
external-memory auto-search time 302
external-memory batch filename 303
external-memory boot permit 301
external-memory config filename 302
external-memory config filename off 302
external-memory exec filename 301
external-memory exec filename off 301
external-memory statistics filename prefix 299
external-memory syslog filename 300

F

fr backup 79
fr cir 78
fr compression use 79
fr congestion control 80
fr de 80
fr dlci 78
fr inarp 79
fr lmi 78
fr pp dequeue type 80

H

heartbeat pre-shared-key 296
heartbeat receive 296
heartbeat send 296
help 42
http revision-down permit 61
http revision-up go 327
http revision-up permit 60
http revision-up proxy 60
http revision-up timeout 61
http revision-up url 60
http upload 305
http upload go 307
http upload permit 306
http upload proxy 306
http upload retry interval 306
http upload timeout 306
http upload url 305
httpd host 280
httpd listen 281
httpd service 280
httpd timeout 280

I

interface reset 322
interface reset pp 323
ip arp timer 95
ip filter 86
ip filter directed-broadcast 88
ip filter dynamic 88
ip filter dynamic timer 89
ip filter set 88
ip filter source-route 88
ip flow timer 113
ip forward filter 116
ip fragment remove df-bit filter 94
ip host 222
ip icmp echo-reply send 170
ip icmp echo-reply send-only-linkup 170
ip icmp error-decrypted-ipsec send 172
ip icmp log 172
ip icmp mask-reply send 170
ip icmp parameter-problem send 170
ip icmp redirect receive 171
ip icmp redirect send 171
ip icmp time-exceeded send 171
ip icmp timestamp-reply send 171
ip icmp unreachable send 172
ip icmp unreachable-for-truncated send 173
ip implicit-route preference 113
ip inbound filter 130
ip interface address 83
ip interface arp mtu discovery 173
ip interface arp queue length 95
ip interface arp static 95
ip interface dhcp lease time 168
ip interface dhcp retry 168
ip interface forward filter 116
ip interface igmp 110
ip interface igmp static 110
ip interface inbound filter list 131
ip interface intrusion detection 90
ip interface intrusion detection notice-interval . . . 90
ip interface intrusion detection repeat-control 91
ip interface intrusion detection report 91
ip interface intrusion detection threshold 91
ip interface mtu 84
ip interface nat descriptor 212
ip interface ospf area 244
ip interface ospf neighbor 246
ip interface pim sparse 111
ip interface proxyarp 94
ip interface proxyarp vrrp 94
ip interface rip auth key 101
ip interface rip auth key text 101
ip interface rip auth type 101
ip interface rip filter 100
ip interface rip force-to-advertise 103
ip interface rip hop 100
ip interface rip receive 100
ip interface rip send 99
ip interface rip trust gateway 99
ip interface secondary address 84
ip interface secure filter 93

ip interface secure filter name . . . 93
ip interface tcp mss limit . . . 92
ip interface traffic list . . . 114
ip interface traffic list threshold . . . 115
ip interface vrrp . . . 105
ip interface vrrp shutdown trigger . . . 105
ip interface wol relay . . . 58
ip keepalive . . . 109
ip local forward filter . . . 116
ip pim sparse join-prune send . . . 112
ip pim sparse log . . . 112
ip pim sparse periodic-prune send . . . 112
ip pim sparse register-checksum . . . 112
ip pim sparse rendezvous-point static . . . 111
ip policy address group . . . 133
ip policy filter . . . 134
ip policy filter set . . . 135
ip policy filter set enable . . . 135
ip policy filter set switch . . . 136
ip policy filter timer . . . 137
ip policy interface group . . . 132
ip policy service . . . 132
ip policy service group . . . 133
ip pp address . . . 83
ip pp forward filter . . . 116
ip pp igmp . . . 110
ip pp igmp static . . . 110
ip pp inbound filter list . . . 131
ip pp intrusion detection . . . 90
ip pp intrusion detection notice-interval . . . 90
ip pp intrusion detection repeat-control . . . 91
ip pp intrusion detection report . . . 91
ip pp intrusion detection threshold . . . 91
ip pp mtu . . . 84
ip pp nat descriptor . . . 212
ip pp ospf area . . . 244
ip pp ospf neighbor . . . 246
ip pp pim sparse . . . 111
ip pp remote address . . . 96
ip pp remote address pool . . . 96
ip pp rip auth key . . . 101
ip pp rip auth key text . . . 101
ip pp rip auth type . . . 101
ip pp rip backup interface . . . 103
ip pp rip connect interval . . . 102
ip pp rip connect send . . . 102
ip pp rip disconnect interval . . . 102
ip pp rip disconnect send . . . 102
ip pp rip filter . . . 100
ip pp rip force-to-advertise . . . 103
ip pp rip hold routing . . . 101
ip pp rip hop . . . 100
ip pp rip receive . . . 100
ip pp rip send . . . 99
ip pp rip trust gateway . . . 99
ip pp secure filter . . . 93
ip pp secure filter name . . . 93
ip pp tcp mss limit . . . 92
ip pp traffic list . . . 114
ip pp traffic list threshold . . . 115
ip route . . . 85
ip route change log . . . 92
ip routing . . . 83
ip routing process . . . 53
ip simple-service . . . 84
ip stealth . . . 172
ip tos supersede . . . 94
ip tunnel address . . . 178
ip tunnel forward filter . . . 116
ip tunnel igmp . . . 110
ip tunnel igmp static . . . 110
ip tunnel inbound filter list . . . 131
ip tunnel intrusion detection . . . 90
ip tunnel intrusion detection notice-interval . . . 90
ip tunnel intrusion detection repeat-control . . . 91
ip tunnel intrusion detection report . . . 91
ip tunnel intrusion detection threshold . . . 91
ip tunnel mtu . . . 84
ip tunnel nat descriptor . . . 212
ip tunnel ospf area . . . 244
ip tunnel ospf neighbor . . . 246
ip tunnel pim sparse . . . 111
ip tunnel remote address . . . 179
ip tunnel rip auth key . . . 101
ip tunnel rip auth key text . . . 101
ip tunnel rip auth type . . . 101
ip tunnel rip filter . . . 100
ip tunnel rip force-to-advertise . . . 103
ip tunnel rip hop . . . 100
ip tunnel rip receive . . . 100
ip tunnel rip send . . . 99
ip tunnel rip trust gateway . . . 99
ip tunnel secure filter . . . 93
ip tunnel secure filter name . . . 93
ip tunnel tcp mss limit . . . 92
ip tunnel traffic list . . . 114
ip tunnel traffic list threshold . . . 115
ipsec auto refresh . . . 181
ipsec ike always-on . . . 182
ipsec ike duration . . . 192
ipsec ike encryption . . . 186
ipsec ike esp-encapsulation . . . 192
ipsec ike group . . . 187
ipsec ike hash . . . 187
ipsec ike keepalive log . . . 186
ipsec ike keepalive use . . . 185
ipsec ike local address . . . 184
ipsec ike local id . . . 185
ipsec ike local name . . . 184
ipsec ike log . . . 191
ipsec ike mode-cfg address . . . 191
ipsec ike mode-cfg address pool . . . 191
ipsec ike nat-traversal . . . 195
ipsec ike negotiate-strictly . . . 182
ipsec ike payload type . . . 188
ipsec ike pfs . . . 188
ipsec ike pre-shared-key . . . 181
ipsec ike queue length . . . 186
ipsec ike remote address . . . 183
ipsec ike remote id . . . 184
ipsec ike remote name . . . 183
ipsec ike restrict-dangling-sa . . . 194
ipsec ike retry . . . 183
ipsec ike send info . . . 188
ipsec ike xauth myname . . . 188
ipsec ike xauth request . . . 190
ipsec ipcomp type . . . 196
ipsec log illegal-spi . . . 187
ipsec refresh sa . . . 193
ipsec sa delete . . . 195

ipsec sa policy 193
ipsec transport 199
ipsec tunnel 196
ipsec tunnel outer df-bit 196
ipsec use 181
ipv6 filter 261
ipv6 filter dynamic 262
ipv6 icmp echo-reply send 174
ipv6 icmp echo-reply send-only-linkup 174
ipv6 icmp error-decrypted-ipsec send 176
ipv6 icmp log 175
ipv6 icmp packet-too-big send 176
ipv6 icmp packet-too-big-for-truncated send 177
ipv6 icmp parameter-problem send 174
ipv6 icmp redirect receive 175
ipv6 icmp redirect send 174
ipv6 icmp time-exceeded send 175
ipv6 icmp unreachable send 175
ipv6 inbound filter 130
ipv6 interface address 253
ipv6 interface dad retry count 254
ipv6 interface inbound filter list 131
ipv6 interface mld 263
ipv6 interface mld static 264
ipv6 interface mtu 252
ipv6 interface ospf area 267
ipv6 interface prefix 254
ipv6 interface rip filter 259
ipv6 interface rip hop 258
ipv6 interface rip receive 258
ipv6 interface rip send 257
ipv6 interface rip trust gateway 258
ipv6 interface rtadv send 256
ipv6 interface secure filter 261
ipv6 interface tcp mss limit 252
ipv6 max auto address 255
ipv6 multicast routing process 264
ipv6 nd ns-trigger-dad 265
ipv6 ospf area 267
ipv6 ospf area network 267
ipv6 ospf configure refresh 266
ipv6 ospf export 271
ipv6 ospf export from ospf 270
ipv6 ospf import 272
ipv6 ospf import from 272
ipv6 ospf log 273
ipv6 ospf preference 270
ipv6 ospf router id 266
ipv6 ospf use 266
ipv6 ospf virtual-link 269
ipv6 policy address group 133
ipv6 policy filter 134
ipv6 policy filter set 135
ipv6 policy filter set enable 135
ipv6 policy filter set switch 136
ipv6 policy interface group 132
ipv6 policy service 132
ipv6 policy service group 133
ipv6 pp address 253
ipv6 pp dad retry count 254
ipv6 pp inbound filter list 131
ipv6 pp mld 263
ipv6 pp mld static 264
ipv6 pp mtu 252
ipv6 pp ospf area 267
ipv6 pp prefix 254
ipv6 pp rip connect interval 259
ipv6 pp rip connect send 259
ipv6 pp rip disconnect interval 260
ipv6 pp rip disconnect send 260
ipv6 pp rip filter 259
ipv6 pp rip hold routing 260
ipv6 pp rip hop 258
ipv6 pp rip receive 258
ipv6 pp rip send 257
ipv6 pp rip trust gateway 258
ipv6 pp rtadv send 256
ipv6 pp secure filter 261
ipv6 pp tcp mss limit 252
ipv6 prefix 255
ipv6 rh0 discard 253
ipv6 rip preference 260
ipv6 rip use 257
ipv6 route 257
ipv6 routing 252
ipv6 routing process 253
ipv6 source address selection rule 255
ipv6 stealth 176
ipv6 tunnel address 253
ipv6 tunnel inbound filter list 131
ipv6 tunnel mld 263
ipv6 tunnel mld static 264
ipv6 tunnel ospf area 267
ipv6 tunnel prefix 254
ipv6 tunnel rip filter 259
ipv6 tunnel rip receive 258
ipv6 tunnel rip send 257
ipv6 tunnel secure filter 261
ipv6 tunnel tcp mss limit 252
ipx filter 118
ipx interface frame type 119
ipx interface network 119
ipx interface ripsap broadcast 120
ipx interface route 120
ipx interface secure filter 119
ipx pp ipxwan primnet 121
ipx pp ipxwan retry 123
ipx pp ipxwan use 121
ipx pp network 120
ipx pp ripsap connect interval 122
ipx pp ripsap connect send 121
ipx pp ripsap disconnect interval 122
ipx pp ripsap disconnect send 122
ipx pp ripsap hold 122
ipx pp route 121
ipx pp routing 120
ipx pp secure filter 124
ipx pp serialization filter 124
ipx pp spx keepalive proxy 124
ipx pp spx keepalive timer 123
ipx pp watchdog interval 123
ipx pp watchdog proxy 123
ipx routing 117
ipx sap 117
ipx sap response 117
isdn arrive permit 71
isdn auto connect 70
isdn call block time 72
isdn call permit 71
isdn call prohibit time 72

isdn callback mscbcp user-specify 73
isdn callback permit 72
isdn callback permit type 73
isdn callback request 72
isdn callback request type 73
isdn callback response time 73
isdn callback wait time 74
isdn disconnect input time 75
isdn disconnect interval time 76
isdn disconnect output time 76
isdn disconnect policy 74
isdn disconnect time 74
isdn dsu 67
isdn fast disconnect time 75
isdn forced disconnect time 75
isdn local address 66
isdn piafs arrive 68
isdn piafs call 69
isdn piafs control 69
isdn remote address 70
isdn remote call order 71
isdn terminator 67

L

lan backup 107
lan backup recovery time 107
lan keepalive interval 108
lan keepalive log 108
lan keepalive use 107
lan port-mirroring 53
lan receive-buffer-size 57
lan shutdown 53
lan type 54
leased backup 69
leased keepalive down 98
less config 329
less config list 330
less config pp 329
less config tunnel 329
less exec list 331
less file list 330
less log 346
line masterclock 52
line type 36, 66, 82
login password 43
login password encrypted 43
login timer 31, 57
login user 44

M

mail notify 278
mail notify status exec 328
mail server name 276
mail server pop 277
mail server smtp 276
mail server timeout 277
mail template 277
mail-notify status exec 275
mail-notify status from 274
mail-notify status server 274
mail-notify status subject 275
mail-notify status timeout 275
mail-notify status to 274
mail-notify status type 275
mail-notify status use 274
mobile access limit length 311
mobile access limit time 311
mobile access-point name 310
mobile auto connect 309
mobile call prohibit auth-error count 311
mobile disconnect input time 310
mobile disconnect output time 310
mobile disconnect time 310
mobile display caller id 312
mobile syslog 312
mobile type 308
mobile use 308

N

nat descriptor address inner 213
nat descriptor address outer 213
nat descriptor ftp port 216
nat descriptor log 217
nat descriptor masquerade incoming 216
nat descriptor masquerade port range 216
nat descriptor masquerade remove df-bit 218
nat descriptor masquerade rlogin 214
nat descriptor masquerade session limit 218
nat descriptor masquerade static 214
nat descriptor masquerade ttl hold 215
nat descriptor masquerade unconvertible port . . 217
nat descriptor sip 217
nat descriptor static 213
nat descriptor timer 215
nat descriptor type 212
netvolante-dns auto hostname 287
netvolante-dns auto hostname pp 287
netvolante-dns delete go 285
netvolante-dns delete go pp 285
netvolante-dns get hostname list 286
netvolante-dns get hostname list pp 286
netvolante-dns go 285
netvolante-dns go pp 285
netvolante-dns hostname host 286
netvolante-dns hostname host pp 286
netvolante-dns port 286
netvolante-dns retry interval 287
netvolante-dns retry interval pp 287
netvolante-dns server 287
netvolante-dns timeout 286
netvolante-dns timeout pp 286
netvolante-dns use 285
netvolante-dns use pp 285
nslookup 324
ntpdate 47

O

operation button function download 303
operation execute batch permit 304
operation external-memory download permit . . 300
operation http revision-up permit 61
operation usb-download permit 291
ospf area 242
ospf area network 242
ospf area stubhost 242
ospf configure refresh 238
ospf export filter 240
ospf export from ospf 239

ospf import filter 241
ospf import from 239
ospf log 246
ospf merge equal cost stub 246
ospf preference 238
ospf router id 238
ospf use 238
ospf virtual-link 243

P

ping 323
ping6 324
pp always-on 70
pp auth accept 141, 202
pp auth multi connect prohibit 142
pp auth myname 142
pp auth request 142, 201
pp auth username 141
pp backup 106
pp backup pp 106
pp backup recovery time 106
pp backup tunnel 106
pp bind 67, 82, 200, 309
pp disable 31, 322
pp enable 31, 321
pp encapsulation 77
pp keepalive interval 97
pp keepalive log 98
pp keepalive use 97
pp name 281
pp select 315
ppp bacp maxconfigure 155
ppp bacp maxfailure 155
ppp bacp maxterminate 154
ppp bacp restart 154
ppp bap maxretry 155
ppp bap restart 155
ppp bcp lanid 149
ppp bcp maxconfigure 149
ppp bcp maxfailure 150
ppp bcp maxterminate 149
ppp bcp restart 149
ppp bcp tinycomp 149
ppp ccp maxconfigure 152
ppp ccp maxfailure 152
ppp ccp maxterminate 151
ppp ccp no-encryption 203
ppp ccp restart 151
ppp ccp type 151, 200
ppp chap maxchallenge 145
ppp chap restart 145
ppp ipcp ipaddress 146
ppp ipcp maxconfigure 147
ppp ipcp maxfailure 147
ppp ipcp maxterminate 146
ppp ipcp msext 147
ppp ipcp remote address check 148
ppp ipcp restart 146
ppp ipcp vjc 146
ppp ipv6cp use 152
ppp ipxcp maxconfigure 148
ppp ipxcp maxfailure 148
ppp ipxcp maxterminate 148
ppp ipxcp restart 148
ppp lcp accm 312
ppp lcp acfc 143
ppp lcp magicnumber 143
ppp lcp maxconfigure 144
ppp lcp maxfailure 144
ppp lcp maxterminate 144
ppp lcp mru 143
ppp lcp pfc 144
ppp lcp restart 144
ppp lcp silent 145
ppp mp control 153
ppp mp divide 154
ppp mp interleave 227
ppp mp load threshold 153
ppp mp maxlink 153
ppp mp minlink 153
ppp mp timer 154
ppp mp use 152
ppp mscbcp maxretry 150
ppp mscbcp restart 150
ppp pap maxauthreq 145
ppp pap restart 145
pppoe access concentrator 156
pppoe auto connect 156
pppoe auto disconnect 156
pppoe disconnect time 157
pppoe invalid-session forced close 158
pppoe padi maxretry 156
pppoe padi restart 156
pppoe padr maxretry 157
pppoe padr restart 157
pppoe service-name 157
pppoe tcp mss limit 158
pppoe use 155
pptp call-id mode 201
pptp hostname 201
pptp keepalive interval 203
pptp keepalive log 203
pptp keepalive use 203
pptp service 200
pptp service type 200
pptp syslog 202
pptp tunnel disconnect time 202
pptp window size 201
pri leased channel 82
pri loopback active 326
pri loopback passive 326
provider auto connect forced disable 284
provider dns server 282
provider dns server pp 283
provider filter routing 283
provider interface dns server 282
provider interface name 283
provider ipv6 connect pp 284
provider ntp server 284
provider ntpdate 283
provider select 282
provider set 282
provider type 281

Q

queue class filter 224
queue interface class control 231
queue interface class filter list 228
queue interface class property 230
queue interface default class 229

queue interface default class secondary 229
queue interface length 228
queue interface length secondary 229
queue interface type 227
queue pp class filter list 228
queue pp class property 230
queue pp default class 229
queue pp length 228
queue pp type 227
queue tunnel class filter list 228
quit 315

R

radius account 209
radius account port 210
radius account server 210
radius auth 209
radius auth port 210
radius auth server 210
radius retry 211
radius secret 211
radius server 209
rdate 47
remote setup 318
remote setup accept 319
restart 36, 322
rip filter rule 104
rip preference 99
rip timer 104
rip use 98

S

save 31, 316
schedule at 294
sd use 298
security class 46
set-default-config 318
set-default-exec 318
show 39, 40, 41
show account 346
show account pp 346
show arp 332
show bridge learning 334
show command 42
show config 329
show config list 330
show config pp 329
show config tunnel 329
show diagnosis config port access 348
show diagnosis config port map 348
show dlci 332
show environment 329
show exec list 331
show file list 330
show history 346
show ip connection 338
show ip connection pp 338
show ip connection tunnel 338
show ip intrusion detection 339
show ip intrusion detection pp 339
show ip intrusion detection tunnel 339
show ip mroute 340
show ip rip table 333
show ip route 333
show ip secure filter 331
show ip secure filter pp 331
show ip secure filter tunnel 331
show ip traffic list 115
show ip traffic list pp 115
show ip traffic list tunnel 115
show ipsec sa 335
show ipsec sa gateway 335
show ipv6 address 330
show ipv6 address pp 330
show ipv6 address tunnel 330
show ipv6 connection 338
show ipv6 connection pp 338
show ipv6 connection tunnel 338
show ipv6 mrout fib 341
show ipv6 neighbor cache 334
show ipv6 ospf 343
show ipv6 rip table 334
show ipv6 route 333
show ipx ipxwan 334
show ipx route 334
show ipx sap 334
show line masterclock 330
show log 346
show nat descriptor address 335
show nat descriptor interface address 336
show nat descriptor interface address pp 336
show nat descriptor interface address tunnel . . . 336
show nat descriptor interface bind 335
show nat descriptor interface bind pp 335
show nat descriptor interface bind tunnel 335
show nat descriptor masquerade port summary 336
show pp connect time 339
show sshd public key 330
show status 332
show status backup 337
show status bgp neighbor 336
show status cooperation 343
show status dhcp 337
show status dhcpc 337
show status external-memory 345
show status heartbeat 344
show status ip igmp 341
show status ip inbound filter 343
show status ip keepalive 338
show status ip pim sparse 341
show status ip policy filter 344
show status ip policy service 344
show status ipv6 inbound filter 343
show status ipv6 mld 341
show status ipv6 policy filter 344
show status ipv6 policy service 344
show status mail service 340
show status netvolante-dns 339
show status netvolante-dns pp 339
show status ospf 336
show status packet-buffer 342
show status pp 332
show status pptp 336
show status qos 342
show status remote setup 345
show status sd 345
show status switching-hub macaddress 339
show status tunnel 340
show status upnp 340

show status usbhost 345
show status user 342
show status vlan 340
show status vrrp 335
show techinfo 345
show url filter 344
show url filter pp 344
show url filter tunnel 344
snmp community read-only 205
snmp community read-write 205
snmp display ipcp force 208
snmp host 204
snmp local address 204
snmp syscontact 205
snmp syslocation 205
snmp sysname 206
snmp trap community 207
snmp trap enable snmp 206
snmp trap host 207
snmp trap link-updown separate-l2switch-port . . 208
snmp trap send linkdown 206
snmp trap send linkdown pp 206
snmp trap send linkdown tunnel 206
snmp yrifppdisplayatmib2 207
snmp yriftunneldisplayatmib2 207
sntpd host 297
sntpd service 297
speed 224
speed pp 224
sshd client alive 63
sshd host 62
sshd host key generate 62
sshd listen 62
sshd service 61
sshd session 62
statistics 349
syslog debug 50
syslog execute command 51
syslog facility 49
syslog host 49
syslog info 50
syslog local address 50
syslog notice 49
syslog srcport 50
system led brightness 65
system packet-buffer 63
system power 51
system temperature threshold 53

T

tcp log 59
telnet 325
telnetd host 52
telnetd listen 51
telnetd service 51
telnetd session 52
tftp host 37, 57
time 47
timezone 47
traceroute 324
traceroute6 324
tunnel backup 197
tunnel backup pp 197
tunnel backup tunnel 197
tunnel disable 178
tunnel enable 178
tunnel encapsulation 178, 200
tunnel endpoint address 179, 200
tunnel endpoint name 202
tunnel name 281
tunnel select 315
tunnel template 198

U

upnp external address refer 288
upnp external address refer pp 288
upnp port mapping timer 289
upnp port mapping timer type 288
upnp syslog 289
upnp use 288
url filter 138
url filter log 140
url filter port 139
url filter reject 139
url filter use 139
url interface filter 138
url pp filter 138
url tunnel filter 138
usbhost config filename 292
usbhost exec filename 292
usbhost modem flow control 293
usbhost modem initialize 292
usbhost statistics filename prefix 291
usbhost syslog filename 290
usbhost use 290
user attribute 44

V

vlan interface 802.1q 295
vlan port mapping 295

W

wins server 147
wol send 327

1. コマンドリファレンスの見方

1.1 対応するプログラムのリビジョン

このコマンドリファレンスは、ヤマハルーターのファームウェア、Rev.6.03.34、Rev.7.00.30、Rev.7.01.53、Rev.8.01.27、Rev.8.02.43、Rev.8.03.76、Rev.9.00.37、Rev.10.00.38、Rev.10.01.01 に対応しています。
このコマンドリファレンスの印刷より後にリリースされた最新のファームウェアや、マニュアル類および差分については以下に示す URL の WWW サーバーにある情報を参照してください。

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

1.2 コマンドリファレンスの見方

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

[書式]　コマンドの入力形式を説明します。キー入力時には大文字と小文字のどちらを使用しても構いません。
コマンドの名称部分は太字 (**Bold face**) で示します。
パラメータ部分は斜体 (*Italic face*) で示します。
キーワードは標準文字で示します。
括弧 ([　]) で囲まれたパラメータは省略可能であることを示します。

[設定値]　コマンドの設定値の種類とその意味を説明します。

[説明]　コマンドの解説部分です。

[ノート]　コマンドを使用する場合に特に注意すべき事柄を示します。

[初期値]　コマンドの初期値 (デフォルト値) を示します。

[設定例]　コマンドの具体例を示します。

[適用モデル]　コマンドが適用できるモデル名称を示します。打ち消し線の引かれたモデルはこのコマンドが使用できません。

1.3 インタフェース名について

コマンドの入力形式において、ルーターの各インタフェースを指定するためにインタフェース名を利用します。
インタフェース名は、インタフェース種別とインタフェース番号を間に空白をおかずに続けて表記します。インタフェース種別には、"lan"、"bri"、"pri" があります。インタフェース番号は、インタフェースの種別ごとに起動時に検出された順番で振られていきます。
また、ヤマハリモートルーター RT300i の BRI 拡張モジュールのように、1 つのモジュールに複数のインタフェースがある場合には、インタフェース番号はモジュールに振られた番号とモジュール内の番号をピリオド (.) でつなげた形式となります。
lan インタフェースについては、LAN 分割機能を適用した場合に分割された LAN はピリオド (.) でつなげた形式となります。
RTX1200 では LAN 分割機能の拡張機能として VLAN インタフェースが使用できます。
タグ VLAN はスラッシュ (/) でつなげた形式となります。

例：

インタフェースの種類	インタフェース名
メインモジュール上の LAN	lan1
タグ VLAN	lan1/1, lan1/2, ..., lan1/8
LAN 分割機能の LAN	lan1.1, lan1.2, lan1.3, lan1.4
LAN 分割機能の拡張機能の LAN	vlan1,vlan2, ..., vlan8
RTX2000 本体上の LAN	lan1.1, lan1.2, ..., lan1.8
メインモジュール上の BRI	bri1
1 つ目の LAN モジュール	lan2
1 つ目の 8BRI モジュール	bri2.1, bri2.2, ..., bri2.8
2 つ目の 8BRI モジュール	bri3.1, bri3.2, ..., bri3.8
1 つ目の PRI モジュール	pri1

また、Rev.8.03 系以降では仮想的なインタフェースである loopback インタフェースと null インタフェースを指定できます。

インタフェースの種類	インタフェース名
LOOPBACK	loopback1, loopback2, ... loopback9
NULL	null

Rev.10.00.38 以降では仮想的なインタフェースである ブリッジインタフェースを指定できます。

インタフェースの種類	インタフェース名
BRIDGE	bridge1

1.4　no で始まるコマンドの入力形式について

コマンドの入力形式に **no** で始まる形のものが並記されているコマンドが多数あります。**no** で始まる形式を使うと、特別な記述がない限り、そのコマンドの設定を削除し、初期値に戻します。

また、***show config*** コマンドでの表示からも外します。言い換えれば、**no** で始まる形式を使わない限り、入力されたコマンドは、たとえ初期値をそのまま設定する場合でも、***show config*** コマンドでの表示の対象となります。

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

1.5　コマンドの入力文字数とエスケープシーケンスについて

1 つのコマンドとして入力できる文字数は、コマンド本体とパラメータ部分を含めて最大 4095 文字以内です。

また、コマンドのパラメータ部分に以下の特殊文字を入力する場合には表に示す方法で入力してください。

特殊文字	入力
?	¥? '?' "?"
#	¥# '#' "#"
¥	¥¥

特殊文字	入力
'	¥' "'"
"	¥" '"'
空白	¥ の後ろに空白 ' ' " "

1.6　相手先情報番号のモデルによる違いについて

相手先情報番号はモデルによって使用できる数値の範囲が異なります。

モデル名称	相手先情報番号の範囲
RTX2000/RTX1500/RT300i/RTX1200	1 - 100
RTX1100/RTX1000/RT107e/SRT100	1 - 30
RTX3000/RT250i	1 - 150

1.7　工場出荷設定値について

RT107e、SRT100、RTX1200 では、お買い上げ頂いた状態および ***cold start*** コマンドを実行した直後の状態は、本書に記載されたコマンドの初期値が適用されるわけではなく、以下に示す工場出荷設定になっています。

```
ip lan1 address 192.168.100.1/24
dhcp service server
dhcp server rfc2131 compliant except remain-silent
dhcp scope 1 192.168.100.2-192.168.100.191/24
```

さらに SRT100 では、ログインパスワードと管理者パスワードとして doremi が設定されています。

2.　コマンドの使い方

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

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

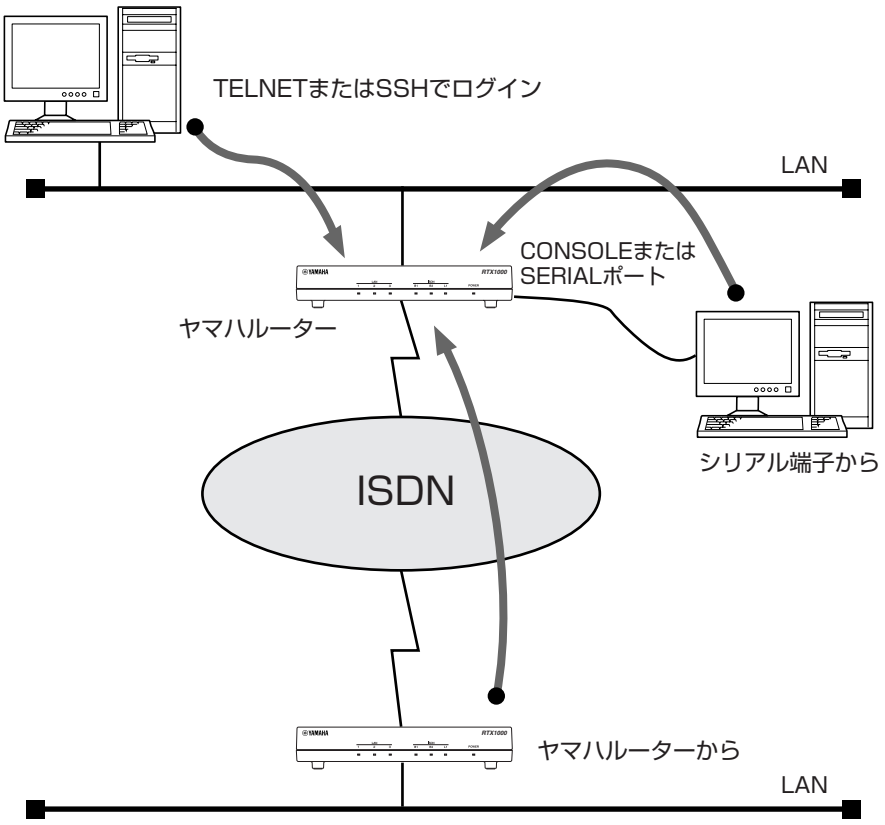
2.1　コンソールについて

各種の設定を行うためには、ヤマハルーターの CONSOLE ポートにシリアル端末を接続する方法と、LAN 上のホストから TELNET、または SSH (SSH サーバー機能対応機種のみ) でログインする方法、ISDN 回線や専用線を介して別のヤマハルーターからログインする方法の 3 つがあります。

ヤマハルーターへのアクセス方法
CONSOLE または SERIAL ポートに接続した端末からアクセス
LAN 上のホストから TELNET または SSH でログイン
ISDN 回線や専用線を介して別のヤマハルーターからログイン

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

TELNET 複数セッション機能および SSH サーバー機能に対応した機種については、TELNET または SSH による同時アクセスが最大 8 ユーザまで可能です。また複数のユーザが同時に管理ユーザになることができ、異なるホストから同時に設定を行うこともできます。そのほか、各ユーザは現在アクセスしている全ユーザのアクセス状況を確認することができ、管理ユーザならば他のユーザの接続を強制的に切断させることもできます。



2.1.1　コンソールによる設定手順

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

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

コンソールコマンドの具体的な内容については、本書の第 3 章以降をご覧ください。

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

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

設定手順のおおまかな流れは次のようになります。

1. 一般ユーザとしてログインした後、***administrator*** コマンドで管理ユーザとしてアクセスします。
   この時管理パスワードが設定してあれば、管理パスワードの入力が必要です。

2. 回線を接続していない相手の相手先情報を変更する場合には、**pp disable** コマンドを実行してから相手先情報の内容を変更してください。回線が接続されている場合には、***disconnect*** コマンドでまず回線を手動切断しておきます。

3. 相手先情報の内容を各種コマンドを使用して変更します。

4. **pp enable** コマンドを実行します。

5. ***save*** コマンドを実行して、不揮発性メモリに設定内容を保存します。

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

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

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

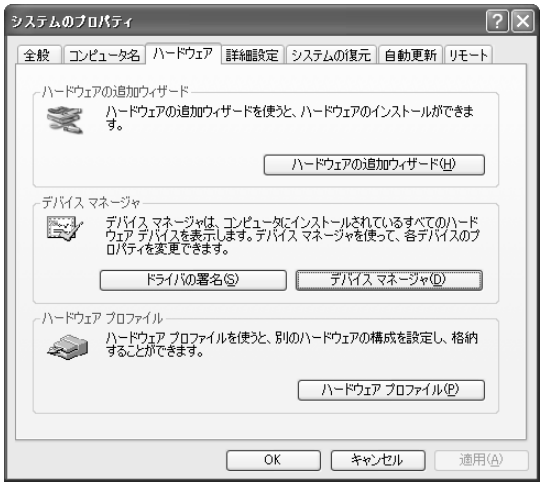
【ご注意】

- ご購入直後の起動や ***cold start*** 後にはログインパスワードも管理パスワードも設定されていません。セキュリティ上、ログインパスワードと管理パスワードの設定をお勧めします。なお SRT100 では、工場出荷状態でパスワードとして doremi が設定されています。
- ヤマハルーターのご購入直後の起動でコンソールから各種の設定が行える状態になりますが、実際にパケットを配送する動作は行いません。
- セキュリティの設定や、詳細な各種パラメータなどの付加的な設定に関しては、個々のネットワークの運営方針などに基づいて行ってください。

2.1.2　CONSOLE または SERIAL ポートからの設定

ここでは、Windows XP の『ハイパーターミナル』を使用する場合を例に説明します。シリアルケーブルの接続は事前にすませておきます。

1. ［スタート］メニューから［マイ コンピュータ］を選び、「システムのタスク」欄にある「システム情報を表示する」を選びます。「システムのプロパティ」ウィンドウが開いたら、[ハードウェア] タブを押します。

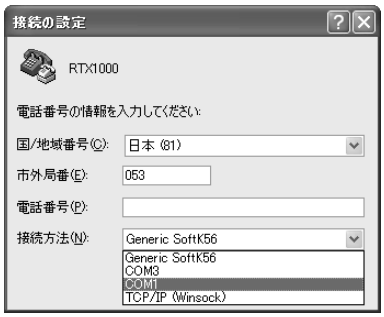


2. [デバイス マネージャ] をクリックします。
「ポート (COM と LPT)」アイコンをダブルクリックして開き、「通信ポート」の「COMx」という表現部分を調べます。通常は「COM1」の場合が多いでしょう。この COM ポート番号は、手順 5 で必要になるために覚えておきます。

3.「デバイス マネージャ」ウィンドウを閉じます。

4. ［スタート］メニューから［すべてのプログラム］－［アクセサリ］－［通信］－［ハイパーターミナル］を選びます。「接続の設定」ウィンドウが開いたら、名前欄に適切な名前を入力して [OK] をクリックします。

5.「接続方法」欄から、手順 2 で調べた COM ポートを選択して [OK] をクリックします。

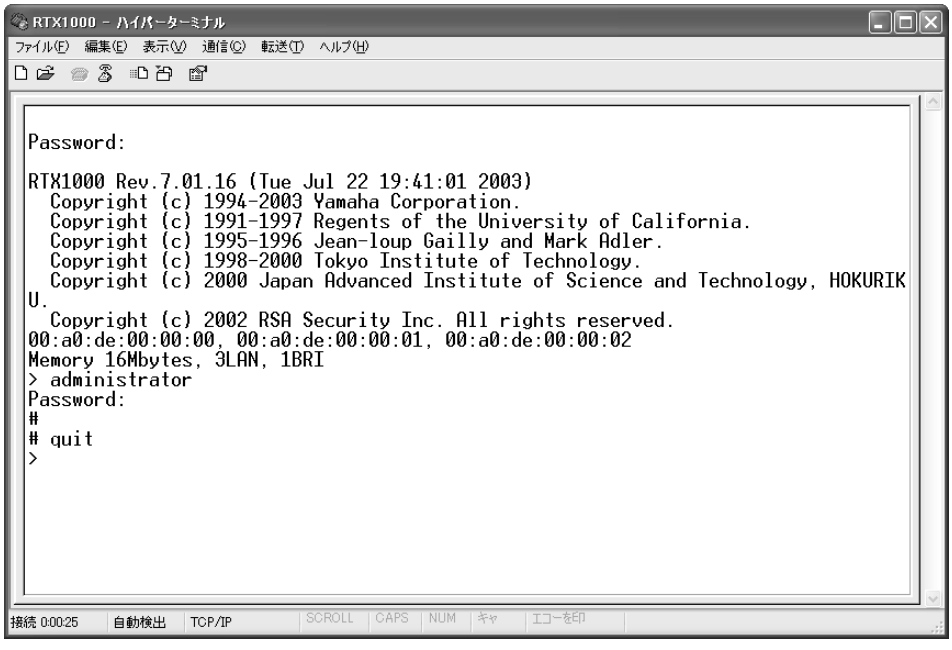


6.「COMx のプロパティ」ウィンドウが開いたら、[ビット／秒] を 9600、[データビット] を 8, [パリティ] をなし、[ストップビット] を 1、[フロー制御] を Xon/Xoff にして、[OK] をクリックします。

7.「Password:」と表示されたら、ログインパスワードを入力してから Enter キーを押します。

※ TELNET 複数セッション機能対応機種で設定した名前ありユーザでログインする場合は、何も入力せずに Enter キーを押します。次に「Username:」と表示され、ユーザ名の入力待ち状態となります。ここで、設定したユーザ名を入力して Enter キーを押し、続いてユーザパスワードを入力します。

何も表示されないときは、1 度 Enter キーを押します。
「>」が表示されると、コンソールコマンドを入力できるようになります。
以下の例は、RTX1000 にログインした場合の表示です。



[ノート]
- 「**help**」と入力してから Enter キーを押すと、キー操作の説明が表示されます。
- 「***show command***」と入力してから Enter キーを押すと、コマンド一覧が表示されます。

8.「***administrator***」と入力してから、Enter キーを押します。

9.「Password:」と表示されたら、管理パスワードを入力します。
「#」が表示されると、各種のコンソールコマンドを入力できます。

10. コンソールコマンドを入力して、設定を行います。

11. 設定が終わったら、「**save**」と入力してから Enter キーを押します。
コンソールコマンドで設定した内容が、本機の不揮発性メモリに保存されます。

12. 設定を終了するには、「**quit**」と入力してから Enter キーを押します。

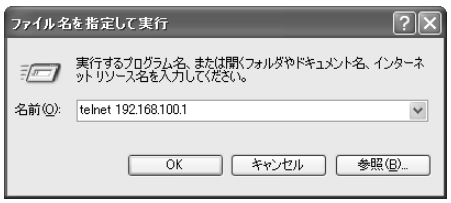
13. コンソール画面を終了するには、もう 1 度「**quit**」と入力してから Enter キーを押します。

2.1.3　TELNET による設定

ここでは、Windows XP の TELNET を使用する場合を例に説明します。ヤマハルーターの IP アドレスは 192.168.100.1 とした場合の例です。

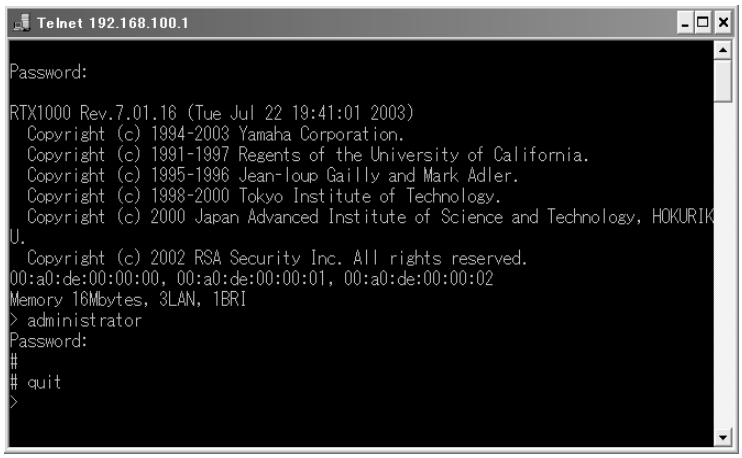
1.［スタート］メニューから［ファイル名を指定して実行］を選びます。

2.「telnet 192.168.100.1」と入力してから、［OK］をクリックします。
本機の IP アドレスを変更している場合には、「192.168.100.1」のかわりにその IP アドレスを入力します。



3.「Password:」と表示されたら、ログインパスワードを入力してから Enter キーを押します。
※ TELNET 複数セッション機能対応機種で設定した名前ありユーザでログインする場合は、何も入力せずに Enter キーを押します。次に「Username:」と表示され、ユーザ名の入力待ち状態となります。ここで、設定したユーザ名を入力して Enter キーを押し、続いてユーザパスワードを入力します。

何も表示されないときは、1 度 Enter キーを押します。
「>」が表示されると、コンソールコマンドを入力できるようになります。



［ノート］　・「**help**」と入力してから Enter キーを押すと、キー操作の説明が表示されます。
・「***show command***」と入力してから Enter キーを押すと、コマンド一覧が表示されます。

4. 「***administrator***」と入力してから、Enter キーを押します。

5. 「Password:」と表示されたら、管理パスワードを入力します。
「#」が表示されると、各種のコンソールコマンドを入力できます。

6. コンソールコマンドを入力して、設定を行います。

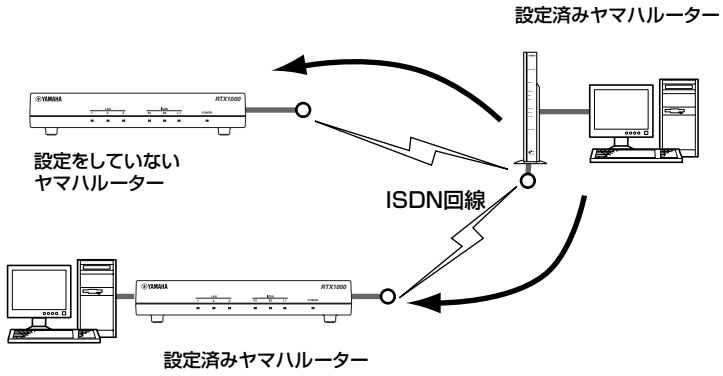
7. 設定が終わったら、「***save***」と入力してから Enter キーを押します。
コンソールコマンドで設定した内容が、本機の不揮発性メモリに保存されます。

8. 設定を終了するには、「**quit**」と入力してから Enter キーを押します。

9. コンソール画面を終了するには、もう 1 度「**quit**」と入力してから Enter キーを押します。

2.1.4　リモートセットアップ

すでにヤマハルーターをお使いの場合は、離れた場所のルーターでも ISDN 回線や専用線経由で設定できます。これを「リモートセットアップ」といいます。ISDN 回線や専用線経由で相手のルーターに直接接続するので、プロバイダに契約していなくても、インターネット接続できない状態でも設定できます。



リモートセットアップを拒否するように設定できるため、拒否に設定しておけば、不特定の相手からの侵入を防げます。

リモートセットアップはコンソールから行います。コンソールを使う方法は、前節の「CONSOLE または SERIAL ポートからの設定」または「TELNET による設定」を参照してください。リモートセットアップのコマンドは ***remote setup*** です。

相手のヤマハルーターへのログインが完了すると、設定したいルーターをコンソールコマンドで設定できるようになります。

【ご注意】　・ヤマハルーター以外のルーターからリモートセットアップすることはできません。
・FTTH や CATV、ADSL などの WAN ポート経由で、リモートセットアップすることはできません。

2.2　SSH サーバーについて

SSH サーバー機能に対応した機種では、LAN 上のホストから SSH でログインして設定することができます。このときホスト側で使用する SSH クライアントは、MacOS X の『ターミナル』アプリケーションや UNIX 環境では標準的に搭載されており、実行することができますが、Windows 系 OS では標準では搭載されていません。SSH クライアントが搭載されていない環境では、フリーソフトなどで SSH クライアント機能のあるものを用意してください。

2.2.1　使用に当たっての注意事項

SSH サーバー機能では以下の機能をサポートしていないことに注意してください。

- SSH プロトコルバージョン 1
- パスワード認証以外のユーザ認証 (ホストベース認証、公開鍵認証、チャレンジ・レスポンス認証、GSSAPI 認証)
- ポートフォワーディング (X11/TCP 転送)
- Gateway Ports(ポート中継)
- 空パスワードの許可
- scp
- sftp

2.2.2　SSH サーバーの設定

SSH サーバー機能は、工場出荷設定では使用しないよう設定されています。SSH サーバー機能を使用できるようにするまでの設定手順は以下の通りです。

1. ***login user*** コマンドで名前ありユーザを登録します。SSH ではログイン時のユーザ名の入力が必須となるため、事前に必ず名前ありユーザを登録しなければなりません。

2. 次に、***sshd host key generate*** コマンドで SSH サーバーのホスト鍵を生成します。このコマンドによって DSA または RSA の公開鍵、および秘密鍵のペアが生成されます。ただし機種によってはこのコマンドの処理に数十秒ほど時間がかかる場合があります。

3. 最後に ***sshd service*** コマンドで SSH サーバー機能を有効にします。

2.3　TFTP について

ヤマハルーターに設定した項目は、TFTP により LAN 上のホストから設定ファイルとして読み出すことができます。またホスト上の設定ファイルを本機に読み込ませて設定を行うこともできます。

TFTP は、Windows XP や MacOS X の『ターミナル』アプリケーション、UNIX 環境で標準的に搭載されており、実行することができます。TFTP が搭載されていない環境では、フリーソフトなどで TFTP クライアント機能のあるものを用意してください。この時、ヤマハルーターは TFTP サーバーとして動作します。

設定ファイルは全体の設定を記述したものであり、特定部分の設定だけを読み出したり差分点だけを書き込んだりすることはできません。設定ファイルは Windows のメモ帳等で直接編集できるテキストファイル (シフト JIS、CRLF 改行) です。

【ご注意】

- 設定ファイルの内容はコマンドの書式やパラメータの指定などの内容が正しく記述されている必要があります。間違った書式や内容があった場合には、その内容は動作に反映されず無視されます。

- **TFTP** により設定ファイルを読み込む場合において **line type** コマンドの設定変更を行う場合は、設定の最後に **restart** コマンドが必要なことに注意してください。

2.3.1　TFTP による設定手順

TFTP により設定ファイルをやりとりするためには、ヤマハルーター側にあらかじめアクセス許可するための設定が必要です。まず **tftp host** コマンドを使用し、本機にアクセスできるホストを設定します。工場出荷設定ではどのホストからもアクセスできない設定になっていることに注意してください。

次に、LAN 上のホストから TFTP コマンドを実行します。使用するコマンドの形式は、そのホストの OS に依存します。次の点に注意して実行してください。

- 本機の IP アドレス
- 転送モードは“アスキー”、"ascii" または“文字”にします。
- 本機に管理パスワードが設定されている場合には、ファイル名称の後ろに管理パスワードを指定する必要があります。
- 読み出したり書き込んだりする設定ファイル名は“config”という名称に固定されています。

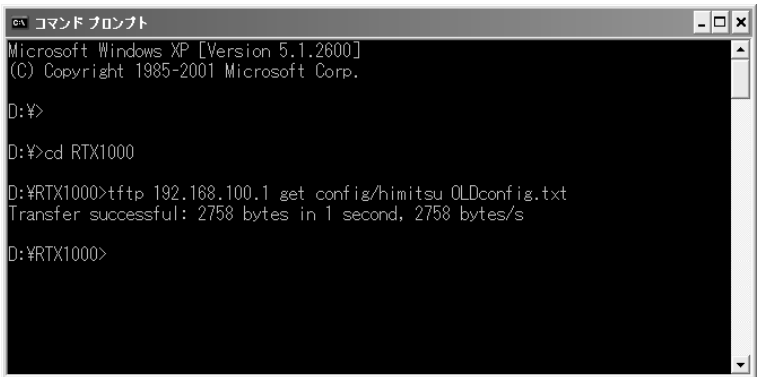
2.3.2　設定ファイルの読み出し

ここでは、Windows XP から設定ファイルを読み出す場合の例を示します。ヤマハルーターのコンソール操作ではないことに注意してください。この例では、ヤマハルーターの IP アドレスを 192.168.100.1、管理パスワードは“himitsu”、Windows に新しくできるファイルの名称を“OLDconfig.txt”とします。

1. ［スタート］メニューから［すべてのプログラム］－［アクセサリ］－［コマンド プロンプト］を選びます。

2. 設定ファイルを保存するディレクトリに移動します。

3. 「tftp 192.168.100.1 get config/himitsu OLDconfig.txt」と入力してから、Enter キーを押します。



2.3.3　設定ファイルの書き込み

ここでは、Windows XP から設定ファイルを書き込む場合の例を示します。ヤマハルーターのコンソール操作ではないことに注意してください。この例では、ヤマハルーターの IP アドレスを 192.168.100.1、管理パスワードは“himitsu”、書き込むべき Windows 上のファイルの名称を“NEWconfig.txt”とします。

1. ［スタート］メニューから［すべてのプログラム］－［アクセサリ］－［コマンド プロンプト］を選びます。
2. 設定ファイルの保存されているディレクトリに移動します。
3. 「tftp 192.168.100.1 put NEWconfig.txt config/himitsu」と入力してから、Enter キーを押します。

2.4　コンソール使用時のキーボード操作について

一画面に収まらない行数の情報を表示する場合は、***console lines*** コマンドで設定された行数分を表示した段階で表示をストップさせ、画面下に「--- つづく ---」と表示されます。

この状態から残りを表示させる場合には、スペースキーを押します。Enter キーを押すと新しい一行を表示します。これらの操作を繰り返し、最後まで表示すると自動的にコマンド入力ができる状態にもどります。

最後まで表示せずにこの段階で表示を終了させたい場合には、q キーを押します。この後コマンドが入力できる状態にもどります。

一画面に収まらない行数の情報を表示する場合にもストップさせたくなければ、***console lines*** infinity コマンドを実行します。

キーボード操作	説明・備考
SPACE	1 画面先に進める
ENTER	1 行先に進める
RETURN	
q	終了
Ctrl-C	

show config, ***show config list***, ***show config pp***, ***show file list***, ***show log*** と同じ内容を、UNIX コマンドの less 風に表示する場合には、それぞれ、***less config***, ***less config list***, ***less config pp***, ***less file list***, ***less log*** コマンドを使用します。

キーボード操作	説明・備考
{n} f	{n} 画面先に進める
{n} Ctrl-F	
{n} SPACE	
{n} b	{n} 画面後ろに戻す
{n} Ctrl-B	
{n} j	{n} 行先に進める
{n} Ctrl-J	
{n} Ctrl-E	
{n} Ctrl-M	
{n} ENTER	
{n} RETURN	
{n} k	{n} 行後ろに戻す
{n} Ctrl-K	
{n} y	
{n} Ctrl-Y	
{n} Ctrl-P	
{n} d	{n} 半画面先に進める
{n} Ctrl-D	
{n} u	{n} 半画面後ろに戻す
{n} Ctrl-U	
{n} g	{n} 行目へ移動 {n} 省略時は先頭行
{n} G	{n} 行目へ移動 {n} 省略時は末尾行
r	現在の画面の書き直し
Ctrl-R	
Ctrl-L	
q	終了
Ctrl-C	

説明：

n	数字のキー入力で整数値を表します。省略時は '1' です。
Ctrl-X	[Ctrl] キーを押しながら [X] キーを押すことを示します。

2.5　「show」で始まるコマンド

「show」で始まるコマンドが表示する内容から、指定した検索パターンに一致する内容だけを抜き出して表示することができます。あるいは「show」で始まるコマンドが表示する内容をページ単位で表示しながら、後ろに戻ったり、指定した検索パターンに一致する内容を検索したりすることができます。

これらの機能は「show」で始まるすべてのコマンドで利用できます。

2.5.1　show コマンドの表示内容から検索パターンに一致する内容だけを抜き出す

[書式]　**show** *[...]* | **grep** *[-i] [-v] [-w] pattern*

[設定値]
- -i ..... *pattern* 中の英大文字 / 小文字を区別せず検索する
- -v ..... *pattern* に一致しなかった行を表示する
- -w ..... *pattern* が単語に一致する時だけ表示する
- *pattern* ..... 検索パターン

[説明]　**show** コマンドの表示内容から検索パターンである *pattern* に一致する行だけを抜き出して表示する。
-i オプションを指定した時には、*pattern* 中の英大文字 / 小文字を区別せずに検索する。例えば、-i オプションがある時には 'abc' という *pattern* は 'abc' や 'ABC'、'aBc'、'ABc' などに一致する。一方、-i オプションがなければ、'abc' は 'abc' としか一致しない。
-v オプションを指定した時には、*pattern* に一致しない行を表示する。
-w オプションを指定した時には、*pattern* に一致するのは単語だけとなる。例えば、-w オプションがある時には 'IP' という *pattern* は 'IPv4' や 'IPv6' とは一致しないが、' IP '(前後に空白がある) や '[IP]' には一致する。一方、-w オプションが無ければ先に上げた例にはすべて一致する。
pattern は限定された正規表現である。一般的な正規表現では多くの特殊文字を使って多様な検索パターンを構成できるが、ここで実装されているのは以下の特殊文字のみである。

文字	意味	使用例	一致する文字列の例
.	任意の 1 文字に一致する	a.b	aab, aXb, a-b
?	直前の文字が 0 回または 1 回出現するパターンに一致する	b?c	ac, abc
*	直前の文字が 0 回以上繰り返すパターンに一致する	ab*c	ac, abc, abbc, abbbbbbbbc
+	直前の文字が 1 回以上繰り返すパターンに一致する	ab+c	abc, abbc, abbbbbbbbc
|	前後の文字のいずれかに一致する	ab|cd	abd, acd
[ ]	[ ] 内の文字のいずれかに一致する	a[bc]d	abd, acd
[^]	[ ] 内の文字以外のものに一致する	a[^bc]d	aad, axd
^	行の先頭に一致する	^abc	abc で始まる行
$	行の末尾に一致する	abc$	abc で終わる行
( )	文字列などをグループとして扱う	(ab|cd)	ab, cd
¥	続く特殊文字の効果を打ち消す	a¥.c	a.c

また、grep は一行に繰り返し指定することもできる。更に、**less** コマンドと同時に使用することもできる。
pattern 中の文字として '¥','?','|' を使用する場合は、それらの文字の前に '¥' をもう一つ重ねて入力しなければならない。

Rev.8.02.40 以降で使用可能。

[設定例]　*show config | grep ip | grep lan*
show config | grep ip | less

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	RT250i	RT107e	SRT100

2.5.2　show コマンドの表示内容を見やすくする

[書式]　***show*** *[...]* | ***less***

[説明]　**show** コマンドの表示内容を 1 画面単位で表示し、最終行でコマンドを受け付ける。
表示内容が 1 画面に満たない場合には、すべての内容を表示して終了する。
コマンドは、数値プレフィクスとコマンド文字を入力することで実行される。数値プレフィクスはオプションで省略できる。数値プレフィクスを省略した場合には 1 と見なされる。検索コマンドでは、コマンド文字の後に検索文字列を入力できる。
コマンドには以下の種類がある。

コマンド	内容 (数値プレフィクスを N とする)
q	less を終了する。
スペース	N 画面先に進む。
b	N 画面後ろに戻る。
j, ENTER	N 行先に進む。
k	N 行後ろに戻る。
g	N 行目にジャンプする。
G	N 行目にジャンプする。ただし、数値プレフィクスを省略した時には、最終行にジャンプする。
/	コマンド文字後に入力された検索パターンを前方に検索する。 検索パターンは grep コマンドと同じものである。
?	コマンド文字後に入力された検索パターンを後方に検索する。 検索パターンは grep コマンドと同じものである。
n	最後に入力された /、あるいは ? と同じ検索パターンで同じ方向に検索する。
N	最後に入力された /、あるいは ? と同じ検索パターンで逆方向に検索する。

Rev.8.02.40 以降で使用可能。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	RT250i	RT107e	SRT100

2.5.3　外部メモリへのリダイレクト機能

[書式]　**show** *[...] > name*

[設定値]　◦ *name*..... ファイル名
- usb1:*filename*.....USB メモリ内のファイル (*filename* は 64 文字以内)
- sd1:*filename*.....microSD メモリカード内のファイル (*filename* は 64 文字以内)

[説明]　**show** コマンドの実行結果を外部メモリに保存させることができるリダイレクト ('>') により指定されたファイルは、常に新規ファイルとして生成される。このため、同名のファイルが外部メモリ中に存在している場合、ファイルは置き換えられる。
パイプ ('|') と併用することで必要な行のみをファイルとして保存させることができる。
保存ファイルの暗号化には対応していない。

[ノート]　リダイレクトの後にパイプ ('|') は指定できない。

リダイレクトを複数回指定できない。
```
# show log > usb1:log.txt > usb2:log.txt
# show log >> usb1:log.txt
```

show 以外から始まるコマンドは適用外となる。
```
# ip filter 1 pass * * > usb1:filter.txt
```

less から始まるコマンドも適用外となる。
```
# less log > usb1:log.txt
```

外部メモリについて、以下の状態では本機能は実行できない。
・接続されていない状態
・ボタンを押された状態
・使用を禁止されている状態
・メモリの容量が不足している状態
この場合、書き込みに成功したサイズ分のファイルが生成される。

[設定例]　show log の内容を USB メモリに保存
```
# show log > usb1:log.txt
```
show config の内容を USB メモリに保存
```
# show config > usb1:config.txt
```

show status pp 1 の内容を microSD カードに保存
```
# show status pp 1 > sd1:status_pp1.txt
```
show techinfo の内容を microSD カードに保存
```
# show techinfo > sd1:techinfo.txt
```

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

3. ヘルプ

3.1 コンソールに対する簡易説明の表示

[書式]　**help**

[設定値]　なし

[説明]　コンソールの使用方法の簡単な説明を表示する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

3.2 コマンド一覧の表示

[書式]　***show command***

[設定値]　なし

[説明]　コマンドの名称とその簡単な説明を一覧表示する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

4. 機器の設定

4.1 ログインパスワードの設定

[書式]　***login password***

[設定値]　なし

[説明]　一般ユーザとしてログインするためのパスワードを 32 文字以内で設定する。パラメータはなく、コマンド入力後にプロンプトに応じて改めてパスワードを入力する形になる。
パスワードに使用できる文字は、半角英数字および記号 (7bit ASCII Code で表示可能なもの)。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

4.2 ログインパスワードの暗号化保存

[書式]　***login password encrypted***

[説明]　無名ユーザのパスワードを 32 文字以内で設定し、暗号化して保存する。パラメータはなく、コマンド入力後にプロンプトに応じて改めてパスワードを入力する形になる。
パスワードに使用できる文字は、半角英数字および記号 (7bit ASCII Code で表示可能なもの)。

[ノート]　パスワードを暗号化して保存する場合は本コマンドを、平文で保存する場合は ***login password*** コマンドを使用する。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

4.3 管理パスワードの設定

[書式]　***administrator password***

[設定値]　なし

[説明]　管理ユーザとしてルーターの設定を変更するための管理パスワードを 32 文字以内で設定する。パラメータはなく、コマンド入力後にプロンプトに応じて改めてパスワードを入力する形になる。
パスワードに使用できる文字は、半角英数字および記号 (7bit ASCII Code で表示可能なもの)。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

4.4 管理パスワードの暗号化保存

[書式]　***administrator password encrypted***

[説明]　管理ユーザのパスワードを 32 文字以内で設定し、暗号化して保存する。パラメータはなく、コマンド入力後にプロンプトに応じて改めてパスワードを入力する形になる。
パスワードに使用できる文字は、半角英数字および記号 (7bit ASCII Code で表示可能なもの)。

[ノート]　パスワードを暗号化して保存する場合は本コマンドを、平文で保存する場合は ***administrator password*** コマンドを使用する。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

4.5　ログインユーザ名とログインパスワードの設定

[書式]　**login user** *user* [*password*]
login user *user* encrypted *password*
no login user *user* [*password*]

[設定値]
- *user*.....ユーザ名 (32 文字以内)
- *password*.....パスワード (32 文字以内)

[説明]　ログインユーザ名とパスワードを設定する。

登録できるユーザは最大 32 人。

ユーザ名に使用できる文字は、半角英数字およびハイフン (-)、アンダーバー (_)。

第 1 書式では、パスワードは平文で入力し、暗号化して保存される。また、パスワードを省略すると、コマンド入力後にプロンプトに応じて改めてパスワードを入力する形になる。パスワードに使用できる文字は、半角英数字および記号 (7bit ASCII Code で表示可能なもの)。

第 2 書式では、*password* に暗号化されたパスワードを入力する。

TFTP で設定を取得した場合は、パスワードが暗号化されて保存されているため、常に第 2 書式の形で表示される。

[ノート]　同一のユーザ名を複数登録することはできない。

既に登録されているユーザ名で設定を行った場合は、元の設定が上書きされる。

syslog execute command を on に設定している場合には、設定パスワードがログに残ることを防ぐために、パスワードを省略した書式で入力するか、一時的に **syslog execute command** を off に設定する、さもなくば **clear log** を実行するなどの操作を行うことが望ましい。

[初期値]　設定ユーザなし

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

4.6　ユーザの属性を設定

[書式]　**user attribute** [*user*] *attribute=value* [*attribute=value...*]
no user attribute [*user...*]

[設定値]
- *user*
  - 登録されているユーザ名
  - *(すべてのユーザ)
- *attribute=value*.....ユーザ属性

[説明]　ユーザの属性を設定する。属性には、以下のものがある。

attribute	*value*	説明
administrator	on	**administrator** コマンドにより管理ユーザに昇格することができる。また GUI の管理者ページへ接続することができる。
	off	**administrator** コマンドにより管理ユーザに昇格することができない。また GUI の管理者ページへ接続することができない。
connection	off	すべての接続を禁止する。
	all	すべての接続を許可する。
	serial	シリアルコンソールからの接続を許可する。
	telnet	TELNET による接続を許可する。
	ssh	SSH による接続を許可する。
	remote	リモートセットアップによる接続を許可する。
	http	GUI 設定画面への接続を許可する。
host	IPアドレス	指定したホストからの接続を許可する。
	any	すべてのホストからの接続を許可する。
	インタフェース名	指定したインタフェースからの接続を許可する。
multi-session	on	同一ユーザ名による TELNET、SSH または HTTP での複数接続を許可する。
	off	同一ユーザ名による TELNET、SSH または HTTP での複数接続を禁止する。

attribute	*value*	説明
login-timer	30..21474836; SRT100 の場合は 120..21474836, clear	ログインタイマを設定する。

[ノート]　*user* を省略した場合は、無名ユーザの属性を設定する。

user をアスタリスク (*) に設定した場合は、すべてのユーザに対して設定を有効にする。ただし、ユーザ名を指定した設定がされている場合は、その設定が優先される。

すでに管理ユーザに昇格しているユーザに対して、このコマンドで administrator 属性を off に変更しても、そのユーザは **exit** コマンドにより一般ユーザに降格するか、あるいはログアウトするまでは管理ユーザで居続けることができる。また GUI の管理者ページへの接続が制限されるのは Rev.10 以降のファームウェアである。

connection 属性では、off、*all* 以外の値はコンマ (,) でつないで複数指定することができる。また http を指定して GUI 設定画面への接続を設定できるのは Rev.10 以降のファームウェアである。

すでに接続しているユーザに対して、このコマンドで connection 属性または host 属性により接続を禁止しても、そのユーザは切断するまでは接続を維持し続けることができる。

host 属性では、TELNET、SSH 及び HTTP で接続できるホストを設定する。指定できる IP アドレスは、1 個の IP アドレスまたは間にハイフン (-) をはさんだ IP アドレス (範囲指定)、およびこれらをコンマ (,) でつないだものである。

multi-session 属性では、TELNET または SSH での複数接続の可否を設定する。この属性を off に変更しても、シリアルと TELNET やリモートセットアップと SSH など、接続方法が異なる場合は同じユーザ名で接続することができる。

すでに複数の接続があるユーザに対して、このコマンドで multi-session 属性を off に変更しても、そのユーザは切断するまでは接続を維持し続けることができる。

無名ユーザに対しては SSH による接続を許可することができない。

無名ユーザに対しては TELNET での複数接続はできない。

TELNET、SSH または HTTP で接続した場合、login-timer 属性の値が clear に設定されていても、タイマ値は 300 秒として扱う。

login timer コマンドの設定値よりも、本コマンドの login-timer 属性の設定値が優先される。

Rev.10.00.31 で login-timer 属性の下限値を 30 から 120 に変更した。

本コマンドにより、すべてのユーザの接続を禁止する、またはすべてのユーザが管理ユーザに昇格できないといった設定を行った場合、ルーターの設定変更や状態確認などができなくなるので注意する必要がある。

[初期値]　*administrator = on*
connection = serial,telnet,remote,ssh,http
host = any
multi-session = on
login-timer = 300

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

4.7　他のユーザの接続の強制切断

[書式]　**disconnect user** *user* [*/connection* [*no*]]
disconnect user [*user*] */connection* [*no*]

[設定値]
- *user*.....ユーザ名
- *connection*.....接続種別 (telnet, serial, remote, ssh, http)
- *no*.....接続番号

[説明]　他ユーザの接続を切断する。

show status user コマンドで表示された接続状況からパラメータを指定する。

無名ユーザを切断する場合は、第二書式で *user* を省略した形で指定する。

パラメータを省略した場合は、指定したパラメータと一致するすべての接続を切断する。

[ノート]　自分自身のセッションを切断することはできない。
http を指定できるのは Rev.10 以降のファームウェアである。

[設定例]　例 1) ユーザ名「test」でログインしているすべての接続を切断する。
disconnect user test

例 2) TELNET で接続しているすべてのユーザを切断する。
disconnect user /telnet

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

4.8　セキュリティクラスの設定

[書式]　**security class** *level forget* [*telnet*]
no security class [*level forget telnet*]

[設定値]
- *level*
  - 1.....シリアルでも、TELNET、SSH でも遠隔地のルーターからでもログインできる
  - 2.....シリアルと TELNET と SSH からは設定できるが、遠隔地のルーターからはログインできない
  - 3.....シリアルからのみログインできる
- *forget*
  - on.....設定したパスワードの代わりに "w,lXlma" (ダブリュー、カンマ、エル、エックス、エル、エム、エー) でもログインでき、設定の変更も可能になる。ただしシリアルのみ
  - off.....パスワードを入力しないとログインできない
- *telnet*
  - on..... TELNET クライアントとして **telnet** コマンドが使用できる
  - off..... **telnet** コマンドは使用できない

[説明]　セキュリティクラスを設定する。

[ノート]　**remote setup accept** コマンドにより、遠隔地のルーターからのログイン (**remote setup**) を細かくアクセス制限することができる。遠隔地のルーターからのログイン機能は、回線交換あるいは専用線を利用するため、それらに接続できる機種だけが持つ機能である。設定を変更したときに変更した値よりも多くのユーザが接続している場合は、接続しているユーザはそれを維持することができるが、接続しているユーザ数が設定値より少なくなるまで新たな接続は許可しない。

[初期値]　*level* = 1
forget = on
telnet = off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

4.9　タイムゾーンの設定

[書式]　**timezone** *timezone*
no timezone [*timezone*]

[設定値]　◦ *timezone*..... その地域と世界標準時との差
- jst..... 日本標準時 (+09:00)
- utc..... 世界標準時 (+00:00)
- 時刻：分 (-12:00 .. +11:59)

[説明]　タイムゾーンを設定する。

[初期値]　jst

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

4.10　現在の日付けの設定

[書式]　**date** *date*

[設定値]　◦ *date*..... yyyy-mm-dd または yyyy/mm/dd

[説明]　現在の日付けを設定する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

4.11　現在の時刻の設定

[書式]　**time** *time*

[設定値]　◦ *time*..... hh:mm:ss

[説明]　現在の時刻を設定する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

4.12　リモートホストによる時計の設定

[書式]　**rdate** *host* [syslog]

[設定値]　◦ *host*
- リモートホストの IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))
- ホストの名称

◦ syslog..... 出力結果を SYSLOG へ出力することを示すキーワード

[説明]　ルーターの時計を、パラメータで指定したホストの時間に合わせる。
このコマンドが実行されるとホストの TCP の 37 番ポートに接続する。

[ノート]　ヤマハルーターシリーズおよび、多くの UNIX コンピュータをリモートホストに指定できる。
syslog キーワードを指定した場合には、コマンドの出力結果を INFO レベルの SYSLOG へ出力する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

4.13　NTP による時計の設定

[書式]　**ntpdate** *ntp_server* [syslog]

[設定値]　◦ *ntp_server*
- NTP サーバーの IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))
- NTP サーバーの名称

◦ syslog..... 出力結果を SYSLOG へ出力することを示すキーワード

[説明]　NTP を利用してルーターの時計を設定する。このコマンドが実行されるとホストの UDP の 123 番ポートに接続する。

[ノート]　インターネットに接続している場合には、**rdate** コマンドを使用した場合よりも精密な時計合わせが可能になる。
NTP サーバーはできるだけ近くのものを指定した方が良い。利用可能な NTP サーバーについてはプロバイダに問い合わせること。
ヤマハルーター自身は NTP サーバーになれない。
syslog キーワードを指定した場合には、コマンドの出力結果を INFO レベルの SYSLOG へ出力する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

4.14　コンソールのプロンプト表示の設定

[書式]　**console prompt** *prompt*
no console prompt [*prompt*]

[設定値]　◦ *prompt* .....コンソールのプロンプトの先頭文字列
(Rev.10 系、Rev.9.00 系、Rev.8.03 系 ...64 文字以内)
(Rev.8.01 系、Rev.8.02 系、Rev.7.01 系 ...16 文字以内)

[説明]　コンソールのプロンプト表示を設定する。空文字列も設定できる。

[初期値]　空文字列

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

4.15　コンソールの言語とコードの設定

[書式]　**console character** *code*
no console character [*code*]

[設定値]　◦ *code*
- ascii.....英語で表示する、文字コードは ASCII
- sjis.....日本語で表示する、文字コードはシフト JIS
- euc.....日本語で表示する、文字コードは EUC

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

[ノート]　本コマンドの設定は、**save** コマンドで保存するまで **show config** コマンドによる設定の表示に反映されない。
Rev.9 系以降では、**save** コマンドで保存しなくても **show config** コマンドで設定が表示される。

[初期値]　sjis

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

4.16　コンソールの表示文字数の設定

[書式]　**console columns** *col*
no console columns [*col*]

[設定値]　◦ *col* .....コンソールの表示文字数 (80..200)

[説明]　コンソールの 1 行あたりの表示文字数を設定する。
本コマンドは一般ユーザでも実行できる。

[ノート]　本コマンドの設定は、**save** コマンドで保存するまで **show config** コマンドによる設定の表示に反映されない。
Rev.9 系以降では、**save** コマンドで保存しなくても **show config** コマンドで設定が表示される。

[初期値]　80

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

4.17　コンソールの表示行数の設定

[書式]　**console lines** *lines*
no console lines [*lines*]

[設定値]　◦ *lines*
- 整数 (10..100)
- infinity.....スクロールを止めない

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

[ノート]　本コマンドの設定は、**save** コマンドで保存するまで **show config** コマンドによる設定の表示に反映されない。
Rev.9 系以降では、**save** コマンドで保存しなくても **show config** コマンドで設定が表示される。

[初期値]　24

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

4.18　コンソールにシステムメッセージを表示するか否かの設定

[書式]　**console info** *info*
no console info [*info*]

[設定値]　◦ *info*
- on..... 表示する
- off..... 表示しない

[説明]　コンソールにシステムメッセージを表示するか否かを設定する。

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

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

4.19　SYSLOG を受けるホストの IP アドレスの設定

[書式]　**syslog host** *host*
no syslog host [*host*]

[設定値]　◦ *host*..... SYSLOG を受けるホストの IP アドレス (空白で区切って最大 4ヶ所まで設定可能)

[説明]　SYSLOG を受けるホストの IP アドレスを設定する。
IP アドレスは IPv4/IPv6 いずれのアドレスも設定できる。
syslog debug コマンドが on に設定されている場合、大量のデバッグメッセージが送信されるので、このコマンドで設定するホストには十分なディスク領域を確保しておくことが望ましい。

[初期値]　SYSLOG ホストは設定されない

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

4.20　SYSLOG ファシリティの設定

[書式]　**syslog facility** *facility*
no syslog facility [*facility*]

[設定値]　◦ *facility*
- 0..23
- user..... 1
- local0..local7 ..... 16..23

[説明]　SYSLOG のファシリティを設定する。

[ノート]　ファシリティ番号の意味づけは、各 SYSLOG サーバーで独自に行う。

[初期値]　user

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

4.21　NOTICE タイプの SYSLOG を出力するか否かの設定

[書式]　**syslog notice** *notice*
no syslog notice [*notice*]

[設定値]　◦ *notice*
- on..... 出力する
- off..... 出力しない

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

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

4.22　INFO タイプの SYSLOG を出力するか否かの設定

[書式]　**syslog info** *info*
no syslog info [*info*]

[設定値]　◦ *info*
- on ..... 出力する
- off..... 出力しない

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

[初期値]　on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

4.23　DEBUG タイプの SYSLOG を出力するか否かの設定

[書式]　**syslog debug** *debug*
no syslog debug [*debug*]

[設定値]　◦ *debug*
- on ..... 出力する
- off..... 出力しない

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

[ノート]　*debug* パラメータを on にすると、大量のデバッグメッセージを送信するため、**syslog host** コマンドで設定するホスト側には十分なディスク領域を確保しておき、必要なデータが得られたらすぐに off にする。

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

4.24　SYSLOG を送信する時の始点 IP アドレスの設定

[書式]　**syslog local address** *address*
no syslog local addrress [*address*]

[設定値]　◦ *address*..... 始点 IP アドレス

[説明]　SYSLOG パケットを送信する時の始点 IP アドレスを設定する。始点 IP アドレスが設定されていない時は、通常の UDP パケット送信ルールに従い、出力インタフェースの IP アドレスを利用する。

[初期値]　始点 IP アドレスは設定されていない。

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

4.25　SYSLOG パケットの始点ポート番号の設定

[書式]　**syslog srcport** *port*
no syslog srcport [*port*]

[設定値]　◦ *port*..... ポート番号 (1..65535)

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

[初期値]　514

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

4.26　SYSLOG に実行コマンドを出力するか否かの設定

[書式]　**syslog execute command** *switch*
no syslog execute command [*switch*]

[設定値]　◦ *switch*
- on..... 実行されたコマンドをログに残す
- off..... 実行されたコマンドをログに残さない

[説明]　実行されたコマンドを SYSLOG で出力するか否かを設定する。

[ノート]　コマンド実行に成功した場合、そのコマンド入力をログに出力する。

[初期値]　off

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

4.27　電源の設定

[書式]　**system power** *module* **use** *switch*
no system power *module* **use** [*switch*]

[設定値]　◦ *module*..... モジュール番号 (1,2)
◦ *switch*
- on..... モジュールを装着している
- off..... モジュールを装着していない

[説明]　電源モジュールの装着状態を設定する。電源モジュールからの電源供給自体は、実際に装着すればこのコマンドに関係なく機能するが、このコマンドを設定することで電源モジュールの監視機能が正しく働くようになる。

[ノート]　電源モジュールを装着していないにも関わらず、*switch* を on に設定すると、監視機能が働き電源モジュールの異常を報告する。

[初期値]　モジュール 1 = on
モジュール 2 = off

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

4.28　TELNET サーバー機能の ON/OFF の設定

[書式]　**telnetd service** *service*
no telnetd service

[設定値]　◦ *service*
- on..... TELNET サーバー機能を有効にする
- off..... TELNET サーバー機能を停止させる

[説明]　TELNET サーバー機能の利用を選択する。

[ノート]　TELNET サーバーが停止している場合、 TELNET サーバーはアクセス要求に一切応答しない。

[初期値]　on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

4.29　TELNET サーバー機能の listen ポートの設定

[書式]　**telnetd listen** *port*
no telnetd listen

[設定値]　◦ *port*..... TELNET サーバー機能の待ち受け (listen) ポート番号 (1..65535)

[説明]　TELNET サーバー機能の listen ポートを選択する。

[ノート]　telnetd は、TCP の 23 番ポートで待ち受けしているが、本コマンドにより待ち受けポートを変更することができる。ただし、待ち受けポートを変更した場合には、ポート番号が変更されても、TELNET オプションのネゴシエーションが行える TELNET クライアントを用いる必要がある。

[初期値]　23

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

4.30　TELNET サーバーへアクセスできるホストの IP アドレスの設定

[書式]　**telnetd host** *ip_range* [*ip_range*...]
no telnetd host

[設定値]　◦ *ip_range*
- TELNET サーバーへアクセスを許可するホストの IP アドレス範囲のリストまたはニーモニック
- 1 個の IP アドレスまたは間にマイナス (-) をはさんだ IP アドレス (範囲指定)、およびこれらを任意に並べたもの
- *any*..... すべてのホストからのアクセスを許可する
- *none*..... すべてのホストからのアクセスを禁止する
- LAN インタフェース名
- ブリッジインタフェース名

[説明]　TELNET サーバーへアクセスできるホストの IP アドレスを設定する。

[ノート]　ニーモニックをリストにすることはできない。
設定後の新しい TELNET 接続から適用される。
ブリッジインタフェースを指定できるのは Rev.10.00.38 以降のリビジョンである。

[初期値]　*any*

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

4.31　TELNET サーバーへ同時に接続できるユーザ数の設定

[書式]　**telnetd session** *num*
no telnetd session

[設定値]　◦ *num*..... 同時接続数 (1..8)

[説明]　TELNET に同時に接続できるユーザ数を設定する。

[ノート]　設定を変更したときに変更した値よりも多くのユーザが接続している場合は、接続しているユーザはそれを維持することができるが、接続しているユーザ数が設定値より少なくなるまで新たな接続は許可しない。

[初期値]　8

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

4.32　マスタクロック用インタフェースの設定

[書式]　**line masterclock** *interface*
no line masterclock

[設定値]　◦ *interface*
- BRI インタフェース名
- PRI インタフェース名
- *auto*..... 自動選択

[説明]　RTX3000 と RT250i、RT300i では、装備されているすべての BRI/PRI インタフェースは 1 つのマスタクロックに同期している必要がある。マスタクロックは通常、BRI/PRI インタフェースに接続された WAN 回線から供給される。このコマンドでは、どのインタフェースからマスタクロックを得るかを指定することができる。*auto* を設定した場合は、実際に回線が接続されている BRI/PRI インタフェースの中からマスタクロックを供給するインタフェースを自動的に選択する。選択基準は、BRI よりは PRI を優先し、同じ回線種別の中ではより若番のポート番号を持つインタフェースを優先する。マスタとなるインタフェースの回線がダウンしてクロックを得られなくなった場合には、同じモジュール内のインタフェースを優先して、次のマスタクロック供給インタフェースを選択する。すべての回線がダウンしている場合には内部クロックを用いたフリーラン状態となる。
インタフェースを指定している場合には、そのインタフェースからマスタクロックを得る。そのインタフェースに接続されている回線がダウンした場合には、常に bri1 をマスタとする。bri1 もダウンした場合には内部クロックを用いたフリーラン状態となる。

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

[初期値]　*auto*

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	RT250i	~~RT107e~~	~~SRT100~~

4.33　温度監視の閾値の設定

[書式]　**system temperature threshold** *t1 t2*
no system temperature threshold *t1 t2*

[設定値]
- *t1* ..... 警告を発する温度 (℃)
- *t2* ..... 警告を解除する温度 (℃)

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

[初期値]　t1 = 65, t2 = 60 (RTX3000)
t1 = 75, t2 = 70 (RTX1200)
t1 = 80, t2 = 75 (上記以外の機種)

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	~~RTX1100~~	~~RTX1000~~	RT300i	RT250i	~~RT107e~~	~~SRT100~~

4.34　ファストパス機能の設定

[書式]　**ip routing process** *process*
no ip routing process

[設定値]
- *process*
  - fast ..... ファストパス機能を利用する
  - normal ..... ファストパス機能を利用せず、すべてのパケットをノーマルパスで処理する

[説明]　パケット転送をファストパス機能で処理するか、ノーマルパス機能で処理するかを設定する。

[ノート]　ファストパスでは使用できる機能に制限は無いが、取り扱うパケットの種類によってはファストパスで処理されずノーマルパスで処理されることもある。

RTX1000 では、優先制御または帯域制御機能を使用した場合にはそれらのパケットは常にノーマルパス処理となる。

ファームウェアが Rev.7.01 以降でのみ有効。

[初期値]　fast

[適用モデル]

~~RTX3000~~	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

4.35　LAN インタフェースの動作設定

[書式]　**lan shutdown** *interface* [*port...*]

[設定値]
- *interface* ..... LAN インタフェース名
- *port* ..... ポート番号 (スイッチングハブ内蔵機種のみ)

[説明]　LAN インタフェースを利用できないようにする。このコマンドを設定した LAN インタフェース、あるいはスイッチングハブのポートでは、LAN ケーブルを接続してもリンクアップしなくなる。

[ノート]　Rev.8.02 系以降のファームウェアで使用できる。LAN インタフェースが 1 つしかない機種ではこのコマンドは利用できない。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

4.36　ポートミラーリング機能の設定

[書式]　**lan port-mirroring** *interface mirror direction port ...* [*direction port ...*]
no lan port-mirroring *interface*

[設定値]
- *interface* ..... LAN インタフェース名
- *mirror* ..... ミラーリングパケットを送出させるポート番号
- *direction* ..... 観測対象のパケットの方向
  - in ..... 入る方向
  - out ..... 出る方向
- *port* ..... 観測対象とするポート番号

[説明]　スイッチングハブインタフェースにおいて、特定ポートでの通信を他のポートで観測できる機能を設定する。LAN インタフェース名にはスイッチングハブを持つインタフェースだけが指定可能である。

[ノート]　LAN 分割機能との併用はできない。
ミラーリングポートから送出されるパケットの送出レートが回線速度を超えないようにする必要がある。ミラーリングパケットがミラーリングポートから送出しきれない場合、他のポート間での通信に影響を与えることがある。
Rev.8.01.12 以降で使用可能。

[初期値]　設定なし

[設定例]　例 1) ポート 4 でポート 1 受信パケットを観測
```
# lan port-mirroring lan1 4 in 1
```

例 2) ポート 4 でポート 1 送受信パケットとポート 2 送信パケットを観測
```
# lan port-mirroring lan1 4 in 1 out 1 2
```

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

4.37　LAN インタフェースの動作タイプの設定

[書式]　**lan type** *interface_with_swhub speed* [*port*] [*speed* [*port*]...] [*option=value*...]
lan type *interface_with_swhub option=value*
lan type *interface_without_swhub speed* [*option=value*...]
lan type *interface_without_swhub option=value*
no lan type *interface* [...]

[設定値]
- *interface_with_swhub*..... スイッチングハブを持つ LAN インタフェース名
- *interface_without_swhub*... スイッチングハブを持たない LAN インタフェース名
- *interface*..... LAN インタフェース名
- *speed*..... LAN 速度および動作モード
  - auto ..... 速度自動判別
  - 1000-fdx..... 1000BASE-T 全二重
  - 100-fdx ..... 100BASE-TX 全二重
  - 100-hdx..... 100BASE-TX 半二重
  - 10-fdx..... 10BASE-T 全二重
  - 10-hdx ..... 10BASE-T 半二重
  - 省略時は auto
- *port*..... スイッチングハブのポート番号
  - 省略時は全ポート
- *option=value*..... オプション機能
  - mtu ..... インタフェースで送受信できる最大データ長
  - auto-crossover..... オートクロスオーバー機能
    - on.....オートクロスオーバー機能を有効にする
    - off .....オートクロスオーバー機能を無効にする
  - macaddress-aging..... MAC アドレスエージング機能
    - on.....MAC アドレスエージング機能を有効にする
    - off .....MAC アドレスエージング機能を無効にする
  - port-based-ks8995m/port-based-option..... LAN 分割機能、ポート分離機能
    - divide-network .....LAN 分割機能を有効にする
    - split-into-*split_pattern*.....ポート分離機能を有効にする
    - off .....LAN 分割機能、ポート分離機能を無効にする
  - speed-downshift..... 速度ダウンシフト機能
    - on.....速度ダウンシフト機能を有効にする
    - off .....速度ダウンシフト機能を無効にする

[説明]　指定した LAN インタフェースの速度と動作モードの種類、およびオプション機能について設定する。

スイッチングハブを持つ LAN インタフェースについては、ポート毎に速度と動作モードを指定できる。

"port-based-ks8995m/port-based-option" を設定する場合、コマンド文字列として、Rev.10.01 系以前のファームウェアでは "port-based-ks8995m" を、Rev.10.01 系以降のファームウェアでは "port-based-option" を入力する。
Rev.10.01 系以降のファームウェアでも "port-based-ks8995m" を入力することはできるが、show config の出力には "port-based-option" と表示される。

◦ *mtu*
インタフェースで送受信できる最大データ長を指定する。データ長には MAC ヘッダと FCS は含まれない。また、タグ VLAN 時のタグ長 (4 バイト) も含まれない。

指定できるデータ長の範囲は LAN インタフェースによって異なる。ジャンボフレームをサポートしていない LAN インタフェースでは、64 ～ 1500 の範囲となる。ジャンボフレームをサポートしている LAN インタフェースでは、以下のようになる。

機種	インタフェース	設定範囲
RTX3000	LAN1、LAN2	64 ～ 9578

インタフェースの *mtu* を設定して、かつ、**ip mtu** コマンドまたは **ipv6 mtu** コマンドが設定されずデフォルトのままの場合、IPv4 や IPv6 での *mtu* としてはインタフェースの *mtu* が利用される。一方、**ip mtu** コマンドまたは **ipv6 mtu** コマンドが設定されている場合には、インタフェースの *mtu* の設定にかかわらず、**ip mtu** コマンドまたは **ipv6 mtu** コマンドの設定値が *mtu* として利用される。インタフェースの *mtu* も含めてすべて設定されていない時には、デフォルト値である 1500 が利用される。

◦オートクロスオーバー機能
LAN ケーブルがストレートケーブルかクロスケーブルかを自動的に判定して接続する機能。この機能が有効になっていると、ケーブルのタイプがどのようなものであるかを気にする必要が無くなる。

このオプションは RTX2000、RT300i では利用できない。

◦MAC アドレスエージング機能
スイッチングハブを持つ LAN インタフェースでのみ利用できる。

スイッチングハブが持つ MAC アドレステーブル内のエントリを、一定時間で消去していく機能。この機能を off にすると、一度スイッチングハブが記憶した MAC アドレスは自動的に消去されないのはもちろん、**clear switching-hub macaddress** コマンドを実行しても消去されない。エントリが消去されるのは、この機能を on に設定し直した時だけになる。

MAC アドレステーブルの大きさは以下の通りとなる。

機種	最大エントリ数
RTX1200	8192
RTX1000、RTX1100、RTX1500、RT107e、SRT100	1024

◦LAN 分割機能
スイッチングハブを持つ LAN インタフェースでのみ利用できる。
このオプションは RT107e では利用できない。

LAN 分割機能には基本機能と拡張機能があり、拡張機能は Rev.10.01 系以降のファームウェアで利用できる。

基本機能では、スイッチングハブの各ポートが個別の LAN インタフェースとして動作する。各インタフェースにはそれぞれ個別の IP アドレスを付与でき、その間でのルーティグも可能になる。
例えば RTX1100 は通常は LAN インタフェースを 3 つ持つルーターなのだが、LAN 分割機能を使えば LAN インタフェースを 6 個利用できることになる。

拡張機能では、スイッチングハブの各ポートを自由に組み合わせて 1 つの LAN インタフェース (VLAN インタフェース) とすることができる。
同一の VLAN インタフェースに所属するポート間はスイッチとして動作する。

LAN 分割で使用するインタフェース名は基本機能と拡張機能で異なる。

基本機能における LAN インタフェースのインタフェース名は元の LAN インタフェース名にピリオドとポート番号をつなげることで表される。
例えば、RTX1100 は lan1 が 4 ポートのスイッチングハブを持つ LAN インタフェースなので、以下の LAN インタフェースが使用できるようになる。

ポート番号	インタフェース名
1	lan1.1
2	lan1.2
3	lan1.3
4	lan1.4

拡張機能では、LAN インタフェースのインタフェース名として vlan1、vlan2、vlan3・・・(VLAN インタフェース) を使用する。基本機能とは異なり、VLAN インタフェースは特定のポートと関連付けられてはいない。**vlan port mapping** コマンドを用いて、スイッチングハブの各ポートがどの VLAN インタフェースに所属するかを設定することで、分割方法を自由に変更することができる。

同時にいくつの VLAN インタフェースを使用できるかは機種ごとに異なり、以下の通りとなる。

機種	設定できる VLAN インタフェース
RTX1200	vlan1-vlan8

LAN分割機能を有効にした場合、lan1 インタフェースに対する設定は、lan1.1 (基本機能の場合) もしくは vlan1 (拡張機能の場合) に引き継がれる。

LAN分割で使用する LAN インタフェースの MAC アドレスは元の LAN インタフェースの MAC アドレスに一致する。したがって上記の例では、lan1.1-lan1.4 や vlan1-vlan8 の MAC アドレスはすべて lan1 と同一になる。

◦ ポート分離機能
Rev.8.03.24 以降のファームウェアで、スイッチングハブを持つ LAN インタフェースでのみ利用できる。

スイッチングハブのポート間での通信を禁止しつつ、ルーターを経由した通信は可能にする機能。

通常は、スイッチングハブの各ポートは他のポートと制限無く通信できるが、ポート分離機能を利用すると、ポートをグループに分離し、グループ内の通信およびルーターとの通信はそのまま可能だけれども、他のグループのポートとは通信できないようになる。

LAN分割機能とは異なり、ポート分離機能によって LAN インタフェースが増減することはない。分離されたポートはすべて同じ LAN インタフェースとして認識され、同一の IP アドレスを持つ。

ポートの分離パターンは、ポート番号の数字の並びで分離する部分に ":" を入れて記述する。例を以下に示す。

Rev.10.01 系以前のファームウェアで、スイッチングハブのポート数が 4 の場合

split_pattern	ポート				説明
	1	2	3	4	
1 : 234	←→	←――――→			ポート 1 とその他
1 : 2 : 34	←→	←→	←――→		ポート 1、ポート 2 とその他
1 : 2 : 3 : 4	←→	←→	←→	←→	全ポートを分離

Rev.10.01 系以降のファームウェアで、スイッチングハブのポート数が 8 の場合
最後のグループの記述を省略することができる。以下の表では、省略形を括弧内に示す。

split_pattern	ポート								説明
	1	2	3	4	5	6	7	8	
123:45678 (123)	←――――――→			←――――――――→					ポート 1 －3 とその他
1:234:5678 (1:234)	←→	←――――――→			←――――――――→				ポート 1 とポート 2 －4 とその他
12:34:56:78 (12:34:56)	←―――→		←―――→		←―――→		←―――→		ポート 1、2、ポート 3、4、ポート 5、6 とその他
1:2:3:4:5:6:7:8 (1:2:3:4:5:6:7)	←→	←→	←→	←→	←→	←→	←→	←→	全ポートを分離

省略形でコマンドを入力しても、show config の出力には省略しない形で表示される。

同一 LAN インタフェースにおけるプライマリアドレスのネットワークとセカンダリアドレスのネットワーク間の通信はルーターを経由するので、他のグループとの通信も可能である。

◦ 速度ダウンシフト機能
Rev.10.01 以降のファームウェアで、1000BASE-T のインタフェースを持つ機種で利用できる。
例えば 1000BASE-T で使用できないケーブルを接続された時に、速度を落としてリンクを試みる機能である。

[ノート]　本コマンドの実行後、LAN インタフェースのリセットが自動で行われ、その後に設定が有効となる。

[初期値]
speed = auto
mtu = 1500
auto-crossover = on
macaddress-aging = on
port-based-ks8995m/port-based-option = off
speed-downshift=on

[設定例]

1. スイッチングハブを持つ LAN インタフェースで、ポート 1、2 は 100BASE-TX 全二重、その他のポートはオートネゴシエーションで接続する。
   # lan type lan1 100-fdx 1 2

2. スイッチングハブを持つ LAN インタフェースで、ポート 1 は 100BASE-TX 全二重、その他のポートはオートネゴシエーションで接続し、LAN 分割機能を使用する。

   [Rev.10.01 系以前のファームウェアの場合]
   # lan type lan1 100-fdx 1 port-based-ks8995m=divide-network

   [Rev.10.01 系以降のファームウェアの場合]
   # lan type lan1 100-fdx 1 port-based-option=divide-network

3. スイッチングハブを持つ LAN インタフェースで、すべてのポートでオートネゴシエーションで接続する。ポート分離機能でポートを分離する。

   [Rev.10.01 系以前のファームウェアで、4 つのポートを持つスイッチングハブの 1、2 と 3、4 を分離する場合]
   # lan type lan1 port-based-ks8995m=split-into-12:34

   [Rev.10.01 系以降のファームウェアで、8 つのポートを持つスイッチングハブの 1、2、3 と 4、5、6 とその他を分離する場合]
   # lan type lan1 port-based-option=split-into-123:456:78

   [分離パターンを省略して記述する場合]
   # lan type lan1 port-based-option=split-into-123:456

4. LAN1 で、ジャンボフレーム (9000 バイト) を使用できるようにする。
   # lan type lan1 auto mtu=9000

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

4.38 LAN インタフェースの受信パケットバッファサイズの設定

[書式] **lan receive-buffer-size** *interface size*
no lan receive-buffer-size *interface*

[設定値]
- *interface* ..... LAN インタフェース名
- *size* ..... 受信パケットバッファサイズ (1..1000)

[説明] LAN インタフェースの受信パケットバッファサイズを設定する。

[初期値] 128 (QoS 設定時は全 LAN インタフェースで 20)

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

4.39 ログインタイマの設定

[書式] **login timer** *time*
no login timer [*time*]

[設定値]
- *time*
  - 秒数 ..... キー入力がない場合には自動的にログアウトするまでの秒数
    30..21474836(SRT100/RTX1200 以外)
    120..21474836(SRT100/RTX1200)
  - *clear* ..... ログインタイマを設定しない

[説明] キー入力がない場合に自動的にログアウトするまでの時間を設定する。

[ノート] TELNET または SSH でログインした場合、*clear* が設定されていてもタイマ値は 300 秒として扱う。
Rev.10.00.31 で *time* の下限値を 30 から 120 に変更した。

[初期値] 300

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

4.40 TFTP によりアクセスできるホストの IP アドレスの設定

[書式] **tftp host** *host*
no tftp host [*host*]

[設定値]
- *host*
  - IP アドレス ..... TFTP によりアクセスできるホストの IP アドレス (IPv6 アドレス可)
  - *any* ..... すべてのホストから TFTP によりアクセスできる
  - *none* ..... すべてのホストから TFTP によりアクセスできない

[説明] TFTP によりアクセスできるホストの IPv4 または IPv6 アドレスを設定する。

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

[初期値] *none*

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

4.41　Magic Packet を LAN に中継するか否かの設定

[書式]　**ip** *interface* **wol relay** *relay*
no ip *interface* **wol relay**

[設定値]
- *interface*.....LAN インタフェース名
- *relay*
  - broadcast.....Magic Packet をブロードキャストパケットとして中継する
  - unicast.....Magic Packet をユニキャストパケットとして中継する
  - off.....Magic Packet かどうか検査しない

[説明]　遠隔地から送信された、ディレクティッドブロードキャスト宛の IPv4 パケットとして構成された Magic Packet を指定した LAN インタフェースに中継する。IPv4 パケットの終点 IP アドレスは指定した LAN インタフェースのディレクティッドブロードキャスト宛でなくてはいけない。

broadcast または unicast を指定した場合には、受信したパケットの内容をチェックし、Magic Packet データシーケンスが存在する場合にのみパケットを中継する。

broadcast を指定した場合には、MagicPacket をブロードキャストパケットとして LAN インタフェースに送信する。

unicast を指定した場合には Magic Packet データシーケンスから MAC アドレスを抜きだし、それを終点 MAC アドレスとしたユニキャストパケットとして送信する。

off を指定した場合には、Magic Packet かどうかの検査は行わない。

[ノート]　いずれの場合も、Magic Packet として中継されなかった場合のパケットは、**ip filter *directed-broadcast*** コマンドの設定に基づき処理される。
Rev.7.01.34 以降、Rev.8.01.12 以降、Rev.10.00.31 以降で使用可能。

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

4.42　インタフェースまたはシステムの説明の設定

[書式]　**description** *id description*
no description *id* [*description*]
description *interface description*
no description *interface* [*description*]

[設定値]
- *id*.....システム全体の説明を記述する場合の ID (1..21474836)
- *interface*.....LAN インタフェース名、'pp'、'tunnel' のいずれか
- *description*.....説明の文字列 (最大 64 文字 /ASCII、32 文字 / シフト JIS)

[説明]　システム全体の説明、あるいはインタフェースの説明を設定しておく。
設定内容はあくまで説明のためだけであり、動作には影響を与えない。

システム全体の説明の場合は、ID の値を変えることで複数行の説明を設定できる。
インタフェースの説明は一行に限定される。

interface として 'pp' あるいは 'tunnel' を指示したときにはそれぞれ、pp select あるいは tunnel select で選択したインタフェースの説明となる。

設定内容は ***show config*** コマンドで表示される。また、インタフェースに対する設定内容はインタフェースに対する ***show status*** コマンドでも表示される。

システム全体の説明は、***show config*** コマンドではすべての設定よりも先に、ID 順に表示される。

説明には、ASCII 文字だけではなく、シフト JIS で表現できる範囲の日本語文字 (半角カタカナを除く) も使用できる。ただし、***console character*** コマンドの設定が sjis の場合にのみ、正しく設定、表示でき、他の設定の場合には文字化けすることがある。

[ノート]　Rev.7.01.41、Rev.8.01.18、Rev.8.02.28 以降で使用可能。
RT250i では ***description tunnel*** コマンドは使用できない。

ID は、Rev.8.03.68、Rev.9.00.31、Rev.10.00.31 以降で使用可能。

[初期値]　なし

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	RT250i	RT107e	SRT100

4.43　TCP のコネクションレベルの syslog を出力するか否かの設定

[書式]

tcp log *switch* [*src_addr*[/*mask*] [*dst_addr*[/*mask*]] [*tcpflag*[*src_port_list* [*dst_port_list*]]]]
no tcp log [...]

[設定値]

◦ *switch*
- on..... TCP コネクションの syslog を出力する
- off..... TCP コネクションの syslog を出力しない

◦ *src_addr*..... 始点 IP アドレス
- xxx.xxx.xxx.xxx は
  - 10 進数
  - *(ネットマスクの対応するビットが 8 ビットとも 0 と同じ)
- 間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定
- *(すべての IP アドレス)

◦ *dst_addr*..... 終点 IP アドレス (*src_addr* と同じ形式)
- 省略時は 1 個の * と同じ

◦ *mask*..... IP アドレスのビットマスク。
- 省略時は 0xffffffff と同じ。*src_addr* および *dst_addr* がネットワークアドレスの場合にのみ指定可能。

◦ *tcpflag*..... フィルタリングする TCP パケットの種類
- プロトコルを表す 10 進数 (6 のみ)
- プロトコルを表すニーモニック

ニーモニック	10 進数	説明
tcp	6	すべての TCP パケット
tcpsyn	-	SYN フラグの立っているパケット
tcpfin	-	FIN フラグの立っているパケット
tcprst	-	RST フラグの立っているパケット
established	-	ACK フラグの立っているパケット

- tcpflag=flag_value/flag_mask、または tcpflag!=flag_value/flag_mask
  - 参考フラグ値
    0x0001　FIN
    0x0002　SYN
    0x0004　RST
    0x0008　PSH
    0x0010　ACK
    0x0020　URG
- *(すべての TCP パケット。ニーモニックに tcp を指定したときと同じ)
- 省略時は * と同じ。

◦ *src_port_list*..... TCP のソースポート番号
- ポート番号を表す 10 進数
- ポート番号を表すニーモニック

ニーモニック	ポート番号
ftp	20,21
ftpdata	20
telnet	23
smtp	25
domain	53
gopher	70
finger	73
www	80
pop3	110
sunrpc	111
ident	113
ntp	123
nntp	119
snmp	161
syslog	514
printer	515
talk	517
route	520
uucp	540

- 間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定
  - 上項目をカンマで区切った並び (10 個以内)
  - *(すべてのポート)
  - 省略時は * と同じ。

◦ *dst_port_list*.....TCP のデスティネーションポート番号
src_port_list と同じ形式。

[説明]　TCP の syslog を出力する。syslog debug on も設定されている必要がある。IPv4 のみに対応している。システムに負荷がかかるため、トラブルシュート等の一時的な使用にしか推奨されない。

[ノート]　Rev.7.01.48、Rev.8.01.18、Rev.8.02.28 以降で使用可能。

[初期値]　off

[設定例]
```
tcp log on * * tcpsyn * 1723          (PPTP のポートに SYN が来ているか )
tcp log on * * tcpflag!=0x0000/0x0007 (FIN,RST,SYN の立った TCP パケット )
tcp log on                            ( すべての TCP パケット。tcp log on * * * * * と同じ )
```

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	RT250i	RT107e	SRT100

4.44　HTTP リビジョンアップ実行を許可するか否かの設定

[書式]　**http revision-up permit** *permit*
no http revision-up permit [*permit*]

[設定値]　◦ *permit*
- on.....許可する
- off.....許可しない

[説明]　HTTP リビジョンアップを許可するか否かを設定する。

[ノート]　このコマンドの設定は、コマンドによる直接の HTTP リビジョンアップ、かんたん設定ページによるリビジョンアップ、DOWNLOAD ボタンによるリビジョンアップに影響する。

[初期値]　on

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

4.45　HTTP リビジョンアップ用 URL の設定

[書式]　**http revision-up url** *url*
no http revision-up url [*url*]

[設定値]　◦ *url*.....ファームウェアが置いてある URL を設定する

[説明]　HTTP リビジョンアップとしてファームウェアが置いてある URL を設定する。
入力形式は“http:// サーバーの IP アドレスあるいはホスト名 / パス名”という形式となる。
サーバーのポート番号が 80 以外の場合は、“http:// サーバーの IP アドレスあるいはホスト名 : ポート番号 / パス名”という形式で、URL の中に指定する必要がある。

[初期値]　http://www.rtpro.yamaha.co.jp/firmware/revision-up/(機種名).bin

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

4.46　HTTP リビジョンアップ用 Proxy サーバーの設定

[書式]　**http revision-up proxy** *proxy_server* [*port*]
no http revision-up proxy [*proxy_server* [*port*]]

[設定値]　◦ *proxy_server*.....HTTP リビジョンアップ時に使用する Proxy サーバー
◦ *port*.....Proxy サーバーのポート番号

[説明]　Proxy サーバーのホスト名または、IP アドレスとポート番号を指定する。

[初期値]　Proxy サーバーは設定されていない

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

4.47　HTTP リビジョンアップ処理のタイムアウトの設定

[書式]　**http revision-up timeout** *time*
no http revision-up timeout [*time*]

[設定値]　◦ *time*..... タイムアウト時間 (秒)

[説明]　HTTP リビジョンアップ処理のタイムアウト時間を設定する。

[初期値]　30

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

4.48　リビジョンダウンを許可するか否かの設定

[書式]　**http revision-down permit** *permit*
no http revision-down permit [*permit*]

[設定値]　◦ *permit*
- on..... 現在のリビジョンより古いリビジョンへのリビジョンダウンを許可する
- off..... 現在のリビジョンより古いリビジョンへのリビジョンダウンを許可しない

[説明]　HTTP リビジョンアップ機能にて、現在のリビジョンよりも古いリビジョンへのファームウェアのリビジョンダウンを許可するか否かを設定する。

[初期値]　off

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

4.49　DOWNLOAD ボタンによるリビジョンアップ操作を許可するか否かの設定

[書式]　**operation http revision-up permit** *permit*
no operation http revision-up permit [*permit*]

[設定値]　◦ *permit*
- on..... DOWNLOAD ボタンによるリビジョンアップ操作を許可する
- off..... DOWNLOAD ボタンによるリビジョンアップ操作を許可しない

[説明]　DOWNLOAD ボタンによりファームウェアのリビジョンアップ機能を使用するか否かを設定する。

[ノート]　リビジョンアップ機能は HTTP リビジョンアップ機能に準ずる。
STATUS ランプがエラーを表示している状態で本コマンドを off に設定すると、エラー表示が解除される。

[初期値]　off

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

4.50　SSH サーバー機能の ON/OFF の設定

[書式]　**sshd service** *service*
no sshd service [*service*]

[設定値]　◦ *service*
- on..... SSH サーバー機能を有効にする
- off..... SSH サーバー機能を停止させる

[説明]　SSH サーバー機能の利用を選択する。

[ノート]　SSH サーバー機能が停止している場合、SSH サーバーはアクセス要求に一切応答しない。

[初期値]　off

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

4.51　SSH サーバー機能の listen ポートの設定

[書式]　**sshd listen** *port*
no sshd listen [*port*]

[設定値]　◦ *port*.....SSH サーバー機能の待ち受け (listen) ポート番号 (1..65535)

[説明]　SSH サーバーの listen ポートを選択する。

[ノート]　SSH サーバーは、TCP の 22 番ポートで待ち受けしているが、本コマンドにより待ち受けポートを変更することができる。

[初期値]　*22*

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

4.52　SSH サーバーへアクセスできるホストの IP アドレスの設定

[書式]　**sshd host** *ip_range* [*ip_range ...*]
no sshd host [*ip_range ...*]

[設定値]　◦ *ip_range*
- SSH サーバーへアクセスを許可するホストの IP アドレス範囲のリストまたはニーモニック
- 1 個の IP アドレスまたは間にハイフン (-) をはさんだ IP アドレス (範囲指定)、およびこれらを任意に並べたもの
- any..... すべてのホストからのアクセスを許可する
- none.....すべてのホストからのアクセスを禁止する
- LAN インタフェース名
- ブリッジインタフェース名

[説明]　SSH サーバーへアクセスできるホストの IP アドレスを設定する。

[ノート]　ニーモニックをリストにすることはできない。
設定後の新しい SSH 接続から適用される。
ブリッジインタフェースを指定できるのは Rev.10.00.38 以降のリビジョンである。

[初期値]　*any*

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

4.53　SSH サーバーへ同時に接続できるユーザ数の設定

[書式]　**sshd session** *num*
no sshd session [*num*]

[設定値]　◦ *num*.....同時接続数 (1..8)

[説明]　SSH に同時に接続できるユーザ数を設定する。

[ノート]　設定を変更したときに変更した値よりも多くのユーザが接続している場合は、接続しているユーザはそれを維持することができるが、接続しているユーザ数が設定値より少なくなるまで新たな接続は許可しない。

[初期値]　8

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

4.54　SSH サーバー ホスト鍵の設定

[書式]　**sshd host key generate** [*seed*]
no sshd host key generate [*seed*]

[設定値]　◦ *seed*.....ホスト鍵の元になる数 (0..4294967295)

[説明]　SSH サーバーのホスト鍵を設定する。

seed を省略した場合は、 ランダムな値が *seed* として自動的に設定される。

[ノート]　SSH サーバー機能を利用する場合は、事前に本コマンドを実行してホスト鍵を生成する必要がある。

seed によって生成されるホスト鍵が一意に決まるため、 *seed* を指定する場合は機器毎に異なる値を設定すべきである。

既にホスト鍵が設定されている状態で本コマンドを実行した場合、ユーザに対してホスト鍵を更新するか否かを確認する。

ホスト鍵の生成には、機種によって異なるが 30 秒から 1 分程度の時間がかかる。

TFTP で設定を取得した場合は、**sshd host key generate** *seed* KEY1 KEY2 という形式で保存される。KEY1 と KEY2 は、それぞれ RSA 秘密鍵と DSA 秘密鍵を機器固有の方式で暗号化した文字列である。そのため、保存した設定を他の機器に適用する場合、*seed* からホスト鍵を生成し、機器固有の方式で暗号化して保存するため、入力した KEY1、KEY2 とは同一の文字列にはならない。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

4.55 SSH クライアントの生存確認

[書式]　**sshd client alive** *switch* [*interval* [*count*]]
no sshd client alive [*switch* ...]

[設定値]
- *switch*
  - on..... クライアントの生存確認を行う
  - off..... クライアントの生存確認を行わない
- *interval*..... 送信間隔の秒数 (1..2147483647)
- *count*..... 試行回数 (1..2147483647)

[説明]　クライアントの生存確認を行うか否かを設定する。

クライアントに *interval* で設定した間隔で応答を要求するメッセージを送る。*count* で指定した回数だけ連続して応答がなかったら、このクライアントとの接続を切り、セッションを終了する。

[初期値]
- *switch*..... off
- *interval* 100
- *count*..... 3

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

4.56 パケットバッファのパラメータの変更

[書式]　**system packet-buffer** *group parameter=value* [*parameter=value* ...]
no system packet-buffer *group* [*parameter=value* ...]

[設定値]
- *group*..... パケットバッファのグループを指定する。
  グループ名 : small, middle, large, jumbo, huge
- *parameter*..... 変更するパラメータを指定する。
  - max-buffer..... パケットバッファの最大割り当て数
  - max-free..... フリーリストの最大値
  - min-free..... フリーリストの最小値
  - buffer-in-chunk.... チャンク内のパケットバッファ数
  - init-chunk..... 起動時に確保するチャンク数
- *value*..... 変更する値を指定する。

[説明]　パケットバッファの管理パラメータを変更する。

パラメータに指定できる値は、huge ブロックとそれ以外で異なる。huge ブロック以外のブロックでは、パラメータには 1 以上の整数を指定できる。同時に、各パラメータは以下に示す条件をすべて満たす必要がある。

- max-buffer ≧ max-free
- max-free ＞ min-free
- max_free ≧ buffer-in-chunk
- max_free ≧ buffer-in-chunk × init-chunk

huge ブロックでは、max-free、min-free、init-chunk には 0 以上の整数を、max-buffer、buffer-in-chunk には 1 以上の整数を指定できる。max-free、min-free、init-chunk に 0 を指定する場合には、3 つのパラメータがすべて 0 でなければならない。max-free、min-free、init-chunk が 1 以上の場合には、各パラメータは他のグループと同様、上記の条件を満たす必要がある。

[ノート]　jumbo グループは、LAN インタフェースとして 1000BASE-T インタフェース対応でかつ、ジャンボパケットの送受信ができる機種でのみ利用できる。

[初期値]

• RTX1100、RT107e、SRT100

グループ	max-buffer	max-free	min-free	buffer-in-chunk	init-chunk
small	500	187	12	125	1
middle	1332	499	33	333	1
large	2000	562	12	125	4
huge	20	0	0	1	0

• RTX1200

グループ	max-buffer	max-free	min-free	buffer-in-chunk	init-chunk
small	2500	937	62	625	1
middle	6664	2499	166	1666	1
large	10000	2812	62	625	4
huge	20	0	0	1	0

• RTX1500

グループ	max-buffer	max-free	min-free	buffer-in-chunk	init-chunk
small	2500	937	62	625	1
middle	6664	2499	166	1666	1
large	10000	5312	62	625	8
huge	20	0	0	1	0

• RTX3000

グループ	max-buffer	max-free	min-free	buffer-in-chunk	init-chunk
small	2500	937	62	625	1
middle	6664	2499	166	1666	1
large	10000	2812	62	625	4
jumbo	10000	2812	62	625	4
huge	20	0	0	1	0

[設定例]

 # system packet-buffer small max-buffer=1000 max-free=500
 # system packet-buffer large min-free=100

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

4.57　有効になっているアラーム音を鳴らすか全く鳴らさないかの設定

[書式]

alarm entire *switch*
no alarm entire

[設定値]

◦ *switch*
- on ..... 鳴らす
- off..... 鳴らさない

[説明]

有効になっているアラーム音を鳴らすか全く鳴らさないかを選択する。

[初期値]

on

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

4.58　USB ホスト機能に関連するアラーム音を鳴らすか否かの設定

[書式]

alarm usbhost *switch*
no alarm usbhost

[設定値]

◦ *switch*
- on ..... 鳴らす
- off..... 鳴らさない

[説明]

USB ホスト機能に関連するアラーム音を鳴らすか否かを選択する。

[初期値]

on

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

4.59　microSD 機能に関連するアラームを鳴らすか否かの設定

［書式］　**alarm sd** *switch*
no alarm sd [*switch*]

［設定値］　◦ *switch*
- on..... 鳴らす
- off..... 鳴らさない

［説明］　microSD 機能に関連するアラームを鳴らすかどうかを設定する。

［初期値］　on

［適用モデル］

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

4.60　起動時のアラーム音を鳴らすか否かの設定

［書式］　**alarm startup** *switch* [*pattern*]
no alarm startup [*switch*]

［設定値］　◦ *switch*
- on..... 鳴らす
- off..... 鳴らさない

◦ *pattern*..... アラーム音のパターン (1…3、省略時は 1)

［説明］　起動時にアラーム音を鳴らすか否かを選択する。

［初期値］　off

［適用モデル］

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

4.61　HTTP リビジョンアップ機能に関連するアラームを鳴らすか否かの設定

［書式］　**alarm http revision-up** *switch*
no alarm http revision-up [*switch*]

［設定値］　◦ *switch*
- on..... 鳴らす
- off..... 鳴らさない

［説明］　HTTP リビジョンアップ機能に関連するアラームを鳴らすかどうかを設定する。

［初期値］　on

［適用モデル］

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

4.62　LED の輝度を調整する

［書式］　**system led brightness** *mode*
no system led brightness [*mode*]

［設定値］　◦ *mode*
- 0 ..... 明るい
- 1 ..... 暗い

［説明］　LED の輝度を調整する。

［初期値］　0

［適用モデル］

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

5. ISDN 関連の設定

5.1 共通の設定

5.1.1 BRI 回線の種類の指定

[書式]　**line type** *interface line* [*channels*]
no line type *interface line* [*channels*]

[設定値]
- *interface*.....BRI インタフェース名
- *line*
  - isdn, isdn-ntt.....ISDN 回線交換
  - l64.....ディジタル専用線、64kbit/s
  - l128 .....ディジタル専用線、128kbit/s
- *channels*.....*line* パラメータが isdn 、isdn-ntt の場合のみ指定可
  - 1b .....B チャネルは 1 チャネルだけ使用
  - 2b .....B チャネルは 2 チャネルとも使用する

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

[ノート]　別の通信機器の発着信のために 1B チャネルを確保したい場合は *channels* パラメータを 1b に設定する。

[初期値]　*line* = isdn
channels = 2b

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

5.1.2 自分の ISDN 番号の設定

[書式]　**isdn local address** *interface isdn_num*[*/sub_address*]
isdn local address *interface /sub_address*
no isdn local address *interface*

[設定値]
- *interface*
  - BRI インタフェース名
  - PRI インタフェース名
- *isdn_num* .....ISDN 番号
- *sub_address*.....ISDN サブアドレス (0x21 から 0x7e の ASCII 文字列)

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

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

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

5.1.3 内蔵 DSU 使用の可否の設定

[書式] **isdn dsu** *interface switch*
no isdn dsu *interface* [*switch*]

[設定値] ◦ *interface*..... BRI インタフェース名
◦ *switch*
• auto ..... 内蔵 DSU 機能を使用するか否かを自動的に判別する
• on..... 内蔵 DSU 機能を使用する
• off..... 内蔵 DSU 機能を使用しない

[説明] 指定した BRI インタフェースの内蔵 DSU 機能を使用するか否かを設定する。

[ノート] auto を指定した場合、終端抵抗は以下の設定になる。
• レイヤ 1 がアップしておらず、自動判別中は ON
• レイヤ 1 がアップし、内蔵 DSU 機能を使用する場合はそのまま ON
• レイヤ 1 がアップし、内蔵 DSU 機能を使用しない場合は **isdn terminator** コマンドに合わせる
• レイヤ 1 がダウンしたら ON

[初期値] auto

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

5.1.4 終端抵抗の設定

[書式] **isdn terminator** *interface terminator*
no isdn terminator *interface* [*terminator*]

[設定値] ◦ *interface*..... BRI インタフェース名
◦ *terminator*
• on..... 終端抵抗を ON にする
• off..... 終端抵抗を OFF にする

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

[ノート] DSU に直結する場合には必ず on にする。
バス配線されている場合、バスの終端でなければ off にする。

[初期値] on

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

5.1.5 PP で使用するインタフェースの設定

[書式] **pp bind** *interface* [*interface*]
no pp bind [*interface*]

[設定値] ◦ *interface*..... BRI インタフェース名と BRI インタフェース名の並び

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

[初期値] どのインタフェースともバインドされていない

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

5.1.6　課金額による発信制限の設定

[書式]
account threshold [*interface*] *yen*
account threshold pp *yen*
no account threshold *interface* [*yen*]
no account threshold [*yen*]
no account threshold pp [*yen*]

[設定値]
◦ *interface*
- BRI インタフェース名
- PRI インタフェース名

◦ *yen*
- 課金額.....円 (1..2147483647)
- off.....発信制限機能を使わない

[説明]
網から通知される課金の合計 (これは **show account** コマンドで表示される) の累計が指定した金額に達したらそれ以上の発信を行わないようにする。
account threshold コマンドではルーター全体の合計金額を設定し、*interface* パラメータを指定した場合には、それぞれのインタフェースでの合計金額、**account threshold pp** コマンドでは選択している相手先に対する発信での合計金額で制御を行う。
課金が網から通知されるのは通信切断時なので、長時間の接続の途中切断することはできず、この場合は制限はできない。この場合に対処するには、**isdn forced disconnect time** コマンドで通信中でも時間を監視して強制的に回線を切るような設定にしておく方法がある。また、課金合計は **clear account** コマンドで 0 にリセットでき、**schedule at** コマンドで定期的に **clear account** を実行するようにしておくと、毎月一定額以内に課金を抑えるといったことが自動で可能になる。

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

[初期値]
off

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

5.1.7　PIAFS の着信を許可するか否かの設定

[書式]
isdn piafs arrive *arrive*
no isdn piafs arrive [*arrive*]

[設定値]
◦ *arrive*
- on.....許可する
- off.....拒否する

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

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

[初期値]
on

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

5.1.8 PIAFS 接続時の起動側の指定

[書式] **isdn piafs control** *switch*
no isdn piafs control

[設定値] ◦ *switch*
- call..... 自分が発信側の場合に PIAFS の起動側となる
- both..... 自分が発着信いずれの場合でも PIAFS の起動側となる
- arrive ..... 自分が着信側の場合に PIAFS の起動側となる

[説明] PIAFS を制御する側を選択する。

[ノート] 本コマンドの設定と、発信 / 着信の組み合わせにより、起動側となるか被起動側となるかが以下のように決定される。

switch **パラメータの設定**	call	both	arrive
発信時	起動時	起動側	被起動側
着信時	被起動側	起動側	起動側

[初期値] call

[設定例] # pp select 2
isdn piafs control call
pp enable 2

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

5.1.9 PIAFS の発信方式の設定

[書式] **isdn piafs call** *speed* [*64kmode*]
no isdn piafs call [*speed* [*64kmode*]]

[設定値] ◦ *speed*
- off..... 発信を同期 PPP とする
- 32k..... 発信を PIAFS 32k とする
- 64k..... 発信を PIAFS 64k とする

◦ *64kmode*
- guarantee ..... PIAFS 64k の発信ではギャランティー方式を使用する
- best-effort..... PIAFS 64k の発信ではベストエフォート方式を使用する

[説明] PIAFS モードの発信を可能にするか否かを設定する。
また、PIAFS モードの速度を選択する。
speed が off に設定されている場合には発信は同期 PPP になり、32k に設定されている場合には発信は PIAFS 32k に、64k に設定されている場合には発信は PIAFS 64k になる。
speed が 64k に設定されている場合には、*64kmode* の設定が有効になる。
64kmode が設定されていない、または guarantee に設定されている場合には、発信はギャランティー方式の PIAFS 64k になる。
64kmode が best-effort に設定されている場合には、発信はベストエフォート方式になる。

[ノート] PIAFS 64k では特別なサブアドレスが用いられるため、ユーザがコマンドで設定した発サブアドレスは無視される。

[初期値] off

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

5.1.10 専用線がダウンした時にバックアップする相手先情報番号の設定

[書式] **leased backup** *peer_num*
no leased backup [*peer_num*]

[設定値] ◦ *peer_num*
- バックアップする相手先情報番号
- none..... ISDN でバックアップをしない

[説明] BRI インタフェースを複数持つ機種で有効なコマンド。
選択した相手先に対する専用線がダウンした場合に ISDN でバックアップする、バックアップ用の相手先情報番号を設定する。

[初期値] none

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	RT250i	~~RT107e~~	~~SRT100~~

5.2　相手側の設定

5.2.1　常時接続の設定

[書式]　**pp always-on** *switch* [*time*]
no pp always-on

[設定値]
- *switch*
  - on ..... 常時接続する
  - off..... 常時接続しない
- *time*..... 再接続を要求するまでの秒数 (60..21474836)

[説明]　選択されている相手について常時接続するか否かを設定する。また、常時接続での通信終了時に再接続を要求するまでの時間間隔を指定する。
常時接続に設定されている場合には、起動時に接続を起動し、通信終了時には再接続を起動し、キープアライブ機能により接続相手のダウン検出を行う。接続失敗時あるいは通信の異常終了時には *time* に設定された時間間隔を待った後に再接続の要求を行い、正常な通信終了時には直ちに再接続の要求を行う。*switch* が on に設定されている場合には、*time* の設定が有効となる。*time* が設定されていない場合には *time* は 60 になる。

[ノート]　PP 毎のコマンドである。
PP として専用線に使用される時あるいは anonymous が選択された時には無効である。

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

5.2.2　相手 ISDN 番号の設定

[書式]　**isdn remote address** *call_arrive isdn_num* [*/sub_address*] [*isdn_num_list*]
isdn remote address *call_arrive isdn_num* [*isdn_num_list*]
no isdn remote address *call_arrive* [*isdn_num* [*/sub_address*] [*isdn_num_list*]]

[設定値]
- *call_arrive*
  - call ..... 発着信用
  - arrive ..... 着信専用
- *isdn_num* ..... ISDN 番号
- *sub_address*..... ISDN サブアドレス (0x21 から 0x7e の ASCII 文字)
- *isdn_num_list*..... ISDN 番号だけまたは ISDN 番号とサブアドレスの組を空白で区切った並び

[説明]　選択されている相手の ISDN 番号とサブアドレスを設定する。ISDN 番号には市外局番も含めて設定する。
選択されている相手が anonymous の場合は無意味である。
複数の ISDN 番号が設定されている場合、まず先頭の ISDN 番号での接続に失敗すると次に指定された ISDN 番号が使われる。同様に、それに失敗すると次の ISDN 番号を使うという動作を続ける。
MP のように相手先に対して複数チャネルで接続しようとする際に発信する順番は、**isdn remote call order** コマンドで設定する。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

5.2.3　自動接続の設定

[書式]　**isdn auto connect** *auto*
no isdn auto connect [*auto*]

[設定値]
- *auto*
  - on ..... 自動接続する
  - off..... 自動接続しない

[説明]　選択されている相手について自動接続するか否かを設定する。

[初期値]　on

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

5.2.4 相手への発信順序の設定

[書式] **isdn remote call order** *order*
no isdn remote call order [*order*]

[設定値] ◦ *order*
- round ..... ラウンドロビン方式
- serial ..... 順次サーチ方式

[説明] ***isdn remote address call*** コマンドで複数の ISDN 番号が設定されている場合に意味を持つ。MP を使用する場合などのように、相手先に対して同時に複数のチャネルで接続しようとする際に、どのような順番で ISDN 番号を選択するかを設定する。
round を指定した場合は、***isdn remote address call*** コマンドで最初に設定した ISDN 番号で発信した次の発信時に、このコマンドで次に設定された ISDN 番号を使う。このように順次ずれていき、最後に設定された番号で発信した次には、最初に設定された ISDN 番号を使い、これを繰り返す。
serial を指定した場合は、発信時には必ず最初に設定された ISDN 番号を使い、何らかの理由で接続できなかった場合は次に設定された ISDN 番号で発信し直す。
なお round、serial いずれの設定の場合でも、どことも接続されていない状態や相手先とすべてのチャネルで切断された後では、最初に設定された ISDN 番号から発信に使用される。

[ノート] MP を使用する場合は、round にした方が効率がよい。

[初期値] serial

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

5.2.5 着信許可の設定

[書式] **isdn arrive permit** *arrive* [vrrp *interface vrid*[slave]]
no isdn arrive permit [*arrive*]

[設定値] ◦ *arrive*
- on..... 許可する
- off..... 許可しない

◦ *interface* ..... LAN インタフェース名

◦ *vrid* ..... VRRP グループ ID(1..255)

[説明] 選択されている相手からの着信を許可するか否かを設定する。
on に設定しかつ VRRP グループを指定することで、VRRP の状態によって着信を許可するか否かの動作を動的に変えることが可能である。
この時、slave パラメータを省略した場合には指定した VRRP グループでマスターとして動作している場合にのみ着信が許可される。slave パラメータを設定した場合には、指定した VRRP グループで非マスターである場合にのみ着信が許可される。

[ノート] ***isdn arrive permit***、***isdn call permit*** コマンドとも off を設定した場合、ISDN 回線経由では通信できない。

[初期値] on

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

5.2.6 発信許可の設定

[書式] **isdn call permit** *permit*
no isdn call permit [*permit*]

[設定値] ◦ *permit*
- on..... 許可する
- off..... 許可しない

[説明] 選択されている相手への発信を許可するか否かを設定する。

[ノート] ***isdn arrive permit***、***isdn call permit*** コマンドとも off を設定した場合は通信できない。

[初期値] on

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

5.2.7　再発信抑制タイマの設定

[書式]　**isdn call block time** *time*
no isdn call block time [*time*]

[設定値]　◦ *time*.....秒数 (0..15.0)

[説明]　選択されている相手との通信が切断された後、同じ相手に対し再度発信するのを禁止する時間を設定する。秒数は 0.1 秒単位で設定できる。
isdn call prohibit time コマンドによるタイマはエラーで切断された場合だけに適用されるが、このコマンドによるタイマは正常切断でも適用される点が異なる。

[ノート]　切断後すぐに発信ということを繰り返す状況では適当な値を設定すべきである。
isdn forced disconnect time コマンドと併用するとよい。

[初期値]　0

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

5.2.8　エラー切断後の再発信禁止タイマの設定

[書式]　**isdn call prohibit time** *time*
no isdn call prohibit time [*time*]

[設定値]　◦ *time*.....秒数 (60..21474836.0)

[説明]　選択されている相手に発信しようとして失敗した場合に、同じ相手に対し再度発信するのを禁止する時間を設定する。秒数は 0.1 秒単位で設定できる。
isdn call block time コマンドによるタイマは切断後に常に適用されるが、このコマンドによるタイマはエラー切断にのみ適用される点が異なる。

[初期値]　60

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

5.2.9　相手にコールバック要求を行うか否かの設定

[書式]　**isdn callback request** *callback_request*
no isdn callback request [*callback_request*]

[設定値]　◦ *callback_request*
- on.....要求する
- off.....要求しない

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

[初期値]　off

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

5.2.10　相手からのコールバック要求に応じるか否かの設定

[書式]　**isdn callback permit** *callback_permit*
no isdn callback permit [*callback_permit*]

[設定値]　◦ *callback_permit*
- on.....応じる
- off.....応じない

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

[初期値]　off

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

5.2.11 コールバック要求タイプの設定

[書式] **isdn callback request type** *type*
no isdn callback request type [*type*]

[設定値] ◦ *type*
- yamaha..... ヤマハ方式
- mscbcp ..... MS コールバック

[説明] コールバックを要求する場合のコールバック方式を設定する。

[初期値] yamaha

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

5.2.12 コールバック受け入れタイプの設定

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

[設定値] ◦ *type1, type2*
- yamaha..... ヤマハ方式
- mscbcp ..... MS コールバック

[説明] 受け入れることのできるコールバック方式を設定する。

[初期値] *type1* = yamaha
type2 = mscbcp

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

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

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

[設定値] ◦ *specify*
- on..... 許可する
- off..... 拒否する

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

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

[初期値] off

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

5.2.14 コールバックタイマの設定

[書式] **isdn callback response time** *type time*

[設定値] ◦ *type*
- 1b..... 1B でコールバックする

◦ *time*..... 秒数 (0..15.0)

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

[初期値] *time* = 0

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

5.2.15　コールバック待機タイマの設定

[書式]　**isdn callback wait time** *time*
no isdn callback wait time [*time*]

[設定値]　◦ *time*.....秒数 (1..60.0)

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

[初期値]　60

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

5.2.16　ISDN 回線を切断するタイマ方式の指定

[書式]　**isdn disconnect policy** *type*
no isdn disconnect policy [*type*]

[設定値]　◦ *type*
- 1.....単純トラフィック監視方式
- 2.....課金単位時間方式

[説明]　単純トラフィック監視方式は従来型の方式であり、**isdn disconnect time**、**isdn disconnect input time**、**isdn disconnect output time** の 3 つのタイマコマンドでトラフィックを監視し、一定時間パケットが流れなくなった時点で回線を切断する。
課金単位時間方式では、課金単位時間と監視時間を **isdn disconnect interval time** コマンドで設定し、監視時間中にパケットが流れなければ課金単位時間の倍数の時間で回線を切断する。通信料金を減らす効果が期待できる。

[初期値]　1

[設定例]　*# isdn disconnect policy 2*
 # isdn disconnect interval time 240 6 2

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

5.2.17　切断タイマの設定 (ノーマル)

[書式]　**isdn disconnect time** *time*
no isdn disconnect time [*time*]

[設定値]　◦ *time*
- 秒数 (1..21474836.0)
- off.....タイマを設定しない

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

[ノート]　本コマンドの設定値を X 秒、**isdn disconnect input time** コマンドの設定値を IN 秒、**isdn disconnect output time** コマンドの設定値を OUT 秒とする。
X>IN または X>OUT のように設定した場合、パケットの入出力が観測されないと IN または OUT 秒で切断される。

[初期値]　60

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

5.2.18　切断タイマの設定 (ファスト)

[書式]　**isdn fast disconnect time** *time*
no isdn fast disconnect time [*time*]

[設定値]　◦ *time*
- 秒数 (1..21474836.0)
- off..... タイマを設定しない

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

[ノート]　同じ ISDN 回線に接続されている他の機器が Bch を使用している場合には、本コマンドは機能しないことがある。また、本機の PP Anonymous の接続がすべての Bch を使用している場合には、新たな PP Anonymous の接続を起動しても、本コマンドは機能しない。

[初期値]　20

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

5.2.19　切断タイマの設定 (強制)

[書式]　**isdn forced disconnect time** *time*
no isdn forced disconnect time [*time*]

[設定値]　◦ *time*
- 秒数 (1..21474836.0)
- off..... タイマを設定しない

[説明]　選択されている相手に接続する最大時間を設定する。秒数は 0.1 秒単位で設定できる。
パケットをやりとりしていても、このコマンドで設定した時間が経過すれば強制的に回線を切断する。
ダイヤルアップ接続でインターネット側からの無効なパケット (ping アタック等) が原因で回線が自動切断できない場合に有効。**isdn call block time** コマンドと併用するとよい。

[初期値]　off

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

5.2.20　入力切断タイマの設定 (ノーマル)

[書式]　**isdn disconnect input time** *time*
no isdn disconnect input time [*time*]

[設定値]　◦ *time*
- 秒数 (1..21474836.0)
- off..... タイマを設定しない

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

[ノート]　例えば、UDP パケットを定期的に出すようなプログラムが暴走したような場合、本タイマを設定しておくことにより回線を切断することができる。
5.2.17 切断タイマの設定 (ノーマル) のノート参照。

[初期値]　120

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

5.2.21　出力切断タイマの設定 (ノーマル)

[書式]　**isdn disconnect output time** *time*
no isdn disconnect output time [*time*]

[設定値]　◦ *time*
- 秒数 (1..21474836.0)
- off.....タイマを設定しない

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

[ノート]　例えば、UDP パケットを定期的に出すようなプログラムが暴走したような場合、本タイマを設定しておくことにより回線を切断することができる。
5.2.17 切断タイマの設定 (ノーマル) のノート参照。

[初期値]　120

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

5.2.22　課金単位時間方式での課金単位時間と監視時間の設定

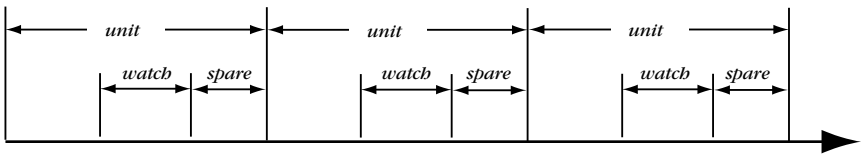
[書式]　**isdn disconnect interval time** *unit watch spare*
no isdn disconnect interval time [*unit watch spare*]

[設定値]　◦ *unit*.....課金単位時間
- 秒数 (1..21474836.0)
- off

◦ *watch*.....監視時間
- 秒数 (1..21474836.0)
- off

◦ *spare*.....切断余裕時間
- 秒数 (1..21474836.0)
- off

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



watch で示した間だけトラフィックを監視し、この間にパケットが流れなければ回線を切断する。*spare* は切断処理に時間がかかりすぎて、実際の切断が単位時間を越えないように余裕を持たせるために使う。
回線を接続している時間が *unit* の倍数になるので、単純トラフィック監視方式よりも通信料金を減らす効果が期待できる。

[初期値]　*unit* = 180
watch = 6
spare = 2

[設定例]　# isdn disconnect policy 2
isdn disconnect interval time 240 6 2

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

6. フレームリレー関連の設定

BRI インタフェースまたは PRI インタフェースを持つ機種ではアクセス回線としてフレームリレーに対応しています。

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

DLCI[2] はフレームリレーで相手先を指定するための識別子です。1 本の回線で複数の DLCI を利用することができ、回線を論理多重化してそれぞれが仮想的な専用線のようにネットワークを構築することができます。具体的な DLCI の値はフレームリレーネットワーク提供者との契約時に決まります。
DLCI をルーターに設定する方法は、ルーターによる自動取得と管理者による手動設定の 2 種類があります。手動設定は **fr dlci** コマンドで行います。
自動取得の場合には PVC[3] 状態確認手順の LMI[4] により行われます。本機は JT-Q933 と ANSI の 2 種類の LMI をサポートしており、**fr lmi** コマンドを使用していずれかを指定します。手動設定の場合、DLCI は最大 96 個まで設定できます。自動取得の場合には、制限はありません。DLCI は **show dlci** コマンドで確認することができます。

一般に、フレームリレーでのルーティングは 1 つの相手先情報番号に複数の相手先 (DLCI) が接続するために PP 側は numbered となります。相手の PP 側の IP アドレスと DLCI の対応を解決するプロトコルが InARP[5] です。InARP を使用するか否かは **fr inarp** コマンドで設定します。
本機の特徴として、直接 DLCI を指定してルーティングすることが可能です。この場合は PP 側の IP アドレス (**ip pp address** コマンド) を設定せず、PP 側 unnumbered のスタティックルーティングとなり InARP も使用されません。
ヤマハルーター同士であれば、unnumbered でダイナミックルーティングが可能です。

データ圧縮機能によってフレームリレー回線上での通信負荷を最大 2/5 程度まで軽減することが可能です。
本機能の実装は Frame Relay Forum の FRF.9 に基づいており、特に、FRF.9 のモード 1 に対応しています。データの圧縮と伸長アルゴリズムは Stac LZS を使用します。
このデータ圧縮機能を使用するか否かは **fr compression use** コマンドで設定します。
なお、このデータ圧縮機能が適用できる対地の最大数は、本機では 50 であり、これを超える数の対地に対して本機能を適用することはできません。

同じフレームリレー回線に PP インタフェースを複数バインドする場合、最も若い PP インタフェースが代表となります。
pp encapsulation fr の設定は、関係するすべてのインタフェースに対して設定する必要があります。一方、**fr lmi** 、**fr inarp** 、**fr congestion control**、そして、**fr pp dequeue type** の各コマンドは代表のインタフェースにのみ設定します。
データリンクの DLCI 値が **fr dlci** コマンドで明示的に設定されている場合には、その設定のあるインタフェースにデータリンクが収容されます。その DLCI 値が複数のインタフェースで設定されている場合には、まず代表のインタフェースが優先され、その後の優先順位は番号の若い順となります。
データリンクの DLCI 値が、**fr dlci** コマンドで明示的に設定されていない場合には、**fr dlci** auto が設定されているインタフェースにデータリンクが収容されます。**fr dlci** auto の設定されたインタフェースがない場合にはどのインタフェースにも収容されません。**fr dlci** auto の設定されたインタフェースが複数ある場合は、まず代表のインタフェースが優先され、その後の優先順位は番号の若い順となります。

6.1 カプセル化の種類の設定

[書式]
pp encapsulation *type*
no pp encapsulation [*type*]

[設定値]
◦ *type*
- ppp ..... PPP でカプセル化する
- fr ..... フレームリレーでカプセル化する

[説明] 選択されている相手のカプセル化の種類を設定する。

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

[初期値] ppp

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

1. High level Data Link Control procedure
2. Data Link Connection Identifier
3. Permanent Virtial Circuit
4. Local Management Interface
5. Inverse Address Resolution Protocol; RFC1293

6.2　DLCI の設定

[書式]　**fr dlci** *dlci_num*
no fr dlci [*dlci_num*]

[設定値]　◦ *dlci_num*
- auto.....DLCI を自動取得する
- DLCI 値 (16..991) を空白で区切って並べたもの (96 個以内)

[説明]　選択されている相手で使用する DLCI を自動設定するか、または手動設定する。
auto に設定した場合は PVC 状態確認手順により DLCI を自動取得する。

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

[初期値]　auto

[設定例]　# fr dlci 16 17 18

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

6.3　DLCI ごとのパラメータの設定

[書式]　**fr cir** dlci=*dlci_num cir* [slowstart-idle=*idle*] [bc=*bc_size*] [be=*be_size*] [s=*step_count*]
no fr cir dlci=*dlci_num*

[設定値]　◦ *dlci_num*.....DLCI 値 (16..991)
◦ *cir*.....CIR 値 (bit/s 単位)
◦ *idle*.....スロースタート状態に戻るまでのアイドル時間
- 秒数 (1..2147483647)
- 0.....スロースタート動作を行わない

◦ *bc_size*.....認定バーストサイズ (ビット)
◦ *be_size* .....超過バーストサイズ (ビット)
◦ *step_count*.....ステップカウント

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

[初期値]　*idle* = 20
bc=*be* = 7000
s=cir/ bc_size/ be_size から計算される値

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

6.4　PVC 状態確認手順の設定

[書式]　**fr lmi** *lmi*
no fr lmi [*lmi*]

[設定値]　◦ *lmi*
- q933.....TTC 標準 JT-Q933 付属資料 A に基づいて状態確認を行う
- ansi .....ANSI T1.617 AnnexD に基づいて状態確認を行う
- off.....PVC 状態確認手順は行わない

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

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

[初期値]　q933

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

6.5　InARP 使用の設定

[書式]　**fr inarp** *inarp*
no fr inarp [*inarp*]

[設定値]　◦ *inarp*
- on..... 使用する
- off..... 使用しない

[説明]　選択されている相手について、InARP (Inverse Address Resolution Protocol) を使用して、相手の IP アドレスを自動取得するかどうかを設定する。この設定が on の場合でも、自分の PP 側のローカル IP アドレスが設定されていない場合 (unnumbered) は InARP は使用しない。
また、自分の PP 側ローカル IP アドレスが設定されていれば、相手から InARP のリクエストが来た場合、この設定に関わらず常にレスポンスを返す。

[ノート]　**ip pp address** コマンドを参照

[初期値]　on

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

6.6　フレームリレーダウン時にバックアップする相手先情報番号の設定

[書式]　**fr backup** dlci=*dlci_num peer_num*
no fr backup dlci=*dlci_num* [*peer_num*]

[設定値]　◦ *dlci_num*..... DLCI 値 (16..991)
◦ *peer_num*..... バックアップする相手先情報番号

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

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

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	RT250i	~~RT107e~~	~~SRT100~~

6.7　FR 圧縮機能の設定

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

[設定値]　◦ *dlci_num*
- DLCI 値 (16..991)
- * (すべてのデータリンク)

◦ *type*
- stac..... Stac LZS 方式を用いてデータを圧縮する
- cstac..... cstac 方式を用いてデータを圧縮する
- none..... データを圧縮しない

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

[初期値]　*type* = none

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

6.8　輻輳制御をするか否かの設定

[書式]　**fr congestion control** *control*
no fr congestion control [*control*]

[設定値]　◦ *control*
- on ..... 輻輳制御を行う
- off..... 輻輳制御を行わない

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

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

[初期値]　off

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

6.9　回線に対する送信順序方式の設定

[書式]　**fr pp dequeue type** *type*
no fr pp dequeue type [*type*]

[設定値]　◦ *type*
- serial .....順次サーチ方式
- round-robin .....ラウンドロビン方式

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

[ノート]　相手先情報番号の若い PP インタフェースがより高い順位を持つものと定義する。

[初期値]　round-robin

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

6.10　指定パケットに DE ビットを立てるか否かの設定

[書式]　**fr de** *protocol* filter dlci=*dlci_num filter_num_list*
no fr de *protocol* filter dlci=*dlci_num* [*filter_num_list*]

[設定値]　◦ *protocol*
- ip.....IP パケット
- ipx.....IPX パケット
- bridge .....ブリッジするパケット

◦ filter.....固定のキーワード

◦ *dlci_num*
- DLCI 値 (16..991)
- * (すべてのデータリンク)

◦ *filter_num_list* .....静的フィルタ番号 (1..100) の並び

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

[ノート]　RTX1200 は、PROTOCOL に ipx,brigde は指定できない。

[初期値]　DE ビットは立てない

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

7.　PRI 関連の設定

RTX3000、RT250i および RT300i は、オプションの PRI 拡張モジュールを装着することにより一次群速度インタフェース (PRI:Primary Rate Interface) に対応します。多重化非対応の PRI 拡張モジュール (製品番号：YBA-1PRI-N) は、192kbit/s ～ 1.5Mbit/s のスーパーリレー FR や DA1500 などの高速ディジタル専用線に最適です。多重化対応の PRI 拡張モジュール (製品番号：YBA-1PRI-M/MB/MC) を利用すると、それに加えて最大 24 対地までの HSD の多重アクセスサービスや INS ネット 1500 を利用することができます。

サービスを利用するためにはオプションモジュールを購入していただく必要があります。また、DSU はどのオプションモジュールにも内蔵しておりませんので別途用意してください。

機種	192kbit/s ～ 1.5Mbit/s 専用線 (A)	192kbit/s ～ 1.5Mbit/s 専用線多重 (B)	回線交換 (C)
RT300i RT250i	YBA-1PRI-N YBA-1PRI-M YBA-1PRI-MB YBA-1PRI-MC	YBA-1PRI-M YBA-1PRI-MB YBA-1PRI-MC	YBA-1PRI-M YBA-1PRI-MB YBA-1PRI-MC
RTX3000	YBA-1PRI-MC	YBA-1PRI-MC	YBA-1PRI-MC

(A): HSD, DA1500, スーパーリレー FR
(B): HSD の多重アクセスサービス
(C): INS ネット 1500
YBA-1PRI-N: 多重化非対応 PRI 拡張モジュール
YBA-1PRI-M/MB/MC: 多重化、回線交換対応 PRI 拡張モジュール

専用線を利用するためには、PRI ネットワーク提供者との契約で指定されたタイムスロットに関する値を **pri leased channel** コマンドで設定します。PRI を経由してパケットをやり取りするためには、**pp bind** コマンドで相手先情報番号 (pp) と PRI インタフェース名、情報チャネル番号 (pri1/1) を関連づけます。専用線に関する設定は次のようになります。

```
pri leased channel 1/1 1 24
pp select 1
pp bind pri1/1
pp enable 1
```

また、回線交換を利用するためには、通信回線種別を **line type** コマンドで isdn に設定します。PRI を経由してパケットをやり取りするためには、**pp bind** コマンドで相手先情報番号 (pp) と PRI インタフェース名 (pri1) を関連づけます。選択されている相手の発着信用の ISDN 番号を ***isdn remote address*** コマンドで設定します。回線交換に関する設定は次のようになります。

```
line type pri1 isdn
pp select 1
pp bind pri1
isdn remote address call ISDN 番号
pp enable 1
```

これにルーティングに関する設定を追加すると PRI を経由してパケットをやり取りすることができます。

実際に、別途用意していただいた DSU とルーター間を付属のコネクタケーブルで繋いで、***show status pri1*** コマンドで表示されるレイヤ 1 情報、回線交換ではレイヤ 2 まで、物理的配線が適切であるか確認することができます。

専用線に対しては、接続環境が適切であるかどうか確認するためのループバック試験を行うことができます。ループバック試験は、指定したデータを指定したループバックポイントまたは対向ルーターで折り返して、送信データと折り返しデータを比較して正常性の検証を行います。ループバックには、検証を行う Active 側と単に受け取ったデータを折り返す Passive 側があり、ルーターはどちらか一方で動作します。Active 側にはハードウェアの正常性を確認するためのループバック A と回線上にデータを流して、対向ルーターからの折り返しデータを比較検証するタイムスロットループバックがあります。Passive 側のループバックポイントは機種により若干異なります。ハードウェアの制限により、タイムスロットポイントで折り返したデータも受けることは出来ませんので注意が必要です。

ループバックは、コンソールコマンドから実行します。結果は Active 側のコンソールにだけ表示します。ループバック試験を行う前に、通常の通信を **pp disable** コマンドで停止させてから行ってください。Active 側のタイムスロットループバックでは、相手側のルーターは **pri loopback passive** コマンドで待ち受け状態にしておく必要があります。ループバック A はコネクタケーブルを抜いた状態でないと実行できません。

7.1　PRI 回線の種類の設定

[書式]　**line type** *interface line*
no line type *interface line*

[設定値]
- *interface*.....PRI インタフェース名
- *line*
  - isdn, isdn-ntt.....ISDN 回線交換
  - leased.....ディジタル専用線

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

[初期値]　leased

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	RT250i	~~RT107e~~	~~SRT100~~

7.2　情報チャネルとタイムスロットの設定

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

[設定値]
- *pri*.....PRI インタフェース名
- *info*.....情報チャネル番号 (1..24)
- *timeslot_head*.....先頭タイムスロット番号 (1..24)
- *timeslot_num*.....タイムスロット数 (1..24)

以下のニーモニックが使用可能

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

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

[ノート]　設定変更時には再起動か、対象の PRI インタフェースに対する **interface reset** コマンドが必要である。
RT250i と RT300i の多重化非対応の PRI 拡張モジュール (YBA-1PRI-N) では、2 つ以上の情報チャネルは設定できない。

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	RT250i	~~RT107e~~	~~SRT100~~

7.3　PP で使用するインタフェースの設定

[書式]　**pp bind** *interface/pri_num* [*interface/info*]
no pp bind [*interface/info*]

[設定値]
- *interface*.....PRI インタフェース名
- *pri_num*.....インタフェース番号
- *info*.....情報チャネル番号

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

[ノート]　PRI 回線を専用線として使用する場合、**pri leased channel** コマンドで設定した情報チャネル番号を、インタフェース名に付加する必要がある。
例えば、pri leased channel 1/1 1 24 の場合は、**pp bind** pri1/1 となる。

[初期値]　どのインタフェースともバインドされていない

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	RT250i	~~RT107e~~	~~SRT100~~

8. IP の設定

8.1 インタフェース共通の設定

8.1.1 IP パケットを扱うか否かの設定

[書式] **ip routing** *routing*
no ip routing [*routing*]

[設定値] ◦ *routing*
- on..... IP パケットを処理対象として扱う
- off..... IP パケットを処理対象として扱わない

[説明] IP パケットをルーティングするかどうかを設定する。

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

[初期値] on

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

8.1.2 IP アドレスの設定

[書式] **ip** *interface* **address** *ip_address/mask* [broadcast *broadcast_ip*]
ip *interface* **address** dhcp
ip pp address *ip_address/mask* [broadcast *broadcast_ip*]
ip *loopback* **address** *ip_address/mask*
ip *bridge_interface* **address** *ip_address/mask* [broadcast *broadcast_ip*]
ip *bridge_interface* **address** dhcp [autoip=*switch*]
no ip *interface* **address** [*ip_address/mask* [broadcast *broadcast_ip*]]
no ip pp address [*ip_address/mask* [broadcast *broadcast_ip*]]
no ip *loopback* **address** [*ip_address/mask*]
no ip *bridge_interface* **address** [*ip_address/mask* [broadcast *broadcast_ip*]]

[設定値] ◦ *interface*..... LAN インタフェース名
◦ *loopback*..... LOOPBACK インタフェース名
◦ *bridge_interface*..... ブリッジインタフェース名
◦ *ip_addres*..... IP アドレス xxx.xxx.xxx.xxx (xxx は十進数)
◦ dhcp..... DHCP クライアントとして IP アドレスを取得することを示すキーワード
◦ *mask*
- xxx.xxx.xxx.xxx (xxx は十進数)
- 0x に続く十六進数
- マスクビット数

◦ *broadcast_ip*..... ブロードキャスト IP アドレス
◦ *switch*
- on..... AutoIP 機能を使う
- off..... AutoIP 機能を使わない

[説明] インタフェースの IP アドレスとネットマスクを設定する。“broadcast *broadcast_ip*”を指定すると、ブロードキャストアドレスを指定できる。省略した場合には、ディレクティッドブロードキャストアドレスが使われる。
dhcp を指定すると、設定直後に DHCP クライアントとして IP アドレスを取得する。また dhcp を指定している場合に **no ip** *interface* **address** を入力すると、取得していた IP アドレスの開放メッセージを DHCP サーバーに送る。
AutoIP 機能を使うに設定し、**ip** *bridge_interface* **dhcp retry** 設定で dhcp の retry 回数が有限に設定してあると、dhcp でのアドレスの 割り当てが失敗した場合に自動的に 169.254.0.0/16 のアドレスが決定される。

[ノート] LAN インタフェースに IP アドレスを設定していない場合には、RARP により IP アドレスを得ようとする。
PP インタフェースに IP アドレスを設定していない場合には、そのインタフェースは unnumberedとして動作する。
DHCP クライアントとして動作させた場合に取得したクライアント ID は、***show status dhcpc*** コマンドで確認することができる。
LOOPBACK インタフェースを指定できるのは Rev.8.03 以降のリビジョンである。

ブリッジインタフェースを指定できるのは Rev.10.00.38 以降のリビジョンである。

工場出荷状態および cold start コマンド実行後の本コマンドの設定値については「1.7 工場出荷設定値について」を参照してください。

[初期値]　IP アドレスは設定されていない
ディレクティッドブロードキャストアドレスが使われる
autoip=off を追加

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.1.3　セカンダリ IP アドレスの設定

[書式]　**ip** *interface* **secondary address** *ip_address*[*/mask*]
ip *interface* **secondary address** dhcp
no ip *interface* **secondary address** [*ip_address/mask*]

[設定値]
- *interface*.....LAN インタフェース名
- *ip_address*.....セカンダリ IP アドレス *xxx.xxx.xxx.xxx* (*xxx* は十進数)
- dhcp.....DHCP クライアントとして IP アドレスを取得することを示すキーワード
- *mask*
  - *xxx.xxx.xxx.xxx* (*xxx* は十進数)
  - 0x に続く十六進数
  - マスクビット数

[説明]　LAN 側のセカンダリ IP アドレスとネットマスクを設定する。
dhcp を指定すると、設定直後に DHCP クライアントとして IP アドレスを取得する。

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

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.1.4　インタフェースの MTU の設定

[書式]　**ip** *interface* **mtu** *mtu0*
ip pp mtu *mtu1*
ip tunnel mtu *mtu2*
no ip *interface* **mtu** [*mtu0*]
no ip pp mtu [*mtu1*]
no ip tunnel mtu [*mtu2*]

[設定値]
- *interface*.....LAN インタフェース名
- *mtu0, mtu1, mtu2*...MTU の値 (64..1500；RTX3000 の LAN1 と LAN2 の場合は 64..9578)

[説明]　各インタフェースの MTU の値を設定する。

[ノート]　実際にはこの設定が適用されるのは IP パケットだけである。他のプロトコルには適用されず、それらではデフォルトのまま 1500 の MTU となる。
RT250i には **ip tunnel mtu** コマンドはない。

[初期値]　*mtu0*=1500
mtu1=1500
mtu2=1280

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.1.5　echo, discard, time サービスを動作させるか否かの設定

[書式]　**ip simple-service** *service*
no ip simple-service [*service*]

[設定値]
- *service*
  - on.....TCP/UDP の各種サービスを動作させる
  - off.....サービスを停止させる

[説明]　TCP/UDP の echo(7)、discard(9)、time(37) の各種サービスを動作させるか否かを設定する。サービスを停止すると該当のポートも閉じる。

[ノート]　Rev.8.01.12 以降で、初期値が on から off に変更。

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.1.6　IP の静的経路情報の設定

[書式]

ip route *network* gateway *gateway1* [*parameter*] [gateway *gateway2* [*parameter*]...]
no ip route *network* [gateway...]

[設定値]

◦ *network*
- default..... デフォルト経路
- IP アドレス ..... 送り先のホスト / マスクビット数
- 省略時は 32

◦ *gateway1, gateway2*
- IP アドレス ..... xxx.xxx.xxx.xxx (xxx は十進数)
- pp *peer_num* [dlci=*dlci*] .PP インタフェースへの経路
  "dlci=*dlci*" が指定された場合は、フレームリレーの DLCI への経路
  - *peer_num*
    - 相手先情報番号
    - anonymous
- pp anonymous name=*name*
  - *name*.....PAP/CHAP による名前
- dhcp *interface*
  - *interface* .....DHCP にて与えられるデフォルトゲートウェイを使う場合の、DHCP クライアントとして動作する LAN インタフェース名、ブリッジインタフェース名 (送り先が Default の時のみ有効)
- tunnel *tunnel_num*.....トンネルインタフェースへの経路
- LOOPBACK インタフェース名、NULL インタフェース名

◦ *parameter*..... 以下のパラメータを空白で区切り複数設定可能
- filter *number* [*number*..]. フィルタ型経路の指定
  - *number* .....フィルタの番号 (1..21474836) (空白で区切り複数設定可能)
- metric *metric* ..... メトリックの指定
  - *metric*
    - メトリック値 (1..15)
    - 省略時は 1
- hide..... 出力インタフェースが LAN インタフェース、または PP インタフェース、TUNNEL インタフェースの場合のみ有効なオプションで、相手先が接続されている場合だけ経路が有効になることを意味する
- weight *weight* .... 異なる経路間の比率を表す値
  - *weight*
    - 経路への重み (0..2147483647)
    - 省略時は 1
- keepalive ..... *gateway1* に到達性のあるときにだけ有効となる。

[説明]

IP の静的経路を設定する。
gateway のパラメータとしてフィルタ型経路を指定した場合には、記述されている順にフィルタを適用していき、適合したゲートウェイが選択される。
適合するゲートウェイが存在しない場合や、フィルタ型経路が指定されているゲートウェイが一つも記述されていない場合には、フィルタ型経路が指定されていないゲートウェイが選択される。
フィルタ型経路が指定されていないゲートウェイも存在しない場合には、その経路は存在しないものとして処理が継続される。
フィルタ型経路が指定されていないゲートウェイが複数記述された場合の経路の選択は、それらの経路を使用する時点でラウンドロビンにより決定される。

filter が指定されていないゲートウェイが複数記述されている場合で、それらの経路を使うべき時にどちらを使うかは、始点 / 終点 IP アドレス、プロトコル、始点 / 終点ポート番号により識別されるストリームにより決定される。同じストリームのパケットは必ず同じゲートウェイに送出される。*weight* で値 (例えば回線速度の比率) が指定されている場合には、その値の他のゲートウェイの *weight* 値に対する比率に比例して、その経路に送出されるストリームの比率が上がる。

いずれの場合でも、hide キーワードが指定されているゲートウェイは、回線が接続している場合のみ有効で、回線が接続していない場合には評価されない。なお LOOPBACK インタフェース、NULL インタフェースは常にアップ状態なので、hide オプションは指定はできるものの意味はない。

複数のゲートウェイを設定した時に、ロードバランスをせずに特定のゲートウェイだけを優先的に使用するには、*weight* オプションで 0 を設定する。*weight* で 0 を指定できるのは Rev.7.01 系以降である。

[ノート]

既に存在する経路を上書きすることができる。
RT107e では、Rev.8.03.42 以降で keepalive オプションを指定することができる。
LOOPBACK インタフェース、NULL インタフェースを指定できるのは Rev.8.03 以降のリビジョンである。
ブリッジインタフェースを指定できるのは Rev.10.00.38 以降のリビジョンである。

[設定例]

◦デフォルトゲートウェイを 192.168.0.1 とする。
 # ip route default gateway 192.168.0.1

◦PP1 で接続している相手のネットワークは 192.168.1.0/24 である。
 # ip route 192.168.1.0/24 gateway pp 1

◦マルチホーミングによる負荷分散を行う。デフォルトゲートウェイとして 2 経路持ち、PP1 には専用線 128k で、PP2 には専用線 64k で接続しており、かつ各専用線ダウン時の経路を無効としてパケットロスを防ぐ。
※ NAT 機能と専用線キープアライブの併用が必要となる。
 # ip route default gateway pp 1 weight 2 hide gateway pp 2 weight 1 hide

◦PP1 が有効な時には PP1 のみが使われる。PP1 がダウンすると PP2 が使われる。
 # ip route 192.168.0.1/24 gateway pp 1 hide gateway pp 2 weight 0

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.1.7　IP パケットのフィルタの設定

[書式]

ip filter *filter_num pass_reject src_addr[/mask] [dest_addr[/mask] [protocol [src_port_list [dest_port_list]]]]*
no ip filter *filter_num [pass_reject]*

[設定値]

◦*filter_num*.....静的フィルタ番号 (1..21474836)

◦*pass_reject*
- pass-log .....一致すれば通す (ログに記録する)
- pass-nolog .....一致すれば通す (ログに記録しない)
- reject-log .....一致すれば破棄する (ログに記録する)
- reject-nolog .....一致すれば破棄する (ログに記録しない)
- restrict-log .....回線が接続されていれば通し、切断されていれば破棄する (ログに記録する)
- restrict-nolog .....回線が接続されていれば通し、切断されていれば破棄する (ログに記録しない)

◦*src_addr*.....IP パケットの始点 IP アドレス
- xxx.xxx.xxx.xxx xxx (xxx は十進数)
- * (ネットマスクの対応するビットが 8 ビットとも 0 と同じ。すべての IP アドレスに対応)
- 間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。

◦*dest_addr*.....IP パケットの終点 IP アドレス (*src_addr* と同じ形式)。
省略時は 1 個の * と同じ。

◦*mask*.....IPアドレスのビットマスク *(src_addr* および *dest_addr* がネットワークアドレスの場合のみ指定可)
- xxx.xxx.xxx.xxx (xxx は十進数)
- 0x に続く十六進数
- マスクビット数
- 省略時は 0xffffffff と同じ

◦*protocol*.....フィルタリングするパケットの種類
- プロトコルを表す十進数 (0..255)
- プロトコルを表すニーモニック

ニーモニック	十進数	説明
icmp	1	ICMP パケット
tcp	6	TCP パケット
udp	17	UDP パケット
ipv6	41	IPv6 パケット
gre	47	GRE パケット
esp	50	ESP パケット
ah	51	AH パケット
icmp6	58	ICMP6 パケット

- 上項目のカンマで区切った並び (5 個以内)
- 特殊指定

icmp-error	TYPE が 3、4、5、11、12、31、32 のいずれかである ICMP パケット
icmp-info	TYPE が 0、8 ～ 10、13 ～ 18、30、33 ～ 36 のいずれかである ICMP パケット
tcpfin	FIN フラグの立っている tcp パケット
tcprst	RST フラグの立っている tcp パケット
established	ACK フラグの立っている tcp パケット内から外への接続は許可するが、外から内への接続は拒否する機能
tcpflag=*value/mask* tcpflag!=*value/mask*	TCP フラグの値と MASK の値の論理積 (AND) が、VALUE に一致、または不一致である TCP パケット VALUE と MASK は 0x に続く十六進数で 0x0000 ～ 0xffff
*	すべてのプロトコル

- 省略時は * と同じ。

◦ *src_port_list*..... PROTOCOL に、TCP (tcp/tcpfin/tcprst/established/tcpflag)、UDP (udp) のいずれかが含まれる場合は、TCP/UDP のソースポート番号。PROTOCOL が ICMP (icmp) 単独の場合には、ICMP タイプ。

- ポート番号、タイプを表す十進数
- ポート番号を表すニーモニック (一部)

ニーモニック	ポート番号
ftp	20,21
ftpdata	20
telnet	23
smtp	25
domain	53
gopher	70
finger	79
www	80
pop3	110
sunrpc	111

ニーモニック	ポート番号
ident	113
ntp	123
nntp	119
snmp	161
syslog	514
printer	515
talk	517
route	520
uucp	540

- 間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。
- 上項目のカンマで区切った並び (10 個以内)
- * (すべてのポート、タイプ)
- 省略時は * と同じ。

◦ *dest_port_list*..... PROTOCOL に、TCP(tcp/tcpfin/tcprst/established/tcpflag)、UDP(udp) のいずれかが含まれる場合は、TCP/UDP のデスティネーションポート番号。PROTOCOL が ICMP(icmp) 単独の場合には、ICMP コード。

[説明]　IP パケットのフィルタを設定する。本コマンドで設定されたフィルタは **ip** *interface* **secure filter**、**ip filter set**、**ip filter dynamic**、および **ip** *interface* **rip filter** コマンドで用いられる。

[ノート]　restrict-log 及び restrict-nolog を使ったフィルタは、回線が接続されている時だけ通せば十分で、そのために回線に発信するまでもないようなパケットに有効である。例えば、時計を合わせるための NTP パケットがこれに該当する。ICMP パケットに対して、ICMP タイプと ICMP コードをフィルタでチェックしたい場合には、PROTOCOL には 'icmp' だけを単独で指定する。PROTOCOL が 'icmp' 単独である場合にのみ、SRC_PORT_LIST は ICMP タイプ、DEST_PORT_LIST は ICMP コードと見なされる。PROTOCOL に 'icmp' と他のプロトコルを列挙した場合には SRC_PORT_LIST と DEST_PORT_LIST の指定は TCP/UDP のポート番号と見なされ、ICMP パケットとの比較は行われない。また、PROTOCOL に 'icmp-error' や 'icmp-info' を指定した場合には、SRC_PORT_LIST と DST_PORT_LIST の指定は無視される。PROTOCOL に '*' を指定するか、TCP/UDP を含む複数のプロトコルを列挙している場合には、SRC_PORT_LIST と DEST_PORT_LIST の指定は TCP/UDP のポート番号と見なされ、パケットが TCP または UDP である場合のみポート番号がフィルタが比較される。パケットがその他のプロトコル (ICMP を含む) の場合には、SRC_PORT_LIST と DEST_PORT_LIST の指定は存在しないものとしてフィルタと比較される。
ICMP のタイプとコードを指定できるのは、
RTX1500、RTX1100、RT107e ..... Rev.8.03.68 以降、
RTX3000 ..... Rev.9.00.31 以降

[設定例]

```
# ip filter 1 pass-nolog 172.20.10.* 172.21.192.0/18 tcp ftp
```

LAN1 で送受信される IPv4 ICMP ECHO/REPLY を pass-log で記録する

```
# ip lan1 secure filter in 1 2 100
# ip lan1 secure filter out 1 2 100
# ip filter 1 pass-log * * icmp 8
# ip filter 2 pass-log * * icmp 0
# ip filter 100 pass * *
```

LAN2 から送信される IPv4 Redirect のうち、"for the Host" だけを通さない

```
# ip lan2 secure filter out 1 100
# ip filter 1 reject * * icmp 5 1
# ip filter 100 pass * *
```

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.1.8　フィルタセットの定義

[書式]　**ip filter set** *name direction filter_list* [*filter_list ...*]
no ip filter set *name* [*direction ...*]

[設定値]
- *name*.....フィルタセットの名前を表す文字列
- *direction*
  - in.....入力方向のフィルタ
  - out.....出力方向のフィルタ
- *filter_list*.....空白で区切られたフィルタ番号の並び (100 個以内)

[説明]　フィルタセットを定義する。フィルタセットは、in/out のフィルタをそれぞれ定義し、RADIUS による指定や、**ip** *interface* **secure filter** コマンドによりインタフェースに適用される。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

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

[書式]　**ip filter source-route** *filter_out*
no ip filter source-route [*filter_out*]

[設定値]
- *filter_out*
  - on.....フィルタアウトする
  - off.....フィルタアウトしない

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

[初期値]　on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.1.10　ディレクテッドブロードキャストパケットをフィルタアウトするか否かの設定

[書式]　**ip filter directed-broadcast** *filter_out*
ip filter directed-broadcast filter *filter_num* [*filter_num ...*]
no ip filter directed-broadcast

[設定値]
- *filter_out*
  - on.....フィルタアウトする
  - off.....フィルタアウトしない
- *filter_num*.....静的フィルタ番号 (1..21474836)

[説明]　終点 IP アドレスがディレクテッドブロードキャストアドレス宛になっている IP パケットをルーターが接続されているネットワークにブロードキャストするか否かを設定する。

on を指定した場合には、ディレクティッドブロードキャストパケットはすべて破棄する。
off を指定した場合には、ディレクティッドブロードキャストパケットはすべて通過させる。
filter を指定した場合には、**ip filter** コマンドで設定したフィルタでパケットを検査し、PASS フィルタにマッチした場合のみパケットを通過させる。

[ノート]　このコマンドでのチェックよりも、**wol relay** コマンドのチェックの方が優先される。**wol relay** コマンドでのチェックにより通過させることができなかったパケットのみが、このコマンドでのチェックを受ける。
いわゆる smurf 攻撃を防止するためには on にしておく。
第 2 書式は Rev.7.01.34、Rev.8.01.12、Rev.10.00.31 以降で使用可能。

[初期値]　on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.1.11　動的フィルタの定義

[書式]　**ip filter dynamic** *dyn_filter_num srcaddr dstaddr protocol* [*option ...*]
ip filter dynamic *dyn_filter_num srcaddr dstaddr* filter *filter_list* [in *filter_list*] [out *filter_list*] [*option ...*]
no ip filter dynamic *dyn_filter_num* [*dyn_filter_num...*]

[設定値]
- *dyn_filter_num*.....動的フィルタ番号 (1..21474836)
- *srcaddr*.....始点 IP アドレス
- *dstaddr*.....終点 IP アドレス
- *protocol*.....プロトコルのニーモニック

- tcp
- udp
- ftp
- tftp
- domain
- www
- smtp
- pop3
- telnet
- netmeeting

◦ *filter_list* ..... **ip filter** コマンドで登録されたフィルタ番号のリスト

◦ *option*

- syslog=*switch*
  - on .....コネクションの通信履歴を SYSLOG に残す
  - off .....コネクションの通信履歴を SYSLOG に残さない
- timeout=*time*
  - *time*.....データが流れなくなったときにコネクション情報を解放するまでの秒数

[説明]　動的フィルタを定義する。第 1 書式では、あらかじめルーターに登録されているアプリケーション名を指定する。第 2 書式では、ユーザがアクセス制御のルールを記述する。キーワードの filter、in、out の後には、**ip filter** コマンドで定義されたフィルタ番号を設定する。
filterキーワードの後に記述されたフィルタに該当するコネクション (トリガ) を検出したら、それ以降 inキーワードと out キーワードの後に記述されたフィルタに該当するコネクションを通過させる。in キーワードはトリガの方向に対して逆方向のアクセスを制御し、out キーワードは動的フィルタと同じ方向のアクセスを制御する。なお、**ip filter** コマンドの IP アドレスは無視される。pass/reject の引数も同様に無視される。
プロトコルとして tcp や udp を指定した場合には、アプリケーションに固有な処理は実施されない。特定のアプリケーションを扱う必要がある場合には、アプリケーション名を指定する。

[初期値]　syslog=on

[設定例]　# ip filter 10 pass * * udp * snmp
ip filter dynamic 1 * * filter 10

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	~~SRT100~~

8.1.12　動的フィルタのタイムアウトの設定

[書式]　**ip filter dynamic timer** [*option*=*timeout* [*option*...]]
no ip filter dynamic timer

[設定値]　◦ *option*.....オプション名

- tcp-syn-timeout ... SYN を受けてから設定された時間内にコネクションが確立しなければセッションを切断する
- tcp-fin-timeout..... FIN を受けてから設定された時間が経てばコネクションを強制的に解放する
- tcp-idle-time ..... 設定された時間内に TCP コネクションのデータが流れなければコネクションを切断する
- udp-idle-time ..... 設定された時間内に UDP コネクションのデータが流れなければコネクションを切断する
- dns-timeout.....DNS の要求を受けてから設定された時間内に応答を受けなければコネクションを切断する

◦ *timeout*.....待ち時間 (秒)

[説明]　動的フィルタのタイムアウトを設定する。

[ノート]　本設定はすべての検査において共通に使用される。

[初期値]　tcp-syn-timeout=30
tcp-fin-timeout=5
tcp-idle-time=3600
udp-idle-time=30
dns-timeout=5

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	~~SRT100~~

8.1.13　侵入検知機能の動作の設定

[書式]

ip *interface* **intrusion detection** *direction* [*type*] *switch* [*option*]
ip pp intrusion detection *direction* [*type*] *switch* [*option*]
ip tunnel intrusion detection *direction* [*type*] *switch* [*option*]
no ip *interface* **intrusion detection** *direction* [*type*] *switch* [*option*]
no ip pp intrusion detection *direction* [*type*] *switch* [*option*]
no ip tunnel intrusion detection *direction* [*type*] *switch* [*option*]

[設定値]

◦ *interface*.....LAN インタフェース名

◦ *direction*.....観察するパケット・コネクションの方向
- in.....インタフェースの内向き
- out.....インタフェースの外向き

◦ *type*.....観察するパケット・コネクションの種類
- ip.....IP ヘッダ
- ip-option.....IP オプションヘッダ
- fragment.....フラグメント
- icmp .....ICMP
- udp.....UDP
- tcp.....TCP
- ftp .....FTP
- winny.....Winny
- share .....Share
- default.....設定していないものすべて

◦ *switch*
- on .....実行する
- off.....実行しない

◦ *option*
- *reject=on*.....不正なパケットを破棄する
- reject=off.....不正なパケットを破棄しない

[説明]

指定したインタフェースで、指定された向きのパケットやコネクションについて異常を検知する。
type パラメータを省略したときには、侵入検知機能の全体についての設定になる。

[ノート]

危険性の高い攻撃については、reject オプションの設定に関わらず、常にパケットを破棄する。

Winny については、バージョン 2 の検知が可能であり、それ以前のバージョンには対応していない。
また対応するのは Rev.8.03 系以降のリビジョンである。

RT250i には **ip tunnel intrusion detection** コマンドはない。

[初期値]

switch
- TYPE を指定しないとき ..... off
- TYPE を指定したとき ..... on

reject ..... off

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.1.14　1 秒間に侵入検知情報を通知する頻度の設定

[書式]

ip *interface* **intrusion detection notice-interval** *frequency*
ip pp intrusion detection notice-interval *frequency*
ip tunnel intrusion detection notice-interval *frequency*
no ip *interface* **intrusion detection notice-interval**
no ip pp intrusion detection notice-interval
no ip tunnel intrusion detection notice-interval

[設定値]

◦ *interface*.....LAN インタフェース名

◦ *frequency*.....頻度 (1…1000)

[説明]

1 秒間に侵入検知情報を通知する頻度を設定する。

[初期値]

1

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

8.1.15　重複する侵入検知情報の通知抑制の設定

[書式]　**ip** *interface* **intrusion detection repeat-control** *time*
ip pp intrusion detection repeat-control *time*
ip tunnel intrusion detection repeat-control *time*
no ip *interface* **intrusion detection repeat-control**
no ip pp intrusion detection repeat-control
no ip tunnel intrusion detection repeat-control

[設定値]　◦ *time*..... 秒数 (1..1000)

[説明]　同じホストに対する同じ種類の攻撃を、*time* 秒に 1 回のみ通知するよう抑制する。

[初期値]　60

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

8.1.16　侵入検知情報の最大表示件数の設定

[書式]　**ip** *interface* **intrusion detection report** *num*
ip pp intrusion detection report *num*
ip tunnel intrusion detection report *num*
no ip *interface* **intrusion detection report**
no ip pp intrusion detection report
no ip tunnel intrusion detection report

[設定値]　◦ *num*..... 件数 (1..1000)

[説明]　**show ip intrusion detection** コマンドで表示される侵入検知情報の最大件数を設定する。

[初期値]　50

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

8.1.17　侵入検知で用いる閾値の設定

[書式]　**ip** *interface* **intrusion detection threshold** *type count*
ip pp intrusion detection threshold *type count*
ip tunnel intrusion detection threshold *type count*
no ip *interface* **intrusion detection threshold** *type*
no ip pp intrusion detection threshold *type*
no ip tunnel intrusion detection threshold *type*

[設定値]　◦ *type*..... 閾値を設定する攻撃の種類
- port-scan..... ポートスキャン
- syn-flood..... SYN フラッド

◦ *count*..... 閾値 (1..65535)

[説明]　侵入検知で用いる閾値を設定する。攻撃のタイプと設定する数値の意味は以下のようになる。

type	*count* **値の意味**
port-scan	同じホストに対して、1 秒間に *count* 種類の異なるポートへのアクセスを検出したらポートスキャンと判定する
syn-flood	同じホストに対するSYN パケットを、1 秒間に *count* 回以上検出したらSYN フラッドと判定する

[初期値]　port-scan = 64
syn-flood = 100

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

8.1.18　TCP セッションの MSS 制限の設定

[書式]　**ip** *interface* **tcp mss limit** *mss*
ip pp tcp mss limit *mss*
ip tunnel tcp mss limit *mss*
no ip *interface* **tcp mss limit** [*mss*]
no ip pp tcp mss limit [*mss*]
no ip tunnel tcp mss limit [*mss*]

[設定値]　◦ *mss*
- MSS の最大長 (536..1460)
- auto ..... 自動設定
- off..... 設定しない

[説明]　インタフェースを通過する TCP セッションの MSS を制限する。インタフェースを通過する TCP パケットを監視し、MSS オプションの値が設定値を越えている場合には、設定値に書き換える。キーワード auto を指定した場合には、インタフェースの MTU、もしくは PP インタフェースの場合で相手の MRU 値が分かる場合にはその MRU 値から計算した値に書き換える。

[ノート]　PPPoE 用の PP インタフェースに対しては、**pppoe tcp mss limit** コマンドでも TCP セッションの MSS を制限することができる。このコマンドと **pppoe tcp mss limit** コマンドの両方が有効な場合は、MSS はどちらかより小さな方の値に制限される。
RT250i には、**ip tunnel tcp mss limit** コマンドはない。

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.1.19　IPv4 の経路情報に変化があった時にログに記録するか否かの設定

[書式]　**ip route change log** *log*

[設定値]　◦ *log*
- on ..... IPv4 経路の変化をログに記録する
- off..... IPv4 経路の変化をログに記録しない

[説明]　IPv4 の経路情報に変化があった時にそれをログに記録するか否かを設定する
ログは INFO レベルで記録される。

[ノート]　Rev.7.01.34 以降、Rev.8.01.07 以降で使用可能。

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	RT250i	RT107e	SRT100

8.1.20　フィルタリングによるセキュリティの設定

[書式]

ip *interface* **secure filter** *direction* [*filter_list...*] [dynamic *filter_list...*]
ip pp secure filter *direction* [*filter_list...*] [dynamic *filter_list...*]
ip tunnel secure filter *direction* [*filter_list...*] [dynamic *filter_list...*]
ip *interface* **secure filter name** *set_name*
ip pp secure filter name *set_name*
ip tunnel secure filter name *set_name*
no ip *interface* **secure filter** *direction* [*filter_list*]
no ip pp secure filter *direction* [*filter_list*]
no ip tunnel secure filter *direction* [*filter_list*]
no ip *interface* **secure filter name** [*set_name*]
no ip pp secure filter name [*set_name*]
no ip tunnel secure filter name [*set_name*]

[設定値]

- *interface* ..... LAN インタフェース名、LOOPBACK インタフェース名、NULL インタフェース名、ブリッジインタフェース名
- *direction*
  - in ..... 受信したパケットのフィルタリング
  - out ..... 送信するパケットのフィルタリング
- *filter_list* ..... 空白で区切られたフィルタ番号の並び (128 個以内)
- *set_name* ..... フィルタセットの名前を表す文字列
- dynamic ..... キーワード後に動的フィルタの番号を記述する

[説明]

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

方向を指定する書式では、それぞれの方向に対して適用するフィルタ列をフィルタ番号で指定する。指定された番号のフィルタが順番に適用され、パケットにマッチするフィルタが見つかればそのフィルタにより通過 / 廃棄が決定する。それ以降のフィルタは調べられない。すべてのフィルタにマッチしないパケットは廃棄される。
フィルタセットの名前を指定する書式では、指定されたフィルタセットが適用される。フィルタを調べる順序などは方向を指定する書式の方法に準ずる。定義されていないフィルタセットの名前が指定された場合には、フィルタは設定されていないものとして動作する。

[ノート]

フィルタリストを走査して、一致すると通過、破棄が決定する。

```
# ip filter 1 pass 192.168.0.0/24 *
# ip filter 2 reject 192.168.0.1
# ip lan1 secure filter in 1 2
```

この設定では、始点 IP アドレスが 192.168.0.1 であるパケットは、最初のフィルタ 1 で通過が決定してしまうため、フィルタ 2 での検査は行われない。そのため、フィルタ 2 は何も意味を持たない。
フィルタリストを操作した結果、どのフィルタにも一致しないパケットは破棄される。

PP Anonymous で認証に RADIUS を利用する場合で、RADIUS サーバーから送られた Access-Response にアトリビュート 'Filter-Id' がついていた場合には、その値に指定されたフィルタセットを適用し、**ip pp secure filter** コマンドの設定は無視される。
ただしアトリビュート "Filter-Id" が存在しない場合には、**ip pp secure filter** コマンドの設定がフィルタとして利用される。
RT250i には **ip tunnel secure filter** コマンドはない。
SRT100 では dynamic キーワードは使用できない。動的フィルタは **ip policy filter** コマンドを使用する。
LOOPBACK インタフェースと NULL インタフェースでは動的フィルタは使用できない。
NULL インタフェースで *direction* に 'in' は指定できない。
LOOPBACK インタフェース、NULL インタフェースを指定できるのは Rev.8.03 以降のリビジョンである。
ブリッジインタフェースを指定できるのは Rev.10.00.38 以降のリビジョンである。

[初期値]

フィルタは設定されていない

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.1.21　フィルタに一致する IP パケットの DF ビットを 0 に書き換えるか否かの設定

[書式]　**ip fragment remove df-bit filter** *filter_num ...*
no ip fragment remove df-bit filter [*filter_num ...*]

[設定値]　◦ *filter_num*..... **ip filter** コマンドで登録されたフィルタ番号

[説明]　フォワーディングする IP パケットの内、フィルタに一致するものは DF ビットを 0 に書き換える。

[ノート]　DF ビットは経路 MTU 探索アルゴリズムで利用されるが、経路の途中に ICMP パケットをフィルタするファイアウォールなどがあるとアルゴリズムがうまく動作せず、特定の通信相手とだけは通信ができないなどの現象になることがある。この様な現象は、「経路 MTU 探索ブラックホール (Path MTU Discovery Blackhole)」と呼ばれている。この経路 MTU 探索ブラックホールがある場合には、このコマンドでそのような相手との通信に関して DF ビットを 0 に書き換えてしまえば、経路 MTU 探索は正しく動作しなくなるものの、通信できなくなるということはなくなる。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.1.22　IP パケットの TOS フィールドの書き換えの設定

[書式]　**ip tos supersede** *id tos* [precedence=*precedence*] *filter_num* [*filter_num_list*]
no ip tos supersede *id* [*tos*]

[設定値]　◦ *id* .....識別番号 (1..65535)

◦ *tos* .....書き換える TOS 値 (0..15)
以下のニーモニックが利用できる

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

◦ *precedence*
- *precedence* 値 (0..7)
- *precedence* を省略した場合、PRECEDENCE 値は変更しない

◦ *filter_num*.....静的フィルタの番号 (1..100)

◦ *filter_num_list* .....静的フィルタの番号 (1..100) の並び

[説明]　IP パケットを中継する場合に TOS フィールドを指定した値に書き換える。
識別番号順にリストをチェックし、*filter_num* リストのフィルタを順次適用していく。そして、最初にマッチした IP フィルタが pass、pass-log、pass-nolog、restrict、restrict-log、restrict-nolog のいずれかであれば TOS フィールドが書き換えられる。
reject、reject-log または reject-nolog である場合は書き換えずに処理を終わる。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.1.23　代理 ARP の設定

[書式]　**ip** *interface* **proxyarp** *proxyarp*
ip *interface* **proxyarp vrrp** *vrid*
no ip *interface* **proxyarp** [*proxyarp*]

[設定値]　◦ *interface*.....LAN インタフェース名

◦ *proxyarp*
- on .....代理 ARP 動作をする
- off.....代理 ARP 動作をしない

◦ *vrid*.....VRRP グループ ID (1..255)

[説明]　代理 ARP 動作をするか否か設定する。on を設定した時には、代理 ARP 動作を行う。この時利用する MAC アドレスは、LAN インタフェースの実 MAC アドレスとなる。

第 2 書式を設定した時には、指定された VRID での VRRP の状態がマスターである場合のみ代理 ARP 動作を行う。利用する MAC アドレスは指定された VRID の仮想 MAC アドレスとなる。

[ノート]　第 2 書式は Rev.7.01.26 以降で使用可能。

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.1.24　ARP エントリの寿命の設定

[書式]　**ip arp timer** *timer*
no ip arp timer [*timer*]

[設定値]　◦ *timer*..... ARP エントリの寿命秒数 (30..32767)

[説明]　ARP エントリの寿命を設定する。ARP 手順で得られた IP アドレスと MAC アドレスの組は ARP エントリとして記憶されるが、このコマンドで設定した時間だけ経過すると、再度 ARP 手順が実行される。その時点で ARP に応答が無い場合にはエントリは消される。

[初期値]　1200

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	RT250i	RT107e	SRT100

8.1.25　静的 ARP エントリの設定

[書式]　**ip** *interface* **arp static** *ip_address mac_address* [mtu=*mtu*]
no ip *interface* **arp static** *ip_address* [...]

[設定値]　◦ *interface*..... LAN インタフェース名
◦ *ip_address*..... IP アドレス
◦ *mac_address*..... MAC アドレス
◦ *mtu*
• interface..... インタフェースの MTU の値を利用する
• discovery..... MTU 探索機能を使用して値を設定する
• MTU 値 (64..1500; RTX3000 の LAN1 と LAN2 の場合は 64..9578)

[説明]　ARP エントリを静的に設定する。このコマンドで設定された ARP エントリは、**show arp** コマンドで TTL が 'permanent' と表示され、常に有効となる。また、**clear arp** コマンドを実行してもエントリは消えない。

mtu オプションに *discovery* を設定すると、ARP による MTU 探索機能が動作する。

mtu オプションを省略した時には、インタフェースの MTU を固定で利用する。

[ノート]　mtu オプションは、RTX3000 で指定可能。

mtu オプションに *discovery* を設定した場合には、探索を行う時に対象のホストと通信できる状況になっている必要があるため、その時点で対象のホストが接続されていないなど通信できない状況の場合には、MTU 探索に失敗し、デフォルトである 1500 バイトを MTU として利用するようになる。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	RT250i	RT107e	SRT100

8.1.26　ARP が解決されるまでの間に送信を保留しておくパケットの数を制御する

[書式]　**ip** *interface* **arp queue length** *len*
no ip *interface* **arp queue length** [*len*]

[設定値]　◦ *interface*..... LAN インタフェース名
◦ *len*..... キュー長 (0..10000)

[説明]　ARP が解決していないホストに対してパケットを送信しようとした時に、ARP が解決するか、タイムアウトにより ARP が解決できないことが確定するまで、インタフェース毎に送信を保留しておくことのできるパケットの最大数を設定する。

0 を設定するとパケットを保留しなくなるため、例えば ARP が解決していない相手に ping を実行すると必ず最初の 1 パケットは失敗するようになる。

[ノート]　このコマンドが新設される以前のバージョンでは、送信を保留する数の上限は設定されておらず、いくらでも保留することができた。
Rev.8.01.18、Rev.8.02.28 以降で使用可能。

[初期値]　200 (1000BASE-T インタフェース対応機種)
40 (ファストパス機能対応機種)
200 (ファストパス機能未対応機種)

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	RT250i	RT107e	SRT100

8.2　PP 側の設定

8.2.1　PP 側 IP アドレスの設定

[書式]

ip pp remote address *ip_address*
ip pp remote address dhcpc [*interface*]
no ip pp remote address [*ip_address*]

[設定値]

◦ *ip_address*
- IP アドレス……*xxx.xxx.xxx.xxx* (xxx は十進数)
- dhcp……自分自身の DHCP サーバー機能より IP アドレスを割り当てる

◦ dhcpc……DHCP クライアントを利用することを示すキーワード

◦ *interface*
- DHCP クライアントとして動作する LAN インタフェース名
- 省略時は lan1

[説明]

選択されている相手の PP 側の IP アドレスを設定する。
dhcp を設定した場合は、自分自身が DHCP サーバーとして動作している必要がある。自分で管理している DHCP スコープの中から、IP アドレスを割り当てる。
装着されている BRI/PRI インタフェースで利用できる ISDN Bch の数まで設定できる。
PP として anonymous が選択された場合のみ有効である。
dhcpc を設定した場合は、*interface* で指定した LAN インタフェースが DHCP クライアントとして IP アドレスを取得し、そのアドレスを PP 側に割り当てる。取得できなかった場合は、0.0.0.0 を割り当てる。

[初期値]

相手側 IP アドレスは設定されていない

[設定例]

ルーター A 側が "**no ip pp remote address**"、"**ppp ipcp ipaddress** on" と設定し、接続するルーター B 側が "**ip pp remote address** yyy.yyy.yyy.yyy" と設定している場合には、実際のルーター A の PP 側の IP アドレスは "yyy.yyy.yyy.yyy" になる。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.2.2　リモート IP アドレスプールの設定

[書式]

ip pp remote address pool *ip_address* [*ip_address…*]
ip pp remote address pool *ip_address-ip_address*
ip pp remote address pool dhcp
ip pp remote address pool dhcpc [*interface*]
no ip pp remote address pool

[設定値]

◦ *ip_address*…… anonymous のためにプールする IP アドレス

◦ *ip_address-ip_address*……IP アドレスの範囲

◦ dhcp…… 自分自身の DHCP サーバー機能を利用することを示すキーワード

◦ dhcpc …… DHCP クライアントを利用することを示すキーワード

◦ *interface*
- DHCP クライアントとして動作する LAN インタフェース名
- 省略時は lan1

[説明]

anonymous で相手に割り当てるための IP アドレスプールを設定する。PP として anonymous が選択された場合のみ有効である。

dhcp を設定した場合は、自分自身が DHCP サーバーとして動作している必要がある。自分で管理している DHCP スコープの中から、IP アドレスを割り当てる。
dhcpc を設定した場合は、*interface* で指定した LAN インタフェースが DHCP クライアントとして IP アドレス情報のみを取得し、そのアドレスを割り当てる。取得できなかった場合は、0.0.0.0 を割り当てる。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.2.3 PP 経由のキープアライブの時間間隔の設定

[書式]

pp keepalive interval *interval* [retry-interval=*retry-interval*] [count=*count*] [time=*time*]
no pp keepalive interval [*interval* [*count*]]

[設定値]

- *interval*..... キープアライブパケットを送出する時間間隔 [秒](1..65535)
- *retry-interval*..... キープアライブパケットの確認に一度失敗した後の送信間隔。単位は秒。キープアライブパケットが確認できれば、送信間隔はまた *interval* に戻る。
- *count*..... この回数連続して応答がなければ相手側のルーターをダウンしたと判定する (3..100)
- *time*..... キープアライブパケットの確認に失敗するようになってから回線断と判断するまでの時間。単位は秒。*count* パラメータとは同時には指定できない。

[説明]

PP インタフェースでのキープアライブパケットの送信間隔と、回線断と判定するまでの再送回数および時間を設定する。

送信したキープアライブパケットに対して返事が返って来ている間は *interval* で指定した間隔でキープアライブパケットを送信する。一度、返事が確認できなかった時には送信間隔が *retry-interval* パラメータの値に変更される。*count* パラメータに示された回数だけ連続して返事が確認できなかった時には回線断と判定する。

回線断判定までの時間を *time* パラメータで指定した場合には、少なくとも指定した時間の間、キープアライブパケットの返事が連続して確認できない時に回線断と判定する。

[ノート]

time パラメータを指定した場合には、その値はキープアライブの間隔と再送回数によって再計算されるため、設定値とは異なる値が **show config** で表示されることがある。

[初期値]

interval = 30
retry-interval = 1
count = 6

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.2.4 PP 経由のキープアライブを使用するか否かの設定

[書式]

pp keepalive use lcp-echo
pp keepalive use icmp-echo *dest_ip* [*option*=*value*...] [*dest_ip* [*option*=*value*...]...]
pp keepalive use lcp-echo icmp-echo *dest_ip* [*option*=*value*...] [*dest_ip* [*option*=*value*...]...]
pp keepalive use off
no pp keepalive use

[設定値]

- lcp-echo ..... LCP Echo Request/Reply を用いる
- icmp-echo..... ICMP Echo/Reply を用いる
- *dest_ip*..... キープアライブ確認先の IP アドレス
- *option* = *value* 列

option	*value*	説明
upwait	ミリ秒	アップ検知のための許容応答時間 (1..10000)
downwait	ミリ秒	ダウン検知のための許容応答時間 (1..10000)
disconnect	秒	無応答切断時噛 (1..21474836)
length	バイト	ICMP Echo パケットの長さ (64-1500)

[説明]

選択した相手先に対する接続のキープアライブ動作を設定する。
lcp-echo 指定で、LCP Echo Request/Reply を用い、icmp-echo も指定すれば ICMP Echo/Reply も同時に用いる。icmp-echo を使用する場合には、IP アドレスの設定が必要である。

[ノート]

このコマンドを設定していない場合でも、**pp always-on** コマンドで on と設定していれば、LCP Echo によるキープアライブが実行される。

icmp-echo で確認する IP アドレスに対する経路は、設定される PP インタフェースが送出先となるよう設定される必要がある。

downwait パラメータで応答時間を制限する場合でも、**pp keepalive interval** コマンドの設定値の方が小さい場合には、**pp keepalive interval** コマンドの設定値が優先される。*downwait*、*upwait* パラメータのうち一方しか設定していない場合には、他方も同じ値が設定されたものとして動作する。

disconnect パラメータは、PPPoE で使用する場合に PPPoE レベルでの再接続が必要な場合に使用する。*disconnect* パラメータが設定されている場合に、設定時間内に icmp-echo の応答がない場合、PPPoE レベルで一度切断操作を行うため、**pp always-on** コマンドとの併用により再接続を行うことができる。

他のパラメータがデフォルト値の場合、*disconnect* パラメータは 70 秒程度に設定しておくと、ダウン検出後の切断動作が確実に行われる。

length パラメータで指定するのは ICMP データ部分の長さであり、IP パケット全体の長さではない。*length* パラメータは、Rev.7.01.43、Rev.8.01.18、Rev.8.02.35 以降で指定可能である。

[初期値]　キープアライブは使用しない

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.2.5　PP 経由のキープアライブのログをとるか否かの設定

[書式]　**pp keepalive log** *log*
no pp keepalive log [*log*]

[設定値]　◦ *log*
- on ..... ログをとる
- off..... ログをとらない

[説明]　PP 経由のキープアライブをログにとるか否かを設定する。

[ノート]　この設定は、すべての PP で共通に用いられる。

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.2.6　専用線ダウン検出時の動作の設定

[書式]　**leased keepalive down** *action*
no leased keepalive down [*action*]

[設定値]　◦ *action*
- silent ..... 何もしない
- reset ..... ルーターを再起動する

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

[初期値]　silent

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

8.3　RIP の設定

8.3.1　RIP を使用するか否かの設定

[書式]　**rip use** *use*
no rip use [*use*]

[設定値]　◦ *use*
- on ..... RIP を使用する
- off..... RIP を使用しない

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

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.3.2 RIP に関して信用できるゲートウェイの設定

[書式] **ip** *interface* **rip trust gateway** [except] *gateway_list*
ip pp rip trust gateway [except] *gateway_list*
ip tunnel rip trust gateway [except] *gateway_list*
no ip *interface* **rip trust gateway** [[except] *gateway_list*]
no ip pp rip trust gateway [[except] *gateway_list*]
no ip tunnel rip trust gateway [[except] *gateway_list*]

[設定値] ◦ *interface*..... LAN インタフェース名
◦ *gateway_list*..... IP アドレスの並び (10 個以内)

[説明] RIP に関して信用できる、あるいは信用できないゲートウェイを設定する。
except キーワードを指定していない場合には、列挙したゲートウェイを信用できるゲートウェイとし、それらからの RIP だけを受信する。
except キーワードを指定した場合は、列挙したゲートウェイを信用できないゲートウェイとし、それらを除いた他のゲートウェイからの RIP だけを受信する。

[ノート] RT250i には **ip tunnel rip trust gateway** コマンドはない。

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

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.3.3 RIP による経路の優先度の設定

[書式] **rip preference** *preference*
no rip preference [*preference*]

[設定値] ◦ *preference*..... 1 以上の数値

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

[ノート] スタティック経路の優先度は 10000 で固定である。

[初期値] 1000

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.3.4 RIP パケットの送信に関する設定

[書式] **ip** *interface* **rip send** *send* [version *version* [*broadcast*]]
ip pp rip send *send* [version *version* [*broadcast*]]
ip tunnel rip send *send* [version *version* [*broadcast*]]
no ip *interface* **rip send** [*send...*]
no ip pp rip send [*send...*]
no ip tunnel rip send [*send...*]

[設定値] ◦ *interface*..... LAN インタフェース名
◦ *send*
• on..... RIP パケットを送信する
• off..... RIP パケットを送信しない
◦ *version*..... 送信する RIP のバージョン (1,2)
◦ *broadcast*..... **ip** *interface* **address** コマンドで指定したブロードキャスト IP アドレス

[説明] 指定したインタフェースに対し、RIP パケットを送信するか否かを設定する。
"version *version*" で送信する RIP のバージョンを指定できる。

[ノート] RT250i には **ip tunnel rip send** コマンドはない。

[初期値] off (トンネルインタフェースの場合)
on version 1 (その他のインタフェースの場合)

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.3.5　RIP パケットの受信に関する設定

[書式]
ip *interface* **rip receive** *receive* [version *version* [*version*]]
ip pp rip receive *receive* [version *version* [*version*]]
ip tunnel rip receive *receive* [version *version* [*version*]]
no ip *interface* **rip receive** [*receive...*]
no ip pp rip receive [*receive...*]
no ip tunnel rip receive [*receive...*]

[設定値]
◦ *interface*.....LAN インタフェース名
◦ *receive*
• on.....RIP パケットを受信する
• off.....RIP パケットを受信しない
◦ *version*.....受信する RIP のバージョン (1,2)

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

[ノート]
RT250i には **ip tunnel rip receive** コマンドはない。

[初期値]
off (トンネルインタフェースの場合)
on version 1 2 (その他のインタフェースの場合)

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.3.6　RIP のフィルタリングの設定

[書式]
ip *interface* **rip filter** *direction filter_list*
ip pp rip filter *direction filter_list*
ip tunnel rip filter *direction filter_list*
no ip *interface* **rip filter** *direction* [*filter_list*]
no ip pp rip filter *direction filter_list*
no ip tunnel rip filter *direction filter_list*

[設定値]
◦ *interface*.....LAN インタフェース名
◦ *direction*
• in.....受信した RIP のフィルタリング
• out.....送信する RIP のフィルタリング
◦ *filter_list*.....空白で区切られた静的フィルタ番号の並び (100 個以内)

[説明]
インタフェースで送受信する RIP のフィルタリングを設定する。
ip filter コマンドで設定されたフィルタの始点 IP アドレスが、送受信する RIP の経路情報にマッチする場合は、フィルタが pass であればそれを処理し、reject であればその経路情報だけを破棄する。

[ノート]
RT250i には **ip tunnel rip filter** コマンドはない。

[初期値]
フィルタは設定されていない

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.3.7　RIP で加算するホップ数の設定

[書式]
ip *interface* **rip hop** *direction hop*
ip pp rip hop *direction hop*
ip tunnel rip hop *direction hop*
no ip *interface* **rip hop** *direction hop*
no ip pp rip hop *direction hop*
no ip tunnel rip hop *direction hop*

[設定値]
◦ *interface*.....LAN インタフェース名
◦ *direction*
• in.....受信した RIP に加算する
• out.....送信する RIP に加算する
◦ *hop*.....加算する値 (0..15)

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

[ノート]
RT250i には **ip tunnel rip hop** コマンドはない。

[初期値]
0

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.3.8　RIP2 での認証の設定

[書式]　**ip** *interface* **rip auth type** *type*
ip pp rip auth type *type*
ip tunnel rip auth type *type*
no ip *interface* **rip auth type** [*type*]
no ip pp rip auth type [*type*]
no ip tunnel rip auth type [*type*]

[設定値]　◦ *interface* ..... LAN インタフェース名
◦ *type*
• text ..... テキスト型の認証を行う

[説明]　RIP2 を使用する場合のインタフェースでの認証の設定をする。text の場合はテキスト型の認証を行う。

[ノート]　RT250i には **ip tunnel rip auth type** コマンドはない。

[初期値]　認証を行わない。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.3.9　RIP2 での認証キーの設定

[書式]　**ip** *interface* **rip auth key** *hex_key*
ip pp rip auth key *hex_key*
ip tunnel rip auth key *hex_key*
ip *interface* **rip auth key text** *text_key*
ip pp rip auth key text *text_key*
ip tunnel rip auth key text *text_key*
no ip *interface* **rip auth key**
no ip pp rip auth key
no ip tunnel rip auth key
no ip *interface* **rip auth key text**
no ip pp rip auth key text
no ip tunnel rip auth key text

[設定値]　◦ *interface* ..... LAN インタフェース名
◦ *hex_key* ..... 十六進数の列で表現された認証キー
◦ *text_key* ..... 文字列で表現された認証キー

[説明]　RIP2 を使用する場合のインタフェースの認証キーを設定する。

[ノート]　RT250i には **ip tunnel rip auth key** コマンド、**ip tunnel rip auth key text** コマンドはない。

[設定例]
```
# ip lan1 rip auth key text testing123
# ip pp rip auth key text "hello world"
# ip lan2 rip auth key 01 02 ff 35 8e 49 a8 3a 5e 9d
```

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.3.10　回線切断時の経路保持の設定

[書式]　**ip pp rip hold routing** *rip_hold*
no ip pp rip hold routing [*rip_hold*]

[設定値]　◦ *rip_hold*
• on ..... 回線が切断されても RIP による経路を保持し続ける
• off ..... 回線が切断されたら RIP による経路を破棄する

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

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.3.11　回線接続時の PP 側の RIP の動作の設定

[書式]　**ip pp rip connect send** *rip_action*
no ip pp rip connect send [*rip_action*]

[設定値]　◦ *rip_action*
- interval..... **ip pp rip connect interval** コマンドで設定された時間間隔で RIP を送出する
- update..... 経路情報が変わった場合にのみ RIP を送出する
- none..... RIP を送出しない

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

[初期値]　update

[設定例]　# ip pp rip connect interval 60
ip pp rip connect send interval

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.3.12　回線接続時の PP 側の RIP 送出の時間間隔の設定

[書式]　**ip pp rip connect interval** *time*
no ip pp rip connect interval [*time*]

[設定値]　◦ *time*.....秒数 (30..21474836)

[説明]　選択されている相手について回線接続時に RIP を送出する時間間隔を設定する。
ip pp rip send と **ip pp rip receive** コマンドが on、**ip pp rip connect send** コマンドが interval の時に有効である。

[初期値]　30

[設定例]　# ip pp rip connect interval 60
ip pp rip connect send interval

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.3.13　回線切断時の PP 側の RIP の動作の設定

[書式]　**ip pp rip disconnect send** *rip_action*
no ip pp rip disconnect send [*rip_action*]

[設定値]　◦ *rip_action*
- none..... 回線切断時に RIP を送出しない
- interval..... **ip pp rip disconnect interval** コマンドで設定された時間間隔で RIP を送出する
- update..... 経路情報が変わった時にのみ RIP を送出する

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

[初期値]　none

[設定例]　# ip pp rip disconnect interval 1800
ip pp rip disconnect send interval

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.3.14　回線切断時の PP 側の RIP 送出の時間間隔の設定

[書式]　**ip pp rip disconnect interval** *time*
no ip pp rip disconnect interval [*time*]

[設定値]　◦ *time*.....秒数 (30..21474836)

[説明]　選択されている相手について回線切断時に RIP を送出する時間間隔を設定する。
ip pp rip send と **ip pp rip receive** コマンドが on、**ip pp rip disconnect send** コマンドで interval の時に有効である。

[初期値]　3600

[設定例]　# ip pp rip disconnect interval 1800
ip pp rip disconnect send interval

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.3.15　バックアップ時の RIP の送信元インタフェース切り替えの設定

[書式]　**ip pp rip backup interface** *switch*
no ip pp rip backup interface

[設定値]　◦ *switch*
- on..... 切り替える
- off..... 切り替えない

[説明]　バックアップ時に RIP の送信元インタフェースを切り替えるか否かを設定する。RIP の送信元インタフェースは、off のときには、バックアップ元のインタフェースであり、on のときには、バックアップ先のインタフェースとなる。

[ノート]　両者の違いは、送信元の IP アドレスの違いとなって現れる。off のときには、バックアップ元のインタフェースのアドレスが選ばれ、on のときには、バックアップ先のインタフェースのアドレスが選ばれる。なお、どちらの場合にも、バックアップ回線を通じて RIP が送信される。

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	SRT100

8.3.16　RIP で強制的に経路を広告する

[書式]　**ip** *interface* **rip force-to-advertise** *ip-address/netmask* [**metric** *metric*]
ip pp rip force-to-advertise *ip-address/netmask* [**metric** *metric*]
ip tunnel rip force-to-advertise *ip-address/netmask* [**metric** *metric*]
no ip *interface* **rip force-to-advertise** *ip-address/netmask* [**metric** *metric*]
no ip pp rip force-to-advertise *ip-address/netmask* [**metric** *metric*]
no ip tunnel rip force-to-advertise *ip-address/netmask* [**metric** *metric*]

[設定値]　◦ *interface*..... LAN インタフェース名
◦ *ip-address/netmask*..... 強制的に広告したい経路のネットワークアドレスとネットマスク長、または 'default'
◦ *metric*..... 広告する際のメトリック値 (1 ～ 15)

[説明]　設定した経路が経路テーブルに存在しない場合でも、指定されたインタフェースに対し、RIP で経路を強制的に広告する。経路として 'default' を指定した場合にはデフォルト経路が広告される。

[ノート]　以下のリビジョンで使用可能
Rev.8.03.75 以降、Rev.9.00.37 以降、Rev.10.00.38 以降、Rev.10.01 系

[初期値]　*metric*: 1

[設定例]　LAN1 側に、LAN2 の一部のホストだけを広告する。

```
ip lan1 address 192.168.0.1/24
ip lan2 address 192.168.1.1/24

rip use on
rip filter rule with-netmask
ip lan1 rip send on version 2
ip lan1 rip receive on version 2

ip filter 1 reject 192.168.1.0/24
ip filter 100 pass *
ip lan1 rip filter out 1 100

ip lan1 rip force-to-advertise 192.168.1.28/30
ip lan1 rip force-to-advertise 192.168.1.100/32
ip lan1 rip force-to-advertise 192.168.1.101/32
```

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

8.3.17　RIP2 でのフィルタの比較方法

[書式]　**rip filter rule** *rule*
no rip filter rule [*rule*]

[設定値]　◦ *rule*
- address-only .....ネットワークアドレスだけを比較対象とする
- with-netmask.....RIP2 の場合、ネットワークアドレスとネットマスクを比較対象とする

[説明]　RIP フィルターで、設定されたフィルターと RIP エントリの内容の比較方法を設定する。

rip filter rule コマンド	プロトコル	比 較 方 法
address-only	RIP1	ネットマスク型のフィルターは範囲指定と解釈され、RIP エントリーのアドレス部がその範囲に入っているかどうかを比較する。
	RIP2	
with-netmask	RIP1	
	RIP2	ネットマスク型のフィルターの、アドレスとネットマスクがそれぞれ、RIP エントリーのアドレス、ネットマスクと一致するかどうかを比較する。

[ノート]　以下のリビジョンで使用可能
Rev.8.03.75 以降、Rev.9.00.37 以降、Rev.10.00.38 以降、Rev.10.01 系

[初期値]　*address-only*

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

8.3.18　RIP のタイマーを調整する

[書式]　**rip timer** *update* [*invalid* [*holddown*]]
no rip timer [*update*]

[設定値]　◦ *update*.....定期的な広告の送信間隔 (10 ～ 60(秒))
◦ *invalid*.....広告を受け取れなくなってから経路を削除するまでの時間 (30 ～ 360(秒))
◦ *holddown*.....経路が削除されたときにメトリック 16 で経路を広告する時間 (20 ～ 240(秒))

[説明]　RIP のタイマー値を設定する。
update、*invalid*、*holddown* の各値の間には以下の不等式が成立している必要がある。
update × 3 ≦ *invalid* ≦ *update* × 6
update × 2 ≦ *holddown* ≦ *update* × 4

[ノート]　PP インタフェースに対し、**ip pp rip connect/disconnect interval** コマンドが設定されているときは、そのコマンドの設定値が rip timer コマンドに優先する。ただし、**ip pp rip connect/disconnect interval** コマンドは *update* タイマーと *invalid* タイマーの値に影響するが、*holddown* タイマーの値には影響しない。**ip pp rip connect/disconnect interval** コマンドの設定値を T とした場合、各タイマーは以下のようになる。
update .....T
invalid.....T × 6
holddown **.....rip timer** コマンドの設定値 (デフォルト 120 秒)
PP インタフェース以外は該当するコマンドがないため、常に **rip timer** コマンドの設定値が有効である。

以下のリビジョンで使用可能
Rev.8.03.75 以降、Rev.9.00.37 以降、Rev.10.00.38 以降、Rev.10.01 系

[初期値]　*update*: 30 秒
invalid: *update* × 6 (180 秒)
holddown: *update* × 4 (120 秒)

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

8.4　VRRP の設定

8.4.1　インタフェース毎の VRRP の設定

[書式]

ip *interface* **vrrp** *vrid ip_address* [priority=*priority*] [preempt=*preempt*] [auth=*auth*] [advertise-interval=*time1*] [down-interval=*time2*]
no ip *interface* **vrrp** *vrid* [*vrid...*]

[設定値]

- *interface*..... LAN インタフェース名
- *vrid*..... VRRP グループ ID (1..255)
- *ip_address*..... 仮想ルーターの IP アドレス
- *priority*..... 優先度 (1..254)
- *preempt*..... プリエンプトモード
  - on
  - off
- *auth*..... テキスト認証文字列 (8 文字以内)
- *time1*..... VRRP 広告の送信間隔 (秒)
- *time2*..... マスターがダウンしたと判定するまでの時間 (秒)

[説明]

指定した VRRP グループを利用することを設定する。
同じ VRRP グループに所属するルーターの間では、VRID および仮想ルーターの IP アドレスを一致させておかなくてはいけない。これらが食い違った場合の動作は予測できない。
auth パラメータを指定しない場合には、認証なしとして動作する。

time1 および *time2* パラメータで、マスターが VRRP 広告を送信する間隔と、バックアップがそれを監視してダウンと判定するまでの時間を設定する。トラフィックが多いネットワークではこれらの値を初期値より長めに設定すると動作が安定することがある。これらの値はすべての VRRP ルーターで一致している必要がある。

[ノート]

priority および *preempt* パラメータの設定は、仮想ルーターの IP アドレスとして自分自身の LAN インタフェースに付与されているアドレスを指定している場合には無視される。この場合、優先度は最高の 255 となり、常にプリエンプトモードで動作する。
time1 および *time2* パラメータは Rev.6.03.33 以降、Rev.8.01.07 以降で使用可能。

[初期値]

priority=100
preempt=on
auth= 認証なし
time1=1
time2=3

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.4.2　シャットダウントリガの設定

[書式]

ip *interface* **vrrp shutdown trigger** *vrid interface*
ip *interface* **vrrp shutdown trigger** *vrid* pp *peer_num* [dlci=*dlci*]
ip *interface* **vrrp shutdown trigger** *vrid* route *network* [*nexthop*]
no ip *interface* **vrrp shutdown trigger** *vrid interface*
no ip *interface* **vrrp shutdown trigger** *vrid* pp *peer_num* [...]
no ip *interface* **vrrp shutdown trigger** *vrid* route *network*

[設定値]

- *interface*..... LAN インタフェース名
- *vrid*..... VRRP グループ ID (1..255)
- *peer_num*..... 相手先情報番号
- *dlci*..... DLCI 番号
- *network*
  - ネットワークアドレス
  - IP アドレス / マスク長
  - default
- *nexthop*
  - インタフェース名
  - IP アドレス

[説明]　設定した VRRP グループでマスタールーターとして動作している場合に、指定した条件によってシャットダウンすることを設定する。

- LAN インタフェース形式..... 指定した LAN インタフェースのリンクが落ちるか、あるいは lan keepalive でダウンが検知されると、シャットダウンする。
- pp 形式..... 指定した相手先情報番号に該当する回線で通信できなくなった場合にシャットダウンする。通信できなくなるとは、ケーブルが抜けるなどレイヤ 1 が落ちた場合と、以下の場合である。
  - 回線が ISDN 回線である時は、呼が接続されていない場合
  - 回線が専用線である時には、LCP キープアライブによって通信相手が落ちたと判断した場合
  - 回線がフレームリレーであって *"dlci=dlci"* を指定している場合には、PVC 状態確認手順によって指定した DLCI 番号が通信できないと判断した場合
  - **pp keepalive use** 設定によりダウンが検出された場合
- route 形式..... 指定した経路が経路テーブルに存在しないか、 *nexthop* で指定したインタフェースもしくは IP アドレスで指定するゲートウェイに向いていない場合に、シャットダウンする。*nexthop* を省略した場合には、経路がどのような先を向いていても存在する限りはシャットダウンしない。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

8.5　バックアップの設定

8.5.1　プロバイダ接続がダウンした時に PP バックアップする接続先の指定

[書式]
pp backup none
pp backup pp *peer_num* [ipsec-fast-recovery=*action*]
pp backup *interface ip_address*
pp backup tunnel *tunnel_num*
no pp backup

[設定値]
- *none*.....バックアップ動作しない
- *peer_num*.....バックアップ先として PP を使用する場合の相手先情報番号
- *action*.....バックアップから復帰した直後に SA の再構築を実施するか否か
  - on.....再構築する
  - off.....再構築しない
- *interface*.....バックアップ先として使用する LAN インタフェース
- *ip_address*.....ゲートウェイの IP アドレス
- *tunnel_num*..... トンネルインタフェース番号

[説明]　PP インタフェースが切断されたときにバックアップするインタフェースを指定する。
バックアップ先のインタフェースが PP インタフェースの場合には、ipsec-fast-recovery オプションを設定できる。このオプションで on を設定したときには、バックアップから復帰した直後に IPsec の SA をすぐに再構築するため、IPsec の通信が可能になるまでの時間を短縮できる。

[ノート]　このコマンドは PP インタフェースごとに設定できる。
PP インタフェースの切断を検知するために **pp always-on** コマンドで on を設定する必要がある。専用線の場合には **pp always-on** コマンドの代わりに、**pp keepalive uselcp-echo** コマンドを使用する。
RT107e は Rev.8.03.42 以降で使用可能。

[初期値]　none
ipsec-fast-recovery=off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	~~SRT100~~

8.5.2　バックアップからの復帰待ち時間の設定

[書式]
pp backup recovery time *time*
no pp backup recovery time [*time*]

[設定値]
- *time*
  - 秒数 (1..21474836)
  - off.....すぐに復帰

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

[ノート]　この設定は、すべての PP で共通に用いられる。また専用線バックアップでも FR バックアップでもこの設定が共通に用いられる。
RT107e は Rev.8.03.42 以降で使用可能。

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	~~SRT100~~

8.5.3　LAN 経由でのプロバイダ接続がダウンした時にバックアップする接続先の指定

[書式]
lan backup *interface* none
lan backup *interface* **pp** *peer_num*
lan backup *interface backup_interface ip_address*
lan backup *interface* **tunnel** *tunnel_num*
no lan backup *interface*

[設定値]
- none ..... バックアップ動作しない
- *interface* ..... バックアップ対象の LAN インタフェース名
- *peer_num* ..... バックアップとして pp を使用する場合の相手先情報番号
- *backup_interface* ..... バックアップとして使用する LAN インタフェース
- *ip_address* ..... ゲートウェイの IP アドレス
- *tunnel_num* ..... トンネルインタフェース番号

[説明]
指定する LAN インタフェースに対して、LAN 経由でのプロバイダ接続がダウンした場合にバックアップするインタフェース情報を設定する。

[ノート]
バックアップ動作のためには、LAN 経由での接続のダウンを検知するために **lan keepalive use** コマンドでの設定が併せて必要である。
RT250i には **lan backup** *interface* **tunnel** コマンドはない。
RT107e は Rev.8.03.42 以降で使用可能。

[初期値]
none

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	~~SRT100~~

8.5.4　バックアップからの復帰待ち時間の設定

[書式]
lan backup recovery time *interface time*
no lan backup recovery time *interface* [*time*]

[設定値]
- *interface* ..... バックアップ対象の LAN インタフェース名
- *time*
  - 秒数 (1.. 21474836)
  - off

[説明]
指定する LAN インタフェースに対して、バックアップから復帰する場合に、すぐに復帰させるか、設定された時間だけ待ってから復帰するかを設定する。

[ノート]
RT107e は Rev.8.03.42 以降で使用可能。

[初期値]
off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	~~SRT100~~

8.5.5　LAN 経由のキープアライブを使用するか否かの設定

[書式]
lan keepalive use *interface* icmp-echo *dest_ip* [*option=value*...] [*dest_ip* [*option=value*...]...]
lan keepalive use *interface* arp *dest_ip* [*dest_ip*...]
lan keepalive use *interface* icmp-echo *dest_ip* [*option=value*...] [*dest_ip* [*option=value*...]...] arp *dest_ip* [*dest_ip*...]
lan keepalive use interface off
no lan keepalive use *interface* [...]

[設定値]
- *interface* ..... バックアップ対象の LAN インタフェース名
- *dest_ip* ..... キープアライブ確認先の IP アドレス
- *option = value* 列

option	*value*	説明
upwait	ミリ秒	アップ検知のための許容応答時間 (1..10000)
downwait	ミリ秒	ダウン検知のための許容応答時間 (1..10000)
length	バイト	ICMP Echo パケットの長さ (64-1500)

[説明]
指定する LAN インタフェースに対して、キープアライブ動作を行うか否かを設定する。icmp-echo を指定すれば ICMP Echo/Reply を用い、arp を指定すれば ARP Request/Reply を用いる。併記することで併用も可能である。

[ノート]　icmp-echo で確認する IP アドレスに対する経路は、バックアップをする LAN インタフェースに向くことが必要である。
downwait パラメータで応答時間を制限する場合でも、**lan keepalive interval** コマンドの設定値の方が小さい場合には、**lan keepalive interval** コマンドの設定値が優先される。*downwait*、*upwait* パラメータのうち一方しか設定していない場合には、他方も同じ値が設定されたものとして動作する。
length パラメータで指定するのは ICMP データ部分の長さであり、IP パケット全体の長さではない。*length* パラメータは、Rev.7.01.43、Rev.8.01.18、Rev.8.02.35 以降で指定可能である。
RT107e は Rev.8.03.42 以降で使用可能。

[初期値]　キープアライブは使用しない

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	~~SRT100~~

8.5.6　LAN 経由のキープアライブの時間間隔の設定

[書式]　**lan keepalive interval** *interface interval* [*count*]
no lan keepalive interval *interface*

[設定値]
- *interface*.....バックアップ対象の LAN インタフェース名
- *interval* .....キープアライブパケットを送出する時間間隔 (1.. 65535)
- *count*..... ダウン検出を判定する回数 (3 ..100)

[説明]　指定する LAN インタフェースに対して、キープアライブパケットの送出間隔とダウン検出を判定する回数を設定する。*count* に設定した回数だけ連続して応答パケットを検出できない場合に、ダウンと判定する。

一度応答が返ってこないのを検出したら、その後のキープアライブパケットの送出間隔は 1 秒に短縮される。そのため、デフォルトの設定値の場合でもダウン検出に要する時間は 35 秒程度である。

[ノート]　RT107e は Rev.8.03.42 以降で使用可能。

[初期値]　*interval* = 30
count = 6

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	~~SRT100~~

8.5.7　LAN 経由のキープアライブのログをとるか否かの設定

[書式]　**lan keepalive log** *interface log*
no lan keepalive log *interface*

[設定値]
- *interface*.....バックアップ対象の LAN インタフェース名
- *log*
  - on ..... ログをとる
  - off..... ログをとらない

[説明]　キープアライブパケットのログをとるか否かを設定する。

[ノート]　RT107e は Rev.8.03.42 以降で使用可能。

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	~~SRT100~~

8.5.8　ネットワーク監視機能の設定

[書式]　**ip keepalive** *num kind interval count gateway* [*gateway* ...] [option=value ...]
no ip keepalive *num*

[設定値]
- *num* ..... このコマンドの識別番号 (1..100 ; RTX3000 は 1...1000 ; RTX2000 は 1..500)
- *kind* ..... 監視方式
  - icmp-echo ..... ICMP Echo を使用する
- *interval* ..... キープアライブの送信間隔秒数 (1..65535)
- *count* ..... 到達性がないと判断するまでに送信する回数 (3..100)
- *gateway* ..... 複数指定可 (10 個以内)
  - IP アドレス ..... xxx.xxx.xxx.xxx(xxx は十進数)
  - dhcp *interface* ..... RT107e、SRT100、RTX1200 で指定可
    - *interface* .....DHCP にて与えられるデフォルトゲートウェイを使う場合の、DHCP クライアントとして動作する LAN インタフェース名
- *option = value* 列

option	*value*	説明
log	on	SYSLOG を出力する
	off	SYSLOG を出力しない
upwait	秒数	到達性があると判断するまでの待機時間 (1..1000000)
downwait	秒数	到達性がないと判断するまでの待機秒数 (1..1000000)
length	バイト	ICMP Echo パケットの長さ (64-1500)
ipsec-refresh	セキュリティ・ゲートウェイの識別子	DOWN → UP または UP → DOWN に状態が変化した場合に、指定のセキュリティ・ゲートウェイに属する SA を強制的に更新 (複数指定する場合はカンマで区切る)
ipsec-refresh-up	セキュリティ・ゲートウェイの識別子	DOWN → UP に状態が変化した場合のみ、指定のセキュリティ・ゲートウェイに属する SA を強制的に更新 (複数指定する場合はカンマで区切る)
ipsec-refresh-down	セキュリティ・ゲートウェイの識別子	UP → DOWN に状態が変化した場合のみ、指定のセキュリティ・ゲートウェイに属する SA を強制的に更新 (複数指定する場合はカンマで区切る)
gateway-selection-rule	head	ICMP Echo パケットを送信する際、該当する経路に複数のゲートウェイが指定されていても、必ず最初に指定されたゲートウェイへ送出する
	normal	ICMP Echo パケットを送信する際、該当する経路に複数のゲートウェイが指定されていたら、通常の規則に従い送出ゲートウェイを選択する

[説明]　指定したゲートウェイに対して ICMP Echo を送信し、その返事を受信できるかどうかを判定する。

[ノート]　Rev.7.01 以上で実行可能である。
length パラメータで指定するのは ICMP データ部分の長さであり、IP パケット全体の長さではない。
length パラメータは、Rev.7.01.43、Rev.8.01.18、Rev.8.02.35 以降で指定可能である。
ipsec-refresh、ipsec-refresh-up、ipsec-refresh-down パラメータは、ネットワークバックアップ機能の主系／従系回線の切り替え時において、IPsec 通信の復旧時間を短縮させる際に有効である。
ipsec-refresh、ipsec-refresh-up、ipsec-refresh-down パラメータは、RT107e を除く Rev.8.03.68 以降で指定可能である。
RTX3000 は、Rev.9.00.31 以降で指定可能。
SRT100 は、Rev.10.00.31 以降で指定可能。
gateway-selection-rule パラメータは、RT107e を除く Rev.8.03.68 以降で指定可能である。
RTX3000 は、Rev.9.00.24 以降で指定可能。
SRT100 は、Rev.10.00.22 以降で指定可能。

[初期値]　*log* = off
upwait = 5
downwait = 5
length = 64
ipsec-refresh 設定なし
ipsec-refresh-up 設定なし
ipsec-refresh-down 設定なし
gateway-selection-rule = head

[設定例]　ネットワークバックアップ機能で従系回線 pp11 から主系回線 pp10 へ復旧する際に、IPsec 接続で使用しているセキュリティ・ゲートウェイの識別子 3 に属する SA を強制的に更新させる。

```
# ip route 172.16.0.0/24 gateway pp 10 keepalive 1 gateway pp 11 weight 0
# ip keepalive 1 icmp-echo 5 5 172.16.0.1 ipsec-refresh-up=3
```

ネットワークバックアップ機能を利用して、IP キープアライブ 1 がダウンしたのをトリガにして経路 172.16.224.0/24 を活性化させる。

```
# ip route 172.16.112.0/24 gateway null keepalive 1 gateway 172.16.0.1 weight 0
# ip route 172.16.224.0/24 gateway 172.16.112.1 keepalive 2
# ip keepalive 1 icmp-echo 5 5 192.168.100.101
# ip keepalive 2 icmp-echo 5 5 172.16.112.1 gateway-selection-rule=normal
```

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	RT250i	RT107e	SRT100

8.6　IGMP の設定

8.6.1　インタフェースごとの IGMP の設定

[書式]

ip *interface* **igmp** *type* [*option ...*]
ip pp igmp *type* [*option ...*]
ip tunnel igmp *type* [*option ...*]
no ip *interface* **igmp** *type* [*option ...*]
no ip pp igmp *type* [*option ...*]
no ip tunnel igmp *type* [*option ...*]

[設定値]

- *interface*.....LAN インタフェース名
- *type*.....IGMP の動作方式
  - off.....IGMP は動作しない
  - router .....IGMP ルーターとして動作する
  - host .....IGMP ホストとして動作する
- *option*
  - version=*version* ...IGMP のバージョン
    - 2 .....IGMPv2
    - 3 .....IGMPv3
    - 2,3.....IGMPv2 と IGMPv3 の両方に対応する (IGMPv2 互換モード)
  - syslog=*switch*.....詳細な情報を syslog に出力するか否か
    - on.....表示する
    - off .....表示しない
  - robust-variable=*value*.....IGMP で規定される Robust Variable の値を設定する *(1..10)*
  - delay-timer=SW....IGMP の report メッセージの転送タイミング
    - on.....ランダムな遅延後に転送する
    - off .....即座に転送する

[説明]

インタフェースの IGMP の動作を設定する。

[ノート]

Rev.8.03 系以降のすべてのリビジョンで使用可能。

[初期値]

type: off
version=2,3
syslog=off
robust-variable=*2*
delay-timer=on

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

8.6.2　静的な IGMP の設定

[書式]

ip *interface* **igmp static** *group* [*filter_mode source ...*]
ip pp igmp static *group* [*filter_mode source ...*]
ip tunnel igmp static *group* [*filter_mode source ...*]
no ip *interface* **igmp static** *group* [*filter_mode source ...*]
no ip pp igmp static *group* [*filter_mode source ...*]
no ip tunnel igmp static *group* [*filter_mode source ...*]

[設定値]

- *interface*.....LAN インタフェース名
- *group*..... グループのマルチキャストアドレス
- *filter_mode*..... フィルタモード
  - include.....IGMP の "INCLUDE" モード
  - exclude.....IGMP の "EXCLUDE" モード
- *source*..... マルチキャストパケットの送信元のアドレス

[説明]　指定したグループについて、常にリスナーが存在するものとみなす。このコマンドは、IGMP をサポートしていないリスナーがいる場合に設定する。*filter_mode* と *source* は、マルチキャストパケットの送信元を限定するものである。*filter_mode* として include を指定したときには、*source* として受信したい送信元を列挙する。*filter_mode* として exclude を指定したときには、*source* として受信したくない送信元を列挙する。

[ノート]　Rev.8.03 系以降のすべてのリビジョンで使用可能。

[初期値]　設定なし

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

8.7　PIM-SM の設定

8.7.1　インタフェースごとの PIM-SM の設定

[書式]　**ip** *interface* **pim sparse** *switch* [*option ...*]
ip pp pim sparse *switch* [*option ...*]
ip tunnel pim sparse *switch* [*option ...*]
no ip *interface* **pim sparse** [*switch* [*option ...*]]
no ip pp pim sparse [*switch* [*option ...*]]
no ip tunnel pim sparse [*switch* [*option ...*]]

[設定値]
- *interface* ..... LAN インタフェース名
- *switch* ..... PIM-SM が動作するか否か
  - off ..... 動作しない
  - on ..... 動作する
- *option*
  - dr-priority=*priority* ..... DR priority
    - off ..... DR priority を送信しない
    - 1..255
  - hold-time=*value* ..... Hold Time の値 (20..600)
  - register-checksum ..... register のチェックサムをどの範囲で計算するか
    - all ..... カプセル化するマルチキャストパケットを含むすべて
    - header ..... PIM のヘッダの 8 バイトのみ

[説明]　インタフェースの PIM-SM の動作を設定する。

[ノート]　Rev.8.03 系以降のすべてのリビジョンで使用可能。

[初期値]　*switch*: off
option: dr-priority=1, register-checksum=header, holdtime=60

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

8.7.2　静的な RP のグループの設定

[書式]　**ip pim sparse rendezvous-point static** *group rendezvous_point* [priority=*priority*]
no ip pim sparse rendezvous-point static *group rendezvous_point*

[設定値]
- *group* ..... IP アドレス / マスク長 (マスク長は省略可)
- *rendezvous_point* ..... RP の IP アドレス
- *priority* ..... 優先度 (1-200)

[説明]　RP のグループの対応を静的に定義する。

[ノート]　Rev.8.03 系以降のすべてのリビジョンで使用可能。

[初期値]　設定なし

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

8.7.3　PIM-SM に関する詳細なログ出力の設定

[書式]　**ip pim sparse log** *[option ...]*
no ip pim sparse log *[option ...]*

[設定値]　◦ *option*.....出力する詳細なログの種類を指定する
- message-info .....PIM のメッセージの送受信に関するログ
- timer-info.....内部で動作する各種タイマーに関するログ
- state-info.....各種状態の変化についてのログ
- data-info.....DATA パケットの送受信に関するログ

[説明]　PIM-SM に関しての詳細なログの出力を設定する。*option* は複数選択が可能で、この場合スペースで区切って羅列する。このコマンドを設定することによって出力されるログは、細かなデバッグを目的とした詳細なものである。なお、このコマンドの設定が無い場合でも、基本情報の出力は行われ、以下のルールに従っている。

syslog info on が設定されている (default 設定) 場合、PIM-SM が動作していることを確認できる最低レベルのログを出力する。
syslog debug on が設定されている場合、動作詳細のログを出力する。

[ノート]　Rev.8.03 系以降のすべてのリビジョンで使用可能。

[初期値]　設定なし

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

8.7.4　register の checksum 計算方法の設定

[書式]　**ip pim sparse register-checksum** *size*
no ip pim sparse register-checksum *[size]*

[設定値]　◦ *size* .....register パケットの checksum 計算範囲
- header .....PIM ヘッダの先頭 8 バイト
- all .....register パケットにカプセル化する IP パケットを含むすべて

[説明]　register パケットの checksum 計算範囲を指定する。RP として接続するルーターによって、register パケットの checksum 計算範囲が異なる場合がある。RP の設定に合わせて指定する。

[ノート]　Rev.8.03 系以降のすべてのリビジョンで使用可能。

[初期値]　header

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

8.7.5　PIM JOIN/PRUNE メッセージの宛先の設定

[書式]　**ip pim sparse join-prune send** *cast*
no ip pim sparse join-prune send *[cast]*

[設定値]　◦ *cast*
- unicast .....近隣ルーターのユニキャストアドレス宛
- multicast.....224.0.0.13 のマルチキャストアドレス宛

[説明]　PIM の JOIN/PRUNE メッセージを送信する際のあて先アドレスを設定する。

[初期値]　unicast

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

8.7.6　PIM の Join(*,G) メッセージ送信時に Periodic Prune メッセージを含ませるかどうかの設定

[書式]　**ip pim sparse periodic-prune send** *sw*
no ip pim sparse periodic-prune send *[sw]*

[設定値]　◦ *sw*
- on .....送信する
- off.....送信しない

[説明]　PIM の Join(*,G) メッセージを送信する際に、Periodic Prune(S,G,rpt) メッセージを含ませるかどうかを設定する。

[初期値]　on

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

8.7.7　implicit 経路の優先度の設定

[書式]　**ip implicit-route preference** *preference*
no ip implicit-route preference [*preference*]

[設定値]　◦ *preference*..... implicit 経路の優先度 (1..2147483647)

[説明]　implicit 経路の優先度を設定する。
優先度は 1 以上の整数で示され、数字が大きいほど優先度が高い。
implicit 経路が動的経路制御プロトコルで得られた経路または **ip route** コマンドで設定された静的な経路と食い違う場合には、優先度が高い方が採用される。静的な経路と優先度が同じ場合には、静的な経路が優先される。
動的経路制御プロトコルで得られた経路と優先度が同じ場合には、時間的に先に採用された経路が有効となる。
なお、**ip implicit-route preference** コマンドで implicit 経路の優先度を変更しても、その時点で既にルーティングテーブルに登録されている implicit 経路の優先度は変更されない。

[ノート]　implicit 経路とは、IP アドレスを設定したインタフェースが有効な状態になったときに暗黙のうちに登録されるそのインタフェースを経由する経路のことである。例えば、IP アドレスを設定した LAN インタフェースがリンクアップ状態のときには、設定した IP アドレスとネットマスクの組み合わせから決定されるネットワークアドレスが、その LAN インタフェースを経由する implicit 経路として登録されている。

[初期値]　10000

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

8.7.8　フローテーブルの各エントリの寿命を設定する

[書式]　**ip flow timer** *protocol time*
no ip flow timer *protocol* [*time*]

[設定値]　◦ *protocol*..... 寿命を指定するプロトコル
- tcp..... TCP パケット
- udp ..... UDP パケット
- icmp..... ICMP パケット
- esp ..... ESP パケット (RTX1500 で有効)
- slow ..... FIN/RST ビットのセットされた TCP パケット

◦ *time*..... 秒数 (1-21474836)

[説明]　フローテーブルの各エントリの寿命をプロトコル毎に設定する。
FIN/RST の通過したエントリには 'slow' が適用される。
NAT や動的フィルタを使用している場合には、それらのエントリの寿命が適用される。

[ノート]　以下のリビジョンで使用可能
Rev.7.01.53 以降、Rev.8.03.75 以降、Rev.10.00.38 以降、Rev.10.01 系

[初期値]　tcp = 900
udp = 30
icmp = 30
esp = 900 (RTX1500 のみ)
slow = 30

[適用モデル]

~~RTX3000~~	RTX2000	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

8.8　受信パケット統計情報の設定

8.8.1　受信パケットの統計情報を記録するか否かの設定

[書式]

ip *interface* **traffic list** *sw*
ip pp traffic list *sw*
ip tunnel traffic list *sw*
no ip *interface* **traffic list** [*sw*]
no ip pp traffic list [*sw*]
no ip tunnel traffic list [*sw*]

[設定値]

◦ *interface*.....LAN インタフェース名

◦ *switch*

- on ..... 指定したインタフェースで受信したパケットの統計情報を記録する
- off..... 指定したインタフェースで受信したパケットの統計情報を記録しない

[説明]

指定したインタフェースで受信したパケットの統計情報を記録するか否かを設定する。
送信元 IP アドレスと送信先 IP アドレスの組み合わせが同じパケットについて、それぞれのパケット数とオクテット数を統計情報として記録する。
最大で 3 つのインタフェースについての統計情報を同時に記録することができる。

[ノート]

ファストパスで処理されたパケットは統計情報には記録されない。
off に設定すると統計情報がクリアされ、記録が停止する。
on に設定したときにもそれまでの統計情報はいったんクリアされ、新たに記録が開始する。
NAT 設定があるインタフェースで動作させる場合に表示される IP アドレスは、NAT 変換可能な状態であれば NAT 変換後の IP アドレスが表示され、NAT 変換ができない状態であれば NAT 変換前の IP アドレスが表示される。
受信フィルタで破棄される通信については記録されない。
Rev.9.00.24 以降で使用可能。

[初期値]

off

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

8.8.2　受信したパケットの統計情報のクリア

[書式]

clear ip traffic list [*interface*]
clear ip traffic list pp [*peer_num*]
clear ip traffic list tunnel [*tunnel_num*]

[設定値]

◦ *interface*.....LAN インタフェース名

◦ *peer_num*.....相手先情報番号、省略時は選択されている相手先情報番号

◦ *tunnel_num*..... トンネル番号、省略時は選択されているトンネル番号

[説明]

受信したパケットの統計情報をクリアする。
interface を省略したときは、全インタフェースの統計情報をクリアする。

[ノート]

Rev.9.00.24 以降で使用可能。

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

8.8.3　受信したパケットの統計情報の表示

[書式]　**show ip traffic list** [*interface*]
show ip traffic list pp [*peer_num*]
show ip traffic list tunnel [*tunnel_num*]

[設定値]　◦ *interface*..... LAN インタフェース名
◦ *peer_num*..... 相手先情報番号、省略時は選択されている相手先情報番号
◦ *tunnel_num*..... トンネル番号、省略時は選択されているトンネル番号

[説明]　受信したパケットの統計情報を表示する。
interface を省略したときは、全インタフェースの統計情報を表示する。

[ノート]　Rev.9.00.24 以降で使用可能。

[表示例]　# show ip traffic list lan1

Source IP	Destination IP	Packets	Octets
192.168.200.2	133.176.200.1	1411449	1326237183
133.176.200.3	133.176.200.226	12080	2115561
192.168.200.1	192.168.100.1	802	97211
192.168.200.2	133.176.200.3	17	17348

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

8.8.4　統計情報を記録する受信パケットの分類数の設定

[書式]　**ip** *interface* **traffic list threshold** *value*
ip pp traffic list threshold *value*
ip tunnel traffic list threshold *value*
no ip *interface* **traffic list threshold** [*value*]
no ip pp traffic list threshold [*value*]
no ip tunnel traffic list threshold [*value*]

[設定値]　◦ *interface*..... LAN インタフェース名
◦ *value*..... 統計情報に記録するパケットの最大分類数 (64..5000)

[説明]　指定したインタフェースにおいて、統計情報として記録する受信パケットの分類数を指定する。

[ノート]　送信元 IP アドレスと送信先 IP アドレスの組み合わせによってパケットを分類する。
記録されている受信パケット情報の分類数が最大値に達した場合、それ以降で新規に分類された受信パケット情報は記録されない。
このコマンドで設定を行なうとそれまでの統計情報はクリアされる。
Rev.9.00.24 以降で使用可能。

[初期値]　64

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

8.9　パケット転送フィルターの設定

8.9.1　パケット転送フィルターの定義

[書式]
ip forward filter *id order* **gateway** *gateway* **filter** *filter_id ...* [**keepalive** *keepalive_id*]
no ip forward filter *id order* [**gateway** *gateway* [*filter filter_id ...*] [**keepalive** *keepalive_id*]]

[設定値]
- *id* .....パケット転送フィルターの識別子 (1 .. 255)
- *order*.....評価の順番 (1 .. 255)
- *gateway*.....転送先のゲートウェイ
  - IP アドレス
  - pp 番号.....PP インタフェース
  - tunnel 番号.....TUNNEL インタフェース
- *filter_id* .....ip filter コマンドの識別子
- *keepalive_id*.....ip keepalive コマンドの識別子

[説明]
パケット転送フィルターを定義する。
id パラメータは、複数のパケット転送フィルターをグループ化するための識別子である。
同じインタフェースに対して複数のパケット転送フィルターを設定するときには、それらのすべてに対して、同じ番号を指定しなければならない。
order パラメータは、評価の順番を示すもので、若い番号を持つものほど優先的に採用される。
filter_id パラメータとしては、**ip filter** コマンドの識別子を最大 16 個まで指定できる。
複数の識別子を指定したときには、前にあるものが優先的に評価される。
前から順に対応する **ip filter** コマンドを調べ、パケットの内容と合致すれば、その **ip filter** コマンドの設定を採用する。
ip filter コマンドの動作が reject であれば、パケットを転送せずに破棄し、そうでなければ、*gateway* パラメータで指定したゲートウェイにパケットを転送する。
keepalive_id には、**ip keepalive** コマンドの識別子を指定する。
ここで指定した IP キープアライブの結果が down であれば、このゲートウェイを使用しない。
つまり、該当する **ip filter** コマンドがあったとしても、該当しなかったものとして扱う。
なお、実際に動作させるためには、**ip** *interface* **forward filter** コマンドも設定する必要がある。

[ノート]
RTX3000 は Rev.9.00.24 以降で使用可能。
RTX1500、RTX1100、RT107e は Rev.8.03.68 以降で使用可能。

[初期値]
設定されない

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	~~SRT100~~

8.9.2　インタフェースへのパケット転送フィルターの適用

[書式]
ip *interface* **forward filter** *id*
ip pp forward filter *id*
ip tunnel forward filter *id*
ip local forward filter *id*
no ip *interface* **forward filter** *[id]*
no ip pp forward filter *[id]*
no ip tunnel forward filter *[id]*
no ip local forward filter *[id]*

[設定値]
- *interface*..... LAN インタフェース名
- *id* ..... **ip forward filter** コマンドで指定したパケット転送フィルターの識別子 (1..255)

[説明]
インタフェースにパケット転送フィルターを適用する。
指定したインタフェースで受信したパケットを、指定したパケット転送フィルターの設定と比較し、転送先のゲートウェイを決定する。
ip local forward filter コマンドは自分自身が送信するパケットを対象にするときに指定する。

[ノート]
RTX3000 は Rev.9.00.24 以降で使用可能。
RTX1500、RTX1100、RT107e は Rev.8.03.68 以降で使用可能。

[初期値]
設定されない

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	~~SRT100~~

9. IPX の設定

9.1 インタフェース共通の設定

9.1.1 IPX パケットを扱うか否かの設定

[書式] **ipx routing** *routing*
no ipx routing [*routing*]

[設定値] ◦ *routing*
- on..... IPX パケットを処理対象として扱う
- off..... IPX パケットを処理対象として扱わない

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

[初期値] off

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

9.1.2 静的な SAP テーブルの設定

[書式] **ipx sap** *service_type server_name network node_num socket hop*
no ipx sap *service_type server_name* [*network node_num socket hop*]

[設定値] ◦ *service_type*..... サービスタイプ
- 十進数 (0..65535)
- 0x に続く 4 桁以内の十六進数
- file ..... 0x0004 のニーモニック
- printer ..... 0x0007 のニーモニック

◦ *server_name*..... サーバー名
- 'A' ～ 'Z','0' ～ '9','_','-','@' で構成された文字列 (47 文字以内)

◦ *network*..... サーバーの IPX ネットワーク番号 (0:0:0:1 .. FF:FF:FF:FE)

◦ *node_num*..... サーバーの IPX ノード番号 (0:0:0:0:0:1 .. FF:FF:FF:FF:FF:FE)

◦ *socket*..... ソケット番号
- 十進数 (0..65535)
- 0x に続く 4 桁以内の十六進数
- プロトコルを表すニーモニック

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

◦ *hop*..... ホップカウント (1..14)

[説明] SAP テーブルを設定する。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

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

[書式] **ipx sap response** *response*
no ipx sap response [*response*]

[設定値] ◦ *response*
- on..... 応答する
- off..... 応答しない

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

[初期値] on

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

9.1.4　IPX パケットのフィルタの設定

[書式]

ipx filter *filter_num pass_reject src_net* [*src_node* [*dst_net* [*dst_node* [*type* [*src_socket* [*dst_socket*]]]]]]
no ipx filter *filter_num* [*pass_reject*]

[設定値]

◦ *filter_num*.....静的フィルタの番号 (1..100)

◦ *pass_reject*

- pass-log .....一致すれば通す (ログに記録する)
- pass-nolog .....一致すれば通す (ログに記録しない)
- reject-log .....一致すれば破棄する (ログに記録する)
- reject-nolog .....一致すれば破棄する (ログに記録しない)
- restrict-log .....回線が接続されていれば通し、切断されていれば破棄する (ログに記録する)
- restrict-nolog .....回線が接続されていれば通し、切断されていれば破棄する (ログに記録しない)

◦ *src_net*.....始点 IPX ネットワーク番号

- 0:0:0:1 .....FF:FF:FF:FE (2 桁以内の十六進数以外に '*' も指定可)
- * (すべての IPX ネットワーク番号)

◦ *src_node*.....始点 IPX ノード番号

- 0:0:0:0:0:1 .....FF:FF:FF:FF:FF:FE (2 桁以内の十六進数以外に '*' も指定可)
- * (すべての IPX ノード番号)
- 省略時は一個の * と同じ

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

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

◦ *type*.....IPX パケットタイプ

- 十進数 (0..255)
- 十六進数 (0x0..0xFF)
- ニーモニック文字列

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

- 間に - をはさんだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。
- 上項目のカンマで区切った並び (5 個以内)
- * (すべての IPX パケットタイプ)
- 省略時は一個の * と同じ

◦ *src_socket*.....始点ソケット番号

- 十進数 (0..65535)
- 0x を先頭に持つ 4 桁以内の十六進数
- プロトコルを表すニーモニック

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

- 間に - をはさんだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。
- 上項目のカンマで区切った並び (5 個以内)
- * (すべてのソケット番号)
- 省略時は一個の * と同じ

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

[説明]

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

[ノート]

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

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

9.2　LAN 側の設定

9.2.1　イーサネットフレームタイプの設定

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

[設定値]
- *interface* ..... LAN インタフェース名
- *type*
  - 0 ..... IEEE 802.3 Raw
  - 1 ..... Ethernet II 、イーサネットタイプは 0x8137
  - 2 ..... IEEE 802.3 + IEEE 802.2,SAP は 0xE0
  - 3 ..... IEEE 802.3 + IEEE 802.2 SNAP、プロトコル ID は 0x0000008137

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

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

[初期値]　0

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

9.2.2　LAN 側の IPX ネットワーク番号の設定

[書式]　**ipx** *interface* **network** *network*
no ipx *interface* **network** [*network*]

[設定値]
- *interface* ..... LAN インタフェース名
- *network* ..... IPX ネットワーク番号 (0:0:0:1 ..FF:FF:FF:FE)

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

[初期値]　IPX ネットワーク番号は設定されていない

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

9.2.3　LAN 側でのフィルタリングによるセキュリティの設定

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

[設定値]
- *interface* ..... LAN インタフェース名
- *direction*
  - in ..... LAN 側から入ってくる方向でフィルタを適用
  - out ..... LAN 側へ出ていく方向でフィルタを適用
- *filter_list* ..... フィルタ番号の並び (100 個以内)

[説明]　LAN 側に対して適用する IPX フィルタを設定する。

[ノート]　フィルタリストを走査して、一致すると通過、破棄が決定する。

```
# ipx filter 1 pass 0:0:1:*
# ipx filter 2 reject 0:0:1:1
# ipx lan secure filter in 1 2
```

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

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

9.2.4　LAN 側の RIP/SAP ブロードキャストの設定

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

[設定値]
- *interface*.....LAN インタフェース名
- *broadcast*
  - 秒数 (60..21474836)
  - off.....RIP/SAP をブロードキャストしない

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

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

[初期値]　60

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

9.2.5　経路情報の追加

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

[設定値]
- *interface*.....LAN インタフェース名
- *network* .....終点 IPX ネットワーク番号 (0:0:0:1 .. FF:FF:FF:FE)
- *gateway*.....ゲートウェイの IPX ノード番号 (0:0:0:0:0:1 .. FF:FF:FF:FF:FF:FE)
- *hop* .....ホップカウント (1..14)
- *ticks*.....ティック (1..65535)

[説明]　IPX の経路情報テーブルに LAN 側の経路情報を追加する。

[ノート]　ティックを省略した場合はホップカウントと同じになる。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

9.3　PP 側相手毎の IPX の設定

9.3.1　IPX ルーティング許可の設定

[書式]　**ipx pp routing** *routing*
no ipx pp routing [*routing*]

[設定値]
- *routing*
  - on .....PP 側に IPX パケットをルーティングする
  - off.....PP 側に IPX パケットをルーティングしない

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

[初期値]　off

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

9.3.2　PP 側 IPX ネットワーク番号の設定

[書式]　**ipx pp network** *network* [*node_num*]
no ipx pp network [*network* [*node_num*]]

[設定値]
- *network* .....IPX ネットワーク番号 (0:0:0:1..FF:FF:FF:FE)
- *node_num*.....IPX ノード番号 (0:0:0:0:0:1..FF:FF:FF:FF:FF:FE)

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

[ノート]　IPX ノード番号は通常デフォルトのままとする。

[初期値]　IPX ネットワーク番号は設定されていない
IPX ノード番号は MAC アドレス

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

9.3.3 経路情報の追加

[書式] **ipx pp route** *network* [*name*] *hop* [*tick*]
ipx pp route *network* [dlci=*dlci_num*] *hop* [*tick*]
no ipx pp route *network* [*network...*]

[設定値] ◦ *network*..... 終点 IPX ネットワーク番号 (0:0:0:1..FF:FF:FF:FE)
◦ *name*..... 名前 (16 文字以内)
◦ *hop*..... ホップカウント (1..14)
◦ *tick*..... ティック (1..65535)
◦ *dlci_num*..... ゲートウェイの DLCI

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

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

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

9.3.4 IPXWAN 使用の設定

[書式] **ipx pp ipxwan use** *use*
no ipx pp ipxwan use [*use*]

[設定値] ◦ *use*
• on..... 接続時に IPXWAN を用いてパラメータのネゴシエーションを行う
• off..... パラメータのネゴシエーションは IPXCP で行い、IPXWANは用いない

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

[初期値] on

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

9.3.5 IPXWAN プライマリネットワーク番号の設定

[書式] **ipx pp ipxwan primnet** *network*
no ipx pp ipxwan primnet [*network*]

[設定値] ◦ *network*..... IPXWAN プライマリネットワーク番号 (0:0:0:1 .. FF:FF:FF:FE)

[説明] IPXWAN で用いるプライマリネットワーク番号を設定する。

[初期値] PP 側インタフェースの MAC アドレスの下位 32 ビット

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

9.3.6 回線接続時の PP 側の RIP/SAP の動作の設定

[書式] **ipx pp ripsap connect send** *send*
no ipx pp ripsap connect send [*send*]

[設定値] ◦ *send*
• none ..... 回線接続時に RIP/SAP を送出しない
• interval..... **ipx pp ripsap connect interval** コマンドで設定された時間間隔で RIP/SAP を送出する
• update..... RIP/SAP テーブルに変更があった場合だけ送出する

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

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

[初期値] update

[設定例] # ipx pp ripsap connect interval 120
ipx pp ripsap connect send interval

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

9.3.7　回線接続時の PP 側の RIP/SAP 送出の時間間隔の設定

[書式]　**ipx pp ripsap connect interval** *time*
no ipx pp ripsap connect interval [*time*]

[設定値]　◦ *time*.....秒数 (60..21474836)

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

[初期値]　60

[設定例]　# ipx pp ripsap connect interval 120
ipx pp ripsap connect send interval

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

9.3.8　回線切断時の PP 側の RIP/SAP の動作の設定

[書式]　**ipx pp ripsap disconnect send** *send*
no ipx pp ripsap disconnect send [*send*]

[設定値]　◦ *send*
- none ..... 回線切断時に RIP/SAP を送出しない
- interval ..... **ipx pp ripsap disconnect interval** コマンドで設定された時間間隔でRIP/SAP を送出する
- update..... RIP/SAP テーブルに変更があった時だけ送出する

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

[初期値]　none

[設定例]　# ipx pp ripsap disconnect interval 120
ipx pp ripsap disconnect send interval

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

9.3.9　回線切断時の PP 側の RIP/SAP 送出の時間間隔の設定

[書式]　**ipx pp ripsap disconnect interval** *interval*
no ipx pp ripsap disconnect interval [*interval*]

[設定値]　◦ *interval* .....秒数 (60..21474836)

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

[初期値]　60

[設定例]　# ipx pp ripsap disconnect interval 120
ipx pp ripsap disconnect send interval

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

9.3.10　回線切断時に RIP/SAP 情報を保持するか否かの設定

[書式]　**ipx pp ripsap hold** *hold*
no ipx pp ripsap hold [*hold*]

[設定値]　◦ *hold*
- on ..... 保持する
- off..... 保持しない

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

[初期値]　on

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

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

[書式] **ipx pp ipxwan retry** *interval max*
no ipx pp ipxwan retry [*interval max*]

[設定値] ◦ *interval*..... 秒数 (10..21474836)
◦ *max*..... 最大再送回数 (0..10)

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

[初期値] *interval* = 20
max = 3

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

9.3.12 Watchdog パケットに対する代理応答の設定

[書式] **ipx pp watchdog proxy** *proxy*
no ipx pp watchdog proxy [*proxy*]

[設定値] ◦ *proxy*
• on..... 代理応答する
• off..... 代理応答しない

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

[初期値] on

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

9.3.13 Watchdog 代理応答の時間間隔の設定

[書式] **ipx pp watchdog interval** *interval*
no ipx pp watchdog interval [*interval*]

[設定値] ◦ *interval*..... 秒数 (1..21474836)

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

[初期値] 3600

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

9.3.14 SPX キープアライブ代理応答のタイマの設定

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

[設定値] ◦ *t1* ..... 秒数 (30..21474836)
◦ *t2* ..... 秒数 (30..65535)
◦ *t3* ..... 秒数 (1..65535)

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

[初期値] *t1* = 7200
t2 = 60
t3 = 10

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

9.3.15　SPX キープアライブ代理応答を行うか否かの設定

[書式]　**ipx pp spx keepalive proxy** *proxy*
no ipx pp spx keepalive proxy [*proxy*]

[設定値]　◦ *proxy*
- on ..... 代理応答を行う
- off..... 代理応答を行わない

[説明]　SPX キープアライブ代理応答を行うか否かを設定する。

[初期値]　on

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

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

[書式]　**ipx pp serialization filter** *filter*
no ipx pp serialization filter [*filter*]

[設定値]　◦ *filter*
- on ..... フィルタアウトする
- off..... フィルタアウトしない

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

[初期値]　on

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

9.3.17　PP 側でのフィルタリングによるセキュリティの設定

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

[設定値]　◦ *direction*
- in..... PP 側から入って来る方向でフィルタを適用
- out..... PP 側へ出て行く方向でフィルタを適用

◦ *filter_list* ..... 空白で区切られたフィルタ番号の並び (30 個以内)

[説明]　PP 側に対し適用するフィルタを設定する。

[ノート]　フィルタリストを走査して、一致すると通過、破棄が決定する。

```
ipx filter 1 pass 0:0:1:*
ipx filter 2 reject 0:0:1:1
ipx pp secure filter in 1 2
```

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

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

10. ブリッジの設定

SRT100 のブリッジ機能と RT300i のブリッジ機能は異なる実装となります。

10.1 インタフェース共通の設定

10.1.1 ブリッジ使用許可の設定

[書式] **bridge use** *use*
no bridge use [*use*]

[設定値] ◦ *use*
- on..... ブリッジする
- off..... ブリッジしない
- multicast ..... マルチキャストのみブリッジする

[説明] ブリッジを行うかどうかを設定する。

[ノート] このスイッチが on でも、**ip routing** on であれば、IP パケットはブリッジング対象外となる。
同様に **ipx routing** on であれば、IPX パケットはブリッジング対象外となる。
同様に **ipv6 routing** on であれば、IPv6 パケットはブリッジング対象外となる。

[初期値] off

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

10.1.2 ブリッジするインタフェースの設定

[書式] **bridge group** *interface_list*
no bridge group [*interface_list*]

[設定値] ◦ *interface_list*
- 相手先情報番号
- anonymous
- LAN インタフェース名

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

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

[初期値] インタフェースは設定されていない

[設定例] ◦LAN1 ポートと LAN2 ポート間でブリッジする
```
# bridge group lan1 lan2
```

◦LAN2 ポートと相手先情報番号 3 の間でブリッジする
```
# bridge group lan2 3
```

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

10.1.3 MAC アドレスのラーニングを行うか否かの設定

[書式] **bridge learning** *switch*
no bridge learning [*switch*]

[設定値] ◦ *switch*
- on..... 行う
- off..... 行わない

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

[初期値] on

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

10.1.4　ラーニング情報消去タイマの設定

[書式]　**bridge learning expire** *time*
no bridge learning expire [*time*]

[設定値]
◦ *time*
- 秒数.(1..21474836)
- off.....タイマを設定しない

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

[初期値]　off

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

10.1.5　ブリッジのフィルタの設定

[書式]　**bridge filter** *filter_num pass_reject src_mac*[*dst_mac*[*offset byte_list*]]
no bridge filter *filter_num* [*pass_reject src_mac*[*dst_mac*[*offset byte_list*]]]

[設定値]
◦ *filter_num*.....静的フィルタの番号 (1..100)
◦ *pass_reject*
- pass-log .....一致すれば通す (ログに記録する)
- pass-nolog .....一致すれば通す (ログに記録しない)
- reject-log.....一致すれば破棄する (ログに記録する)
- reject-nolog .....一致すれば破棄する (ログに記録しない)
- restrict-log .....回線が接続されていれば通し、切断されていれば破棄する (ログに記録する)
- restrict-nolog .....回線が接続されていれば通し、切断されていれば破棄する (ログに記録しない)

◦ *src_mac*.....始点 MAC アドレス
- xx:xx:xx:xx:xx:xx(xx は十六進数、または *)
- * (すべての MAC アドレスに対応)

◦ *dst_mac*
- 終点 MAC アドス *src_mac* と同じ形式
- 省略時は一個の * と同じ

◦ *offset*.....オフセットを表す十進数(イーサネットフレームの始点MACアドレスの直後を0とするバイト数)
◦ *byte_list*
- バイト列
  - xx(xx は 2 桁の十六進数)
  - 上項目のカンマで区切った並び (16 個以内)
- * (すべてのバイト表現)

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

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

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

10.2　LAN 側の設定

10.2.1　静的なラーニング情報の設定

[書式]　**bridge** *interface* **learning** *mac_address*
no bridge *interface* **learning** [*mac_address*]

[設定値]
◦ *interface*..... LAN インタフェース名
◦ *mac_address*..... xx:xx:xx:xx:xx:xx (xx は十六進数)

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

[ノート]　ラーニング情報は全体で 30 個まで設定できる。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

10.2.2 LAN 側でのブリッジのフィルタリングの設定

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

[設定値] ◦ *interface*..... LAN インタフェース名
◦ *direction*
• in..... LAN 側から入ってくるパケットのフィルタリング
• out ..... LAN 側に出ていくパケットのフィルタリング
◦ *filter_list* ..... 空白で区切られた静的フィルタ番号の並び (100 個以内)

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

[初期値] フィルタは設定されていない

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

10.3 PP 側相手毎のブリッジの設定

10.3.1 ラーニング情報の設定

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

[設定値] ◦ *mac_address*..... xx:xx:xx:xx:xx:xx (xx は十六進数)
◦ *dlci_num*..... DLCI 番号

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

[ノート] ラーニング情報は全体で 30 個まで設定できる。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

10.3.2 PP 側でのブリッジのフィルタリングの設定

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

[設定値] ◦ *direction*
• in..... PP 側から入ってくるパケットのフィルタリング
• out ..... PP 側に出ていくパケットのフィルタリング
◦ *filter_list* ..... 空白で区切られた静的フィルタ番号の並び (100 個以内)

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

[初期値] フィルタは設定されていない

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

11. イーサネットフィルタの設定

11.1　フィルタ定義の設定

[書式]

ethernet filter *num kind src_mac* [*dst_mac* [*offset byte_list*]]
ethernet filter *num kind type* [*scope*] [*offset byte_list*]
no ethernet filter *num* [*kind src_mac* [*dst_mac* [*offset byte_list*]]]
no ethernet filter *num* [*kind* dhcp-bind N [*offset byte_list*]]

[設定値]

◦ *num*.....静的フィルタの番号 (1-100)

◦ *kind*
- pass-log .....一致すれば通す (ログに記録する)
- pass-nolog .....一致すれば通す (ログに記録しない)
- reject-log .....一致すれば破棄する (ログに記録する)
- reject-nolog .....一致すれば破棄する (ログに記録しない)

◦ *src_mac*.....始点 MAC アドレス
xx:xx:xx:xx:xx:xx (xx は 16 進数、または *)
* (すべての MAC アドレスに対応)

◦ *dst_mac* .....終点 MAC アドレス
始点 MAC アドレス *src_mac* と同じ形式
省略時は一個の * と同じ

◦ *type*
- dhcp-bind .....指定された DHCP スコープで予約設定されているホストを対象にする
- dhcp-not-bind .....指定された DHCP スコープで予約設定されていないホストを対象にする

◦ *scope*.....DHCP スコープ
1..65535 の整数
DHCP スコープのリース範囲に含まれる IP アドレス

◦ *offset*.....オフセットを表す 10 進数 (イーサネットフレームの始点 MAC アドレスの直後を 0 とする)

◦ *byte_list*.....バイト列
xx(2 桁の 16 進数) あるいは *(任意のバイト) をカンマで区切った並び (16 個以内)

[説明]

イーサネットフレームのフィルタを設定する。本コマンドで設定されたフィルタは、**ethernet lan filter** コマンドで用いられる。

通常型のフィルタでは、始点 MAC アドレス、終点 MAC アドレスなどで送受信するイーサネットフレームにフィルタを適用する。

dhcp-bind 型のフィルタでは、以下のイーサネットフレームにフィルタを適用する。対象とならないイーサネットフレームはフィルタに合致しないものとして扱う。

◦ 以下のいずれかに該当する、IPv4 パケットの場合
- イーサネットタイプが IPv4(0x0800)
- PPPoE 環境で、イーサネットタイプが PPPoE データフレーム (0x8864)、プロトコル ID が IPv4(0x0800)
- 802.1Q タグ VLAN 環境で、TPID が 802.1Q タグ (0x8100)、イーサネットタイプが IPv4(0x0800)

イーサネットフレームの始点 MAC アドレスと始点 IP アドレスの組が、対象となる DHCP スコープで予約されているならフィルタに合致するとみなす。

◦ イーサネットタイプが、以下のいずれかの場合
- ARP(0x0806)
- RARP(0x8035)
- PPPoE 制御パケット (0x8863)
- MAC レイヤ制御パケット (0x8808)

イーサネットフレームの始点 MAC アドレスが、対象となる DHCP スコープで予約されているならフィルタに合致するとみなす。

dhcp-not-bind 型のフィルタでは、以下のイーサネットフレームにフィルタを適用する。対象とならないイーサネットフレームはフィルタに合致しないものとして扱う。

◦ イーサネットタイプが IPv4(0x0800) である場合

イーサネットフレームの始点 IP アドレスが、対象となる DHCP スコープのリース範囲に含まれていて、かつ、始点 MAC アドレスが DHCP スコープで予約されていない時にフィルタに合致するとみなす。

dhcp-bind、dhcp-not-bind 型のフィルタで対象とする DHCP スコープは、*scope* パラメータで指定する。

*scope*パラメータとしては DHCP スコープ番号を指定することもできるし、DHCP スコープが定義されているサブネットに含まれる IP アドレスで指定することもできる。IP アドレスで DHCP スコープを指定する場合に、複数の DHCP スコープが該当する時には、その中で最も長いネットマスク長を持つ DHCP スコープを選択する。

*scope*パラメータを省略した場合には、フィルタが適用されるインタフェースで使用される DHCP スコープがすべて対象となる。

dhcp-bind、dhcp-not-bind 型のフィルタが DHCP リレーエージェントとして動作しているルーターに設定された場合、DHCP サーバーから DHCP スコープとその DHCP スコープにおけるクライアントの予約情報を取得し、フィルタの適用時に参照する。DHCP サーバーからの DHCP スコープおよび予約情報の取得は、DHCP メッセージをリレーする際、DHCP メッセージのオプション部に予約情報を書き込んで通知することにより行なわれる。

[ノート]　LAN 分割機能を使用する場合には、オフセットとバイト列を指定したフィルタの定義に注意が必要である。
LAN 分割機能では、イーサネットフレームの MAC アドレス直後に 4 バイトの識別用フィールドが置かれる。
その識別用フィールドをスキップするために、オフセットに 4 バイトを加えることが必要である。
例えばイーサネットタイプフィールドを指定する場合、LAN 分割機能を使用しない場合はオフセットに 0 を指定するが、LAN 分割機能を使用する場合はオフセットに 4 を指定する。

dhcp-bind、dhcp-not-bind 型のフィルタでは、イーサネットフレームの始点 MAC アドレスや始点 IP アドレスを用いてフィルタの判定をするため、**ethernet lan filter** コマンドでは通常 in 方向にのみ使用することになる。out 方向の場合、始点 MAC アドレスはルーター自身の MAC アドレスになるため、DHCP の予約情報と一致することはない。

dhcp-bind 型フィルタは、予約されているクライアントだけを通過させる、という形になるため、通常は pass 等と組み合わせて使用する。一方、dhcp-not-bind 型フィルタは、予約されていないクライアントを破棄する、という形になるため、通常は reject 等と組み合わせて使用することになる。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

11.2　インタフェースへの適用の設定

[書式]　**ethernet** *interface* **filter** *dir list*
no ethernet *interface* **filter** *dir* [*list*]

[設定値]
- *interface* ..... LAN インタフェース名
- *dir*
  - in ..... LAN 側から入ってくるパケットのフィルタリング
  - out ..... LAN 側に出ていくパケットのフィルタリング
- *list* ..... 空白で区切られた静的フィルタ番号の並び (100 個以内)

[説明]　LAN 側を通るパケットについて、**ethernat filter** コマンドによるパケットのフィルタを組み合わせて、通過するパケットの種類を制限する。

[ノート]　LAN インタフェース名に指定できるのは物理的な LAN だけであり、VLAN インタフェースは指定できない。

[初期値]　フィルタは設定されていない

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

12. 入力遮断フィルタの設定

12.1　フィルタ定義の設定

[書式]

ip inbound filter *id action src_address[/mask] [dst_address[/mask] [protocol [src_port [dst_port]]]]*
ipv6 inbound filter *id action src_address[/mask] [dst_address[/mask] [protocol [src_port [dst_port]]]]*
no ip inbound filter *id [action [src_address[/mask] [dst_address[/mask] [protocol [src_port [dst_port]]]]]]*
no ipv6 inbound filter *id [action [src_address[/mask] [dst_address[/mask] [protocol [src_port [dst_port]]]]]]*

[設定値]

◦ *id* ..... フィルタの識別子 (1..65535)

◦ *action* ..... 動作
- pass-log ..... 通過させてログを記録する
- pass-nolog ..... 透過させてログを記録しない
- reject-log ..... 遮断してログを記録する
- reject-nolog ..... 遮断してログを記録しない

◦ *src_address* ..... 始点アドレス
- IP アドレス
- * (すべての IP アドレス)
- 間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目。これらは範囲を指定する。

◦ *dst_address* ..... 終点アドレス
- *src_address* と同じ形式
- 省略時は 1 個の * と同じ。

◦ *mask* ..... IP アドレスのビットマスク (*src_address* および *dst_address* がネットワークアドレスの場合のみ指定可)
- XXX.XXX.XXX.XXX(XXX は十進数、IPv4 の場合のみ有効)
- 0x に続く十六進数 (IPv4 の場合のみ有効)
- マスクビット数
- 省略時は最大長のマスク

◦ *protocol* ..... プロトコル
- プロトコルを表す十進数 (0..255)
- プロトコルを表すニーモニック

ニーモニック	10 進数	説明
icmp	1	icmp パケット
icmp-error	-	特定の TYPE コードの icmp パケット
icmp-info	-	特定の TYPE コードの icmp パケット
tcp	6	tcp パケット
tcpsyn	-	SYN フラグの立っている tcp パケット
tcpfin	-	FIN フラグの立っている tcp パケット
tcprst	-	RST フラグの立っている tcp パケット
established	-	ACK フラグの立っている tcp パケット 内から外への接続は許可するが、外から内への接続は拒否する機能
udp	17	udp パケット
gre	47	PPTP の gre パケット
esp	50	IPsec の esp パケット
ah	51	IPsec の ah パケット

- 上項目のカンマで区切った並び (5 個以内)
- tcpflag=flag_value/flag_mask または tcpflag!=flag_value/flag_mask
  - flag_value ..... 0x に続く十六進数、 0x0000 .. 0xffff
  - flag_mask ..... 0x に続く十六進数、 0x0000 .. 0xffff
- * (すべてのプロトコル)
- 省略時は * と同じ。

◦ *src_port* ..... ソースポート番号
- ポート番号を表す十進数
- ポート番号を表すニーモニック (一部)

ニーモニック	ポート番号
ftp	20,21
ftpdata	20
telnet	23
smtp	25
domain	53

ニーモニック	ポート番号
gopher	70
finger	79
www	80
pop3	110
sunrpc	111
ident	113
ntp	123
nntp	119
snmp	161
syslog	514
printer	515
talk	517
route	520
uucp	540

- 間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目。これらは範囲を指定する。
- 上項目のカンマで区切った並び (10 個以内)
- * (すべてのポート)
- 省略時は * と同じ。

◦ *dst_port*..... デスティネーションポート番号

- 書式は *src_port* と同じ。

[説明]　インタフェースの入り口で破棄または通過を決定したいパケットの条件を定義する。
このコマンドの設定は、**ip/ipv6** *interface* **inbound filter list** コマンドで参照される。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

12.2　適用の設定

[書式]
ip *interface* **inbound filter list** *id ...*
ipv6 *interface* **inbound filter list** *id ...*
ip pp inbound filter list *id ...*
ipv6 pp inbound filter list *id ...*
ip tunnel inbound filter list *id ..*
ipv6 tunnel inbound filter list *id ..*
no ip *interface* **inbound filter list** [*id ...]*
no ipv6 *interface* **inbound filter list** [*id ...]*
no ip pp inbound filter list [*id ...*]
no ipv6 pp inbound filter list [*id ...*]
no ip tunnel inbound filter list [*id ...*]
no ipv6 tunnel inbound filter list [*id ...*]

[設定値]
◦ *interface*..... LAN インタフェース名
◦ *id* **..... ip/ipv6 inbound filter** コマンドで定義したフィルタの識別子

[説明]　**ip/ipv6 inbound filter** コマンドによる設定を組み合わせて、インタフェースで受信するパケットの種類を制限する。
複数の ID を指定したときには、先に指定したものから順に、対応する **ip/ipv6 inbound filter** コマンドの条件とマッチするかどうかを評価する。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

13. ポリシーフィルタの設定

13.1　サービスの定義

[書式]　**ip policy service** *id service_name protocol* [*source_port destination_port*]
ipv6 policy service *id service_name protocol* [*source_port destination_port*]
no ip policy service *id* [*service_name* [*protocol* [*source_port destination_port*]]]
no ipv6 policy service *id* [*service_name* [*protocol* [*source_port destination_port*]]]

[設定値]
- *id* ..... サービスの識別子 (1 .. 65535)
- *service_name* ..... サービスの名前 (最大 16 文字まで)
- *protocol* ..... プロトコル (tcp, udp, icmp, ipv6, rsvp, gre, esp, ah, icmp6, ospf, pim)
- *source_port* ..... 始点ポート番号 (プロトコルが tcp または udp のときのみ指定できる)
  - * ... すべて
  - 番号 (0 .. 65535)
  - 番号の範囲 (例 : 6000-、6000-6010、-6010)
- *destination_port* ..... 終点ポート番号 (プロトコルが tcp または udp のときのみ指定できる)
  - 書式は *source_port* と同じ。

[説明]　サービスを定義する。このコマンドで定義したサービスは、**ip/ipv6 policy filter** コマンドや、**ip/ipv6 policy service group** コマンドで指定できる。

[ノート]　*service_name* として整数は設定できない。

[初期値]　設定されていない

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

13.2　インタフェースグループの定義

[書式]　**ip policy interface group** *id* [name=*name*] [*interface* ...] [group *group_id* ...]
ipv6 policy interface group *id* [name=*name*] [*interface* ...] [group *group_id* ...]
no ip policy interface group *id* [name=*name*] [*interface* ...] [group *group_id* ...]
no ipv6 policy interface group *id* [name=*name*] [*interface* ...] [group *group_id* ...]

[設定値]
- *id* ..... インタフェースグループの識別子 (1 .. 65535)
- *name* ..... 名前 (半角 32 文字以内)
- *interface* ..... インタフェース
  - * ..... すべて
  - lan* ..... すべての LAN インタフェース
  - pp* ..... すべての PP インタフェース
  - tunnel* ..... すべての TUNNEL インタフェース
  - lanN-lanM ..... LAN インタフェースの範囲 (例 : lan1-lan3)
  - ppN-ppM ..... PP インタフェースの範囲 (例 : pp1-pp30)
  - tunnelN-tunnelM ..... TUNNEL インタフェースの範囲 (例 : tunnel1-tunnel10)
  - lanN ..... LAN インタフェース
  - ppN ..... PP インタフェース
  - tunnelN ..... TUNNEL インタフェース
  - local ..... ルーター自身
- *group_id* ..... 他の **ip/ipv6 policy interface group** コマンドで定義したインタフェースグループの識別子 (1 .. 65535)

[説明]　インタフェースのグループを定義する。group キーワードの後ろに *group_id* を記述することで、他のインタフェースグループを入れ子にすることができる。ただし、さらにその先のグループは参照されない。ここで定義したグループは、**ip/ipv6 policy filter** コマンドで指定できる。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

13.3　アドレスグループの定義

[書式]

ip policy address group *id* [name=*name*] [*address* ...] [group *group_id* ...]
ipv6 policy address group *id* [name=*name*] [*address* ...] [group *group_id* ...]
no ip policy address group *id* [name=*name*] [*address* ...] [group *group_id* ...]
no ipv6 policy address group *id* [name=*name*] [*address* ...] [group *group_id* ...]

[設定値]

◦ *id*..... アドレスグループの識別子 (1 .. 65535)
◦ *name*..... 名前 (半角 32 文字以内)
◦ *address*..... アドレス
- * ..... すべて
- IP アドレス ..... 単一の IP アドレス
- IP アドレス / ネットマスク長 ..... 単一のネットワーク
- IP アドレス -IP アドレス..... IP アドレスの範囲

◦ *group_id*..... 他の **ip/ipv6 policy address group** コマンドで定義したアドレスグループの識別子 (1 .. 65535)

[説明]

アドレスのグループを定義する。group キーワードの後ろに *group_id* を記述することで、他のアドレスグループを入れ子にすることができる。ただし、さらにその先のグループは参照されない。このコマンドで定義したグループは、**ip/ipv6 policy filter** コマンドで指定できる。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

13.4　サービスグループの定義

[書式]

ip policy service group *id* [name=*name*] [*service* ...] [group *group_id* ...]
ipv6 policy service group *id* [name=*name*] [*service* ...] [group *group_id* ...]
no ip policy service group *id* [name=*name*] [*service* ...] [group *group_id* ...]
no ipv6 policy service group *id* [name=*name*] [*service* ...] [group *group_id* ...]

[設定値]

◦ *id*..... サービスグループの識別子 (1 .. 65535)
◦ *name*..... 名前 (半角 32 文字以内)
◦ *service*..... サービス
- *..... すべて
- 定義済みサービス..... http, ftp, dns など **ip filter** コマンドのポート設定のニーモニックに準ずる
- ユーザ定義サービス ..... **ip/ipv6 policy service** コマンドで定義した名前
- プロトコルとポート番号..... tcp/ ポート番号、または udp/ ポート番号

◦ *group_id*..... 他の **ip/ipv6 policy service group** コマンドで定義したサービスグループの識別子 (1 .. 65535)

[説明]

サービスのグループを定義する。group キーワードの後ろに *group_id* を記述することで、他のサービスグループを入れ子にすることができる。ただし、さらにその先のグループは参照されない。このコマンドで定義したグループは、**ip/ipv6 policy filter** コマンドで指定できる。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

13.5　ポリシーフィルタの定義

[書式]

ip policy filter *id action source_interface* [*dest_interface* [*source_address* [*dest_address* [*service*]]]]
ipv6 policy filter *id action source_interface* [*dest_interface* [*source_address* [*dest_address* [*service*]]]]
no ip policy filter *id* [*action* [*source_interface* [*dest_interface* [*source_address* [*dest_address* [*service*]]]]]]
no ipv6 policy filter *id* [*action* [*source_interface* [*dest_interface* [*source_address* [*dest_address* [*service*]]]]]]

[設定値]

◦ *id* ..... ポリシーフィルタの識別子 (1 .. 65535)

◦ *action* ..... 動作
- pass-log ..... 通過させてログに記録する
- pass-nolog ..... 通過させてログに記録しない
- reject-log ..... 破棄してログに記録する
- reject-nolog ..... 破棄してログに記録しない
- restrict-log ..... 回線がつながっているときのみ通過させてログに記録する
- restrict-nolog ..... 回線がつながっているときのみ通過せてログに記録しない
- static-pass-log ..... Stateful Inspection を使わずに通過させてログに記録する
- static-pass-nolog ..... Stateful Inspection を使わずに通過させてログに記録しない

◦ *source_interface* ..... 始点インタフェース
- * ..... すべて
- lan* ..... すべての LAN インタフェース
- pp* ..... すべての PP インタフェース
- tunnel* ..... すべての TUNNEL インタフェース
- lanN-lanM ..... LAN インタフェースの範囲 (例 : lan1-lan3)
- ppN-ppM ..... PP インタフェースの範囲 (例 : pp1-pp30)
- tunnelN-tunnelM ..... TUNNEL インタフェースの範囲 (例 : tunnel1-tunnel10)
- lanN ..... LAN インタフェース
- ppN ..... PP インタフェース
- tunnelN ..... TUNNEL インタフェース
- local ..... ルーター自身
- グループ番号 ..... **ip/ipv6 policy interface group** コマンドで定義した番号

◦ *dest_interface* ..... 終点インタフェース
- 書式は始点インタフェースと同じ

◦ *source_address* ..... 始点アドレス
- * ..... すべて
- IP アドレス ..... 単一の IP アドレス
- IP アドレス / ネットマスク長 ..... 単一のネットワーク
- IP アドレス -IP アドレス ..... IP アドレスの範囲
- グループ番号 ..... **ip/ipv6 policy address group** コマンドで定義した番号

◦ *dest_address* ..... 終点アドレス
- 書式は始点アドレスと同じ

◦ *service* ..... サービス
- * ..... すべて
- ユーザ定義サービス ..... **ip/ipv6 policy service** コマンドで定義した名前
- プロトコルとポート番号 ..... tcp/ ポート番号、または udp/ ポート番号
- グループ番号 ..... **ip/ipv6 policy service group** コマンドで定義した番号

[説明]

ポリシーフィルタを定義する。パラメータを省略したときには「*」が指定されたものとして扱う。
インタフェースとして anonymous インタフェースは定義できない。
なお、このコマンドの定義は、**ip/ipv6 policy filter set** コマンドや **ip/ipv6 policy filter set enable** コマンドを設定しないと有効にならない。

[初期値]

設定されていない

[設定例]

LAN1 の PC から LAN2 の Web サーバーへのアクセスを許可する
ip policy filter 1 pass-log lan1 lan2 * * http

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

13.6　ポリシーセットの定義

[書式]　**ip policy filter set** *id* [name=*name*] *filter_set …*
ipv6 policy filter set *id* [name=*name*] *filter_set …*
no ip policy filter set *id* [name=*name*] *filter_set …*
no ipv6 policy filter set *id* [name=*name*] *filter_set …*

[設定値]　◦ *id*..... ポリシーセットの識別子 (1 .. 65535)
◦ *name*..... 名前 (半角 32 文字以内)
◦ *filter_set*..... 空白で区切られたポリシー番号の並び (最大 128 個まで)
「[」や「]」記号により階層構造を表現できる

[説明]　ポリシーセットを定義する。新しいコネクションが発生するたびに、先頭から順に一致するか否かを評価する。
階層的な構造になっている場合には、上位のポリシーフィルタから順に評価し、より深い階層のポリシーフィルタを採用する。
階層を表現するためには「[」と「]」の記号を用いる。「[」は 1 つ下の階層への移動、「]」は 1 つ上の階層への移動を意味する。
「[」は番号の前に記述し「]」は番号の直後に記述する。
ポリシーフィルタの番号の直後に「-」を付け加えることで、そのポリシーフィルタを無効にすることができる。
なお、同じポリシーフィルタを重複して設定することはできない。

[初期値]　設定されていない

[設定例]　LAN から PP へは WEB サイトの閲覧のみを許可する
```
#ip policy filter 1 reject-nolog lan1 pp1 * * *
#ip policy filter 2 pass-nolog * * * * www
#ip policy filter set 1 name="WWW Access" 1 [2]
#ip policy filter set enable 1
```

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

13.7　ポリシーセットの有効化

[書式]　**ip policy filter set enable** *id*
ipv6 policy filter set enable *id*
no ip policy filter set enable [*id*]
no ipv6 policy filter set enable [*id*]

[設定値]　◦ *id*..... ポリシーセットの識別子 (1 .. 65535)

[説明]　ポリシーセットを指定する。このコマンドで指定したポリシーセットだけが実際に有効になる。
同時に有効にできるポリシーセットは 1 つだけである。

[ノート]　有効なポリシーセットの内容が変更された後には必ず本コマンドを実行する。

[初期値]　設定されていない

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

13.8　ポリシーセットの自動切り替え

[書式]

ip policy filter set switch *original backup* trigger *trigger ...* [count=*count*] [interval=*interval*] [recovery-time=*time*]
ipv6 policy filter set switch *original backup* trigger *trigger ...* [count=*count*] [interval=*interval*] [recovery-time=*time*]
no ip policy filter set switch *original backup* [trigger *trigger ...* [count=*count*] [interval=*interval*] [recovery-time=*time*]]
no ipv6 policy filter set switch *original backup* [trigger *trigger ...* [count=*count*] [interval=*interval*] [recovery-time=*time*]]

[設定値]

- *original* .....切り替え元のポリシーセットの番号 (1 .. 65535)
- *backup* .....切り替え後のポリシーセットの番号 (1 .. 65535)
- *trigger* .....切り替えのトリガ
  - winny ..... 不正アクセス検知機能で Winny を検知したとき
  - share ..... 不正アクセス検知機能で Share を検知したとき
  - ethernet-filter..... イーサネットフィルタで IP パケットが破棄されたとき
  - qos-class-control ..... DCC (Dynamic Class Control) で帯域の占有を検知したとき
- *count*..... ポリシーセットを切り替えるまでに受信するトリガの回数。*interval* で設定した時間中に *count* で設定した個数のトリガを受信したらポリシーセットを切り替える。
  - 1 .. 10
- *interval* ..... トリガの発生回数を計測する時間。*interval* で設定した時間中に *count* で設定した個数のトリガを受信したらポリシーセットを切り替える。
  - 秒数 (2 .. 600)
- *time*..... トリガの事象が最後に発生してから元のポリシーセットに戻すまでの猶予時間
  - 秒数 (60 .. 604800)
  - infinity .....ポリシーセットを元に戻さない

[説明]

trigger パラメータで指定した事象を契機として、ポリシーセットを自動的に切り替える。
original、*backup* パラメータには、**ip/ipv6 policy filter set** コマンドで定義したポリシーセットの識別番号を指定する。
事象によって切り替えるポリシーセットを変えることができる。このためには、下記のように複数のコマンドを設定すればよい。

- **ip policy filter set switch** 1 2 triger winny
- **ip policy filter set switch** 1 3 triger ethernet-filter
- **ip policy filter set switch** 1 4 triger qos-class-control

事象が発生したときに切り替えるタイミングを、*count* と *interval* の組み合わせで指定できる。
interval で指定した時間内に *count* で指定した回数の事象が発生したら、ポリシーセットを切り替える。
count が 1 のときには、最初の事象が発生したときにすぐにポリシーセットを切り替えるので、*interval* の設定は意味を持たない。
事象が発生しなくなってから元のポリシーセットに戻すまでの時間を *time* で指定できる。
time として infinity を指定したときには、ポリシーセットを元に戻さない。
この場合には、**ip/ipv6 policy filter set enable** コマンドを実行することでポリシーセットを元に戻すことができる。
切り替えが動作しているときに **ip/ipv6 policy filter set** コマンドや **ip/ipv6 policy filter set enable** コマンドの設定を変更したときには、切り替えに関する動作は中断し、切り替え前の状態に戻る。
なお、*original* と *backup* に同じポリシーセットを指定することはできない。
また、*original*、*backup* パラメータで指定したポリシーセットが定義されていないときには、ポリシーセットは切り替わらない。

[初期値]

count.....1[回]
interval.....5[秒]
time .....3600[秒]

[設定例]

winny の検知とイーサネットフィルタによるパケット破棄を契機として、ポリシーセットを 1 番から 2 番に切り替える。

```
ip policy filter set 1 name="main" 101 102 103 104 105 106
ip policy filter set 2 name="backup" 201 202 203 204 205 206
ip policy filter set switch 1 2 trigger winny ethernet-filter
```

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

13.9　タイマーの設定

[書式]　**ip policy filter timer** [*option=timeout ...*]
no ip policy filter timer

[設定値]
- *option* ..... オプション名
  - tcp-syn-timeout ..... SYN を受けてから設定された時間内にデータが流れなければセッションを切断する
  - tcp-fin-timeout ..... FIN を受けてから設定された時間が経てばセッションを強制的に解放する
  - tcp-idle-time ..... 設定された時間内に TCP セッションのデータが流れなければセッションを切断する
  - udp-idle-time ..... 設定された時間内に UDP セッションのデータが流れなければセッションを切断する
  - dns-timeout ..... DNS の query を受けてから設定された時間内にデータが流れなければセッションを切断する
  - icmp-timeout ..... 設定された時間内に ICMP セッションのデータが流れなければセッションを切断する (ping に適用される)
- *timeout* ..... タイムアウト時間 (秒)

[説明]　ポリシーフィルタで使用するタイマーの値を設定する。このコマンドの設定は IPv4 と IPv6 で共通である。

[初期値]　tcp-syn-timeout=30
tcp-fin-timeout=5
tcp-idle-time=3600
udp-idle-time=30
dns-timeout=5
icmp-timeout=10

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

14. URL フィルタの設定

14.1　フィルタ定義の設定

[書式]　**url filter** *Id kind keyword [src_addr[/mask]]*
no url filter *id*

[設定値]
- *id* ..... フィルタ番号 (1..65535)
- *kind*
  - pass, pass-nolog..... 一致すれば通す (ログに記録しない)
  - pass-log ..... 一致すれば通す (ログに記録する)
  - reject, reject-log..... 一致すれば破棄する (ログに記録する)
  - reject-nolog ..... 一致すれば破棄する (ログに記録しない)
- *keyword*
  - フィルタリングする URL の全部もしくは一部 (半角 255 文字以内)
  - *..... すべての URL に対応
- *src_addr*.....IP パケットの始点 IP アドレス
  - 1 個の IPv4 アドレス
  - 間に - (ハイフン) を挟んだ 2 つの IP アドレス、- を後ろにつけた IP アドレス、または - を前につけた IP アドレス (範囲指定)
  - *..... すべての IP アドレスに対応
  - 省略時は * と同じ
- *mask* ..... ネットマスク長 (*src_addr* がネットワークアドレスの場合のみ指定可)

[説明]　URL によるフィルタを設定する。本コマンドで設定されたフィルタは、**url** *interface* **filter** コマンドで用いられる。
指定されたキーワードに、大文字のアルファベットが含まれる場合、それらを小文字に変換して保存する。

[ノート]　RTX1100、RT107e の Rev.8.03.75 以降、RTX3000 の Rev.9.00.31 以降、SRT100 の Rev.10.00.38 以降で、src_addr をコンマ (,) で区切って複数指定することができる。

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

14.2　URL フィルタのインタフェースへの適用

[書式]　**url** *interface* **filter** *dir list*
url pp filter *dir list*
url tunnel filter *dir list*
no url *interface* **filter**
no url pp filter
no url tunnel filter

[設定値]
- *interface*.....LAN インタフェース名
- *dir*
  - in.....入力方向の HTTP コネクションをフィルタリングする
  - out.....出力方向の HTTP コネクションをフィルタリングする
- *list*.....空白で区切られた URL フィルタ番号の並び
  (512 個以内 ...RTX3000, 128 個以内 ...RTX3000 以外の機種)

[説明]　**url filter** コマンドで設定したフィルタを組み合わせて、インタフェースで送受信する HTTP パケットの URL によって制限を行う。
設定できるフィルタの数は、RTX3000 では 512 個以内、RTX3000 以外の機種では 128 個以内、またはコマンドライン文字列長 (4095 文字) で入力できる範囲内である。
指定されたすべてのフィルタにマッチしないパケットは破棄される。

[ノート]　RTX3000 は、Rev.9.00.31 以降で使用可能。
RTX1100、RT107e は、Rev.8.03.60 以降で使用可能。

[初期値]　フィルタは設定されていない。

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

14.3　URL フィルタでチェックを行う HTTP のポート番号の設定

[書式]　**url filter port** *list*
no url filter port

[設定値]　◦ *list* ..... 空白で区切られたポート番号の並び (4 個以内)

[説明]　URL フィルタでチェックを行う HTTP のポート番号を設定する。

[ノート]　RTX3000 は、Rev.9.00.31 以降で使用可能。
RTX1100、RT107e は、Rev.8.03.60 以降で使用可能。

[初期値]　80

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

14.4　URL フィルターを使用するか否かの設定

[書式]　**url filter use** *switch*
no url filter use

[設定値]　◦ *switch*
- on..... URL フィルターを使用する
- off..... URL フィルターを使用しない

[説明]　URL フィルターを使用するか否かを設定する。

[ノート]　RTX1100、RT107e の Rev.8.03.75 以降、RTX3000 の Rev.9.00.31 以降、SRT100 の Rev.10.00.31 以降で使用可能。

[初期値]　on

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

14.5　URL フィルタで破棄するパケットの送信元に HTTP レスポンスを返す動作の設定

[書式]　**url filter reject** *redirect*
url filter reject *redirect url*
url filter reject *off*
no url filter reject [*action*]

[設定値]　◦ *redirect* ..... HTTP リダイレクトの HTTP レスポンスを返し、ブロック画面へ転送する
◦ *off* ..... HTTP レスポンスは返さずに、TCP RST によって TCP セッションを終了する
◦ *url* ..... リダイレクトする URL(http:// または https:// で始まる文字列で、半角 255 文字以内)
◦ *action*
- redirect
- off

[説明]　URL フィルタで破棄するパケットの送信元に HTTP レスポンスを返す動作を設定する。
ブロック画面には、一致したキーワードまたは、アクセスを遮断した理由を表示する。
URL を指定した場合、実際にリダイレクトするときには指定した URL の後ろに "?" に続けて以下の内容のクエリを付加する。
- アクセスを遮断した URL
- マッチしたフィルタに設定されているキーワード

URL に http:// または https:// で始まる文字列以外を設定することはできない。

[ノート]　HTTP サーバー機能に対応した機種では、redirect を設定して Web ブラウザにブロック画面を表示する場合、httpd service on の設定が必要である。
URL は、RTX3000 ... Rev.9.00.31 以降で使用可。RTX1100、RT107e ... Rev.8.03.75 以降で使用可。

[初期値]　off RTX3000
redirect..... 上記以外の機種

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

14.6　フィルタにマッチした際にログを出力するか否かの設定

[書式]　**url filter log** *switch*
no url filter log

[設定値]　◦ *switch*
- on ..... フィルタにマッチした際にログを出力する
- off..... フィルタにマッチした際にログを出力しない

[説明]　フィルタにマッチした際にログを出力するか否かを設定する。

[ノート]　on を設定した場合でも、**url filter** コマンドで *kind* に pass、p pass-nolog、または reject-nolog を指定したフィルタにマッチした場合はログを出力しない。

以下のリビジョンで使用可能
Rev.8.03.75 以降、Rev.9.00.31 以降、Rev.10.00.38 以降、Rev.10.01 系

[初期値]　on

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

15. PPP の設定

15.1 相手の名前とパスワードの設定

[書式] **pp auth username** *username password* [myname *myname mypass*] [*isdn1*] [clid [*isdn2*]] [mscbcp] [*ip_address*] [*ip6_prefix*]
pp auth username *username password* [myname *myname mypass*] [*ip_address*] [*ip6_prefix*]
no pp auth username *username* [*password...*]

[設定値]
- *username*..... 名前 (64 文字以内)
- *password*..... パスワード (64 文字以内)
- myname..... 自分側の設定を入力するためのキーワード
- *myname*..... 自分側のユーザ名
- *mypass*..... 自分側のパスワード
- *isdn1*..... 相手の ISDN アドレス
- clid..... 発番号認証を利用することを示すキーワード
- *isdn2*..... 発番号認証に用いられる ISDN アドレス
- mscbcp..... MS コールバックを許可することを示すキーワード
- *ip_address*..... 相手に割り当てる IP アドレス
- *ip6_prefix*..... ユーザに割り当てるプレフィックス

[説明] 相手の名前とパスワードを設定する。複数の設定が可能。
オプションで自分側の設定も入力ができる。

BRI インタフェースを持たないモデルでは第 2 書式を用いる。

双方向で認証を行う場合には、相手のユーザ名が確定してから自分を相手に認証させるプロセスが動き始める。これらのパラメータが設定されていない場合には、**pp auth myname** コマンドの設定が参照される。
オプションで ISDN 番号が設定でき、名前と結びついたルーティングやリモート IP アドレスに対しての発信を可能にする。*isdn1* は発信用の ISDN アドレスである。*isdn1* を省略すると、この相手には発信しなくなる。
名前に '*' を与えた場合にはワイルドカードとして扱い、他の名前とマッチしなかった相手に対してその設定を使用する。

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

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

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.2 受け入れる認証タイプの設定

[書式] **pp auth accept** *accept* [*accept*]
no pp auth accept [*accept*]

[設定値]
- *accept*
  - pap ..... PAP による認証を受け入れる
  - chap ..... CHAP による認証を受け入れる
  - mschap ..... MSCHAP による認証を受け入れる
  - mschap-v2..... MSCHAP Version2 による認証を受け入れる

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

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

[ノート] PPTP 機能を持たないモデルでは pap, chap のみ指定が可能。

[初期値] 認証を受け入れない

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.3　要求する認証タイプの設定

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

[設定値]　◦ *auth*
- pap .....PAP による認証を要求する
- chap .....CHAP による認証を要求する
- mschap.....MSCHAP による認証を要求する
- mschap-v2 .....MSCHAP Version2 による認証を要求する
- chap-pap.....CHAP もしくは PAP による認証を要求する

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

chap-pap キーワードの場合には、最初CHAP を要求し、それが相手から拒否された場合には改めて PAP を要求するよう動作する。これにより、相手が PAP または CHAP の片方しかサポートしていない場合でも容易に接続できるようになる。
arrive-only キーワードが指定された場合には、着信時にのみ PPP による認証を要求するようになり、発信時には要求しない。

[ノート]　PPTP 機能を持たないモデルでは pap, chap, chap-pap のみ指定が可能。

[初期値]　設定なし

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.4　自分の名前とパスワードの設定

[書式]　**pp auth myname** *myname password*
no pp auth myname [*myname password*]

[設定値]　◦ *myname*.....名前 (64 文字以内)
◦ *password*.....パスワード (64 文字以内)

[説明]　PAP または CHAP で相手に送信する自分の名前とパスワードを設定する。
PP 毎のコマンドである。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

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

[書式]　**pp auth multi connect prohibit** *prohibit*
no pp auth multi connect prohibit [*prohibit*]

[設定値]　◦ *prohibit*
- on .....禁止する
- off.....禁止しない

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

[ノート]　定額制プロバイダを営む場合に便利である。ユーザ管理を RADIUS で行う場合には、二重接続の禁止は RADIUS サーバーの方で対処する必要がある。
anonymous が選択された場合のみ有効である。

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.6　LCP 関連の設定

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

[書式]　**ppp lcp acfc** *acfc*
no ppp lcp acfc [*acfc*]

[設定値]　◦ *acfc*
- on..... 用いる
- off..... 用いない

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

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

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.6.2　Magic Number オプション使用の設定

[書式]　**ppp lcp magicnumber** *magicnumber*
no ppp lcp magicnumber [*magicnumber*]

[設定値]　◦ *magicnumber*
- on..... 用いる
- off..... 用いない

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

[ノート]　on を設定していても相手に拒否された場合は用いない。

[初期値]　on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.6.3　Maximum Receive Unit オプション使用の設定

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

[設定値]　◦ *mru*
- on..... 用いる
- off..... 用いない

◦ *length* ..... MRU の値 (1280..1792)

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

[ノート]　on を設定していても相手に拒否された場合は用いない。一般には on でよいが、このオプションをつけると接続できないルーターに接続する場合には off にする。
データ圧縮を利用する設定の場合には、*length* パラメータの設定は常に 1792 として動作する。

[初期値]　*mru* = on
length = 1792

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

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

[書式]　**ppp lcp pfc** *pfc*
no ppp lcp pfc [*pfc*]

[設定値]　◦ *pfc*
- on ..... 用いる
- off..... 用いない

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

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

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.6.5　lcp-restart パラメータの設定

[書式]　**ppp lcp restart** *time*
no ppp lcp restart [*time*]

[設定値]　◦ *time*..... ミリ秒 (20..10000)

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

[初期値]　3000

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.6.6　lcp-max-terminate パラメータの設定

[書式]　**ppp lcp maxterminate** *count*
no ppp lcp maxterminate [*count*]

[設定値]　◦ *count*..... 回数 (1..10)

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

[初期値]　2

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.6.7　lcp-max-configure パラメータの設定

[書式]　**ppp lcp maxconfigure** *count*
no ppp lcp maxconfigure [*count*]

[設定値]　◦ *count*..... 回数 (1..10)

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

[初期値]　10

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.6.8　lcp-max-failure パラメータの設定

[書式]　**ppp lcp maxfailure** *count*
no ppp lcp maxfailure [*count*]

[設定値]　◦ *count*..... 回数 (1..10)

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

[初期値]　10

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.6.9 Configure-Request をすぐに送信するか否かの設定

[書式] **ppp lcp silent** *switch*
no ppp lcp silent [*switch*]

[設定値] ◦ *switch*
- on..... PPP/LCP で、回線接続直後の Configure-Request の送信を、相手から Configure-Request を受信するまで遅らせる
- off..... PPP/LCP で、回線接続直後に Configure-Request を送信する

[説明] PPP/LCP で、回線接続後 Configure-Request をすぐに送信するか、あるいは相手から Configure-Request を受信するまで遅らせるかを設定する。通常は回線接続直後に Configure-Request を送信して構わないが、接続相手によってはこれを遅らせた方がよいものがある。

[初期値] off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.7 PAP 関連の設定

15.7.1 pap-restart パラメータの設定

[書式] **ppp pap restart** *time*
no ppp pap restart [*time*]

[設定値] ◦ *time*..... ミリ秒 (20..10000)

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

[初期値] 3000

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.7.2 pap-max-authreq パラメータの設定

[書式] **ppp pap maxauthreq** *count*
no ppp pap maxauthreq [*count*]

[設定値] ◦ *count*..... 回数 (1..10)

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

[初期値] 10

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.8 CHAP 関連の設定

15.8.1 chap-restart パラメータの設定

[書式] **ppp chap restart** *time*
no ppp chap restart [*time*]

[設定値] ◦ *time*..... ミリ秒 (20..10000)

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

[初期値] 3000

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.8.2 chap-max-challenge パラメータの設定

[書式] **ppp chap maxchallenge** *count*
no ppp chap maxchallenge [*count*]

[設定値] ◦ *count*..... 回数 (1..10)

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

[初期値] 10

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.9　IPCP 関連の設定

15.9.1　Van Jacobson Compressed TCP/IP 使用の設定

[書式]　**ppp ipcp vjc** *compression*
no ppp ipcp vjc [*compression*]

[設定値]　◦ *compression*
- on ..... 使用する
- off..... 使用しない

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

[ノート]　on を設定していても相手に拒否された場合は用いない。

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.9.2　PP 側 IP アドレスのネゴシエーションの設定

[書式]　**ppp ipcp ipaddress** *negotiation*
no ppp ipcp ipaddress [*negotiation*]

[設定値]　◦ *negotiation*
- on ..... ネゴシエーションする
- off..... ネゴシエーションしない

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

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.9.3　ipcp-restart パラメータの設定

[書式]　**ppp ipcp restart** *time*
no ppp ipcp restart [*time*]

[設定値]　◦ *time*..... ミリ秒 (20..10000)

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

[初期値]　3000

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.9.4　ipcp-max-terminate パラメータの設定

[書式]　**ppp ipcp maxterminate** *count*
no ppp ipcp maxterminate [*count*]

[設定値]　◦ *count*..... 回数 (1..10)

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

[初期値]　2

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.9.5 ipcp-max-configure パラメータの設定

[書式] **ppp ipcp maxconfigure** *count*
no ppp ipcp maxconfigure [*count*]

[設定値] ◦ *count*..... 回数 (1..10)

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

[初期値] 10

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.9.6 ipcp-max-failure パラメータの設定

[書式] **ppp ipcp maxfailure** *count*
no ppp ipcp maxfailure [*count*]

[設定値] ◦ *count*..... 回数 (1..10)

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

[初期値] 10

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.9.7 WINS サーバーの IP アドレスの設定

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

[設定値] ◦ *server1, server2*..... IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))

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

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

[初期値] WINS サーバーは設定されていない

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.9.8 IPCP の MS 拡張オプションを使うか否かの設定

[書式] **ppp ipcp msext** *msext*
no ppp ipcp msext [*msext*]

[設定値] ◦ *msext*
- on..... 使用する
- off..... 使用しない

[説明] 選択されている相手について、[PPP,IPCP] の MS 拡張オプションを使うか否かを設定する。
IPCP の Microsoft 拡張オプションを使うように設定すると、DNS サーバーの IP アドレスと WINS (Windows Internet Name Service) サーバーの IP アドレスを、接続した相手である Windows マシンに渡すことができる。渡すための DNS サーバーや WINS サーバーの IP アドレスはそれぞれ、**dns server** コマンドおよび **wins server** コマンドで設定する。
off の場合は、DNS サーバーや WINS サーバーのアドレスを渡されても受け取らない。

[初期値] off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.9.9　ホスト経路が存在する相手側 IP アドレスを受け入れるか否かの設定

[書式]　**ppp ipcp remote address check** *sw*
no ppp ipcp remote address check *[sw]*

[設定値]　◦ *sw*
- on ..... 通知された相手の PP 側 IP アドレスを拒否する
- off..... 通知された相手の PP 側 IP アドレスを受け入れる

[説明]　他の PP 経由のホスト経路が既に存在している IP アドレスを PP 接続時に相手側 IP アドレスとして通知されたときに、その IP アドレスを受け入れるか否かを設定する。

[ノート]　Rev.7.01.53、Rev.8.03 以降のファームウェアで利用可能。

[初期値]　on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

15.10　IPXCP 関連の設定

15.10.1　ipxcp-restart パラメータの設定

[書式]　**ppp ipxcp restart** *time*
no ppp ipxcp restart *[time]*

[設定値]　◦ *time*..... ミリ秒 (20..10000)

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

[初期値]　3000

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

15.10.2　ipxcp-max-terminate パラメータの設定

[書式]　**ppp ipxcp maxterminate** *count*
no ppp ipxcp maxterminate *[count]*

[設定値]　◦ *count*..... 回数 (1..10)

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

[初期値]　2

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

15.10.3　ipxcp-max-configure パラメータの設定

[書式]　**ppp ipxcp maxconfigure** *count*
no ppp ipxcp maxconfigure *[count]*

[設定値]　◦ *count*..... 回数 (1..10)

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

[初期値]　10

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

15.10.4　ipxcp-max-failure パラメータの設定

[書式]　**ppp ipxcp maxfailure** *count*
no ppp ipxcp maxfailure *[count]*

[設定値]　◦ *count*..... 回数 (1..10)

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

[初期値]　10

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

15.11　BCP 関連の設定

15.11.1　LAN Identification 使用の設定

[書式]　**ppp bcp lanid** *lan_id*
no ppp bcp lanid [*lan_id*]

[設定値]　◦ *lan_id*
- 十六進数 (0x1 .. 0xfffffffe)
- off..... LAN-Identification を使用しない

[説明]　選択されている相手について LAN-Identification の値を設定する。

[初期値]　off

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

15.11.2　Tinygram compression 使用の設定

[書式]　**ppp bcp tinycomp** *compression*
no ppp bcp tinycomp [*compression*]

[設定値]　◦ *compression*
- on..... 使用する
- off..... 使用しない

[説明]　選択されている相手について Tinygram compression を使用するか否かを設定する。

[初期値]　on

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

15.11.3　bcp-restart パラメータの設定

[書式]　**ppp bcp restart** *time*
no ppp bcp restart [*time*]

[設定値]　◦ *time*..... ミリ秒 (20..10000)

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

[初期値]　3000

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

15.11.4　bcp-max-terminate パラメータの設定

[書式]　**ppp bcp maxterminate** *count*
no ppp bcp maxterminate [*count*]

[設定値]　◦ *count*..... 回数 (1..10)

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

[初期値]　2

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

15.11.5　bcp-max-configure パラメータの設定

[書式]　**ppp bcp maxconfigure** *count*
no ppp bcp maxconfigure [*count*]

[設定値]　◦ *count*..... 回数 (1..10)

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

[初期値]　10

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

15.11.6　bcp-max-failure パラメータの設定

[書式]　**ppp bcp maxfailure** *count*
no ppp bcp maxfailure [*count*]

[設定値]　◦ *count*..... 回数 (1..10)

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

[初期値]　10

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

15.12　MSCBCP 関連の設定

15.12.1　mscbcp-restart パラメータの設定

[書式]　**ppp mscbcp restart** *time*
no ppp mscbcp restart [*time*]

[設定値]　◦ *time*..... ミリ秒 (20..10000)

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

[初期値]　1000

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

15.12.2　mscbcp-maxretry パラメータの設定

[書式]　**ppp mscbcp maxretry** *count*
no ppp mscbcp maxretry [*count*]

[設定値]　◦ *count*..... 回数 (1..30)

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

[初期値]　30

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	RTX1200	RTX1100	~~RTX1000~~	RT300i	RT250i	~~RT107e~~	~~SRT100~~

15.13　CCP 関連の設定

15.13.1　全パケットの圧縮タイプの設定

[書式]　**ppp ccp type** *type*
no ppp ccp type [*type*]

[設定値]　◦ *type*
- stac0 ..... Stac LZS で圧縮する
- stac ..... Stac LZS で圧縮する
- cstac ..... Stac LZS で圧縮する (接続相手が Cisco ルーターの場合)
- mppe-40 ..... 40bit MPPE で暗号化する
- mppe-128 ..... 128bit MPPE で暗号化する
- mppe-any ..... 40bit, 128bit MPPE いずれかの暗号化を行う
- none ..... 圧縮しない

[説明]　選択されている相手について [PPP,CCP] 圧縮方式を選択する。

[ノート]　Van Jacobson Compressed TCP/IP との併用も可能である。
type に *stac* を指定した時、回線状態が悪い場合や、高負荷で、パケットロスが頻繁に起きると、通信が正常に行えなくなることがある。このような場合、自動的に「圧縮なし」になる。その後、リスタートまで「圧縮なし」のままである。このような状況が改善できない時は、*stac0* を指定すればよい。ただしその時は接続先も *stac0* に対応していなければならない。*stac0* は stac よりも圧縮効率は落ちる。

接続相手が Cisco ルーターの場合に *stac* を適用すると通信できないことがある。そのような場合には、設定を *cstac* に変更すると通信が可能になることがある。

mppe-40, *mppe-128*, *mppe-any* の場合には 1 パケット毎に鍵交換される。MPPE は Microsoft Point- To-Point Encryption (Protocol) の略で CCP を拡張したものであり、暗号アルゴリズムとして RC4 を採用し、鍵長 40bit または 128bit を使う。暗号鍵生成のために認証プロトコルの MS-CHAP または MS- CHAPv2 と合わせて設定する。
RTX3000 では *stac0, stac, cstac, none* の指定が可能。
RT107e と SRT100 では none のみ指定が可能。

[初期値]　*none* (RT107e、SRT100)
stac (上記以外のモデル)

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.13.2　ccp-restart パラメータの設定

[書式]　**ppp ccp restart** *time*
no ppp ccp restart [*time*]

[設定値]　◦ *time* ..... ミリ秒 (20..10000)

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

[初期値]　*3000*

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.13.3　ccp-max-terminate パラメータの設定

[書式]　**ppp ccp maxterminate** *count*
no ppp ccp maxterminate [*count*]

[設定値]　◦ *count* ..... 回数 (1..10)

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

[初期値]　*2*

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.13.4　ccp-max-configure パラメータの設定

[書式]　**ppp ccp maxconfigure** *count*
no ppp ccp maxconfigure [*count*]

[設定値]　◦ *count*..... 回数 (1..10)

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

[初期値]　10

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.13.5　ccp-max-failure パラメータの設定

[書式]　**ppp ccp maxfailure** *count*
no ppp ccp maxfailure [*count*]

[設定値]　◦ *count*..... 回数 (1..10)

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

[初期値]　10

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.14　IPV6CP 関連の設定

15.14.1　IPV6CP を使用するか否かの設定

[書式]　**ppp ipv6cp use** *use*
no ppp ipv6cp use [*use*]

[設定値]　◦ *use*
- on..... 使用する
- off..... 使用しない

[説明]　選択されている相手について IPV6CP を使用するか否かを選択する。

[初期値]　on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

15.15　MP 関連の設定

15.15.1　MP を使用するか否かの設定

[書式]　**ppp mp use** *use*
no ppp mp use [*use*]

[設定値]　◦ *use*
- on..... 使用する
- off..... 使用しない

[説明]　選択されている相手について MP を使用するか否かを選択する。
on に設定していても、LCP の段階で相手とのネゴシエーションが成立しなければ MP を使わずに通信する。

[初期値]　off

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

15.15.2 MP の制御方法の設定

[書式] **ppp mp control** *type*
no ppp mp control [*type*]

[設定値] ◦ *type*
- arrive ..... 自分が 1B 目の着信側の場合に MP を制御する
- both ..... 自分が 1B 目の発信着信いずれの場合でも MP を制御する
- call..... 自分が 1B 目の発信側の場合に MP を制御する

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

[初期値] *call*

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

15.15.3 MP のための負荷閾値の設定

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

[設定値] ◦ *call_load*..... 発信負荷閾値 %(1..100)
◦ *call_count*..... 回数 (1..100)
◦ *disc_load*..... 切断負荷閾値 %(0..50)
◦ *disc_count*..... 回数 (1..100)

[説明] 選択されている相手について [PPP, MP] の 2B 目を発信したり切断したりする場合のデータ転送負荷の閾値を設定する。
負荷は回線速度に対する % で評価し、送受信で大きい方の値を採用する。*call_load* を超える負荷が *call_count* 回繰り返されたら 2B 目の発信を行う。逆に *disc_load* を下回る負荷が *disc_count* 回繰り返されたら 2B 目を切断する。

[初期値] *call_load* = 70
call_count = 1
disc_load = 30
disc_count = 2

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

15.15.4 MP の最大リンク数の設定

[書式] **ppp mp maxlink** *number*
no ppp mp maxlink [*number*]

[設定値] ◦ *number* ..... リンク数

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

[初期値] *2*

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

15.15.5 MP の最小リンク数の設定

[書式] **ppp mp minlink** *number*
no ppp mp minlink [*number*]

[設定値] ◦ *number* ..... リンク数

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

[初期値] *1*

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

15.15.6　MP のための負荷計測間隔の設定

[書式]　**ppp mp timer** *time*
no ppp mp timer [*time*]

[設定値]　◦ *time*.....秒数 (1..21474836)

[説明]　選択されている相手について [PPP, MP] のための負荷計測間隔を設定する。
単位は秒。負荷計測だけでなく、すべての MP の動作はこのコマンドで設定した間隔で行われる。

[初期値]　10

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

15.15.7　MP のパケットを分割するか否かの設定

[書式]　**ppp mp divide** *divide*
no ppp mp divide [*divide*]

[設定値]　◦ *divide*
- on.....分割する
- off.....分割しない

[説明]　選択されている相手について [PPP, MP] に対して、MP パケットの送信時にパケットを分割するか否かを設定する。
分割するとうまく接続できない相手に対してだけ off にする。
分割しないように設定した場合、特に TCP の転送効率に悪影響が出る可能性がある。
64 バイト以下のパケットは本コマンドの設定に関わらず分割されない。

[初期値]　on

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

15.16　BACP 関連の設定

15.16.1　bacp-restart パラメータの設定

[書式]　**ppp bacp restart** *time*
no ppp bacp restart [*time*]

[設定値]　◦ *time*.....ミリ秒 (20..10000)

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

[初期値]　3000

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

15.16.2　bacp-max-terminate パラメータの設定

[書式]　**ppp bacp maxterminate** *count*
no ppp bacp maxterminate [*count*]

[設定値]　◦ *count*.....回数 (1..10)

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

[初期値]　2

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

15.16.3　bacp-max-configure パラメータの設定

[書式]　**ppp bacp maxconfigure** *count*
no ppp bacp maxconfigure [*count*]

[設定値]　◦ *count*..... 回数 (1..10)

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

[初期値]　10

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

15.16.4　bacp-max-failure パラメータの設定

[書式]　**ppp bacp maxfailure** *count*
no ppp bacp maxfailure [*count*]

[設定値]　◦ *count*..... 回数 (1..10)

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

[初期値]　10

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

15.17　BAP 関連の設定

15.17.1　bap-restart パラメータの設定

[書式]　**ppp bap restart** *time*
no ppp bap restart [*time*]

[設定値]　◦ *time*..... ミリ秒 (20..10000)

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

[初期値]　1000

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

15.17.2　bap-max-retry パラメータの設定

[書式]　**ppp bap maxretry** *count*
no ppp bap maxretry [*count*]

[設定値]　◦ *count*..... 再送回数 (1..30)

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

[初期値]　30

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

15.18　PPPoE 関連の設定

15.18.1　PPPoE で使用する LAN インタフェースの指定

[書式]　**pppoe use** *interface*
no pppoe use

[設定値]　◦ *interface*..... LAN インタフェース名

[説明]　選択されている相手に対して、PPPoE で使用する LAN インタフェースを指定する。設定がない場合は、PPPoE は使われない。

[初期値]　PPPoE を使用しない。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

15.18.2　アクセスコンセントレータ名の設定

[書式]　**pppoe access concentrator** *name*
no pppoe access concentrator

[設定値]　◦ *name*.....アクセスコンセントレータの名前を表す文字列 (7bit US-ASCII)

[説明]　選択されている相手について PPPoE で接続するアクセスコンセントレータの名前を設定する。接続できるアクセスコンセントレータが複数ある場合に、どのアクセスコンセントレータに接続するのかを指定するために使用する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

15.18.3　セッションの自動接続の設定

[書式]　**pppoe auto connect** *switch*
no pppoe auto connect

[設定値]　◦ *switch*
- on.....自動接続する
- off.....自動接続しない

[説明]　選択されている相手に対して、PPPoE のセッションを自動で接続するか否かを設定する。

[初期値]　on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

15.18.4　セッションの自動切断の設定

[書式]　**pppoe auto disconnect** *switch*
no pppoe auto disconnect

[設定値]　◦ *switch*
- on.....自動切断する
- off.....自動切断しない

[説明]　選択されている相手に対して、PPPoE のセッションを自動で切断するか否かを設定する。

[初期値]　on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

15.18.5　PADI パケットの最大再送回数の設定

[書式]　**pppoe padi maxretry** *times*
no pppoe padi maxretry

[設定値]　◦ *times*.....回数 (1..10)

[説明]　PPPoE プロトコルにおける PADI パケットの最大再送回数を設定する。

[初期値]　5

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

15.18.6　PADI パケットの再送時間の設定

[書式]　**pppoe padi restart** *time*
no pppoe padi restart

[設定値]　◦ *time*.....ミリ秒 (20..10000)

[説明]　PPPoE プロトコルにおける PADI パケットの再送時間を設定する。

[初期値]　3000

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

15.18.7　PADR パケットの最大再送回数の設定

[書式]　**pppoe padr maxretry** *times*
no pppoe padr maxretry

[設定値]　◦ *times* ..... 回数 (1..10)

[説明]　PPPoE プロトコルにおける PADR パケットの最大再送回数を設定する。

[初期値]　5

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

15.18.8　PADR パケットの再送時間の設定

[書式]　**pppoe padr restart** *time*
no pppoe padr restart

[設定値]　◦ *time* ..... ミリ秒 (20..10000)

[説明]　PPPoE プロトコルにおける PADR パケットの再送時間を設定する。

[初期値]　3000

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

15.18.9　PPPoE セッションの切断タイマの設定

[書式]　**pppoe disconnect time** *time*
no pppoe disconnect time

[設定値]　◦ *time*
- 秒数 (1..21474836)
- off ..... タイマを設定しない

[説明]　選択されている相手に対して、タイムアウトにより PPPoE セッションを自動切断する時間を設定する。

[ノート]　LCP と NCP パケットは監視対象外。

[初期値]　off

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

15.18.10　サービス名の指定

[書式]　**pppoe service-name** *name*
no pppoe service-name

[設定値]　◦ *name* ..... サービス名を表す文字列 (7bit US-ASCII、255 文字以内)

[説明]　選択されている相手について PPPoE で要求するサービス名を設定する。
接続できるアクセスコンセントレータが複数ある場合に、要求するサービスを提供することが可能なアクセスコンセントレータを選択して接続するために使用する。

[初期値]　指定なし

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

15.18.11　TCP パケットの MSS の制限の有無とサイズの指定

[書式]　**pppoe tcp mss limit** *length*
no pppoe tcp mss limit

[設定値]　◦ *length*
- データ長 (1240..1452)
- auto.....MSS を MTU の値に応じて制限する
- off.....MSS を制限しない

[説明]　PPPoE セッション上で TCP パケットの MSS(Maximum Segment Size) を制限するか否かを設定する。

[ノート]　このコマンドと **ip** *interface* **tcp mss limit** コマンドの両方が有効な場合は、MSS はどちらかより小さな方の値に制限される。

[初期値]　*auto*

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

15.18.12　ルーター側には存在しない PPPoE セッションを強制的に切断するか否かの設定

[書式]　**pppoe invalid-session forced close** *sw*
no pppoe invalid-session forced close

[設定値]　◦ *sw*
- on.....ルーター側には存在しない PPPoE セッションを強制的に切断する
- off.....ルーター側には存在しない PPPoE セッションを強制的に切断しない

[説明]　ルーター側には存在しない PPPoE セッションを強制的に切断するか否かを設定します。

[ノート]　Rev.7.01.53、Rev.8.01.24、Rev.8.03.60 以降で使用可能。

[初期値]　*on*

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

16. DHCP の設定

本機は DHCP[1] 機能として、DHCP サーバー機能、DHCP リレーエージェント機能、DHCP クライアント機能を実装しています。DHCP 機能の利用により、基本的なネットワーク環境の自動設定を実現します。

DHCP クライアント機能は Windows 等の OS に実装されており、これらと本機の DHCP サーバー機能、DHCP リレーエージェント機能を組み合わせることにより DHCP クライアントの基本的なネットワーク環境の自動設定を実現します。

ルーターが DHCP サーバーとして機能するか DHCP リレーエージェントとして機能するか、どちらとしても機能させないかは **dhcp service** コマンドにより設定します。現在の設定は、**show status dhcp** コマンドにより知ることができます。

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

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

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

また DHCP クライアント機能により、インタフェースの IP アドレスやデフォルト経路情報などを外部の DHCP サーバーから受けることができます。ルーターを DHCP クライアントとして機能させるかどうかは、**ip** *interface* **address**、**ip** *interface* **secondary address**、**ip pp remote address**、**ip pp remote address pool** の各コマンドの設定値により決定されます。設定されている内容は、**show status dhcpc** コマンドにより知ることができます。

16.1 DHCP サーバー・リレーエージェント機能

16.1.1 DHCP の動作の設定

[書式]
dhcp service *type*
no dhcp service [*type*]

[設定値]
◦ *type*
- server..... DHCP サーバーとして機能させる
- relay..... DHCP リレーエージェントとして機能させる

[説明]
DHCP に関する機能を設定する。
DHCP リレーエージェント機能使用時には、NAT 機能を使用することはできない。

[ノート]
工場出荷状態および **cold start** コマンド実行後の本コマンドの設定値については「1.7 工場出荷設定値について」を参照してください。

[初期値]
DHCP サービスは機能しない

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

1. Dynamic Host Configuration Protocol; RFC1541, RFC2131
URL 参照 : http://rfc.netvolante.jp/rfc/rfc1541.txt (rfc2131.txt)

16.1.2　RFC2131 対応動作の設定

[書式]　**dhcp server rfc2131 compliant** *comp*
dhcp server rfc2131 compliant [except] *function* [*function..*]
no dhcp server rfc2131 compliant

[設定値]
◦ *comp*
- on ..... RFC2131 準拠
- off..... RFC1541 準拠

◦ except..... 指定した機能以外が RFC2131 対応となるキーワード

◦ *function*
- broadcast-nak..... ..... DHCPNAK をブロードキャストで送る
- none-domain-null ..... ドメイン名の最後に NULL 文字を付加しない
- remain-silent .... リース情報を持たないクライアントからの DHCPREQUEST を無視する
- reply-ack .... DHCPNAK の代わりに許容値を格納した DHCPACK を返す
- use-clientid .... クライアントの識別に Client-Identifier オプションを優先する

[説明]　DHCP サーバーの動作を指定する。on の場合には RFC2131 準拠となる。off の場合には、RFC1541 準拠の動作となる。
また RFC1541 をベースとして RFC2131 記述の個別機能のみを対応させる場合には以下のパラメータで指定する。これらのパラメータはスペースで区切り複数指定できる。except キーワードを指示すると、指定したパラメータ以外の機能が RFC2131 対応となる。

- broadcast-nak..... 同じサブネット上のクライアントに対しては DHCPNAK はブロードキャストで送る。DHCPREQUEST をクライアントが INIT-REBOOT state で送られてきたものに対しては、giaddr 宛てあれば Bbit を立てる。
- none-domain-null ..... 本ドメイン名の最後に NULL 文字を付加しない。RFC1541 ではドメイン名の最後に NULL 文字を付加するかどうかは明確ではなかったが、RFC2131 では禁止された。一方、Windows NT/2000 の DHCP サーバーは NULL 文字を付加している。そのため、Windows 系の OS での DHCP クライアントは NULL 文字があることを期待している節があり、NULL 文字がない場合には winipcfg.exe での表示が乱れるなどの問題が起きる可能性がある。
- remain-silent ..... クライアントから DHCPREQUEST を受信した場合に、そのクライアントのリース情報を持っていない場合には DHCPNAK を送らないようにする。
- reply-ack ..... クライアントから、リース期間などで許容できないオプション値 (リクエスト IP アドレスは除く) を要求された場合でも、DHCPNAK を返さずに許容値を格納した DHCPACK を返す。
- use-clientid ..... クライアントの識別に chaddr フィールドより Client-Identifier オプションを優先して使用する。

[ノート]　工場出荷状態および **cold start** コマンド実行後の本コマンドの設定値については「 1.7 工場出荷設定値について」を参照してください。

[初期値]　on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

16.1.3　リースする IP アドレスの重複をチェックするか否かの設定

[書式]　**dhcp duplicate check** *check1 check2*
no dhcp duplicate check

[設定値]
◦ *check1*..... LAN 内を対象とするチェックの確認用待ち時間
- ミリ秒 (*1..1000*)
- off..... LAN 内を対象とするチェックを行わない

◦ *check2*..... LAN 外 (DHCP リレーエージェント経由) を対象とするチェックの確認用待ち時間
- ミリ秒 (*1..3000*)
- off..... LAN 外 (DHCP リレーエージェント経由) を対象とするチェックを行わない

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

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

[初期値]　*check1* = 100
check2 = 500

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

16.1.4　DHCP スコープの定義

[書式]

dhcp scope *scope_num ip_address-ip_address/netmask* [except *ex_ip ...*] [gateway *gw_ip*] [expire *time*] [maxexpire *time*]
no dhcp scope *scope_num* [*ip_address-ip_address/netmask* [except *ex_ip ...*] [gateway *gw_ip*] [expire *time*] [maxexpire *time*]]

[設定値]

◦ *scope_num* ..... スコープ番号 (1..65535)
◦ *ip_address-ip_address* .....対象となるサブネットで割り当てる IP アドレスの範囲
◦ *netmask*
- xxx.xxx.xxx.xxx (xxx は十進数)
- 0x に続く十六進数
- マスクビット数

◦ *ex_ip* ..... IP アドレス指定範囲の中で除外する IP アドレス (空白で区切って複数指定可能、'-' を使用して範囲指定も可能)
◦ *gw_ip* .....IP アドレス対象ネットワークのゲートウェイの IP アドレス
◦ *time* ..... 時間
- 分 (1..2147483647)
- 時間 : 分
- infinity ..... 無期限リース

[説明]

DHCP サーバーとして割り当てる IP アドレスのスコープを設定する。
除外 IP アドレスは複数指定できる。リース期間としては無期限を指定できるほか、DHCP クライアントから要求があった場合の許容最大リース期間を指定できる。

[ノート]

ひとつのネットワークについて複数の DHCP スコープを設定することはできない。複数の DHCP スコープで同一の IP アドレスを含めることはできない。IP アドレス範囲にネットワークアドレス、ブロードキャストアドレスを含む場合、割り当て可能アドレスから除外される。
DHCP リレーエージェントを経由しない DHCP クライアントに対して *gateway* キーワードによる設定パラメータが省略されている場合にはルーター自身の IP アドレスを通知する。
DHCP スコープを上書きした場合、以前のリース情報および予約情報は消去される。
expire の設定値は maxexpire の設定値以下でなければならない。
except で除外 IP アドレスの範囲指定ができるのは Rev7.01 以降である。
工場出荷状態および **cold start** コマンド実行後の本コマンドの設定値については「 1.7 工場出荷設定値について」を参照してください。

[初期値]

expire *time* = 72:00
maxexpire *time* = 72:00

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

16.1.5　DHCP 予約アドレスの設定

[書式]

dhcp scope bind *scope_num ip_address* [*type*] *id*
dhcp scope bind *scope_num ip_address mac_address*
dhcp scope bind *scope_num ip_address* ipcp
no dhcp scope bind *scope_num ip_address*

[設定値]

◦ *scope_num* ..... スコープ番号 (1..65535)
◦ *ip_address*
- xxx.xxx.xxx.xxx... (xxx は十進数) 予約する IP アドレス
- * ..... 割り当てる IP アドレスを指定しない

◦ *type* ..... Client-Identifier オプションの type フィールドを決定する
- text 0x00
- ethernet 0x01

◦ *id*
- *type* が ethernet の場合 ...MAC アドレス
- *type* が text の場合 ..... 文字列
- *type* が省略された場合 .....2 桁十六進数の列で先頭は type フィールド

◦ *mac_address* ..... xx:xx:xx:xx:xx:xx (xx は十六進数) 予約 DHCP クライアントの MAC アドレス
◦ ipcp ..... IPCP でリモート側に与えることを示すキーワード

[説明]

IP アドレスを割り当てる DHCP クライアントを固定的に設定する。

Rev.8.03 以降のファームウェアでは、IP アドレスを固定せずにクライアントだけを指定することもできる。この形式を削除する場合はクライアント識別子を省略できない。

[ノート]　IP アドレスは、*scope_num* パラメータで指定された DHCP スコープ範囲内でなければならない。1 つの DHCP スコープ内では、1 つの MAC アドレスに複数の IP アドレスを設定することはできない。他の DHCP クライアントにリース中の IP アドレスを予約設定した場合、リース終了後にその IP アドレスの割り当てが行われる。

dhcp scope コマンド、あるいは **dhcp delete scope** コマンドを実行した場合、関連する予約はすべて消去される。
ipcp の指定は、同時に接続できる B チャネルの数に限られる。また、IPCP で与えるアドレスは LAN 側のスコープから選択される。

コマンドの第 1 書式を使う場合は、あらかじめ **dhcp server rfc2131 compliant** on あるいは use-clientid 機能を使用するよう設定されていなければならない。また **dhcp server rfc2131 compliant** off あるいは use-clientid 機能が使用されないよう設定された時点で、コマンドの第 2 書式によるもの以外の予約は消去される。

コマンドの第 1 書式でのクライアント識別子は、クライアントがオプションで送ってくる値を設定する。*type* パラメータを省略した場合には、*type* フィールドの値も含めて入力する。*type* パラメータにキーワードを指定する場合には *type* フィールド値は一意に決定されるので Client-Identifier フィールドの値のみを入力する。

コマンドの第 2 書式による MAC アドレスでの予約は、クライアントの識別に DHCP パケットの chaddr フィールドを用いる。この形の予約機能は、RT の設定が **dhcp server rfc2131 compliant** off あるいは use-clientid 機能を使用しない設定になっているか、もしくは DHCP クライアントが DHCP パケット中に Client-Identifier オプションを付けてこない場合でないと動作しない。

クライアントが Client-Identifier オプションを使う場合、コマンドの第 2 書式での予約は、**dhcp server rfc2131 compliant** on あるいは use-clientid パラメータが指定された場合には無効になるため、新たに Client-Identifer オプションで送られる値で予約し直す必要がある。

[設定例]　A. # dhcp scope bind *scope_num ip_address* ethernet 00:a0:de:01:23:45
B. # dhcp scope bind *scope_num ip_address* text client01
C. # dhcp scope bind *scope_num ip_address* 01 00 a0 de 01 23 45 01 01 01
D. # dhcp scope bind *scope_num ip_address* 00:a0:de:01:23:45

1. **dhcp server rfc2131 compliant** on あるいは use-clientid 機能ありの場合

dhcp scope bind での指定方法	A. B. C.	D.
クライアントの識別に用いる情報	Client-Identifier オプション	chaddr(※ 1)

※ 1 Client-Identifier オプションが存在しない場合に限られ、Client-Identifier オプションが存在する場合にはこの設定は無視される

dhcp server rfc2131 compliant on あるいは use-clientid 機能ありでアドレスをリースする場合、DHCP サーバーは chaddr に優先して Client-Identifier オプションを使用する。そのため、この場合の **show status dhcp** コマンド実行でクライアントの識別子を確認することで、クライアントが Client-Identifier オプションを使っているか否かを判別することも可能である。

すなわち、リースしているクライアントとして MAC アドレスが表示されていれば Client-Identifier オプションは使用されておらず、十六進文字列あるいは文字列でクライアントが表示されていれば、Client-Identifier オプションが使われている。この場合、Client-Identifier オプションを使うクライアントへの予約は、ここで表示される十六進文字列あるいは文字列を使用する。

2. **dhcp server rfc2131 compliant** off あるいは use-clientid 機能なしの場合

dhcp scope bind での指定方法	(※ 2)	D.
クライアントの識別に用いる情報	(※ 3)	chaddr

※ 2 他の方法での指定は出来ない
※ 3 Client-Identifier オプションは無視される

なお、クライアントとの相互動作に関して下記の留意点がある。

- 個々の機能を単独で用いるとクライアント側の思わぬ動作を招く可能性があるため、**dhcp server rfc2131 compliant** on あるいは **dhcp server rfc2131 compliant** off で使用することを推奨する。
- ルーターの再起動、スコープの再設定などでリース情報が消去されている場合、アドレス延長要求時、あるいはリース期間内のクライアントの再起動時、クライアントの使用する IP アドレスが変わることがある。
  - これを防ぐために **dhcp server rfc2131 compliant** on (あるいは remain-silent 機能) が有効である場合がある。この設定では、ヤマハルーターがリース情報を持たないクライアントからの DHCPREQUEST に DHCPNAK を返さず無視する。
  - この結果、リース期限満了時にクライアントが出す DHCPDISCOVER に Requested IP Address オプションが含まれていれば、そのクライアントには引き続き同じ IP アドレスをリースできる。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

16.1.6　DHCP アドレス割り当て動作の設定

[書式]　**dhcp scope lease type** *scope_num type* [fallback=*fallback_scope_num*]
no dhcp scope lease type *scope* [*type ...*]

[設定値]　◦ *scope_num, fallback_scope_num*.....スコープ番号 (1-65535)

◦ *type*..... 割り当ての動作
- bind-priority ..... 予約情報を優先して割り当てる
- bind-only ..... 予約情報だけに制限して割り当てる

[説明]　*scope_num* で指定した DHCP スコープにおける、アドレスの割り当て方法を制御する。

type に bind-priority を指定した場合には、**dhcp scope bind** コマンドで予約されたクライアントには予約どおりの IP アドレスを、予約されていないクライアントには他のクライアントに予約されていない空きアドレスがスコープ内にある限りそれを割り当てる。

type に bind-priority を指定した場合には、fallback オプションは指定できない。

type に bind-only を指定した場合は、fallback オプションでフォールバックスコープを指定しているかどうかによって動作が変わる。

fallback オプションの指定が無い場合、**dhcp scope bind** コマンドで予約されているクライアントにのみ IP アドレスを割り当て、予約されていないクライアントにはたとえスコープに空きがあっても IP アドレスを割り当てない。

type に bind-only を指定し、同時に fallback オプションでフォールバックスコープを指定している場合には、以下のような動作になる。

(1) クライアントが、スコープで IP アドレスを予約されている時には、予約どおりの IP アドレスを割り当てる。

(2) クライアントが、スコープでは IP アドレスが予約されていないが、フォールバックスコープでは予約されている時には、フォールバックスコープでの予約どおりの IP アドレスを割り当てる。

(3) クライアントが、スコープ、フォールバックスコープのいずれでも IP アドレスを予約されていない時には、フォールバックスコープに対する **dhcp scope lease type** コマンドの設定によって動作が変わる。

(3a) フォールバックスコープに対する **dhcp scope lease type** コマンドの設定が bind-priority になっている時には、クライアントにはフォールバックスコープに空きアドレスがある限りそれを割り当てる。

(3b) フォールバックスコープに対する **dhcp scope lease type** コマンドの設定が bind-only になっている時には、クライアントには IP アドレスは割り当てられない。

いずれの場合も、リース期間は各 DHCP スコープの定義に従う。

[初期値]　bind-priority

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

16.1.7　DHCP 割り当て情報を元にした予約設定の生成

[書式]　**dhcp convert lease to bind** *scope_n* [except] [*idx* [...]]

[設定値]
- *scope_n* .....スコープ番号 (1-65535)
- *idx*
  - 番号 **..... show status dhcp summary** コマンドで表示されるインデックス番号、最大 100 個
  - *all* .....割り当て中の情報全てを対象とする
  - 省略時は *all*

[説明]　現在の割り当て情報を元に予約設定を作成する。except キーワードを指示すると、指定した番号以外の情報が予約設定に反映される。

[ノート]　以下の変換規則で IP アドレス割り当て情報が予約設定に変換される。

IP アドレス割り当て情報のクライアント識別種別 (show status dhcp で表示される名称)	クライアント識別情報例	予約設定情報例
クライアントイーサネットアドレス	00:a0:de:01:02:03	ethernet 00:a0:de:01:02:03 ※ 1
		00:a0:de:01:02:03 ※ 2
クライアント ID	(01) 00 a0 de 01 02 03	ethernet 00:a0:de:01:02:03
	(01) 00 a0 de 01 02 03 04	01 00 a0 de 01 02 03 04
	(01) 31 32 33	00 31 32 33

※ 1：rfc2131 compliant on あるいは use-clientid ありの場合、このような IP アドレス割り当て情報の表示は ARP チェックの結果である可能性が高く、通常の割り当て時にはクライアント ID オプションが使われるため、この形式で予約設定をする。
ただし、MAC アドレスと異なるクライアント ID を使うホストが存在する場合はこの自動変換による予約は有効に機能しないため、そのようなホストに対する予約設定は別途、手動で行う必要がある。

※ 2：rfc2131 compliant off あるいは use-clientid なしの場合、chaddr フィールドを使用する

コマンド実行時点での割り当て情報を元に予約設定を作成する。サマリ表示からこの変換コマンドの実行までに時間が経過した場合には、本コマンド実行後に意図したペアの予約が作成されていることを show config で確認するべきである。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

16.1.8　DHCP オプションの設定

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

[設定値]
- *scope_num* ..... スコープ番号 (1..65535)
- *option* ..... オプション番号 (1..49,64..76,128..254) またはニーモニック
  - 主なニーモニック

router	3
dns	6
hostname	12
domain	15
wins_server	44

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

1 オクテット整数	0..255
2 オクテット整数	0..65535
2 オクテット整数の配列	2 オクテット整数をコンマ (,) で並べたもの
4 オクテット整数	0..4294967295
IP アドレス	IP アドレス
IP アドレスの配列	IP アドレスをコンマ (,) で並べたもの
文字列	文字列
スイッチ	"on", "off", "1", "0" のいずれか
バイナリ	2 桁十六進数をコンマ (,) で並べたもの

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

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

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

16.1.9　DHCP リース情報の手動追加

[書式]　**dhcp manual lease** *ip_address* [*type*] *id*
dhcp manual lease *ip_address mac_address*
dhcp manual lease *ip_address* ipcp

[設定値]
- *ip_address* ..... リースする IP アドレス
- *type* ..... Client-Identifier オプションの *type* フィールドを決定する
  - text 0x00
  - ethernet 0x01
- *id*
  - *type* が text の場合 ..... 文字列
  - *type* が ethernet の場合 ... MAC アドレス
  - *type* が省略された場合 ..... 2 桁十六進数の列で先頭は *type* フィールド
- *mac_address* ..... XX:XX:XX:XX:XX:XX (XX は十六進数) DHCP クライアントの MAC アドレス
- ipcp ..... IPCP でリモート側に与えたものとするキーワード

[説明]　手動で、特定 IP アドレスのリース情報を追加する。

[ノート]　本コマンドは自動で行われる DHCP のアドレス配布に影響を与えるため、意図して特定の IP アドレスのリース情報を追加したい場合を除いて、使用するべきではない。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

16.1.10　DHCP リース情報の手動削除

[書式]　**dhcp manual release** *ip_address*

[設定値]　◦ *ip_address*.....解放する IP アドレス

[説明]　手動で、特定 IP アドレスのリース情報を削除する。

[ノート]　本コマンドは自動で行われる DHCP のアドレス配布に影響を与えるため、意図して特定の IP アドレスのリース情報を削除したい場合を除いて、使用するべきではない。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

16.1.11　DHCP サーバーの指定の設定

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

[設定値]　◦ *host1*..*host4*.....DHCP サーバーの IP アドレス

[説明]　DHCP BOOTREQUEST パケットを中継するサーバーを最大 4 つまで設定する。
サーバーが複数指定された場合は、BOOTREQUEST パケットを複写してすべてのサーバーに中継するか、あるいは 1 つだけサーバーを選択して中継するかは **dhcp relay select** コマンドの設定で決定される。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

16.1.12　DHCP サーバーの選択方法の設定

[書式]　**dhcp relay select** *type*
no dhcp relay select [*type*]

[設定値]　◦ *type*
- *hash* .....Hash 関数を利用して一つだけサーバーを選択する
- *all* ..... すべてのサーバーを選択する

[説明]　**dhcp relay server** コマンドで設定された複数のサーバーの取り扱いを設定する。
hash が指定された場合は、Hash 関数を利用して一つだけサーバーが選択されてパケットが中継される。この Hash 関数は、DHCP メッセージの chaddr フィールドを引数とするので、同一の DHCP クライアントに対しては常に同じサーバーが選択されるはずである。*all* が指定された場合は、パケットはすべてのサーバーに対し複写中継される。

[初期値]　*hash*

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

16.1.13　DHCP BOOTREQUEST パケットの中継基準の設定

[書式]　**dhcp relay threshold** *time*
no dhcp relay threshold [*time*]

[設定値]　◦ *time*.....秒数 (0..65535)

[説明]　DHCP BOOTREQUEST パケットの secs フィールドとこのコマンドによる秒数を比較し、設定値より小さな secs フィールドを持つ DHCP BOOTREQUEST パケットはサーバーに中継しないようにする。
これにより、同一 LAN 上に別の DHCP サーバーがあるにも関わらず遠隔地の DHCP サーバーにパケットを中継してしまうのを避けることができる。

[初期値]　*0*

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

16.2　DHCP クライアント機能

16.2.1　DHCP クライアントのホスト名の設定

[書式]

dhcp client hostname *interface* **primary** *host*
dhcp client hostname *interface* **secondary** *host*
dhcp client hostname pp *peer_num host*
dhcp client hostname pool *pool_num host*
no dhcp client hostname *interface* **primary** [*host*]
no dhcp client hostname *interface* **secondary** [*host*]
no dhcp client hostname pp *peer_num* [*host*]
no dhcp client hostname pool *pool_num* [*host*]

[設定値]

◦ *interface*..... LAN インタフェース名、ブリッジインタフェース名

◦ *peer_num*
- 相手先情報番号
- anonymous

◦ *pool_num*..... **ip pp remote address pool dhcpc** コマンドで取得する IP アドレスの番号。例えば、**ip pp remote address pool dhcpc** コマンドで IP アドレスを 2 個取得できる機種で、*pool_num*に"1"または"2"を設定することで、それぞれのクライアント ID オプションに任意の ID を付けることができる。(1..**ip pp remote address pool dhcpc** コマンドで取得できる IP アドレスの最大数)

◦ *host*..... DHCP クライアントのホスト名

[説明]

DHCP クライアントのホスト名を設定する。

[ノート]

ブリッジインタフェースを指定できるのは Rev.10.00.38 以降のリビジョンである。

[初期値]

DHCP クライアントのホスト名は設定されていない

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

16.2.2　DNS サーバーアドレスを取得する LAN インタフェースの設定

[書式]

dns server dhcp *interface*
no dns server dhcp

[設定値]

◦ *interface*..... LAN インタフェース名、ブリッジインタフェース名

[説明]

DNS サーバーアドレスを取得する LAN インタフェースを設定する。このコマンドで LAN インタフェース名が設定されていると、DNS で名前解決を行うときに、指定した LAN インタフェースで DHCP サーバーから取得した DNS サーバーアドレスに対して問い合わせを行う。DHCP サーバーから DNS サーバーアドレスを取得できなかった場合は名前解決を行わない。
dns server コマンドで DNS サーバーが明示的に指定されているか、**dns server select**、**dns server pp** コマンドの設定により問い合わせをする DNS サーバーが決められた場合には、その設定が優先される。

[ノート]

この機能は指定した LAN インタフェースが DHCP クライアントとして動作していなければならない。
ブリッジインタフェースを指定できるのは Rev.10.00.38 以降のリビジョンである。

[初期値]

LAN インタフェースは設定されていない

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

16.2.3　要求する IP アドレスリース期間の設定

[書式]　**ip** *interface* **dhcp lease time** *time*
no ip *interface* **dhcp lease time** [*time*]

[設定値]
- *interface*.....LAN インタフェース名、ブリッジインタフェース名
- *time*
  - 分数 (1..21474836)
  - 時間 : 分

[説明]　DHCP クライアントが要求する IP アドレスのリース期間を設定する。

[ノート]　リース期間の要求が受け入れられなかった場合、要求しなかった場合は、DHCP サーバーからのリース期間を利用する。
ブリッジインタフェースを指定できるのは Rev.10.00.38 以降のリビジョンである。

[初期値]　リース期間を要求しない

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

16.2.4　IP アドレス取得要求の再送回数と間隔の設定

[書式]　**ip** *interface* **dhcp retry** *retry interval*
no ip *interface* **dhcp retry** [*retry interval*]

[設定値]
- *interface*.....LAN インタフェース名、ブリッジインタフェース名
- *retry*
  - 回数 (1..100)
  - infinity.....無制限
- *interval* .....秒数 (1..100)

[説明]　IP アドレスの取得に失敗したときにリトライする回数とその間隔を設定する。

[ノート]　ブリッジインタフェースを指定できるのは Rev.10.00.38 以降のリビジョンである。

[初期値]　*retry* = infinity
interval = 5

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

16.2.5　DHCP クライアント ID オプションの設定

[書式]　**dhcp client client-identifier** *interface* **primary** [type *type*] *id*
dhcp client client-identifier *interface* **secondary** [type *type*] *id*
dhcp client client-identifier pp *peer_num* [type *type*] *id*
dhcp client client-identifier pool *pool_num* [type *type*] *id*
no dhcp client client-identifier *interface* **primary**
no dhcp client client-identifier *interface* **secondary**
no dhcp client client-identifier pp *peer_num*
no dhcp client client-identifier pool *pool_num*

[設定値]
- *interface*.....LAN インタフェース名、ブリッジインタフェース名
- type.....ID オプションの type フィールドの値を設定することを示すキーワード
- *type*.....ID オプションの type フィールドの値
- *id*
  - ASCII 文字列で表した ID
  - 2 桁の十六進数列で表した ID
- *peer_num*
  - 相手先情報番号
  - anonymous
- *pool_num*..... **ip pp remote address pool dhcpc** コマンドで取得する IP アドレスの番号。例えば、**ip pp remote address pool dhcpc** コマンドで IP アドレスを 2 個取得できる機種で、*pool_num* に "1" または "2" を設定することで、それぞれのクライアント ID オプションに任意の ID を付けることができる。(1..**ip pp remote address pool dhcpc** コマンドで取得できる IP アドレスの最大数)

[説明]　DHCP クライアント ID オプションの type フィールドと ID を設定する。

[ノート]　ブリッジインタフェースを指定できるのは Rev.10.00.38 以降のリビジョンである。

[初期値]　*type* = 1

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

16.2.6　DHCP クライアントが DHCP サーバーへ送るメッセージ中に格納するオプションの設定

[書式]
dhcp client option *interface* **primary** *option=value*
dhcp client option *interface* **secondary** *option=value*
dhcp client option pp *peer_num option=value*
dhcp client option pool *pool_num option=value*
no dhcp client option *interface* **primary** [*option=value*]
no dhcp client option *interface* **secondary** [*option=value*]
no dhcp client option pp *peer_num* [*option=value*]
no dhcp client option pool *pool_num* [*option=value*]

[設定値]
- *interface*..... LAN インタフェース名、ブリッジインタフェース名
- *option*..... オプション番号 (十進数)
- *value*..... 格納するオプション値 (十六進数、"," で区切って複数指定可能)
  なおオプション長情報は入力の必要はない
- *peer_num*
  - 相手先情報番号
  - anonymous
- *pool_num*..... **ip pp remote address pool dhcpc** コマンドで取得する IP アドレスの番号。例えば、**ip pp remote address pool dhcpc** コマンドで IP アドレスを 2 個取得できる機種で、*pool_num*に"1"または"2"を設定することで、それぞれのクライアントIDオプションに任意の ID を付けることができる。(1.. **ip pp remote address pool dhcpc** コマンドで取得できる IP アドレスの最大数)

[説明]　DHCP クライアントが DHCP サーバーへ送るメッセージ中に格納するオプションを設定する。

[ノート]　このコマンドはサーバーとの相互接続に必要な場合にのみ設定する。
得られたオプション値は内部では利用されない。
Rev.7.01.34 以降、Rev.8.01.07 以降で使用可能。
ブリッジインタフェースを指定できるのは Rev.10.00.38 以降のリビジョンである。

[初期値]　設定なし

[設定例]　1. LAN2 プライマリアドレスを DHCP サーバーから得る場合に特定アドレス (192.168.0.128) を要求する。

```
# dhcp client option lan2 primary 50=c0,a8,00,80
# ip lan2 address dhcp
```

(注：ただし、この場合でも要求アドレスがサーバーから与えられるか否かはサーバー次第である。)

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

17. ICMP の設定

17.1 IPv4 の設定

17.1.1 ICMP Echo Reply を送信するか否かの設定

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

[設定値]　◦ *send*
- on ..... 送信する
- off..... 送信しない

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

[初期値]　on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

17.1.2 ICMP Echo Reply をリンクダウン時に送信するか否かの設定

[書式]　**ip icmp echo-reply send-only-linkup** *send*
no ip icmp echo-reply send-only-linkup *[send]*

[設定値]　◦ *send*
- on ..... リンクアップしている時だけ ICMP Echo Reply を返す
- off..... リンクの状態に関わらず ICMP Echo Reply を返す

[説明]　リンクダウンしているインタフェースに付与された IP アドレスを終点 IP アドレスとする ICMP Echo を受信した時に、それに対して ICMP Echo Reply を返すかどうかを設定する。on に設定した時には、リンクアップしている時だけ ICMP Echo を返すので、リンクの状態を ping で調べることができるようになる。off に設定した場合には、リンクの状態に関わらず ICMP Echo を返す。

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	RT250i	RT107e	SRT100

17.1.3 ICMP Mask Reply を送信するか否かの設定

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

[設定値]　◦ *send*
- on ..... 送信する
- off..... 送信しない

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

[初期値]　on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

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

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

[設定値]　◦ *send*
- on ..... 送信する
- off..... 送信しない

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

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

17.1.5 ICMP Redirect を送信するか否かの設定

[書式] **ip icmp redirect send** *send*
no ip icmp redirect send [*send*]

[設定値] ◦ *send*
- on..... 送信する
- off..... 送信しない

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

[初期値] on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

17.1.6 ICMP Redirect 受信時の処理の設定

[書式] **ip icmp redirect receive** *action*
no ip icmp redirect receive [*action*]

[設定値] ◦ *action*
- on..... 処理する
- off..... 無視する

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

[初期値] off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

17.1.7 ICMP Time Exceeded を送信するか否かの設定

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

[設定値] ◦ *send*
- on..... 送信する
- off..... 送信しない

[説明] 受信した IP パケットの TTL が 0 になってしまったため、そのパケットを破棄した場合に、同時にパケットの送信元に対して ICMP Time Exceeded を送信するか否かを設定する。

[初期値] on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

17.1.8 ICMP Timestamp Reply を送信するか否かの設定

[書式] **ip icmp timestamp-reply send** *send*
no ip icmp timestamp-reply send [*send*]

[設定値] ◦ *send*
- on..... 送信する
- off..... 送信しない

[説明] ICMP Timestamp を受信した場合に、ICMP Timestamp Reply を返すか否かを設定する。

[初期値] on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

17.1.9　ICMP Destination Unreachable を送信するか否かの設定

[書式]　**ip icmp unreachable send** *send*
no ip icmp unreachable send [*send*]

[設定値]　◦ *send*
- on ..... 送信する
- off..... 送信しない

[説明]　経路テーブルに宛先が見つからない場合や、あるいは ARP が解決できなくて IP パケットを破棄することになった場合に、同時にパケットの送信元に対して ICMP Destination Unreachable を送信するか否かを設定する。

[初期値]　on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

17.1.10　IPsec で復号したパケットに対して ICMP エラーを送るか否かの設定

[書式]　**ip icmp error-decrypted-ipsec send** *switch*
no ip icmp error-decrypted-ipsec send [*switch*]

[設定値]　◦ *switch*
- on ..... IPsec で復号したパケットに対して ICMP エラーを送る
- off..... IPsec で復号したパケットに対して ICMP エラーを送らない

[説明]　IPsec で復号したパケットに対して ICMP エラーを送るか否か設定する。

[ノート]　ICMP エラーには復号したパケットの先頭部分が含まれるため、ICMP エラーが送信元に返送される時にも IPsec で処理されないようになっていると、本来 IPsec で保護したい通信が保護されずにネットワークに流れてしまう可能性がある。特に、フィルタ型ルーティングでプロトコルによって IPsec で処理するかどうか切替えている場合には注意が必要となる。

ICMP エラーを送らないように設定すると、traceroute に対して反応がなくなるなどの現象になる。

このコマンドが実装される以前の動作は、ノーマルパスでは off、ファストパスでは on であった。

このコマンドは、Rev.7.01.41 以降および Rev.8.01.16 以降、Rev.8.02 系ではすべてのリビジョンで実装されている。

[初期値]　on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

17.1.11　受信した ICMP のログを記録するか否かの設定

[書式]　**ip icmp log** *log*
no ip icmp log [*log*]

[設定値]　◦ *log*
- on ..... 記録する
- off..... 記録しない

[説明]　受信した ICMP を debug タイプのログに記録するか否かを設定する。

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

17.1.12　ステルス機能の設定

[書式]　**ip stealth** *all*
ip stealth *interface* [*interface*...]
no ip stealth [...]

[設定値]　◦ all..... すべての論理インタフェースからのパケットに対してステルス動作を行う
◦ *interface*..... 指定した論理インタフェースからのパケットに対してステルス動作を行う

[説明]　このコマンドを設定すると、指定されたインタフェースから自分宛に来たパケットが原因で発生する ICMP および TCP リセットを返さないようになる。

自分がサポートしていないプロトコルや IPv6 ヘッダ、あるいはオープンしていない TCP/UDP ポートに対して指定されたインタフェースからパケットを受信した時に、通常であれば ICMP unreachable や TCP リセットを返送する。しかし、このコマンドを設定しておくとそれを禁止することができ、ポートスキャナーなどによる攻撃を受けた時にルーターの存在を隠すことができる。

[ノート]　指定されたインタフェースからの PING にも答えなくなるので注意が必要である。

自分宛ではないパケットが原因で発生する ICMP はこのコマンドでは制御できない。それらを送信しないようにするには、**ip icmp *** コマンド群を用いる必要がある。
Rev.10.00.38 以降のリビジョンでは *interface* にブリッジインタフェースを指定できる。

[初期値]　ステルス動作を行わない

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

17.1.13　ARP による MTU 探索を行うか否かの設定

[書式]　**ip** *interface* **arp mtu discovery** *sw* [minimum=*min_mtu*]
no ip *interface* **arp mtu discovery** [*sw* [minimum=*min_mtu*]]

[設定値]
- *interface* ..... LAN インタフェース名
- *sw*
  - on ..... ARP による MTU 探索を行う
  - off ..... ARP による MTU 探索を行わない
- *min_mtu* ..... 探索範囲の最低 MTU

[説明]　ARP による MTU 探索を行うか否かを設定します。

指定したインタフェースで、**lan type** コマンドおよび **ip mtu** コマンドによりジャンボフレームが利用できる状況にある時にこのコマンドが on と設定されていると、ARP 解決できた相手に対して大きなサイズの ARP を繰り返し送ることで相手の MTU を探索します。

[初期値]　on minimum=4000

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

17.1.14　切り詰められたパケットに対して、ICMP Destination Unreachable を送信するか否かの設定

[書式]　**ip icmp unreachable-for-truncated send** *send*
no ip icmp unreachable-for-truncated send [*send*]

[設定値]
- *send*
  - on ..... 送信する
  - off ..... 送信しない

[説明]　LAN インタフェースで受信したが、そのインタフェースの MTU を越える長さだったために切り詰められたパケットに対して ICMP DestinationUnreachable (TOO BIG) を送信するか否かを設定する。

[ノート]　ジャンボフレームを使用する LAN では、ホストやスイッチングハブによってジャンボフレームの最大値が異なる。そのため、LAN 上に存在するすべての機器のジャンボフレームサイズをそろえておかないと通信できなくなってしまう。

設定ミスにより、ルーターのフレームサイズより大きなパケットを送信するよう設定されたホストがあった時に、ルーターは通常、自身のインタフェースの MTU を越える長さのパケットを受信した場合には単にそれを破棄するが、このコマンドを on と設定しておくとそのようなパケットにも ICMP エラーを返すようになる。このことにより経路 MTU 探索が有効に働き、ホストが早めにフレームサイズを小さく切り詰めることが期待できる。

[初期値]　on

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

17.2　IPv6 の設定

17.2.1　ICMP Echo Reply を送信するか否かの設定

[書式]　**ipv6 icmp echo-reply send** *send*
no ipv6 icmp echo-reply send [*send*]

[設定値]　◦ *send*
- on ..... 送信する
- off..... 送信しない

[説明]　ICMP Echo Reply を送信するか否かを設定する。

[初期値]　on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

17.2.2　ICMP Echo Reply をリンクダウン時に送信するか否かの設定

[書式]　**ipv6 icmp echo-reply send-only-linkup** *send*
no ipv6 icmp echo-reply send-only-linkup [*send*]

[設定値]　◦ *send*
- on ..... リンクアップしている時だけ ICMP Echo Reply を返す
- off..... リンクの状態に関わらず ICMP Echo Reply を返す

[説明]　リンクダウンしているインタフェースに付与された IP アドレスを終点 IP アドレスとする ICMP Echo を受信した時に、それに対して ICMP Echo Reply を返すかどうかを設定する。on に設定した時には、リンクアップしている時だけ ICMP Echo を返すので、リンクの状態を ping で調べることができるようになる。off に設定した場合には、リンクの状態に関わらず ICMP Echo を返す。

[初期値]　off

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	RT250i	RT107e	SRT100

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

[書式]　**ipv6 icmp parameter-problem send** *send*
no ipv6 icmp parameter-problem send [*send*]

[設定値]　◦ *send*
- on ..... 送信する
- off..... 送信しない

[説明]　ICMP Parameter Problem を送信するか否かを設定する。

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

17.2.4　ICMP Redirect を送信するか否かの設定

[書式]　**ipv6 icmp redirect send** *send*
no ipv6 icmp redirect send [*send*]

[設定値]　◦ *send*
- on ..... 送信する
- off..... 送信しない

[説明]　ICMP Redirect を出すか否かを設定する。

[初期値]　on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

17.2.5 ICMP Redirect 受信時の処理の設定

[書式] **ipv6 icmp redirect receive** *action*
no ipv6 icmp redirect receive [*action*]

[設定値] ◦ *action*
- on..... 処理する
- off..... 無視する

[説明] ICMP Redirect を受けた場合に処理するか無視するかを設定する。

[初期値] off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

17.2.6 ICMP Time Exceeded を送信するか否かの設定

[書式] **ipv6 icmp time-exceeded send** *send*
no ipv6 icmp time-exceeded send [*send*]

[設定値] ◦ *send*
- on..... 送信する
- off..... 送信しない

[説明] ICMP Time Exceeded を出すか否かを設定する。

[初期値] on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

17.2.7 ICMP Destination Unreachable を送信するか否かの設定

[書式] **ipv6 icmp unreachable send** *send*
no ipv6 icmp unreachable send [*send*]

[設定値] ◦ *send*
- on..... 送信する
- off..... 送信しない

[説明] ICMP Destination Unreachable を出すか否かを設定する。

[初期値] on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

17.2.8 受信した ICMP のログを記録するか否かの設定

[書式] **ipv6 icmp log** *log*
no ipv6 icmp log [*log*]

[設定値] ◦ *log*
- on..... 記録する
- off..... 記録しない

[説明] 受信した ICMP を DEBUG タイプのログに記録するか否かを設定する。

[初期値] off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

17.2.9　ICMP Packet-Too-Big を送信するか否かの設定

[書式]　**ipv6 icmp packet-too-big send** *send*
no ipv6 icmp packet-too-big send [*send*]

[設定値]　◦ *send*
- on ..... 送信する
- off..... 送信しない

[説明]　ICMP Packet-Too-Big を出すか否かを設定する。

[初期値]　on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

17.2.10　IPsec で復号したパケットに対して ICMP エラーを送るか否かの設定

[書式]　**ipv6 icmp error-decrypted-ipsec send** *switch*
no ipv6 icmp error-decrypted-ipsec send [*switch*]

[設定値]　◦ *switch*
- on ..... IPsec で復号したパケットに対して ICMP エラーを送る
- off..... IPsec で復号したパケットに対して ICMP エラーを送らない

[説明]　IPsec で復号したパケットに対して ICMP エラーを送るか否か設定する。

[ノート]　ICMP エラーには復号したパケットの先頭部分が含まれるため、ICMP エラーが送信元に返送される時にも IPsec で処理されないようになっていると、本来 IPsec で保護したい通信が保護されずにネットワークに流れてしまう可能性がある。特に、フィルタ型ルーティングでプロトコルによって IPsec で処理するかどうか切替えている場合には注意が必要となる。

ICMP エラーを送らないように設定すると、traceroute に対して反応がなくなるなどの現象になる。

このコマンドが実装される以前の動作は、ノーマルパスでは off、ファストパスでは on であった。

このコマンドは、Rev.7.01.41 以降および Rev.8.01.16 以降、Rev.8.02 系ではすべてのリビジョンで実装されている。

[初期値]　on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

17.2.11　ステルス機能の設定

[書式]　**ipv6 stealth** *all*
ipv6 stealth *interface* [*interface*...]
no ipv6 stealth [...]

[設定値]　◦ *all* ..... すべての論理インタフェースからのパケットに対してステルス動作を行う
◦ *interface* ..... 指定した論理インタフェースからのパケットに対してステルス動作を行う

[説明]　このコマンドを設定すると、指定されたインタフェースから自分宛に来たパケットが原因で発生する ICMP および TCP リセットを返さないようになる。

自分がサポートしていないプロトコルや IPv6 ヘッダ、あるいはオープンしていない TCP/UDP ポートに対して指定されたインタフェースからパケットを受信した時に、通常であれば ICMP unreachable や TCP リセットを返送する。しかし、このコマンドを設定しておくとそれを禁止することができ、ポートスキャナーなどによる攻撃を受けた時にルーターの存在を隠すことができる。

[ノート]　指定されたインタフェースからの PING にも答えなくなるので注意が必要である。
自分宛ではないパケットが原因で発生する ICMP はこのコマンドでは制御できない。それらを送信しないようにするには、**ipv6 icmp** * コマンド群を用いる必要がある。

[初期値]　ステルス動作を行わない

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

17.2.12　サイズエラーで切り詰められたフレームに対して、ICMP エラー (Packet Too Big) を送信するか否かの設定

[書式]　**ipv6 icmp packet-too-big-for-truncated send** *send*
no ipv6 icmp packet-too-big-for-truncated send *[send]*

[設定値]　○ *send*
- on..... 送信する
- off..... 送信しない

[説明]　LAN インタフェースで受信したが、そのインタフェースの MTU を越える長さだったために切り詰められたフレームに対して ICMP Packet Too Big を送信するか否かを設定する。

[ノート]　ジャンボフレームを使用する LAN では、ホストやスイッチングハブによってジャンボフレームの最大値が異なる。そのため、LAN 上に存在するすべての機器のジャンボフレームサイズをそろえておかないと通信できなくなってしまう。

設定ミスにより、ルーターのフレームサイズより大きなフレームを送信するよう設定されたホストがあった時に、ルーターは通常、自身のインタフェースの MTU を越える長さのフレームを受信した場合には単にそれを破棄するが、このコマンドを on と設定しておくとそのようなフレームにも ICMP エラーを返すようになる。このことにより経路 MTU 探索が有効に働き、ホストが早めにフレームサイズを小さく切り詰めることが期待できる。

[初期値]　on

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

18. トンネリング

18.1　トンネルインタフェースの使用許可の設定

[書式]　**tunnel enable** *tunnel_num*
no tunnel enable

[設定値]　◦ *tunnel_num*
- トンネルインタフェース番号
- all ..... すべてのトンネルインタフェース

[説明]　トンネルインタフェースを使用できる状態にする。
工場出荷時は、すべてのトンネルインタフェースは disable 状態であり、使用する場合は本コマンドにより、インタフェースを有効にしなければならない。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

18.2　トンネルインタフェースの使用不許可の設定

[書式]　**tunnel disable** *tunnel_num*

[設定値]　◦ *tunnel_num*
- トンネルインタフェース番号
- all ..... すべてのトンネルインタフェース

[説明]　トンネルインタフェースを使用できない状態にする。
トンネル先の設定を行う場合は、disable 状態で行うのが望ましい。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

18.3　トンネルインタフェースの種別の設定

[書式]　**tunnel encapsulation** *type*
no tunnel encapsulation

[設定値]　◦ *type*
- ipsec .....IPsec トンネル
- ipip.....IPv6 over IPv4 トンネル、IPv4 over IPv6 トンネル、IPv4 over IPv4 トンネルまたは IPv6 over IPv6 トンネル
- pptp.....PPTP トンネル

[説明]　トンネルインタフェースの種別を設定する。

[ノート]　トンネリングと NAT を併用する場合には **tunnel endpoint address** コマンドにより始点 IP アドレスを設定することが望ましい。
PPTP 機能を実装していないモデルでは、pptp キーワードは使用できない。

[初期値]　ipsec

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

18.4　トンネルインタフェースの IPv4 アドレスの設定

[書式]　**ip tunnel address** *ip_address* [*/mask*]
no ip tunnel address [*ip_address*[*/mask*]]

[設定値]　◦ *ip_address*.....IPv4 アドレス

◦ *mask*
- xxx.xxx.xxx.xxx（xxx は十進数）
- 0x に続く十六進数
- マスクビット数

[説明]　トンネルインタフェースの IPv4 アドレスとネットマスクを設定する。
このコマンドの設定によりトンネルインタフェースを経由して BGP のコネクションを確立できるようになる。

[ノート]　Rev.8.01.12 以降で使用可能。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

18.5 トンネルインタフェースの相手側の IPv4 アドレスの設定

[書式] **ip tunnel remote address** *ip_address*
no ip tunnel remote address [*ip_address*]

[設定値] ◦ *ip_address* ..... IPv4 アドレス

[説明] トンネルインタフェースの相手側の IPv4 アドレスを設定する。
このコマンドの設定によりトンネルインタフェースを経由して BGP のコネクションを確立できるようになる。

[ノート] Rev.8.01.12 以降で使用可能。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

18.6 トンネルインタフェースの端点 IP アドレスの設定

[書式] **tunnel endpoint address** [*local*] *remote*
no tunnel endpoint address [[*local*] *remote*]

[設定値] ◦ *local*..... 自分側のトンネルインタフェース端点の IP アドレス
◦ *remote*..... 相手側のトンネルインタフェース端点の IP アドレス

[説明] トンネルインタフェース端点の IP アドレスを設定する。IP アドレスは IPv4/IPv6 いずれのアドレスも設定できるが、LOCAL と REMOTE では IPv4/IPv6 の種別が揃っていなくてはいけない。トンネルインタフェース端点として IPv4 アドレスを設定した場合には、IPv4 over IPv4 トンネルと IPv6 over IPv4 トンネルが、IPv6 アドレスを設定した場合には IPv4 over IPv6 トンネルと IPv6 over IPv6 トンネルが利用できる。

local を省略した場合は、適当なインタフェースの IP アドレスが利用される。

[ノート] このコマンドにより設定した IP アドレスが利用されるのは、**tunnel encapsulation** コマンドの設定値が pptp と ipip の場合だけである。IPsec トンネルでは、トンネル端点は **ipsec ike local address** および **ipsec ike remote address** コマンドにより設定される。
PPTP サーバーの Anonymous で受ける場合には設定する必要はない。

[初期値] IP アドレスは設定されていない

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19. IPsec の設定

RT250i 以外の機種では、暗号化により IP 通信に対するセキュリティを保証する IPsec 機能を実装しています。IPsec では、鍵交換プロトコル IKE (Internet Key Exchange) を使用します。必要な鍵は IKE により自動的に生成されますが、鍵の種となる事前共有鍵は **ipsec ike pre-shared-key** コマンドで事前に登録しておく必要があります。この鍵はセキュリティ・ゲートウェイごとに設定できます。また、鍵交換の要求に応じるかどうかは、**ipsec ike remote address** コマンドで設定します。

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

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

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

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

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

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

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

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

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

リビジョン系列	IPsec リリース 1	IPsec リリース 2	IPsec リリース 3
3.00	3.00.09 ～3.00.11	—	—
3.01	3.01.07	3.01.11 ～	
4.02	—	4.00.02 ～4.00.14	4.02.04 ～
6.00 以降	—	—	6.00.01 ～

セキュリティ・ゲートウェイの識別子とトンネルインタフェース番号はモデルにより異なり、以下の表のようになります。

モデル	セキュリティ・ゲートウェイの識別子	トンネルインタフェース番号
RTX3000	1 - 1000	1 - 1000
RTX2000 + YBB-VPN-A RTX2000 + YBB-VPN-B	1 - 500	1 - 500
RTX1500	1 - 100	1 - 100
RTX1100	1 - 30	1 - 30
RTX1000	1 - 30	1 - 30
RT300i + YBA-VPN	1 - 500	1 - 500
RT300i	1 - 100	1 - 100
RT250i	IPsec 非搭載	IPsec 非搭載
RT107e	1 - 6	1 - 6
SRT100	1 - 10	1 - 10
RTX1200	1 - 100	1 - 100

本機は**メインモード** (main mode) と**アグレッシブモード** (aggressive mode) に対応しています。VPN を構成する両方のルーターが固定のグローバルアドレスを持つときにはメインモードを使用し、一方のルーターしか固定のグローバルアドレスを持たないときにはアグレッシブモードを使用します。

メインモードを使用するためには、**ipsec ike remote address** コマンドで対向のルーターの IP アドレスを設定する必要があります。アグレッシブモードを使用するときには、固定のグローバルアドレスを持つかどうかによって設定が異なります。固定のグローバルアドレスを持つルーターには、**ipsec ike remote name** コマンドを設定し、**ipsec ike remote address** コマンドで any を設定します。固定のグローバルアドレスを持たないルーターでは、**ipsec ike local name** コマンドを設定し、**ipsec ike remote address** コマンドで IP アドレスを設定します。

メインモードでは、**ipsec ike local name** コマンドや **ipsec ike remote name** コマンドを設定することはできません。また、アグレッシブモードでは、**ipsec ike local name** コマンドと **ipsec ike remote name** コマンドの両方を同時に設定することはできません。このように設定した場合には、正しく動作しない可能性があります。

19.1　IPsec の動作の設定

[書式]　**ipsec use** *use*
no ipsec use [*use*]

[設定値]　◦ *use*
- on..... 動作させる
- off..... 動作させない

[説明]　IPsec を動作させるか否かを設定する。

[初期値]　on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.2　事前共有鍵の登録

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

[設定値]　◦ *gateway_id* ..... セキュリティ・ゲートウェイの識別子
◦ *key*..... 鍵となる 0x ではじまる十六進数列 (32 バイト以内)
◦ *text* ..... ASCII 文字列で表した鍵 (32 文字以内)

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

[初期値]　事前共有鍵は設定されていない

[設定例]
```
ipsec ike pre-shared-key 1 text himitsu
ipsec ike pre-shared-key 8 0xCDEEEDC0CDEDCD
```

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.3　IKE の鍵交換を始動するか否かの設定

[書式]　**ipsec auto refresh** [*gateway_id*] *switch*
no ipsec auto refresh [*gateway_id*]

[設定値]　◦ *gateway_id* ..... セキュリティ・ゲートウェイの識別番号
◦ *switch*
- on..... 鍵交換を始動する
- off..... 鍵交換を始動しない

[説明]　IKE の鍵交換を始動するかどうかを設定する。他のルーターが始動する鍵交換については、このコマンドに関係なく常に受け付ける。

gateway_id パラメータを指定しない書式は、ルーターの全体的な動作を決める。この設定が off のときにはルーターは鍵交換を始動しない。

gateway_id パラメータを指定する書式は、指定したセキュリティゲートウェイに対する鍵交換の始動を抑制するために用意されている。
例えば、次の設定では、1 番のセキュリティゲートウェイのみが鍵交換を始動しない。

```
ipsec auto refresh on
ipsec auto refresh 1 off
```

[ノート]　ipsec auto refresh off の設定では、*gateway_id* パラメータを指定する書式は効力を持たない。例えば、次の設定では、1 番のセキュリティゲートウェイでは鍵交換を始動しない。

```
ipsec auto refresh off ( デフォルトの設定 )
ipsec auto refresh 1 on
```

なお、*gateway_id* パラメータの指定ができるのは、Rev.7.01.15 以降のファームウェアに限られる。

[初期値]　ipsec auto refresh off
ipsec auto refresh *gateway_id* on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.4　設定が異なる場合に鍵交換を拒否するか否かの設定

[書式]　**ipsec ike negotiate-strictly** *gateway_id switch*
no ipsec ike negotiate-strictly *gateway_id*

[設定値]
- *gateway_id*..... セキュリティ・ゲートウェイの識別子
- *switch*
  - on..... 鍵交換を拒否する
  - off..... 鍵交換を受理する

[説明]　設定が異なる場合に鍵交換を拒否するか否かを設定する。
このコマンドの設定が off のときには、従来のファームウェアと同様に動作する。すなわち、相手の提案するパラメータが自分の設定と異なる場合でも、そのパラメータをサポートしていれば、それを受理する。このコマンドの設定が on のときには、同様の状況で相手の提案を拒否する。このコマンドが適用されるパラメータと対応するコマンドは以下の通りである。

パラメータ	対応するコマンド
暗号アルゴリズム	**ipsec ike encryption**
グループ	**ipsec ike group**
ハッシュアルゴリズム	**ipsec ike hash**
PFS	**ipsec ike pfs**
フェーズ 1 のモード	**ipsec ike local name** など

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.5　IKE の鍵交換に失敗したときに鍵交換を休止せずに継続するか否かの設定

[書式]　**ipsec ike always-on** *gateway_id switch*
no ipsec ike always-on

[設定値]
- *gateway_id*..... セキュリティ・ゲートウェイの識別子
- *switch*
  - on..... 鍵交換を継続する
  - off..... 鍵交換を休止する

[説明]　IKE の鍵交換に失敗したときに鍵交換を休止せずに継続できるようにする。IKE キープアライブを用いるときには、このコマンドを設定しなくても、常に鍵交換を継続する。

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.6　鍵交換の再送回数と間隔の設定

[書式]　**ipsec ike retry** *count interval* [*max_session*]
no ipsec ike retry [*count interval* [*max_session*]]

[設定値]
- *count*..... 再送回数 (1..50)
- *interval*..... 再送間隔の秒数 (1..100)
- *max_session*..... 同時に動作するフェーズ 1 の最大数 (1..5)

[説明]　鍵交換のパケットが相手に届かないときに実施する再送の回数と間隔を設定する。
また、オプションのパラメータとして、同時に動作するフェーズ 1 の最大数を指定できる。ルーターは、フェーズ 1 が確立せずに再送を継続する状態にあるとき、鍵の生成を急ぐ目的で、新しいフェーズ 1 を始動することがある。このパラメータは、このような状況で、同時に動作するフェーズ 1 の数を制限するものである。なお、このパラメータは、始動側のフェーズ 1 のみを制限するものであり、応答側のフェーズ 1 に対しては効力を持たない。

[ノート]　*max_session* パラメータは Rev.7.01.47 以降で使用可能。

[初期値]　*count* = 10
interval = 5
max_session = 3

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.7　相手側のセキュリティ・ゲートウェイの名前の設定

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

[設定値]
- *gateway*..... セキュリティ・ゲートウェイの識別子
- *name*..... 名前 (32 文字以内)

[説明]　相手側のセキュリティ・ゲートウェイの名前を設定する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.8　相手側セキュリティ・ゲートウェイの IP アドレスの設定

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

[設定値]
- *gateway_id*..... セキュリティ・ゲートウェイの識別子
- *ip_address*
  - 相手側セキュリティ・ゲートウェイの IP アドレス、またはホスト名
  - any..... 自動選択

[説明]　相手側セキュリティ・ゲートウェイの IP アドレスまたはホスト名を設定する。ホスト名で設定した場合には、鍵交換の始動時にホスト名から IP アドレスを DNS により検索する。そのため、**dns server** コマンドなどで必ず DNS サーバーが設定されていなくてはいけない。

any が設定された場合には、相手側セキュリティ・ゲートウェイとして任意のホストからのアクセスを受け付ける。その代わりに、自分から鍵交換を始動することはできない。any はアグレッシブモードで固定のグローバルアドレスを持つ側の場合に利用する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.9　相手側の ID の設定

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

[設定値]
- *gateway_id*.....セキュリティ・ゲートウェイの識別子
- *ip_address*..... IP アドレス
- *mask*.....ネットマスク

[説明]　IKE のフェーズ 2 で用いる相手側の ID を設定する。

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

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.10　自分側のセキュリティ・ゲートウェイの名前の設定

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

[設定値]
- *gateway_id*.....セキュリティ・ゲートウェイの識別子
- *name*.....名前 (32 文字以内)
- *type*.....id の種類
  - fqdn.....ID_FQDN
  - use-fqdn.....ID_USER_FQDN
  - key-id.....ID_KEY_ID

[説明]　自分側のセキュリティゲートウェイの名前と ID の種類を設定する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.11　自分側セキュリティ・ゲートウェイの IP アドレスの設定

[書式]　**ipsec ike local address** *gateway_id ip_address*
ipsec ike local address *gateway_id* vrrp *interface vrid*
ipsec ike local address *gateway_id* ipv6 prefix *prefix on interface*
ipsec ike local address *gateway_id* ipcp pp *pp_num*
no ipsec ike local address *gateway_id* [*ip_address*]

[設定値]
- *gateway_id*.....セキュリティ・ゲートウェイの識別子
- *ip_address*.....自分側セキュリティ･ゲートウェイの IP アドレス
- *interface*.....LAN インタフェース名
- *vrid*.....VRRP グループ ID (1..255)
- *pp_num*.....PP インタフェース番号

[説明]　自分側セキュリティ・ゲートウェイの IP アドレスを設定する。

vrrp キーワードを指定する第 2 書式では、VRRP マスターとして動作している場合のみ、指定した LAN インタフェース /VRRP グループ ID の仮想 IP アドレスを自分側セキュリティ・ゲートウェイアドレスとして利用する。VRRP マスターでない場合には鍵交換は行わない。

ipv6 キーワードを指定する第 3 書式では、IPv6 のダイナミックアドレスを指定する。

ipcp キーワードを指定する第 4 書式では、IPCP アドレスを取得する PP インタフェースを指定する。これは Rev.8.03 系以降で使用可能である。

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

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.12　自分側の ID の設定

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

[設定値]
- *gateway_id* ..... セキュリティ・ゲートウェイの識別子
- *ip_address* ..... IP アドレス
- *mask*..... ネットマスク

[説明]　IKE のフェーズ 2 で用いる自分側の ID を設定する。

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

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.13　IKE キープアライブ機能の設定

[書式]　**ipsec ike keepalive use** *gateway_id switch*
ipsec ike keepalive use *gateway_id switch* heartbeat [*interval count* [*upwait*]]
ipsec ike keepalive use *gateway_id switch* icmp-echo *ip_address* [length=*length*] [*interval count* [*upwait*]]
ipsec ike keepalive use *gateway_id switch* dpd [*interval count* [*upwait*]]
no ipsec ike keepalive use *gateway_id* [*switch ....]*

[設定値]
- *gateway_id* ..... セキュリティ・ゲートウェイの識別子
- *switch* ..... キープアライブの動作
  - on..... キープアライブを使用する
  - off..... キープアライブを使用しない
  - auto .....対向のルーターがキープアライブを送信するときに限って送信する (heartbeat でのみ有効)
- *ip_address* ..... ping を送信する宛先の IP アドレス (IPv4/IPv6)
- *length* ..... TYPE で icmp-echo を設定したときのデータ部の長さ (64..1500)
- *interval*..... キープアライブパケットの送信間隔秒数 (1..600)
- *count*..... キープアライブパケットが届かないときに障害とみなすまでの試行回数 (1..50)
- *upwait* ..... IPsec SA が生成されてから実際にトンネルインタフェースを有効にするまでの時間 (0..1000000)

[説明]　IKE キープアライブの動作を設定する。このコマンドの設定は、双方のルーターで一致させる必要がある。
キープアライブの方式としては、heartbeat、ICMP Echo、DPD(RFC3706) の 3 種類から選ぶことができる。
キープアライブの方式として、heartbeat を利用するときには、1 行目か 2 行目の書式を使う。heartbeat に限っては、*switch* パラメータとして auto を設定できる。
auto を設定したときには、相手から heartbeat パケットを受信したときにのみ、heartbeat パケットを送信する。なお、双方の設定が auto になっているときには、IKE キープアライブは動作しない。
キープアライブの方式として、ICMP Echo を利用するときには、3 行目の書式を使い、送信先の IP アドレスを設定する。オプションとして、ICMP Echo のデータ部の長さを指定できる。
キープアライブの方式として、DPD を利用するときには、4 行目の書式を使う。

[ノート]　*length* パラメータで指定するのは ICMP データ部分の長さであり、IP パケット全体の長さではない。*length* パラメータは、Rev.7.01 系以降で指定可能である。
同じ相手に対して、複数の方法を併用することはできない。
DPD を利用できるのは Rev.8.03 以降のファームウェアである。

[初期値]　*switch* = auto
length = 64
interval = 10
count = 6
upwait = 0

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.14　IKE キープアライブに関する SYSLOG を出力するか否かの設定

[書式]　**ipsec ike keepalive log** *gateway_id log*
no ipsec ike keepalive log *gateway_id* [*log*]

[設定値]　◦ *gateway_id*.....セキュリティ・ゲートウェイの識別子
◦ *log*
• on.....出力する
• off.....出力しない

[説明]　IKE キープアライブに関する SYSLOG を出力するか否かを設定する。この SYSLOG は DEBUG レベルの出力である。

[初期値]　on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.15　IKE が用いる暗号アルゴリズムの設定

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

[設定値]　◦ *gateway_id*.....セキュリティ・ゲートウェイの識別子
◦ *algorithm*
• 3des-cbc.....3DES-CBC
• des-cbc .....DES-CBC
• aes-cbc.....AES-CBC

[説明]　IKE が用いる暗号アルゴリズムを設定する。

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

[初期値]　3des-cbc (RTX3000、SRT100、RTX1200)
des-cbc (上記以外の機種)

[設定例]　# ipsec ike encryption 1 aes-cbc

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.16　受信した IKE パケットを蓄積するキューの長さの設定

[書式]　**ipsec ike queue length** *length*
no ipsec ike queue length [*length*]

[設定値]　◦ *length*.....キュー長
1000...2000 (RTX3000)
100....200 (RTX1200)
10...20 (SRT100)
8...64 (上記以外の機種)

[説明]　受信した IKE パケットを蓄積するキューの長さを設定する。
この設定は、短時間に集中して IKE パケットを受信した際のルーターの振る舞いを決定する。設定した値が大きいほど、IKE パケットが集中したときにより多くのパケットを取りこぼさないで処理することができるが、逆に IKE パケットがルーターに滞留する時間が長くなるためキープアライブの応答が遅れ、トンネルの障害を間違って検出する可能性が増える。
通常の運用では、この設定を変更する必要はないが、多数のトンネルを構成しており、多数の SA を同時に消す状況があるならば値を大きめに設定するとよい。

[ノート]　Rev.7.01.15 以前のファームウェアでは、このキューの長さは 8 で固定されていた。

キューの長さを長くすると、一度に受信して処理できる IKE パケットの数を増やすことができる。しかし、あまり大きくすると、ルーター内部にたまった IKE パケットの処理が遅れ、対向のルーターでタイムアウトと検知されてしまう可能性が増える。そのため、このコマンドの設定を変更する時には、慎重に行う必要がある。

通常の運用では、この設定を変更する必要はない。

[初期値]　2000 (RTX3000)
200 (RTX1200)
20 (SRT100)
8 (上記以外の機種)

[適用モデル]	RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

19.17　IKE が用いるグループの設定

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

[設定値]
◦ *gateway_id* ..... セキュリティ・ゲートウェイの識別子
◦ *group*..... グループ識別子
- modp768
- modp1024
- modp1536
- modp2048

[説明]　IKE で用いるグループを設定する。

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

[初期値]　modp1024 (RTX3000、SRT100、RTX1200)
modp768 (上記以外の機種)

[適用モデル]	RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.18　IKE が用いるハッシュアルゴリズムの設定

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

[設定値]
◦ *gateway_id* ..... セキュリティ・ゲートウェイの識別子
◦ *algorithm*
- md5 ..... MD5
- sha SHA-1

[説明]　IKE が用いるハッシュアルゴリズムを設定する。

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

[初期値]　sha (RTX3000、SRT100、RTX1200)
md5 (上記以外の機種)

[適用モデル]	RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.19　受信したパケットの SPI 値が無効な値の場合にログに出力するか否かの設定

[書式]　**ipsec log illegal-spi** *switch*
no ipsec log illegal-spi

[設定値]
◦ *switch*
- on..... ログに出力する
- off..... ログに出力しない

[説明]　IPsec で、受信したパケットの SPI 値が無効な値の場合に、その旨をログに出力するか否かを設定する。SPI 値と相手の IP アドレスがログに出力される。
無効な SPI 値を含むパケットを大量に送り付けられることによる DoS の可能性を減らすため、ログは 1 秒あたり最大 10 種類のパケットだけを記録する。実際に受信したパケットの数を知ることはできない。

[ノート]　鍵交換時には、鍵の生成速度の差により一方が新しい鍵を使い始めても他方ではまだその鍵が使用できない状態になっているためにこのログが一時的に出力されてしまうことがある。

[初期値]　off

[適用モデル]	RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.20　IKE ペイロードのタイプの設定

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

[設定値]
- *gateway_id*.....セキュリティ・ゲートウェイの識別子
- *type*.....メッセージのフォーマット
  - 1.....ヤマハルーターのリリース 2 との互換性を保持する
  - 2.....ヤマハルーターのリリース 3 に合わせる
  - 3.....初期ベクトル (IV) の生成方法を一部の実装に合わせる

[説明]　IKE ペイロードのタイプを設定する。ヤマハルーターの古いリビジョンと接続する場合には、タイプを 1 に設定する必要がある。

[ノート]　Rev.7.01.08 以降でタイプ 3 が指定可能。

[初期値]　2

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.21　IKE の情報ペイロードを送信するか否かの設定

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

[設定値]
- *gateway_id*.....セキュリティ・ゲートウェイの識別子
- *info*
  - on.....送信する
  - off.....送信しない

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

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

[初期値]　on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.22　PFS を用いるか否かの設定

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

[設定値]
- *gateway_id*.....セキュリティ・ゲートウェイの識別子
- *pfs*
  - on.....用いる
  - off.....用いない

[説明]　IKE で PFS(Perfect Forward Secrecy) を用いるか否かを設定する。

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

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.23　XAUTH の設定

[書式]　**ipsec ike xauth myname** *gateway_id name password*
no ipsec ike xauth myname *gateway_id*

[設定値]
- *gateway_id*.....セキュリティ・ゲートウェイの識別子
- *name*.....XAUTH で通知する名前 (32 文字以内)
- *password*.....XAUTH で通知するパスワード (32 文字以内)

[説明]　XAUTH の認証を要求されたときに通知する名前とパスワードを設定する。

[初期値]　なし

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

19.24　XAUTH 認証に使用するユーザ ID の設定

[書式]　**auth user** *userid username password*
no auth user *userid* [*username ...*]

[設定値]　◦ *userid*..... ユーザ識別番号 (1..500)
◦ *username*..... ユーザ名 (32 文字以内) (* 3 文字以上に設定してください。)
◦ *password*..... パスワード (32 文字以内) (*　同上　)

[説明]　IPsec の XAUTH 認証に使用するユーザ ID を設定する。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

19.25　XAUTH 認証に使用するユーザ ID の属性の設定

[書式]　**auth user attribute** *userid attribute=value* [*attribute=value ...*]
no auth user attribute *userid* [*attribute=value ...*]

[設定値]　◦ *userid*..... ユーザ識別番号 (1..500)
◦ *attribute=value*..... ユーザ属性

[説明]　IPsec の XAUTH 認証に使用するユーザ ID の属性を設定する。
設定できる属性は以下のとおり。

attribute	*value*	説明
xauth	on	IPsec の XAUTH 認証にこの ID を使用する
	off	IPsec の XAUTH 認証にこの ID を使用しない
xauth-address	IP address[/netmask] (IPv6 アドレス可)	IPsec の接続時に、このアドレスを内部 IP アドレスとして通知する
xauth-dns	IP address (IPv6 アドレス可)	IPsec の接続時に、このアドレスを DNS サーバーアドレスとして通知する
xauth-wins	IP address (IPv6 アドレス可)	IPsec の接続時に、このアドレスを WINS サーバーアドレスとして通知する
xauth-filter	フィルタセットの名前を表す文字列	IPsec の接続時に、このフィルタを適用する

[ノート]　本コマンドにて明示的に設定した属性値は、
該当のユーザ ID が属しているユーザグループに対して、
　# auth user group attribute
コマンドによって設定された属性値に優先して適用される。

[初期値]　xauth　: off
xauth-address　: 設定なし
xauth-dns　: 設定なし
xauth-wins　: 設定なし
xauth-filter　: 設定なし

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

19.26　XAUTH 認証に使用するユーザグループの設定

[書式]　**auth user group** *groupid userid* [*userid ...*]
no auth user group *groupid*

[設定値]　◦ *groupid*..... ユーザグループ識別番号 (1..500)
◦ *userid*..... ユーザ識別番号もしくはユーザ識別番号の範囲
(複数指定することが可能)

[説明]　IPsec の XAUTH 認証に使用するユーザグループを設定する。

[設定例]　*# auth user group 1 100 101 102*
 # auth user group 1 200-300
 # auth user group 1 100 103 105 107-110 113

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

19.27　XAUTH 認証に使用するユーザグループの属性の設定

[書式]　**auth user group attribute** *groupid attribut*E=*value* [*attribute*=*value* ...]
no auth user group attribute *groupid* [*attribute*=*value* ...]

[設定値]
- *groupid*.....ユーザグループ識別番号 (1..500)
- *attribute*=*value*.....ユーザグループ属性

[説明]　IPsec の XAUTH 認証に使用するユーザグループの属性を設定する。
設定できる属性は以下のとおり。

attribute	*value*	説明
xauth	on	IPsec の XAUTH 認証にこのグループに含まれるユーザ ID を使用する
	off	IPsec の XAUTH 認証にこのグループに含まれるユーザ ID を使用しない
xauth-address-pool	IP アドレスの範囲 (IPv6 アドレス可)	IPsec の接続時に、このアドレスプールからアドレスを選択し、内部 IP アドレスとして通知する
xauth-dns	IP address (IPv6 アドレス可)	IPsec の接続時に、このアドレスを DNS サーバーアドレスとして通知する
xauth-wins	IP address (IPv6 アドレス可)	IPsec の接続時に、このアドレスを WINS サーバーアドレスとして通知する
xauth-filter	フィルタセットの名前を表す文字列	IPsec の接続時に、このフィルタを適用する

xauth-address-pool の属性値である IP アドレスの範囲は、以下のいずれかの書式にて記述する。
- IP address[/netmask]
- IP address-IP address[/netmask]

[ノート]　本コマンドで設定した属性値は、該当のユーザグループに含まれるすべてのユーザに対して有効となる。

[初期値]
xauth　: off
xauth-address-pool　: 設定なし
xauth-dns　: 設定なし
xauth-wins　: 設定なし
xauth-filter　: 設定なし

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

19.28　XAUTH によるユーザ認証の設定

[書式]　**ipsec ike xauth request** *gateway_id auth* [*group_id*]
no ipsec ike xauth request *gateway_id* [*auth* ...]

[設定値]
- *gateway_id*.....セキュリティゲートウェイの識別子
- *group_id*.....認証に使用するユーザグループの識別番号
- *auth*
  - on.....要求する
  - off.....要求しない

[説明]　IPsec の認証を行なう際、Phase1 終了後に XAUTH によるユーザ認証をクライアントに要求するか否かを設定する。
group_id を指定した場合には、該当のユーザグループに含まれるユーザを認証の対象とする。
group_id の指定がない場合や、指定したユーザグループに含まれるユーザ情報では認証できなかった場合、RADIUS サーバーの設定があれば RADIUS サーバーを用いた認証を追加で試みる。

本コマンドによる設定はルーターが受動側として動作する時にのみ有効であり、始動側のセキュリティゲートウェイから送信された isakmp SA パラメータの提案に、認証方式として XAUTHInitPreShared(65001) が含まれていた場合に、この提案を受け入れ、XAUTH によるユーザ認証を行なう。

[初期値]　off

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

19.29　内部 IP アドレスプールの設定

[書式]　**ipsec ike mode-cfg address pool** *pool_id ip_address*[*/mask*]
ipsec ike mode-cfg address pool *pool_id ip_address-ip_address*[*/mask*]
no ipsec ike mode-cfg address pool *pool_id* [*ip_address ...*]

[設定値]
- *pool_id* .....アドレスプール ID(1..65535)
- *ip_address* .....IP アドレス (IPv6 アドレス可)
- *ip_address-ip_address*.....IP アドレスの範囲 (IPv6 アドレス可)
- *mask*.....ネットマスク (IPv6 アドレスの時はプレフィックス長)

[説明]　IPsec クライアントに割り当てる内部 IP アドレスのアドレスプールを設定する。
本コマンドにて設定したアドレスプールは、
　# **ipsec ike mode-cfg address** *gateway_id ...*
コマンドにて用いられる。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

19.30　IPsec クライアントに割り当てる内部 IP アドレスプールの設定

[書式]　**ipsec ike mode-cfg address** *gateway_id pool_id*
no ipsec ike mode-cfg address *gateway_id* [*pool_id*]

[設定値]
- *gateway_id* ..... セキュリティゲートウェイの識別子
- *pool_id* ..... アドレスプール ID

[説明]　IPsec クライアントに内部 IP アドレスを割り当てる際に参照する、内部 IP アドレスプールを設定する。
内部 IP アドレスの IPsec クライアントへの通知は、XAUTH 認証に使用する Config-Mode にて行なわれるため、XAUTH 認証を行なわない場合には通知は行なわれない。

以下のいずれかの方法にて、認証ユーザ毎に割り当てる内部 IP アドレスが設定されている場合には、アドレスプールからではなく、個別に設定されているアドレスを通知する。
- RADIUS サーバーに登録されている場合
- 以下のコマンドを用いて設定されている場合
　# **auth user attribute** *userid* xauth-address=*address*[*/mask*]
　# **auth user group attribute** *groupid* xauth-address-pool=*address-address*[*/mask*]

アドレスプールに登録されているアドレスが枯渇した場合には、アドレスの割当を行なわない。

[ノート]　VPN クライアントとして YMS-VPN1 を用いる場合、XAUTH 認証を行なうためには必ず内部 IP アドレスの通知を行なう設定にしなければならない。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

19.31　IKE のログの種類の設定

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

[設定値]
- *gateway_id* ..... セキュリティ・ゲートウェイの識別子
- *type*
  - message-info ..... IKE メッセージの内容
  - payload-info..... ペイロードの処理内容
  - key-info ..... 鍵計算の処理内容

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

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

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.32　ESP を UDP でカプセル化して送受信するか否かの設定

[書式]　**ipsec ike esp-encapsulation** *gateway_id encap*
no ipsec ike esp-encapsulation *gateway_id*

[設定値]
- *gateway_id*.....セキュリティ・ゲートウェイの識別子
- *encap*
  - on.....ESP を UDP でカプセル化して送信する
  - off.....ESP を UDP でカプセル化しないで送信する

[説明]　NAT などの影響で ESP が通過できない環境で IPsec の通信を確立するために、ESP を UDP でカプセル化して送受信できるようにする。このコマンドの設定は双方のルーターで一致させる必要がある。

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.33　SA 関連の設定

再起動されるとすべての SA がクリアされることに注意しなくてはいけない。

19.33.1　SA の寿命の設定

[書式]　**ipsec ike duration** *sa gateway_id second* [*kbytes*] [rekey *rekey*]
no ipsec ike duration *sa gateway_id* [*second* [*kbytes*] [rekey *rekey*]]

[設定値]
- *sa*
  - ipsec-sa.....IPsec SA
  - isakmp-sa.....ISAKMP SA
- *gateway_id*.....セキュリティ・ゲートウェイの識別子
- *second*.....秒数 (300..691200)
- *kbytes*.....キロ単位のバイト数 (100..100000)
- *rekey*.....SA を更新するタイミング
  - パーセント (70% - 90%)
  - off.....更新しない
    (*sa* パラメータで isakmp-sa を指定したときのみ設定可能)

[説明]　IKE で提案する IPsec SA または ISAKMP SA の寿命を設定する。
kbytes パラメータを指定した場合には、 *second* パラメータで指定した時間が経過するか、指定したバイト数のデータを処理した後に SA は消滅する。*kbytes* パラメータは *sa* パラメータとして ipsec-sa を指定したときのみ有効である。

rekey パラメータは SA を更新するタイミングを決定する。例えば、 *second* パラメータで 20000 を指定し、*rekey* パラメータで 75% を指定したときには、SA を生成してから 15000 秒経過したときに新しい SA を生成する。*rekey* パラメータは *second* パラメータに対する比率を表すもので、*kbytes* パラメータの値とは関係がない。

sa パラメータで isakmp-sa を指定したときに限り、*rekey* パラメータで off を設定できる。
この場合には、IPsec SA を作る必要がない限り、ISAKMP SA の更新を保留するので、ISAKMP SA の生成を最小限に抑えることができる。ただし、この効果を得るためには次の 2 点に注意して設定する必要がある。

1.IPsec SA よりも ISAKMP SA の寿命を短く設定する。
2. ダングリング SA を許可する。すなわち、**ipsec ike restrict-dangling-sa** コマンドの設定を off にする。

なお、このコマンドを設定しても、すでに存在する SA の寿命値は変化せず、新しく作られる SA にのみ、新しい寿命値が適用される。

[初期値]　*second* : 28800 秒
rekey : 75%

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.33.2　SA のポリシーの定義

[書式]　**ipsec sa policy** *policy_id gateway_id* ah *ah_algorithm* [local-id=*local-id*] [remote-id=r*emote-id*] [anti-replay-check=*check*]
ipsec sa policy *policy_id gateway_id* esp *esp_algorithm* [*ah_algorithm*] [anti-replay-check=*check*]
no ipsec sa policy *policy_id* [*gateway_id*]

[設定値]
- *policy_id*..... ポリシー ID (1..2147483647)
- *gateway_id* ..... セキュリティ・ゲートウェイの識別子
- ah ..... 認証ヘッダ (Authentication Header) を示すキーワード
- esp..... 暗号ペイロード (Encapsulating Security Payload) を示すキーワード
- *ah_algorithm*
  - md5-hmac..... HMAC-MD5
  - sha-hmac..... HMAC-SHA
- *esp_algorithm*
  - 3des-cbc 3DES-CBC
  - des-cbc..... DES-CBC
  - aes-cbc ..... AES-CBC
- *local-id* ..... 自分側のプライベートネットワーク
- *remote-id* ..... 相手側のプライベートネットワーク
- *check*
  - on..... シーケンス番号のチェックを行う
  - off..... シーケンス番号のチェックを行わない

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

check=on の場合、受信パケット毎にシーケンス番号の重複や番号順のチェックを行い、エラーとなるパケットは破棄する。破棄する際には debug レベルで
[IPSEC] sequence difference
[IPSEC] sequence number is wrong
といったログが記録される。
相手側が、トンネルインタフェースでの優先 / 帯域制御を行っている場合、シーケンス番号の順序が入れ替わってパケットを受信することがある。その場合、実際にはエラーではないのに上のログが表示され、パケットが破棄されることがあるので、そのような場合には設定を off にするとよい。

[ノート]　*local-id* と *remote-id* は Rev.6.03.18 以降、Rev.7.00.14 以降で使用可能。
双方で設定する *local-id* と *remote-id* は一致している必要がある。
check パラメータは Rev.7.01.26 以降で使用可能。

[初期値]　anti-replay-check = on

[設定例]　*# ipsec sa policy 101 1 esp aes-cbc sha-hmac*

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.33.3　SA の手動更新

[書式]　**ipsec refresh sa**

[設定値]　なし

[説明]　SA を手動で更新する。

[ノート]　管理されている SA をすべて削除して、IKE の状態を初期化する。
このコマンドでは、SA の削除を相手に通知しないので、通常の運用では **ipsec sa delete all** コマンドの方が望ましい。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.33.4　ダングリング SA の動作の設定

[書式]　**ipsec ike restrict-dangling-sa** *gateway_id action*
no ipsec ike restrict-dangling-sa *gateway_id* [*action*]

[設定値]　◦ *gateway_id*.....セキュリティ・ゲートウェイの識別子
◦ *action*
• auto.....アグレッシブモードの始動側でのみ IKE SA と IPsec SA を同期させる
• off.....IKE SA と IPsec SA を同期させない。

[説明]　このコマンドはダングリング SA の動作に制限を設ける。

ダングリング SA とは、IKE SA を削除するときに対応する IPsec SA を削除せずに残したときの状態を指す。RT シリーズでは基本的にはダングリング SA を許す方針で実装しており、IKE SA と IPsec SA を独立のタイミングで削除する。

auto を設定したときには、アグレッシブモードの始動側でダングリング SA を排除し、IKE SA と IPsec SA を同期して削除する。この動作は IKE keepalive が正常に動作するために必要な処置である。
off を設定したときには、常にダングリング SA を許す動作となり、IKE SA と IPsec SA を独立なタイミングで削除する。
ダイヤルアップ VPN のクライアント側ではない場合には、このコマンドの設定に関わらず常に IKE SA と IPsec SA は独立に管理され、削除のタイミングは必ずしも同期しない。

[ノート]　ダングリング SA の強制削除が行われても、通常は新しい IKE SA に基づいた新しい IPsec SA が存在するので通信に支障が出ることはない。

ダイヤルアップ VPN のクライアント側でダングリング SA を許さないのは、IKE キープアライブを正しく機能させるために必要なことである。
IKE キープアライブでは、IKE SA に基づいてキープアライブを行う。ダングリング SA が発生した場合には、その SA についてはキープアライブを行う IKE SA が存在せず、キープアライブ動作が行えない。そのため、IKE キープアライブを有効に動作させるにはダングリング SA が発生したら強制的に削除して、通信は対応する IKE SA が存在する IPsec SA で行われるようにしなくてはいけない。

ダングリング SA の扱いについては、動作モードとリビジョンによって動作が異なる。

リビジョン	7.01.05 以前	7.01.08	7.01.15	7.01.16 以降
ダイヤルアップ VPN のクライアント側	(A)	(B)		(C)
それ以外	(A)	(B)	(A)	

(A) ダングリング SA が発生しても何もせず通信を続ける
(B) ダングリング SA が発生した時にはそれを消去し、必要であれば新しい SA を作成して通信を行う
(C) このコマンドにより動作を変更できる

[初期値]　auto

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

19.33.5　IPsec NAT トラバーサルを利用するための設定

[書式]　**ipsec ike nat-traversal** *gateway switch* [keepalive=*interval*]
no ipsec ike nat-traversal *gateway* [*switch* [keepalive=*interval*]]

[設定値]
- *gateway*..... セキュリティゲートウェイの識別子
- *switch* ..... 動作の有無
  - on..... NAT トラバーサルの動作を有効にする
  - off..... NAT トラバーサルの動作を無効にする
- *interval*..... NAT キープアライブの送信間隔
  - off..... 送信しない
  - 時間..... 30 - 100000[秒]

[説明]　NAT トラバーサルの動作を設定する。この設定があるときには、IKE で NAT トラバーサルの交渉を行う。
相手が NAT トラバーサルに対応していないときや、通信経路上に NAT の処理がないときには、NAT トラバーサルを使用せず、ESP パケットを使って通信する。
対向のルーターや端末でも NAT トラバーサルの設定が必要である。いずれか一方にしか設定がないときには、NAT トラバーサルを使用せず、ESP パケットを使って通信する。

[ノート]　**ipsec ike esp-encapsulation** コマンドとの併用はできない。
また、IPComp が設定されているトンネルインタフェースでは利用できない。
アグレッシブモードの ESP トンネルでのみ利用できる。メインモードや AH では利用できず、トランスポートモードでも利用できない。
Rev.8.03.43 以降で使用可能。

[初期値]　*switch* = off
interval = 300

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

19.33.6　SA の削除

[書式]　**ipsec *sa* delete** *id*

[設定値]
- *id*
  - SA の ID
  - all..... すべての SA

[説明]　指定した SA を削除する。
SA の ID は自動的に付与され、**show ipsec *sa*** コマンドで確認することができる。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.34　トンネルインタフェース関連の設定

19.34.1　IPsec トンネルの外側の IPv4 パケットに対する DF ビットの制御の設定

[書式]　**ipsec tunnel outer df-bit** *mode*
no ipsec tunnel outer df-bit [*mode*]

[設定値]　◦ *mode*
- copy .....内側の IPv4 パケットの DF ビットを外側にもコピーする
- set.....常に 1
- clear.....常に 0

[説明]　IPsec トンネルの外側の IPv4 パケットで、DF ビットをどのように設定するかを制御する。
copy の場合には、内側の IPv4 パケットの DF ビットをそのまま外側にもコピーする。
set または clear の場合には、内側の IPv4 パケットの DF ビットに関わらず、外側の IPv4 パケットの DF ビットはそれぞれ 1、または 0 に設定される。
トンネルインタフェース毎のコマンドである。

[ノート]　トンネルインタフェースの MTU と実インタフェースの MTU の値の大小関係により、IPsec 化されたパケットをフラグメントしなくてはいけない時には、このコマンドの設定に関わらず DF ビットは 0 になる。
Rev.7.01.26 以降で使用可能。

[初期値]　copy

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

19.34.2　使用する SA のポリシーの設定

[書式]　**ipsec tunnel** *policy_id*
no ipsec tunnel [*policy_id*]

[設定値]　◦ *policy_id* .....整数 (1..2147483647)

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

[初期値]　SA のポリシーは設定されていない

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.34.3　IPComp によるデータ圧縮の設定

[書式]　**ipsec ipcomp type** *type*
no ipsec ipcomp type [*type*]

[設定値]　◦ *type*
- deflate.....deflate 圧縮でデータを圧縮する
- none.....データ圧縮を行わない

[説明]　IPComp でデータ圧縮を行うかどうかを設定する。サポートしているアルゴリズムは deflate のみである。
受信した IPComp パケットを展開するためには、特別な設定を必要としない。すなわち、サポートしているアルゴリズムで圧縮された IPComp パケットを受信した場合には、設定に関係なく展開する。
必ずしもセキュリティ・ゲートウェイの両方にこのコマンドを設定する必要はない。片側にのみ設定した場合には、そのセキュリティ・ゲートウェイから送信される IP パケットのみが圧縮される。
トランスポートモードのみを使用する場合には、IPComp を使用することはできない。

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

[初期値]　none

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

19.34.4　トンネルバックアップの設定

[書式]

tunnel backup none
tunnel backup *interface ip_address*
tunnel backup pp *peer_num* [switch-router=*switch1*]
tunnel backup tunnel *tunnel_num* [switch-interface=*switch2*]
no tunnel backup

[設定値]

- *interface* ..... LAN インタフェース名
- *ip_address* ..... バックアップ先のゲートウェイの IP アドレス
- *peer_num* ..... バックアップ先の相手先情報番号
- *tunnel_num* ..... トンネルインタフェース番号
- *switch1* ..... バックアップの受け側のルーターを 2 台に分けるか否か
  - on ..... 分ける
  - off ..... 分けない
- *switch2* ..... LAN/PP インタフェースのバックアップにしたがってトンネルを作り直すか否か
  - on ..... 作り直す
  - off ..... 作り直さない

[説明]

トンネルインタフェースに障害が発生したときにバックアップとして利用するインタフェースを指定する。

switch-router オプションについては、以下の 2 つの条件を満たすときに on を設定する。

- バックアップの受け側に 2 台のルーターがあり、一方がバックアップ元の回線に接続し、もう一方がバックアップ先の回線に接続している。
- バックアップ先の回線に接続しているルーターのファームウェアがこのリビジョンよりも古い。

[初期値]

none
switch1 = off
switch2 = on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

19.34.5　トンネルテンプレートの設定

[書式]　**tunnel template** *tunnel_num* [*tunnel_num* ...]
no tunnel template

[設定値]　◦ *tunnel_num*.....適用するトンネルインタフェース番号もしくは適用するトンネルインタフェース番号の範囲 (複数指定することが可能)

[説明]　選択されているトンネルインタフェースの設定を、テンプレートとして他のトンネルインタフェースにも適用するかどうかを設定する。

選択されているトンネルインタフェースに対して設定したコマンドは、以下のパラメータがトンネルインタフェース番号に等しい場合、これらのパラメータを適用先のトンネルインタフェース番号に置換した上で、適用先のトンネルインタフェースにも設定する。
- **ipsec sa policy** コマンドにて設定される、ポリシー ID
- **ipsec** で始まるコマンドにて設定される、セキュリティ・ゲートウェイの識別番号

なお、**ipsec ike remote name** コマンドに関しては、コマンド適用の際、相手側セキュリティゲートウェイの名前の末尾に、トンネルインタフェース番号を付加する。

選択されているトンネルインタフェース対して設定されているコマンドと同じコマンドが、適用先のトンネルインタフェースに既に設定されている場合、適用先のトンネルインタフェースに設定されているコマンドを優先して適用する。

テンプレートとなるトンネルインタフェースに設定することで、他のトンネルインタフェースにも展開して適用されるコマンドの一覧は以下のとおりである。
- **ipsec ike** で始まるコマンドのうち、パラメータに「セキュリティ・ゲートウェイの識別子」をとるもの
- **ipsec auto refresh** コマンド
  (引数の「セキュリティ・ゲートウェイの識別子」を省略しない場合のみ)
- **ipsec tunnel** コマンド
- **ipsec sa policy** コマンド
- **tunnel enable** コマンド

テンプレートの設定が、実際の設定にどのように反映されているかは、以下のコマンドを用いることで確認できる。
　# **show config tunnel** *tunnel_num* expand

[ノート]　本コマンドは Rev.8.03 以降で使用可能である。またトンネルインタフェースが選択されている時にのみ使用できる。

[初期値]　トンネルテンプレートは設定されていない

[設定例]　◦ **ipsec sa policy** コマンドについて
tunnel select 1
tunnel template 2-3
ipsec sa policy 1 1 esp aes-cbc sha-hmac
上記のコマンドが設定されている時、以下のコマンドが自動的に有効となる。
ipsec sa policy 2 2 esp aes-cbc sha-hmac
ipsec sa policy 3 3 esp aes-cbc sha-hmac

◦ **ipsec ike** ... コマンドについて
tunnel select 1
tunnel template 2-3
ipsec ike local address 1 192.168.0.1
上記のコマンドが設定されている時、以下のコマンドが自動的に有効となる。
ipsec ike local address 2 192.168.0.1
ipsec ike local address 3 192.168.0.1

◦ **ipsec ike remote name** コマンドについて
tunnel select 1
tunnel template 2-3
ipsec ike remote name 1 pc
上記のコマンドが設定されている時、以下のコマンドが自動的に有効となる。
ipsec ike remote name 2 pc2
ipsec ike remote name 3 pc3

◦ トンネルインタフェース番号の指定について
適用するトンネルインタフェース番号は、番号の指定と範囲の指定を同時に記述することが可能である。
tunnel template 2 4-100
tunnel template 100 200-300 400

◦以下の 2 つの設定例は同じ内容を示している。

```
( 設定例 1)
tunnel select 1
 ipsec tunnel 1
  ipsec sa policy 1 1 esp aes-cbc sha-hmac
  ipsec ike encryption 1 aes-cbc
  ipsec ike group 1 modp1024
  ipsec ike local address 1 192.168.0.1
  ipsec ike pre-shared-key 1 text himitsu1
  ipsec ike remote address 1 any
  ipsec ike remote name 1 pc
 tunnel enable 1
tunnel select 2
 ipsec tunnel 2
  ipsec sa policy 2 2 esp aes-cbc sha-hmac
  ipsec ike encryption 2 aes-cbc
  ipsec ike group 2 modp1024
  ipsec ike local address 2 192.168.0.1
  ipsec ike pre-shared-key 2 text himitsu2
  ipsec ike remote address 2 any
  ipsec ike remote name 2 pc2
 tunnel enable 2

( 設定例 2)
tunnel select 1
 tunnel template 2
 ipsec tunnel 1
  ipsec sa policy 1 1 esp aes-cbc sha-hmac
  ipsec ike encryption 1 aes-cbc
  ipsec ike group 1 modp1024
  ipsec ike local address 1 192.168.0.1
  ipsec ike pre-shared-key 1 text himitsu1
  ipsec ike remote address 1 any
  ipsec ike remote name 1 pc
 tunnel enable 1
tunnel select 2
  ipsec ike pre-shared-key 2 text himitsu2
```

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

19.35　トランスポートモード関連の設定

19.35.1　トランスポートモードの定義

[書式]

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

[設定値]

◦ *id*..... トランスポート ID (1..2147483647)
◦ *policy_id*..... ポリシー ID (1..2147483647)
◦ *proto*..... プロトコル
◦ *src_port_list*..... UDP、TCP のソースポート番号列
- ポート番号を表す十進数
- ポート番号を表すニーモニック
- * (すべてのポート)

◦ *dst_port_list*..... UDP、TCP のデスティネーションポート番号列
- ポート番号を表す十進数
- ポート番号を表すニーモニック
- * (すべてのポート)

[説明]

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

[設定例]

◦ 192.168.112.25 のルーターへの TELNET のデータをトランスポートモードで通信

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

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

20. PPTP 機能の設定

本機能を使用して PC と接続するためには、PC 側には Microsoft 社 Windows の「仮想プライベートネットワーク」が必要となります。

20.1 共通の設定

tunnel encapsulation、**tunnel endpoint address**、**ppp ccp type** コマンドも合わせて参照のこと。

20.1.1 PPTP サーバーを動作させるか否かの設定

[書式]
pptp service *service*
no pptp service [*service*]

[設定値]
◦ *service*
- on ..... PPTP サーバーとして動作する
- off ..... PPTP サーバーとして動作しない

[説明]
PPTP サーバー機能を動作させるか否かを設定する。

[ノート]
PPTP サーバーで使う TCP のポート番号 1723 を閉じる。デフォルト off なので、PPTP サーバーを起動する場合には、**pptp service** on を設定する。

[初期値]
off

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

20.1.2 相手先情報番号にバインドされるトンネルインタフェースの設定

[書式]
pp bind *tunnel_num*
pp bind *tunnel_num-tunnel_num*
no pp bind [*tunnel_num*]

[設定値]
◦ *tunnel_num* ..... トンネルインタフェース番号 (tunnel1 .. tunnel20)

[説明]
選択されている相手先情報番号にバインドされるトンネルインタフェースを指定する。
第 2 書式は anonymous インタフェースを使って多数の接続先を登録するために複数連続したトンネルインタフェースをバインドする場合に用いる。

[ノート]
PPTP は PP 毎に設定する。
tunnel encapsulationコマンドで pptp を設定したトンネルインタフェースをバインドすることによって PPTP で通信することを可能にする。

[初期値]
設定されていない

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

20.1.3 PPTP の動作タイプの設定

[書式]
pptp service type *type*
no pptp service type [*type*]

[設定値]
◦ *type*
- server ..... サーバーとして動作
- client ..... クライアントとして動作

[説明]
PPTP サーバーとして動作するか、PPTP クライアントとして動作するかを設定する。

[ノート]
PPTP はサーバー、クライアント方式の接続で、ルーター間で接続する場合には必ず一方がサーバーで、もう一方がクライアントである必要がある。

[初期値]
server

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

20.1.4 PPTP ホスト名の設定

[書式] **pptp hostname** *name*
no pptp hostname [*name*]

[設定値] ◦ *name*..... ホスト名 (64 バイト以下)

[説明] PPTP ホスト名を設定する。

[ノート] コマンドで設定したユーザ定義の名前が相手先に通知される。何も設定していない場合には機種名が通知される。
相手先のルーターには、**show status pp** コマンドの ' 接続相手先 :' で表示される。

[初期値] 機種名

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

20.1.5 PPTP パケットのウィンドウサイズの設定

[書式] **pptp window size** *size*
no pptp window size [*size*]

[設定値] ◦ *size*..... パケットサイズ (1..128)

[説明] 受信済みで無応答の PPTP パケットをバッファに入れることができるパケットの最大数を設定する。

[初期値] 32

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

20.1.6 PPTP の動作モードの設定

[書式] **pptp call-id mode** *mode*
no pptp call-id mode [*mode*]

[設定値] ◦ *mode*
- normal ..... 通常モード
- backward-compatibility...Rev.4.06.16 互換モード

[説明] PPTP の動作モードを設定する。
接続相手が Rev.4.06.16 の場合にのみ、動作モードを backward-compatibility にする。

[初期値] normal

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	~~RTX1200~~	RTX1100	RTX1000	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

20.1.7 PPTP 暗号鍵生成のための要求する認証方式の設定

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

[設定値] ◦ *auth*
- pap ..... PAP
- chap ..... CHAP
- mschap ..... MSCHAP
- mschap-v2..... MSCHAP-Version2
- chap-pap..... CHAP と PAP 両方

[説明] 要求する認証方式を設定します

[ノート] PPTP 暗号鍵生成のために認証プロトコルの MS-CHAP または MS-CHAPv2 を設定する。通常サーバー側で設定する。

[初期値] 設定されない

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

20.1.8　PPTP 暗号鍵生成のための受け入れ可能な認証方式の設定

[書式]　**pp auth accept** *auth* [*auth*]
no pp auth accept [*auth auth*]

[設定値]　◦ *auth*
- pap .....PAP
- chap .....CHAP
- mschap.....MSCHAP
- mschap-v2 .....MSCHAP-Version2

[説明]　受け入れ可能な認証方式を設定します。

[ノート]　PPTP 暗号鍵生成のために認証プロトコルの MS-CHAP または MS-CHAPv2 を設定する。通常クライアント側で設定する。
MacOS 10.2 以降のクライアントに対しては mschap-v2 を用いる。

[初期値]　設定されない

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

20.1.9　PPTP のコネクション制御の syslog を出力するか否かの設定

[書式]　**pptp syslog** *syslog*
no pptp syslog [*syslog*]

[設定値]　◦ *syslog*
- on .....出力する
- off.....出力しない

[説明]　PPTP のコネクション制御の syslog を出力するか否かを設定する。
キープアライブ用の Echo-Request, Echo-Reply については出力されない。

[初期値]　off

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

20.2　リモートアクセス VPN 機能

20.2.1　PPTP トンネルの切断タイマの設定

[書式]　**pptp tunnel disconnect time** *time*
no pptp tunnel disconnect time [*time*]

[設定値]　◦ *time*
- 秒数 (1..21474836)
- off.....タイマを設定しない

[説明]　選択されている PPTP トンネルに対して、データパケット無入力・無送信時に、タイムアウトにより PPTP トンネルを切断する時間を設定する。

[初期値]　60

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

20.2.2　PPTP トンネルの端点の名前の設定

[書式]　**tunnel endpoint name** [*local_name*] *remote_name*
no tunnel endpoint name [*local_name remote_name*]

[設定値]　◦ *local_name*.....自分側端点

◦ *remote_name*.....相手側端点

[説明]　トンネル端点の名前を指定する。

[ノート]　名前にはドメイン名 (FQDN) を指定する。**tunnel endpoint address** コマンドが設定されている場合には、そちらが優先される。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

20.2.3 PPTP キープアライブの設定

[書式] **pptp keepalive use** *use*
no pptp keepalive use [*use*]

[設定値] ◦ *use*
- on..... 使用する
- off..... 使用しない

[説明] トンネルキープアライブを使用するか否かを選択する。

[ノート] PPTP トンネルの端点に対して、PPTP 制御コネクション確認要求 (Echo-Request) を送出して、それに対する PPTP 制御コネクション確認要求への応答 (Echo-Reply) で相手先からの応答があるかどうか確認する。応答がない場合には、**pptp keepalive interval** コマンドに従った切断処理を行う。

[初期値] on

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

20.2.4 PPTP キープアライブのログ設定

[書式] **pptp keepalive log** *log*
no pptp keepalive log [*log*]

[設定値] ◦ *log*
- on..... ログにとる
- off..... ログにとらない

[説明] トンネルキープアライブをログに取るかどうか選択する。

[初期値] off

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

20.2.5 PPTP キープアライブを出すインターバルとカウントの設定

[書式] **pptp keepalive interval** *interval* [*count*]
no pptp keepalive interval [*interval count*]

[設定値] ◦ *interval*..... インターバル (1..65535)

◦ *count*..... カウント (3..100)

[説明] トンネルキープアライブを出すインターバルとダウン検出用のカウントを設定する。

[ノート] 一度 PPTP 制御コネクション確認要求 (Echo-Request) に対するリプライが返ってこないのを検出したら、その後の監視タイマは 1 秒に短縮される。

[初期値] *interval* = 30
count = 6

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

20.2.6 PPTP 接続において暗号化の有無により接続を許可するか否かの設定

[書式] **ppp ccp no-encryption** *mode*
no ppp ccp no-encryption [*mode*]

[設定値] ◦ *mode*
- reject..... 暗号化なしでは接続拒否
- accept ..... 暗号化なしでも接続許可

[説明] MPPE(Microsoft Point-to-Point Encryption) の暗号化がネゴシエーションされないときの動作を設定する。

[初期値] accept

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

21. SNMP の設定

SNMP(Simple Network Management Protocol; RFC1157) の設定を行うことにより、SNMP 管理ソフトウェアに対してネットワーク管理情報のモニタと変更を行うことができるようになります。この時ヤマハルーターは SNMP エージェントとなります。

ヤマハルーターは MIB (Management information Base) として RFC1213(MIB-II) とプライベート MIB に対応しています。プライベート MIB については http://www.rtpro.yamaha.co.jp/ にある情報を参照してください。

SNMP により情報を交換するグループをコミュニティと呼びます。コミュニティ間のアクセスには、読み出し専用 (read-only) と読み書き可能 (read-write) の 2 つのアクセスモードがあります。

ヤマハルーターの状態を通知する SNMP メッセージをトラップと呼びます。どのようなトラップを送信するかは **snmp trap enable snmp** コマンドで設定し、受信するホストは **snmp trap host** コマンドで設定します。

読み出し専用のコミュニティ名と送信トラップのコミュニティ名の初期値は“public”になっています。SNMP 管理ソフトウェア側のコミュニティ名も“public”の場合が多いので、セキュリティを重要視する場合は適切なコミュニティ名に設定変更します。コミュニティ名にログインパスワードや管理パスワードを使用しないように注意してください。

工場出荷状態では SNMP によるアクセス許可に関する **snmp host** コマンドの設定が none であるので、ヤマハルーターへの SNMP によるアクセスは一切できない状態にあります。また、トラップの受信ホストを設定する **snmp trap host** コマンドの設定が clear であるので、どこにもトラップを送信しません。

21.1　SNMP によるアクセスを許可するホストの設定

[書式]　**snmp host** *host* [*ro_community* [*rw_community*]]
no snmp host [*host*]

[設定値]
- *host*
  - SNMP によるアクセスを許可するホストの IP アドレス
  - any..... すべてのホストから SNMP によりアクセスできる
  - none..... すべてのホストからの SNMP によるアクセスを禁止する
- *ro_community*.....Read-Only コミュニティ文字列
- *rw_community*.....Read-Write コミュニティ文字列

[説明]　SNMP によるアクセスを許可するホストを設定する。
any を設定した場合は任意のホストからの SNMP によるアクセスを許可する。
IP アドレスでホストを指定した場合には、同時にコミュニティ文字列も設定できる。*Read-Write* コミュニティ文字列を省略した場合には、*Read-Write* アクセスが禁止される。*Read-Only* コミュニティ文字列も省略した場合には、コミュニティ文字列には **snmp community** コマンドの設定が用いられる。

[ノート]　Rev.7.01.12 からコマンドの入力形式が拡張された。

[初期値]　none

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

21.2　SNMP 送信パケットの始点アドレスの設定

[書式]　**snmp local address** *ip_address*
no snmp local address [*ip_address*]

[設定値]
- *ip_address*.....IP アドレス

[説明]　SNMP 送信パケットの始点 IP アドレスを設定する。

[初期値]　インタフェースに設定されているアドレスから自動選択

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

21.3　読み出し専用のコミュニティ名の設定

［書式］　**snmp community read-only** *name*
no snmp community read-only [*name*]

［設定値］　◦ *name*..... SNMP によるアクセスモードが読み出し専用であるコミュニティ名 (1 文字以上 16 文字以内)

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

［初期値］　public

［適用モデル］

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

21.4　読み書き可能なコミュニティ名の設定

［書式］　**snmp community read-write** *name*
no snmp community read-write [*name*]

［設定値］　◦ *name*..... SNMP によるアクセスモードが読み書き可能であるコミュニティ名 (1 文字以上 16 文字以内)

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

［初期値］　空文字列

［適用モデル］

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

21.5　sysContact の設定

［書式］　**snmp syscontact** *name*
no snmp syscontact [*name*]

［設定値］　◦ *name*..... sysContact として登録する名称 (255 文字以内の文字列)

［説明］　MIB 変数 sysContact を設定する。空白を含ませるためには、パラメータ全体をダブルクォート (”)、もしくはシングルクォート (’) で囲む。
sysContact は一般的に、管理者の名前や連絡先を記入しておく変数である。

［初期値］　sysContact は設定されていない

［設定例］　*# snmp syscontact “RT administrator”*

［適用モデル］

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

21.6　sysLocation の設定

［書式］　**snmp syslocation** *name*
no snmp syslocation [*name*]

［設定値］　◦ *name*..... sysLocation として登録する名称 (255 文字以内の文字列)

［説明］　MIB 変数 sysLocation を設定する。空白を含ませるためには、パラメータ全体をダブルクォート (”)、もしくはシングルクォート (’) で囲む。
sysLocation は一般的に、機器の設置場所を記入しておく変数である。

［初期値］　sysLocation は設定されていない

［設定例］　*# snmp syslocation “RT room”*

［適用モデル］

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

21.7　sysName の設定

[書式]　**snmp sysname** *name*
no snmp sysname [*name*]

[設定値]
- *name*..... sysName として登録する名称 (255 文字以内の文字列)

[説明]　MIB 変数 sysName を設定する。空白を含ませるためには、パラメータ全体をダブルクォート (")、もしくはシングルクォート (') で囲む。
sysName は一般的に、機器の名称を記入しておく変数である。

[初期値]　sysName は設定されていない

[設定例]　*# snmp sysname "RT300i with VPN module"*

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

21.8　SNMP トラップを送信するか否かの設定

[書式]　**snmp trap enable snmp** *trap* [*trap...*]
snmp trap enable snmp *all*
no snmp trap enable snmp

[設定値]
- *trap*..... トラップの種類
  - coldstart .... 全設定初期化時
  - warmstart..... ..... 再起動時
  - linkup..... ..... リンクアップ時
  - linkdown..... ..... リンクダウン時
  - authenticationfailure..... 認証失敗時
- all..... すべてのトラップを送信することを示すキーワード

[説明]　SNMP トラップを送信するか否かを設定する。
all を設定した場合には、すべてのトラップを送信する。個別にトラップを設定した場合には、設定されたトラップだけが送信される。

[ノート]　authenticationFailure トラップを送信するか否かはこのコマンドによって制御される。
coldStart トラップについては、Rev.7.01.15 以前のファームウェアでは、"**cold start**" コマンド投入時およびファームウェアリビジョンアップ後の再起動直前に coldStart トラップを送信する。それ以外のファームウェアでは、電源投入、再投入による起動後およびファームウェアリビジョンアップによる再起動後に coldStart トラップを送信する。
linkDown トラップについては、**snmp trap send linkdown** コマンドによってインタフェース毎に制御できる。あるインタフェースについて、linkDown トラップが送信されるか否かは、**snmp trap send linkdown** コマンドで送信が許可されており、かつ、このコマンドでも許可されている場合に限られる。
Rev.7.00 系および RT300i では、**snmp enableauthentraps** コマンドを使用する。

[初期値]　*all*

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	RT250i	RT107e	SRT100

21.9　SNMP の linkDown トラップの送信制御の設定

[書式]　**snmp trap send linkdown** *interface switch*
snmp trap send linkdown pp *peer_num switch*
snmp trap send linkdown tunnel *tunnel_num switch*
no snmp trap send linkdown *interface*
no snmp trap send linkdown pp *peer_num* [*switch*]
no snmp trap send linkdown tunnel *tunnel_num* [*switch*]

[設定値]
- *interface*
  - LAN インタフェース名
  - BRI インタフェース名
- *peer_num*..... 相手先情報番号
- *tunnel_num*..... トンネルインタフェース番号
- *switch*
  - on..... 送信する
  - off..... 送信しない

[説明]　指定したインタフェースの linkDown トラップを送信するか否かを設定する。

[初期値]　on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	RT250i	RT107e	SRT100

21.10　SNMP トラップのコミュニティ名の設定

[書式]　**snmp trap community** *name*
no snmp trap community [*name*]

[設定値]　◦ *name*..... 送信トラップのコミュニティ名 (1 文字以上 16 文字以内)

[説明]　トラップを送信する際のコミュニティ名を設定する。

[初期値]　public

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

21.11　SNMP トラップの送信先の設定

[書式]　**snmp trap host** *host* [*community*]
no snmp trap host *host* [*community*]

[設定値]　◦ *host*..... SNMP トラップを送信する先のホストの IP アドレス
◦ *community*..... コミュニティ名

[説明]　SNMP トラップを送信するホストを指定する。コマンドを複数設定することで、複数のホストを同時に指定できる。トラップ送信時のコミュニティ文字列にはこのコマンドの設定値が用いられるが、省略されている場合には **snmp trap community** コマンドの設定値が用いられる。

[ノート]　Rev.7.00.26 以降で *community* パラメータが指定可能。

[初期値]　SNMP トラップを送信しない

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

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

[書式]　**snmp yrifppdisplayatmib2** *switch*
no snmp yrifppdisplayatmib2

[設定値]　◦ *switch*
• on..... MIB 変数 yrIfPpDisplayAtMib2 を "enabled(1)" とする
• off..... MIB 変数 yrIfPpDisplayAtMib2 を "disabled(2)" とする

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

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	RT250i	RT107e	SRT100

21.13　トンネルインタフェースの情報を MIB2 の範囲で表示するか否かの設定

[書式]　**snmp yriftunneldisplayatmib2** *switch*
no snmp yriftunneldisplayatmib2

[設定値]　◦ *switch*
• on..... MIB 変数 yrIfTunnelDisplayAtMib2 を "enabled(1)" とする
• off..... MIB 変数 yrIfTunnelDisplayAtMib2 を "disabled(2)" とする

[説明]　MIB 変数 yrIfTunnelDisplayAtMib2 の値をセットする。この MIB 変数はトンネルインタフェースを MIB2 の範囲で表示するかどうかを決定する。Rev.4 以前と同じ表示にする場合には、MIB 変数を "enabled(1)" に、つまり、このコマンドで on を設定する。

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

21.14　PP インタフェースのアドレスの強制表示の設定

[書式]　**snmp display ipcp force** *switch*
no snmp display ipcp force

[設定値]
◦ *switch*
- on ..... IPCP により付与された IP アドレスを PP インタフェースのアドレスとして必ず表示する
- off..... IPCP により付与された IP アドレスは PP インタフェースのアドレスとして必ずしも表示されない

[説明]　NAT を使用しない場合や、NAT の外側アドレスとして固定の IP アドレスが指定されている場合には、IPCP で得られた IP アドレスはそのまま PP インタフェースのアドレスとして使われる。この場合、SNMP では通常のインタフェースの IP アドレスを調べる手順で IPCP としてどのようなアドレスが得られたのか調べることができる。
しかし、NAT の外側アドレスとして 'ipcp' と指定している場合には、IPCP で得られた IP アドレスは NAT の外側アドレスとして使用され、インタフェースには付与されない。そのため、SNMP でインタフェースの IP アドレスを調べても、IPCP でどのようなアドレスが得られたのかを知ることができない。
本コマンドを on に設定しておくと、IPCP で得られた IP アドレスが NAT の外側アドレスとして使用される場合でも、SNMP ではそのアドレスをインタフェースのアドレスとして表示する。アドレスが実際にインタフェースに付与されるわけではないので、始点 IP アドレスとして、その IP アドレスが利用されることはない。

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

21.15　LAN インタフェースの各ポートのリンクが up/down したときにトラップを送信するか否かの設定

[書式]　**snmp trap link-updown separate-l2switch-port** *interface switch*
no snmp trap link-updown separate-l2switch-port *interface* [*switch*]

[設定値]
◦ *interface*..... インタフェース (現状では 'lan1' のみ設定可能)
- lan1

◦ *switch*
- on ..... トラップを送信する
- off..... トラップを送信しない

[説明]　各ポートのリンクが up/down したときにトラップを送信するか否かを設定する。

[初期値]　off

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

22. RADIUS の設定

ISDN 接続のための認証とアカウントを RADIUS サーバーを利用して管理できます。PPTP 接続のための認証とアカウントの管理はサポートされません。

22.1 RADIUS による認証を使用するか否かの設定

[書式]
radius auth *auth*
no radius auth [*auth*]

[設定値]
◦ *auth*
- on..... 使用する
- off..... 使用しない

[説明]
anonymous に対して何らかの認証を要求する設定の場合に、相手から受け取ったユーザネーム (PAP であれば UserID、CHAP であれば NAME) が、自分で持つユーザネーム (**pp auth username** コマンドで指定) の中に含まれていない場合には RADIUS サーバーに問い合わせるか否かを設定する。

[ノート]
RADIUS による認証と RADIUS によるアカウントは独立して使用できる。
サポートしているアトリビュートについては、WWW サイトのドキュメント <http://www.rtpro.yamaha.co.jp/> を参照すること。

[初期値]
off

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	SRT100

22.2 RADIUS によるアカウントを使用するか否かの設定

[書式]
radius account *account*
no radius account [*account*]

[設定値]
◦ *account*
- on..... 使用する
- off..... 使用しない

[説明]
RADIUS によるアカウントを使用するか否かを設定する。

[ノート]
RADIUS による認証と RADIUS によるアカウントは独立して使用できる。
サポートしているアトリビュートについては、WWW サイトのドキュメント <http://www.rtpro.yamaha.co.jp/> を参照すること。

[初期値]
off

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	SRT100

22.3 RADIUS サーバーの指定

[書式]
radius server *ip1* [*ip2*]
no radius server [*ip1* [*ip2*]]

[設定値]
◦ *ip1* ..... RADIUS サーバー (正) の IP アドレス (IPv6 アドレス可)
◦ *ip2* ..... RADIUS サーバー (副) の IP アドレス (IPv6 アドレス可)

[説明]
RADIUS サーバーを設定する。2 つまで指定でき、最初のサーバーから返事をもらえない場合は、2 番目のサーバーに問い合わせを行う。

[ノート]
RADIUS には認証とアカウントの 2 つの機能があり、それぞれのサーバーは **radius auth server** / **radius account server** コマンドで個別に設定できる。**radius server** コマンドでの設定は、これら個別の設定が行われていない場合に有効となり、認証、アカウントいずれでも用いられる。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	SRT100

22.4　RADIUS 認証サーバーの指定

[書式]　**radius auth server** *ip1* [*ip2*]
no radius auth server [*ip1* [*ip2*]]

[設定値]
- *ip1*.....RADIUS 認証サーバー (正) の IP アドレス (IPv6 アドレス可)
- *ip2*.....RADIUS 認証サーバー (副) の IP アドレス (IPv6 アドレス可)

[説明]　RADIUS 認証サーバーを設定する。2 つまで指定でき、最初のサーバーから返事をもらえない場合は、2 番目のサーバーに問い合わせを行う。

[ノート]　このコマンドで RADIUS 認証サーバーの IP アドレスが指定されていない場合は、**radius server** コマンドで指定した IP アドレスを認証サーバーとして用いる。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	SRT100

22.5　RADIUS アカウントサーバーの指定

[書式]　**radius account server** *ip1* [*ip2*]
no radius account server [*ip1* [*ip2*]]

[設定値]
- *ip1*.....RADIUS アカウントサーバー (正) の IP アドレス (IPv6 アドレス可)
- *ip2*.....RADIUS アカウントサーバー (副) の IP アドレス (IPv6 アドレス可)

[説明]　RADIUS アカウントサーバーを設定する。2 つまで指定でき、最初のサーバーから返事をもらえない場合は、2 番目のサーバーに問い合わせを行う。

[ノート]　このコマンドで RADIUS アカウントサーバーの IP アドレスが指定されていない場合は、**radius server** コマンドで指定した IP アドレスをアカウントサーバーとして用いる。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	SRT100

22.6　RADIUS 認証サーバーの UDP ポートの設定

[書式]　**radius auth port** *port_num*
no radius auth port [*port_num*]

[設定値]
- *port_num*.....UDP ポート番号

[説明]　RADIUS 認証サーバーの UDP ポート番号を設定する。

[ノート]　RFC2138 ではポート番号として 1812 を使うことになっている。

[初期値]　1645

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	SRT100

22.7　RADIUS アカウントサーバーの UDP ポートの設定

[書式]　**radius account port** *port_num*
no radius account port [*port_num*]

[設定値]
- *port_num*.....UDP ポート番号

[説明]　RADIUS アカウントサーバーの UDP ポート番号を設定する。

[ノート]　RFC2138 ではポート番号として 1813 を使うことになっている。

[初期値]　1646

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	SRT100

22.8　RADIUS シークレットの設定

[書式]　**radius secret** *secret*
no radius secret [*secret*]

[設定値]　◦ *secret*..... シークレット文字列

[説明]　RADIUS シークレットを設定する。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	SRT100

22.9　RADIUS 再送信パラメータの設定

[書式]　**radius retry** *count time*
no radius retry [*count time*]

[設定値]　◦ *count*..... 再送回数 (1..10)
◦ *time*..... ミリ秒 (20..10000)

[説明]　RADIUS パケットの再送回数とその時間間隔を設定する。

[初期値]　*count* = 4
time = 3000

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	SRT100

23. NAT 機能

NAT 機能は、ルーターが転送する IP パケットの始点 / 終点 IP アドレスや、TCP/UDP のポート番号を変換することにより、アドレス体系の異なる IP ネットワークを接続することができる機能です。
NAT 機能を用いると、プライベートアドレス空間とグローバルアドレス空間との間でデータを転送したり、1 つのグローバル IP アドレスに複数のホストを対応させたりすることができます。

ヤマハルーターでは、始点 / 終点 IP アドレスの変換だけを行うことを NAT と呼び、TCP/UDP のポート番号の変換を伴うものを IP マスカレードと呼んでいます。

アドレス変換規則を表す記述を NAT ディスクリプタと呼び、それぞれの NAT ディスクリプタには、アドレス変換の対象とすべきアドレス空間が定義されます。アドレス空間の記述には、**nat descriptor address inner**、**nat descriptor address outer** コマンドを用います。前者は NAT 処理の内側 (INNER) のアドレス空間を、後者は NAT 処理の外側 (OUTER) のアドレス空間を定義するコマンドです。原則的に、これら 2 つのコマンドを対で設定することにより、変換前のアドレスと変換後のアドレスとの対応づけが定義されます。

NAT ディスクリプタはインタフェースに対して適用されます。インタフェースに接続された先のネットワークが NAT 処理の外側であり、インタフェースから本機を経由して他のインタフェースから繋がるネットワークが NAT 処理の内側になります。
NAT ディスクリプタは動作タイプ属性を持ちます。IP マスカレードやアドレスの静的割当てなどの機能を利用する場合には、該当する動作タイプを選択する必要があります。

23.1　インタフェースへの NAT ディスクリプタ適用の設定

[書式]

ip *interface* **nat descriptor** *nat_descriptor_list* [reverse *nat_descriptor_list*]
ip pp nat descriptor *nat_descriptor_list* [reverse *nat_descriptor_list*]
ip tunnel nat descriptor *nat_descriptor_list* [reverse *nat_descriptor_list*]
no ip *interface* **nat descriptor** [*nat_descriptor_list* [reverse *nat_descriptor_list*]]
no ip pp nat descriptor [*nat_descriptor_list* [reverse *nat_descriptor_list*]]
no ip tunnel nat descriptor [*nat_descriptor_list* [reverse *nat_descriptor_list*]]

◦ *interface*.....LAN インタフェース名
◦ *nat_descriptor_list*....空白で区切られた NAT ディスクリプタ番号 (1..2147483647) の並び (16 個以内)

[説明]

適用されたインタフェースを通過するパケットに対して、リストに定義された順番で NAT ディスクリプタによって定義された NAT 変換を順番に処理する。

reverse の後ろに記述した NAT ディスクリプタでは、通常処理される IP アドレス、ポート番号とは逆向きの IP アドレス、ポート番号に対して NAT 変換を施す。

[ノート]

LAN インタフェースの場合、NAT ディスクリプタの外側アドレスに対しては、同一 LAN の ARP 要求に対して応答する。
reverse を指定できるのは Rev.8.03 系以降のリビジョンである。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

23.2　NAT ディスクリプタの動作タイプの設定

[書式]

nat descriptor type *nat_descriptor type*
no nat descriptor type *nat_descriptor* [*type*]

[設定値]

◦ *nat_descriptor* .....NAT ディスクリプタ番号 (1..2147483647)
◦ *type*
- none.....NAT 変換機能を利用しない
- nat.....動的 NAT 変換と静的 NAT 変換を利用
- masquerade .....静的 NAT 変換と IP マスカレード変換
- nat-masquerade..動的 NAT 変換と静的 NAT 変換と IP マスカレード変換

[説明]

NAT 変換の動作タイプを指定する。

[ノート]

nat-masquerade は、動的 NAT 変換できなかったパケットを IP マスカレード変換で救う。例えば、外側アドレスが 16 個利用可能の場合は先勝ちで 15 個 NAT 変換され、残りは IP マスカレード変換される。

[初期値]

none

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

23.3　NAT 処理の外側 IP アドレスの設定

[書式]　**nat descriptor address outer** *nat_descriptor outer_ipaddress_list*
no nat descriptor address outer *nat_descriptor* [*outer_ipaddress_list*]

[設定値]
- *nat_descriptor*..... NAT ディスクリプタ番号 (1..2147483647)
- *outer_ipaddress_list*. NAT 対象の外側 IP アドレス範囲のリストまたはニーモニック
  - 1 個の IP アドレスまたは間に - をはさんだ IP アドレス (範囲指定)、およびこれらを任意に並べたもの
  - ipcp..... PPP の IPCP の IP-Address オプションにより接続先から通知される IP アドレス
  - primary..... **ip** *interface* **address** コマンドで設定されている IP アドレス
  - secondary..... **ip** *interface* **secondary address** コマンドで設定されている IP アドレス

[説明]　動的 NAT 処理の対象である外側の IP アドレスの範囲を指定する。IP マスカレードでは、先頭の 1 個の外側の IP アドレスが使用される。

[ノート]　ニーモニックをリストにすることはできない。
適用されるインタフェースにより使用できるパラメータが異なる。

適用インタフェース	LAN	PP	トンネル
ipcp	×	○	×
primary	○	×	×
secondary	○	×	×
IP アドレス	○	○	○

[初期値]　ipcp

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

23.4　NAT 処理の内側 IP アドレスの設定

[書式]　**nat descriptor address inner** *nat_descriptor inner_ipaddress_list*
no nat descriptor address inner *nat_descriptor* [*inner_ipaddress_list*]

[設定値]
- *nat_descriptor*..... NAT ディスクリプタ番号 (1..2147483647)
- *inner_ipaddress_list*. NAT 対象の内側 IP アドレス範囲のリストまたはニーモニック
  - 1 個の IP アドレス、または間に - をはさんだ IP アドレス (範囲指定)、およびこれらを任意に並べたもの
  - auto ..... すべて

[説明]　NAT/IP マスカレード処理の対象である内側の IP アドレスの範囲を指定する。

[初期値]　auto

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

23.5　静的 NAT エントリの設定

[書式]　**nat descriptor static** *nat_descriptor id outer_ip=inner_ip* [*count*]
no nat descriptor static *nat_descriptor id* [*outer_ip=inner_ip* [*count*]]

[設定値]
- *nat_descriptor*..... NAT ディスクリプタ番号 (1..2147483647)
- *id*..... 静的 NAT エントリの識別情報 (1..2147483647)
- *outer_ip*..... 外側 IP アドレス (1 個)
- *inner_ip*..... 内側 IP アドレス (1 個)
- *count*
  - 連続設定する個数
  - 省略時は 1

[説明]　NAT 変換で固定割り付けする IP アドレスの組み合せを指定する。個数を同時に指定すると指定されたアドレスを始点とした範囲指定とする。

[ノート]　外側アドレスが NAT 処理対象として設定されているアドレスである必要は無い。
静的 NAT のみを使用する場合には、**nat descriptor address outer** コマンドと **nat descriptor address inner** コマンドの設定に注意する必要がある。初期値がそれぞれ ipcp と auto であるので、例えば何らかの IP アドレスをダミーで設定しておくことで動的動作しないようにする。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

23.6　IP マスカレード使用時に rlogin,rcp と ssh を使用するか否かの設定

[書式]　**nat descriptor masquerade rlogin** *nat_descriptor use*
no nat descriptor masquerade rlogin *nat_descriptor* [*use*]

[設定値]
- *nat_descriptor* .....NAT ディスクリプタ番号 (1..2147483647)
- *use*
  - on .....使用する
  - off.....使用しない

[説明]　IP マスカレード使用時に rlogin、rcp、ssh の使用を許可するか否かを設定する。

[ノート]　on にすると、rlogin、rcp と ssh のトラフィックに対してはポート番号を変換しなくなる。
また on の場合に rsh は使用できない。

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

23.7　静的 IP マスカレードエントリの設定

[書式]　**nat descriptor masquerade static** *nat_descriptor id inner_ip protocol* [*outer_port*=]*inner_port*
no nat descriptor masquerade static *nat_descriptor id* [*inner_ip protocol* [*outer_port*=]*inner_port*]

[設定値]
- *nat_descriptor* .....NAT ディスクリプタ番号 (1..2147483647)
- *id* .....静的 IP マスカレードエントリの識別情報 (1 以上の数値)
- *inner_ip*.....内側 IP アドレス (1 個)
- *protocol*
  - esp.....ESP
  - tcp.....TCP プロトコル
  - udp .....UDP プロトコル
  - icmp .....ICMP プロトコル
  - プロトコル番号 .....IANA で割り当てられている protocol numbers
- *outer_port*.....固定する外側ポート番号 (ニーモニック)
- *inner_port* .....固定する内側ポート番号 (ニーモニック)

[説明]　IP マスカレードによる通信でポート番号変換を行わないようにポートを固定する。

[ノート]　*outer_port* と *inner_port* を指定した場合には IP マスカレード適用時にインタフェースの外側から内側へのパケットは *outer_port* から *inner_port* に、内側から外側へのパケットは *inner_port* から *outer_port* へとポート番号が変換される。
outer_port を指定せず、*inner_port* のみの場合はポート番号の変換はされない。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

23.8　NAT の IP アドレスマップの消去タイマの設定

[書式]
nat descriptor timer *nat_descriptor time*
nat descriptor timer *nat_descriptor* protocol=*protocol* [port=*port_range*] *time*
nat descriptor timer *nat_desciptor* tcpfin *time2*
no nat descriptor timer *nat_descriptor* [*time*]
no nat descriptor timer *nat_descriptor* protocol=*protocol* [port=*port_range*] [*time*]
no nat descriptor timer *nat_desciptor* tcpfin [*time2*]

[設定値]
◦ *nat_descriptor*..... NAT ディスクリプタ番号 (1..2147483647)
◦ *time*..... 消去タイマの秒数 (30..21474836)
◦ *time2*..... TCP/FIN 通過後の消去タイマの秒数 (1-21474836)
◦ *protocol*..... プロトコル
◦ *port_range*..... ポート番号の範囲、プロトコルが TCP または UDP の場合にのみ有効

[説明]
NAT や IP マスカレードのセッション情報を保持する期間を表す NAT タイマを設定する。IP マスカレードの場合には、プロトコルやポート番号別の NAT タイマを設定することもできる。指定されていないプロトコルの場合は、第一の形式で設定した NAT タイマの値が使われる。
IP マスカレードの場合には、TCP/FIN 通過後の NAT タイマを設定することができる。TCP/FIN が通過したセッションは終了するセッションなので、このタイマを短くすることで NAT テーブルの使用量を抑えることができる。

[ノート]
第 3、第 6 書式は以下のリビジョンで使用可能。
Rev.8.03.75 以降、Rev.9.00.37 以降、Rev.10.00.31 以降、Rev.10.01 系

[初期値]
TIME ..... 900, プロトコルごとの設定はなし
TIME2 60

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

23.9　IP マスカレードテーブルの TTL 処理方式の設定

[書式]
nat descriptor masquerade ttl hold *type*
no nat descriptor masquerade ttl hold

[設定値]
◦ *type*
- auto ..... 自動認識可能なアプリケーションのコネクションの制御チャネルとデータチャネルの TTL を同期させる
- all..... 同じホストによるすべての TCP コネクションを対象
- ftp..... FTP の制御チャネルのみを対象

[説明]
制御チャネルとデータチャネルからなるアプリケーションにおいて、データチャネル上でのデータ転送中に、対応する制御チャネルが消滅することによるデータ通信不良が発生しないようにするために、制御チャネルとデータチャネルの両 IP マスカレードテーブルの TTL を同期させる方法を設定する。

auto と設定した場合には、ルーターが自動認識可能なアプリケーションのコネクションに対応するテーブルの TTL を同期させる。
all と設定した場合には、同じホストによるすべてのコネクションに対応するテーブルの TTL を同期させる。
ftp と設定した場合には、FTP コネクションに対応するテーブルの TTL のみを同期させる。

[ノート]
all と設定した場合には、多くのテーブルの TTL が同期して、多くのテーブルが残留するために、内部リソースが枯渇することがある。
auto と設定した場合に正常動作しないアプリケーションがあるときは all と設定しなければならない。

[初期値]
auto (Rev.7.01.41 以降)
all (上記以外)

[適用モデル]

~~RTX3000~~	RTX2000	RTX1500	~~RTX1200~~	RTX1100	RTX1000	RT300i	RT250i	RT107e	~~SRT100~~

23.10　外側から受信したパケットに該当する変換テーブルが存在しないときの動作の設定

[書式]　**nat descriptor masquerade incoming** *nat_descriptor action* [*ip_address*]
no nat descriptor masquerade incoming *nat_descriptor*

[設定値]
- *nat_descriptor* .....NAT ディスクリプタ番号 (1..2147483647)
- *action*
  - through .....変換せずに通す
  - reject .....破棄して、TCP の場合は RST を返す
  - discard .....破棄して、何も返さない
  - forward.....指定されたホストに転送する
- *ip_address*.....転送先の IP アドレス

[説明]　IP マスカレードで外側から受信したパケットに該当する変換テーブルが存在しないときの動作を設定する。*action* が forward のときには *ip_address* を設定する必要がある。

[初期値]　reject

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

23.11　IP マスカレードで利用するポートの範囲の設定

[書式]　**nat descriptor masquerade port range** *nat_descriptor port_range1* [*port_range2* [*port_range3*]]
no nat descriptor masquerade port range *nat_descriptor* [*port_range1* [*port_range2* [*port_range3*]]]

[設定値]
- *nat_descriptor* .....NAT ディスクリプタ番号 (1..2147483647)
- *port_range1, port_range2, port_range3*....間に - をはさんだポート番号の範囲

[説明]　IP マスカレードで利用するポート番号の範囲を設定する。

ポート番号は、まず最初に *port_range1* の範囲から利用される。*port_range1* のポート番号がすべて使用中になったら、*port_range2* の範囲のポート番号を使い始める。*port_range1*、*port_range2* ともすべて使用中になったら、*port_range3* の範囲のポート番号を使い始める。

[ノート]　NAT の同時セッション数が 4096 となっている機種では *port_range1* のみが設定でき、*port_range2*、*3* は設定も利用もできない。*port_range2*、*3* が利用できるのは、以下の機種である。

機種	NAT の同時セッション数
RTX3000	40000
RTX1200	20000

[初期値]　*port_range1*=60000-64095
port_range2=49152-59999
port_range3=24096-49151(RTX3000)
port_range3=44096-49151(RTX1200)

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

23.12　FTP として認識するポート番号の設定

[書式]　**nat descriptor ftp port** *nat_descriptor port* [*port...*]
no nat descriptor ftp port *nat_descriptor* [*port...*]

[設定値]
- *nat_descriptor* .....NAT ディスクリプタの識別番号 (1..2147483647)
- *port*.....ポート番号 (1..65535)

[説明]　TCP で、このコマンドにより設定されたポート番号を FTP の制御チャネルの通信だとみなして処理をする。

[初期値]　21

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

23.13　IP マスカレードで変換しないポート番号の範囲の設定

[書式]　**nat descriptor masquerade unconvertible port** *nat_descriptor* if-possible
nat descriptor masquerade unconvertible port *nat_descriptor protocol port*
no nat descriptor masquerade unconvertible port *nat_descriptor protocol* [*port*]

[設定値]　◦ *nat_descriptor*..... NAT ディスクリプタの識別番号 (1..2147483647)
◦ *protocol*
• tcp ..... TCP
• udp..... UDP
◦ *port* ..... ポート番号の範囲

[説明]　IP マスカレードで変換しないポート番号の範囲を設定する。
if-possible が指定されている時には、処理しようとするポート番号が他の通信で使われていない場合には値を変換せずそのまま利用する。

[初期値]　設定されていない

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

23.14　NAT のアドレス割当をログに記録するか否かの設定

[書式]　**nat descriptor log** *switch*
no nat descriptor log

[設定値]　◦ *switch*
• on..... 記録する
• off..... 記録しない

[説明]　NAT のアドレス割当をログに記録するか否かを設定します。

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

23.15　SIP メッセージに含まれる IP アドレスを書き換えるか否かの設定

[書式]　**nat descriptor sip** *nat_descriptor sip*
no nat descriptor sip *nat_descriptor*

[設定値]　◦ *nat_descriptor*..... NAT ディスクリプタの識別番号 (1..2147483647)
◦ *sip*
• on..... 変換する
• off..... 変換しない

[説明]　静的 NAT や静的 IP マスカレードで SIP メッセージに含まれる IP アドレスを書き換えるか否かを設定する。

[ノート]　Rev.8.01.18、Rev.8.02.35 で初期値を off から on に変更した。

[初期値]　on

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

23.16　IP マスカレード変換時に DF ビットを削除するか否かの設定

[書式]　**nat descriptor masquerade remove df-bit** *remove*
no nat descriptor masquerade remove df-bit [*remove*]

[設定値]　◦ *remove*
- on ..... IP マスカレード変換時に DF ビットを削除する
- off..... IP マスカレード変換時に DF ビットを削除しない

[説明]　IP マスカレード変換時に DF ビットを削除するか否かを設定する。

DF ビットは経路 MTU 探索のために用いるが、そのためには長すぎるパケットに対する ICMP エラーを正しく発信元まで返さなくてはいけない。しかし、IP マスカレード処理では IP アドレスなどを書き換えてしまうため、ICMP エラーを正しく発信元に返せない場合がある。そうなると、パケットを永遠に届けることができなくなってしまう。このように、経路 MTU 探索のための ICMP エラーが正しく届かない状況を、経路 MTU ブラックホールと呼ぶ。

IP マスカレード変換時に同時に DF ビットを削除してしまうと、この経路 MTU ブラックホールを避けることができる。その代わりに、経路 MTU 探索が行われないことになるので、通信効率が下がる可能性がある。

[ノート]　ファストパス処理は、一度ノーマルパス処理で通過させたパケットの情報を保存しておき、同じ種類のパケットであれば高速に転送するという処理を行っている。そのため、例えば **ping** コマンドを実行した場合、最初の 1 回目はノーマルパス処理、2 回目以降はファストパス処理となる。そのため、最初の 1 回は DF ビットが削除されるが、2 回目以降は DF ビットが削除されないという状況だった。
Rev.7.01.26 以降で使用可能。

[初期値]　on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	RT250i	RT107e	SRT100

23.17　IP マスカレードで変換するセッション数の設定

[書式]　**nat descriptor masquerade session limit** *nat_descriptor id limit*
no nat descriptor masquerade session limit *nat_descriptor id*

[設定値]　◦ *nat_descriptor* ..... NAT ディスクリプタ番号 (1..2147483647)
◦ *id* ..... セッション数設定の識別番号 (1)
◦ *limit* ..... 制限値 (1..40000)(RTX3000)
制限値 (1..20000)(RTX1200)
制限値 (1..4096)(上記以外)

[説明]　ホスト毎に IP マスカレードで変換するセッションの最大数を設定する。
ホストはパケットの始点 IP アドレスで識別され、任意のホストを始点とした変換テーブルの登録数が *limit* に制限される。

[ノート]　Rev.8.03.68 以降、Rev.9.00.31 以降、Rev.10.00.27 以降で使用可能。

[初期値]　40000 (RTX3000)
20000 (RTX1200)
4096 (上記以外)

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

24. DNS の設定

本機は、DNS (Domain Name Service) 機能として名前解決、リカーシブサーバー機能、上位 DNS サーバーの選択機能、簡易 DNS サーバー機能 (静的 DNS レコードの登録) を持ちます。

名前解決の機能としては、**ping** や **traceroute**、**rdate**、**ntpdate**、**telnet** コマンドなどの IP アドレスパラメータの代わりに名前を指定したり、SYSLOG などの表示機能において IP アドレスを名前解決したりします。

リカーシブサーバー機能は、DNS サーバーとクライアントの間に入って、DNS パケットの中継を行います。本機宛にクライアントから届いた DNS 問い合わせパケットを ***dns server*** コマンドで設定された DNS サーバーに中継します。DNS サーバーからの回答は本機宛に届くので、それをクライアントに転送します。最大 256 件のキャッシュを持ち、キャッシュにあるデータに関しては DNS サーバーに問い合わせることなく返事を返すため、DNS によるトラフィックを削減する効果があります。キャッシュは、DNS サーバーからデータを得た場合にデータに記されていた時間だけ保持されます。

DNS の機能を使用するためには、***dns server*** コマンドを設定しておく必要があります。また、この設定は DHCP サーバー機能において、DHCP クライアントの設定情報にも使用されます。

24.1 DNS を利用するか否かの設定

[書式]
dns service *service*
no dns service [*service*]

[設定値]
◦ *service*
- recursive ..... DNS リカーシブサーバーとして動作する
- off..... サービスを停止させる

[説明]
DNS リカーシブサーバーとして動作するかどうかを設定する。off を設定すると、DNS 的機能は一切動作しない。また、ポート 53/udp も閉じられる。

[初期値]
recursive

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

24.2 DNS サーバーの IP アドレスの設定

[書式]
dns server *ip_address* [*ip_address ...*]
no dns server [*ip_address ...*]

[設定値]
◦ *ip_address* ..... DNS サーバーの IP アドレス (空白で区切って最大 4ヶ所まで設定可能)

[説明]
DNS サーバーの IP アドレスを指定する。
この IP アドレスはルーターが DHCP サーバーとして機能する場合に DHCP クライアントに通知するためや、IPCP の MS 拡張オプションで相手に通知するためにも使用される。

[ノート]
DHCP サーバーから通知された DNS サーバーを使うときには、***dns server dhcp*** コマンドを使う。

[初期値]
DNS サーバーは設定されていない

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

24.3 DNS ドメイン名の設定

[書式]
dns domain *domain_name*
no dns domain [*domain_name*]

[設定値]
◦ *domain_name* ..... DNS ドメインを表す文字列

[説明]
ルーターが所属する DNS ドメインを設定する。
ルーターのホストとしての機能 (ping, traceroute) を使うときに名前解決に失敗した場合、このドメイン名を補完して再度解決を試みる。ルーターが DHCP サーバーとして機能する場合、設定したドメイン名は DHCP クライアントに通知するためにも使用される。ルーターのあるネットワークおよびそれが含むサブネットワークの DHCP クライアントに対して通知する。
空文字列を設定する場合には、***dns domain .*** と入力する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

24.4　DNS サーバーを通知してもらう相手先情報番号の設定

[書式]　**dns server pp** *peer_num*
no dns server pp [*peer_num*]

[設定値]　◦ *peer_num*.....DNS サーバーを通知してもらう相手先情報番号

[説明]　DNS サーバーを通知してもらう相手先情報番号を設定する。このコマンドで相手先情報番号が設定されていると、DNS での名前解決を行う場合に、まずこの相手先に発信して、そこで PPP の IPCP MS 拡張機能で通知された DNS サーバーに対して問い合わせを行う。
相手先に接続できなかったり、接続できても DNS サーバーの通知がなかった場合には名前解決は行われない。**dns server** コマンドで DNS サーバーが明示的に指定されている場合には、そちらの設定が優先される。**dns server** コマンドに指定したサーバーから返事がない場合には、相手先への接続と DNS サーバーの通知取得が行われる。

[ノート]　この機能を使用する場合には、**dns server pp** コマンドで指定された相手先情報に、**ppp ipcp msext** on の設定が必要である。
DHCP サーバーから通知された DNS サーバーを使うときには、**dns server dhcp** コマンドを使う。

[初期値]　DNS サーバーを通知してもらう相手先は設定されていない

[設定例]
```
# pp select 2
pp2# ppp ipcp msext on
pp2# dns server pp 2
```

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

24.5　DHCP/IPCP MS 拡張で DNS サーバーを通知する順序の設定

[書式]　**dns notice order** *protocol server* [*server*]
no dns notice order *protocol* [*server* [*server*]]

[設定値]　◦ *protocol*
- dhcp..... DHCP による通知
- msext..... IPCP MS 拡張による通知

◦ *server*
- none..... 一切通知しない
- me ..... 本機自身
- server ..... **dns server** コマンドに設定したサーバー群

[説明]　DHCP や IPCP MS 拡張では DNS サーバーを複数通知できるが、それをどのような順序で通知するかを設定する。
none を設定すれば、他の設定に関わらず DNS サーバーの通知を行わなくなる。me は本機自身の DNS リカーシブサーバー機能を使うことを通知する。*server* では、**dns server** コマンドに設定したサーバー群を通知することになる。IPCP MS 拡張では通知できるサーバーの数が最大 2 に限定されているので、後ろに *me* が続く場合は先頭の 1 つだけと本機自身を、*server* 単独で設定されている場合には先頭の 2 つだけを通知する。

[初期値]
```
dhcp me server
msext me server
```

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

24.6　プライベートアドレスに対する問い合わせを処理するか否かの設定

[書式]　**dns private address spoof** *spoof*
no dns private address spoof [*spoof*]

[設定値]　◦ *spoof*
- on.....処理する
- off.....処理しない

[説明]　on の場合、DNS リカーシブサーバー機能で、プライベートアドレスの PTR レコードに対する問い合わせに対し、上位サーバーに問い合わせを転送することなく、自分でその問い合わせに対し“NXDomain”、すなわち「そのようなレコードはない」というエラーを返す。

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

24.7　SYSLOG 表示で DNS により名前解決するか否かの設定

[書式]　**dns syslog resolv** *resolv*
no dns syslog resolv [*resolv*]

[設定値]　◦ *resolv*
- on..... 解決する
- off..... 解決しない

[説明]　SYSLOG 表示で DNS により名前解決するか否かを設定する。

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

24.8　DNS 問い合わせの内容に応じた DNS サーバーの選択

[書式]　**dns server select** *id server* [*server2*] [*type*] *query* [*original-sender*] [restrict pp *connection-pp*]
dns server select *id* pp *peer_num* [*default-server*] [*type*] *query* [*original-sender*]
[restrict pp *connection-pp*]
dns server select *id* dhcp *interface* [*default-server*] [*type*] *query* [*original-sender*]
[restrict pp *connection-pp*]
dns server select *id* reject [*type*] *query* [*original-sender*]
no dns server select *id*

[設定値]　◦ *id*..... DNS サーバー選択テーブルの番号
◦ *server*..... プライマリ DNS サーバーの IP アドレス
◦ *server2*..... セカンダリ DNS サーバーの IP アドレス
◦ *type*..... DNS レコードタイプ
- a ..... ホストの IP アドレス
- ptr ..... IP アドレスの逆引き用のポインタ
- mx..... メールサーバー
- ns..... ネームサーバー
- cname ..... 別名
- any ..... すべてのタイプにマッチする
- 省略時は *a*

◦ *query*..... DNS 問い合わせの内容
- *type* が a、mx、ns、cname の場合
  query はドメイン名を表す文字列であり、後方一致とする。例えば、"yamaha.co.jp" であれば、rtpro.yamaha.co.jp などにマッチする。"." を指定するとすべてのドメイン名にマッチする。
- *type* が ptr の場合 . *query* は IP アドレス (*ip_address*[*/masklen*]) であり、*masklen* を省略したときは IP アドレスにのみマッチし、*masklen* を指定したときはネットワークアドレスに含まれるすべての IP アドレスにマッチする。DNS 問い合わせに含まれる .in-addr.arpa ドメインで記述された FQDN は、IP アドレスへ変換された後に比較される。すべての IP アドレスにマッチする設定はできない。
- reject キーワードを指定した場合
  query は完全一致とし、前方一致、及び後方一致には "*" を用いる。つまり、前方一致では、"NetVolante.*" であれば、NetVolante.jp、NetVolante.rtpro.yamaha.co.jp などにマッチする。また、後方一致では、"*yamaha.co.jp" と記述する。

◦ *original-sender*..... DNS 問い合わせの送信元の IP アドレスの範囲
◦ *connection-pp*..... DNS サーバーを選択する場合、接続状態を確認する接続相手先情報番号
◦ *peer_num*..... IPCP により接続相手から通知される DNS サーバーを使う場合の接続相手先情報番号
◦ *interface*..... DHCP サーバーより取得する DNS サーバーを使う場合の LAN インタフェース名
◦ *default-server*..... *peer_num* パラメータで指定した接続相手から DNS サーバーを獲得できなかったときに使う DNS サーバーの IP アドレス

[説明]　DNS 問い合わせの解決を依頼する DNS サーバーとして、DNS 問い合わせの内容および DNS 問い合わせの送信元および回線の接続状態を確認する接続相手先情報番号と DNS サーバーとの組合せを複数登録しておき、DNS 問い合わせに応じてその組合せから適切な DNS サーバーを選択できるようにする。テーブルは小さい番号から検索され、DNS 問い合わせの内容に *query* がマッチしたら、その DNS サーバーを用いて DNS 問い合わせを解決しようとする。一度マッチしたら、それ以降のテーブルは検索しない。すべてのテーブルを検索してマッチするものがない場合には、**dns server** コマンドで指定された DNS サーバーを用いる。

reject キーワードを使用した書式の場合、*query* がマッチしたら、その DNS 問い合わせパケットを破棄し、DNS 問い合わせを解決しない。

restrict pp 節が指定されていると、*connection-pp* で指定した相手先がアップしているかどうかがサーバーの選択条件に追加される。相手先がアップしていないとサーバーは選択されない。相手先がアップしていて、かつ、他の条件もマッチしている場合に指定したサーバーが選択される。

[ノート]　セカンダリ DNS サーバー *server2* は Rev.7.00.26, 6.03.25 以降で指定可能。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

24.9　静的 DNS レコードの登録

[書式]

ip host *fqdn value* [ttl=*ttl*]
dns static *type name value* [ttl=*ttl*]
no ip host *fqdn* [*value*]
no dns static *type name* [*value*]

[設定値]

◦ *type*.....名前のタイプ
- a.....ホストの IPv4 アドレス
- aaaa .....ホストの IPv6 アドレス
- ptr.....IP アドレスの逆引き用のポインタ
- mx.....メールサーバー
- ns.....ネームサーバー
- cname.....別名

◦ *name, value*..... *type* パラメータによって以下のように意味が異なる

type パラメータ	*name*	*value*
a	FQDN	IPv4 アドレス
aaaa	FQDN	IPv6 アドレス
ptr	IPv4 アドレス	FQDN
mx	FQDN	FQDN
ns	FQDN	FQDN
cname	FQDN	FQDN

◦ *fqdn*..... ドメイン名を含んだホスト名
◦ *ttl* .....秒数 (1 ～ 4294967295)

[説明]

静的な DNS レコードを定義する。
ip host コマンドは、***dns static*** コマンドで a と ptr を両方設定することを簡略化したものである。

[ノート]

問い合わせに対して返される DNS レコードは以下のような特徴を持つ。
◦ TTL フィールドには、*ttl* パラメータの設定値がセットされる。*ttl* パラメータが省略された時には 1 がセットされる。(RTX2000 では ttl パラメータの指定はできない。)
◦ Answer セクションに回答となる DNS レコードが 1 つセットされるだけで、Authority/Additional セクションには DNS レコードがセットされない
◦ MX レコードの preference フィールドは 0 にセットされる

aaaa タイプは Rev.7.01.34 以降、Rev.8.01.07 以降で使用可能。

[設定例]

 # ip host pc1.rtpro.yamaha.co.jp 133.176.200.1
 # dns static ptr 133.176.200.2 pc2.yamaha.co.jp
 # dns static cname mail.yamaha.co.jp mail2.yamaha.co.jp

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

24.10　DNS 問い合わせパケットの始点ポート番号の設定

[書式]

dns srcport *port*[-*port*]
no dns srcport [*port*-[*port*]]

[設定値]

◦ *port*.....ポート番号 (1..65535)

[説明]

ルーターが送信する DNS 問い合わせパケットの始点ポート番号を設定する。
ポート番号を一つだけしか設定しなかった場合には、指定したポート番号を始点ポートとして利用する。
ポート番号を範囲で指定した場合には、DNS 問い合わせパケットを送信するたびに、範囲内のポート番号をランダムに利用する。

[ノート]

DNS 問い合わせパケットをフィルタで扱うとき、始点番号がランダムに変化するということを考慮しておく必要がある。
本コマンドは Rev.7.01.34 以降、Rev.8.01.07 以降で使用可能。

[初期値]

53 ... (RTX1200 以外)
10000-10999 ... (RTX1200)

[設定例]

10000-10999 の範囲のポート番号をランダムに利用する
 # dns srcport 10000-10999

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	RT250i	RT107e	SRT100

24.11　DNS サーバーへアクセスできるホストの IP アドレス設定

[書式]　**dns host** *host* [*host* [...]]
no dns host

[設定値]　◦ *host*
- *any* ..... すべてのホストからのアクセスを許可する
- *lan* ..... すべての LAN ポート側ネットワーク内ならば許可する
- *lanN* ..... ひとつの任意の LAN ポート側ネットワーク内ならば許可する (N はインタフェース番号)
- *none* ..... すべてのホストからのアクセスを禁止する
- DNS サーバーへアクセスを許可するホストの IP アドレス
- DNS サーバーへアクセスを許可するホストの IP アドレスの範囲 (ip_address-ip_address)

[説明]　DNS サーバー機能へのアクセスを許可するホストを設定する。

[ノート]　このコマンドで LAN インタフェースを指定した場合には、ネットワークアドレスと limited broadcast address を除く IP アドレスからのアクセスを許可する。指定した LAN インタフェースにプライマリアドレスもセカンダリアドレスも設定していなければ、アクセスを許可しない。

[初期値]　any

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

24.12　DNS キャッシュを使用するか否かの設定

[書式]　**dns cache use** *switch*
no dns cache uset [*sw*]

[設定値]　◦ *switch*
- on ..... DNS キャッシュを利用する
- off ..... DNS キャッシュは利用しない

[説明]　DNS キャッシュを利用するか否かを設定する。
switch を on に設定した場合、DNS キャッシュを利用する。すなわち、ルーターが送信した DNS 問い合わせパケットに対する上位 DNS サーバーからの返答をルーター内部に保持し、次に同じ問い合わせが発生したときでも、サーバーには問い合わせず、キャッシュの内容を返す。
上位 DNS サーバーから得られた返答には複数の RR レコードが含まれているが、DNS キャッシュの保持時間は、それらの RR レコードの TTL のうちもっとも短い時間になる。また、まったく RR レコードが存在しない場合には、60 秒となる。
ルーター内部に保持する DNS エントリの数は **dns cache max entry** コマンドで設定する。
switch を off にした場合、DNS キャッシュは利用しない。ルーターが送信した DNS 問い合わせパケットに対する上位 DNS サーバーからの返答はルーター内部に保持せず、同じ問い合わせがあっても毎回 DNS サーバーに問い合わせを行う。

[初期値]　on

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

24.13　DNS キャッシュの最大エントリ数の設定

[書式]　**dns cache max entry** *num*
no dns cache max entry [*num*]

[設定値]　◦ *num* ..... 最大エントリ数 (1...1024)

[説明]　DNS キャッシュの最大エントリ数を設定する。
設定した数だけ、ルーター内部に DNS キャッシュとして上位 DNS サーバーからの返答を保持できる。設定した数を超えた場合、返答が返ってきた順で古いものから破棄される。
上位 DNS サーバーから得られた返答には複数の RR レコードが含まれているが、DNS キャッシュの保持時間は、それらの RR レコードの TTL のうちもっとも短い時間になる。また、まったく RR レコードが存在しない場合には、60 秒となる。返答が得られてから保持時間を経過したエントリは、DNS キャッシュから削除される。

[初期値]　256

[設定例]　*dns cache max entry 16*

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

25. 優先制御／帯域制御

優先制御と帯域制御の機能は、インタフェースに入力されたパケットの順序を入れ換えて別のインタフェースに出力します。これらの機能を使用しない場合には、パケットは入力した順番に処理されます。

優先制御は、クラス分けしたキューに優先順位をつけ、まず高位のキューのパケットを出力し、そのキューが空になると次の順位のキューのパケットを出力する、という処理を行います。
帯域制御は、クラス分けしたキューをラウンドロビン方式で監視しますが、監視頻度に差を与えてキューごとに利用できる帯域に差をつけます。
クラスは、**queue class filter** コマンドにより、パケットのフィルタリングと同様な定義でパケットを分類します。RTX3000 では、クラスは 1 から 100 まで、その他のモデルでは 1 から 16 までの番号で識別します。優先制御、帯域制御で使用可能なクラスは以下の通りです。

モデル	優先制御で使用可能なクラス	帯域制御で使用可能なクラス
RTX3000	1 ～ 16	1 ～ 100
上記以外の機種	1 ～ 4	1 ～ 16

クラスは番号が大きいほど優先順位が高くなります。
パケットの処理アルゴリズムは、**queue** *interface* **type** コマンドにより、優先制御、帯域制御、単純 FIFO の中から選択します。これはインタフェースごとに選択することができます。
RTX3000 ではクラス構造を階層化し、2 階層目に優先制御クラスを持つことができます。つまり、1 階層目は帯域制御、または、優先制御が設定でき、2 階層目は優先制御が設定できます。

25.1　インタフェース速度の設定

[書式]

speed *interface speed*
speed pp *speed*
no speed *interface* [*speed*]
no speed pp [*speed*]

[設定値]

◦ *interface*.....LAN インタフェース名
◦ *speed*.....インタフェース速度 (bit/s)

[説明]

指定したインタフェースに対して、インタフェースの速度を設定する。帯域制御のためのパラメータ計算に用いられるもので、実際の速度を設定できるわけではない。物理的な速度と一致しているのが望ましい。MP により動的に回線速度が変動する場合などは、最低限の速度に設定しておく。

[ノート]

speed パラメータの後ろに 'k' または 'M' をつけると、それぞれ kbit/s、Mbit/s として扱われる。
RT107e、SRT100 では **speed pp** コマンドは使用できない。

[初期値]

0 (PP インタフェースの場合)

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

25.2　クラス分けのためのフィルタ設定

[書式]

queue class filter *num class1*[*/class2*] [cos=*cos*] ip *src_addr* [*dest_addr* [*protocol* [*src_port* [*dest_port*]]]]
queue class filter *num class1* ipx *src_net* [*src_node* [*dst_net* [*dst_node* [*type* [*src_socket* [*dst_socket*]]]]]]
queue class filter *num class1* bridge *src_mac* [*dst_mac* [*offsettype_list*]]
no queue class filter *num* [*class1...*]

[設定値]

◦ *num*.....クラスフィルタの識別番号
◦ *class1*
- クラス (1..16; RTX3000 の場合は 1..100)
- precedence.....転送するパケットの TOS フィールドの precedence(0-7) に応じてクラス (1-8) を分けて優先制御もしくはシェーピング、Dynamic Traffic Control や CBQ による帯域制御を行う (RTX3000、RTX1500、RTX1100、SRT100、RTX1200 のみ指定可能)
- dscp.....転送するパケットの DS フィールドの DSCP 値により定義される PHB に応じてクラス (1-9) を分けて優先制御もしくはシェーピングや Dynamic Traffic Control による帯域制御を行う (RTX3000、RTX1500 のみ指定可能)

◦ *class2*.....第 2 階層クラス (1..4)
◦ *cos*
- CoS 値 (0-7)
- precedence.....転送するパケットの TOS の precedence(0-7) を ToS-CoS 変換として COS 値に格納する

◦ *src_addr*..... IP パケットの始点 IP アドレス
- xxx.xxx.xxx.xxx (xxx は十進数)
- * (ネットマスクの対応するビットが 8 ビットとも 0 と同じ。すべての IP アドレスに対応)

◦ *dest_addr*
- IP パケットの終点 IP アドレス
- 省略した場合は一個の * と同じ

◦ *protocol*..... フィルタリングするパケットの種類
- プロトコルを表す十進数
- プロトコルを表すニーモニック

icmp	1
tcp	6
udp	17

- 上項目のカンマで区切った並び (5 個以内)
- * (すべてのプロトコル)
- established
- 省略時は * と同じ

◦ *src_port* ..... UDP、TCP のソースポート番号
- ポート番号を表す十進数
- ポート番号を表すニーモニック (一部)

ニーモニック	ポート番号
ftp	20,21
ftpdata	20
telnet	23
smtp	25
domain	53
gopher	70
finger	79
www	80
pop3	110
sunrpc	111

ニーモニック	ポート番号
ident	113
ntp	123
nntp	119
snmp	161
syslog	514
printer	515
talk	517
route	520
uucp	540

- 間に - をはさんだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。
- 上項目のカンマで区切った並び (10 個以内)
- * (すべてのポート)
- 省略時は * と同じ。

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

IPX フィルタ

◦ *src_net*..... 始点 IPX ネットワーク番号
- 0:0:0:1 ..... FF:FF:FF:FE(2 桁以内の十六進数以外に '*' も指定可)
- * (すべての IPX ネットワーク番号)

◦ *src_node* ..... 始点 IPX ノード番号
- 0:0:0:0:0:1 ..... FF:FF:FF:FF:FF:FE(2 桁以内の十六進数以外に '*' も指定可)
- * (すべての IPX ノード番号)
- 省略した場合は一個の * と同じ。

◦ *dst_net*..... 終点 IPX ネットワーク番号 (*src_net* と同じ形式)

◦ *dst_node*..... 終点 IPX ノード番号 (*src_node* と同じ形式)

◦ *type*..... IPX パケットタイプ
- プロトコルを表す十進数 (0..255)
- プロトコルを表す十六進数 (0x0..0xFF)
- プロトコルを表すニーモニック

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

- 間に - をはさんだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。
- 上項目のカンマで区切った並び (5 個以内)
- * (すべてのプロトコル)
- 省略時は * と同じ。

◦ *src_socket*.....始点ソケット番号
- ポート番号を表す十進数 (0..255)
- ポート番号を表す十六進数 (0x0..0xFF)
- ポート番号を表すニーモニック

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

- 間に - をはさんだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。
- 上項目のカンマで区切った並び (10 個以内)
- * (すべてのポート)
- 省略時は * と同じ。

◦ *dst_socket*.....終点ソケット番号 (*src_socket* と同じ形式)

ブリッジフィルタ

◦ *src_mac*.....始点 MAC アドレス
- xx:xx:xx:xx:xx:xx (xx は十六進数)
- * (すべての MAC アドレスに対応)

◦ *dst_mac*
- 終点 MAC アドレス (*src_mac* と同じ形式)
- 省略時は一個の * と同じ。

◦ *offset*.....オフセットをあらわす十進数 (イーサネットフレームの始点 MAC アドレスの直後を 0 とするバイト数)

◦ *byte_list*
- バイト列
  - xx (xx は 2 桁の十六進数)
  - 上項目のカンマで区切った並び (16 個以内)
- * (すべてのバイト表現)

[説明]　クラス分けのためのフィルタを設定する。

class1 に precedence を指定した場合、フィルタに合致したパケットは、そのパケットの IP ヘッダの precedence 値に応じたクラスに分けられる。RTX3000、RTX1500、RTX1100、SRT100、RTX1200 で指定可能である。

class1 に dscp を指定した場合、フィルタに合致したパケットは、そのパケットの IP ヘッダの DSCP 値により定義される PHB に応じたクラスに分けられる。RTX3000、RTX1500 で指定可能である。

cos=*cos* 指定を行うと、フィルタに合致したパケットに付加される IEEE802.1Q タグの user_priority フィールドには、指定した CoS 値が格納される。*cos* に precedence を指定した場合、そのパケットの IP ヘッダの precedence 値に対応する値が user_priority フィールドに格納される。*cos* パラメータは RTX3000、RTX1500 と RTX1100 で指定可能である。

パケットフィルタに該当したパケットは、指定したクラスに分類される。このコマンドで設定したフィルタを使用するかどうか、あるいはどのような順番で適用するかは、各インタフェースにおける **queue** *interface* **class filter list** コマンドで設定する。

class1 と *class2* を「/」(スラッシュ) で連結して指定することができる。*class2* は RTX3000 で指定可能。

第 2、第 3 書式は RT300i でのみ使用できる。

[ノート]　RTX1500 では Rev.8.03 以降で *dscp* パラメータを指定することができる。

[設定例]
```
# queue class filter 1 4 ip * * udp 5004-5060 *
# queue class filter 2 10/3 ip * 172.16.1.0/24 tcp telnet *
# queue class filter 5 precedence ip 172.16.5.0/24 * tcp * *
# queue class filter 6 precedence/4 ip * 172.16.6.0/24 tcp * *
# queue class filter 10 dscp ip 172.16.10.0/24 *
# queue class filter 11 dscp/4 ip * 172.16.11.0/24
```

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

25.3　キューイングアルゴリズムタイプの選択

[書式]

queue *interface* **type** *type*
queue pp type *type*
no queue *interface* **type** [*type*]
no queue pp type [*type*]

[設定値]

◦ *interface*..... LAN インタフェース名

◦ *type*
- fifo..... First In, First Out 形式のキューイング
- priority..... 優先制御キューイング
- cbq..... 帯域制御キューイング
- wfq ..... Weighted Fair Queue 形式のキューイング
- shaping..... 帯域制御

[説明]

指定したインタフェースに対して、キューイングアルゴリズムタイプを選択する。

fifo は最も基本的なキューである。fifo の場合、パケットは必ず先にルーターに到着したものから送信される。パケットの順番が入れ替わることは無い。fifo キューにたまったパケットの数が **queue** *interface* **length** コマンドで指定した値を越えた場合、キューの最後尾、つまり最後に到着したパケットが破棄される。

wfq は、送信待ちのパケットを始点・終点 IP アドレスやプロトコル、ポート番号でフローとしてグループ分けして、それぞれのフローで使用する帯域のバランスが取れるようにするキューイングアルゴリズムである。wfq を使用すると、TELNET のような、帯域はあまり必要としないが速い応答時間を必要とするプロトコルと、FTP のような応答時間よりも広い帯域を必要とするプロトコルを同時に利用した場合に、TELNET の応答時間の落ち込みを fifo に比べて軽減することができる。

wfq のもう一つの特徴は、設定がいらないということである。設定するところがないため、優先制御や帯域制御に比べて細かい調整はできないが、簡単にフロー間での帯域のバランスを図ることができる。

priority は優先制御を行う。**queue class filter** コマンドおよび **queue** *interface* **class filter list** コマンドでパケットをクラス分けし、送信待ちのパケットの中から最も優先順位の高いクラスのパケットを送信する。

cbq は BRI と PRI インタフェースに対する帯域制御を行う。PP インタフェースにだけ設定できる。**queue** *interface* **class property** コマンドで各クラスに割り振る帯域をあらかじめ設定しておき、**queue class filter** コマンドおよび **queue** *interface* **class filter list** コマンドでクラス分けされたパケットが指定の帯域になるように送信する。

shaping は LAN インタフェースに対する帯域制御を行う。LAN インタフェースにだけ設定できる。

[ノート]

RT107e、RT250i ..... *type* パラメータに fifo、priority を指定することができる。
RT300i ..... *type* パラメータに fifo、priority、cbq、wfq を指定することができる。
上記以外の機種 ..... *type* パラメータに fifo、priority、shaping を指定することができる。

[初期値]

fifo

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

25.4　MP インタリーブの設定

[書式]

ppp mp interleave [*delay*] *switch*
no ppp mp interleave [[*delay*] *switch*]

[設定値]

◦ *delay*..... 遅延 (ミリ秒)

◦ *switch*
- on..... MP インタリーブを使用する
- off..... MP インタリーブを使用しない

[説明]

MP インタリーブを使用するかどうかを設定する。*delay* では、優先されるプロトコルで許容できる最大遅延を設定する。パケットをどのような大きさに分割するかは、*delay* の値と回線速度により決定される。

[ノート]

delay で設定した遅延が保証されるわけではない。
データの受信側でも同じ設定をしておかないと、効果が発揮されない。
同時に圧縮は利用できない。圧縮を利用する設定の場合、この機能は無視されるので、以下の設定で圧縮を無効にしておく必要がある。

```
ppp ccp type none
```

[初期値]

delay = 30
switch = off

[設定例]
```
# queue class filter 1 4 ip VOIP-GATEWAY * * * *
# queue class filter 2 3 ip * * icmp * *
# queue class filter 3 1 ip * * * * *
# pp select 1
pp1# pp bind bri2.1
pp1# queue pp type priority
pp1# queue class filter list 1 2 3
pp1# isdn remote address call 03-123-4567
pp1# ppp mp use on
pp1# ppp mp interleave on
pp1# ppp mp maxlink 1
pp1# ppp ccp type none
pp1# pp enable 1
```

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

25.5　クラス分けフィルタの適用

[書式]

queue *interface* **class filter list** *filter_list*
queue pp class filter list *filter_list*
queue tunnel class filter list *filter_list*
no queue *interface* **class filter list** [*filter_list*]
no queue pp class filter list [*filter_list*]
no queue tunnel class filter list [*filter_list*]

[設定値]

- *interface*.....LAN インタフェース名
- *filter_list*.....空白で区切られたクラスフィルタの並び

[説明]

指定した LAN インタフェースまたは選択されている PP、トンネルに対して、**queue class filter** コマンドで設定したフィルタを適用する順番を設定する。フィルタにマッチしなかったパケットは、**queue** *interface* **default class** コマンドで指定したデフォルトクラスに分類される。

[ノート]

RT250i では **queue tunnel class filter list** コマンドは使用できない。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

25.6　クラス毎のキュー長の設定

[書式]

queue *interface* **length** *len1* [*len2...lenN*] [drop-threshold=*dthreshold-mid*[,*dthreshold-high*]]
queue pp length *len1* [*len2...len16*]
no queue *interface* **length** [*len1...*]
no queue pp length [*len1...*]

[設定値]

- *interface*.....LAN インタフェース名
- *len1..lenN*.....クラス 1 からクラス 16 のキュー長 (1..10000; RTX1500 の場合は 1..2000)
  RTX3000 の場合はクラス 1 からクラス 100 のキュー長 (1..10000)
- *len1..len16*.....クラス 1 からクラス 16 のキュー長 (1..10000; RTX1500 の場合は 1..2000)
- *dthreshold-mid*.....AF PHB の廃棄優先度が中の場合のキューサイズの閾値 (1%..100%)
- *dthreshold-high*.....AF PHB の廃棄優先度が高の場合のキューサイズの閾値 (1%..100%)

[説明]

インタフェースに対して、指定したクラスのキューに入れることができるパケットの個数を指定する。指定を省略したクラスに関しては、最後に指定されたキュー長が残りのクラスにも適用される。

DiffServ ベース QoS の場合、*dthreshold-mid*、*dthreshold-high* パラメータで指定した値が AF PHB の廃棄優先度が中と高に対応するキューに積むことができる閾値となる。閾値は、クラスのキュー長に対する割合 (%) として表す。

dthreshold-high を省略した場合は、*dthreshold-mid* と同じ値となる。廃棄優先度が低に対応する閾値は常に 100% である。*dthreshold-mid*、*dthreshold-high* パラメータは、RTX3000 と RTX1500 で指定可能である。

[ノート]

dthreshold-mid、*dthreshold-high* パラメータは RTX3000 と Rev.8.03 系以降の RTX1500 で指定可能。

RTX3000 で **queue** *interface* **length secondary** コマンドで第 2 階層クラスのキュー長が指定されている場合は、**queue** *interface* **length secondary** コマンドで設定されたキュー長が優先して適用される。

[初期値] 200 (LAN: RTX3000、RTX1200、RT300i)
40 (LAN: 上記以外)
20 (PP: 全機種共通)
drop-threshold=75%, 50%

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

25.7 第２階層クラスのキュー長の設定

[書式] **queue** *interface* **length secondary** [primary=*primary_class*] *len1* [*len2* ...*len4*]
no queue *interface* **length secondary** [primary=*primary_class* ...]

[設定値]
- *interface* ..... LAN インタフェース名
- *primary_class* ..... 第１階層クラス (1..100)
  省略時、すべての第１階層クラスに従属する第２階層クラスのキュー長を一律に指定する
- *len1* ...*len4* ..... クラス１からクラス４のキュー長 (1..10000)

[説明] インタフェースに対して、指定した第１階層クラスに従属する第２階層クラスのキューに入ることのできるパケットの個数を指定する。設定を省略したクラスに関しては、最後に指定されたキュー長が残りのクラスにも適用される。

[初期値] 200

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

25.8 デフォルトクラスの設定

[書式] **queue** *interface* **default class** *class*
queue pp default class *class*
no queue *interface* **default class** *class*
no queue pp default class [*class*]

[設定値]
- *interface* ..... LAN インタフェース名
- *class* ..... クラス (1..16; RTX3000 の場合は 1..100)

[説明] インタフェースに対して、フィルタにマッチしないパケットをどのクラスに分類するかを指定する。

[初期値] 2

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

25.9 第２階層のデフォルトクラスの設定

[書式] **queue** *interface* **default class secondary** [primary=*primary_class*] *class*
no queue *interface* **default class secondary** [primary=*primary_class* ...]

[設定値]
- *interface* ..... LAN インタフェース名
- *primary_class* ..... 第１階層クラス (1..100)
  省略時、すべての第１階層クラスに従属する第２階層クラスのデフォルトクラスを一律に指定する
- *class* ..... クラス (1..4)

[説明] 指定した第１階層クラスに従属する第２階層クラスにおいて、フィルタにマッチしないパケットをどのクラスに分類するかを指定する。

[初期値] 2

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

25.10　クラスの属性の設定

[書式]

queue *interface* **class property** *class* bandwidth=*bandwidth*
queue *interface* **class property** *class* type=*type*
queue pp class property *class* bandwidth=*bandwidth* [parent=*parent*] [borrow=*borrow*] [maxburst=*maxburst*] [minburst=*minburst*] [packetsize=*packetsize*]
no queue *interface* **class property** *class* [bandwidth=*bandwidth* ...]
no queue pp class property *class* [bandwidth=*bandwidth* ...]

[設定値]

- *interface*.....LAN インタフェース名
- *class*.....クラス (1..16; RTX3000 の場合は 1..100)
- *bandwidth*.....クラスに割り当てる帯域 (bit/s)
  数値の後ろに 'k'、'M' をつけるとそれぞれ kbit/s、Mbit/s として扱われる。また、数値の後ろに '%' をつけると、回線全体の帯域に対するパーセンテージとなる。
- *parent*.....親クラスの番号 (0..16)
- *borrow*.....帯域が足りなくなった場合に親クラスから帯域を借りるか否かの設定
  - on.....借りる
  - off.....借りない
- *maxburst*.....連続送信できる最大バイト数 (1..10000)
- *minburst*.....安定送信中に連続送信できる最大バイト数 (1..10000)
- *packetsize*.....クラスで流れるパケットの平均パケット長 (1..10000)
- *type*
  - priority.....優先制御クラスとして使用することを明示する。

[説明]

指定したクラスの属性を設定する。

[ノート]

bandwidth パラメータで各クラスに割り当てる帯域の合計は、回線全体の帯域を越えてはいけない。回線全体の帯域は、**speed** コマンドで設定される。なお、cbq による帯域制御を行う場合、各クラスに割り当てる帯域は、親クラス以下の値でなければいけない。

queue *interface* **type** コマンドで shaping が指定されている場合は、Dynamic Traffic Control による帯域制御を行うことが可能である。Dynamic Traffic Control を行うためには、*bandwidth* パラメータに「,」(コンマ) でつないだ 2 つの速度を指定することで、保証帯域と上限帯域を設定する。記述順に関係なく、常に値の小さな方が保証帯域となる。なお、保証帯域の合計が回線全体の帯域を越えてはいけない。Dynamic Traffic Control は RTX1100、RTX1500、RTX3000 と SRT100 で利用可能である。

parent/borrow/maxburst/minburst/packetsize パラメータは **queue** *interface* **type** コマンドで cbq が指定されている場合のみ有効である。
cbq において、クラス番号 0 はルートクラスを表す。ルートクラスは仮想的なクラスで、常に 100% の帯域を持ち、デフォルトでは他のクラスの親クラスになっている。ルートクラスに直接パケットを割り振ることはできず、その帯域は他のクラスに貸し出すためにだけ割り当てられている。
帯域が足りなくなった場合に、親クラスから帯域を借りてくる (borrow = on) と設定すると、このクラスの最大速度は親クラスの最大速度まで増えることができる。通常は 100% の帯域を持つルートクラスを親クラスとするので、クラスの帯域は回線速度一杯に広がることができる。この場合、*bandwidth* の設定は、回線が混雑している場合に他のクラスとどの程度の割り合いで帯域を分けるかの目安として使われる。
帯域を借りてこない設定 (borrow = off) だと、このクラスの最大速度は *bandwidth* の値になり、それ以上の帯域を使わなくなる。特定のトラフィックの帯域を制限したい場合に有効である。

type パラメータは **queue** *interface* **type** コマンドで shaping が指定されている場合のみ有効である。インタフェースにおいて帯域制御による速度配分がされている場合でも、*type* パラメータに priority を指定することで、そのクラスは優先制御クラスとなり、帯域制御クラスよりも優先してパケットの転送が行われる。*type* パラメータに priority を指定したクラスが複数ある場合は、クラス番号が大きいほど優先順位が高くなる。*type* パラメータは RTX3000 で指定可能である。

このコマンドが設定されていないクラスには、常に 100% の帯域が割り振られている。そのため、帯域制御の設定をする場合には最低限でも対象としているクラスと、デフォルトクラスの 2 つに関してこのコマンドを設定しなくてはいけない。デフォルトクラスの設定を忘れると、デフォルトクラスに 100% の帯域が割り振られるため、対象とするクラスは常にデフォルトクラスより狭い帯域を割り当てられることになる。
SRT100、RTX2000 では **queue pp class property** は指定できない。

[初期値]

parent = 0
borrow = on
maxburst = 20
minburst = *maxburst* / 10
packetsize = 512

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	SRT100

25.11　動的なクラス変更 (Dynamic Class Control) の設定

[書式]

queue *interface* **class control** *class* [*except ip_address …*] [option=*value …*]
no queue *interface* **class control** *class* [*except ip_address …*]

[設定値]

◦ *interface*..... LAN インタフェース名
◦ *class*..... DCC を有効にするクラス (1..16)
◦ *ip_address*
• IP アドレス ..... サーバーなどの監視対象から除外するホストの IP アドレスを設定する
(空白で区切って複数指定可能、ハイフン「-」を使用して範囲指定も可能)
◦ *option = value* 列

option	*value*	説明
forwarding	reject, 1..16	過剰送信と見なしたトラフィックの転送先のクラス
watch	source	送信元 IP アドレス単位で帯域を監視する
	destination	宛先 IP アドレス単位で帯域を監視する
threshold	占有率 , 秒数	過剰送信と見なす閾値を帯域の占有率と占有時間をカンマ「,」で結び設定する (占有率 1%..100%、秒数 10..86400)
time	infinity, 10..604800	過剰送信と見なしたトラフィックを遮断する時間、または、使用するクラスを変更する時間 (秒)
mode	forced	動作モードを強制制御モードにする
	adaptive	動作モードを適応制御モードにする
trigger	winny	Winny 検知をトリガとして制御を開始する
	share	Share 検知をトリガとして制御を開始する
	masquerade-session	IP マスカレード変換セッション数制限をトリガとして制御を開始する
notice	on	制御されていることを通知する
	off	制御されていることを通知しない

[説明]

指定したインタフェースについて、同一のホストが過剰な送信 / 受信を行い、帯域を逼迫していないか監視をする。
監視対象のインタフェースに適用されている QoS 種別が shaping の場合は、**queue** *interface* **class property** コマンドで設定されたクラス帯域に対する占有率 (クラス帯域に保証値と上限値を指定している場合は保証値に対する占有率) を監視する。QoS 種別が priority の場合は、インタフェース帯域に対する占有率を監視する。監視時は 10 秒毎に占有率を求め、その占有率が指定秒数を超えたときに閾値超過と判定される。
例えば、threshold=70%,30 と設定した場合、帯域使用率 70% 以上である 10 秒間が連続して 3 回続いたときに閾値超過と判定される。

同一のホストから (watch = source)、あるいは、同一のホスト宛て (watch = destination) の過剰送信を検知した場合、そのトラフィックは *forwarding* パラメータに指定されたクラスへ転送され、転送先のクラス設定に従ってパケットの送出が行われる。なお、*forwarding* パラメータに reject を指定した場合、当該トラフィックは遮断される。また、*forwarding* パラメータは省略することも可能で、この場合転送制御は行われないが、threshold を超過しているホストを **show status qos** コマンドから確認することができる。

time パラメータは転送制御が行われる時間を示し、infinity を指定した場合は、無期限に対象のトラフィックの遮断、または、使用クラスの変更がなされる。

mode パラメータは動作モードを指定する。forced を指定した場合は、*threshold* パラメータで指定した占有時間が経過したら直ちに当該フローの制御を実行する。また、*time* パラメータで指定した制御時間が経過したら直ちに当該フローの制御を解除する。adaptive を指定した場合は、*threshold* パラメータで指定した占有時間が経過しても当該クラスの使用帯域が保証帯域の 90% 未満である間は制御を保留する。また、*time* パラメータで指定した制御時間が経過しても当該クラスの使用帯域が保証帯域の 90% 以上である間は制御解除を保留する。
制御が保留されているホストは **show status qos** コマンドで表示されず、制御が保留されている間に threshold の占有率を割ったらその時点で制御は解除される。

mode パラメータは Rev.10.00 系以降で使用可能。

trigger パラメータは制御開始のトリガとなるルーター内部のイベントを指定する。カンマ「,」で区切って併記することができる。*trigger* パラメータは Rev.10.00 系以降で使用可能。

notice パラメータは Dynamic Class Control により制御されていることをホストに通知するかどうかを指定する。on を指定した場合は、当該ホストが制御されてから初めていずれかの http サーバー (ポート番号：80) へ Web アクセスをした時に、Web 画面上にその旨を表示して通知する。
notice パラメータは Rev.10.01 系以降で使用可能。

[ノート]　トラフィックの転送は 1 段のみ可能である。転送先のクラスにも当コマンドが設定されている場合、2 段目の設定は無効となり、トラフィックの 2 重転送は行われない。

[初期値]　*watch* = source
threshold = 70%,30
time = 600
mode = forced
notice = on

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

26. 連携機能

26.1 連携動作を行うか否かの設定

[書式] **cooperation** *type role sw*
no cooperation *type role* [*sw*]

[設定値] ◦ *type* ..... 連携動作タイプ
- bandwidth-measuring .... 回線帯域検出
- load-watch ..... 負荷監視通知

◦ *role* ..... 連携動作での役割
- server ..... サーバー側動作
- client ..... クライアント側動作

◦ *sw*
- on ..... 機能を有効にする
- off ..... 機能を無効にする

[説明] 連携動作の機能毎の動作を設定する。

[初期値] すべての連携動作で off

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

26.2 連携動作で使用するポート番号の設定

[書式] **cooperation port** *port*
no cooperation port [*port*]

[設定値] ◦ *port* ..... ポート番号

[説明] 連携動作で使用する UDP のポート番号を設定する。連携動作で送出されるパケットの送信元ポート番号にこの番号を使用する。またこのポート番号宛のパケットを受信した場合には連携動作に関わるパケットとして処理する。

[初期値] 59410

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

26.3 帯域測定で連携動作を行う相手毎の動作の設定

[書式] **cooperation bandwidth-measuring remote** *id role address* [*option=value*]
no cooperation bandwidth-measuring remote *id* [*role address* [*option=value*]]

[設定値] ◦ *id* ..... 相手先 ID 番号 (1..100)

◦ *role* ..... 連携動作での相手側の役割
- server ..... 相手側がサーバー側動作を行う
- client ..... 相手側がクライアント側動作を行う

◦ *address* ..... 連携動作の相手側 IP アドレス、FQDN または 'any'

◦ *option* ..... オプション
- apply ..... 測定結果を LAN インタフェースの速度設定に反映させるか否か、'on' or 'off'
- port ..... 相手側が使用する UDP のポート番号 (1-65535)
- initial-speed ..... 測定開始値 (64000-100000000)[bit/s]
- interval ..... 定期監視間隔 (60..2147483647)[sec] or 'off'
- retry-interval ..... エラー終了後の再試行までの間隔 (60..2147483647)[sec]
- sensitivity ..... 測定感度、'high', 'middle' or 'low'
- syslog ..... 動作をログに残すか否か、'on' or 'off'
- interface ..... 測定結果を反映させる LAN インタフェース
- class ..... 測定結果を反映させるクラス
- limit-rate ..... 設定値の最大変化割合 (1-10000)[%]
- number ..... 測定に使用するパケット数 (5..100)
- local-address ..... パケット送信時の始点 IP アドレス

[説明] 帯域測定で連携動作を行う相手毎の動作を設定する。

[ノート]　*role* パラメータで client を設定する場合には、オプションは port と syslog だけが設定できる。server を設定する場合には全てのオプションが設定できる。

連携動作の相手側設定として any を指定できるのは、 *role* パラメータで client を設定した場合のみである。

applyオプションが 'on' の場合、帯域測定の結果を相手先に向かうLANインタフェースの **speed lan** コマンドの設定値に上書きする。*class* オプションに値が設定されている場合には、**queue lan class property** コマンドの *bandwidth* パラメータに測定結果が反映される。

initial-speed オプションでは初期状態で測定を開始する速度を設定できる。パラメータの後ろに 'k' または 'M' をつけると、それぞれ kbit/s、Mbit/s として扱われる。

interval オプションでは、帯域測定が正常終了した後、帯域に変化がないか定期的に確認測定する間隔を設定できる。'off' を指定した場合には測定終了後の定期的な確認測定を行わない。

retry-interval オプションでは、帯域測定が相手先からの応答がなかったり測定値が許容範囲を越えたなど、何らかの障害で正しい測定ができなかった場合の再試行までの時間を設定できる。ただし、網への負荷等を考慮すると正常に動作できない状況でむやみに短時間間隔で試行を繰り返すべきではない。正常に測定できない原因を回避することが先決である。

number オプションでは、測定に使用するパケット数を設定できる。パケット間隔のゆらぎが大きい環境ではこの数を多くすることで、より安定した結果が得られる。ただし測定に使用するパケットの数が増えるため測定パケットが他のデータ通信に与える影響も大きくなる可能性がある。

sensitivity オプションでは、測定感度を変更することができる。パケット間隔のゆらぎが大きかったりパケットロスのある環境では、測定感度を鈍くすることで、頻繁な設定変更を抑制したり測定完了までの時間を短縮することができる。

interface オプションでLAN インタフェースが設定されている場合には、そのLAN インタフェースの **speed lan** コマンドに測定結果が反映される。*class* オプションに値が設定されている場合には **queue lan class property** コマンドの *bandwidth* パラメータに測定結果が反映される。

class オプションは帯域制御機能が実装されている機種でのみ利用できる。

limit-rate オプションは、設定値の急激な変動をある割合内に抑えたい場合に設定する。直前の測定結果と今回の測定結果に大きな差がある場合、今回の測定結果そのものではなく、この limit-rate に応じた値を今回の設定値として採用する。

local-address オプションでは、送信パケットの始点 IP アドレスを設定できる。設定がない場合、インタフェースに付与された IP アドレスを使用する。

local-address オプションは、Rev.8.03.60 以降から使用可能。

[初期値]　*apply = on*
port = 59410
initial-speed = 10000000
interval = 3600
retry-interval=3600
sensitivity = high
syslog = off
interface 設定なし
class 設定なし
limit-rate 設定なし
number=30
local-address 設定なし

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

26.4　負荷監視通知で連携動作を行う相手毎の動作の設定

[書式]　**cooperation load-watch remote** *id role address* [*option=value*]
no cooperation load-watch remote *id* [*role address* [*option=value*]]

[設定値]
- *id*..... 相手先 ID 番号 (1..100)
- *role*..... 連携動作での相手側の役割
  - server..... 相手側がサーバー側動作を行う
  - client..... 相手側がクライアント側動作を行う
- *address*..... 連携動作の相手側 IP アドレス、FQDN または 'any'
- *option*..... オプション
  - trigger ..... サーバー動作として、クライアントに通知を行う条件のトリガ定義番号 (1-65535)、',' で区切って複数の指定が可能、相手側動作をクライアントに設定する時にのみ可能
  - control..... クライアント動作として、サーバーから通知を受けた時の制御動作定義番号 (1-65535)、相手側動作をサーバーに設定する時にのみ可能
  - port ..... 相手側が使用する UDP のポート番号 (1-65535)
  - syslog ..... 動作をログに残すか否か、'on' or 'off'
  - apply..... 負荷監視通知の結果を動作に反映させるかどうか、'on' or 'off'
  - register ..... サーバーに対する登録パケットを送るか否か、'on' or 'off'
  - register-interval.... クライアントからサーバーへの登録パケット送信間隔、(1..2147483647)[sec]
  - register-time ..... サーバーでのクライアント登録情報保持時間、(1..2147483647)[sec]
  - name ..... 相手側を識別する名前 (最大 16 文字)
  - local-address ..... パケット送信時の始点 IP アドレス

[説明]　負荷監視通知で連携動作を行う相手毎の動作を設定する。

[ノート]　trigger オプションを利用できるのは *role* パラメータで client を設定する場合であり、control オプションが利用できるのは *role* パラメータで server を設定する場合である。

サーバー側で any を指定した場合、サーバー側にクライアントの存在を通知登録するためにクライアント側では register=on を設定する必要がある。

name オプションを設定した場合、サーバーとクライアントの双方で同じ名前を設定した場合にのみ機能する。

local-address オプションでは、送信パケットの始点 IP アドレスを設定できる。設定がない場合、インタフェースに付与された IP アドレスを使用する。

複数のトリガを設定した場合、抑制要請の送信タイミングはそれぞれのトリガで個別に検出される。それらの送信タイミングが異なる時には抑制要請はそれぞれのタイミングで個別に送られ、送信タイミングが一致する時にはひとつの抑制要請となる。
相手先に一度抑制解除が送られた後は、次に抑制要請を送信するまで抑制解除は送信しない。
抑制要請を送信していないトリガ条件が抑制解除条件を満たしても抑制解除通知は送信しない。
抑制制御を行っている最中に相手先情報が削除されると、制御対象のインタフェースの速度はその時点の設定が保持される。

local-address オプションは、Rev.8.03.60 以降から使用可能。

[初期値]　port=59410
syslog=off
apply=on
register=off
register-interval=1200
register-time=3600
local-address 設定なし

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

26.5　負荷監視サーバーとしての動作トリガの設定

[書式]

cooperation load-watch trigger *id point* high=*high* [*, count*] low=*low* [*, count*] [*option=vallue*]
no cooperation load-watch trigger *id* [*point* high=*high* [*, count*] low=*low* [*, count*] [*option=vallue*]]

[設定値]

- *id* ..... 相手先 ID 番号 (1-100)
- *point* ..... 負荷監視対象ポイント
  - cpu load ..... 単位時間間隔で CPU 負荷率を監視する値は % で指定する
  - *interface* receive ..... インタフェースでの単位時間当たりの受信量を監視する
    値は 1 秒あたりのビット数で指定する
    - *interface* ..... インタフェース名 (LAN, TUNNEL)
  - *interface* overflow ..... LAN インタフェースでの単位時間当たりの受信オーバーフロー数と受信
    バッファエラー数の増加を監視し、値は回数で指定する
    - *interface* ..... LAN インタフェース名
  - *interface* [*class*] transmit ..... インタフェースでの単位時間当たりの送信量を監視する
    値は 1 秒あたりのビット数で指定する
    - *interface* ..... インタフェース名 (LAN, TUNNEL)
    - *class* ..... クラス番号 (LAN インタフェースの場合)
- *high* ..... 高負荷検出閾値
- *low* ..... 負荷減少検出閾値
- *count* ..... 通知を送出するに至る検出回数 (1-100)、省略時は 3
- *option* ..... オプション
  - interval ..... 監視する間隔 (1-65535)[*sec*]、省略時は 10[*sec*]
  - syslog ..... 動作をログに残すか否か、'on' or 'off'、省略時は 'off'

[説明]

機器の負荷を検出して相手側にトラフィック抑制要請を送出する条件を設定する。監視対象ポイントの負荷を単位時間毎に監視し、*high* に設定された閾値を上回ることを *count* 回数続けて検出すると抑制要請を送出する。この状態で閾値を上回る高負荷状態が続く限り、*count* の間隔で抑制要請を送出し続ける。
同様に、*low* に設定された閾値を *count* 回数続けて下回って検出すると抑制解除を送出する。抑制解除は同じ相手に対して連続して送出されない。
class オプションは帯域制御機能が実装されている機種でのみ利用できる。

[ノート]

閾値を決定する際の参考値として、**show environment** や **show status lan** で表示される情報のほか、syslog オプションによりログに表示される値も利用できる。

[設定例]

```
# cooperation load-watch trigger 1 cpu load high=80 low=30
```

一定間隔で CPU の負荷率を観測し、負荷率が 80% 以上であることが連続 3 回測定されたら抑制要請を送り、その後 30% 以下であることが 3 回続けて観測されたら抑制解除を送る。

```
# cooperation load-watch trigger 2 lan2 receive high=80m,5 low=50m,1
```

単位時間内での LAN2 からの受信バイト数から受信速度を求め、その値が 80[Mbit/s] 以上であることが連続 5 回あれば抑制要請を送り、その後 50[Mbit/s] 以下であることが 1 度でも観測されれば抑制解除を送る。

```
# cooperation load-watch trigger 3 lan2 overflow high=2,1 low=0,5
```

単位時間内での LAN2 での受信オーバーフロー数の増加を監視し、2 回検出されることが 1 度でもあれば抑制要請を送り、検出されないことが 5 回続けば抑制解除を送る。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

26.6　負荷監視クライアントとしての動作の設定

[書式]　**cooperation load-watch control** *id* high=*high* [raise=*raise*] low=*low* [lower=*lower*] [interval=*interval*]
no cooperation load-watch control *id* [high=*high* [raise=*raise*] low=*low* [lower=*lower*] [interval=*interval*]]

[設定値]
- *id*..... 相手先 ID 番号 (1-100)
- *high*..... bit/sec、帯域上限値
- *raise*..... %、帯域上限値に達していない限り、定時間毎にこの割合だけ帯域を増加させる
  省略時は 5%
- *low*..... bit/sec、帯域下限値
- *lower*..... %、帯域下限値に達していない限り、抑制要請を受けた時に現在の帯域からこの割合だけ送出帯域を減少させる
  省略時は 30%
- *interval*..... 帯域を増加させる間隔 (1-65535)[sec]、省略時は 10[sec]

[説明]　トラフィック抑制要請を受けた場合の動作を設定する。帯域は *high* に設定された帯域と *low* に設定された帯域との間で制御される。

抑制要請を受信すると、送出帯域は現状の運用帯域値の *lower* の値に応じた割合に減少する。帯域が *high* に達していない限り、*raise* の値に応じて運用帯域は増加する。

トラフィック抑制解除を受信した場合には、帯域は *high* に設定された帯域に増加する。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

26.7　連携動作の手動実行

[書式]　**cooperation** *type* **go** *id*

[設定値]
- *type*..... 連携動作タイプ
  - bandwidth-measuring .... 回線帯域検出
  - load-watch ..... 負荷監視通知
- *id*..... 相手先 ID 番号 (1-100)

[説明]　手動で連携動作を実行する。

[ノート]　測定結果がコンソールに表示される。

インタフェース速度の設定で回線帯域検出の値を使用するように設定されている場合には、この実行結果の値も設定への反映の対象となる。

load-watch を指定した場合は、相手の役割がクライアントである相手にのみ有効である。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

27. OSPF

OSPFはインテリアゲートウェイプロトコルの一種で、グラフ理論をベースとしたリンク状態型の動的ルーティングプロトコルである。

27.1　OSPFの有効設定

[書式]　**ospf configure refresh**

[設定値]　なし

[説明]　OSPF関係の設定を有効にする。OSPF関係の設定を変更したら、ルーターを再起動するか、あるいはこのコマンドを実行しなくてはいけない。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

27.2　OSPFの使用設定

[書式]　**ospf use** *use*
no ospf use [*use*]

[設定値]　◦ *use*
- on.....OSPFを使用する
- off.....OSPFを使用しない

[説明]　OSPFを使用するか否かを設定する。

[ノート]　いずれかのインタフェースにセカンダリアドレスを割り当てた場合、OSPFを使用することはできない。

[初期値]　off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

27.3　OSPFによる経路の優先度設定

[書式]　**ospf preference** *preference*
no ospf preference [*preference*]

[設定値]　◦ *preference*.....OSPFによる経路の優先度(1以上の数値)

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

[ノート]　静的経路の優先度は10000で固定である。

[初期値]　2000

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

27.4　OSPFのルーターID設定

[書式]　**ospf router id** *router-id*
no ospf router id [*router-id*]

[設定値]　◦ *router_id*.....IPアドレス

[説明]　OSPFのルーターIDを指定する。

[初期値]　LANインタフェースの中でインタフェースの若いものから順にサーチして、プライマリIPアドレスがついているインタフェースのIPアドレスをルーターIDとする

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

27.5 OSPF で受け取った経路をルーティングテーブルに反映させるか否かの設定

[書式] **ospf export from ospf** filter *filter_num...*
no ospf export from ospf [filter *filter_num...*]

[設定値] ◦ *filter_num* ..... **ospf export filter** コマンドのフィルタ番号

[説明] OSPF で受け取った経路をルーティングテーブルに反映させるかどうかを設定する。指定したフィルタに一致する経路だけがルーティングテーブルに反映される。コマンドが設定されていない場合には、すべての経路がルーティングテーブルに反映される。

[ノート] このコマンドは OSPF のリンク状態データベースには影響を与えない。つまり、OSPF で他のルーターと情報をやり取りする動作としては、このコマンドがどのように設定されていても変化は無い。OSPF で計算した経路が、実際にパケットをルーティングするために使われるかどうかだけが変わる。
Rev.8.01.18 以降で使用可能。

[初期値] すべての経路がルーティングテーブルに反映される

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

27.6 外部プロトコルによる経路導入

[書式] **ospf import from** *protocol* [filter *filter_num...*]
no ospf import from [*protocol* [filter *filter_num...*]]

[設定値] ◦ *protocol*..... OSPF の経路テーブルに導入する外部プロトコル
- static ..... 静的経路
- rip..... RIP
- bgp ..... BGP

◦ *filter_num* ..... フィルタ番号

[説明] OSPF の経路テーブルに外部プロトコルによる経路を導入するかどうかを設定する。導入された経路は外部経路として他の OSPF ルーターに広告される。

*filter_num*は **ospf import filter** コマンドで定義したフィルタ番号を指定する。外部プロトコルから導入されようとする経路は指定したフィルタにより検査され、フィルタに該当すればその経路は OSPF に導入される。該当するフィルタがない経路は導入されない。また、filter キーワード以降を省略した場合には、すべての経路が OSPF に導入される。

経路を広告する場合のパラメータであるメトリック値、メトリックタイプ、タグは、フィルタの検査で該当した **ospf import filter** コマンドで指定されたものを使う。filter キーワード以降を省略した場合には、以下のパラメータを使用する。
- metric = 1
- type = 2
- tag = 1

[初期値] 外部経路は導入しない

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

27.7　OSPF で受け取った経路をどう扱うかのフィルタの設定

[書式]　**ospf export filter** *filter_num* [*nr*] *kind ip_address/mask...*
no ospf export filter *filter_num* [*...*]

[設定値]
- *filter_num*.....フィルタ番号
- *nr*.....フィルタの解釈の方法
  - not.....フィルタに該当しない経路を導入する
  - reject .....フィルタに該当した経路を導入しない
  - 省略時は、フィルタに該当した経路を導入する
- *kind*.....フィルタ種別
  - include.....指定したネットワークアドレスに含まれる経路 (ネットワークアドレス自身を含む)
  - refines .....指定したネットワークアドレスに含まれる経路 (ネットワークアドレス自身を含まない)
  - equal .....指定したネットワークアドレスに一致する経路
- *ip_address/mask*.....ネットワークアドレスをあらわす IP アドレスとマスク長

[説明]　OSPF により他の OSPF ルーターから受け取った経路を経路テーブルに導入する際に適用するフィルタを定義する。このコマンドで定義したフィルタは、**ospf export from** コマンドの filter 項で指定されてはじめて効果を持つ。
ip_address/mask では、ネットワークアドレスを設定する。これは、複数設定でき、経路の検査時にはそれぞれのネットワークアドレスに対して検査を行う。

nr が省略されている場合には、一つでも該当するフィルタがある場合には経路が導入される。
not 指定時には、すべての検査でフィルタに該当しなかった場合に経路が導入される。reject 指定時には、一つでも該当するフィルタがある場合には経路が導入されない。

kind では、経路の検査方法を設定する。
- include.....ネットワークアドレスと一致する経路および、ネットワークアドレスに含まれる経路が該当となる
- refines .....ネットワークアドレスに含まれる経路が該当となるが、ネットワークアドレスと一致する経路が含まれない
- equal .....ネットワークアドレスに一致する経路だけが該当となる

[ノート]　*nr* パラメータの reject キーワードは Rev.8.02.02 以降で使用可能。

not 指定のフィルタを **ospf export from** コマンドで複数設定する場合には注意が必要である。not 指定のフィルタに合致するネットワークアドレスは、そのフィルタでは導入するかどうかが決定しないため、次のフィルタで検査されることになる。そのため、例えば、以下のような設定ではすべての経路が導入されることになり、フィルタの意味が無い。

```
ospf export from ospf filter 1 2
ospf export filter 1 not equal 192.168.1.0/24
ospf export filter 2 not equal 192.168.2.0/24
```

1 番のフィルタでは、192.168.1.0/24 以外の経路を導入し、2 番のフィルタで 192.168.2.0/24 以外の経路を導入している。つまり、経路 192.168.1.0/24 は 2 番のフィルタにより、経路 192.168.2.0/24 は 1 番のフィルタにより導入されるため、導入されない経路は存在しない。

経路 192.168.1.0/24 と経路 192.168.2.0/24 を導入したくない場合には以下のような設定を行う必要がある。

```
ospf export from ospf filter 1
ospf export filter 1 not equal 192.168.1.0/24 192.168.2.0/24
```

あるいは、

```
ospf export from ospf filter 1 2 3
ospf export filter 1 reject equal 192.168.1.0/24
ospf export filter 2 reject equal 192.168.2.0/24
ospf export filter 3 include 0.0.0.0/0
```

Rev.8.01.18 以降で使用可能。

[初期値]　フィルタは設定されていない

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	RT250i	RT107e	SRT100

27.8 外部経路導入に適用するフィルタ定義

[書式] **ospf import filter** *filter_num* [*nr*] *kind ip_address/mask*...[*parameter*...]
no ospf import filter *filter_num* [[not] *kind ip_address/mask*...[*parameter*...]]

[設定値]
- *filter_num* ..... フィルタ番号
- *nr* ..... フィルタの解釈の方法
  - not ..... フィルタに該当しない経路を広告する
  - reject..... フィルタに該当した経路を広告しない
  - 省略時は、フィルタに該当した経路を広告する
- *kind*
  - include..... 指定したネットワークアドレスに含まれる経路 (ネットワークアドレス自身を含む)
  - refines..... 指定したネットワークアドレスに含まれる経路 (ネットワークアドレス自身は含まない)
  - equal ..... 指定したネットワークアドレスに一致する経路
- *ip_address/mask* ..... ネットワークアドレスをあらわす IP アドレスとマスク長
- *parameter*..... 外部経路を広告する場合のパラメータ
  - metric ..... メトリック値 (0..16777215)
  - type..... メトリックタイプ (1..2)
  - tag..... タグの値 (0..4294967295)

[説明] OSPF の経路テーブルに外部経路を導入する際に適用するフィルタを定義する。このコマンドで定義したフィルタは、**ospf import from** コマンドの filter 項で指定されてはじめて効果を持つ。
ip_address/mask では、ネットワークアドレスを設定する。これは、複数設定でき、経路の検査時にはそれぞれのネットワークアドレスに対して検査を行い、1 つでも該当するものがあればそれが適用される。

nr が省略されている場合には、一つでも該当するフィルタがある場合には経路を広告する。not 指定時には、すべての検査でフィルタに該当しなかった場合に経路を広告する。reject 指定時には、一つでも該当するフィルタがある場合には経路を広告しない。

kind では、経路の検査方法を設定する。
- include..... ネットワークアドレスと一致する経路および、ネットワークアドレスに含まれる経路が該当となる
- refines..... ネットワークアドレスに含まれる経路が該当となるが、ネットワークアドレスと一致する経路が含まれない
- equal ..... ネットワークアドレスに一致する経路だけが該当となる

kind の前に not キーワードを置くと、該当 / 非該当の判断が反転する。例えば、not equal では、ネットワークアドレスに一致しない経路が該当となる。

parameter では、該当した経路を OSPF の外部経路として広告する場合のパラメータとして、メトリック値、メトリックタイプ、タグがそれぞれ metric、type、tag により指定できる。これらを省略した場合には、以下の値が採用される。
- metric = 1
- type = 2
- tag = 1

[ノート] *nr* パラメータの reject キーワードは Rev.8.02.02 以降で使用可能。

not 指定のフィルタを **ospf import from** コマンドで複数設定する場合には注意が必要である。not 指定のフィルタに合致するネットワークアドレスは、そのフィルタでは導入するかどうかが決定しないため、次のフィルタで検査されることになる。そのため、例えば、以下のような設定ではすべての経路が広告されることになり、フィルタの意味が無い。

```
ospf import from static filter 1 2
ospf import filter 1 not equal 192.168.1.0/24
ospf import filter 2 not equal 192.168.2.0/24
```

1 番のフィルタでは、192.168.1.0/24 以外の経路を広告し、2 番のフィルタで 192.168.2.0/24 以外の経路を広告している。つまり、経路 192.168.1.0/24 は 2 番のフィルタにより、経路 192.168.2.0/24 は 1 番のフィルタにより広告されるため、広告されない経路は存在しない。

経路 192.168.1.0/24 と経路 192.168.2.0/24 を広告したくない場合には以下のような設定を行う必要がある。

```
ospf import from static filter 1
ospf import filter 1 not equal 192.168.1.0/24 192.168.2.0/24
```

あるいは、

```
ospf import from static filter 1 2 3
ospf import filter 1 reject equal 192.168.1.0/24
ospf import filter 2 reject equal 192.168.2.0/24
ospf import filter 3 include 0.0.0.0/0
```

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

27.9　OSPF エリア設定

[書式]

ospf area *area* [auth=*auth*] [stub [cost=*cost*]]
no ospf area *area* [auth=*auth*] [stub [cost=*cost*]]

[設定値]

◦ *area*
- backbone.....バックボーンエリア
- 1 以上の数値 .....非バックボーンエリア
- IP アドレス表記 (0.0.0.0 は不可) 非バックボーンエリア

◦ *auth*
- text..... プレーンテキスト認証
- md5.....MD5 認証

◦ *cost* .....0 以上の数値

◦ stub [cost=*cost*] .....スタブエリアであることを指定する。*cost* は 0 以上の数値で、エリアボーダルーターがエリア内に広告するデフォルト経路のコストとして使われる。*cost* を指定しないとデフォルト経路の広告は行われない。

[説明]

OSPF エリアを設定する。

[初期値]

認証は行わない
スタブエリアではない

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

27.10　エリアへの経路広告

[書式]

ospf area network *area network/mask* [restrict]
no ospf area network *area network/mask* [restrict]

[設定値]

◦ *area*
- backbone.....バックボーンエリア
- 1 以上の数値 .....非バックボーンエリア
- IP アドレス表記 (0.0.0.0 は不可) 非バックボーンエリア

◦ *network* .....IP アドレス

◦ *mask* ..... ネットマスク長

[説明]

エリア境界ルーターが他のエリアに経路を広告する場合に、このコマンドで指定したネットワークの範囲内の経路は単一のネットワーク経路として広告する。restrict キーワードが指定された場合には、範囲内の経路は要約した経路も広告しない。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

27.11　スタブ的接続の広告

[書式]

ospf area stubhost *area host* [cost *cost*]
no ospf area stubhost *area host*

[設定値]

◦ *area*
- backbone.....バックボーンエリア
- 1 以上の数値 .....非バックボーンエリア
- IP アドレス表記 (0.0.0.0 は不可) 非バックボーンエリア

◦ *host*.....IP アドレス

◦ *cost* ..... 1 以上の数値

[説明]

指定したホストが指定したコストでスタブ的に接続されていることをエリア内に広告する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

27.12 仮想リンク設定

[書式] **ospf virtual-link** *router_id area [parameters...]*
no ospf virtual-link *router_id [area [parameters...]]*

[設定値]
◦ *router_id* ..... 仮想リンクの相手のルーター ID
◦ *area*
- 1 以上の数値 ..... 非バックボーンエリア
- IP アドレス表記 (0.0.0.0 は不可) 非バックボーンエリア

◦ *parameters*..... NAME=VALUE の列

[説明] 仮想リンクを設定する。仮想リンクは *router_id* で指定したルーターに対して、 *area* で指定したエリアを経由して設定される。*parameters* では、仮想リンクのパラメータが設定できる。パラメータは NAME=VALUE の形で指定され、以下の種類がある。

NAME	VALUE	説明
retransmit-interval	秒数	LSA を連続して送る場合の再送間隔を秒単位で設定する。
transmit-delay	秒数	リンクの状態が変わってから LSA を送信するまでの時間を秒単位で設定する。
hello-interval	秒数	HELLO パケットの送信間隔を秒単位で設定する。
dead-interval	秒数	相手から HELLO を受け取れない場合に、相手がダウンしたと判断するまでの時間を秒単位で設定する。
authkey	文字列	プレーンテキスト認証の認証鍵を表す文字列を設定する。 KEY は文字列で、8 文字以内。
md5key	ID, 文字列	MD5 認証の認証鍵を表す ID と鍵文字列を設定する。ID は十進数で 0 ～ 255、KEY は文字列で 16 文字以内。MD5 認証鍵は 2 つまで設定できる。複数の MD5 認証鍵が設定されている場合には、送信パケットは同じ内容のパケットを複数個、それぞれの鍵による認証データを付加して送信する。受信時には鍵 ID が一致する鍵が比較対象となる。
md5-sequence-mode	second	送信時刻の秒数
	increment	単調増加

[ノート]
◦ hello-interval/dead-interval について
hello-interval と dead-interval の値は、そのインタフェースから直接通信できるすべての近隣ルーターとの間で同じ値でなくてはいけない。これらのパラメータの値が設定値とは異なっている OSPF HELLO パケットを受信した場合には、それは無視される。

◦ MD5 認証鍵について
MD5 認証鍵を複数設定できる機能は、MD5 認証鍵を円滑に変更するためである。
通常の運用では、MD5 認証鍵は 1 つだけ設定しておく。MD5 認証鍵を変更する場合は、まず 1 つのルーターで新旧の MD5 認証鍵を 2 つ設定し、その後、近隣ルーターで MD5 認証鍵を新しいものに変更していく。そして、最後に 2 つの鍵を設定したルーターで古い鍵を削除すれば良い。

Rev.7.00.26 だけは、md5-sequence-mode の設定は increment の動作となっている。それ以外のリビジョンでは second の動作となっている。

[初期値]
router_id, area = なし
retransmit-interval = 5 秒
transmit-delay = 1 秒
hello-interval = 10 秒
dead-interval = 40 秒
authkey = なし
md5key = なし
md5-sequence-mode = second

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

27.13　指定インタフェースの OSPF エリア設定

[書式]

ip *interface* **ospf area** *area* [*parameters...*]
ip pp ospf area *area* [*parameters...*]
ip tunnel ospf area *area* [*parameters...*]
no ip *interface* **ospf area** [*area* [*parameters...*]]
no ip pp ospf area [*area* [*parameters...*]]
no ip tunnel ospf area [*area* [*parameters...*]]

[設定値]

◦ *interface*.....LAN インタフェース名、LOOPBACK インタフェース名

◦ *area*
- backbone.....バックボーンエリア
- 1 以上の数値 .....非バックボーンエリア
- IP アドレス表記 (0.0.0.0 は不可) 非バックボーンエリア

◦ *parameters*.....NAME=VALUE の列

[説明]

指定したインタフェースの属する OSPF エリアを設定する。
NAME パラメータの type はインタフェースのネットワークがどのようなタイプであるかを設定する。
parameters では、リンクパラメータを設定する。パラメータは NAME=VALUE の形で指定され、以下の種類がある。

NAME	VALUE	説明
type	broadcast	ブロードキャスト
	point-to-point	ポイント・ポイント
	point-to-multi-point	ポイント・マルチポイント
	non-broadcast	NBMA
passive		インタフェースに対して、OSPF パケットを送信しない。該当インタフェースに他の OSPF ルーターがいない場合に設定する。
cost	コスト	インタフェースのコストを設定する。初期値は、インタフェースの種類と回線速度によって決定される。LAN インタフェースの場合は 1、PP インタフェースの場合は、バインドされている回線の回線速度を S[kbit/s] とすると、以下の計算式で決定される。例えば、64kbit/s の場合は 1562、1.536Mbit/s の場合には 65 となる。(0 .. 65535) ・COST = 100000 / S TUNNEL インタフェースの場合は、1562 がデフォルト値となる。
priority	優先度	指定ルーターの選択の際の優先度を設定する。PRIORITY 値が大きいルーターが指定ルーターに選ばれる。0 を設定すると、指定ルーターに選ばれなくなる。(0 .. 255)
retransmit-interval	秒数	LSA を連続して送る場合の再送間隔を秒単位で設定する。
transmit-delay	秒数	リンクの状態が変わってから LSA を送信するまでの時間を秒単位で設定する。
hello-interval	秒数	HELLO パケットの送信間隔を秒単位で設定する。
dead-interval	秒数	近隣ルーターから HELLO を受け取れない場合に、近隣ルーターがダウンしたと判断するまでの時間を秒単位で設定する。
poll-interval	秒数	非ブロードキャストリンクでのみ有効なパラメータで、近隣ルーターがダウンしている場合の HELLO パケットの送信間隔を秒単位で設定する。
authkey	文字列	プレーンテキスト認証の認証鍵を表す文字列を設定する。文字列で、8 文字以内。
md5key	ID, 文字列	MD5 認証の認証鍵を表す ID と鍵文字列を設定する。ID は十進数で 0 ～255、文字列は 16 文字以内。MD5 認証鍵は 2 つまで設定できる。複数の MD5 認証鍵が設定されている場合には、送信パケットは同じ内容のパケットを複数個、それぞれの鍵による認証データを付加して送信する。受信時には鍵 ID が一致する鍵が比較対象となる。
md5-sequence-mode	second increment	送信時刻の秒数 単調増加

LOOPBACK インタフェースに設定する場合は、*type* パラメータでインタフェースタイプを、*cost* パラメータでインタフェースのコストを指定できる。LOOPBACK インタフェースのタイプで指定できるのは、以下の 2 種類だけとなる。

NAME	VALUE	広告される経路の種類	OSPF 的なインタフェースの扱い	
			タイプ	状態
type	loopback	LOOPBACK インタフェースの IP アドレスのみのホスト経路	point-to-point	Loopback
	loopback-network	LOOPBACK インタフェースの implicit なネットワーク経路	NBMA	DROther

[ノート]

◦ NAME パラメータの type について
NAME パラメータの type として、LAN インタフェースは broadcast のみが許される。PP インタフェースは、PPP を利用する場合は point-to-point、フレームリレーを利用する場合は point-to-multipoint と non-broadcast のいずれかが設定できる。
フレームリレーで non-broadcast (NBMA) を利用する場合には、フレームリレーの各拠点間のすべての間で PVC が設定されており、FR に接続された各ルーターは他のルーターと直接通信できるような状態、すなわちフルメッシュになっていなくてはならない。また、non-broadcast では近隣ルーターを自動的に認識することができないため、すべての近隣ルーターを **ip pp ospf neighbor** コマンドで設定する必要がある。
point-to-multipoint を利用する場合には、フレームリレーの PVC はフルメッシュである必要はなく、一部が欠けたパーシャルメッシュでも利用できる。近隣ルーターは InArp を利用して自動的に認識するため、InArp が必須となる。RT では InArp を使うかどうかは **fr inarp** コマンドで制御できるが、デフォルトでは InArp を使用する設定になっているので、**ip pp address** コマンドでインタフェースに適切な IP アドレスを与えるだけでよい。

point-to-multipoint と設定されたインタフェースでは、**ip pp ospf neighbor** コマンドの設定は無視される。point-to-multipoint の方が non-broadcast よりもネットワークの制約が少なく、また設定も簡単だが、その代わりに回線を流れるトラフィックは大きくなる。non-broadcast では、broadcast と同じように指定ルーターが選定され、HELLO などの OSPF トラフィックは各ルーターと指定ルーターの間だけに限定されるが、point-to-multipoint ではすべての通信可能なルーターペアの間に point-to-point リンクがあるという考え方なので、OSPF トラフィックもすべての通信可能なルーターペアの間でやりとりされる。

◦ passive について
passive は、インタフェースが接続しているネットワークに他の OSPF ルーターが存在しない場合に指定する。passive を指定しておくと、インタフェースから OSPF パケットを送信しなくなるので、無駄なトラフィックを抑制したり、受信側で誤動作の原因になるのを防ぐことができる。

LAN インタフェース (type=broadcast であるインタフェース) の場合には、インタフェースが接続しているネットワークへの経路は、**ip** *interface* **ospf area** コマンドを設定していないと他の OSPF ルーターに広告されない。そのため、OSPF を利用しないネットワークに接続する LAN インタフェースに対しては、passive を付けた **ip** *interface* **ospf area** コマンドを設定しておくことでそのネットワークでは OSPF を利用しないまま、そこへの経路を他の OSPF ルーターに広告することができる。

PP インタフェースに対して **ip** *interface* **ospf area** コマンドを設定していない場合は、インタフェースが接続するネットワークへの経路は外部経路として扱われる。外部経路なので、他の OSPF ルーターに広告するには **ospf import** コマンドの設定が必要である。

◦ hello-interval/dead-interval について
hello-interval/dead-interval の値は、そのインタフェースから直接通信できるすべての近隣ルーターとの間で同じ値でなくてはいけない。これらのパラメータの値が設定値とは異なっている OSPF HELLO パケットを受信した場合には、それは無視される。

◦ MD5 認証鍵について
MD5 認証鍵を複数設定できる機能は、MD5 認証鍵を円滑に変更するためである。
通常の運用では、MD5 認証鍵は 1 つだけ設定しておく。MD5 認証鍵を変更する場合は、まず 1 つのルーターで新旧の MD5 認証鍵を 2 つ設定し、その後、近隣ルーターで MD5 認証鍵を新しいものに変更していく。そして、最後に 2 つの鍵を設定したルーターで古い鍵を削除すれば良い。
RT250i では **ip tunnel ospf area** コマンドは使用できない。
LOOPBACK インタフェースを指定できるのは Rev.8.03 以降のリビジョンである。

[初期値]

area = インタフェースは OSPF エリアに属していない
type = broadcast (LAN インタフェース設定時)
= point-to-point (PP インタフェース設定時)
= loopback (LOOPBACK インタフェース設定時)
passive = インタフェースは passive ではない
cost = 1 (LAN インタフェース、LOOPBACK インタフェース設定時)、pp は回線速度に依存
priority = 1
retransmit-interval = 5 秒
transmit-delay = 1 秒
hello-interval= 10 秒 (type = broadcast 設定時)
= 10 秒 (point-to-point 設定時)
= 30 秒 (non-broadcast 設定時)
= 30 秒 (point-to-multipoint 設定時)
dead-interval = hello-interval の 4 倍
poll-interval = 120 秒
authkey = なし
md5key = なし
md5-sequence-mode = second

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

27.14　非ブロードキャスト型ネットワークに接続されている OSPF ルーターの指定

[書式]
ip *interface* **ospf neighbor** *ip_address* [eligible]
ip pp ospf neighbor *ip_address* [eligible]
ip tunnel ospf neighbor *ip_address* [eligible]
no ip *interface* **ospf neighbor** *ip_address* [eligible]
no ip pp ospf neighbor *ip_address* [eligible]
no ip tunnel ospf neighbor *ip_address* [eligible]

[設定値]
◦ *interface*.....LAN インタフェース名
◦ *ip_address*.....近隣ルーターの IP アドレス

[説明]
非ブロードキャスト型のネットワークに接続されている OSPF ルーターを指定する。
eligible キーワードが指定されたルーターは指定ルーターとして適格であることを表す。

[ノート]
RT250i では **ip tunnel ospf neighbor** コマンドは使用できない。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

27.15　スタブが存在する時のネットワーク経路の扱いの設定

[書式]
ospf merge equal cost stub *merge*
no ospf merge equal cost stub

[設定値]
◦ *merge*
- on.....イコールコストになるスタブを他の経路とマージする
- off.....イコールコストになるスタブを他の経路とマージしない

[説明]
他の経路と同じコストになるスタブをどう扱うかを設定する。
on の場合にはスタブへの経路を他の経路とマージして、イコールコストマルチパス動作をする。これは、RFC2328 の記述に沿うものである。
off の場合にはスタブへの経路を無視する。

[ノート]
Rev.7.01.16 以前は off
Rev.7.01.17 以降は on

[初期値]
on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	RT250i	RT107e	SRT100

27.16　OSPF の状態遷移とパケットの送受信をログに記録するか否かの設定

[書式]
ospf log *log* [*log...*]
no ospf log [*log...*]

[設定値]
◦ *log*
- interface.....インタフェースの状態遷移
- neighbor.....近隣ルーターの状態遷移
- packet.....送受信したパケット

[説明]
指定した種類のログを INFO レベルで記録する。

[ノート]
Rev.7.01.41、Rev.8.01.18 以降で使用可能。

[初期値]
OSPF のログは記録しない。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	RT250i	RT107e	SRT100

28. BGP

28.1 BGP の起動の設定

[書式] **bgp use** *use*
no bgp use [*use*]

[設定値] ◦ *use*
- on..... 起動する
- off..... 起動しない

[説明] BGP を起動するか否かを設定する。

[ノート] いずれかのインタフェースにセカンダリアドレスを割り当てた場合、BGP を使用することはできない。

[初期値] off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

28.2 経路の集約の設定

[書式] **bgp aggregate** *ip_address/mask* filter *filter_num …*
no bgp aggregate *ip_address/mask* [filter *filter_num …]*

[設定値] ◦ *ip_address/mask*
- IP アドレス / ネットマスク
- all..... すべてのネットワーク

◦ *filter_num*..... フィルタ番号 (1 .. 2147483647)

[説明] BGP で広告する集約経路を設定する。フィルタの番号には、**bgp aggregate filter** コマンドで定義した番号を指定する。

[初期値] デフォルトでは経路は集約されない。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

28.3 経路を集約するためのフィルタの設定

[書式] **bgp aggregate filter** *filter_num protocol* [reject] *kind ip_address/mask …*
no bgp aggregate filter *filter_num* [*protocol* [reject] *kind ip_address/mask …]*

[設定値] ◦ *filter_num*..... フィルタ番号 (1..2147483647)

◦ *protocol*
- static ..... 静的経路
- rip..... RIP
- ospf..... OSPF
- bgp ..... BGP
- all..... すべてのプロトコル

◦ *kind*
- include..... 指定したネットワークに含まれる経路 (ネットワークアドレス自身を含む)
- refines..... 指定したネットワークに含まれる経路 (ネットワークアドレス自身を含まない)
- equal ..... 指定したネットワークに一致する経路

◦ *ip_address/mask*
- IP アドレス / ネットマスク

[説明] BGP で広告する経路を集約するためのフィルタを定義する。このコマンドで定義したフィルタは、**bgp aggregate** コマンドの filter 節で指定されてはじめて効果を持つ。
ip_address/mask では、ネットワークアドレスを設定する。これは複数設定でき、そのうち、一致するネットワーク長が長い設定が採用される。
kind の前に reject キーワードを置くと、その経路は集約されない。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

28.4　AS 番号の設定

[書式]　**bgp autonomous-system** *as*
no bgp autonomous-system [*as*]

[設定値]　◦ *as*.....AS 番号 (1..65535)

[説明]　ルーターの AS 番号を設定する。

[ノート]　AS 番号を設定するまで BGP は動作しない。

[初期値]　AS 番号は設定されない。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

28.5　ルーター ID の設定

[書式]　**bgp router id** *ip_address*
no bgp router id [*ip_address*]

[設定値]　◦ *ip_address*.....IP アドレス

[説明]　ルーター ID を設定する。

[ノート]　通常はこのコマンドを設定する必要はない。

[初期値]　インタフェースに付与されているプライマリアドレスから自動的に選択する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

28.6　BGP による経路の優先度の設定

[書式]　**bgp preference** *preference*
no bgp preference [*preference*]

[設定値]　◦ *preference*.....優先度 (1..2147483647)

[説明]　BGP による経路の優先度を設定する。優先度は 1 以上の整数で示され、数字が大きいほど優先度が高い。BGP とその他のプロトコルで得られた経路が食い違う場合には、優先度の高い経路が採用される。優先度が同じ場合には、先に採用された経路が有効になる。

[ノート]　各プロトコルに与えられた優先度の初期値は次のとおり。
◦ スタティック.....10000
◦ RIP.....1000
◦ OSPF.....2000
◦ BGP.....500

[初期値]　500

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

28.7　BGP で受信した経路に対するフィルタの適用

[書式]　**bgp export** *remote_as* filter *filter_num ...*
bgp export aspath *seq "aspath_regexp"* filter *filter_num ...*
no bgp export *remote_as* [filter *filter_num ...]*
no bgp export aspath *seq ["aspath_regexp" [* filter *filter_num ...]]*

[設定値]　◦ *remote_as*.....相手の AS 番号 (1..65535)
◦ *seq*.....AS パスを指定したときの評価順序 (1..65535)
◦ *aspath_regexp*.....正規表現
◦ *filter_num*.....フィルタ番号 (1..2147483647)

[説明] BGP で受けた経路に対してフィルタを設定する。*remote_as* を指定してフィルタを設定した場合、接続先から受けた経路についてフィルタに該当した経路が実際のルーティングテーブルに導入され、RIP や OSPF のような他のプロトコルにも通知される。フィルタに該当しない経路はルーティングには適用されず、他のプロトコルに通知されることもない。フィルタの番号には **bgp export filter** コマンドで定義した番号を指定する。
aspath_regexp を指定してフィルタを設定した場合、*remote_as* を指定した場合と同様に、AS パスが正規表現と一致する経路についてフィルタに該当した経路が導入される。*aspath_regexp* には **grep** コマンドで使用できる検索パターンを指定する。

aspath_regexp を指定したフィルタを複数設定した場合、*seq* の小さい順に評価される。また、*aspath_regexp* を指定したフィルタを設定した場合、*remote_as* を指定したフィルタよりも優先して評価される。

[ノート] 正規表現によって AS パスを表す例
- すべての AS パスと一致する
  # bgp export aspath 10 ".*" filter 1
- AS 番号が 1000 または 1100 で始まる AS パスと一致する
  # bgp export aspath 20 "^1[01]00 .*" filter 1
- AS 番号に 2000 を含む AS パスと一致する
  # bgp export aspath 30 "2000" filter 1
- AS パスが 3000 3100 3200 であるパスと完全一致する
  # bgp export aspath 40 "^3000 3100 3200$" filter 1
- AS パスに AS_SET を含むパスと一致する
  # bgp export aspath 50 "{.*}" filter 1

aspath は、RTX1500、RTX1100、RT107e は Rev.8.03.68 以降、RTX3000 は Rev.9.00.31 以降、SRT100 は Rev.10.00.31 以降で使用可能。

[初期値] このコマンドが設定されていないときには、BGP が受信したすべての経路が破棄される。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

28.8 BGP で受信する経路に適用するフィルタの設定

[書式] **bgp export filter** *filter_num* [reject] *kind ip_address/mask ...* [*parameter*]
no bgp export filter *filter_num* [[reject] *kind ip_address/mask ...* [*parameter*]]

[設定値]
- *filter_num* ..... フィルタ番号 (1..2147483647)
- *kind*
  - include ..... 指定したネットワークに含まれる経路 (ネットワークアドレス自身を含む)
  - refines ..... 指定したネットワークに含まれる経路 (ネットワークアドレス自身を含まない)
  - equal ..... 指定したネットワークに一致する経路
- *ip_address/mask*
  - IP アドレス / ネットマスク
  - all ..... すべてのネットワーク
- *parameter* ..... TYPE=VALUE の組

TYPE	VALUE	説明
preference	0..255	同じ経路を複数の相手から受信したときに、一方を選択するための優先度

[説明] BGP で受信する経路に適用するフィルタを定義する。このコマンドで定義したフィルタは、**bgp export** コマンドの filter 節で指定されてはじめて効果を持つ。
ip_address/mask では、ネットワークアドレスを設定する。複数の設定があるときには、プレフィックスが最も長く一致する設定が採用される。
kind の前に reject キーワードを置くと、その経路が拒否される。

[ノート] preference の設定は BGP 経路の間で優先順位をつけるために使用される。BGP 経路の全体の優先度は、**bgp preference** コマンドで設定する。

[初期値] preference = 0

[設定例]
```
# bgp export filter 1 include 10.0.0.0/16 172.16.0.0/16
# bgp export filter 2 reject equal 192.168.0.0/24
```

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

28.9 BGP に導入する経路に対するフィルタの適用

[書式] **bgp import** *remote_as protocol* [*from_as*] filter *filter_num* ...
no bgp import *remote_as protocol* [*from_as*] [filter *filter_num* ...]

[設定値]
- *remote_as*.....相手の AS 番号 (1..65535)
- *protocol*
  - static .....静的経路
  - rip.....RIP
  - ospf.....OSPF
  - bgp.....BGP
  - aggregate.....集約経路
- *from_as*.....導入する経路を受信した AS (*protocol* で bgp を指定したときのみ) (1..65535)
- *filter_num*.....フィルタ番号 (1 .. 2147483647)

[説明] RIP や OSPF のような BGP 以外の経路を導入するときに適用するフィルタを設定する。フィルタに該当しない経路は導入されない。フィルタの番号には、**bgp import filter** コマンドで定義した番号を指定する。BGP の経路を導入するときには、その経路を受信した AS 番号を指定する必要がある。

[初期値] このコマンドが設定されていないときには、外部経路は導入されない。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

28.10 BGP の設定の有効化

[書式] **bgp configure refresh**

[設定値] なし

[説明] BGP の設定を有効にする。BGP の設定を変更したら、ルーターを再起動するか、このコマンドを実行する必要がある。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

28.11 BGP に導入する経路に適用するフィルタの設定

[書式] **bgp import filter** *filter_num* [reject] *kind ip_address/mask* ... [*parameter*]
no bgp import filter *filter_num* [[reject] *kind ip_address/mask* ... [*parameter*]]

[設定値]
- *filter_num*.....フィルタ番号 (1..2147483647)
- *kind*
  - include.....指定したネットワークに含まれる経路 (ネットワークアドレス自身を含む)
  - refines .....指定したネットワークに含まれる経路 (ネットワークアドレス自身を含まない)
  - equal .....指定したネットワークに一致する経路
- *ip_address/mask*
  - IP アドレス / ネットマスク
  - all... .....すべてのネットワーク
- *parameter*.....TYPE=VALUE の組

TYPE	VALUE	説明
metric	1..16777215	MED(Multi-Exit Discriminator) で通知するメトリック値 (指定しないときは MED を送信しない)

[説明] BGP に導入する経路に適用するフィルタを定義する。このコマンドで定義したフィルタは、**bgp import** コマンドの filter 節で指定されてはじめて効果を持つ。
ip_address/mask では、ネットワークアドレスを設定する。複数の設定があるときには、プレフィックスが最も長く一致する設定が採用される。
kind の前に reject キーワードを置くと、その経路が拒否される。

[初期値] metric = 1

[設定例]
```
# bgp import filter 1 include 10.0.0.0/16 172.16.0.0/16
# bgp import filter 2 reject equal 192.168.0.0/24
```

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

28.12 BGPによる接続先の設定

[書式] **bgp neighbor** *neighbor_id remote_as remote_address* [*parameter ...]*
no bgp neighbor *neighbor_id* [*remote_as ...]*

[設定値] ◦ *neighbor_id*..... 近隣ルーターの番号 (1...2147483647)
◦ *remote_as*..... 相手の AS 番号 (1..65535)
◦ *remote_address* ..... 相手の IP アドレス
◦ *parameter*..... TYPE=VALUE の組

TYPE	VALUE	説明
hold-time	offもしくは3以上の整数[秒]	キープアライブの送信間隔
metric	1 .. 21474836	MED (Multi-Exit Discriminator) で通知するメトリック
passive	on または off	能動的なBGP コネクションの接続を抑制するか否か
gateway	IP アドレス / インタフェース	接続先に対するゲートウェイ
local-address	IP アドレス	BGP コネクションの自分のアドレス

[説明] BGP コネクションを接続する近隣ルーターを定義する。

[ノート] *metric*パラメータはすべてのMEDの初期値として働くので、**bgp import**コマンドでMEDを設定したときにはそれが優先される。

gateway オプションは、接続先が同一のセグメントにないときに、その接続先に対するゲートウェイ (ネクストホップ) を指定する。*gateway* オプションは Rev.8.01.12 以降で使用可能。

RTX2000、RTX1000 は、Rev.7.01.41 以降で使用可能。
RTX2000、RTX1000、RT250i では local-address は指定できない。

[初期値] *hold-time* = 180
metric は送信されない
passive = off
gateway は指定されない
local-address は指定されない

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	RT250i	RT107e	SRT100

28.13 BGPのログの設定

[書式] **bgp log** *log* [*log*]
no bgp log [*log ...*]

[設定値] ◦ *log*
- neighbor..... 近隣ルーターに対する状態遷移
- packet..... 送受信したパケット

[説明] 指定した種類のログを INFO レベルで記録する。

[ノート] RTX1000 は Rev.8.01.24 以降で使用可能。

[初期値] ログを記録しない。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

29. IPv6

29.1 共通の設定

29.1.1 IPv6 パケットを扱うか否かの設定

[書式] **ipv6 routing** *routing*
no ipv6 routing [*routing*]

[設定値] ◦ *routing*
- on ..... 処理対象として扱う
- off ..... 処理対象として扱わない

[説明] IPv6 パケットをルーティングするか否かを設定する。本スイッチを on にしないと PP 側の IPv6 関連は一切動作しない。
off の場合でも TELNET による設定や TFTP によるアクセス、PING 等は可能。

[初期値] on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

29.1.2 IPv6 インタフェースのリンク MTU の設定

[書式] **ipv6** *interface* **mtu** *mtu*
ipv6 pp mtu *mtu*
no ipv6 *interface* **mtu** [*mtu*]
no ipv6 pp mtu [*mtu*]

[設定値] ◦ *interface* ..... LAN インタフェース名
◦ *mtu* ..... MTU の値 (1280..1500; RTX3000 の LAN1 と LAN2 の場合は 1280..9578)

[説明] IPv6 インタフェースのリンク MTU を設定する。

[初期値] 1500

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

29.1.3 TCP セッションの MSS 制限の設定

[書式] **ipv6** *interface* **tcp mss limit** *mss*
ipv6 pp tcp mss limit *mss*
ipv6 tunnel tcp mss limit *mss*
no ipv6 *interface* **tcp mss limit** [*mss*]
no ipv6 pp tcp mss limit [*mss*]
no ipv6 tunnel tcp mss limit [*mss*]

[設定値] ◦ *interface* ..... LAN インタフェース名
◦ *mss*
- MSS の最大長 (536 .. 1440)
- auto ..... 自動設定
- off ..... 設定しない

[説明] インタフェースを通過する TCP セッションの MSS を制限する。インタフェースを通過する TCP パケットを監視し、MSS オプションの値が設定値を越えている場合には、設定値に書き換える。キーワード auto を指定した場合には、インタフェースの MTU、もしくは PP インタフェースの場合で相手の MRU 値が分かる場合にはその MRU 値から計算した値に書き換える。

[ノート] PPPoE 用の PP インタフェースに対しては、**pppoe tcp mss limit** コマンドでも TCP セッションの MSS を制限することができる。このコマンドと **pppoe tcp mss limit** コマンドの両方が有効な場合は、MSS はどちらかより小さな方の値に制限される。
RT250i では **ipv6 tunnel tcp mss limit** コマンドは使用できない。

[初期値] off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

29.1.4 タイプ 0 のルーティングヘッダ付き IPv6 パケットを破棄するか否かの設定

[書式] **ipv6 rh0 discard** *switch*
no ipv6 rh0 discard

[設定値] ◦ *switch*
- on..... 破棄する
- off..... 破棄しない

[説明] タイプ 0 のルーティングヘッダ付き IPv6 パケットを破棄するか否かを選択する。

[ノート] RTX2000、RTX1000 は Rev.7.01.53 以降で使用可能。
RTX3000 は、Rev.9.00.24 以降で使用可能。

[初期値] on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

29.1.5 IPv6 ファストパス機能の設定

[書式] **ipv6 routing process** *process*
no ipv6 routing process

[設定値] ◦ *sprocess*
- fast..... ファストパス機能を利用する
- normal..... ファストパス機能を利用せず、すべての IPv6 パケットをノーマルパスで処理する

[説明] IPv6 パケットの転送をファストパス機能で処理するか、ノーマルパス機能で処理するかを設定する。

[ノート] ファストパスでは使用できる機能に制限は無いが、取り扱うパケットの種類によってはファストパスで処理されず、ノーマルパスで処理されることもある。

Rev.8.03.37 以降、**ipv6 multicast routing process** コマンドを廃止し、本コマンドに統合した。そのため、本コマンドで fast を設定した場合、IPv6 マルチキャストパケットもファストパス機能で処理される。
RTX1100、RT107e では Rev.8.03.37 以降で使用可能。

[初期値] fast

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

29.2 IPv6 アドレスの管理

29.2.1 インタフェースの IPv6 アドレスの設定

[書式] **ipv6** *interface* **address** *ipv6_address/prefix_len*
ipv6 *interface* **address** auto
ipv6 pp address *ipv6_address/prefix_len*
ipv6 pp address auto
ipv6 tunnel address *ipv6_address/prefix_len*
ipv6 tunnel address auto
no ipv6 *interface* **address** *ipv6_address/prefix_len*
no ipv6 *interface* **address** auto
no ipv6 pp address *ipv6_address/prefix_len*
no ipv6 pp address auto
no ipv6 tunnel address *ipv6_address/prefix_len*
no ipv6 tunnel address auto

[設定値] ◦ *interface*..... LAN インタフェース名、LOOPBACK インタフェース名、ブリッジインタフェース名
◦ *ipv6_address*..... IPv6 アドレス部分
◦ *prefix_len*..... IPv6 プレフィックス長
◦ auto..... 自動設定を行うことを示すキーワード

[説明] インタフェースに IPv6 アドレスを付与する。

[ノート]　このコマンドで付与したアドレスは、**show ipv6 address** コマンドで確認することができる。
複数の LAN インタフェースで自動設定機能を利用することができる。その場合、デフォルト経路は最後に自動設定が完了したインタフェースに向く。
RT250i では **ipv6 tunnel address** コマンドは使用できない。
LOOPBACK インタフェースを指定できるのは Rev.8.03 以降のリビジョンである。
LOOPBACK インタフェースを指定した場合は、auto は指定できない。
ブリッジインタフェースを指定できるのは Rev.10.00.38 以降のリビジョンである。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

29.2.2　インタフェースのプレフィックスに基づく IPv6 アドレスの設定

[書式]
ipv6 *interface* **prefix** *ipv6_prefix/prefix_len*
ipv6 *interface* **prefix** auto
ipv6 pp prefix *ipv6_prefix/prefix_len*
ipv6 pp prefix auto
ipv6 tunnel prefix *ipv6_prefix/prefix_len*
ipv6 tunnel prefix auto
no ipv6 *interface* **prefix** *ipv6_prefix/prefix_len*
no ipv6 *interface* **prefix** auto
no ipv6 pp prefix *ipv6_prefix/prefix_len*
no ipv6 pp prefix auto
no ipv6 tunnel prefix *ipv6_prefix/prefix_len*
no ipv6 tunnel prefix auto

[設定値]
- *interface*.....LAN インタフェース名、ブリッジインタフェース名
- *ipv6_prefix*.....IPv6 プレフィックスのアドレス部分
- *prefix_len*.....IPv6 プレフィックス長
- auto .....自動設定を行うことを示すキーワード

[説明]　インタフェースに IPv6 アドレスを付与する。類似のコマンドに **ipv6** *interface* **address** コマンドがあるが、このコマンドではアドレスではなくプレフィックスのみを指定する。プレフィックス以降の部分は MAC アドレスに基づいて自動的に補完する。このときに使用する MAC アドレスは、設定しようとするインタフェースに割り当てられているものが使われる。ただし、MAC アドレスを持たない PP インタフェースやトンネルインタフェースでは LAN1 インタフェースの MAC アドレスを使用する。

なお、類似の名前を持つ **ipv6 prefix** コマンドはルーター広告で通知するプレフィックスを定義するものであり、IPv6 アドレスを付与するものではない。しかしながら、通常の運用では、インタフェースに付与する IPv6 アドレスのプレフィックスとルーター広告で通知するプレフィックスは同じであるから、双方のコマンドに同じプレフィックスを設定することが多い。

auto の場合は、他のルーターから受け取った RA(ルーター広告) により自動的に設定される。

[ノート]　このコマンドで設定された IPv6 アドレスは **show ipv6 address** コマンドで確認できる。
RT250i では **ipv6 tunnel prefix** コマンドは使用できない。
ブリッジインタフェースを指定できるのは Rev.10.00.38 以降のリビジョンである。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

29.2.3　DAD(Duplicate Address Detection) の送信回数の設定

[書式]
ipv6 *interface* **dad retry count** *count*
ipv6 pp dad retry count *count*
no ipv6 *interface* **dad retry count** [*count*]
no ipv6 pp dad retry count [*count*]

[設定値]
- *interface*.....LAN インタフェース名、ブリッジインタフェース名
- *count*.....選択したインタフェースでの DAD の再送回数 (0..10)

[説明]　インタフェースに IPv6 アドレスが設定されたときに、アドレスの重複を検出するために送信する DAD の送信回数を設定する。ただし、0 を設定した場合は、DAD を送信せずにアドレスを有効なものとして扱う。

[ノート]　Rev.7.01.47、Rev.8.01.18、Rev.8.02.28 以降で使用可能。
ブリッジインタフェースを指定できるのは Rev.10.00.38 以降のリビジョンである。

[初期値]　1

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	RT250i	RT107e	SRT100

29.2.4 自動的に設定される IPv6 アドレスの最大数の設定

[書式] **ipv6 max auto address** *max*
no ipv6 max auto address [*max*]

[設定値] ◦ *max* ..... 自動的に設定される IPv6 アドレスの 1 インタフェースあたりの最大数 (1 ～ 256)

[説明] RA によりインタフェースに自動的に設定される IPv6 アドレスの 1 インタフェースあたりの最大数を設定する。

[ノート] RTX1000 は、Rev.8.01.27 以降、SRT100 は、Rev.10.00.38 以降で使用可能。

[初期値] 16

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	RTX1000	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

29.2.5 始点 IPv6 アドレスを選択する規則の設定

[書式] **ipv6 source address selection rule** *rule*
no ipv6 source address selection rule [*rule*]

[設定値] ◦ *rule* ..... LAN インタフェース名
- prefix ..... プレフィクスの最長一致
- lifetime ..... 寿命の長いほうを優先

[説明] 始点 IPv6 アドレスを選択する規則を設定する。
'prefix' を設定した場合には、終点 IPv6 アドレスと候補を選択して、先頭から一致している部分 (プレフィクス) がもっとも長いものを始点アドレスとして選択する。
'lifetime' を設定した場合には、IPv6 アドレスの寿命が長いものを優先して選択する。

[ノート] 通常は 'prefix' を設定しておけばいいが、アドレスリナンバリングが発生するときには、'lifetime' の設定が有効な場合がある。
SRT100 は、Rev.10.00.38 以降で使用可能。

[初期値] prefix

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

29.3 近隣探索

29.3.1 ルーター広告で配布するプレフィックスの定義

[書式] **ipv6 prefix** *prefix_id prefix/prefix_len* [preferred_lifetime=*time*] [valid_lifetime=*time*] [l_flag=*switch*] [a_flag=*switch*]
no ipv6 prefix *prefix_id*

[設定値] ◦ *prefix_id* ..... プレフィックス番号
◦ *prefix* ..... プレフィックス
◦ *prefix_len* ..... プレフィックス長
◦ valid_lifetime ..... プレフィックスの有効寿命 (60..15552000)
◦ preferred_lifetime ..... プレフィックスの推奨寿命 (60..15552000)
◦ *time* ..... 時間設定
- *yyyy-mm-dd*[,*hh:mm*[:*ss*]]
  - *yyyy* .....年 (1980..2079)
  - *mm* .....月 (01..12)
  - *dd* .....日 (01..31)
  - *hh* .....時 (00..23)
  - *mm* .....分 (00..59)
  - *ss* .....秒 (00..59、省略時は 00)

◦ l_flag ..... on-link フラグ
◦ a_flag ..... autonomous address configuration フラグ
◦ *switch*
- on
- off

[説明] ルーター広告で配布するプレフィックスを定義する。実際に広告するためには、**ipv6** *interface* **rtadv send** コマンドの設定が必要である。
time では寿命を秒数または寿命が尽きる時刻のいずれかを設定できる。*time* として数値 (60 以上 15552000 以下) を設定すると、その秒数を寿命として広告する。*time* として時刻を設定すると、その時刻に寿命が尽きるものとして寿命を計算し、広告する。時刻を設定する場合は、上記のフォーマットに従う。有効寿命とはアドレスが無効になるまでの時間であり、推奨寿命とはアドレスを新たな接続での使用が不可となる時間である。また、on-link フラグはプレフィックスがそのデータリンクに固有である時に on とする。autonomous address configuration フラグはプレフィックスを自律アドレス設定で使うことができる場合に on とする。

[ノート] リンクローカルのプレフィックスを設定することはできない。

[初期値] valid_lifetime = 2592000
preferred_lifetime = 604800
l_flag = on
a_flag = on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

29.3.2 ルーター広告の送信の制御

[書式] **ipv6** *interface* **rtadv send** *prefix_id* [*prefix_id...*] [*option=value...*]
ipv6 pp rtadv send *prefix_id* [*prefix_id...*] [*option=value...*]
no ipv6 *interface* **rtadv send** [*...*]
no ipv6 pp rtadv send [*...*]

[設定値]
- *interface*.....LAN インタフェース名
- *prefix_id*.....プレフィックス番号
- *option=value*.....NAME=VALUE の列

NAME	VALUE	説明
m_flag	on, off	managed address configuration フラグ。ルーター広告による自動設定とは別に、DHCP6 に代表されるルーター広告以外の手段によるアドレス自動設定をホストに許可させるか否かの設定。
o_flag	on, off	other stateful configuration フラグ。ルーター広告以外の手段により IPv6 アドレス以外のオプション情報をホストに自動的に取得させるか否かの設定。
max-rtr-adv-interval	秒数	ルーター広告を送信する最大間隔 (4-1800 秒)
min-rtr-adv-interval	秒数	ルーター広告を送信する最小間隔 (3-1350 秒)
adv-default-lifetime	秒数	ルーター広告によって設定される端末のデフォルト経路の有効時間 (0-9,000 秒)
adv-reachable-time	ミリ秒数	ルーター広告を受信した端末が、ノード間で確認した到達性の有効時間 (0-3,600,000 ミリ秒)
mtu	auto, off, バイト数	ルーター広告に MTU オプションを含めるか否かと、含める場合の値の設定。auto の場合はインタフェースの MTU を採用する。

[説明] インタフェースごとにルーター広告の送信を制御する。送信されるプレフィックスとして、**ipv6 prefix** コマンドで設定されたものが用いられる。また、オプションとして m_flag および o_flag を利用して、管理するホストがルーター広告以外の自動設定情報をどのように解釈するかを設定することができる。オプションでは、送信するルーター広告の送信間隔や、ルーター広告に含まれる情報の設定を行うこともできる。

[ノート] RTX2000 では mtu= オプションは指定できない。

[初期値] m_flag = off
o_flag = off
max-rtr-adv-interval = 600
min-rtr-adv-interval = 200
adv-default-lifetime = 1800
adv-reachable-time = 0
mtu=auto

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

29.4 経路制御

29.4.1 IPv6 の経路情報の追加

[書式] **ipv6 route** *network* gateway *gateway* [*parameter*] [gateway *gateway* [*parameter*]]
no ipv6 route *network*

[設定値] ◦ *network*
- IPv6 アドレス / プレフィックス長
- default..... デフォルト経路

◦ *gateway*..... ゲートウェイ
- IP アドレス % スコープ識別子
- pp *peer_num* [dlci=*dlci*]..... PP インタフェースへの経路
  "dlci=*dlci*" が指定された場合は、フレームリレーの DLCI への経路
  - *peer_num*
    - 相手先情報番号
    - anonymous
- pp anonymous name=*name*
  - *name*.....PAP/CHAP による名前
- tunnel *tunnel_num*..... トンネルインタフェースへの経路

◦ *parameter*..... 以下のパラメータを空白で区切り複数設定可能
- metric *metric* ..... メトリックの指定
  - メトリック値 (1..15)
  - 省略時は 1
- hide..... 出力インタフェースが PP インタフェースの場合のみ有効なオプションで、回線が接続されている場合だけ経路が有効になることを意味する

[説明] IPv6 の経路情報を追加する。LAN インタフェースが複数ある機種ではスコープ識別子でインタフェースを指定する必要がある。インタフェースに対応するスコープ識別子は show ipv6 address コマンドで表示される。
LAN インタフェースがひとつである機種に関しては、スコープ識別子が省略されると LAN1 が指定されたものとして扱う。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

29.5 RIPng

29.5.1 RIPng の使用の設定

[書式] **ipv6 rip use** *use*
no ipv6 rip use

[設定値] ◦ *use*
- on..... RIPng を使う
- off..... RIPng を使わない

[説明] RIPng を使うか否かを設定する。

[初期値] off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

29.5.2 インタフェースにおける RIPng の送信ポリシーの設定

[書式] **ipv6** *interface* **rip send** *send*
ipv6 pp rip send *send*
ipv6 tunnel rip send *send*
no ipv6 *interface* **rip send**
no ipv6 pp rip send
no ipv6 tunnel rip send

[設定値] ◦ *interface*..... LAN インタフェース名

◦ *send*
- on..... RIPng を送信する
- off..... RIPng を送信しない

[説明] RIPng の送信ポリシーを設定する。

[ノート] RT250i では **ipv6 tunnel rip send** コマンドは使用できない。

[初期値] on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

29.5.3 インタフェースにおける RIPng の受信ポリシーの設定

[書式]

ipv6 *interface* **rip receive** *receive*
ipv6 pp rip receive *receive*
ipv6 tunnel rip receive *receive*
no ipv6 *interface* **rip receive**
no ipv6 pp rip receive
no ipv6 tunnel rip receive

[設定値]

◦ *interface*.....LAN インタフェース名
◦ *receive*
• on.....受信した RIPng パケットを処理する
• off.....受信した RIPng パケットを無視する

[説明]

RIPng の受信ポリシーを設定する。

[ノート]

RT250i では **ipv6 tunnel rip receive** コマンドは使用できない。

[初期値]

on

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

29.5.4 RIPng の加算ホップ数の設定

[書式]

ipv6 *interface* **rip hop** *direction hop*
ipv6 pp rip hop *direction hop*
no ipv6 *interface* **rip hop** *direction*
no ipv6 pp rip hop *direction*

[設定値]

◦ *direction*
• in.....受信時に加算する
• out.....送信時に加算する
◦ *hop*.....加算ホップ数 (0..15)

[説明]

PP インタフェースで送受信する RIPng のメトリックに対して加算するホップ数を設定する。

[初期値]

0

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

29.5.5 インタフェースにおける信頼できる RIPng ゲートウェイの設定

[書式]

ipv6 *interface* **rip trust gateway** [except] *gateway* [*gateway ...]*
ipv6 pp rip trust gateway [except] *gateway* [*gateway ...]*
no ipv6 *interface* **rip trust gateway**
no ipv6 pp rip trust gateway

[設定値]

◦ *interface*.....LAN インタフェース名
◦ *gateway*.....IPv6 アドレス

[説明]

信頼できる RIPng ゲートウェイを設定する。
except キーワードを指定していない場合には、列挙したゲートウェイを信用できるゲートウェイとし、それらからの RIP だけを受信する。
except キーワードを指定した場合は、列挙したゲートウェイを信用できないゲートウェイとし、それらを除いた他のゲートウェイからの RIP だけを受信する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

29.5.6 RIPng で送受信する経路に対するフィルタリングの設定

[書式] **ipv6** *interface* **rip filter** *direction filter_list* [*filter_list...*]
ipv6 pp rip filter *direction filter_list* [*filter_list...*]
ipv6 tunnel rip filter *direction filter_list* [*filter_list...*]
no ipv6 *interface* **rip filter** *direction*
no ipv6 pp rip filter *direction*
no ipv6 tunnel rip filter *direction*

[設定値] ◦ *interface* ..... LAN インタフェース名
◦ *direction*
• in ..... 内向きのパケットを対象にする
• out ..... 外向きのパケットを対象にする
◦ *filter_list* ..... フィルタ番号

[説明] インタフェースで送受信する RIPng パケットに対して適用するフィルタを設定する。

[ノート] RT250i では **ipv6 tunnel rip filter** コマンドは使用できない。

[初期値] フィルタは設定されていない

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

29.5.7 回線接続時の PP 側の RIPng の動作の設定

[書式] **ipv6 pp rip connect send** *action*
no ipv6 pp rip connect send

[設定値] ◦ *action*
• none ..... RIPng を送信しない
• interval ..... **ipv6 pp rip connect interval** コマンドで設定された時間間隔で RIPng を送出する
• update ..... 経路情報が変わった時にのみ RIPng を送出する

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

[初期値] update

[設定例] # ipv6 pp rip connect interval 60
ipv6 pp rip connect send interval

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

29.5.8 回線接続時の PP 側の RIPng 送出の時間間隔の設定

[書式] **ipv6 pp rip connect interval** *time*
no ipv6 pp rip connect interval

[設定値] ◦ *time* ..... 秒数 (30..21474836)

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

[初期値] 30

[設定例] # ipv6 pp rip connect interval 60
ipv6 pp rip connect send interval

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

29.5.9 回線切断時の PP 側の RIPng の動作の設定

[書式] **ipv6 pp rip disconnect send** *action*
no ipv6 pp rip disconnect send

[設定値] ◦ *action*
- none..... RIPng を送信しない
- interval..... **ipv6 pp rip disconnect interval** コマンドで設定された時間間隔で RIPng を送出する
- update ..... 経路情報が変わった時にのみ RIPng を送信する

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

[初期値] none

[設定例] # ipv6 pp rip disconnect interval 1800
ipv6 pp rip disconnect send interval

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

29.5.10 回線切断時の PP 側の RIPng 送出の時間間隔の設定

[書式] **ipv6 pp rip disconnect interval** *time*
no ipv6 pp rip disconnect interval

[設定値] ◦ *time*.....秒数 (30..21474836)

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

[初期値] 3600

[設定例] # ipv6 pp rip disconnect interval 1800
ipv6 pp rip disconnect send interval

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

29.5.11 RIPng による経路を回線切断時に保持するか否かの設定

[書式] **ipv6 pp rip hold routing** *hold*
no ipv6 pp rip hold routing

[設定値] ◦ *hold*
- on.....保持する
- off.....保持しない

[説明] PP インタフェースから RIPng で得られた経路を、回線が切断されたときに保持するか否かを設定する。

[初期値] off

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

29.5.12 RIPng による経路の優先度の設定

[書式] **ipv6 rip preference** *preference*
no ipv6 rip preference [*preference*]

[設定値] ◦ *preference*.....RIPng による経路の優先度 (1-2147483647)

[説明] RIPng による経路の優先度を設定する。優先度は 1 以上の数値で表され、数字が大きい程優先度が高い。
OSPFv3 とスタティックなど複数のプロトコルで得られた経路が食い違う場合には、優先度が高い方が採用される。優先度が同じ場合には時間的に先に採用された経路が有効となる

[ノート] 静的経路の優先度は 10000 で固定である。

[初期値] 1000

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

29.6 フィルタの設定

29.6.1 IPv6 フィルタの定義

[書式] **ipv6 filter** *filter_num pass_reject src_addr*[*/prefix_len*] [*dest_addr*[*/prefix_len*] [*protocol* [*src_port_list* [*dest_port_list*]]]]
no ipv6 filter *filter_num* [*pass_reject*]

[設定値]
- *filter_num* ..... 静的フィルタ番号 (1..21474836)
- *pass_reject* ..... フィルタのタイプ (**ip filter** コマンドに準ずる)
- *src_addr* ..... IP パケットの始点 IP アドレス
- *prefix_len* ..... プレフィックス長
- *dst_addr* ..... IP パケットの終点 IP アドレス (*src_addr* と同じ形式)
  省略時は 1 個の * と同じ。
- *protocol* ..... *フィルタリングするパケットの種類 (**ip filter** コマンドに準ずる)*
  - icmp-nd ..... 近隣探索に関係するパケットの指定を示すキーワード
    (TYPE が 133、134、135、136 のいずれかである ICMPv6 パケット)
  - icmp6 ..... ICMPv6 パケットの指定を示すキーワード
- *src_port_list* ..... TCP/UDP のソースポート番号、あるいは ICMPv6 タイプ (**ip filter** コマンドに準ずる)
  - *dst_port_list* ..... TCP/UDP のデスティネーションポート番号、あるいは ICMPv6 コード

[説明] IPv6 のフィルタを定義する。

[ノート] 近隣探索に関係するパケットとは以下の 4 つを意味する。
- 133: Router Solicitation
- 134: Router Advertisement
- 135: Neighbor Solicitation
- 136: Neighbor Advertisement

ICMP のタイプとコードを指定できるのは、
RTX1500、RTX1100、RT107e ..... Rev.8.03.68 以降、
RTX3000 ..... Rev.9.00.31 以降

[設定例] PP 1 で送受信される IPv6 Packet Too Big を記録する
```
# pp select 1
#  ip pp secure filter in 1 100
#  ip pp secure filter out 1 100
# ipv6 filter 1 pass-log * * icmp6 2
# ipv6 filter 100 pass * *
```

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

29.6.2 IPv6 フィルタの適用

[書式] **ipv6** *interface* **secure filter** *direction* [*filter_list...*] [dynamic *filter_list*]
ipv6 pp secure filter *direction* [*filter_list...*] [dynamic *filter_list*]
ipv6 tunnel secure filter *direction* [*filter_list...*] [dynamic *filter_list*]
no ipv6 *interface* **secure filter** *direction*
no ipv6 pp secure filter *direction*
no ipv6 tunnel secure filter *direction*

[設定値]
- *interface* ..... LAN インタフェース名、LOOPBACK インタフェース名、NULL インタフェース名、
  ブリッジインタフェース名
- *direction*
  - in ..... 受信したパケットのフィルタリング
  - out ..... 送信するパケットのフィルタリング
- *filter_list* ..... 空白で区切られたフィルタ番号の並び (128 個以内)
- dynamic ..... キーワード後に動的フィルタの番号を記述する

[説明] IPv6 フィルタをインタフェースに適用する。

[ノート] RT250i では **ipv6 tunnel secure filter** コマンドは使用できない。
LOOPBACK インタフェースと NULL インタフェースでは動的フィルタは使用できない。
SRT100 では dynamic キーワードは使用できない。動的フィルタは **ip policy filter** コマンドを使用する。
NULL インタフェースで *direction* に 'in' は指定できない。
LOOPBACK インタフェース、NULL インタフェースを指定できるのは Rev.8.03 以降のリビジョンである。
ブリッジインタフェースを指定できるのは Rev.10.00.38 以降のリビジョンである。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

29.6.3 IPv6 動的フィルタの定義

[書式]

ipv6 filter dynamic *dyn_filter_num srcaddr dstaddr protocol* [*option ...*]
ipv6 filter dynamic *dyn_filter_num srcaddr dstaddr* filter *filter_list* [in *filter_list*] [out *filter_list*] [*option ...*]
no ipv6 filter dynamic *dyn_filter_num* [*srcaddr...*]

[設定値]

- *dyn_filter_num*.....動的フィルタ番号 (1..21474836)
- *srcaddr*.....始点 IPv6 アドレス
- *dstaddr*.....終点 IPv6 アドレス
- *protocol*.....プロトコルのニーモニック
  - tcp
  - udp
  - ftp
  - tftp
  - domain
  - www
  - smtp
  - pop3
  - telnet
- *filter_list*..... **ipv6 filter** コマンドで登録されたフィルタ番号のリスト
- *option*
  - syslog=*switch*
    - on..... コネクションの通信履歴を syslog に残す
    - off..... コネクションの通信履歴を syslog に残さない
  - timeout=*time*
    - *time*..... データが流れなくなったときにコネクション情報を解放するまでの秒数

[説明]

IPv6 の動的フィルタを定義する。第 1 書式では、あらかじめルーターに登録されているアプリケーション名を指定する。第 2 書式では、ユーザがアクセス制御のルールを記述する。キーワードの filter、in、out の後には、**ipv6 filter** コマンドで定義されたフィルタ番号を設定する。
filterキーワードの後に記述されたフィルタに該当するコネクション (トリガ) を検出したら、それ以降 in キーワードと out キーワードの後に記述されたフィルタに該当するコネクションを通過させる。in キーワードはトリガの方向に対して逆方向のアクセスを制御し、out キーワードは動的フィルタと同じ方向のアクセスを制御する。なお、**ipv6 filter** コマンドの IP アドレスは無視される。pass/reject の引数も同様に無視される。
ここに記載されていないアプリケーションについては、filter キーワードを使って定義することで扱える可能性がある。特に snmp のように動的にポート番号が変化しないプロトコルの扱いは容易である。

tcp か udp を設定することで扱える可能性がある。特に、telnet のように動的にポート番号が変化しないプロトコルは tcp を指定することで扱うことができる。

[初期値]

syslog = on
timeout = 60

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	~~SRT100~~

29.7 IPv6 マルチキャストパケットの転送の設定

MLDv1、MLDv2、MLD プロキシの機能を提供します。MLDv1 と MLDv2 については、ホスト側とルーター側の双方に対応し、インタフェースごとにホストとルーターの機能を使い分けることができます。MLDv1 は RFC2710、MLDv2 は draft-vida-mld-v2-07.txt に対応します。MLD プロキシは、下流のインタフェースに存在するリスナーの情報を、上流のインタフェースに中継する機能であり、draft-ietf-magma-igmp-proxy-04.txt に基づいて実装しています。

マルチキャストは、マルチキャストのルーティングに対応した特別な網で実現されます。マルチキャスト網を構成するルーターは、特定の端末が送信するマルチキャストパケットを複製して、複数の端末に配送します。マルチキャストパケットを送信する端末をソース (source) と呼び、それを受信する端末をリスナー (listener) と呼びます。以下の説明では、マルチキャストパケットを単にパケットと書きます。
ソースが送信するパケットは原則としてすべてのリスナーに届きます。しかし、リスナーによって受信するパケットを変えたければ、リスナーをグループに分けることができます。同じグループに属する端末は同じパケットを受信し、異なるグループに属する端末は異なるパケットを受信します。それぞれのグループには識別子としてマルチキャストアドレスが割り当てられます。
パケットの IP ヘッダの終点アドレスには、グループに対応するマルチキャストアドレスが格納されます。網内のルーターは、このマルチキャストアドレスを見て、パケットの転送先のグループを確認します。網内のルーターはグループごとに編成された経路表を持っているので、その経路表にしたがってパケットを配布します。経路表は、通常、PIM-SM、PIM-DM、DVMRP などのルーティングプロトコルによって自動的に生成されます。

MLD(Multicast Listener Discovery) の目的は、端末がマルチキャスト網に対して、端末が参加するグループを通知することです。
網内のルーターは端末に対してクエリー (Query) というメッセージを送信します。クエリーを受信した端末は、ルーターに対してレポート (Report) というメッセージを返信します。レポートの中には、端末が参加するグループのマルチキャストアドレスを格納します。レポートを受信したルーターはその情報をルーティングに反映します。
MLDv2 では、受信するパケットのソースを制限することができますが、この機能を実現するためにフィルタモード (Filter Mode) とソースリスト (Source List) を使用します。フィルタモードには INCLUDE と EXCLUDE があり、INCLUDE では許可するソースを列挙し、EXCLUDE では許可しないソースを列挙します。
例えば、次の場合には、2001:x:x:x::1 と 2001:x:x:x::2 をソースとするパケットだけが転送の対象になります。

- フィルタモード : INCLUDE
- ソースリスト : { 2001:x:x:x::1, 2001:x:x:x::2 }

MLD のメッセージは原則としてルーターを超えることができません。そこで、端末とマルチキャスト網の間にルーターが介在する場合には、ルーターが MLD プロキシの機能を持つ必要があります。MLD プロキシの機能を持つルーターは、LAN 側に対してクエリを送信し、LAN 側からレポートを受信します。また、そのレポートに含まれる情報を WAN 側に転送します。

29.7.1 MLD の動作の設定

[書式]

ipv6 *interface* **mld** *type* [*option ...*]
ipv6 pp mld *type* [*option ...*]
ipv6 tunnel mld *type* [*option ...*]
no ipv6 *interface* **mld** [*type* [*option ...*]]
no ipv6 pp mld [*type* [*option ...*]]
no ipv6 tunnel mld [*type* [*option ...*]]

[設定値]

- *interface*..... LAN インタフェース名
- *type*..... MLD の動作方式
  - off..... MLD は動作しない
  - router ..... MLD ルーターとして動作する
  - host..... MLD ホストとして動作する
- *option*..... オプション
  - version=*version* ... MLD のバージョン
    - 1 .....MLDv1
    - 2 .....MLDv2
    - 1,2 .....MLDv1 と MLDv2 の両方に対応する。(MLDv1 互換モード)
  - syslog=*switch*..... 詳細な情報を syslog に出力するか否か
    - on .....表示する
    - off .....表示しない
  - robust-variable=VALUE (1 .. 10)
    - MLD で規定される Robust Variable の値を設定する。

[説明] インタフェースの MLD の動作を設定する。

[ノート] Rev.8.01.12 以降で使用可能。

[初期値]

type=off
version=1,2
syslog=off
robust-variable=2

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

29.7.2 MLD の静的な設定

[書式]

ipv6 *interface* **mld static** *group* [*filter_mode source ...*]
ipv6 pp mld static *group* [*filter_mode source ...*]
ipv6 tunnel mld static *group* [*filter_mode source ...*]
no ipv6 *interface* **mld static** *group* [*filter_mode source ...*]
no ipv6 pp mld static *group* [*filter_mode source ...*]
no ipv6 tunnel mld static *group* [*filter_mode source ...*]

[設定値]

- *interface*.....LAN インタフェース名
- *group*..... グループのマルチキャストアドレス
- *filter_mode*..... フィルタモード
  - include.....MLD の "INCLUDE" モード
  - exclude.....MLD の "EXCLUDE" モード
- *source*..... マルチキャストパケットの送信元のアドレス

[説明]

指定したグループについて、常にリスナーが存在するものとみなす。
このコマンドは、MLD をサポートするリスナーがいないときに設定する。
filter_mode と *source* は、マルチキャストパケットの送信元を限定するものである。*filter_mode* として include を指定したときには、*source* として受信したい送信元を列挙する。*filter_mode* として exclude を指定したときには、*source* として受信したくない送信元を列挙する。

[ノート]

このコマンドで設定されたリスナーは、**ipv6** *interface* **mld** コマンドで host を設定したインタフェースで通知される。もし、このインタフェースが MLDv1 を使う場合には、*filter_mode* や *source* の値は無視される。
Rev.8.01.12 以降で使用可能。

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

29.7.3 IPv6 マルチキャストの転送モードの設定

[書式]

ipv6 multicast routing process *mode*
no ipv6 multicast routing process

[設定値]

- *mode*
  - fast..... ファストパスで処理する
  - normal ..... ノーマルパスで処理する

[説明]

IPv6 マルチキャストの転送モードを設定する。

[ノート]

パケットの受信インタフェースと送信インタフェースが、LAN インタフェースか PPPoE インタフェースのいずれかであれば、ファストパスで処理することができる。そうでなければ、このコマンドの設定に関係なく、ノーマルパスとなる。
Rev.8.01.12 以降で使用可能。
このコマンドは、Rev.8.03.37 以降では **ipv6 routing process** コマンドに統合された。

[初期値]

fast

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

29.8 近隣要請

29.8.1 アドレス重複チェックをトリガに近隣要請を行うか否かの設定

[書式]

ipv6 nd ns-trigger-dad on *[option=value]*
ipv6 nd ns-trigger-dad off
no ipv6 nd ns-trigger-dad *[...]*

[設定値]

- on ..... 近隣要請を行う
- off ..... 近隣要請を行わない
- *option=value* 列

option	*value*	説明
na-proxy	all	近隣要請を行った後で、アドレス重複チェックの送信元への近隣広告はすべてプロキシする
	discard-one-time	近隣要請を行った後で、アドレス重複チェックの送信元への近隣広告を一回のみ破棄し、その後はプロキシする

[説明]

RA プロキシにおいて、下流よりアドレス重複チェックの近隣要請を受信した際に、そのグローバルアドレスを送信元とした近隣要請を上流に送信するか否かを設定する。

[ノート]

以下のリビジョンで使用可能。
Rev.8.01.27 以降、Rev.8.03.75 以降、Rev.10.00.38 以降、Rev.10.01 系

[初期値]

off
na-proxy=all

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

30. OSPFv3

30.1 OSPFv3 の有効設定

[書式] **ipv6 ospf configure refresh**

[説明] OSPFv3 の設定を有効にする。OSPFv3 関係の設定を変更したら、ルーターを再起動するか、あるいはこのコマンドを実行しなくてはならない。

[ノート] このコマンドを入力したとき、次のいずれかならば、OSPFv3 の設定は有効にならない。
- ルーター ID が設定されていない
- エリアが設定されていない
- いずれのインタフェースもエリアに属していない
- 仮想リンクが経由するエリアが存在しない
- 仮想リンクが経由するエリアに属するインタフェースが存在しない

すでに OSPFv3 の設定が有効であるときにこのコマンドを入力した場合、初期状態から再度設定を読み込む。よって、それまで OSPFv3 が保持していた経路情報や、他のプロトコルに配布した経路情報は一旦破棄され、初期状態から動作を開始する。

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

30.2 OSPFv3 の使用設定

[書式] **ipv6 ospf use** *use*
no ipv6 ospf use [*use*]

[設定値] ◦ *use*
- on ..... OSPFv3 を使用する
- off..... OSPFv3 を使用しない

[説明] OSPFv3 を使用するか否かを設定する。

[初期値] off

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

30.3 OSPFv3 のルーター ID 設定

[書式] **ipv6 ospf router id** *router-id*
no ipv6 ospf router id [*router-id*]

[設定値] ◦ *router-id* .....IPv4 アドレス表記 (0.0.0.0 は不可)

[説明] ルーター ID を設定する。

[ノート] **ipv6 ospf configure refresh** コマンドが入力されたとき、このコマンドによってルーターID が設定されていない場合、LAN インタフェースの中でインタフェースの若いものから順にサーチして、プライマリ IPv4 アドレスが付与されているインタフェースの IPv4 アドレスをルーター ID とする。

プライマリ IPv4 アドレスが付与されたインタフェースがない場合は初期値は設定されない。

[初期値] なし

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

30.4 OSPFv3 エリア設定

[書式] **ipv6 ospf area** *area* [stub [cost=*cost*]]
no ipv6 ospf area *area* [stub [cost=*cost*]]

[設定値] ◦ *area*
- backbone ..... バックボーンエリア
- 1 以上の数値 (1…4294967295) ..... 非バックボーンエリア
- IPv4 アドレス表記 (0.0.0.0 は不可) ..... 非バックボーンエリア

◦ *cost* ..... デフォルト経路のコスト (0 ～ 16777215)

[説明] OSPFv3 エリアを設定する。

stub キーワードを指定した場合、そのエリアはスタブエリアであることを表わす。*cost* は 0 以上の数値で、エリア境界ルーターがエリア内に広告するデフォルト経路のコストとして使われる。*cost* を指定しないとデフォルト経路の広告は行われない。

[初期値] スタブエリアではない
cost = 0

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

30.5 エリアへの経路広告

[書式] **ipv6 ospf area network** *area ipv6_prefix/prefix_len* [restrict]
no ipv6 ospf area network *area ipv6_prefix/prefix_len* [restrict]

[設定値] ◦ *area*
- backbone ..... バックボーンエリア
- 1 以上の数値 (1…4294967295) ..... 非バックボーンエリア
- IPv4 アドレス表記 (0.0.0.0 は不可) ..... 非バックボーンエリア

◦ *ipv6_prefix/prefix_len* ..... IPv6 プレフィクス

[説明] エリア境界ルーターが他のエリアに経路を広告する場合に、このコマンドで指定したサブネットの範囲内の経路は単一のサブネット経路として広告する。restrict キーワードが指定された場合には、範囲内の経路は要約した経路も広告しない。

[初期値] サブネットの範囲は設定されていない

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

30.6 指定インタフェースの OSPFv3 エリア設定

[書式] **ipv6** *interface* **ospf area** *area* [*parameters …*]
ipv6 pp ospf area *area* [*parameters …*]
ipv6 tunnel ospf area *area* [*parameters …*]
no ipv6 *interface* **ospf area** [*area* [*parameters …*]]
no ipv6 pp ospf area [*area* [*parameters …*]]
no ipv6 tunnel ospf area [*area* [*parameters …*]]

[設定値] ◦ *interface* ..... LAN インタフェース名、LOOPBACK インタフェース名

◦ *area*
- backbone ..... バックボーンエリア
- 1 以上の数値 (1…4294967295) ..... 非バックボーンエリア
- IPv4 アドレス表記 (0.0.0.0 は不可) ..... 非バックボーンエリア

◦ *parameters* ..... NAME=VALUE の列

[説明]

指定したインタフェースの属する OSPFv3 エリアを設定する。NAME パラメータの type はインタフェースの接続するリンクがどのようなタイプであるかを設定する。*parameters* では、リンクパラメータを設定する。パラメータは NAME=VALUE の形で指定され、以下の種類がある。

NAME	VALUE	説明
type	broadcast	ブロードキャスト型
	point-to-point	ポイント・ポイント型
passive		インタフェースに対して、OSPFv3 パケットを送信しない。該当インタフェースに他の OSPFv3 ルーターがいない場合に設定する。
cost	コスト (1…65535)	インタフェースのコストを設定する。初期値はインタフェースの種類と回線速度によって決定される。LAN インタフェースの場合は 1、トンネルインタフェースの場合は 1562、PP インタフェースの場合は、バインドされている回線の回線速度を S[kbit/s] とすると、以下の計算式で決定される。例えば、64kbit/s の場合は 1562、1.536Mbit/s の場合には 65 となる。 *cost* = 100000 / S
priority	優先度 (0…255)	指定ルーター選択の際の優先度を設定する。値が大きいルーターが指名ルーターに選ばれる。0 を指定すると指定ルーターに選ばれなくなる。
retransmit-interval	秒数 (1…65535)	LSA を連続して送る場合の再送間隔を秒単位で指定する。
transmit-delay	秒数 (1…65535)	リンクの状態が変わってから LSA を送信するまでの時間を秒単位で設定する。
hello-interval	秒数 (1…65535)	HELLO パケットの送信間隔を秒単位で設定する
dead-interval	秒数 (1…65535)	近隣ルーターから HELLO を受け取れない場合に、近隣ルーターがダウンしたと判断するまでの時間を秒単位で設定する。

LOOPBACK インタフェースに設定する場合は、type パラメータでインタフェースタイプを、cost パラメータでインタフェースのコストを指定できる。LOOPBACK インタフェースのタイプで指定できるのは、以下の 2 種類だけとなる。

NAME	VALUE	広告される経路の種類	OSPF 的なインタフェースの扱い	
			タイプ	状態
type	loopback	LOOPBACK インタフェースの IP アドレスのみのホスト経路	point-to-point	Loopback
	loopback-network	LOOPBACK インタフェースの implicit なネットワーク経路	NBMA	DROther

[ノート]

◦ NAME パラメータの type について

NAME パラメータの type として、LAN インタフェースは broadcast のみが設定できる。PP インタフェースで PPP を利用する場合や、トンネルインタフェースを利用する場合は、point-to-point のみが設定できる。

◦ passive について

passive は、インタフェースが接続しているリンクに他の OSPFv3 ルーターが存在しない場合に指定する。passive を指定しておくと、インタフェースから OSPFv3 パケットを送信しなくなるので、無駄なトラフィックを抑制したり、受信側で誤動作の原因になるのを防ぐことができる。

LAN インタフェース (type=broadcast であるインタフェース) の場合には、インタフェースが接続しているリンクへの経路は、**ipv6** *interface* **ospf area** コマンドを設定していないと他の OSPFv3 ルーターに広告されない。そのため、OSPFv3 を利用しないリンクに接続する LAN インタフェースに対しては、passive を付けた **ipv6** *interface* **ospf area** コマンドを設定しておくことでそのリンクでは OSPFv3 を利用しないまま、そこへの経路を他の OSPFv3 ルーターに広告することができる。

PP インタフェースに対して **ipv6 pp ospf area** コマンドを設定していない場合は、インタフェースが接続するリンクへの経路は外部経路として扱われる。外部経路なので、他の OSPFv3 ルーターに広告するには **ipv6 ospf import** コマンドの設定が必要である。

◦ hello-interval/dead-interval について

hello-interval/dead-interval の値は、そのインタフェースから直接通信できるすべての近隣ルーターとの間で同じ値でなくてはならない。これらのパラメータが設定値とは異なる HELLO パケットを受信した場合には、それは無視される。

◦ インスタンス ID について

本機のインスタンス ID は常に 0 であり、OSPFv3 パケットを受信する場合には、同じ値を持つパケットのみを受信する。

LOOPBACK インタフェースを指定できるのは Rev.8.03 以降のリビジョンである。

[初期値] area = インタフェースは OSPFv3 エリアに属していない
type = broadcast (LAN インタフェース設定時)
= point-to-point (PP インタフェース設定時、トンネルインタフェース設定時)
= loopback (LOOPBACK インタフェース設定時)
passive = インタフェースは passive ではない
cost = 1 (LAN インタフェース、LOOPBACK インタフェース設定時)、1562 (トンネル設定時)、
pp は回線速度に依存
priority = 1
retransmit-interval = 5 秒
transmit-delay = 1 秒
hello-interval = 10 秒
dead-interval = 40 秒

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

30.7 仮想リンク設定

[書式] **ipv6 ospf virtual-link** *router_id area* [*parameters ...*]
no ipv6 ospf virtual-link *router_id* [*area* [*parameters ...*]]

[設定値]
◦ *router_id* ..... 仮想リンクの相手のルーター ID
◦ *area* ..... 経由するエリア
- 1 以上の数値 (1...4294967295) ..... 非バックボーンエリア
- IPv4 アドレス表記 (0.0.0.0 は不可) ..... 非バックボーンエリア

◦ *parameters* ..... NAME=VALUE の列

[説明] 仮想リンクを設定する。仮想リンクは *router_id* で指定したルーターに対して、*area* で指定したエリアを経由して設定される。*parameters* では、仮想リンクのパラメータが設定できる。パラメータは NAME=VALUE の形で指定され、以下の種類がある。

NAME	VALUE	説明
retransmit-interval	秒数 (1...65535)	LSA を連続して送る場合の再送間隔を秒数で設定する。
transmit-delay	秒数 (1...65535)	リンクの状態が変わってから LSA を送信するまでの時間を秒単位で設定する。
hello-interval	秒数 (1...65535)	HELLO パケットの送信間隔を秒単位で設定する。
dead-interval	秒数 (1...65535)	相手から HELLO を受け取れない場合に、相手がダウンしたと判断するまでの時間を秒単位で設定する。

[ノート] ◦ hello-interval/dead-interval について
hello-interval と dead-interval の値は、そのインタフェースから直接通信できるすべての近隣ルーターとの間で同じ値でなくてはならない。これらのパラメータの値が設定値とは異なっている HELLO パケットを受信した場合には、それは無視される。

◦ インスタンス ID について
本機のインスタンス ID は常に 0 であり、OSPFv3 パケットを受信する場合には、同じ値を持つパケットのみを受信する。

◦ 出力インタフェースについて
仮想リンクを設定した場合、経由するエリアへの出力インタフェースにグローバルアドレスが付与されていなければ、仮想リンクは使用できない。

[初期値] *router_id*, *area* = なし
retransmit-interval = 5 秒
transmit-delay = 1 秒
hello-interval = 10 秒
dead-interval = 40 秒

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

30.8 OSPFv3 による経路の優先度設定

[書式] **ipv6 ospf preference** *preference*
no ipv6 ospf preference [*preference*]

[設定値] ◦ *preference*.....OSPFv3 による経路の優先度 (1...2147483647)

[説明] OSPFv3 による経路の優先度を設定する。優先度は 1 以上の数値で表され、数字が大きい程優先度が高い。OSPFv3 と RIPng など複数のプロトコルで得られた経路が食い違う場合には、優先度が高い方が採用される。優先度が同じ場合には時間的に先に採用された経路が有効となる。

[ノート] 静的経路の優先度は 10000 で固定である。

[初期値] 2000

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

30.9 OSPFv3 で受け取った経路をルーティングテーブルに反映させるか否かの設定

[書式] **ipv6 ospf export from ospf** filter *filter_num ...*
no ipv6 ospf export from ospf [filter *filter_num ...*]

[設定値] ◦ *filter_num* **..... ipv6 ospf export filter** コマンドのフィルタ番号 (1...2147483647)

[説明] OSPFv3 で受け取った経路をルーティングテーブルに導入するかどうかを設定する。指定した順にフィルタを評価し、最初に合致したフィルタによって導入すると判断された経路だけがルーティングテーブルに導入される。導入しないと判断された経路や合致するフィルタがない経路は導入されない。

このコマンドが設定されていない場合には、すべての経路がルーティングテーブルに導入される。

[ノート] このコマンドは OSPFv3 のリンク状態データベースには影響を与えない。つまり、OSPFv3 で他のルーターと情報をやり取りする動作としては、このコマンドがどのように設定されていても変化はない。OSPFv3 で計算した経路が実際にパケットをルーティングするために使われるかどうかだけが変わる。

[初期値] すべての経路がルーティングテーブルに導入される

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

30.10 OSPFv3 で受け取った経路をどう扱うかのフィルタの設定

[書式] **ipv6 ospf export** filter *filter_num* [*nr*] *kind ipv6_prefix/prefix_len* ...
no ipv6 ospf export filter *filter_num* [...]

[設定値]
- *filter_num* ..... フィルタ番号 (1...2147483647)
- *nr* ..... フィルタの解釈の方法
  - not ..... IPv6 プレフィクスに該当しない経路を導入する
  - reject ..... IPv6 プレフィクスに該当した経路を導入しない
- *kind* ..... IPv6 プレフィクスの解釈の方法
  - include ..... 指定した IPv6 プレフィクスに含まれる経路 (IPv6 プレフィクス自身を含む)
  - refines ..... 指定した IPv6 プレフィクスに含まれる経路 (IPv6 プレフィクス自身を含まない)
  - equal ..... 指定した IPv6 プレフィクスに一致する経路
- *ipv6_prefix/prefix_len* ..... IPv6 プレフィクス

[説明] OSPFv3 により他の OSPFv3 ルーターから受け取った経路をルーティングテーブルに導入する際に適用するフィルタを定義する。このコマンドで定義したフィルタは、**ipv6 ospf export from** コマンドの *filter* 項で指定されてはじめて効果を持つ。

ipv6_prefix/prefix_len では、IPv6 プレフィクスを設定する。これは複数設定でき、*kind* に指定した方法で解釈される。

- include ..... IPv6 プレフィクスと一致する経路および、IPv6 プレフィクスに含まれる経路が該当
- refines ..... IPv6 プレフィクスに含まれる経路が該当するが、IPv6 プレフィクスと一致する経路は含まれない
- equal ..... IPv6 プレフィクスに一致する経路のみ該当

nr が省略されている場合には、一つでも該当する IPv6 プレフィクスがある場合にフィルタに合致したものとし、その経路を導入する。not 指定時には、いずれの IPv6 プレフィクスにも該当しなかった場合にフィルタに合致したものとし、その経路を導入する。reject 指定時には、一つでも該当する IPv6 プレフィクスがある場合にフィルタに合致したものとし、その経路を導入しない。

[ノート] not 指定のフィルタを **ipv6 ospf export from ospf** コマンドで複数設定する場合には注意が必要である。not 指定のフィルタに合致する IPv6 プレフィクスは、そのフィルタでは導入するかどうかが決定しないため、**ipv6 ospf export from ospf** コマンドで指定された次のフィルタで評価される。そのため、例えば、以下のような設定ではすべての経路が導入されることになりフィルタの意味がない。

```
ipv6 ospf export from ospf filter 1 2
ipv6 ospf export filter 1 not equal fec0:12ab:34cd:1::/64
ipv6 ospf export filter 2 not equal fec0:12ab:34cd:2::/64
```

1 番のフィルタは fec0:12ab:34cd:1::/64 以外の経路に合致し、2 番のフィルタは fec0:12ab:34cd:2::/64 以外の経路に合致する。つまり、経路 fec0:12ab:34cd:1::/64 は 1 番のフィルタに合致しないが、2 番のフィルタに合致するため導入される。一方で経路 fec0:12ab:34cd:2::/64 は 1 番のフィルタに合致するため、2 番のフィルタにかかわらず導入される。よって、導入されない経路は存在しない。

経路 fec0:12ab:34cd:1::/64 と経路 fec0:12ab:34cd:2::/64 を導入したくない場合には以下のような設定を行なう必要がある。

```
ipv6 ospf export from ospf filter 1
ipv6 ospf export filter 1 not equal fec0:12ab:34cd:1::/64 fec0:12ab:34cd:2::/64
```

あるいは、

```
ipv6 ospf export from ospf filter 1 2 3
ipv6 ospf export filter 1 reject equal fec0:12ab:34cd:1::/64
ipv6 ospf export filter 2 reject equal fec0:12ab:34cd:2::/64
ipv6 ospf export filter 3 include ::/0
```

[初期値] フィルタは設定されていない

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

30.11 外部プロトコルによる経路導入

[書式] **ipv6 ospf import from** *protocol* [filter *filter_num* ...]
no ipv6 ospf import from [*protocol* [filter *filter_num* ...]]

[設定値]
- *protocol*..... OSPFv3 の経路テーブルに導入する外部プロトコル
  - static ..... 静的経路
  - rip..... RIPng
- *filter_num*..... **ipv6 ospf import filter** コマンドのフィルタ番号 (1...2147483647)

[説明] OSPFv3 の経路テーブルに外部プロトコルによる経路を導入するかどうかを設定する。導入した経路は外部経路として他の OSPFv3 ルーターに広告される。
filter_num は **ipv6 ospf import filter** コマンドで定義したフィルタ番号を指定する。外部プロトコルから導入されようとする経路は指定した順にフィルタにより評価される。最初に合致したフィルタによって導入すると判断された経路は OSPFv3 に導入される。導入しないと判断された経路や合致するフィルタがない経路は導入されない。また、filter キーワード以降を省略した場合には、すべての経路が OSPFv3 に導入される。

経路を広告する場合のパラメータであるメトリック値、メトリックタイプは、フィルタの検査で該当した **ipv6 ospf import filter** コマンドで指定されたものを使う。filter キーワード以降を省略した場合には、以下のパラメータを使用する。

metric = 1
type = 2

[初期値] 外部プロトコルから経路は導入しない

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

30.12 外部経路導入に適用するフィルタ定義

[書式] **ipv6 ospf import** filter *filter_num* [*nr*] *kind ipv6_prefix/prefix_len* ... [*parameters* ...]
no ipv6 ospf import filter *filter_num* [[*nr*] *kind ipv6_prefix/prefix_len* ... [*parameters* ...]]

[設定値]
- *filter_num*..... フィルタ番号 (1...2147483647)
- *nr*..... フィルタの解釈の方法
  - not..... IPv6 プレフィクスに該当しない経路を導入する
  - reject ..... IPv6 プレフィクスに該当する経路を導入しない
- *kind*..... IPv6 プレフィクスの解釈の方法
  - include..... 指定した IPv6 プレフィクスに含まれる経路 (IPv6 プレフィクス自身を含む)
  - refines ..... 指定した IPv6 プレフィクスに含まれる経路 (IPv6 プレフィクス自身を含まない)
  - equal ..... 指定した IPv6 プレフィクスに一致する経路
- *ipv6_prefix/prefix_len*..... IPv6 プレフィクス
- *parameters*..... 外部経路を広告するときのパラメータ
  - metric = *metric*..... メトリック値 (1 ～ 16777215)
  - type = *type* ..... メトリックのタイプ (1 または 2)

[説明] OSPFv3 の経路テーブルに外部経路を導入する際に適用するフィルタを定義する。このコマンドで定義したフィルタは **ipv6 ospf import from** コマンドの filter 項で指定されてはじめて効果を持つ。

ipv6_prefix/prefix_len では IPv6 プレフィクスを指定する。これは複数指定でき、*kind* に指定した方法で解釈される。

- include .....IPv6 プレフィクスと一致する経路および、IPv6 プレフィクスに含まれる経路が該当
- refines.....IPv6 プレフィクスに含まれる経路が該当するが、IPv6 プレフィクスと一致する経路は該当しない
- equal .....IPv6 プレフィクスに一致する経路のみ該当

nr が省略されている場合には、一つでも該当する IPv6 プレフィクスがある場合にフィルタに合致したものとし、その経路を導入する。not 指定時には、いずれの IPv6 プレフィクスにも該当しなかった場合にフィルタに合致したものとし、その経路を導入する。reject 指定時には、一つでも該当する IPv6 プレフィクスがある場合にフィルタに合致したものとし、その経路を導入しない。

parameters では、導入する経路を OSPFv3 の外部経路として広告する場合のパラメータとして、メトリック値、メトリックタイプがそれぞれ metric、type により指定できる。これらを省略した場合には、以下の値が採用される。

```
metric = 1
type = 2
```

[ノート] not 指定のフィルタを **ipv6 ospf import from** コマンドで複数設定する場合には注意が必要である。not 指定のフィルタに合致しない経路は、そのフィルタでは導入するかどうかが決定しないため、**ipv6 ospf import from** コマンドで指定された次のフィルタで評価される。そのため、例えば以下のような設定ではすべての経路が導入されることになりフィルタの意味がない。

```
ipv6 ospf import from static filter 1 2
ipv6 ospf import filter 1 not equal fec0:12ab:34cd:1::/64
ipv6 ospf import filter 2 not equal fec0:12ab:34cd:2::/64
```

1 番のフィルタは fec0:12ab:34cd:1::/64 以外の経路に合致し、2 番のフィルタは fec0:12ab:34cd:2::/64 以外の経路に合致する。つまり、経路 fec0:12ab:34cd:1::/64 は 1 番のフィルタに合致しないが、2 番のフィルタに合致するため導入される。一方で経路 fec0:12ab:34cd:2::/64 は 1 番のフィルタに合致するため、2 番のフィルタにかかわらず導入される。よって、導入されない経路は存在しない。

経路 fec0:12ab:34cd:1::/64 と経路 fec0:12ab:34cd:2::/64 を導入したくない場合には以下のような設定を行う必要がある。

```
ipv6 ospf import from static filter 1
ipv6 ospf import filter 1 not equal fec0:12ab:34cd:1::/64 fec0:12ab:34cd:2::/64
```

あるいは、

```
ipv6 ospf import from static filter 1 2 3
ipv6 ospf import filter 1 reject equal fec0:12ab:34cd:1::/64
ipv6 ospf import filter 2 reject equal fec0:12ab:34cd:2::/64
ipv6 ospf import filter 3 include ::/0
```

[初期値] フィルタは設定されていない

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

30.13 OSPFv3 のログ出力設定

[書式] **ipv6 ospf log** *log ...*
no ipv6 ospf log [*log ...*]

[設定値] ◦ *log*
- interface..... インタフェースの状態や仮想リンクに関わるログ
- neighbor..... 近隣ルーターの状態に関わるログ
- packet..... OSPFv3 パケットに関わるログ

[説明] OSPFv3 に関わるログ出力の種類を設定する。

[初期値] いずれの種類のログも出力しない

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

31. 状態メール通知機能

この機能は、ルーターの状態を表現する情報を一括してメールで送信する仕組みを提供します。本来は、WWW ブラウザ設定機能のために追加された機能ですが、下記のコマンドを設定するとコンソールからも利用することができます。

31.1　状態メール通知機能の動作の設定

[書式]　**mail-notify status use** *use*
no mail-notify status use

[設定値]　◦ *use*
- on ..... 使用する
- off..... 使用しない

[説明]　状態メール通知機能を使用するか否かを設定する。

[ノート]　Rev.8.01.07 以降で使用可能。

[初期値]　on

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	~~RTX1200~~	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

31.2　メールサーバーの設定

[書式]　**mail-notify status server** *server*
no mail-notify status server

[設定値]　◦ *server*..... SMTP サーバーの IP アドレスまたはドメイン名

[説明]　状態メール通知機能で使用するメールサーバーを設定する。

[ノート]　Rev.8.01.07 以降で使用可能。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	~~RTX1200~~	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

31.3　送信元のメールアドレスの設定

[書式]　**mail-notify status from** *address*
no mail-notify status from

[設定値]　◦ *address*.....送信元メールアドレス

[説明]　状態メール通知機能で使用する送信元メールアドレスを設定する。

[ノート]　Rev.8.01.07 以降で使用可能。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	~~RTX1200~~	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

31.4　送信先メールアドレスの設定

[書式]　**mail-notify status to** *id address* [*option*]
no mail-notify status to *id*

[設定値]　◦ *id* .....識別子 (1..4)
◦ *address*.....送信先メールアドレス
◦ *option*
- alert .....警告のみを送信する。

[説明]　状態メール通知機能の送信先メールアドレスを設定する。複数のメールアドレスを設定する場合には、異なる識別子を使って複数のコマンドを設定する。

[ノート]　Rev.8.01.07 以降で使用可能。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	~~RTX1200~~	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

31.5　サブジェクトの設定

[書式]　**mail-notify status subject** *subject*
no mail-notify status subject

[設定値]　◦ *subject*..... メールのサブジェクト

[説明]　状態メール通知機能で送信するメールのサブジェクトを設定する。

[ノート]　Rev.8.01.07 以降で使用可能。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	~~RTX1200~~	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

31.6　送信タイムアウトの設定

[書式]　**mail-notify status timeout** *timeout*
no mail-notify status timeout

[設定値]　◦ *timeout*..... タイムアウト秒数 (1..180)

[説明]　メールの送信が成功しないときに失敗と判断するまでの時間を設定する。

[ノート]　Rev.8.01.07 以降で使用可能。

[初期値]　30

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	~~RTX1200~~	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

31.7　通知内容の設定

[書式]　**mail-notify status type** *info* [*info* ...]
no mail-notify status type

[設定値]　◦ *info*..... 通知する情報
- all..... すべての内容を通知
- interface..... インタフェースの情報を通知
- routing..... ルーティングの情報を通知
- vpn..... VPN の情報を通知
- nat..... NAT の情報を通知
- firewall..... ファイウォールの情報を通知
- config-log..... 設定情報とログを通知

[説明]　状態メール通知機能で送信するメールの内容を設定する。all を設定したときには、他のキーワードに関係なく、すべてを通知する。

[ノート]　Rev.8.01.07 以降で使用可能。

[初期値]　all

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	~~RTX1200~~	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

31.8　状態メール通知の実行

[書式]　**mail-notify status exec**

[説明]　状態メール通知機能でメールを送信する。

[ノート]　Rev.8.01.07 以降で使用可能。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	~~RTX1200~~	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

32. トリガによるメール通知機能

この機能は、あらかじめ設定したトリガを検出してその内容をメールで通知する機能です。
mail notify コマンドで設定したトリガを検出すると、**mail template** コマンドで設定したメールテンプレートを基にメールを作成し、**mail server smtp** コマンドで指定したメールサーバーを使用して変更内容を記述したメールを送信します。

SMTP 認証として、CRAM-MD5/DIGEST-MD5/PLAIN に対応しており、POP-before-SMTP にも対応しています。

32.1　メール設定識別名の設定

[書式]
mail server name *id name*
no mail server name *id* [*name*]

[設定値]
- *id* ..... メールサーバー設定 ID(1..10)
- *name* ..... 識別名

[説明]
メール設定の識別名を設定する。空白を伴う識別名の場合は、「"」で囲む必要がある。

[ノート]
Rev.8.03 系以降のすべてのリビジョンで使用可能。

[初期値]
なし

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

32.2　SMTP メールサーバーの設定

[書式]
mail server smtp *id address* [port = *port*] [smtp-auth *username password* [*auth_protocol*]]
[pop-before-smtp]
no mail server smtp *id* [...]

[設定値]
- *id* ..... メールサーバー設定 ID(1..10)
- *address* ..... サーバーの IP アドレスまたはホスト名
- *port* ..... サーバーのポート番号 (省略時は 25)
- *username* ..... 認証用ユーザ名
- *password* ..... 認証用パスワード
- *auth_protocol* ..... SMTP-AUTH 認証プロトコル
  - cram-md5 ..... CRAM-MD5
  - digest-md5 ..... DIGEST-MD5
  - plain ..... PLAIN 認証
- pop-before-smtp ..... POP before SMTP の使用

[説明]
メール送信に使用するサーバー情報を設定する。
smtp-auth パラメータでは、メール送信の際の SMTP 認証のためのデータ (ユーザ名、パスワード) を指定する。SMTP サーバーで認証が必要ない場合は smtp-auth の設定は必要ない。
SMTP 認証でサポートしている認証プロトコルは、CRAM-MD5、DIGEST-MD5 および PLAIN 認証の 3 種類である。*smtp-auth* パラメータでプロトコルを指定した場合にはそれを用い、プロトコルが省略された場合には SMTP サーバーとの前記の順で認証交渉を行う。
pop-before-smtp パラメータを設定すると、メール送信時に POP before SMTP 動作を行う。ここで行う POP 動作は、**mail server pop** コマンドで同じ ID で設定したものを利用する。*pop-before-smtp* パラメータが設定されているのに、対応する **mail server pop** コマンドの設定がないと、メールは送信できない。

[ノート]
Rev.8.03 系以降のすべてのリビジョンで使用可能。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

32.3　POP メールサーバーの設定

[書式]　**mail server pop** *id address* [port = *port*] *protocol username password*
no mail server pop *id* [...]

[設定値]
- *id*..... メールサーバー設定 ID(1..10)
- *address*..... サーバーの IP アドレスまたはホスト名
- *port*..... サーバーのポート番号 (省略時は 110)
- *Protocol*
  - pop3..... POP3
  - apop..... APOP
- *username*..... 認証用ユーザ名
- *password*..... 認証用パスワード

[説明]　メール受信に使用するサーバー情報を設定する。

[ノート]　Rev.8.03 系以降のすべてのリビジョンで使用可能。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

32.4　メール処理のタイムアウト値の設定

[書式]　**mail server timeout** *id timeout*
no mail server timeout *id* [*timeout*]

[設定値]
- *id*..... メールサーバー設定 ID(1..10)
- *timeout*..... タイムアウト値 (1..600 秒)

[説明]　メールの送受信処理に対するタイムアウト値を設定する。
指定した時間以内にメールの処理が終らない時には、いったん処理を中断して、**mail template** コマンドで設定した待機時間 (デフォルトは 30 秒) の間を置いた後、メール処理を最初からやり直す。処理のやり直しは、最初のメール処理を除き、最大 3 回行われる。最大回数を超えた場合には、メール処理は失敗となる。

[ノート]　Rev.8.03 系以降のすべてのリビジョンで使用可能。

[初期値]　60 秒

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

32.5　メールの送信時に使用するテンプレートの設定

[書式]　**mail template** *template_id mailserver_id* From:*from_address* To:*to_address* [Subject:*subject*] [Date:*date*] [*mime*-Version:*mime_version*] [Content-Type:*content_type*] [notify-log=*switch*] [notify-wait-time=*sec*]
no mail template *template_id* [...]

[設定値]
- *template_id*..... メールテンプレート ID(1..10)
- *mailserver_id*..... このテンプレートで使用するメールサーバー ID(1..10)
- From:*from_address*..... 送信元メールアドレス
- To:*to_address*..... 宛先メールアドレス
- Subject:*subject*..... 送信時の件名
- Date:*date*..... メールのヘッダに表示する時刻
- MIME-Version:*mime_version*..... メールのヘッダに表示する MIME-Version
- Content-Type:*content_type*..... メールのヘッダに表示する Content-Type
- *switch*
  - on..... 通知系のメール内容に syslog の内容を含める
  - off..... 通知系のメール内容に syslog の内容を含めない
- *sec*..... 通知系のメール送信時に、実際に送信されるまでの待機時間を指定する。

[説明]　メール送信時に使用するメールサーバー設定 ID、送信元メールアドレス、宛先メールアドレスおよびヘッダ等を設定する。
from_address に送信元メールアドレスを指定する。送信元メールアドレスは一つしか指定できない。
to_address に宛先メールアドレスを指定する。宛先メールアドレスは複数指定できる。複数指定する場合はカンマ (,) で区切り、間に空白を入れてはいけない。
メールアドレスは local-part@domain もしくは local-part@ipaddress の形式のみ対応している。"NAME >local-part@domain<" 等の形式には対応していない。

subject でメールの件名を指定する。空白を含む場合は、ダブルクォーテーション (") で Subject:*subject* 全体を囲む必要がある。
date には、RFC822 に示されるフォーマットの時刻を指定する。RFC822 のフォーマットでは必ず空白が含まれるため、ダブルクォーテーション (") で Date:*date* 全体を囲む必要がある。
content-type に指定できる type/subtype は "text/plain" のみで、パラメータは "charset=us-ascii" および "charset=iso-2022-jp" のみ対応している。

[ノート]　メールヘッダ情報として必須のものは、" 送信元メールアドレス " と " 宛先メールアドレス " になる。
Rev.8.03 系のすべてのリビジョンで使用可能。

[初期値]
subject.....なし
date.....送信時の時刻
mime-version.....1.0
content-type.....text/plain; charset=iso-2022-jp
notify-log.....off
notify-wait-time.....30

[表示例]
```
mail template 1 1 From:test@test.com To:test1@test.com,test2@test.com
    "Subject:Test Mail" notify-log=on
mail template 1 2 From:test@test.com To:test1@test.com
    "Subject:RTX1500 test" "Date:Mon, 23 Feb 2004 09:54:20 +0900"
    MIME-Version:1.0 "Content-Type:text/plain; charset=iso-2022-jp"
```

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

32.6　メール通知のトリガの設定

[書式]
mail notify *id template_id* **trigger backup** *if_b* [[*range_b*] *if_b* ...]
mail notify *id template_id* **trigger route** *route* [*route* ...]
mail notify *id template_id* **trigger filter ethernet** *if_f dir_f* [*if_f dir_f* [...]]
mail notify *id template_id* **trigger status** *type* [*type* [...]]
mail notify *id template_id* **trigger intrusion** *if_i* [*range_i*] *dir_i* [*if_i* [*range_i*] *dir_i* [...]]
no mail notify *id* [...]

[設定値]
◦ *id*.....設定番号 (1..10)
◦ *template_id*.....テンプレート ID (1..10)
◦ *if_b*.....メール通知を行うバックアップ対象のインタフェース
- pp.....PP バックアップ
- lanN.....LAN バックアップ
- tunnel.....TUNNEL バックアップ

◦ *range_b*.....インタフェース番号および範囲指定
pp, tunnel のみ (*,xx-yy,zz etc)
◦ *route*.....ネットマスク付きの経路
◦ *if_f*.....メール通知を行うフィルタの設定された LAN インタフェース
◦ *dir_f*.....フィルタ設定の方向
- in.....受信方向
- out.....送信方向

◦ *type*.....メール通知で通知する情報
- all.....全ての内容
- interface.....インタフェースの情報
- routing.....ルーティングの情報
- vpn.....VPN の情報
- nat.....NAT の情報
- firewall.....ファイアウォールの情報
- config-log.....設定情報とログ

◦ *if_i*.....不正アクセス検知設定のインタフェース (Rev.10.00.27 以降で利用可)
- pp.....PP インタフェース
- lanN(N,M, N/M)..LAN インタフェース
- tunnel.....TUNNEL インタフェース
- *.....全てのインタフェース

◦ *range_i*.....インタフェース番号および範囲指定 (Rev.10.00.27 以降で利用可)
lan (*, x)
pp, tunnel (*, x, xx-yy, zz etc)
◦ *dir_i*.....不正アクセス検知設定の方向 (Rev.10.00.27 以降で利用可)
- in.....受信方向
- out.....送信方向
- in/out.....受信 / 送信方向

[説明]　メール通知の行うトリガ動作の設定を行う。バックアップ、経路変更、フィルタログ表示、**mail notify status exec** コマンド実行時、および不正アクセス検知をトリガとして指定できる。

バックアップおよび経路については以下で設定されたものが対象となる。
- PP バックアップ..... **pp backup** コマンド
- LAN バックアップ..... **lan backup** コマンド
- TUNNEL バックアップ..... **tunnel backup** コマンド
- 経路に対するバックアップ..... **ip route** コマンド

フィルタについてはログ表示されるものが対象となる。
- イーサネットフィルタ ..... pass-log, reject-log パラメータの定義

内部状態を通知する場合は、**mail notify status exec** コマンドを実行する必要がある。

不正アクセス検知については **ip** *interface* **intrusion detection** コマンドの設定により検出されたものが通知対象となる。

また、一つのテンプレート ID に所属するメール通知設定はまとめて処理される。

[ノート]　trigger intrusion は以下のリビジョンで使用可能。
Rev.9.00.37 以降、Rev.10.00.27 以降、Rev.10.01 系

[初期値]　なし

[設定例]
```
mail notify 1 1 trigger backup pp * lan2 lan3 tunnel 1-10,12
mail notify 2 1 trigger route 192.168.1.0/24 172.16.0.0/16
mail notify 3 1 trigger filter ethernet lan1 in
mail notify 4 1 trigger status all
mail notify 5 1 trigger intrusion lan1 in/out pp * in tunnel 1-3,5 out
```

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

33. HTTP サーバー機能

33.1　共通の設定

33.1.1　HTTP サーバー機能の有無の設定

[書式]　**httpd service** *switch*
no httpd service

[設定値]　◦ *switch*
- on.....HTTP サーバー機能を有効にする
- off.....HTTP サーバー機能を無効にする

[説明]　HTTP サーバーを有効にするか否かを選択する。

[ノート]　Rev.8.01.07 以降で使用可能。

[初期値]　on

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

33.1.2　HTTP サーバーへアクセスできるホストの IP アドレス設定

[書式]　**httpd host** *host*
no httpd host

[設定値]　◦ *host*
- any.....すべてのホストからのアクセスを許可する
- lan.....LAN ポート (LAN1) 側ネットワーク内、あるいは、WAN ポート (LAN2) 側ネットワーク内ならば許可する
- lan1 .....LAN ポート (LAN1) 側ネットワーク内ならば許可する
- lan2 .....WAN ポート (LAN2) 側ネットワーク内ならば許可する
- lan3 .....LAN3 側ネットワーク内ならば許可する
- bridge1.....ブリッジ 側ネットワーク内ならば許可する
- none.....すべてのホストからのアクセスを禁止する
- HTTP サーバーへアクセスを許可するホストの IP アドレス
- HTTP サーバーへアクセスを許可するホストの IP アドレス範囲 (*ip_address-ip_address*)

[説明]　HTTP サーバーへのアクセスを許可するホストを設定します。

[ノート]　このコマンドで LAN インタフェースを指定した場合には、ネットワークアドレスとリミテッドブロードキャストアドレスを除く IP アドレスからのアクセスを許可する。指定した LAN インタフェースにプライマリアドレスもセカンダリアドレスも設定していなければ、アクセスを許可しない。

Rev.8.01.07 以降で使用可能。
LAN3 インタフェースを持たないモデルでは lan3 を指定することができない。
ブリッジインタフェースを指定できるのは Rev.10.00.38 以降のリビジョンである。

[初期値]　lan

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

33.1.3　HTTP サーバーのセッションタイムアウト時間の設定

[書式]　**httpd timeout** *time*
no httpd timeout [*time*]

[設定値]　◦ *time*.....秒数 (1..180)

[説明]　HTTP サーバーのタイムアウト時間を設定する。

[ノート]　インターネット経由でルーターにアクセスするときに、通信タイムアウトが発生するならば、このコマンドで大きな値を設定する。

Rev.8.01.07 以降で使用可能。

[初期値]　5

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

33.1.4　HTTP サーバー機能の listen ポートの設定

[書式]　**httpd listen** *port*
no httpd listen

[設定値]　◦ *port* ..... ポート番号 (1..65535)

[説明]　HTTP サーバーの待ち受けるポートを設定する。

[ノート]　Rev.8.01.07 以降で使用可能。

[初期値]　80

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

33.1.5　PP インタフェースとトンネルインタフェースの名前の設定

[書式]　**pp name** *name*
tunnel name *name*
no pp name
no tunnel name

[設定値]　◦ *name*..... 名前 (64 文字以内)

[説明]　PP インタフェースやトンネルインタフェースの名前を設定する。

[ノート]　このコマンドはかんたん設定ページ (RT107e) と WWW ブラウザ設定支援機能 (RT107e 以外) でのみ用いられる。
Rev.8.01.07 以降で使用可能。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

33.2　かんたん設定ページ用の設定

本節のコマンドは、RT107e のかんたん設定ページでプロバイダ接続を登録する際に使用され、「設定の確定」ボタンをクリックすることで自動的に設定されるものです。本節のコマンドを手動で設定することは、かんたん設定ページで登録した内容を変更することになるため、各コマンドの機能や動作を十分に理解した上で行ってください。

かんたん設定ページからはプロバイダの情報は最大 10 個まで登録でき、既に設定されている相手先情報番号のいずれかに **provider set** コマンドを使用して対応させます。
解除する場合には **no provider set** コマンドを使用します。
設定されたプロバイダを選択するには、**provider select** コマンドを使用します。本コマンドによりプロバイダを変更すると、プロバイダごとに異なる DNS やデフォルトルートの設定など、そのプロバイダに接続するために必要な事項を自動的に設定変更します。
プロバイダ設定の状況はかんたん設定ページで調べるか、**show config** コマンドで調べます。

33.2.1　プロバイダ接続タイプの設定

[書式]　**provider type** *provider_type*
no provider type [*provider_type*]

[設定値]　◦ *provider_type*
- isdn-terminal..... PPPoE 型の端末接続
- isdn-network..... PPPoE 型のネットワーク接続
- none..... 設定なし

[説明]　プロバイダの接続タイプを設定する。

[初期値]　none

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	~~SRT100~~

33.2.2　プロバイダ情報の PP との関連付けと名前の設定

[書式]　**provider set** *peer_num* [*name*]
no provider set *peer_num* [*name*]

[設定値]　◦ *peer_num*.....相手先情報番号
◦ *name*.....名前 (32 文字以内)

[説明]　プロバイダ切り替えを利用するために設定する。
結び付けられた相手先情報番号はプロバイダとして扱われる。何も設定されていない相手先情報番号に対しては無効である。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	~~SRT100~~

33.2.3　プロバイダ接続設定

[書式]　**provider select** *peer_num*
no provider select *peer_num*

[設定値]　◦ *peer_num*.....相手先情報番号

[説明]　接続するプロバイダ情報を選択し、利用可能にセットアップする。
本コマンドが実行されると、各種プロバイダ設定コマンドに記録された情報に基づき、デフォルトルート、DNS サーバー、スケジュール等の変更が行われる。
また、かんたん設定のプロバイダ接続設定において、接続先の変更や手動接続を行った場合にも、本コマンドが実行され接続先が切り替えられる。

本コマンドの上書き対象コマンドは以下の通り。
すべてのプロバイダ情報：pp disable
選択されたプロバイダ情報：pp enable、ip route、dns server および schedule at。

[ノート]　**provider set** コマンドに設定されていない相手先情報番号に対しては無効。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	~~SRT100~~

33.2.4　プロバイダの DNS サーバーのアドレス設定

[書式]　**provider dns server** *peer_num ip_address* [*ip_address..*]
no provider dns server *peer_num* [*ip_address..*]

[設定値]　◦ *peer_num*.....相手先情報番号
◦ *ip_address*.....DNS サーバーの IP アドレス (最大 4 つ)

[説明]　プロバイダごとの情報として DNS サーバーのアドレスを設定する。
プロバイダが選択された場合に、このアドレスが **dns server** コマンドに上書きされる。

[ノート]　**provider set** コマンドに設定されていない相手先情報番号に対しては無効。
削除時、**dns server** コマンドの内容はクリアされない。クリアされるのは **provider dns server** コマンドで設定された内容だけである。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	~~SRT100~~

33.2.5　LAN インタフェースの DNS サーバーのアドレスの設定

[書式]　**provider** *interface* **dns server** *ip_address* [*ip_address*]
no provider *interface* **dns** [*ip_address* [*ip_address*]]

[設定値]　◦ *interface*.....LAN インタフェース名
◦ *ip_address*.....DNS サーバーの IP アドレス (最大 2 つ)

[説明]　かんたん設定ページでプロバイダ情報として LAN インタフェース側 DNS サーバーの IP アドレスを設定する。

[初期値]　なし

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	~~SRT100~~

33.2.6 DNS サーバーを通知してくれる相手の相手先情報番号の設定

[書式] **provider dns server pp** *peer_num dns_peer_num*
no provider dns server pp *peer_num* [*dns_peer_num*]

[設定値] ◦ *peer_num*..... 相手先情報番号 (1..30)
◦ *dns_peer_num*..... DNS 通知相手先情報番号 (1..30)

[説明] プロバイダ情報として DNS サーバーを通知してくれる相手先情報番号を設定する。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	~~SRT100~~

33.2.7 フィルタ型ルーティングの形式の設定

[書式] **provider filter routing** *type*
no provider filter routing [*type*]

[設定値] ◦ *type*..... フィルタ型ルーティングの形式
• off..... かんたん設定で手動接続をした場合に、自動接続先が自動的に切り替わる
• connection..... かんたん設定で手動接続をした場合に、自動接続している間だけ有効なデフォルト経路が選択される。手動接続先が切断されると自動接続先に接続される

[説明] かんたん設定専用の識別コマンド。かんたん設定ページで選択中のフィルタ型ルーティングの形式を設定する。

[ノート] コンソールなどから設定した場合の動作は保証されない。

[初期値] off

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	~~SRT100~~

33.2.8 LAN 側のプロバイダ名称の設定

[書式] **provider** *interface* **name** *type:name*
no provider *interface* **name** [*type:name*]

[設定値] ◦ *interface*..... LAN インタフェース名
◦ *type*..... プロバイダ情報の識別情報 ("PRV" など)
◦ *name*..... ユーザが設定したプロバイダの名称など

[説明] かんたん設定専用の識別コマンド。かんたん設定ページでプロバイダ名称等で入力した名称が設定される。

[初期値] なし

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	~~SRT100~~

33.2.9 NTP サーバーの設定

[書式] **provider ntpdate** *server_name*
no provider ntpdate [*server_name*]

[設定値] ◦ *server_name*..... NTP サーバー名 (IP アドレスまたは FQDN)

[説明] かんたん設定専用の識別コマンド。
NTP サーバーを 1 箇所設定する。**provider ntp server** コマンドでは接続先ごとの IP アドレス情報を設定し、本コマンドでは 1 箇所の IP アドレスまたは FQDN を設定する。

[ノート] コンソールなどから手動設定した場合の動作は保証されない。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	~~SRT100~~

33.2.10　プロバイダの NTP サーバーのアドレス設定

[書式]　**provider ntp server** *peer_num ip_address*
no provider ntp server *peer_num* [*ip_address*]

[設定値]
- *peer_num*.....相手先情報番号
- *ip_address*.....NTP サーバーの IP アドレス

[説明]　プロバイダごとの情報として NTP サーバーのアドレスを設定する。
本コマンドで IP アドレスが設定されていると、プロバイダが選択されている場合に定期的に時刻を問い合わせる。プロバイダが選択された場合にスケジュールに組み込まれる。

[ノート]　**provider set** コマンドが実行されていない相手先情報番号に対しては無効。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	~~SRT100~~

33.2.11　かんたん設定ページの切断ボタンを押した後に自動接続するか否かの設定

[書式]　**provider auto connect forced disable** *switch*
no provider auto connect forced disable [*switch*]

[設定値]
- *switch*
  - on.....自動接続しない
  - off.....自動接続する

[説明]　かんたん設定ページの切断ボタンを押した後、自動接続を禁止するか否かを設定する。

[ノート]　on に設定してある場合、かんたん設定ページの手動切断ボタンを押した後に **pp disable** コマンドを、接続ボタンを押した後に **pp enable** コマンドを自動設定する。
そのため、切断ボタンを押した後は、自動接続をしなくなる。また、**connect** コマンドからは接続できなくなる。接続するには、手動接続ボタンを押すか、ルーターを再起動する必要がある。

[初期値]　off

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	~~SRT100~~

33.2.12　かんたん設定ページで IPv6 接続を行うか否かの設定

[書式]　**provider ipv6 connect pp** *peer_num connect*
no provider ipv6 connect pp *peer_num* [*connect*]

[設定値]
- *peer_num*.....相手先情報番号
- *connect*
  - on.....接続する
  - off.....接続しない

[説明]　かんたん設定ページでプロバイダ情報として IPv6 接続を有効にするか否かを設定する。

[ノート]　かんたん設定ページで IPv6 接続設定をした時に自動的に on になる。

[初期値]　off

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	~~SRT100~~

34. ネットボランチ DNS サービスの設定

ネットボランチ DNS とは、一種のダイナミック DNS 機能であり、ルーターの IP アドレスをヤマハが運営するネットボランチ DNS サーバーに希望の名前で登録することができる。そのため、動的 IP アドレス環境でのサーバー公開や拠点管理などに用いることができます。IP アドレスの登録、更新などの手順には独自のプロトコルを用いるため、他のダイナミック DNS サービスとの互換性はありません。

ヤマハが運営するネットボランチ DNS サーバーは現時点では無料、無保証の条件で運営されています。利用料金は必要ありませんが、ネットボランチ DNS サーバーに対して名前が登録できること、および登録した名前が引けることは保証できません。また、ネットボランチ DNS サーバーは予告無く停止することがあることに注意してください。

ネットボランチ DNS には、ホストアドレスサービスと電話番号サービスの 2 種類がありますが、本書で記述するモデルでは電話番号サービスは利用できません。

ネットボランチ DNS では、個々の RT シリーズ、ネットボランチシリーズルーターを MAC アドレスで識別しているため、機器の入れ換えなどをした場合には同じ名前がそのまま利用できる保証はありません。

34.1 ネットボランチ DNS サービスの使用の可否

[書式]
netvolante-dns use *interface switch*
netvolante-dns use pp *switch*
no netvolante-dns use *interface* [*switch*]
no netvolante-dns use pp [*switch*]

[設定値]
- *interface* ..... LAN インタフェース名
- *switch*
  - auto ..... 自動更新する
  - off ..... 自動更新しない

[説明]
ネットボランチ DNS サービスを使用するか否かを設定する。
IP アドレスが更新された時にネットボランチ DNS サーバーに自動で IP アドレスを更新する。

[初期値]
auto

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

34.2 ネットボランチ DNS サーバーへの手動更新

[書式]
netvolante-dns go *interface*
netvolante-dns go pp *peer_num*

[設定値]
- *interface* ..... LAN インタフェース名
- *peer_num* ..... 相手先情報番号

[説明]
ネットボランチ DNS サーバーに手動で IP アドレスを更新する。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

34.3 ネットボランチ DNS サーバーからの削除

[書式]
netvolante-dns delete go *interface* [*host*]
netvolante-dns delete go pp *peer_num* [*host*]

[設定値]
- *interface* ..... LAN インタフェース名
- *peer_num* ..... 相手先情報番号
- *host* ..... ホスト名

[説明]
登録した IP アドレスをネットボランチ DNS サーバーから削除する。
インタフェースの後にホスト名を指定することで、指定したホスト名のみを削除可能。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

34.4　ネットボランチ DNS サービスで使用するポート番号の設定

[書式]　**netvolante-dns port** *port*
no netvolante-dns port [*port*]

[設定値]　◦ *port*.....ポート番号 (1..65535)

[説明]　ネットボランチ DNS サービスで使用するポート番号を設定する。

[初期値]　2002

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

34.5　ネットボランチ DNS サーバーに登録済みのホスト名一覧を取得

[書式]　**netvolante-dns get hostname list** *interface*
netvolante-dns get hostname list pp *peer_num*
netvolante-dns get hostname list *all*

[設定値]　◦ *interface*.....LAN インタフェース名
◦ *peer_num*.....相手先情報番号
◦ all.....すべてのインタフェース

[説明]　ネットボランチ DNS サーバーに登録済みのホスト名一覧を取得し、表示する。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

34.6　ホスト名の登録

[書式]　**netvolante-dns hostname host** *interface host* [duplicate]
netvolante-dns hostname host pp *host* [duplicate]
no netvolante-dns hostname host *interface* [*host* [duplicate]]
no netvolante-dns hostname host pp [*host* [duplicate]]

[設定値]　◦ *interface*.....LAN インタフェース名
◦ *host*.....ホスト名 (63 文字以内)

[説明]　ネットボランチ DNS サービス (ホストアドレスサービス) で使用するホスト名を設定する。ネットボランチ DNS サーバーから取得されるホスト名は、『(ホスト名).(サブドメイン).netvolante.jp』という形になる。(ホスト名) はこのコマンドで設定した名前となり、(サブドメイン) はネットボランチ DNS サーバーから割り当てられる。(サブドメイン) をユーザが指定することはできない。

このコマンドを一番最初に設定する際は、(ホスト名) 部分のみを設定する。ネットボランチ DNS サーバーに対しての登録・更新が成功すると、コマンドが上記の完全な FQDN の形になって保存される。

duplicate を付加すると、1 台のルーターで異なるインタフェースに同じ名前を登録できる

[初期値]　なし

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

34.7　通信タイムアウトの設定

[書式]　**netvolante-dns timeout** *interface time*
netvolante-dns timeout pp *time*
no netvolante-dns timeout *interface* [*time*]
no netvolante-dns timeout pp [*time*]

[設定値]　◦ *interface*.....LAN インタフェース名
◦ *time*.....タイムアウト秒数 (1..180)

[説明]　ネットボランチ DNS サーバーとの間の通信がタイムアウトするまでの時間を秒単位で設定する。

[初期値]　90

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

34.8　ホスト名を自動生成するか否かの設定

[書式]　**netvolante-dns auto hostname** *interface switch*
netvolante-dns auto hostname pp *switch*
no netvolante-dns auto hostname *interface* [*switch*]
no netvolante-dns auto hostname pp [*switch*]

[設定値]
- *interface* ..... LAN インタフェース名
- *switch*
  - on ..... 自動生成する
  - off ..... 自動生成しない

[説明]　ホスト名の自動生成機能を利用するか否かを設定する。自動生成されるホスト名は、『'y' + (MAC アドレス下 6 桁).auto.netvolante.jp』という形になる。
このコマンドを 'on' に設定して、**netvolante-dns go** コマンドを実行すると、ネットボランチ DNS サーバーから上記のホスト名が割り当てられる。割り当てられたドメイン名は、**show status netvolante-dns** コマンドで確認することができる。

[初期値]　off

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

34.9　ネットボランチ DNS サーバーの設定

[書式]　**netvolante-dns server** *ip_address*
netvolante-dns server *name*
no netvolante-dns server [*ip_address*]
no netvolante-dns server [*name*]

[設定値]
- *ip_address* ..... IP アドレス
- *name* ..... ドメイン名

[説明]　ネットボランチ DNS サーバーの IP アドレスまたはホスト名を設定する。

[初期値]　netvolante-dns.netvolante.jp

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

34.10　自動更新に失敗した場合のリトライ間隔と回数の設定

[書式]　**netvolante-dns retry interval** *interface interval count*
netvolante-dns retry interval pp *interval count*
no netvolante-dns retry interval *interface* [*interval count*]
no netvolante-dns retry interval pp [*interval count*]

[設定値]
- *interface* ..... LAN インタフェース名
- *interval*
  - auto
  - 秒数 (60-300)
- *count* ..... 回数 (1-50)

[説明]　ネットボランチ DNS で自動更新に失敗した場合に、再度自動更新を行う間隔と回数を設定する。

[ノート]　*interval* に auto を設定した時には、自動更新に失敗した場合には 30 秒から 90 秒の時間をおいて再度自動更新を行う。それにも失敗した場合には、その後、60 秒後間隔で自動更新を試みる。
自動更新に失敗してから、指定した時間までの間に手動実行をした場合は、その後の自動更新は行われない。
Rev.7.01.41、Rev.8.01.18 以降で使用可能。

[初期値]　auto 10

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

35. UPnP の設定

35.1 UPnP を使用するか否かの設定

[書式]　**upnp use** *use*
no upnp use

[設定値]
- *use*
  - on ..... 使用する
  - off..... 使用しない

[説明]　UPnP 機能を使用するか否かを設定する。

[ノート]　Rev.8.01.07 以降で使用可能。

[初期値]　off

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

35.2 UPnP に使用する IP アドレスを取得するインタフェースの設定

[書式]　**upnp external address refer** *interface*
upnp external address refer pp *peer_num*
upnp external address refer default
no upnp external address refer [*interface*]
no upnp external address refer pp [*peer_num*]

[設定値]
- *interface*.....LAN インタフェース名
- default .....デフォルトルートのインタフェース
- *peer_num*
  - 相手先情報番号
  - *anonymous*

[説明]　UPnP に使用する IP アドレスを取得するインタフェースを設定する。

[ノート]　Rev.8.01.07 以降で使用可能。

[初期値]　default

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

35.3 UPnP のポートマッピング用消去タイマのタイプの設定

[書式]　**upnp port mapping timer type** *type*
no upnp port mapping timer type

[設定値]
- *type*
  - normal ..... ARP 情報を参照しない
  - arp..... ARP 情報を参照する

[説明]　UPnP のポートマッピングを消去するためのタイマのタイプを設定する。
このコマンドで変更を行うと arp の場合の消去タイマ値は 3600 秒、normal の場合は 172800 秒にセットされる。消去タイマの秒数は **upnp port mapping timer** コマンドで変更できる。

arp を指定すると upnp port mapping timer off の設定よりも優先する。
arp に影響されずにポートマッピングを残す場合は normal を指定する。

[ノート]　Rev.8.01.07 以降で使用可能。

[初期値]　arp

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

35.4　UPnP のポートマッピングの消去タイマの設定

[書式]　**upnp port mapping timer** *time*
no upnp port mapping timer

[設定値]　◦ *time*
- 秒数 (600..21474836)
- off..... 消去しない

[説明]　UPnP によって生成されたポートマッピングを消去するまでの時間を設定する。

[ノート]　**upnp port mapping timer type** コマンドで設定を行った後、このコマンドの設定を変更する。
off に設定した場合でも upnp port mapping timer type arp の設定にしてあるとポートマッピングは消去される。ARP がタイムアウトした状態でもポートマッピングを消去したくない場合は upnp port mapping timer type normal に設定するようにする。

Rev.8.01.07 以降で使用可能。

[初期値]　172800 (SRT100)
3600 (上記機種以外)

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

35.5　UPnP の syslog を出力するか否かの設定

[書式]　**upnp syslog** *syslog*
no upnp syslog

[設定値]　◦ *syslog*
- on..... UPnP の syslog を出力する
- off..... UPnP の syslog を出力しない

[説明]　UPnP の syslog を出力するか否かを設定する。デバッグレベルで出力される。

[ノート]　Rev.8.01.07 以降で使用可能。

[初期値]　off

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

36. USB の設定

36.1　USB ホスト機能を使うか否かの設定

[書式]　**usbhost use** *switch*
no usbhost use [*switch*]

[設定値]
◦ *switch*
- on.....USB ホスト機能を使用する
- off.....USB ホスト機能を使用しない

[説明]　USB ホスト機能を使用するか否かを設定する。
このコマンドが off に設定されているときは USB メモリをルーターに接続しても認識されない。
また、過電流により USB ホスト機能に障害が発生した場合、USB メモリが接続されていない状態で本コマンドを再設定すると復旧させることができる。

[初期値]　on

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

36.2　USB メモリに保存する SYSLOG ファイル名の指定

[書式]　**usbhost syslog filename** *name* [*crypto password*]
no usbhost syslog filename [*name*]

[設定値]
◦ *name*.....SYSLOG ファイル名
- usb1:*filename*.....USB メモリ内のファイル (*filename* は 64 文字以内。ただし、.bak 拡張子を含む名前は指定できない)

◦ *crypto*.....SYSLOG を暗号化して保存する場合の暗号アルゴリズムの選択
- *aes128*.....AES128 で暗号化する。
- *aes256*.....AES256 で暗号化する。

◦ *password*.....ASCII 文字列で表したパスワード (半角 8 文字以上、32 文字以内)

[説明]　USB メモリ内に保存する SYSLOG ファイル名を指定する。
このコマンドを設定することで USB メモリへの SYSLOG の記録を開始する。
このコマンドを消去することで USB メモリへの SYSLOG の記録が停止する。
ファイルに書き込むことのできるサイズの上限は、USB メモリへの書き込み開始時の空き容量から自動計算される。また、USB メモリ内には本コマンドで設定したファイルの他、必要に応じてバックアップファイルが作成される。これは SYSLOG ファイルが上限サイズに達した場合の退避先ファイルであり、ファイル名は以下の規則に従って決定される。
filename に拡張子が含まれている場合 ..... 拡張子を .bak に置き換える
filename に拡張子が含まれていない場合 .....*filename*.bak とする
バックアップファイルとの名前の重複を避けるため、*filename* に .bak 拡張子を含むファイル名は指定できない。
このコマンドが設定されていないときは SYSLOG を USB メモリに書き込まない。
crypto および *password* を指定した場合、SYSLOG を暗号化してから USB メモリに書き込む。暗号化する場合、*filename* に .rtfg 拡張子を含めるか、拡張子を省略した名前を指定する必要がある。拡張子を省略した場合、自動的にファイル名に .rtfg 拡張子を追加する。

[ノート]　以下の変更を行う場合、*filename* を変更しなければならない。
- SYSLOG を暗号化しないで保存するから、暗号化して保存するに変更する場合
- SYSLOG を暗号化して保存するから、暗号化しないで保存するに変更する場合
- 暗号アルゴリズムまたは、パスワードを変更する場合

[初期値]　設定されていない

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

36.3　統計情報を書き出すファイル名のプレフィックスの設定

[書式]　**usbhost statistics filename prefix** *prefix* [*term*] [*crypto password*]
no usbhost statistics filename prefix [*prefix* [*term*] [*crypto password*]]

[設定値]
- *prefix*..... ファイル名のプレフィックス (英数字のみ、15 文字以内)
  - usb1:*filename*..... ファイル名のプレフィックス
- *term*..... 1 つのファイルに含めるデータの期間
  - monthly ..... 月ごと
  - daily ..... 日ごと
- *crypto* ..... 暗号アルゴリズムの選択
  - aes128 ..... AES128 で暗号化する。
  - aes256 ..... AES256 で暗号化する。
- *password* ..... ASCII 文字列で表したパスワード (半角 8 文字以上、32 文字以内)

[説明]　統計情報を書き出すファイル名のプレフィックス (接頭語) を設定する。
実際のファイル名は、このプレフィックスをもとにして自動的に決まる。
例えば、プレフィックスを「yamaha」と設定した場合、LAN2 インタフェースのトラフィック量を書き出すファイル名は、yamaha_traffic_lan2_20071231.csv のようになる。
暗号化をしないときには、*crypto*、*password* パラメータを指定してはならない。

[ノート]　*term* として daily を設定したときには 1 日ごとに新しいファイルが生成されるが、統計情報のファイル数は 100 個に制限されているため、統計情報の種類を絞るか、頻繁にファイルを削除しないと、すぐにファイルが最大数に達してしまうので注意が必要である。
実際のファイル名は、*prefix* の後に種別や日付を表す文字列が加わる。
ファイル名の書式は以下に従う。
prefix_type[*_id*]*_yyyymm*[*dd*]*.ext*

- *prefix*..... 本コマンドにより設定される任意の文字列
- *type*..... 統計情報の種類
  - cpu..... CPU 使用率
  - memory ..... メモリ使用率
  - flow..... ファストパスのフロー数
  - route..... 経路数
  - nat..... NAT テーブルのエントリー数
  - filter..... ポリシーフィルターのセッション数
  - traffic..... インタフェース別のトラフィック量
  - qos ..... QoS のクラス別のトラフィック量
- *id*..... ID の意味は統計情報の種類によって異なる
  - インタフェース別のトラフィック量 ... インタフェースを表す
  - QoS のクラス別のトラフィック量 ... インタフェースとクラスを表す
  - これ以外の統計情報では ID は省略される
- *yyyy*..... 西暦 (4 桁)
- *mm*..... 月 (2 桁)
- *dd*..... 日 (2 桁)
  - ファイルを月ごとに分割するときには、DD は省略される
- *ext*..... 拡張子
  - csv..... CSV
  - rtfg ..... 暗号化されたファイル

[初期値]　*term*....monthly

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

36.4　USB ボタンと DOWNLOAD ボタン同時押下による設定ファイル、ファームウェアファイルのコピー操作を許可するか否かの設定

[書式]　**operation usb-download permit** *switch*
no operation usb-download permit [*switch*]

[設定値]
- *switch*
  - on..... 許可する
  - off..... 許可しない

[説明]　USB ボタンと DOWNLOAD ボタンの同時押下により、設定ファイル、およびファームウェアファイルを内蔵フラッシュ ROM へコピーするか否かを設定する。

[初期値]　on

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

36.5　USB ボタンと DOWNLOAD ボタン同時押下によりコピーする設定ファイル名の指定

[書式]　**usbhost config filename** *from to* [*password*]
no usbhost config filename [*from to*]

[設定値]
◦ *from*
• usb1:*filename*.....USB メモリ内の設定ファイル名 (*filename* は 64 文字以内)
◦ *to*
• 内蔵フラッシュ ROM の設定ファイル番号 (0..4)
◦ *password*.....ASCII 文字列で表したパスワード (半角 8 文字以上、32 文字以内)

[説明]　USB ボタンと DOWNLOAD ボタンの同時押下により内蔵フラッシュ ROM へコピーする設定ファイル名を指定する。
暗号化された USB メモリ内の設定ファイルを復号してから内蔵フラッシュ ROM へコピーする場合に *password* オプションを指定する。復号するときの暗号アルゴリズムは自動的に判別する。

[ノート]　暗号化された設定ファイルを復号しないで内蔵フラッシュ ROM にコピーすることはできない。
暗号化された設定ファイルを復号するとき、暗号データのチェックを行い、データが破壊されていないかを検知する。

[初期値]　usb1:config.txt 0

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

36.6　USB ボタンと DOWNLOAD ボタン同時押下によりコピーするファームウェアファイル名の指定

[書式]　**usbhost exec filename** *from to*
no usbhost exec filename [*from to*]

[設定値]
◦ *from*
• usb1:*filename*.....USB メモリ内の実行形式ファームウェアファイル名 (*filename* は 64 文字以内)
◦ *to*
• 内蔵フラッシュ ROM の実行形式ファームウェアファイル番号 (SRT100 は、0 のみ) (RTX1200 は、0, 1)

[説明]　USB ボタンと DOWNLOAD ボタンの同時押下により内蔵フラッシュ ROM へコピーする実行形式ファームウェアファイル名を指定する。

[初期値]　usb1:srt100.bin 0 (SRT100)
usb1:rtx1200.bin 0 (RTX1200)

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

36.7　USB ポートに接続した機器の初期化に使う AT コマンドの設定

[書式]　**usbhost modem initialize** *interface command* [*command_list*]
no usbhost modem initialize *interface*

[設定値]
◦ *interface*.....インタフェース名
• usb1
◦ *command*.....AT コマンド文字列 (最大 64 文字)
◦ *command_list*.....AT コマンド文字列を空白で区切った並び

[説明]　USB ポートに接続した機器を初期化するための AT コマンドを設定する。
USB ポートに機器が接続されている状態で起動したときには起動時に、機器が接続されていない状態で起動したときには機器を接続したときに、本コマンドで指定した AT コマンドが機器に設定される。
コマンドは AT(アテンションコード) を付加した AT コマンド文字列で指定する。
なお、1 つの AT コマンド文字列に複数のコマンドを指定することも可能である。

[ノート]　FOMA を使ったリモートセットアップを行う場合は、この初期化設定は不要です。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

36.8　USB ポートに接続した機器のフロー制御を行うか否かの設定

[書式]　**usbhost modem flow control** *interface sw*
no usbhost modem flow control *interface*

[設定値]
- *interface* ..... インタフェース名
  - usb1
- *sw*
  - on ..... フロー制御を行う
  - off ..... フロー制御を行わない

[説明]　USB ポートに接続した機器のフロー制御を行うかどうかを設定する。
接続した機器を用いたリモートセットアップ通信時に通信が意図せず切断されてしまう場合に off に設定すると効果がある場合がある。

[初期値]　on

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

37. スケジュール

37.1　スケジュールの設定

[書式]

schedule at *id* [*date*] *time* * *command...*
schedule at *id* [*date*] *time* pp *peer_num command...*
schedule at *id* [*date*] *time* tunnel *tunnel_num command...*
no scudule at *id* [[*date*]...]

[設定値]

◦ *id* .....スケジュール番号

◦ *date*.....日付 (省略可)

- 月 / 日
- 省略時は */* とみなす

月の設定例	設定内容
1,2	1 月と 2 月
2-	2 月から 12 月まで
2-7	2 月から 7 月まで
-7	1 月から 7 月まで
*	毎月

日の設定例	設定内容
1	1 日のみ
1,2	1 日と 2 日
2-	2 日から月末まで
2-7	2 日から 7 日まで
-7	1 日から 7 日まで
mon	月曜日のみ
sat,sun	土曜日と日曜日
mon-fri	月曜日から金曜日
-fri	日曜日から金曜日
*	毎日

◦ *time*.....時刻

- 時 (0..23 または *): 分 (0..59 または *)
- startup.....起動時
- usb-attached .....USB デバイス認識時

◦ *peer_num*

- 相手先情報番号
- anonymous

◦ *tunnel_num*..... トンネルインタフェースの番号

◦ *command*.....実行するコマンド (制限あり)

[説明]

time で指定した時刻に *command* で指定されたコマンドを実行する。
第 2、第 3 書式で指定された場合には、それぞれあらかじめ指定された相手先情報番号 / トンネル番号での、**pp select** / **tunnel select** コマンドが発行済みであるように動作する。
schedule at コマンドは複数指定でき、同じ時刻に指定されたものは *id* の小さな順に実行される。

以下のコマンドは指定できない。
administrator、**administrator password**、**cold start**、**console info** と **console prompt** を除く **console** で始まるコマンド、**date**、**exit**、**help**、**http revision-up go**、**interface reset**、**less** で始まるコマンド、**login password**、**login timer**、**ping**、**ping6**、**pp select**、**provider** *interface* **dns server**、**provider** *interface* **name**、**quit**、**remote setup**、**save**、**schedule at**、**show** で始まるコマンド、**telnet**、**time**、**timezone**、**traceroute**、**traceroute6**、**tunnel select**

[ノート]

入力時、*command* パラメータに対して TAB キーによるコマンド補完は行うが、シンタックスエラーなどは実行時まで検出されない。**schedule at** コマンドにより指定されたコマンドを実行する場合には、何を実行しようとしたかを INFO タイプの SYSLOG に出力する。
date に数字と曜日を混在させて指定はできない。
startup を指定したスケジュールはルーター起動時に実行される。電源を入れたらすぐ発信したい場合などに便利。
RT250i では第 3 書式は使用できない。
usb-attached を指定できるのは Rev.10.01 系以降である。

[設定例]

◦ ウィークデイの 8:00 ～ 17:00 だけ接続を許可する

```
# schedule at 1 */mon-fri 8:00 pp 1 isdn auto connect on
# schedule at 2 */mon-fri 17:00 pp 1 isdn auto connect off
# schedule at 3 */mon-fri 17:05 * disconnect 1
```

◦ 毎時 0 分から 15 分間だけ接続を許可する

```
# schedule at 1 *:00 pp 1 isdn auto connect on
# schedule at 2 *:15 pp 1 isdn auto connect off
# schedule at 3 *:15 * disconnect 1
```

◦ 今度の元旦にルーティングを切替える

```
# schedule at 1 1/1 0:0 * ip route NETWORK gateway pp 2
```

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

38. VLANの設定

38.1 VLAN ID の設定

[書式] **vlan** *interface/sub_interface* **802.1q** vid=*vid* name=*name*
no vlan *interface/sub_interface* **802.1q**

[設定値] ◦ *interface* ..... LAN インタフェース名
◦ *sub_interface* ..... 1 - 32 (RTX3000)
1 - 8 (上記以外の機種)
◦ *vid* ..... VLAN ID (IEEE802.1Q タグの VID フィールド格納値) (2 - 4094)
◦ *name* ..... VLAN に付ける任意の名前 (最大 127 文字)

[説明] LAN インタフェースで使用する VLANの VLAN ID を設定する。
設定された VID を格納した IEEE802.1Q タグ付きパケットを扱うことができる。
ひとつの LAN インタフェースあたり最大 8VLAN の設定ができる。

[ノート] タグ付きパケットを受信した場合、そのタグの VID が受信 LANインタフェースに設定されていなければパケットを破棄する。同一 LAN インタフェースで LAN分割機能 (**lan type** コマンドの port-based-ks8995m=on) との併用はできない。両者のうち先に入力されたものが有効となり、後から入力されるものはコマンドエラーになる。
Rev.8.02.28 以降で使用可能。

[初期値] VID 設定なし

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

38.2 スイッチングハブのポートが所属する VLAN の設定

[書式] **vlan port mapping** *sw_port vlan_interface*
no vlan port mapping *sw_port [vlan_interface...]*

[設定値] ◦ *sw_port* ..... スイッチングハブのポート (lan1.1 - lan1.N)
◦ *vlan_interface* ..... VLAN インタフェース (vlan1 - vlanN)

[説明] LAN 分割機能の拡張機能において、スイッチングハブの各ポートが所属する VLAN インタフェースを指定する。
ポートの名称には lan1.N を使用する。
同一の VLAN インタフェースに所属するポート間はスイッチとして動作する。

[ノート] **lan type** コマンドで "port-based-option=divide-network" を設定し、LAN 分割機能を有効にしなければ本コマンドは機能しない。
"port-based-option=divide-network" の設定が無い場合でも vlan port mapping は設定できるが、スイッチングハブの動作は変化しない。

[初期値] lan1.N が所属する VLAN インタフェースは vlanN となる。

[設定例]
```
# vlan port mapping lan1.3 vlan7
# vlan port mapping lan1.4 vlan7
```

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

39. 生存通知機能

39.1　生存通知の共有鍵の設定

[書式]　**heartbeat pre-shared-key** *key*
no heartbeat pre-shared-key

[設定値]　◦ *key*.....ASCII 文字列で表した鍵 (32 文字以内)

[説明]　生存通知を受信する側で認証を行うための共有鍵を設定する。生存通知の送信側、受信側の両方で同じ鍵が設定されている必要がある。
このコマンドが設定されていない場合、生存通知の送信および受信時のログ出力は行われない。

[ノート]　RTX3000 は、Rev.9.00.31 以降で使用可能。
RTX1500、RTX1100、RT107e は、Rev.8.03.60 以降で使用可能。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

39.2　生存通知を受信するか否かの設定

[書式]　**heartbeat receive** *switch* [*option=value ...*]
no heartbeat receive [*switch*]

[設定値]　◦ *switch*
- on.....生存通知パケットを受信する
- off.....生存通知パケットを受信しない

◦ *option=value*

option	*value*	説明
log	on	受信した内容を syslog に出力する。
	off	受信した内容を syslog に出力しない。
monitor	監視時間 [秒](30..21474836)	指定した秒数の間に通知がない場合にアラートを上げる。
	off	生存通知の受信がない場合でもアラートを上げない。

[説明]　受信した生存通知の内容を syslog に出力するか否かを設定する。
monitor オプションで指定した監視時間内に生存通知が届かないとき、syslog を出力し SNMP トラップを送出する。

[ノート]　本コマンドを設定する前に、**heartbeat pre-shared-key** コマンドで、送信側ルーターとの共有鍵を設定する必要がある。
RTX3000 は、Rev.9.00.31 以降で使用可能。
RTX1500、RTX1100、RT107e は、Rev.8.03.60 以降で使用可能。

[初期値]　*switch* .. off
log=off
monitor=off

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

39.3　生存通知の実行

[書式]　**heartbeat send** *dest_addr* [log=*switch*]

[設定値]　◦ *dest_addr*.....送信先ルーターの IPv4 アドレスまたは FQDN

◦ *switch*.....syslog の出力
- on.....syslog を出力する
- off.....syslog を出力しない

[説明]　*dest_addr* で指定した IP アドレスに、snmp sysname で設定した機器の名称と IP アドレスを送り、通信できる状態であることを通知する。
log=on の場合、パケットを送信するときに syslog を出力する。

[ノート]　本コマンドを実行する前に、**heartbeat pre-shared-key** コマンドで、受信側ルーターとの共有鍵を設定する必要がある。
RTX3000 は、Rev.9.00.31 以降で使用可能。
RTX1500、RTX1100、RT107e は、Rev.8.03.60 以降で使用可能。

[初期値]　log=off

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

40. SNTP サーバー機能

SNTP は、ネットワークを利用してコンピュータやネットワーク機器の時刻を同期させるためのプロトコルです。SNTP サーバー機能ではクライアントからの時刻の問い合わせに対してルーターの内蔵クロックの値を返します。SNTP サーバー機能は SNTP バージョン 4 を実装しています。また、下位互換として SNTP バージョン 1 ～ 3 のリクエストにも対応しています。

SNTP サーバー機能を利用して正確な時刻を得るために、定期的に **ntpdate** コマンドを実行して、他の NTP サーバーにルーターの時刻を合わせておくことを推奨します。

40.1 SNTP サーバー機能を有効にするか否かの設定

[書式]

sntpd service *switch*
no sntpd service

[設定値]

◦ *switch*
- on..... SNTP サーバー機能を有効にする
- off..... SNTP サーバー機能を無効にする

[説明]

SNTP サーバー機能を有効にするか否かを設定します。

[ノート]

Rev.8.03.68、Rev.9.00.31、Rev.10.00.27 以降で使用可能。

[初期値]

on

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

40.2 SNTP サーバーへのアクセスを許可するホストの設定

[書式]

sntpd host *host*
no sntpd host

[設定値]

◦ *host*
- any..... すべてのホストからのアクセスを許可する
- lan..... すべての LAN 側ネットワーク内ならば許可する
- lan1..... LAN1 側ネットワーク内ならば許可する
- lan2..... LAN2 側ネットワーク内ならば許可する
- lan3..... LAN3 側ネットワーク内ならば許可する (LAN3 インタフェースを持つ機種)
- none..... すべてのホストからのアクセスを禁止する
- SNTP サーバーへのアクセスを許可するホストの IPv4 アドレス
- SNTP サーバーへのアクセスを許可するホストの IPv4 アドレス範囲 (IP_ADDRESS - IP_ADDRESS)

[説明]

SNTP サーバーへのアクセスを許可するホストを設定します。

[ノート]

このコマンドで LAN インタフェースを指定した場合には、ネットワークアドレスとディレクテッドブロードキャストアドレスを除く IPv4 アドレスからのアクセスを許可する。
指定した LAN インタフェースにプライマリアドレスもセカンダリアドレスも設定していなければアクセスを許可しない。
Rev.8.03.68、Rev.9.00.31、Rev.10.00.27 以降で使用可能。
LAN3 インタフェースを持たないモデルでは lan3 を指定することはできない。

[初期値]

lan

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

41. 外部メモリ機能

本機能は、ルーター本体へ外部メモリ (USB メモリ、microSD メモリカード) を接続することにより、ルーターと外部メモリ間で各種データの操作を行います。
使用できる外部メモリは機種によって異なります。

本機能により、以下の動作が可能となります。

○コマンド設定、あるいは実行コマンドによる動作
・外部メモリへ SYSLOG メッセージを出力する。
・外部メモリへ設定ファイルをコピーする。
・外部メモリから設定ファイルをコピーする。
・外部メモリからファームウェアファイルをコピーする。
○ルーター本体の外部メモリボタンおよび DOWNLOAD ボタンの操作による動作
・外部メモリボタンと DOWNLOAD ボタンを同時に 3 秒以上押下し続け、外部メモリから設定ファイルおよびファームウェアファイルをコピーする。

さらに Rev.10.01 以降では、以下の動作が可能となります。
○外部メモリからの起動
○バッチファイル実行機能

バッチファイル実行機能

外部メモリの中に、コマンドを羅列したファイル (バッチファイルと呼びます) を入れておき、そのファイルに記述されたコマンドを実行する機能です。
設定によって DOWNLOAD ボタンを押して実行させることができます。コンソールでの **execute batch** コマンドによって実行することもできます。
コマンドの実行結果やログは、ファイルとして外部メモリに書き出します。

本機能を用いると、PC がない環境でも PING での疎通確認などを行うことができます。
例えばルーターの設置作業時に、必要な装置や作業手順を大幅に減らすことができます。
実行結果や設定内容、ルーターの状態などは、外部メモリにファイルとして書き出されます。
書き出されたファイルは、外部メモリを取り出して携帯電話で確認することができます。
作業ログとして利用することもできます。

本機能に関する技術情報は以下に示す URL で公開されています。
http://www.rtpro.yamaha.co.jp/

41.1　microSD カードスロットを使うか否かの設定

[書式]　***sd use*** *switch*
no sd use *[switch]*

[設定値]　◦ *switch*
- on ..... microSD カードスロットを使用する
- off..... microSD カードスロットを使用しない

[説明]　microSD カードスロットを使用するか否かを設定する。このコマンドが off に設定されているときは microSD メモリカードをカードスロットに差し込んでも認識されない。

[初期値]　on

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

41.2　外部メモリに保存する統計情報のファイル名のプレフィックスの設定

[書式]

external-memory statistics filename prefix *prefix* [*term*] [*crypto password*]
no external-memory statistics filename prefix [*prefix* [*term*] [*crypto password*]]

[設定値]

◦ *prefix*..... ファイル名のプレフィックス (英数字のみ、15 文字以内)
- usb1:*filename*..... ファイル名のプレフィックス
- sd1:*filename*..... ファイル名のプレフィックス

◦ *term*..... 1 つのファイルに含めるデータの期間
- monthly ..... 月ごと
- daily ..... 日ごと

◦ *crypto* ..... 暗号化して保存するときの暗号アルゴリズム
- aes128 ..... AES128 で暗号化する
- aes256 ..... AES256 で暗号化する

◦ *password*..... 暗号化して保存するときの暗号鍵 ASCII 文字列で表したパスワード (半角 8 文字以上、32 文字以内)

[説明]

統計情報を書き出すファイル名のプレフィックス (接頭語) を設定する。
実際のファイル名は、このプレフィックスをもとにして自動的に決まる。
例えば、プレフィックスを「yamaha」と設定した場合、LAN2 インタフェースのトラフィック量を書き出すファイル名は、yamaha_traffic_lan2_20080708.csv のようになる。
暗号化をしないときには、*crypto*、*password* パラメータを指定してはならない。

[ノート]

TERM として daily を設定したときには 1 日ごとに新しいファイルが生成されるが、統計情報のファイル数は 100 個に制限されているため、統計情報の種類を絞るか、頻繁にファイルを削除しないと、すぐにファイルが最大数に達してしまうので注意が必要である。
実際のファイル名は、prefix の後に種別や日付を表す文字列が加わる。
ファイル名の書式は以下に従う。

prefix_type[_id]_yyyymm[dd].ext

◦ *prefix*..... 本コマンドにより設定される任意の文字列

◦ *type*..... 統計情報の種類
- cpu..... CPU 使用率
- memory..... メモリ使用率
- flow..... ファストパスのフロー数
- route..... 経路数
- nat..... NAT テーブルのエントリー数
- filter..... ポリシーフィルターのセッション数
- traffic..... インタフェース別のトラフィック量
- qos ..... QoS のクラス別のトラフィック量

◦ *id*..... *id* の意味は統計情報の種類によって異なる
- インタフェース別のトラフィック量..... インタフェースを表す
- QoS のクラス別のトラフィック量..... インタフェースとクラスを表す
- これ以外の統計情報では *id* は省略される

◦ *yyyy*..... 西暦 (4 桁)

◦ *mm*..... 月 (2 桁)

◦ *dd*..... 日 (2 桁)
- ファイルを月ごとに分割するときには、*dd* は省略される

◦ *ext*..... 拡張子
- csv..... CSV
- rtfg ..... 暗号化されたファイル

[初期値]

term .... monthly

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

41.3　外部メモリに保存する SYSLOG ファイル名の指定

[書式]　**external-memory syslog filename** *name* [*crypto password*]
no external-memory syslog filename [*name*]

[設定値]
- *name*.....SYSLOG ファイル名
  - usb1:*filename*.....USB メモリ内のファイル (*filename* は 64 文字以内。ただし、.bak 拡張子を含む名前は指定できない)
  - sd1:*filename*.....microSD メモリカード内のファイル (*filename* は 64 文字以内。ただし、.bak 拡張子を含む名前は指定できない)
- *crypto*.....SYSLOG を暗号化して保存する場合の暗号アルゴリズムの選択
  - *aes128*.....AES128 で暗号化する
  - *aes256*.....AES256 で暗号化する
- *password*.....ASCII 文字列で表したパスワード (半角 8 文字以上、32 文字以内)

[説明]　外部メモリ内に保存する SYSLOG ファイル名を指定する。
ファイルに書き込むことのできるサイズの上限は、外部メモリへの書き込み開始時の空き容量から自動計算される。
また、外部メモリ内には本コマンドで設定したファイルの他、必要に応じてバックアップファイルが作成される。これは SYSLOG ファイルが上限サイズに達した場合の退避先ファイルであり、ファイル名は以下の規則に従って決定される。
filename に拡張子が含まれている場合 ..... 拡張子を .bak に置き換える
filename に拡張子が含まれていない場合 ..... FILENAME.bak とする
バックアップファイルとの名前の重複を避けるため、*filename* に .bak 拡張子を含むファイル名は指定できない。
このコマンドが設定されていないときは SYSLOG を外部メモリに書き込まない。
crypto および *password* を指定した場合、SYSLOG を暗号化してから外部メモリに書き込む。暗号化する場合、FILENAME に .rtfg 拡張子を含めるか、拡張子を省略した名前を指定する必要がある。拡張子を省略した場合、自動的にファイル名に rtfg 拡張子を追加する。

[ノート]　以下の変更を行う場合、FILENAME を変更しなければならない。
・SYSLOG を暗号化しないで保存するから、暗号化して保存するに変更する場合
・SYSLOG を暗号化して保存するから、暗号化しないで保存するに変更する場合
・暗号アルゴリズムまたは、パスワードを変更する場合

[初期値]　設定されていない

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

41.4　外部メモリボタンと DOWNLOAD ボタンの同時押下による設定ファイル、ファームウェアファイルのコピー操作を許可するか否かの設定

[書式]　**operation external-memory download permit** *switch*
no operation external-memory download permit [*switch*]

[設定値]
- *switch*
  - on.....許可する
  - off.....許可しない

[説明]　外部メモリボタンと DOWNLOAD ボタンの同時押下による、設定ファイルとファームウェアファイルのコピー操作を許可するか否かを設定する。

[初期値]　on

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

41.5　外部メモリ内のファイルからの起動を許可するか否かの設定

[書式]　**external-memory boot permit** *switch*
no external-memory boot permit [*switch*]

[設定値]　◦ *switch*
- on..... 許可する
- off..... 許可しない

[説明]　外部メモリ内のファイルからの起動を許可するか否かを設定する。この設定を OFF に設定すると外部メモリ内のファイルからの起動はできなくなる。

起動時に読み込む設定ファイルとファームウェアファイルの名前はそれぞれ、**external-memory config filename** コマンドと **external-memory exec filename** コマンドで設定できる。

[初期値]　on

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

41.6　起動時、あるいは外部メモリボタンと DOWNLOAD ボタン同時押下により読み込まれる、ファームウェアファイル名の指定

[書式]　**external-memory exec filename** *from* [*to*]
external-memory exec filename off
no external-memory exec filename [*from*] [*to*]
no external-memory exec filename [*off*]

[設定値]　◦ *from*..... 外部メモリとファームウェアファイル名
- usb1:*filename*..... USB メモリ内のファームウェアファイル名 (*filename* は 64 文字以内)
- sd1:*filename*..... microSD カード内のファームウェアファイル (*filename* は 64 文字以内)
- *:*filename*..... USB メモリおよび microSD カード内のファームウェアファイル (*filename* は 64 文字以内)

◦ *to*..... コピー先ファイル名
- *num*..... 内蔵 FlashROM の実行形式ファームウェアファイル番号 (0,1) (省略時は 0)

[説明]　外部メモリを差して起動した時、あるいは外部メモリボタンと DOWNLOAD ボタンを同時に押下した時に読み込まれる、外部メモリ上のファームウェアファイル名を指定する。

外部メモリボタンと DOWNLOAD ボタンを同時に押下した時は、ファームウェアファイルは内蔵フラッシュ ROM にコピーされるが、その時のコピー先の内蔵フラッシュ ROM のファームウェアファイル番号も指定できる。

外部メモリに "*" を指定した場合、指定するファイルの検索はまず microSD メモリカードから行われ、指定したファイルがなければ USB メモリが検索される。ボタン操作の場合は該当するボタンの外部メモリだけがファイル検索の対象となる。

filename は絶対パスを使って指定するかファイル名のみを指定する。ファイル名のみを指定した場合は指定された外部メモリ内から検索される。

検索の結果複数のファイルが該当する場合、ディレクトリ階層上最もルートディレクトリに近く、アルファベット順に先のディレクトリにあるファイルが選ばれる。

off に指定した場合、ファームウェアファイルの検索と読み込みを行わない。

[ノート]　外部メモリのディレクトリ構成やファイル数によっては、ファイルの検索に時間がかかることがある。
検索時間を短くするためには、階層の深いディレクトリの作成は避けてルートに近い位置にファイルを格納したり、ファイルを絶対パスで直接指定することが望ましい。
自動検索のタイムアウトの時間は **external-memory auto-search time** コマンドで設定できる。

[初期値]　*:rtx1200.bin 0

[設定例]　microSD カード内から "rtx1200.bin" を検索し、ファームウェアファイルとして読み込む
```
# external-memory config filename sd1:rtx1200.bin
```

microSD カード内のディレクトリ "test" から "rtx1200.bin" を検索し、ファームウェアファイルとして読み込む
```
# external-memory config filename sd1:/test/rtx1200.bin
```

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

41.7　起動時、あるいは外部メモリボタンと DOWNLOAD ボタン同時押下により読み込まれる、設定ファイル名の指定

[書式]　**external-memory config filename** *from*[,*from*] [*to*] [*password*]
external-memory config filename off
no external-memory config filename [*from*] [*to*] [*password*]
no external-memory config filename [*off*]

[設定値]
- *from*.....外部メモリ内の設定ファイル名を指定する
  - usb1:*filename*.....USB メモリ内の設定ファイル (*filename* は 64 文字以内)
  - sd1:*filename*.....microSD カード内の設定ファイル (*filename* は 64 文字以内)
  - *:*filename*.....USB メモリおよび microSD カード内の設定ファイル (*filename* は 64 文字以内)
- *to*.....コピー先ファイル名
  - *num*.....内蔵 FlashROM の設定ファイル番号 (0..4) (省略時は 0)
- *password*.....復号化のパスワード (ASCII 文字列で半角 8 文字以上、32 文字以内)

[説明]　外部メモリを差して起動した時に、あるいは外部メモリボタンと DOWNLOAD ボタンを同時に押下した時に読み込まれる、外部メモリ上の設定ファイル名を指定する。

また外部メモリボタンと DOWNLOAD ボタンを同時に押下した時は、設定ファイルは内蔵フラッシュ ROM にコピーされるが、その時のコピー先の内蔵フラッシュ ROM の設定ファイル番号も指定できる。

外部メモリに "*" を指定した場合、指定するファイルの検索はまず microSD メモリカードから行われ、指定したファイルがなければ USB メモリが検索される。ボタン操作の場合は該当するボタンの外部メモリだけがファイル検索の対象となる。

filename は絶対パスを使って指定するかファイル名のみを指定する。ファイル名のみを指定した場合は指定された外部メモリ内から検索される。

検索の結果複数のファイルが該当する場合、ディレクトリ階層上最もルートディレクトリに近く、アルファベット順に先のディレクトリにあるファイルが選ばれる。

パスワードを指定して暗号化されている設定ファイルを復号化して読み込む場合は、PASSWORD に暗号化したときのパスワードを設定する。

off に指定した場合、設定ファイルの検索と読み込みを行わない。

[ノート]　外部メモリのディレクトリ構成やファイル数によっては、ファイルの検索に時間がかかることがある。
検索時間を短くするためには、階層の深いディレクトリの作成は避けてルートに近い位置にファイルを格納したり、ファイルを絶対パスで直接指定することが望ましい。
自動検索のタイムアウトの時間は **external-memory auto-search time** コマンドで設定できる。

[初期値]　*:config.rtfg,*:config.txt 0

[設定例]　microSD カード内から "config.txt" を検索し、設定ファイルとして読み込む
```
# external-memory config filename sd1:config.txt
```

microSD カード内のディレクトリ "test" から "config.txt" を検索し、設定ファイルとして読み込む
```
# external-memory config filename sd1:/test/config.txt
```

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

41.8　ファイル検索時のタイムアウトを設定する

[書式]　**external-memory auto-search time** *time*
no external-memory auto-search time [*time*]

[設定値]
- *time*
  - 秒数 (1..600)

[説明]　外部メモリに格納されているファイルを検索する時のタイムアウト時間を設定する。

[初期値]　300

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

41.9 バッチファイルを実行する

[書式] **execute batch**

[設定値] なし

[説明] 外部メモリのバッチファイルを実行する。実行されるバッチファイル名は **external-memory batch filename** コマンドで指定する。

[ノート] 実行中のバッチファイルを中断したい場合は Ctrl+C を入力する。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

41.10 バッチファイルと実行結果ファイルの設定

[書式] **external-memory batch filename** *batchfile* [*logfile*]
no external-memory batch filename [*batchfile* [*logfile*]]

[設定値]
◦ *batchfile* ..... バッチファイル名、64 文字以内
- usb1:*filename*..... USB メモリ内のバッチファイル名
- sd1:*filename*..... microSD カード内のバッチファイル名
- *:*filename*..... SB メモリおよび microSD カード内のバッチファイル名

◦ *logfile*
- *filename*..... 実行結果ファイル名、64 文字以内

[説明] 外部メモリ内のバッチファイル名と実行結果ファイル名を指定する。

外部メモリに "*" を指定した場合、指定するファイルの検索はまず microSD カードから行われ、指定したファイルがなければ USB メモリが検索される。

filename は絶対パスを使ってファイルを指定するかファイル名のみを指定する。バッチファイルの *filename* にファイル名のみを指定した場合は外部メモリ内から自動検索する。複数のファイルがある場合、ディレクトリ階層上最もルートディレクトリに近く、アルファベット順に先のディレクトリにあるファイルが選ばれる。

logfile を省略した場合、" バッチファイル名 -log.txt" という名前で実行結果ファイルが作成される。

[初期値] *batchfile*..... *:command.txt
logfile ..... command-log.txt

[設定例] microSD カードのファイルから "command_test.txt" をバッチファイルとして検索する。
```
# external-memory batch filename sd1:command_test.txt
```

microSD カードのディレクトリ "test" から "command_test.txt" を読み込む。
```
# external-memory batch filename sd1:/test/command_test.txt
```

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

41.11 DOWNLOAD ボタンを押した時に実行する機能の設定

[書式] **operation button function download** *function*
no operation button function download [*function*]

[設定値]
◦ *function*..... DOWNLOAD ボタンを押した時に実行する機能
- http revision-up... HTTP リビジョンアップ
- execute batch..... バッチファイルの実行

[説明] DOWNLOAD ボタンを押した時に実行する機能を設定する。機能実行中は DOWNLOAD ボタンの下のランプが点灯し、機能の実行が完了すると消灯する。

[初期値] http revision-up

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

41.12　DOWNLOAD ボタンによるバッチファイルの実行を許可するか否かの設定

[書式]　**operation execute batch permit** *permit*
no operation execute batch permit [*permit*]

[設定値]　◦ *permit*
- on ..... DOWNLOAD ボタンによるバッチファイルの実行を許可する
- off..... DOWNLOAD ボタンによるバッチファイルの実行を許可しない

[説明]　DOWNLOAD ボタンによりバッチファイルの実行機能を使用するか否かを設定する。

[初期値]　*off*

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

42. HTTP アップロード機能

ヤマハルーター内の情報 (設定ファイルあるいは SYSLOG) を指定した HTTP サーバーにアップロードすることができる機能です。複数拠点の設定ファイルやログの集中管理に使用することができます。

設定ファイルは ***show config*** コマンドまたは ***show config N*** コマンド、SYSLOG は ***show log*** コマンドの実行結果がファイルとして保存されます。
保存したファイルの先頭には、実行したコマンド名が表示されます。

HTTP サーバーに複数のヤマハルーターからの情報を集める場合など、 ファイルをディレクトリ指定して格納することができます。ディレクトリを指定する場合には **http upload** コマンドで設定します。

この機能を使用するためには、HTTP サーバー側での対応も必要です。
HTTP サーバーの OS の種類には依存しません (Windows、UNIX、etc.) が、UNIX 上の HTTP サーバーを使用する場合、CGI スクリプトは nobody ユーザー権限として実行されるため、生成されるファイルも nobody ユーザー権限となります。CGI 実行ディレクトリのパーミッションは、[------rw-] を満たしておく必要があります。
HTTP サーバー側で動作させる必要のあるスクリプトファイル、および本機能に関する技術情報は以下に示す URL で公開されています。

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

42.1 HTTP アップロードするファイルの設定

[書式]　**http upload** *type* [*config_no*] [*directory/*] *filename*
no http upload [*..*]

[設定値]
- *type* ..... 'config' or 'log'
- *config_no* 0-4.2
- *directory* ..... 出力先のディレクトリ名
- *filename* ..... 出力先のファイル名

[説明]　HTTP サーバーにアップロードする情報と、保存先のディレクトリ名及びファイル名を設定する。
指定したディレクトリ名でディレクトリを生成し、そのディレクトリ内に指定したファイル名のファイルを生成する (例：dir1/dir2/config.txt)。
TYPE に 'config' を指定したときのみ CONFIG_NO が有効になり、CONFIG_NO を省略した場合は起動中の config がアップロードの対象になる。
なお、CONFIG_NO は設定ファイル多重機能に対応した機種でのみ設定することができる。

[初期値]　なし

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

42.2 HTTP アップロード先 URL の設定

[書式]　**http upload url** *url*
no http upload url [*url*]

[設定値]
- *url* ..... アップロード先の URL

[説明]　HTTP アップロードで使用する HTTP サーバーの URL を設定する。
HTTP サーバーでは cgi を許可するよう設定にする必要があり、アップロードを受け入れるための cgi を実行させる必要がある。

[初期値]　なし

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

42.3　HTTP アップロードを許可するか否かの設定

[書式]　**http upload permit** *switch*
no http upload permit [*switch*]

[設定値]　◦ *switch*
- on ..... HTTP アップロードを許可する
- off..... HTTP アップロードを許可しない

[説明]　HTTP アップロードを許可するか否かを設定する。

[初期値]　*off*

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

42.4　HTTP アップロードのタイムアウト時間の設定

[書式]　**http upload timeout** *time*
no http upload timeout [*time*]

[設定値]　◦ *time* ..... 1-180[秒]

[説明]　HTTP アップロードでタイムアウトするまでの時間を設定する。

[初期値]　30

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

42.5　HTTP アップロードのリトライの間隔と回数の設定

[書式]　**http upload retry interval** *interval count*
no http upload retry interval [*..*]

[設定値]　◦ *interval*..... 1-60[秒]
◦ *count*..... 1-10

[説明]　HTTP アップロードに失敗したときのリトライ間隔と時間を設定する。

[初期値]　*interval*=30
count=5

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

42.6　HTTP アップロードで使用するプロキシサーバーの設定

[書式]　**http upload proxy** *proxy* [*port*]
no http upload proxy [*..*]

[設定値]　◦ *proxy* ..... プロキシサーバー
◦ *port* 1-65535

[説明]　HTTP アップロードで使用するプロキシサーバーを設定する。

[初期値]　80

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

42.7　HTTP アップロードの実行

[書式]　**http upload go**

[説明]　HTTP アップロードを実行する。
アップロードに失敗した場合、**http upload retry interval** コマンドの設定に基づいてリトライをする。

[ノート]　**alarm http upload** コマンドが 'on' の場合は、アップロードの成否に応じてアラーム音を鳴らす。
schedule at コマンドで指定することができ、startup を指定して起動時に実行させることもできる。
startup を指定した場合、起動直後は HTTP サーバーへの経路が確立しておらずアップロードに失敗することがある。
こうした場合には **http upload retry interval** コマンドの設定でリトライすることで対応できるようになる。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

42.8　HTTP アップロード機能に関連するアラーム音を鳴らすか否かの設定

[書式]　**alarm http upload** *switch*
no alarm http upload [*switch*]

[設定値]　◦ *switch*
- on..... 鳴らす
- off..... 鳴らさない

[説明]　HTTP アップロード機能に関連するアラーム音を鳴らすか否かを選択する。

[初期値]　on

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

43. モバイルインターネット接続機能

携帯端末をルーター本体に接続し、携帯端末から発信してインターネット接続する機能です。
固定回線がなくても本機能に対応した携帯端末があればインターネット接続をすることができます。
本機能は発信のみに対応し、着信での利用はできません。

現時点で対応する携帯端末は USB ケーブルで接続するものだけとなります。
この場合、携帯端末を USB モデムとして制御することになります。
本機能をご利用になるには以下の機材等が必要になります。

・対応ルーター
・対応携帯端末
・対応携帯端末のデータ通信に必要なプロバイダ契約 (mopera 等)
・USB ケーブル (対応携帯端末用のもの)

本機能ではパケット通信量およびパケット通信時間の制限が初期値として設定されています。これら上限値に達した場合、通信を強制的に切断し、その後発信できなくなります。発信を許可するためには **clear mobile access limitation** コマンドを発行するか、ルーター本体を再起動します。これらの上限値は **mobile access limit length** および **mobile access limit time** コマンドで変更することができます。

43.1　携帯端末を使用するか否かの設定

[書式]
mobile use *interface use*
no mobile use *interface* [*use*]

[設定値]
◦ *interface*
- usb1 .....USB1 をモバイルインターネット接続に使用

◦ *use*
- on .....携帯端末を使用する
- off.....携帯端末を使用しない

[説明]
指定のバスに接続された携帯端末をインターネット接続に使用するか否かを設定する。

[初期値]
off

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

43.2　携帯端末の種別設定

[書式]
mobile type *interface type*
no mobile type *interface* [*type*]

[設定値]
◦ *interface*
- usb1

◦ *type*
- auto .....装着されている対応携帯端末を使用する
- foma.....FOMA 端末に限定する

[説明]
インターネット接続に使用する携帯端末の種別を指定する。
特定の携帯端末を指定した場合、その端末以外が装着されたときは使用できない。

[初期値]
auto

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

43.3　携帯端末に直接コマンドを発行する

[書式]　**execute at-command** *interface command*

[設定値]
- *interface*
  - usb1
- *command*
  - AT コマンド

[説明]　指定したインタフェースに接続された携帯端末に対して、AT コマンドを直接発行する。

以下のコマンドも同様に AT コマンドを発行するので、本コマンドと併用するときは注意が必要である
usbhost modem initialize

[ノート]　特別な理由がない限り本コマンドを使用する必要はない。

[設定例]　execute at-command usb1 AT+CGDCONT=<1>,¥"PPP¥",¥"mopera.ne.jp¥"
ダブルクォート (") を指定するときは ¥" のように ¥ を付加する必要がある。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

43.4　指定した相手に対して発信制限を解除する

[書式]　**clear mobile access limitation** *interface*
clear mobile access limitation pp [*peer_num*]

[設定値]
- *interface*
  - usb1 ..... USB インタフェース
- *peer_num*
  - 相手先情報番号..... 省略時は現在選択している相手先

[説明]　**mobile access limit** コマンドによって発信制限がかかったインタフェースに対し、制限を解除して再び発信できるようにする。
なお、電源の再投入でも発信制限は解除される。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

43.5　PP で使用するインタフェースの設定

[書式]　**pp bind** *interface*
no pp bind [*interface*]

[設定値]
- *interface*
  - usb1 ..... usb1 を使用する

[説明]　選択されている相手について使用するインタフェースを設定する。

[初期値]　どのインタフェースともバインドされていない

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

43.6　携帯端末からの自動発信設定

[書式]　**mobile auto connect** *auto*
no mobile auto connect [*auto*]

[設定値]
- *auto*
  - on..... 携帯端末から自動発信する
  - off..... 携帯端末から自動発信しない

[説明]　選択されている相手について自動接続するか否かを設定する。

[初期値]　off

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

43.7　携帯端末を切断するタイマの設定

[書式]　**mobile disconnect time** *time*
no mobile disconnect time [*time*]

[設定値]　◦ *time*
- 1-21474836 .....秒数
- off.....タイマを設定しない

[説明]　選択されている相手について PP 側の送受信がない場合の切断までの時間を設定する。

[初期値]　60

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

43.8　携帯端末を入力がないときに切断するタイマの設定

[書式]　**mobile disconnect input time** *time*
no mobile disconnect input time [*time*]

[設定値]　◦ *time*
- 1-21474836 .....秒数
- off.....タイマを設定しない

[説明]　選択されている相手について PP 側からデータ受信がない場合の切断までの時間を設定する。

[初期値]　120

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

43.9　携帯端末を出力がないときに切断するタイマの設定

[書式]　**mobile disconnect output time** *time*
no mobile disconnect output time [*time*]

[設定値]　◦ *time*
- 1-21474836 .....秒数
- off.....タイマを設定しない

[説明]　選択されている相手について PP 側へのデータ送信がない場合の切断までの時間を設定する。

[初期値]　120

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

43.10　発信先アクセスポイントの設定

[書式]　**mobile access-point name** *apn* cid=*cid*
no mobile access-point name [*apn* cid=*cid*]

[設定値]　◦ *apn*
- FOMA パケット通信に対応したアクセスポイント名 (Access Point Name) を指定する。

◦ *cid*
- 1-10 .....CID 番号

FOMA 端末の CID と APN の組み合わせ初期値は以下となっている。
この組み合わせを用いることを推奨する。
1 = mopera.ne.jp (mopera)
2 = 未設定
3 = mopera.net (mopera U)
4-10 = 未設定

[説明]　選択されている相手についてアクセスポイント名 (APN) と CID 番号の割り当てを設定する。

[初期値]　なし

[設定例]　mobile access-point name mopera.ne.jp cid=1　(mopera の場合)
mobile access-point name mopera.net cid=3　(mopera U の場合)

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

43.11　パケット通信量制限の設定

[書式]　**mobile access limit length** *length*
no mobile access limit length [*length*]

[設定値]　◦ *length*
- 1-100000000 ..... 送受信する累積パケットデータ長の上限値
- off..... 制限しない

[説明]　選択されている相手について、送受信するパケットの累積データ長の上限値を設定する。
上限に達した場合は通信を強制的に切断し、その後の通信もブロックする。
携帯端末のパケット通信は 128 バイトごとに課金されるが、ルーターと携帯端末間で送受信されるデータが 128 バイト単位である保証はない。
例えばルーターが 512 バイト (128 バイト× 4) のデータを送受信したとしても、4 パケット分の通信料金である保証はなく、携帯網ではそれより多くのパケットに分割されて送受信されている可能性がある。
また、ルーターと携帯端末の間を流れるデータは非同期データであり、データの内容によっては本来のデータよりも長くなることがある。
従って、本コマンドで設定するデータ長はあくまで目安にしかならないので注意が必要である。
一度上限に達した場合は **clear mobile access limitation** コマンドを発行するか、システムを再起動しないと発信制限が解除されない。
なお、**show status pp** コマンドにて、現在までの累積パケットデータ長を確認可能である。

[初期値]　200000

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

43.12　パケット通信時間制限の設定

[書式]　**mobile access limit time** *time*
no mobile access limit time [*time*]

[設定値]　◦ *time*
- 1-21474836..... 累積通信秒数の上限値
- off..... タイマを設定しない

[説明]　選択されている相手について、送受信するパケットの累積通信時間の上限値を設定する。
上限に達した場合は通信を強制的に切断し、その後の通信もブロックする。
本コマンドは **mobile disconnect time** コマンドとは独立して動作する。
一度上限に達した場合は **clear mobile access limitation** コマンドを発行するか、システムを再起動しないと発信制限が解除されない。
show status pp コマンドにて、現在までの累積通信時間を確認可能である。

[初期値]　3600

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

43.13　同じ発信先に対して連続して認証に失敗できる回数の設定

[書式]　**mobile call prohibit auth-error count** *count*
no mobile call prohibit auth-error count [*count*]

[設定値]　◦ *count*
- 1-21474836..... 連続して認証に失敗できる回数
- off..... 発信制限をかけない

[説明]　選択された相手に対して連続して認証に失敗できる回数を指定する。ここで設定した回数だけ連続して認証に失敗した場合、その後は、その発信先に発信しない。

なお、以下のコマンドを実行すると、再び発信が可能となる。
pp auth accept/pp auth request/pp auth myname/pp auth username/
no pp auth myname/no pp auth username
また、電源の再投入でも発信制限は解除される。

[初期値]　5

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

43.14　LCP の Async Control Character Map オプション使用の設定

[書式]　**ppp lcp accm** *accm*
no ppp lcp accm [*accm*]

[設定値]　◦ *accm*
- on ..... 用いる
- off..... 用いない

[説明]　選択された相手に対して [PPP,LCP] の Async-Control-Character-Map オプションを用いるか否かを設定する。
これを設定することで通信量を減らせることがある。
本設定はモバイルインターネット接続機能でのみ有効である。

[ノート]　on を設定しても相手に拒否された場合は用いない。また、Async-Control-Character-Map の値は、自分から送出する場合も相手から受信する場合も 0x00000000 のみが用いられる。

[初期値]　off

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

43.15　発信者番号通知 (186) を付加するかどうかの設定

[書式]　**mobile display caller id** *display*
no mobile display caller id [*display*]

[設定値]　◦ *display*
- on ..... 発信者番号を通知する (186 を付加して発信する)
- off..... 発信者番号を通知しない (186 を付加せず発信する)

[説明]　選択された相手に対して、発信時に 186 を付けて発信者番号を通知するかどうかを設定する。

[初期値]　off

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

43.16　詳細な SYSLOG を出力するか否かの設定

[書式]　**mobile syslog** *switch*
no mobile syslog [*switch*]

[設定値]　◦ *switch*
- on ..... 詳細な SYSLOG を出力する
- off..... 詳細な SYSLOG を出力しない

[説明]　携帯端末に対して発行した AT コマンドを SYSLOG として詳細に出力するかどうかを指定する。
モバイルインターネット接続として発信動作に入ってからのものだけが記録され、発信動作前のものは記録されない。FOMA リモートセットアップ時も記録されない。
併せて syslog debug on の設定が必要となる。

[初期値]　off

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

43.17　携帯端末が接続状態になったときにアラーム音を鳴らすかどうかの設定

[書式]　**alarm mobile** *switch*
no alarm mobile [*switch*]

[設定値]　◦ *switch*
- on ..... 鳴らす
- off..... 鳴らさない

[説明]　携帯端末が接続状態になったときにアラーム音を鳴らすかどうかを設定する。

[ノート]　FOMA リモートセットアップのときは対象外である。

[初期値]　on

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

44. ブリッジインタフェース (ブリッジ機能)

ブリッジインタフェースは複数のインタフェースを 1 つの仮想インタフェースに収容し、収容したインタフェース間でブリッジングを行う機能です。
収容された各インタフェースが接続する物理的なセグメントは 1 つのセグメントとして扱います。

注意事項
・本機能におけるブリッジ処理はワイヤレートを保証するものではありません。
・QoS 機能には対応していません。
そのため、QoS 機能を利用した Dynamic Traffic Control 機能を利用することはできません。
・スパニングツリープロトコルには対応していません。
・BPDU フレームは透過します。
・IEEE802.1Q タグ付きパケットは透過します。
・RT300i のブリッジ機能とは異なる実装です。

44.1 ブリッジインタフェースに収容する実インタフェースを設定する

[書式]
bridge member *bridge_interface interface interface* [...]
no bridge member *bridge_interface* [*interface* ...]

[設定値]
◦ *bridge_interface*..... ブリッジインタフェース名
◦ *interface*..... LAN インタフェース名

[説明]
仮想インタフェースであるブリッジインタフェースに収容する実インタフェースを指定する。
収容したインタフェース間でブリッジ動作が行われる。

[ノート]
・収容する LAN インタフェースについて
収容した実インタフェースに IPv4,IPv6 アドレスを付与してはならない。
収容した実インタフェースの IPv6 リンクローカルアドレスは削除される。
収容する LAN インタフェースの MTU はすべて同一の値でなければならない。
いずれかのブリッジインタフェースに収容した実インタフェースは、他のブリッジインタフェースに収容することはできない。
収容するインタフェースがスイッチングハブを持つインタフェースである場合、スイッチングハブのポート間で完結する通信は本機能によるブリッジ動作ではなく、スイッチングハブ LSI 内部で処理される。

・ブリッジインタフェースについて
ブリッジインタフェースのリンク状態は収容した LAN インタフェースのリンク状態に応じて変化する。
いずれかの収容したインタフェースがアップ状態だった場合、ブリッジインタフェースはアップ状態になる。
すべてのインタフェースがダウン状態だった場合、ブリッジインタフェースもダウン状態になる。
ブリッジインタフェースの MAC アドレスは、収容した LAN インタフェースのうち、インタフェース番号がもっとも小さいインタフェースのアドレスを使用する。

[初期値]
設定されていない

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

44.2　自動的なラーニングを行うか否かの設定

[書式]　**bridge learning** *bridge_interface switch*
no bridge learning *bridge_interface* [*switch*]

[設定値]
- *bridge_interface*.....ブリッジインタフェース名
- *switch*
  - on ..... ラーニングする
  - off..... ラーニングしない

[説明]　ブリッジ機能で自動的な MAC アドレスのラーニングを行うか否かを設定する。
bridge_interface には対象となるブリッジインタフェース名を指定する。
ラーニングを行う場合、ブリッジインタフェースに収容したインタフェースでパケットを受信すると、そのパケットの始点 MAC アドレスと受信インタフェースを学習してラーニングテーブルに登録する。

学習した情報はブリッジ処理が行われるときに参照され、パケットが不要なインタフェースに出力されることを抑制する。

[ノート]　学習時にラーニングテーブルが上限に達していた場合、もっとも古いエントリーを削除した上で登録される。
ブリッジ処理においてラーニングテーブルを参照したとき、一致するエントリーが存在しなかった場合、受信インタフェースを除くすべての収容インタフェースにパケットが出力される。これはリピーターと同様の動作である。

[初期値]　on

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

44.3　ブリッジがラーニングした情報の消去タイマーの設定

[書式]　**bridge learning** *bridge_interface* **timer** *time*
no bridge learning *bridge_interface* **timer** [*time*]

[設定値]
- *bridge_interface*.....ブリッジインタフェース名
- *time*
  - 秒数 .....(30..32767)
  - off..... タイマを設定しない

[説明]　ブリッジが自動的にラーニングした情報の寿命を設定する。
bridge_interface には対象となるブリッジインタフェース名を指定する。
指定した時間内に、ある始点 MAC アドレスからパケットを受信しなかった場合はその MAC アドレスに関する学習した情報を消去する。

off を指定した場合には、学習した情報が自動的に消去されることはなくなる。

[初期値]　300

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

44.4　静的なラーニング情報の設定

[書式]　**bridge learning** *bridge_interface* **static** *mac_address interface*
no bridge learning *bridge_interface* **static** *mac_address* [*interface*]

[設定値]
- *bridge_interface*.....ブリッジインタフェース名
- *mac_address*.....MAC アドレス
- *interface*.....LAN インタフェース名

[説明]　ブリッジが参照する静的な登録情報を設定する。
bridge_interface には対象となるブリッジインタフェース名を指定する。
mac_address に指定した MAC アドレスが宛先であるパケットは、*interface* で指定したインタフェースに出力されるようになる。
interface には *bridge_interface* に収容された LAN インタフェースを指定する。

[ノート]　静的に登録した情報は自動的に学習した情報よりも優先して参照される。
interface で指定した LAN インタフェースが *bridge_interface* に収容されていない場合、登録した情報は無視される。

[初期値]　設定されていない

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

45. 操作

45.1 相手先情報番号の選択

[書式] **pp select** *peer_num*
no pp select

[設定値] ◦ *peer_num*
- 相手先情報番号
- none ..... 相手を選択しない
- anonymous ..... ISDN 番号が不明である相手の設定

[説明] 設定や表示の対象となる相手先情報番号を選択する。以降プロンプトには、**console prompt** コマンドで設定した文字列と相手先情報番号が続けて表示される。
none を指定すると、プロンプトに相手先情報番号を表示しない。

[ノート] この操作コマンドは一般ユーザでも実行できる。
no pp select コマンドは **pp select** none コマンドと同じ動作をする。
選択できる相手先情報番号のモデルによる違いは 1.6(29 ページ) を参照。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

45.2 トンネルインタフェース番号の選択

[書式] **tunnel select** *tunnel_num*
no tunnel select

[設定値] ◦ *tunnel_num*
- トンネルインタフェース番号
- none ..... トンネルインタフェースを選択しない

[説明] トンネルモードの設定や表示の対象となるトンネルインタフェース番号を選択する。

[ノート] 本コマンドの操作は、一般ユーザでも実行できる。
プロンプトが tunnel の場合は、pp 関係のコマンドは入力できない。
no tunnel select コマンドは **tunnel select** none コマンドと同じ動作をする。
選択できるトンネルインタフェース番号のモデルによる違いは 19.(180 ページ) を参照。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

45.3 設定に関する操作

45.3.1 管理ユーザへの移行

[書式] **administrator**

[設定値] なし

[説明] このコマンドを発行してからでないと、ルーターの設定は変更できない。また操作コマンドも実行できない。
パラメータはなく、コマンド入力後にプロンプトに応じて改めて管理パスワードを入力する。入力されるパスワードは画面には表示されない。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

45.3.2 終了

[書式] **quit**
quit save
exit
exit save

[設定値] ◦ save ..... 管理ユーザから抜ける際に指定すると、設定内容を不揮発性メモリに保存して終了

[説明] ルーターへのログインを終了、または管理ユーザーから抜ける。
設定を変更して保存せずに管理ユーザーから抜けようとすると、新しい設定内容を不揮発性メモリに保存するか否かを問い合わせる。不揮発性メモリに保存されれば、再起動を経ても同じ設定での起動が可能となる。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

45.3.3　設定内容の保存

[書式]　***save*** *[filename [comment]]*

[設定値]
- *filename*.....設定を保存するファイル名
  - 内蔵 Flash ROM の設定ファイル番号
  - ext0:*filename* .....PCMCIA Flash ATA カードの設定ファイル名 (RT300i)
  - usb1:*filename* .....USB メモリ内の設定ファイル名、*filename* は 64 文字以内
  - sd1:*filename*.....microSD カード内の設定ファイル名、*filename* は 64 文字以内
- *comment*.....設定ファイルのコメント (200 文字以内)

[説明]　現在の設定内容を不揮発性メモリに保存する。
ファイル指定を省略すると、起動時に使用した設定ファイルに保存する。
指定可能なファイル名は以下の通りである。

RTX2000, RT300i	0..9
RTX1000	0
上記以外のモデル	0..4

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

45.3.4　設定ファイルの複製

[書式]　**copy config** *from to*
copy config *from to crypto* [*password*]
copy config *from to* [*password*]

[設定値]
- *from*.....コピー元ファイル名
  - 内蔵フラッシュ ROM の設定ファイル番号 (0..4.2)
  - usb1:*filename* .....USB メモリ内の設定ファイル名、*filename* は 64 文字以内
  - sd1:*filename*.....microSD カード内の設定ファイル名、*filename* は 64 文字以内
  - *:*filename*.....USB メモリおよび microSD カード内の設定ファイル名 (*filename* は 64 文字以内)
- *to*.....コピー先ファイル名
  - 内蔵フラッシュ ROM の設定ファイル番号 (0..4)
  - usb1:*filename* .....USB メモリ内の設定ファイル名、*filename* は 64 文字以内
  - sd1:*filename*.....microSD カード内の設定ファイル名、*filename* は 64 文字以内
- *crypto*.....暗号アルゴリズムの選択
  - *aes128*.....AES128 で暗号化する。
  - *aes256*.....AES256 で暗号化する。
- *password*.....ASCII 文字列で表したパスワード (半角 8 文字以上、32 文字以内)

[説明]　保存されている設定ファイルを複製する。
コピー元、コピー先の両方に外部メモリのファイルを指定することはできない。
cold start 直後は設定ファイルが存在しないので内蔵フラッシュ ROM から外部メモリへ設定ファイルのコピーはできない。この場合、一度 **save** コマンドで設定を保存してから実行する必要がある。
内蔵フラッシュ ROM へコピーした内容を、実際の動作に反映させるためには、本コマンドの実行後にルーターを再起動する必要がある。

外部メモリに "*" を指定した場合、指定するファイルの検索はまず microSD メモリカードから行われ、指定したファイルがなければ USB メモリが検索される。*filename* は絶対パスを使ってファイルを指定するかファイル名のみを指定する。*filename* にファイル名のみを指定した場合は外部メモリ内から自動検索する。
複数のファイルがある場合、ディレクトリ階層上最もルートディレクトリに近く、アルファベット順に先のディレクトリにあるファイルが選ばれる。
コピー先に外部メモリを指定する場合、*filename* に絶対パスを使ってファイルを指定する。

外部メモリを対象として暗号化機能を利用することができる。
外部メモリへファイルを暗号化してコピーする場合、ファイル名には .rtfg 拡張子を含めるか、拡張子を省略した名前を指定する必要がある。拡張子を省略した場合、自動的にファイル名に .rtfg 拡張子を追加する。
Rev.10.01 系以降では、パスワードを省略した暗号化を行うことができる。

[ノート]　外部メモリ上の暗号化された設定ファイルを復号しないで内蔵フラッシュ ROM にコピーすることはできない。
第 2 書式は、内蔵フラッシュ ROM の設定ファイルを外部メモリへ暗号化してコピーする場合にのみ利用できる。
第 3 書式は、外部メモリ内の暗号化された設定ファイルを復号化して内蔵フラッシュ ROM 内にコピーする場合にのみ利用できる。
外部メモリ内のファイルを指定できるのは、外部メモリインタフェースを持つ機種に限られる。
内蔵フラッシュ ROM の設定ファイル番号をコピー先ファイルとした場合、元のコピー先ファイルはこのコマンドの実行後は退避ファイルとなる。

ファイルの自動検索ができるのは Rev.10.01 系以降である。
外部メモリのディレクトリ構成やファイル数によっては、ファイルの検索に時間がかかることがある。
検索時間を短くするためには、階層の深いディレクトリの作成は避けてルートに近い位置にファイルを格納したり、ファイルを絶対パスで直接指定することが望ましい。
自動検索のタイムアウトの時間は **external-memory auto-search time** コマンドで設定できる。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	RT250i	RT107e	SRT100

45.3.5　ファームウェアファイルを内蔵フラッシュ ROM にコピー

[書式]　**copy exec** *from to*

[設定値]
- *from* ..... コピー元ファイル名
  - 内蔵フラッシュROM の実行形式ファームウェアファイル番号 (RT300i、SRT100 以外の機種で指定可能)、0 のみ指定可
  - usb1:*filename*..... USB メモリ内の実行形式ファームウェアファイル名、 *filename* は 64 文字以内 (USB インタフェースを持つ機種のみ)
  - sd1:*filename*..... microSD カード内の実行形式ファームウェアファイル名、 *filename* は 64 文字以内 (microSD インタフェースを持つ機種のみ)
  - *:*filename*..... USB メモリおよび microSD カード内の実行形式ファームウェアファイル名 (*filename* は 64 文字以内)
  - ext0:*filename*..... PCMCIA Flash ATA カードの実行形式ファームウェアファイル名 (RT300i のみ)
- *to* ..... コピー先ファイル名
  - 内蔵フラッシュ ROM の実行形式ファームウェアファイル番号 (RT300i 以外の機種で指定可能) RTX1200..0、 1 が指定可、SRT100..0 のみ指定可、左記以外の機種 ..1 のみ指定可
  - internal..... 保存先を示すキーワード (RT300i のみ)

[説明]　実行形式ファームウェアファイルを内蔵フラッシュ ROM にコピーする。
内蔵フラッシュ ROM へコピーした内容を、実際の動作に反映させるためには、本コマンドの実行後にルーターを再起動する必要がある。

外部メモリに "*" を指定した場合、指定するファイルの検索はまず microSD メモリカードから行われ、指定したファイルがなければ USB メモリが検索される。
filename は絶対パスを使ってファイルを指定するかファイル名のみを指定する。
filename にファイル名のみを指定した場合は外部メモリ内から自動検索する。
複数のファイルがある場合、ディレクトリ階層上最もルートディレクトリに近く、アルファベット順に先のディレクトリにあるファイルが選ばれる。

[ノート]　外部メモリ内のファイルを指定できるのは、外部メモリインタフェースを持つ機種に限られる。
コピー先ファームウェアファイル番号に 0 以外を指定できるのはファームウェア多重機能を持つ機種に限られる。

ファイルの自動検索ができるのは Rev.10.01 系以降である。
外部メモリのディレクトリ構成やファイル数によっては、ファイルの検索に時間がかかることがある。
検索時間を短くするためには、階層の深いディレクトリの作成は避けてルートに近い位置にファイルを格納したり、ファイルを絶対パスで直接指定することが望ましい。
自動検索のタイムアウトの時間は **external-memory auto-search time** コマンドで設定できる。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	RT300i	RT250i	~~RT107e~~	SRT100

45.3.6　設定ファイルの削除

[書式]　**delete config** *filename*

[設定値]
- *filename* ..... 削除するファイル名
  - ext0:*name*..... PCMCIA Flash ATA カードのファームウェア (RT300i)
  - 内蔵フラッシュ ROM の設定ファイル番号

[説明]　保存されている設定ファイルを削除する。
指定可能なファイル名は以下の通りである。

RTX2000, RT300i	0..9
RTX1000	0
上記以外のモデル	0..4.2

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

45.3.7　実行形式ファームウェアファイルの削除

[書式]　**delete exec** *filename*

[設定値]
- *filename*.....削除するファイル名
  - ext0:*name*.....PCMCIA Flash ATA カードのファームウェア (RT300i)
  - 実行形式ファームウェアファイル番号 (1 のみ指定可能)

[説明]　保存されている実行形式ファームウェアファイルを削除する。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	RT300i	RT250i	~~RT107e~~	~~SRT100~~

45.3.8　デフォルト設定ファイルの設定

[書式]　**set-default-config** *filename*

[設定値]
- *filename*.....設定ファイル番号 (0..4.2)

[説明]　起動時に使用する設定ファイルを設定する。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	RT250i	RT107e	SRT100

45.3.9　デフォルトファームウェアファイルの設定

[書式]　**set-default-exec** *filename*

[設定値]
- *filename*.....実行形式ファームウェアファイル番号 (0..1)

[説明]　起動時に使用するファームウェアファイルを設定する。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	RT250i	~~RT107e~~	~~SRT100~~

45.3.10　設定の初期化

[書式]　**cold start**

[設定値]　なし

[説明]　工場出荷時の設定に戻し、再起動する。
コマンド実行時に管理パスワードを入力する必要がある。

[ノート]　内蔵 Flash ROM の設定ファイルがすべて削除されることに注意。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

45.3.11　遠隔地のルーターの設定

[書式]　**remote setup** *interface* [*number* [*/sub_address*]] [*type*]
remote setup *interface* dlci=*dlci*

[設定値]
- *interface*.....インタフェース名
  - BRI インタフェース名
  - PRI インタフェース名
- *number*.....ISDN 番号
- *sub_address*.....ISDN サブアドレス (0x21 から 0x7e の ASCII 文字列)
- *dlci*.....フレームリレーの DLCI 番号
- *type*.....リモートセットアップの方式
  - retransmission.....データの欠落に対応できる方式

[説明]　指定したインタフェースを利用して、遠隔地のルーターの設定をする。
インタフェースには BRI、PRI とも利用でき、また、ISDN、専用線、フレームリレーいずれの場合でも設定できる。
FOMA に対してリモートセットアップを行う場合のみ、retransmission の指定が必要である。
retransmission を指定した場合は、データの欠落を復旧できる仕組みのリモートセットアップを行い、今までのリモートセットアップ機能とは互換性がない。
retransmission を指定できるのは RTX3000、RTX1100、RTX1500、RTX1200 である。

[ノート]　専用線の場合は、*number*、*sub_address* パラメータは不要。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

45.3.12　遠隔地のルーターからの設定に対する制限

[書式]　**remote setup accept** *isdn_num*[/*sub_address*] [*isdn_num_list*]
remote setup accept *any*
remote setup accept none
no remote setup accept

[設定値]
- *isdn_num*..... ISDN 番号
- *sub_address*..... ISDN サブアドレス (0x21 から 0x7e の ASCII 文字列)
- *isdn_num_list*..... ISDN 番号だけまたは ISDN 番号とサブアドレスを空白で区切った並び
- any ..... すべての遠隔地のルーターからの設定を許可することを示すキーワード
- none ..... すべての遠隔地のルーターからの設定を拒否することを示すキーワード

[説明]　自分のルーターの設定を許可する相手先を設定する。

[初期値]　any

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	SRT100

45.4　動的情報のクリア操作

45.4.1　アカウントのクリア

[書式]　**clear account**
clear account *interface*
clear account pp [*peer_num*]

[設定値]
- *interface*
  - BRI インタフェース名
  - PRI インタフェース名
- *peer_num*
  - 相手先情報番号
  - 省略時は現在選択している相手先

[説明]　指定したインタフェース (第 1 書式ではすべての合計) に関するアカウントをクリアする。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

45.4.2　ARP テーブルのクリア

[書式]　**clear arp**

[設定値]　なし

[説明]　ARP テーブルをクリアする。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

45.4.3　IP の動的経路情報のクリア

[書式]　**clear ip dynamic routing**

[設定値]　なし

[説明]　動的に設定された IP の経路情報をクリアする。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

45.4.4　IPX の動的経路情報のクリア

[書式]　**clear ipx dynamic routing**

[設定値]　なし

[説明]　動的に設定された IPX の経路情報をクリアする。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

45.4.5　IPX の動的 SAP 情報のクリア

[書式]　**clear ipx dynamic sap**

[設定値]　なし

[説明]　IPX SAP テーブル中、動的に得られた SAP 情報をクリアする。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

45.4.6　ブリッジのラーニング情報のクリア

[書式]　**clear bridge learning**
clear bridge learning *bridge_interface*

[設定値]　◦ *bridge_interface*.....ブリッジインタフェース名

[説明]　動的に受け取ったブリッジのラーニング情報をすべて消去する。
RT300i は、第 1 書式を使用する。
SRT100 は、第 2 書式を使用する。

[ノート]　静的に設定した登録情報は消去されない。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	SRT100

45.4.7　ログのクリア

[書式]　**clear log**

[設定値]　なし

[説明]　ログをクリアする。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

45.4.8　InARP のクリア

[書式]　**clear inarp**

[設定値]　なし

[説明]　選択されている相手について InARP で得られた相手 IP アドレスをクリアし、InARP が on なら再度 InARP を開始する。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

45.4.9　DNS キャッシュのクリア

[書式]　**clear dns cache**

[設定値]　なし

[説明]　DNS リカーシブサーバーで持っているキャッシュをクリアする。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

45.4.10　PRI のステータス情報のクリア

[書式]　**clear pri status** *pri*

[設定値]　◦ *pri*.....PRI 番号 (1..4)

[説明]　PRI のステータス情報をクリアする。

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	RT250i	~~RT107e~~	~~SRT100~~

45.4.11　NAT アドレステーブルのクリア

[書式]　**clear nat descriptor dynamic** *nat_descriptor*

[設定値]　◦ *nat_descriptor*
- NAT ディスクリプタ番号 (1..2147483647)
- *all*..... すべての NAT ディスクリプタ番号

[説明]　NAT アドレステーブルをクリアする。

[ノート]　通信中にアドレス管理テーブルをクリアした場合、通信が一時的に不安定になる可能性がある。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

45.4.12　インタフェースの NAT アドレステーブルのクリア

[書式]　**clear nat descriptor interface dynamic** *interface*
clear nat descriptor interface dynamic pp [*peer_num*]
clear nat descriptor interface dynamic tunnel [*tunnel_num*]

[設定値]　◦ *interface*..... LAN インタフェース名

◦ *peer_num*
- 相手先情報番号
- *anonymous*
- 省略時は現在選択されている相手先

◦ *tunnel_num*
- トンネルインタフェース番号
- 省略時は現在選択されているトンネルインタフェース

[説明]　インタフェースに適用されている NAT アドレステーブルをクリアする。

[ノート]　RT250i では **clear nat descriptor interface dynamic tunnel** コマンドは使用できない。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

45.4.13　IPv6 の動的経路情報の消去

[書式]　**clear ipv6 dynamic routing**

[設定値]　なし

[説明]　経路制御プロトコルが得た IPv6 の経路情報を消去する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

45.4.14　近隣キャッシュの消去

[書式]　**clear ipv6 neighbor cache**

[設定値]　なし

[説明]　近隣キャッシュを消去する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

45.5　その他の操作

45.5.1　相手先の使用許可の設定

[書式]　**pp enable** *peer_num*
no pp enable *peer_num*

[設定値]　◦ *peer_num*
- 相手先情報番号
- *anonymous*
- *all*..... すべての相手先情報番号

[説明]　相手先を使用できる状態にする。工場出荷時、すべての相手先は disable 状態なので、使用する場合は必ずこのコマンドで enable 状態にしなければならない。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

45.5.2　相手先の使用不許可の設定

[書式]　**pp disable** *peer_num*

[設定値]
- *peer_num*
  - 相手先情報番号
  - *anonymous*
  - *all* ..... すべての相手先情報番号

[説明]　相手先を使用できない状態にする。
相手先の設定を行う場合は disable 状態であることが望ましい。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

45.5.3　再起動

[書式]　**restart**
restart *binary*
restart *binary config*
restart *config_name*

[設定値]
- *binary*
  - PCMCIA Flash ATA カードの実行形式ファイル名 (RT300i)
  - 実行形式ファームウェアファイル番号 (0..1)
- *config*
  - PCMCIA Flash ATA カードの設定ファイル名 (RT300i)
  - 内蔵フラッシュ ROM の設定ファイル番号
    (RT300i：0..9, それ以外のモデル：0..4.2)
- *config_name*
  - PCMCIA Flash ATA カードの設定ファイル名 (RT300i)
  - 設定ファイル名 (config0..config4.2)

[説明]　ルーターを再起動する。
RTX2000 と RTX1000 では第 1 書式のみ使用可能。
RT107e と SRT100 では第 1、4 書式のみ使用可能。
起動時の設定ファイルと実行形式ファームウェアファイルを指定できる。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

45.5.4　インタフェースの再起動

[書式]　**interface reset** *interface* [*interface ...*]

[設定値]
- *interface*
  - LAN インタフェース名
  - BRI インタフェース名
  - PRI インタフェース名

[説明]　指定したインタフェースを再起動する。
LAN インタフェースでは、オートネゴシエーションする設定になっていればオートネゴシエーション手順が起動される。
BRI と PRI インタフェースでは、回線種別を **line type** コマンドで変更した場合には、本コマンドでインタフェースを再起動する必要がある。
なお、MP を使用しているインタフェースに対しては、**interface reset pp** コマンドを使用する。

[ノート]　RTX1500/RTX1100/RTX1000/RT107e/SRT100 では、lan1 または lan2 に対してこのコマンドを実行すると、lan1 および lan2 インタフェースが同時にリセットされる。
RTX1200 では、いずれか一つの LAN インタフェースに対してこのコマンドを実行すると、すべての LAN インタフェースが同時にリセットされる。
LAN インタフェースだけを持つモデルでは、*interface* パラメータに LAN インタフェース名のみ指定可能。

line type コマンド、**pp bind** コマンド、経路情報などすべての設定を整えた後に実行する。対象とするインタフェースがバインドされているすべての相手先情報番号の通信を停止した状態で、また回線種別を変更する場合には回線を抜いた状態で実行すること。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

45.5.5 PP インタフェースの再起動

[書式] **interface reset pp** [*peer_num*]

[設定値] ◦ *peer_num*
- 相手先情報番号
- *anonymous*

[説明] 選択した相手先番号にバインドされているインタフェースをリセットする。MP を使用しているインタフェースに対して使用する。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

45.5.6 発信

[書式] **connect** *peer_num*

[設定値] ◦ *peer_num*..... 発信相手の相手先情報番号

[説明] 手動で発信する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

45.5.7 切断

[書式] **disconnect** *peer_num*

[設定値] ◦ *peer_num*
- 切断する相手先情報番号
- *all*..... すべての相手先情報番号
- *anonymous*..... anonymous のすべて
- 指定した anonymous(*anonymous*1 ..)

[説明] 手動で切断する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

45.5.8 ping

[書式] **ping** [*-s datalen*] [*-c count*] [*-sa ip_address*] [*-w wait*] *host*

[設定値] ◦ *datalen*..... データ長 (64 .. 65535)

◦ *count*..... 実行回数 (1..21474836)

◦ *ip_address*..... 始点 IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))

◦ *wait*..... パケット送信間隔秒数 (0.1..99.9)

◦ *host*
- ping をかけるホストの IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))
- ping をかけるホストの名称

[説明] ICMP Echo を指定したホストに送出し、ICMP Echo Reply が送られてくるのを待つ。送られてきたら、その旨表示する。コマンドが終了すると簡単な統計情報を表示する。
count パラメータを省略すると、Ctrl+c キーを入力するまで実行を継続する。
-w オプションを指定した時には、次のパケットを送信するまでの間に相手からの返事を確認できなかった時にはその旨のメッセージを表示する。-w オプションを指定していない時には、パケットが受信できなくても何もメッセージを表示しない。

[ノート] -w オプションは Rev.7.01.34 以降で使用可能。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

45.5.9　ping6 の実行

[書式]　**ping6** *destination* [*count*]
ping6 *destination%scope_id* [*count*]
ping6 *destination interface* [*count*]
ping6 *destination* pp *peer_num* [*count*]
ping6 *destination* tunnel *tunnel_num* [*count*]

[設定値]
- *destination* ..... 送信する宛先の IPv6 アドレス、または名前
- *scope_id* ..... スコープ識別子
- *interface* ..... LAN インタフェース名
- *peer_num* ..... 相手先情報番号
- *tunnel_num* ..... トンネルインタフェース番号
- *count* ..... 送信回数 (1..21474836)

[説明]　指定した宛先に対して ICMPv6 Echo Request を送信する。
スコープ識別子は、**show ipv6 address** コマンドで表示できる。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

45.5.10　traceroute

[書式]　**traceroute** *host* [noresolv]

[設定値]
- *host*
  - traceroute をかけるホストの IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))
  - traceroute をかけるホストの名称
- noresolv ..... DNS による解決を行わないことを示すキーワード

[説明]　指定したホストまでの経路を調べて表示する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

45.5.11　traceroute6 の実行

[書式]　**traceroute6** *destination*

[設定値]
- *destination* ..... 送信する宛先の IPv6 アドレス、または名前

[説明]　指定した宛先までの経路を調べて表示する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

45.5.12　nslookup

[書式]　**nslookup** *host*

[設定値]
- *host*
  - IP アドレス (xxx.xxx.xxx.xxx(xxx は十進数))
  - ホスト名

[説明]　DNS による名前解決を行う。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

45.5.13　IPv4 動的フィルタのコネクション管理情報の削除

[書式]　**disconnect ip connection** *session_id* [*channel_id*]

[設定値]
- *session_id* ..... セッションの識別子
- *channel_id* ..... チャネルの識別子

[説明]　指定したセッションに属する特定のチャネルを削除する。チャネルを指定しないときには、そのセッションに属するすべてのチャネルを削除する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	~~SRT100~~

45.5.14 TELNET クライアント

[書式] **telnet** *host* [*port* [*mode* [*negotiation* [*abort*]]]]

[設定値] ◦ *host*..... TELNET をかける相手の IP アドレス、またはホスト名

◦ *port*..... 使用するポート番号
- 十進数
- ポート番号のニーモニック
- 省略時は 23 (TELNET)

◦ *mode*..... TELNET 通信 (送信) の動作モード
- character ..... 文字単位で通信する
- line ..... 行単位で通信する
- auto ..... *port* パラメータの設定値により character/line を選択
- 省略時は auto

◦ *negotiation*..... TELNET オプションのネゴシエーションの選択
- on..... ネゴシエーションする
- off..... ネゴシエーションしない
- auto ..... *port* パラメータの設定値により on/off を選択
- 省略時は auto

◦ *abort*..... TELNET クライアントを強制的に終了させるためのアボートキー
- 十進数の ASCII コード
- 省略時は 29(^])

[説明] TELNET クライアントを実行する。

[ノート] character モードは、通常の TELNET サーバーなどへの接続のための透過的な通信を行う。
line モードは、入力行を編集して行単位の通信を行う。行編集の終了は、改行コード (CR:0x0d または LF:0x0a) の入力で判断する。

ポート番号による機能自動選択について
1. TELNET 通信の動作モードの自動選択
   port 番号が 23 の場合は文字単位モードとなり、そうでない場合は行単位モードとなる。
2. TELNET オプションのネゴシエーションの自動選択
   port 番号が 23 の場合はネゴシエーションし、そうでない場合はネゴシエーションしない。

[初期値] *port* = 23
mode = auto
negotiation = auto
abort = 29

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

45.5.15 IPv6 動的フィルタのコネクション管理情報の削除

[書式] **disconnect ipv6 connection** *session_id* [*channel_id*]

[設定値] ◦ *session_id*..... セッションの識別子

◦ *channel_id*..... チャネルの識別子

[説明] 指定したセッションに属する特定のチャネルを削除する。チャネルを指定しないときには、そのセッションに属するすべてのチャネルを削除する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	~~SRT100~~

45.5.16 スイッチングハブ MAC アドレステーブルの消去

[書式] **clear switching-hub macaddress** [*interface*]

[設定値] ◦ *interface*
- LAN インタフェース名

[説明] スイッチングハブ LSI 内部に保持している動的 MAC アドレステーブルを消去する。

[ノート] **lan type** コマンドの *macaddress-aging* パラメータが off の場合にこのコマンドを実行してもテーブルエントリ情報は消去されず、次に *macaddress-aging* パラメータが on にされた時点で消去される。
Rev.7.01.34 以降、Rev.8.01.12 以降で使用可能。

[適用モデル]

~~RTX3000~~	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

45.5.17　PRI のループバックの実行

[書式]　**pri loopback active** *pri a data*
pri loopback active *pri* timeslot *head num data*

[設定値]
- *pri*.....PRI 番号 (1..4)
- a.....ループバック A を示すキーワード
- timeslot.....タイムスロットループバックを示すキーワード
- *data*.....送信データパターン (1..4)

data	**擬似ランダムパターン**
1	$2^6 - 1$
2	$2^7 - 1$
3	$2^9 - 1$
4	$2^{11} - 1$

- *head*.....先頭タイムスロット番号 (1..24)
- *number*.....タイムスロット数 (1..24)

[説明]　指定したデータパターンを送信して、ループバックテストを行う。コマンドを実行する場合に、管理パスワードを入力する必要がある。*a* キーワードの場合は、24B すべてのタイムスロットがループバックする。ループバックするポイントはルーターの PRI コネクタの直前であり、PRI コネクタにケーブルを接続しているとその先の機器を破壊する可能性があるので、必ずケーブルを抜いてからテストを行わなければならない。timeslot キーワードの場合には、指定したタイムスロットに対してだけループバックテストを行う。データがループバックするのは、接続相手のルーターなので、あらかじめ相手のルーターをループバックを待ち受けるモードに設定しておく必要がある。ループバックテストが終わると、自動的に通信モードに復帰する。

[ノート]　ループバック A の場合は、PRI コネクタを外した状態で行う必要がある。タイムスロットループバックを実行する前に、相手ルーターはループバック待ち受け状態になっている必要がある。**save** コマンドを実行しても不揮発性メモリには保存されない。専用回線に対してのみ実行可能。

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	RT250i	~~RT107e~~	~~SRT100~~

45.5.18　PRI のループバック待ち受けの設定

[書式]　**pri loopback passive** *pri* remote
pri loopback passive *pri* payload
pri loopback passive *pri* timeslot *head number*
pri loopback passive *pri* **off**

[設定値]
- *pri*.....PRI 番号 (1..4)
- remote.....ループバックポイントが PRI コネクタであることを示すキーワード
- payload.....ループバックポイントがペイロードであることを示すキーワード
- timeslot.....タイムスロットループバックを示すキーワード
- *head*.....先頭タイムスロット番号 (1..24)
- *number*.....タイムスロット数 (1..24)

[説明]　相手からのタイムスロットループバックテストに対して待ち受けるモードに入る。コマンドを実行する場合に、管理パスワードを入力する必要がある。また、このコマンド実行後には、通常の通信は行えなくなる。remote および payload キーワードの場合は、24B すべてのタイムスロットがループバックされる。timeslot キーワードの場合には、指定したタイムスロットに対してだけループバックテストされる。**pri loopback passive off** コマンドを実行すると、ループバックテストを終了して待ち受けモードから通常の通信モードへ復帰する。

[ノート]　ループバックテストの結果は、実行側にしか表示されない。**save** コマンドを実行しても不揮発性メモリには保存されない。専用回線に対してのみ実行可能。

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	RT250i	~~RT107e~~	~~SRT100~~

45.5.19 Magic Packetの送信

[書式]
wol send [-i *interval*] [-c *count*] *interface mac_address* [*ip_address* [udp *port*]]
wol send [-i *interval*] [-c *count*] *interface mac_address* ethernet *type*

[設定値]
- *interval*..... パケットの送信間隔 (秒)
- *count*..... パケットの送信回数
- *interface*..... LAN インタフェース名
- *mac_address*..... MAC アドレス
- *ip_address*..... IPv4 アドレス
- *port*..... UDP ポート番号
- *type*..... イーサネットタイプフィールドの値 (1501..65535)

[説明]
指定した LAN インタフェースに Magic Packet を送信する。

第 1 書式では、IPv4 UDP パケットとして UDP ペイロードに Magic Packet データシーケンスを格納したパケットを送信する。終点 IP アドレスと、終点 UDP ポート番号を指定できるが、省略した場合には、終点 IP アドレスとしてはインタフェースのディレクティッドブロードキャストアドレスが、終点ポート番号には 9(discard) が使われる。
また、終点 IP アドレスを指定した場合にはユニキャストでパケットを送信する。その場合、通常のルーティングや ARP の手順は踏まず、終点 MAC アドレスはコマンドで指定したものになる。終点 IP アドレスを省略した場合にはブロードキャストでパケットを送信する。

第 2 書式では、Ethernet ヘッダの直後から Magic Packet のデータシーケンスが始まるパケットを送信する。

どちらの形式でも、-i、-c オプションで Magic Packet の送信間隔および回数を指定できる。パケットの送信中でも、^C キーでコマンドを中断できる。

[ノート]
ヤマハ製ルーター自身が直結している LAN インタフェース以外には Magic Packet を送信できない。
Rev.7.01.34 以降、Rev.8.01.12 以降、Rev.10.00.31 以降で使用可能。

[初期値]
interval = 1
count = 4

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

45.5.20 HTTP を利用したファームウェアのチェックおよびリビジョンアップの実行

[書式]
http revision-up go [no-confirm [prompt]]

[設定値]
- no-confirm..... 書き換え可能なリビジョンのファームウェアが存在するときに、ファームウェアの更新を行うかどうかを確認しない
- prompt ..... コマンド実行後、すぐにプロンプトを表示させ、他のコマンドを実行できるようにする

[説明]
WEB サーバーに置いているファームウェアと現在実行中のファームウェアのリビジョンをチェックし、書き換え可能であればファームウェアのリビジョンアップを行う。書き換え可能なリビジョンのファームウェアが存在すると、「更新しますか？ (Y/N)」という確認を求めてくるので、更新する場合は "Y" を、更新しない場合は "N" を入力する必要がある。

"no-confirm" オプションを指定すると、更新の確認をせずにファームウェアの書き換えを行う。さらに、"prompt" オプションを指定すると、コマンド実行直後にプロンプトが表示され、続けて他のコマンドを実行することができるようになる。ただし、ファームウェアを内蔵フラッシュ ROM に書き込んでいる間は他の操作ができなくなる。"prompt" オプションは RTX1100、RTX1500 でのみ指定することが可能。

http revision-up permit コマンドで HTTP リビジョンアップを許可されていない時は、ファームウェアの書き換えは行わない。

http revision-down permit コマンドでリビジョンダウンが許可されている場合は、WEB サーバーにおいてあるファームウェアが現在のファームウェアよりも古いリビジョンであってもファームウェアの書き換えを行う。

なお、WEB サーバーにおいてあるファームウェアが現在のファームウェアと同一リビジョンの場合には、ファームウェアの書き換えは行わない。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

45.5.21　入力遮断フィルタの状態のクリア

[書式]　**clear ip inbound filter** [*interface* [*id*]]
clear ipv6 inbound filter [*interface* [*id*]]

[設定値]
- *interface*.....インタフェース
  - LAN インタフェース (lan1、lan2 など)
  - PP インタフェース (pp 1、pp 2 など) ※ 'pp' と番号の間には空白が必要
  - TUNNEL インタフェース (tunnel 1、tunnel 2 など) ※ 'tunnel' と番号の間には空白が必要
- *id* .....フィルタの識別子 (1 .. 65535)

[説明]　指定した入力遮断フィルタに関するログなどの情報をクリアする。インタフェースや ID を指定しないときには、すべてのインタフェースや ID が対象になる。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

45.5.22　ポリシーフィルタの状態のクリア

[書式]　**clear ip policy filter** [*id*]
clear ipv6 policy filter [*id*]

[設定値]
- *id* .....フィルタの識別子 (1 .. 65535)

[説明]　指定したポリシーフィルタに関するログなどの情報をクリアする。ID を指定しないときにはすべてのポリシーフィルタが対象になる。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

45.5.23　URL フィルタの統計情報のクリア

[書式]　**clear url filter**
clear url filter [*interface*]
clear url filter pp [*perr_num*]
clear url filter tunnel [*tunnel_num*]

[設定値]
- *interface*.....LAN インタフェース名
- *peer_num*.....相手先情報番号
- *tunnel_num*..... トンネルインタフェース番号

[説明]　URL フィルタの統計情報を消去する。インタフェースが指定されない場合は、すべてのインタフェースの情報を消去する。

[ノート]　RTX3000 は、Rev.9.00.31 以降で使用可能。
RTX1100、RT107e は、Rev.8.03.60 以降で使用可能。

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

45.5.24　状態メール通知の実行

[書式]　**mail notify status exec** *id*

[設定値]
- *id* .....設定番号 (1..10)

[説明]　状態メール通知機能でメールを送信する。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

46. 設定の表示

46.1 機器設定の表示

[書式] **show environment**

[設定値] なし

[説明] 以下の項目が表示される。
- ポリシーフィルタリングモジュールのバージョン (ポリシーフィルタ機能をもつ機種)
- システムのリビジョン
- CPU、メモリの使用量 (%)
- 動作しているファームウェアと設定ファイル (Rev.8.02 系以降のファームウェア)
- 起動時に使用されるファームウェアと設定ファイル (Rev.8.02 系以降のファームウェア)
- 電源の状態 (RT300i)
- ファンの状態 (RTX3000、RT300i、RTX2000)
- 内部温度の状態 (RTX3000、RTX2000、RTX1500、RT250i、RTX1200)

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

46.2 すべての設定内容の表示

[書式] **show config**
show config *filename*
less config
less config *filename*

[設定値] ◦ *filename* ..... 設定ファイル名または退避ファイル名 (0..4.2)

[説明] 設定されたすべての設定内容を表示する。
Rev.8.02 系以降のファームウェアで第 2 書式が利用できる。ファイルを指定した場合には、ログインパスワードと管理パスワードを問い合わせられる。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

46.3 指定した PP の設定内容の表示

[書式] **show config pp** [*peer_num*]
less config pp [*peer_num*]

[設定値] ◦ *peer_num*
- 相手先情報番号
- anonymous
- 省略時、選択されている相手について表示する

[説明] **show config**、**less config** コマンドの表示の中から、指定した相手先情報番号に関するものだけを表示する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

46.4 指定したトンネルの設定内容の表示

[書式] **show config tunnel** [*tunnel_num*] [expand]
less config tunnel [*tunnel_num*] [expand]

[設定値] ◦ *tunnel_num* ..... トンネル番号
省略時は、選択されているトンネルについて表示する

[説明] **show config**、**less config** コマンドの表示の中から、指定したトンネル番号に関するものだけを表示する。

expand キーワードを指定すると、**tunnel template** コマンドにて指定したトンネルテンプレートが適用された後の、実際にルーターの動作時に参照される設定を表示する。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

46.5　設定ファイルの一覧

[書式]　**show config list**
less config list

[設定値]　なし

[説明]　内蔵 Flash ROM に保存されている設定ファイルのファイル名、日時、コメントの一覧を表示する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

46.6　ファイル情報の一覧の表示

[書式]　**show file list** *location*
less file list *location*

[設定値]　◦ *location*.....表示するファイルのある位置
- internal .....内蔵フラッシュ ROM
- ext0 .....外付け Flash ATA カード

[説明]　指定した場所に格納されているファイルの情報を表示する。
RT300i 以外では *location* として internal のみ指定可能。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

46.7　インタフェースに付与されている IPv6 アドレスの表示

[書式]　**show ipv6 address** [*interface*]
show ipv6 address pp [*peer_num*]
show ipv6 address tunnel [*tunnel_num*]

[設定値]　◦ *interface*.....LAN インタフェース名、LOOPBACK インタフェース名、NULL インタフェース、ブリッジインタフェース名
◦ *peer_num*
- 相手先情報番号
- anonymous
- 省略時、選択されている相手について表示する

◦ *tunnel_num*.....相手先情報番号

[説明]　各インタフェースに付与されている IPv6 アドレスを表示する。
インタフェースを指定しない場合は、すべてのインタフェースについて情報を表示する。

[ノート]　インタフェース名を指定できるのは Rev.8.03 以降のファームウェアである。
ブリッジインタフェースを指定できるのは Rev.10.00.38 以降のリビジョンである。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

46.8　マスタクロックを得ている回線の表示

[書式]　**show line masterclock**

[設定値]　なし

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

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	RT250i	~~RT107e~~	~~SRT100~~

46.9　SSH サーバー公開鍵の表示

[書式]　**show sshd public key**

[説明]　SSH サーバーの公開鍵を表示する。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

46.10　指定したインタフェースのフィルタ内容の表示

[書式]　**show ip secure filter** *interface* [*dir*]
show ip secure filter pp [*peer_num*] [*dir*]
show ip secure filter tunnel [*tunnel_num*] [*dir*]

[設定値]　◦ *interface* ..... フィルタの適用されたインタフェース名
◦ *dir* ..... フィルタの適用された方向、'in' または 'out'

[説明]　指定したインタフェースに適用されているフィルタ定義の内容を表示する。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

46.11　ファームウェアファイルの一覧

[書式]　**show exec list**
less exec list

[設定値]　なし

[説明]　内蔵 Flash ROM に保存されている設定ファイルの情報を表示する

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

47. 状態の表示

47.1 ARP テーブルの表示

[書式]　**show arp** [*interface*[*/sub_interface*]]

[設定値]
- *interface*.....LAN インタフェース名
- *sub_interface* ..... 1 - 32 (RTX3000)
  1 - 8 (上記以外の機種)

[説明]　ARP テーブルを表示する。インタフェース名を指定した場合、そのインタフェース経由で得られた ARP テーブル情報だけを表示する。

[ノート]　インタフェース名を指定できるのは Rev.8.02 系のファームウェア以降である。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

47.2 インタフェースの状態の表示

[書式]　**show status** *interface*

[設定値]
- *interface*
  - LAN インタフェース名
  - BRI インタフェース名
  - PRI インタフェース名
  - ブリッジ インタフェース名

[説明]　インタフェースの状態を表示する。

[ノート]　ブリッジインタフェースを指定できるのは Rev.10.00.38 以降のリビジョンである。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

47.3 各相手先の状態の表示

[書式]　**show status pp** [*peer_num*]

[設定値]
- *peer_num*
  - 相手先情報番号
  - anonymous
  - 省略時、選択されている相手について表示する

[説明]　各相手先の接続中または最後に接続された場合の状態を表示する。
- 現在接続されているか否か
- 直前の呼の状態
- 接続 (切断) した日時
- 回線の種類
- 通信時間
- 切断理由
- 通信料金
- 相手とこちらの PP 側 IP アドレス
- 正常に送信したパケットの数
- 送信エラーの数と内訳
- 正常に受信したパケットの数
- 受信エラーの数と内訳
- PPP の状態
- CCP の状態
- その他

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

47.4 DLCI の表示

[書式]　**show dlci** [*peer_num*]

[設定値]
- *peer_num*.....相手先情報番号

[説明]　DLCI の値および InARP の状態を表示する。InARP が成功していれば相手の IP アドレスも表示される。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

47.5　IP の経路情報テーブルの表示

[書式]　**show ip route** *[destination]*
show ip route detail
show ip route summary

[設定値]　◦ *destination*
- 相手先 IP アドレス
- 省略時、経路情報テーブル全体を表示する

◦ detail ..... 現在有効な IPv4 経路に加えて、動的経路制御プロトコルによって得られた経路により隠されている静的経路も表示する
◦ summary ..... IPv4 の経路数をプロトコル毎に合計して表示する

[説明]　IP の経路情報テーブルまたは相手先 IP アドレスへのゲートウェイを表示する。
ネットマスクは設定時の表現に関わらず連続するビット数で表現される。
フレームリレーの場合は DLCI の値が表示される。

detail を指定した時には、現在有効な IPv4 経路に加えて、動的経路制御プロトコルによって得られた経路とのプリファレンス値の比較で隠されている静的経路も表示する。
summary を指定した時には、IPv4 の経路数をプロトコル毎に合計して表示する。

[ノート]　動的経路制御プロトコルで得られた経路については、プロトコルに応じて付加情報を表示する。表示する付加情報は以下のようになる。

プロトコル	付加情報
RIP	メトリック値
OSPF	内部 / 外部経路の別、コスト値、メトリック値 (外部経路のみ) Type 1 の外部経路の場合、コスト値はメトリック値を含んだ経路へのコスト値となる。 Type 2 の外部経路の場合、コスト値は ASBR へのコスト値となる。
BGP	無し

第 2 書式と第 3 書式は Rev.7.01.34 以降で使用可能。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

47.6　RIP で得られた経路情報の表示

[書式]　**show ip rip table**

[設定値]　なし

[説明]　RIP で得られた経路情報を表示する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

47.7　IPv6 の経路情報の表示

[書式]　**show ipv6 route**
show ipv6 route detail
show ipv6 route summary

[設定値]　◦ detail ..... 現在有効な IPv6 経路に加えて隠されている IPv6 経路も表示する
◦ summary ..... IPv6 の経路数をプロトコル毎に合計して表示する

[説明]　IPv6 の経路情報を表示する。

detail を指定したときには、現在有効な IPv6 経路に加えて、プリファレンス値の比較で隠されている IPv6 経路も表示する。

summary を指定したときには、IPv6 の経路数をプロトコル毎に合計して表示する。

[ノート]　第 2 書式と第 3 書式は Rev.9 以降で使用可能。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

47.8　IPv6 の RIP テーブルの表示

[書式]　**show ipv6 rip table**

[設定値]　なし

[説明]　IPv6 の RIP テーブルを表示する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

47.9　近隣キャッシュの表示

[書式]　**show ipv6 neighbor cache**

[設定値]　なし

[説明]　近隣キャッシュの状態を表示する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

47.10　IPXWAN の状態の表示

[書式]　**show ipx ipxwan** [*peer_num*]

[設定値]　◦ *peer_num*
- 相手先情報番号
- *anonymous*
- 省略時、選択されている相手先について表示する。

[説明]　IPXWANの状態を表示する。

[ノート]　複数 WAN ポートモデルでは *leased* を指定することはできない。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

47.11　SAP テーブルの表示

[書式]　**show ipx sap**

[設定値]　なし

[説明]　IPX SAP テーブルを表示する。
非 ASCII 文字は八進数で表示される。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

47.12　IPX の経路情報テーブルの表示

[書式]　**show ipx route**

[設定値]　なし

[説明]　IPX の経路情報テーブルを表示する。
フレームリレーの場合は DLCI の値が表示される。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

47.13　ブリッジのラーニング情報の表示

[書式]　**show bridge learning**
show bridge learning *bridge_interface*

[設定値]　◦ *bridge_interface*.....ブリッジインタフェース名

[説明]　ブリッジの MAC アドレスのラーニング情報を表示する。
フレームリレーの場合は DLCI の値が表示される。(RT300i のみ)
RT300i は、第 1 書式を使用する。
SRT100 は、第 2 書式を使用する。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	RT300i	~~RT250i~~	~~RT107e~~	SRT100

47.14　IPsec の SA の表示

[書式]　**show ipsec sa** [*id*]
show ipsec sa gateway [*gateway_id*] [detail]

[設定値]　◦ *id*
- SA の識別子
- 省略時はすべての SA について表示する

◦ *gateway_id*
- セキュリティ・ゲートウェイの識別子
- 省略時はすべてのセキュリティ・ゲートウェイの SA のサマリを表示する。

◦ detail ..... SA の詳細な情報を表示する。

[説明]　IPsec の SA の状態を表示する。
id で与えられた識別子を持つ SA の情報を表示する。

[ノート]　該当の SA の生成時に XAUTH 認証を行なった場合、
認証に使用したユーザ名
◦ RADIUS 認証を行なったか否か
◦ 通知した内部 IP アドレス
◦ 追加した経路情報
◦ 適用したフィルタの情報
を同時に表示する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	RT107e	SRT100

47.15　VRRP の情報の表示

[書式]　**show status vrrp** [*interface* [*vrid*]]

[設定値]　◦ *interface* ..... LAN インタフェース名
◦ *vrid* ..... VRRP グループ ID (1..255)

[説明]　VRRP の情報を表示する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

47.16　動的 NAT ディスクリプタのアドレスマップの表示

[書式]　**show nat descriptor address** [*nat_descriptor*]

[設定値]　◦ *nat_descriptor*
- NAT ディスクリプタ番号 (1..2147483647)
- all ..... すべての NAT ディスクリプタ番号

[説明]　*nat_descriptor* を省略した場合にはすべての NAT ディスクリプタ番号について表示する。
動的な NAT ディスクリプタのアドレスマップを表示する。

[ノート]　IP マスカレードで大量にポートを使用している場合は、全エントリの表示に時間がかかり通信に影響を及ぼすことがあるため、IP マスカレードで使用中のポートの個数を確認したいときは、**show nat descriptor masquerade port summary** コマンドを使うことを推奨する。
なお、**show nat descriptor masquerade port summary** コマンドは Rev.10.01.01 以降で使用可能である。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

47.17　動作中の NAT ディスクリプタの適用リストの表示

[書式]　**show nat descriptor interface bind** *interface*
show nat descriptor interface bind pp
show nat descriptor interface bind tunnel

[設定値]　◦ *interface* ..... LAN インタフェース名

[説明]　NAT ディスクリプタと適用インタフェースのリストを表示する。

[ノート]　RT250i では **show nat descriptor interface bind tunnel** コマンドは使用できない。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

47.18　LAN インタフェースの NAT ディスクリプタのアドレスマップの表示

[書式]　**show nat descriptor interface address** *interface*
show nat descriptor interface address pp *peer_num*
show nat descriptor interface address tunnel *tunnel_num*

[設定値]
- *interface*.....LAN インタフェース名
- *peer_num*.....相手先情報番号
- *tunnel_num*.....トンネルインタフェース番号

[説明]　インタフェースに適用されている NAT ディスクリプタのアドレスマップを表示する。

[ノート]　RT250i では ***show nat descriptor interface address tunnel*** コマンドは使用できない。
IP マスカレードで大量にポートを使用している場合は、全エントリの表示に時間がかかり通信に影響を及ぼすことがあるため、IP マスカレードで使用中のポートの個数を確認したいときは、***show nat descriptor masquerade port summary*** コマンドを使うことを推奨する。
なお、***show nat descriptor masquerade port summary*** コマンドは Rev.10.01.01 以降で使用可能である。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

47.19　IP マスカレードで使用しているポート番号の個数の表示

[書式]　**show nat descriptor masquerade port** [*nat_descriptor*] **summary**

[設定値]
- *nat_descriptor*
  - NAT ディスクリプタ番号 (1..2147483647)
  - *nat_descriptor* 省略時はすべての NAT ディスクリプタについて表示する。

[説明]　IP マスカレードで使用しているポート番号の個数を表示する。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

47.20　PPTP の状態の表示

[書式]　**show status pptp**

[設定値]　なし

[説明]　PPTP の状態や GRE の統計情報などを表示する。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	RTX1100	RTX1000	RT300i	~~RT250i~~	~~RT107e~~	~~SRT100~~

47.21　OSPF 情報の表示

[書式]　**show status ospf** *info*

[設定値]
- *info*.....表示する情報の種類
  - database.....OSPF のデータベース
  - neighbor.....近隣ルーター
  - interface.....各インタフェースの状態
  - virtual-link.....バーチャルリンクの状態

[説明]　OSPF の各種情報を表示する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

47.22　BGP の状態の表示

[書式]　**show status bgp neighbor** [*ip-address*]
show status bgp neighbor *ip-address route-type*

[設定値]
- *ip-address*.....隣接ルーターの IP アドレス
- *route-type*.....経路情報の表示
  - advertised-routes.....隣接ルーターに広告している経路を表示する
  - received-routes.....隣接ルーターから受信した経路を表示する
  - routes.....隣接ルーターから受信した経路のうち有効なものを表示する

[説明]　BGP の隣接ルーターに関する情報を表示する。

ip-address を指定した場合には特定の隣接ルーターの情報を表示する。ip-address を省略した場合には、すべての隣接ルーターの情報を表示する。

route-type を指定した場合には、隣接ルーターとの間でやり取りしている経路の情報を表示する。*advertised-routes* を指定した時には、隣接ルーターに対して広告している経路を表示する。*received-routes* を指定した時には、隣接ルーターから受信した経路をすべて表示する。*routes* を指定した時には、隣接ルーターから受信した経路のうち、**bgp export filter** などで受け入れられた経路だけを表示する。

[ノート]　Rev.7.01 系以降のファームウェアで使用できる。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

47.23　DHCP サーバーの状態の表示

[書式]　**show status dhcp** *[summary] [scope_n]*

[設定値]
- *summary*..... 各 DHCP スコープの IP アドレス割り当て状況の概要を表示する
- *scope_n*..... スコープ番号 (1-65535)

[説明]　各 DHCP スコープのリース状況を表示する。以下の項目が表示される。
- DHCP スコープのリース状態
- DHCP スコープ番号
- ネットワークアドレス
- 割り当て中 IP アドレス
- 割り当て中クライアント MAC アドレス
- リース残時間
- 予約済 (未使用) IP アドレス
- DHCP スコープの全 IP アドレス数
- 除外 IP アドレス数
- 割り当て中 IP アドレス数
- 利用可能アドレス数 (うち予約済 IP アドレス数)

[ノート]　Rev.8.03 系以降のファームウェアで summary を指定可能。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

47.24　DHCP クライアントの状態の表示

[書式]　**show status dhcpc**

[設定値]　なし

[説明]　DHCP クライアントの状態を表示する。

◦ クライアントの状態
- インタフェース
- IP アドレス (取得できないときはその状態)
- DHCP サーバー
- リース残時間
- クライアント ID
- ホスト名 (設定時)

◦ 共通情報
- DNS サーバー
- ゲートウェイ

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

47.25　バックアップ状態の表示

[書式]　**show status backup**

[設定値]　なし

[説明]　バックアップ設定されたインタフェースについて、バックアップの状態を表示する。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

47.26　動的フィルタによって管理されているコネクションの表示

[書式]　**show ip connection**
show ip connection *interface* [*direction*]
show ip connection pp [*peer_num* [*direction*]]
show ip connection tunnel [*tunnel_num* [*direction*]]
show ip connection summary

[設定値]
- *interface*.....LAN インタフェース名
- *peer_num*.....相手先情報番号
- *tunnel_num*..... トンネルインタフェース番号
- *direction*
  - in.....入力方向
  - out.....出力方向
- summary.....インタフェース / 方向単位の管理コネクション数、および全体の合計を表示する

[説明]　指定したインタフェースについて、動的なフィルタによって管理されているコネクションを表示する。インタフェースを指定しないときには、すべてのインタフェースの情報を表示する。

[ノート]　RT250i では **show ip connection tunnel** コマンドは使用できない。

show ip connection summary コマンドは RTX3000 のみ使用可能。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	~~SRT100~~

47.27　IPv6 の動的フィルタによって管理されているコネクションの表示

[書式]　**show ipv6 connection**
show ipv6 connection *interface* [*direction*]
show ipv6 connection pp [*peer_num* [*direction*]]
show ipv6 connection tunnel [*tunnel_num* [*direction*]]
show ipv6 connection summary

[設定値]
- *interface*.....LAN インタフェース名
- *peer_num*.....相手先情報番号
- *tunnel_num*..... トンネルインタフェース番号
- *direction*
  - in.....入力方向
  - out.....出力方向
- summary.....インタフェース / 方向単位の管理コネクション数、および全体の合計を表示する

[説明]　指定したインタフェースについて、動的なフィルタによって管理されているコネクションを表示する。インタフェースを指定しないときには、すべてのインタフェースの情報を表示する。

[ノート]　RT250i では **show ipv6 connection tunnel** コマンドは使用できない。

show ipv6 connection summary コマンドは RTX3000 のみ使用可能。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	~~SRT100~~

47.28　ネットワーク監視機能の状態の表示

[書式]　**show status ip keepalive**

[設定値]　なし

[説明]　ネットワーク監視機能の状態を表示する。

[ノート]　Rev.7.01 以上で実行可能。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	RT250i	RT107e	SRT100

47.29　侵入情報の履歴の表示

[書式]　**show ip intrusion detection**
show ip intrusion detection *interface* [*direction*]
show ip intrusion detection pp [*peer_num* [*direction*]]
show ip intrusion detection tunnel [*tunnel_num* [*direction*]]

[設定値]
- *interface* ..... LAN インタフェース名
- *peer_num* ..... 相手先情報番号
- *tunnel_num* ..... トンネルインタフェース番号
- *direction*
  - in ..... 入力方向
  - out ..... 出力方向

[説明]　最近の侵入情報を表示する。侵入情報は各インタフェースの各方向ごとに表示され、表示される最大件数は、RTX3000 では **ip intrusion detection report** コマンドで設定した値、それ以外の機種では 50 件までとなる。

[ノート]　RT250i では **show ip intrusion detection tunnel** コマンドは使用できない。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

47.30　相手先ごとの接続時間情報の表示

[書式]　**show pp connect time** [*peer_num*]

[設定値]
- *peer_num*
  - 相手先情報番号
  - anonymous
  - 省略時、選択されている相手について表示

[説明]　選択されている相手の接続時間情報を表示する。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

47.31　ネットボランチ DNS サービスに関する設定の表示

[書式]　**show status netvolante-dns** *interface*
show status netvolante-dns pp [*peer_num*]

[設定値]
- *interface* ..... LAN インタフェース名
- *peer_num*
  - 相手先情報番号
  - 省略時、選択されている相手について表示

[説明]　ダイナミック DNS に関する設定を表示する。

[表示内容]
```
ネットボランチ DNS サービス : AUTO/OFF
インタフェース :        INTERFACE
ホストアドレス :        aaa.bbb.netvolante.jp
 IP アドレス :          aaa.bbb.ccc.ddd
最新更新日時 :          2001/01/25 15:00:00
タイムアウト :          90 秒
```

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

47.32　スイッチングハブ MAC アドレステーブルの表示

[書式]　**show status switching-hub macaddress** [*interface* [*port*]]

[設定値]
- *interface* ..... LAN インタフェース名
- *port* ..... ポート番号 (1..4) (RTX1200 以外の機種)
  (1..8) (RTX1200)

[説明]　スイッチングハブ LSI 内部に保持しているポート毎の動的 MAC アドレステーブルを表示する。ポート番号を指定するとそのポートに関する情報のみが表示される。LAN インタフェース名にはスイッチングハブを持つインタフェースだけが指定可能である。

[ノート]　Rev.7.01.34 以降、Rev.8.01.12 以降で使用可能。

[適用モデル]

~~RTX3000~~	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

47.33　UPnP に関するステータス情報の表示

[書式]　**show status upnp**

[設定値]　なし

[説明]　UPnP に関するステータス情報を表示する。

[ノート]　Rev.8.01.07 以降で使用可能。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

47.34　トンネルインタフェースの状態の表示

[書式]　**show status tunnel** [*tunnel_num*]

[設定値]　◦ *tunnel_num*..... トンネルインタフェース番号

[説明]　トンネルインタフェースの状態を表示する。

[ノート]　Rev.8.01.07 以降で使用可能。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

47.35　VLAN インタフェースの状態の表示

[書式]　**show status vlan** [*interface/sub_interface*]

[設定値]　◦ *interface*.....LAN インタフェース名
◦ *sub_interface*..... 1 - 8

[説明]　VLAN インタフェースの情報を表示する。VLAN インタフェース名を指定した場合はそのインタフェースの情報だけを表示する。

[ノート]　Rev.8.02.28 以降で使用可能。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

47.36　トリガによるメール通知機能の状態の表示

[書式]　**show status mail service** [*template_id*] [debug]

[設定値]　◦ *template_id*..... テンプレート ID
◦ debug..... デバッグ用の内部情報を表示させる

[説明]　トリガによりメール通知する機能の内部情報を表示する。テンプレート ID を指定しない場合はすべてのテンプレート ID についての情報を表示する。

[ノート]　Rev.8.03 系のすべてのリビジョンで使用可能。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

47.37　マルチキャストの経路情報の表示

[書式]　**show ip mroute** [*option*]

[設定値]　◦ *option*..... 出力する経路情報の粒度
- summary..... マルチキャストのソース , グループ , 出力インタフェースに注目した最低限の情報を表示する
- normal..... summary で表示される内容に加え、各インタフェースの基本的な状態確認を目的とした表示をする
- detail ..... PIM-SM の各種状態管理を考慮した詳細な情報を表示する
- fib..... マルチキャストパケットの転送状況に注目した内容を出力する。マルチキャストパケットがどのインタフェースから入力され、どのインタフェースに転送されるかを確認することができる。

* 出力される表中の各項目
  - Inbound IF ..... 受信インタフェース
  - Source ..... 転送するパケットの送信元アドレス
  - Group ..... 転送するパケットの宛て先アドレス
  - Outbound IF ..... 送信インタフェース
  - TTL ..... パケットの受信の無い状態が続いた場合にルーターが転送情報を保持している時間
  - KAT ..... PIM-SM を利用している場合の Keepalive Timer の残り時間
  - Flags ..... PIM の各パラメータの動作状況 K (Keepalive), S (spt_bit)

[説明]　マルチキャストの経路情報を表示する。
オプションを指定することにより、表示内容の粒度を設定できる。

[ノート]　Rev.8.03 系以降のすべてのリビジョンで使用可能。

[初期値]　*option* = normal
オプションを指定しない場合は normal オプションと同じ内容を表示する

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

47.38　IGMP のグループ管理情報の表示

[書式]　***show status ip igmp***

[説明]　IGMP で管理されている情報を一覧表示する。
IGMP プロキシが動作している場合は、このコマンドで転送先を確認することができる。

[ノート]　Rev.8.03 系以降のすべてのリビジョンで使用可能。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

47.39　PIM-SM によって管理される情報の表示

[書式]　***show status ip pim sparse***

[説明]　PIM-SM で管理されている情報を一覧表示する。

[ノート]　Rev.8.03 系以降のすべてのリビジョンで使用可能。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

47.40　MLD のグループ管理情報の表示

[書式]　***show status ipv6 mld***

[説明]　MLD で管理されている情報を一覧表示する。
MLD プロキシが動作している場合は、このコマンドで転送先を確認することができる。

[ノート]　Rev.8.01.12 以降で使用可能。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	~~RT300i~~	~~RT250i~~	RT107e	SRT100

47.41　IPv6 マルチキャストの経路情報の表示

[書式]　***show ipv6 mroute fib***

[説明]　IPv6 マルチキャストパケットの転送経路を表示する。
このコマンドでは、転送経路ごとに以下の内容を一覧表示する。

- Inbound IF ..... 入力インタフェース
- Source ..... マルチキャストパケットのソースアドレス
- Group ..... マルチキャストパケットのグループアドレス
- Outbound IFs ..... 出力インタフェース。複数のインタフェースに出力される場合は、"," 区切りで表示される。

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

47.42　ログインしているユーザ情報の表示

[書式]　**show status user**

[説明]　ルーターにログインしているユーザの情報を表示する。以下の内容が表示される。

- ユーザ名
- 接続種別
- 接続した時間
- アイドル時間
- 接続相手の IP アドレス
- 管理ユーザか否か

自分自身のユーザ情報には、先頭にアスタリスク (*) が付く。

管理者モードになっているユーザは、ユーザ名の前にプラス (+) が付く。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

47.43　パケットバッファの状態の表示

[書式]　**show status packet-buffer** [*group*]

[設定値]
- *group* ..... 表示するパケットバッファのグループを指定する。グループ名 : small, middle, large, jumbo, huge パラメータを省略すると、すべてのグループを表示する。

[説明]　パケットバッファの状態を表示する。表示する項目は以下の通り :

- グループ名
- 格納できるパケットサイズ
- 管理パラメータ
- 現在、割り当て中のパケットバッファ数
- 現在、フリーリストにつながれているパケットバッファ数
- 現在、確保しているチャンク数
- パケットバッファの割り当て要求を受けた回数
- パケットバッファの割り当てに成功した回数
- パケットバッファの割り当てに失敗した回数
- パケットバッファが解放された回数
- チャンクを確保した回数
- チャンクを確保しようとして失敗した回数
- チャンクを解放した回数

[ノート]　jumbo グループは、LAN インタフェースとして 1000BASE-T インタフェース対応でかつ、ジャンボパケットの送受信ができる機種でのみ利用できる。

[実行例]
```
# show status packet-buffer large
large group: 2048 bytes length
parameters: max-buffer=10000 max-free=2812 min-free=62
                buffers-in-chunk=625 initial-chunk=4
2372 buffers in free list
128 buffers are allocated, req/succ/fail/rel = 137/137/0/9
4 chunks are allocated, req/succ/fail/rel = 4/4/0/0
```

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

47.44　QoS ステータスの表示

[書式]　**show status qos** *info* [*interface* [*class*]]

[設定値]
- *info* ..... 表示する情報の種類
  - bandwidth ..... 使用帯域
  - length ..... キューイングしているパケット数
  - dcc ..... Dynamic Class Control の制御状況
  - all ..... すべての情報
- *interface* ..... LAN インタフェース名
  省略時、全ての LAN インタフェースについて表示する
- *class* ..... クラス (1..16)

[説明]　インタフェースに対して、QoS の設定情報や各クラスの使用状況を表示する。
- LAN インタフェース名
- キューイングアルゴリズム
- インタフェース速度
- クラス数
- 各クラスの設定帯域、使用帯域、使用帯域のピーク値と記録日時
- 設定帯域の合計
- 各クラスのエンキュー成功回数 / 失敗回数、デキュー回数、保持しているパケット数、パケット数のピーク値と記録日時
- Dynamic Class Control により制御されているホストの情報と制御内容

[ノート]　*info* で *dcc* を設定できるのは SRT100 と RTX1200 である。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

47.45　連携動作の状態の表示

[書式]　**show status cooperation** *type* [*id*]

[設定値]
- *type*.....連携動作タイプ
  - bandwidth-measuring ....回線帯域検出
  - load-watch .....負荷監視通知
- *id*.....相手先 ID 番号 (1-100)

[説明]　連携動作の情報を表示する。

回線帯域検出の場合、以下の項目が表示される。
- 相手先情報
- 状態表示
  - 回数
  - 測定時刻
  - 測定結果 (クライアント動作のみ)
  - 現状 (クライアント動作のみ)
  - 設定変更履歴 (クライアント動作のみ)
  - 次の測定までの残り時間 (クライアント動作のみ)

負荷監視通知の場合、以下の項目が表示される。
- 相手先情報
- 状態表示
  - 抑制要請回数
  - 抑制解除回数
  - 履歴

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

47.46　OSPFv3 情報の表示

[書式]　**show ipv6 ospf** *info*

[設定値]
- *info*
  - database..... OSPFv3 のデータベース
  - neighbor..... 近隣ルーター
  - interface..... 各インタフェースの状態
  - virtual-link..... 仮想リンクの状態

[説明]　OSPFv3 の状態を表示する

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

47.47　入力遮断フィルタの状態表示

[書式]　**show status ip inbound filter** [*type*]
show status ipv6 inbound filter [*type*]

[設定値]
- *type*..... 表示の種類
  - summary..... サマリーだけを表示する

[説明]　入力遮断フィルタの状態を表示する。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

47.48　ポリシーフィルタの状態表示

[書式]　**show status ip policy filter** [*id* [*type*]]
show status ipv6 policy filter [*id* [*type*]]

[設定値]
- *id* .....表示したいフィルタの識別子 (1..65535)
  ※省略時はすべてのフィルタについて表示する
- *type*.....表示の形式
  - connection .....指定したフィルタに関係するコネクションの情報を表示する

[説明]　ポリシーフィルタの状態を表示する。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

47.49　ポリシーフィルタの制御対象サービスの表示

[書式]　**show status ip policy service**
show status ipv6 policy service

[説明]　ポリシーフィルタの制御対象とするサービスを表示する。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

47.50　URL フィルタの情報の表示

[書式]　**show url filter**
show url filter [*interface*]
show url filter pp [*peer_num*]
show url filter tunnel [*tunnel_num*]

[設定値]
- *interface*.....LAN インタフェース名
- *peer_num*.....相手先情報番号
- *tunnel_num*..... トンネルインタフェース番号

[説明]　インタフェースに適用されている URL フィルタの中で、どのフィルタに何回マッチしたかの統計情報を表示する。
インタフェースが指定されない場合は、すべてのインタフェースの情報を表示する。

表示される内容は以下の通り。
- フィルタ番号
- 始点 IP アドレス
- HTTP コネクションとフィルタが一致した回数

[ノート]　**url filter** コマンドで、キーワード、IP アドレスの両方に "*" を設定したフィルタがインタフェースに適用されている場合、HTTP コネクションがこのフィルタとマッチした回数は表示されない。
RTX3000 は、Rev.9.00.31 以降で使用可能。
RTX1100、RT107eは、Rev.8.03.60 以降で使用可能。

[適用モデル]

RTX3000	~~RTX2000~~	~~RTX1500~~	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

47.51　生存通知の状態の表示

[書式]　**show status heartbeat**

[設定値]　なし

[説明]　受信した生存通知の情報を表示する。
表示する内容は以下の通り。
- 通知された名前
- 通知された IP アドレス
- 最後に生存通知を受信した時刻
- 受信間隔 (秒)

[ノート]　RTX3000 は、Rev.9.00.31 以降で使用可能。
RTX1500、RTX1100、RT107eは、Rev.8.03.60 以降で使用可能。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

47.52　USB ホスト機能の動作状態を表示

[書式]　**show status usbhost** *[modem]*

[設定値]　なし

[説明]　USB ホスト機能の動作状態を表示する。
modem を指定した場合、USB ポートに接続した機器に関する接続情報を表示する。現在の通信状態や通信時に発生したエラーの累計、送受信した総 byte 数、発着信の回数、最新の接続情報などを表示する。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

47.53　リモートセットアップ機能に関する接続情報の表示

[書式]　**show status remote setup**

[設定値]　なし

[説明]　リモートセットアップ機能に関する接続情報を表示する。
現在の通信状態や通信時に発生したエラーの累計、送受信した総フレーム数、発着信の回数、最新の接続情報などを表示する。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

47.54　技術情報の表示

[書式]　**show techinfo**

[説明]　技術サポートに必要な情報を一度に出力する。
他の **show** コマンドとは異なり、**show techinfo** コマンドの出力は **console columns/lines** コマンドの設定を無視して一度に出力される。一画面ごとに出力が停止するページ動作は行わない。そのため、ターミナルソフトのログ機能を用いて、出力を PC のファイルとして保存することが望ましい。
また、**console character** コマンドの設定も無視され、常に英語モードで出力される。
一画面ごとに内容を確認しながら出力したいときには、以下のように **less** コマンドを併用するとよい。ただし、**less** コマンドは画面制御シーケンスを多数出力するため、ログを記録しながら **less** コマンドを使用すると、ログファイルがわかりにくくなる。
show techinfo | less

[ノート]　ルーターに対して PC で動作する TFTP クライアントからアクセスし、ファイル名 'techinfo' を GET すると、**show techinfo** コマンドの出力と同じものが得られる。
Windows XP の TFTP.EXE を使用した例 :
C:¥>tftp 192.168.0.1 get techinfo techinfo.txt

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	SRT100

47.55　microSD スロットの動作状態を表示

[書式]　**show status sd**

[設定値]　なし

[説明]　microSD スロットの動作状態を表示する。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

47.56　外部メモリの動作状態を表示

[書式]　**show status external-memory**

[設定値]　なし

[説明]　USB ポートと microSD スロットに接続されている外部メモリの状態や共通情報を表示する。

[ノート]　USB ポートに FOMA が接続されている場合は、USB ポートについては「外部メモリが接続されていません」と表示される。
FOMA の状態は show status usbhost modem で確認する。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	~~SRT100~~

48. ロギング

48.1　ログの表示

[書式]　**show log** *[reverse]*
less log *[reverse]*

[設定値]　◦ reverse.....ログを逆順に表示する

[説明]　ルーターの動作状況を記録したログを表示する。

RTX1200 はログを最大 10,000 件保持することができる。RTX1200 以外の機種ではログは最大 500 件保持することができる。最大数を越えた場合には、発生時刻の古いものから消去されていく。最大数以上のログを保存する場合には、**syslog host** コマンドでログを SYSLOG サーバーに転送して、そちらで保存する必要がある。

このコマンドでは、通常は発生時刻の古いものからログを順に表示するが、'reverse' を指定することで新しいものから表示させることができる。

ログは、ルーターの電源を切ると消去される。

[ノート]　RTX1000, RTX2000, RT300i では、**restart** コマンドや TFTP によるファームウェアのバージョンアップなどで電源を入れたままルーターが再起動した場合でもログは消去される。他の機種では、電源を切らない限りはログは保存される。

[適用モデル]

RTX3000	RTX2000	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	RT107e	SRT100

48.2　アカウントの表示

[書式]　**show account**
show account *interface*
show account pp *[peer_num]*

[設定値]　◦ *interface*
- BRI インタフェース名
- PRI インタフェース名

◦ *peer_num*
- 相手先情報番号
- *anonymous*
- 省略時、選択されている相手について表示する

[説明]　以下の項目を表示
- 発信回数
- 着信回数
- ISDN 料金の総計

[ノート]　電源 OFF や再起動により、それまでの課金情報がクリアされる。
課金額は通信の切断時に NTT から ISDN で通知される料金情報を集計しているため、割引サービスなどを利用している場合には、最終的に NTT から請求される料金とは異なる場合がある。また、NTT 以外の通信事業者を利用して通信した場合には料金情報は通知されないため、アカウントとしても集計されない。

[適用モデル]

RTX3000	~~RTX2000~~	RTX1500	RTX1200	RTX1100	RTX1000	RT300i	RT250i	~~RT107e~~	~~SRT100~~

48.3　通信履歴の表示

[書式]　**show history**

[設定値]　なし

[説明]　通信履歴を表示する。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	~~RTX1200~~	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	RT107e	~~SRT100~~

49. 診断

49.1 ポートの開閉状態の診断

[書式] **diagnose config port map** *interface protocol* [*src_addr* [*src_port*]] *dst_addr*

[設定値]
- *interface* ..... 受信側の LAN、PP インタフェース名
- *protocol* ..... 診断対象のパケット種別 (カンマで区切って複数指定可能)
  - プロトコルを表す十進数 (0..255)
  - プロトコルを表すニーモニック
    - tcp ..... TCP パケット
    - udp ..... UDP パケット
    - icmp ..... ICMP パケット
    - gre ..... PPTP の gre パケット
    - esp ..... IPsec の esp パケット
    - ah ..... IPsec の ah パケット
- *src_addr* ..... 入力パケットの送信元 IP アドレス
- *src_port* ..... 入力パケットの送信元ポート番号
- *dst_addr* ..... 診断対象の宛先 IP アドレス (カンマで区切って複数指定可能)

[説明] *interface* パラメータで指定されたインタフェースから受信するパケットがルーターを通過することが可能か診断をする。

tcp、udp パケットでは、*dst_addr* パラメータで指定された宛先 IP アドレスのウェルノウンポートに対して、ルーターを通過することのできるポートが存在した場合、その内容を表示する。tcp、udp 以外のパケットについては、ポートに関する設定は無視され、*dst_addr* までパケットが到達可能であった場合にその内容を表示する。

src_addr、及び、*src_port* が省略された場合、送信元 IP アドレスと送信元ポート番号は、フィルタの設定内容から必要と思われる組み合わせをルーターが自動的にサンプリングする。

[ノート] 本コマンドはルーターの内部だけで擬似的にパケットの転送処理を行うことにより実現しているため、*dst_addr* に指定されるホストに対して診断対象のパケットを送信することはない。そのため、ホスト側では閉じられているポートでもルーターを通過することが可能である場合は、そのポートは開いていると判断される。これは、*dst_addr* にルーター自身の IP アドレスが指定された場合も同様であり、ルーター自身のポートの開閉状態を診断するわけではない。

なお、本コマンドでは ethernet フィルタは考慮されない。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

49.2 ポートへ到達可能なアクセス範囲の診断

[書式] **diagnose config port access** *interface* [*protocol*] *dst_addr dst_port*

[設定値]
- *interface* ..... 受信側の LAN、PP インタフェース名
- *protocol* ..... 診断対象のパケット種別 (カンマで区切って複数指定可能、省略時は全種別)
  - tcp ..... TCP パケット
  - udp ..... UDP パケット
- *dst_addr* ..... 診断対象の宛先 IP アドレス
- *dst_port* ..... 診断対象の宛先ポート番号

[説明] *dst_addr/dst_port* パラメータで指定されたホストのポート番号へ、*protocol* パラメータで指定されたパケットが到達可能な送信元 IP アドレスと送信元ポート番号の範囲を表示する。

[ノート] 本コマンドはルーターの内部だけで擬似的にパケットの転送処理を行うことにより実現しているため、*dst_addr* に指定されるホストに対して診断対象のパケットを送信することはない。そのため、ホスト側では閉じられているポートでもルーターを通過することが可能である場合は、そのポートへ到達可能と判断される。これは、*dst_addr* にルーター自身の IP アドレスが指定された場合も同様であり、ルーター自身のポートの開閉状態には依存しない。

なお、本コマンドでは ethernet フィルタは考慮されない。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

49.3　ポートの開閉状態の診断で検出可能な通過パケットの最大数の設定

[書式]　**diagnosis config port max-detect** *num*

[設定値]　◦ *num*.....検出可能な通過パケットの最大数 (100..1000000)

[説明]　ポートの開閉状態の診断、および、ポートへ到達可能なアクセス範囲の診断で検出が可能な通過パケットの最大数を設定する。この数値を超えて通過パケットを検出した場合、診断が中断される。

[ノート]　ポートの開閉状態の診断結果では、通過可能な送信元アドレス空間と送信元ポート番号空間を可能な限り集約して表示している。しかし、集約前の通過数が本設定値を超えた時点で診断が中断されるため、診断結果で表示される通過数が、実際には本設定値を下回る場合でも診断が中断されることがある。

[初期値]　2000

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

49.4　ポートの開閉状態の診断結果の履歴数の設定

[書式]　**diagnosis config port history-num** *num*

[設定値]　◦ *num*.....診断結果として保存する履歴数 (1..10)

[説明]　ポートの開閉状態の診断、および、ポートへ到達可能なアクセス範囲の診断の診断結果として保存する履歴数を設定する。

[ノート]　本コマンドを実行したときに設定値を上回る履歴が既に保存されていた場合、設定値を超える履歴は消去される。

[初期値]　3

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

49.5　ポートの開閉状態の診断結果の表示

[書式]　**show diagnosis config port map**

[説明]　ポートの開閉状態の診断結果を表示する。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

49.6　ポートへ到達可能なアクセス範囲の診断結果の表示

[書式]　**show diagnosis config port access**

[説明]　ポートへ到達可能なアクセス範囲の診断結果を表示する。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

49.7　ポートの開閉状態の診断結果の消去

[書式]　**clear diagnosis config port**

[説明]　ポートの開閉状態の診断、および、ポートへ到達可能なアクセス範囲の診断の診断結果をすべて消去する。

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

50. 統計

50.1 統計機能を有効にするか否かの設定

[書式] **statistics** *type sw*
no statistics *type* [*sw*]

[設定値] ◦ *type*..... 内部リソースの種別
- cpu..... CPU 利用率
- memory..... メモリ使用率
- traffic..... 通信量
- flow..... ファストパスフロー数
- nat..... NAT エントリ数
- route..... 経路数
- filter..... フィルタにヒットした数
- qos ..... 各キューの処理量

◦ *sw*
- on..... 統計機能を有効にする
- off..... 統計機能を無効にする

[説明] 各種統計機能を有効にするか否かを設定する。

[ノート] off にするとそれ以前の統計情報はクリアされる。
当該ページにアクセスしても、統計情報を閲覧することはできない。

[初期値] off

[適用モデル]

~~RTX3000~~	~~RTX2000~~	~~RTX1500~~	RTX1200	~~RTX1100~~	~~RTX1000~~	~~RT300i~~	~~RT250i~~	~~RT107e~~	SRT100

本書は大豆油インクで印刷しています。
本書は無塩素紙(ECF:無塩素紙漂白パルプ)を使用しています。

WQ86290 0809 第13版CP