

コマンドリファレンス

Rev.8.02.53, Rev.8.03.94, Rev.9.00.60
Rev.10.00.61, Rev.10.01.76, Rev.11.01.33
Rev.14.00.33, Rev.14.01.41, Rev.15.02.25
Rev.15.04.04

目次

序文：はじめに.....	26
第 1 章：コマンドリファレンスの見方.....	27
1.1 対応するプログラムのリビジョン.....	27
1.2 コマンドリファレンスの見方.....	27
1.3 インタフェース名について.....	27
1.4 no で始まるコマンドの入力形式について.....	28
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.....	28
1.6 相手先情報番号のモデルによる違いについて.....	28
1.7 工場出荷設定値について.....	29
1.8 拡張ライセンスについて.....	29
第 2 章：コマンドの使い方.....	31
2.1 コンソールについて.....	31
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.....	35
2.1.4 リモートセットアップ.....	36
2.2 SSH サーバーについて.....	37
2.2.1 SSH サーバー機能の使用に当たっての注意事項.....	37
2.2.2 SSH サーバーの設定.....	37
2.3 TFTP について.....	38
2.3.1 TFTP による設定手順.....	38
2.3.2 設定ファイルの読み出し.....	39
2.3.3 設定ファイルの書き込み.....	39
2.4 コンソール使用時のキーボード操作について.....	40
2.5 「show」で始まるコマンド.....	41
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.....	41
2.5.2 show コマンドの表示内容を見やすくする.....	43
2.5.3 外部メモリへのリダイレクト機能.....	43
第 3 章：ヘルプ.....	45
3.1 コンソールに対する簡易説明の表示.....	45
3.2 コマンド一覧の表示.....	45
第 4 章：機器の設定.....	46
4.1 ログインパスワードの設定.....	46
4.2 ログインパスワードの暗号化保存.....	46
4.3 管理パスワードの設定.....	46
4.4 管理パスワードの暗号化保存.....	46
4.5 一般ユーザ名とログインパスワードの設定.....	47
4.6 ログイン時のパスワード認証に RADIUS を使用するか否かの設定.....	47
4.7 管理ユーザーへの移行時のパスワード認証に RADIUS を使用するか否かの設定.....	48
4.8 拡張ライセンスの操作.....	48
4.8.1 拡張ライセンスのパスワードの設定.....	48
4.8.2 拡張ライセンスのインポート.....	49
4.8.3 拡張ライセンスの削除.....	49
4.9 ユーザーの属性を設定.....	49
4.10 他のユーザの接続の強制切断.....	52
4.11 セキュリティクラスの設定.....	53
4.12 タイムゾーンの設定.....	54

4.13 現在の日付けの設定.....	54
4.14 現在の時刻の設定.....	54
4.15 リモートホストによる時計の設定.....	55
4.16 NTP による時計の設定.....	55
4.17 NTP パケットを送信するときの始点 IP アドレスの設定.....	56
4.18 Stratum 0 の NTP サーバーとの時刻同期を許可する設定.....	56
4.19 コンソールのプロンプト表示の設定.....	57
4.20 コンソールの言語とコードの設定.....	57
4.21 コンソールの表示文字数の設定.....	58
4.22 コンソールの表示行数の設定.....	58
4.23 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.....	59
4.24 SYSLOG を受けるホストの IP アドレスの設定.....	59
4.25 SYSLOG ファシリティの設定.....	59
4.26 NOTICE タイプの SYSLOG を出力するか否かの設定.....	60
4.27 INFO タイプの SYSLOG 出力の設定.....	60
4.28 DEBUG タイプの SYSLOG を出力するか否かの設定.....	61
4.29 SYSLOG を送信する時の始点 IP アドレスの設定.....	61
4.30 SYSLOG パケットの始点ポート番号の設定.....	61
4.31 SYSLOG に実行コマンドを出力するか否かの設定.....	62
4.32 インタフェースパケットのダンプを SYSLOG へ出力するか否かの設定.....	62
4.33 TELNET サーバー機能の ON/OFF の設定.....	63
4.34 TELNET サーバー機能の listen ポートの設定.....	63
4.35 TELNET サーバーへアクセスできるホストの設定.....	64
4.36 TELNET サーバーへ同時に接続できるユーザ数の設定.....	65
4.37 マスタクロック用インタフェースの設定.....	65
4.38 CPU 使用率の閾値の設定.....	66
4.39 メモリ使用率の閾値の設定.....	66
4.40 温度監視の閾値の設定.....	66
4.41 ファストパス機能の設定.....	67
4.42 LAN インタフェースの動作設定.....	67
4.43 HUB IC での受信オーバーフロー数を取得するか否かの設定.....	68
4.44 LAN インタフェースのリンクアップ後の送信抑制時間の設定.....	68
4.45 ポートミラーリング機能の設定.....	69
4.46 LAN インタフェースの動作タイプの設定.....	70
4.47 スタティックリンクアグリゲーションの設定.....	75
4.48 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.....	76
4.49 ログインタイマの設定.....	77
4.50 TFTP によりアクセスできるホストの設定.....	78
4.51 Magic Packet を LAN に中継するか否かの設定.....	78
4.52 インタフェースまたはシステムの説明の設定.....	79
4.53 TCP のコネクションレベルの syslog を出力するか否かの設定.....	80
4.54 HTTP リビジョンアップ実行を許可するか否かの設定.....	83
4.55 HTTP リビジョンアップ用 URL の設定.....	83
4.56 HTTP リビジョンアップ用 Proxy サーバーの設定.....	83
4.57 HTTP リビジョンアップ処理のタイムアウトの設定.....	84
4.58 リビジョンダウンを許可するか否かの設定.....	84
4.59 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.....	85
4.60 リビジョンアップ実行のスケジュール.....	85
4.61 SSH サーバー機能の ON/OFF の設定.....	86
4.62 SSH サーバー機能の listen ポートの設定.....	87
4.63 SSH サーバーへアクセスできるホストの設定.....	87
4.64 SSH サーバーへ同時に接続できるユーザ数の設定.....	88
4.65 SSH サーバーホスト鍵の設定.....	88
4.66 SSH サーバーホスト鍵の表示.....	89
4.67 SSH サーバーで利用可能な暗号アルゴリズムの設定.....	90
4.68 SSH クライアントの生存確認.....	90
4.69 SSH サーバー応答に含まれる OpenSSH のバージョン情報の非表示設定.....	91
4.70 SSH サーバーで利用可能な認証方式の設定.....	91
4.71 SSH サーバーの公開鍵認証に用いる公開鍵情報を保存するファイルの設定.....	92
4.72 SSH サーバーの公開鍵認証に用いる公開鍵の設定.....	93
4.73 SSH サーバーの公開鍵認証に用いる公開鍵の表示.....	94

4.74 SFTP サーバーへアクセスできるホストの設定.....	95
4.75 SSH クライアント.....	96
4.76 SCP クライアント.....	97
4.77 SSH クライアントで利用可能な暗号アルゴリズムの設定.....	97
4.78 SSH サーバーの公開鍵情報を保存するファイルの設定.....	98
4.79 パケットバッファのパラメータを変更する.....	98
4.80 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.....	100
4.81 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.....	101
4.82 microSD 機能に関連するアラームを鳴らすか否かの設定.....	101
4.83 バッチファイル実行機能に関連するアラーム音を鳴らすか否かの設定.....	101
4.84 起動時のアラーム音を鳴らすか否かの設定.....	102
4.85 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.....	102
4.86 LED の輝度を調整する.....	102
4.87 環境変数の設定.....	103
4.88 エイリアスの設定.....	103
4.89 マクロの設定.....	104
4.90 EMFS ファイルの作成、削除.....	105
4.91 CPU スケジューリング方式の設定.....	106
4.92 CPU スケジューリングフィルターの設定.....	107
4.93 CPU スケジューリングフィルターの適用.....	109

第 5 章 : ヤマハルーター用ファイルシステム RTFS.....111

5.1 RTFS のフォーマット.....	111
5.2 RTFS のガベージコレクション.....	111

第 6 章 : ISDN 関連の設定.....112

6.1 共通の設定.....	112
6.1.1 BRI 回線の種類の指定.....	112
6.1.2 自分の ISDN 番号の設定.....	112
6.1.3 内蔵 DSU 使用の可否の設定.....	113
6.1.4 終端抵抗の設定.....	113
6.1.5 PP で使用するインタフェースの設定.....	114
6.1.6 課金額による発信制限の設定.....	114
6.1.7 PIAFS の着信を許可するか否かの設定.....	115
6.1.8 PIAFS 接続時の起動側の指定.....	115
6.1.9 PIAFS の発信方式の設定.....	116
6.1.10 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.....	117
6.2 相手側の設定.....	117
6.2.1 常時接続の設定.....	117
6.2.2 相手 ISDN 番号の設定.....	118
6.2.3 自動接続の設定.....	119
6.2.4 相手への発信順序の設定.....	119
6.2.5 着信許可の設定.....	119
6.2.6 発信許可の設定.....	120
6.2.7 再発信抑制タイマの設定.....	120
6.2.8 エラー切断後の再発信禁止タイマの設定.....	121
6.2.9 相手にコールバック要求を行うか否かの設定.....	121
6.2.10 相手からのコールバック要求に応じるか否かの設定.....	122
6.2.11 コールバック要求タイプの設定.....	122
6.2.12 コールバック受け入れタイプの設定.....	122
6.2.13 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.....	123
6.2.14 コールバックタイマの設定.....	123
6.2.15 コールバック待機タイマの設定.....	124
6.2.16 ISDN 回線を切断するタイマ方式の指定.....	124
6.2.17 切断タイマの設定 (ノーマル).....	124
6.2.18 切断タイマの設定 (ファスト).....	125
6.2.19 切断タイマの設定 (強制).....	125
6.2.20 入力切断タイマの設定 (ノーマル).....	126
6.2.21 出力切断タイマの設定 (ノーマル).....	126

6.2.22 課金単位時間方式での課金単位時間と監視時間の設定.....	127
--------------------------------------	-----

第 7 章 : フレームリレー関連の設定.....	129
7.1 カプセル化の種類の設定.....	129
7.2 DLCI の設定.....	130
7.3 DLCI ごとのパラメータの設定.....	130
7.4 PVC 状態確認手順の設定.....	131
7.5 InARP 使用の設定.....	131
7.6 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.....	132
7.7 FR 圧縮機能の設定.....	132
7.8 輻輳制御をするか否かの設定.....	133
7.9 回線に対する送信順序方式の設定.....	133
7.10 指定パケットに DE ビットを立てるか否かの設定.....	134
第 8 章 : PRI 関連の設定.....	135
8.1 PRI 回線の種類の設定.....	136
8.2 情報チャンネルとタイムスロットの設定.....	136
8.3 PP で使用するインタフェースの設定.....	137
第 9 章 : IP の設定.....	138
9.1 インタフェース共通の設定.....	138
9.1.1 IP パケットを扱うか否かの設定.....	138
9.1.2 IP アドレスの設定.....	138
9.1.3 セカンダリ IP アドレスの設定.....	139
9.1.4 インタフェースの MTU の設定.....	140
9.1.5 同一インタフェースに折り返すパケットを送信するか否かの設定.....	141
9.1.6 echo,discard,time サービスを動作させるか否かの設定.....	141
9.1.7 IP の静的経路情報の設定.....	142
9.1.8 DHCP で IP アドレスを取得したときにデフォルト経路を自動的に追加するか否かを設定.....	144
9.1.9 DHCP で IP アドレスを取得したときに implicit 経路を自動的に追加するか否かを設定.....	145
9.1.10 IP パケットのフィルタの設定.....	145
9.1.11 フィルタセットの定義.....	149
9.1.12 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.....	149
9.1.13 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.....	150
9.1.14 動的フィルタの定義.....	150
9.1.15 動的フィルタのタイムアウトの設定.....	152
9.1.16 FQDN フィルタで使用するキャッシュのタイマーの設定.....	153
9.1.17 侵入検知機能の動作の設定.....	153
9.1.18 1 秒間に侵入検知情報を通知する頻度の設定.....	155
9.1.19 重複する侵入検知情報の通知抑制の設定.....	155
9.1.20 侵入検知情報の最大表示件数の設定.....	156
9.1.21 侵入検知で用いる閾値の設定.....	156
9.1.22 TCP セッションの MSS 制限の設定.....	157
9.1.23 TCP ウィンドウ・スケール・オプションを変更する.....	158
9.1.24 ルーターが端点となる TCP のセッション数の設定.....	158
9.1.25 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.....	159
9.1.26 フィルタリングによるセキュリティーの設定.....	159
9.1.27 ルールに一致する IP パケットの DF ビットを 0 に書き換えるか否かの設定.....	161
9.1.28 IP パケットの TOS フィールドの書き換えの設定.....	161
9.1.29 代理 ARP の設定.....	162
9.1.30 ARP エントリの寿命の設定.....	163
9.1.31 静的 ARP エントリの設定.....	163
9.1.32 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.....	164
9.1.33 ARP エントリの変化をログに残すか否かの設定.....	165
9.1.34 implicit 経路の優先度の設定.....	165
9.1.35 フローテーブルの各エントリの寿命を設定する.....	166
9.1.36 フローテーブルのエントリー数の設定.....	166
9.1.37 フラグメントパケットを再構成するために保持しておく時間を設定.....	167

9.2 PP 側の設定.....	167
9.2.1 PP 側 IP アドレスの設定.....	167
9.2.2 リモート IP アドレスプールの設定.....	168
9.2.3 PP 経由のキープアライブの時間間隔の設定.....	169
9.2.4 PP 経由のキープアライブを使用するか否かの設定.....	170
9.2.5 PP 経由のキープアライブのログをとるか否かの設定.....	171
9.2.6 専用線ダウン検出時の動作の設定.....	172
9.3 RIP の設定.....	172
9.3.1 RIP を使用するか否かの設定.....	172
9.3.2 RIP に関して信用できるゲートウェイの設定.....	172
9.3.3 RIP による経路の優先度の設定.....	173
9.3.4 RIP パケットの送信に関する設定.....	174
9.3.5 RIP パケットの受信に関する設定.....	174
9.3.6 RIP のフィルタリングの設定.....	175
9.3.7 RIP で加算するホップ数の設定.....	176
9.3.8 RIP2 での認証の設定.....	176
9.3.9 RIP2 での認証キーの設定.....	177
9.3.10 RIP2 での広告動作モードの設定.....	177
9.3.11 回線切断時の経路保持の設定.....	178
9.3.12 回線接続時の PP 側の RIP の動作の設定.....	178
9.3.13 回線接続時の PP 側の RIP 送出の時間間隔の設定.....	179
9.3.14 回線切断時の PP 側の RIP の動作の設定.....	179
9.3.15 回線切断時の PP 側の RIP 送出の時間間隔の設定.....	180
9.3.16 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.....	180
9.3.17 RIP で強制的に経路を広告する.....	181
9.3.18 RIP2 でのフィルタの比較方法.....	182
9.3.19 RIP のタイマーを調整する.....	182
9.4 VRRP の設定.....	183
9.4.1 インタフェース毎の VRRP の設定.....	183
9.4.2 シャットダウントリガの設定.....	184
9.5 バックアップの設定.....	186
9.5.1 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.....	186
9.5.2 バックアップからの復帰待ち時間の設定.....	187
9.5.3 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.....	187
9.5.4 バックアップからの復帰待ち時間の設定.....	188
9.5.5 LAN 経由のキープアライブを使用するか否かの設定.....	189
9.5.6 LAN 経由のキープアライブの時間間隔の設定.....	189
9.5.7 LAN 経由のキープアライブのログをとるか否かの設定.....	190
9.5.8 ネットワーク監視機能の設定.....	190
9.6 IGMP の設定.....	193
9.6.1 インタフェースごとの IGMP の設定.....	193
9.6.2 静的な IGMP の設定.....	194
9.7 PIM-SM の設定.....	194
9.7.1 インタフェースごとの PIM-SM の設定.....	194
9.7.2 静的な RP のグループの設定.....	195
9.7.3 PIM-SM に関する詳細なログ出力の設定.....	196
9.7.4 register の checksum 計算方法の設定.....	196
9.7.5 PIM JOIN/PRUNE メッセージの宛先の設定.....	197
9.7.6 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.....	197
9.8 受信パケット統計情報の設定.....	197
9.8.1 受信パケットの統計情報を記録するか否かの設定.....	197
9.8.2 受信したパケットの統計情報のクリア.....	198
9.8.3 受信したパケットの統計情報の表示.....	199
9.8.4 統計情報を記録する受信パケットの分類数の設定.....	199
9.9 パケット転送フィルターの設定.....	200
9.9.1 パケット転送フィルターの定義.....	200
9.9.2 インタフェースへのパケット転送フィルターの適用.....	201

第 10 章 : イーサネットフィルタの設定.....202

10.1 フィルタ定義の設定.....	202
---------------------	-----

10.2 インタフェースへの適用の設定.....	204
10.3 イーサネットフィルタの状態の表示.....	205
第 11 章 : 入力遮断フィルタの設定.....	206
11.1 フィルタ定義の設定.....	206
11.2 適用の設定.....	208
第 12 章 : ポリシーフィルタの設定.....	210
12.1 サービスの定義.....	210
12.2 インタフェースグループの定義.....	210
12.3 アドレスグループの定義.....	211
12.4 サービスグループの定義.....	212
12.5 ポリシーフィルタの定義.....	213
12.6 ポリシーセットの定義.....	215
12.7 ポリシーセットの有効化.....	215
12.8 ポリシーセットの自動切り替え.....	216
12.9 タイマーの設定.....	217
第 13 章 : URL フィルタの設定.....	219
13.1 フィルタ定義の設定.....	219
13.2 URL フィルタのインタフェースへの適用.....	220
13.3 URL フィルタでチェックを行う HTTP のポート番号の設定.....	220
13.4 URL フィルターを使用するか否かの設定.....	221
13.5 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.....	221
13.6 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.....	222
13.7 利用するデータベースの選択.....	222
13.8 データベースを持つサーバーアドレスの設定.....	223
13.9 Proxy サーバーの設定.....	224
13.10 チェックするカテゴリーの設定.....	224
13.11 Web レピュテーションによるフィルタの設定.....	225
13.12 外部データベースへのアクセスに失敗したときにパケットを破棄するか否かの設定.....	226
13.13 URL フィルター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.....	227
13.14 IP アドレスを直接指定した URL へのアクセスを許可するか否かの設定.....	227
13.15 指定した拡張子の URL を評価するか否かの設定.....	228
13.16 評価しない URL の拡張子の設定.....	228
13.17 フィルターにマッチした際にログを出力するか否かの設定.....	229
13.18 シリアル ID を登録する URL の設定.....	230
13.19 データベースへアクセスするためのシリアル ID の設定.....	230
13.20 URL フィルタリングサービス事業者にシリアル ID の登録.....	230
13.21 URL フィルタリングサービス事業者との契約状況の確認.....	231
13.22 データベース情報の更新.....	232
13.23 ユーザー認証に失敗した場合の再送間隔と回数の設定.....	232
第 14 章 : PPP の設定.....	234
14.1 相手の名前とパスワードの設定.....	234
14.2 受け入れる認証タイプの設定.....	235
14.3 要求する認証タイプの設定.....	235
14.4 自分の名前とパスワードの設定.....	236
14.5 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.....	237
14.6 LCP 関連の設定.....	237
14.6.1 Address and Control Field Compression オプション使用の設定.....	237
14.6.2 Magic Number オプション使用の設定.....	238
14.6.3 Maximum Receive Unit オプション使用の設定.....	238
14.6.4 Protocol Field Compression オプション使用の設定.....	239
14.6.5 lcp-restart パラメータの設定.....	239
14.6.6 lcp-max-terminate パラメータの設定.....	239
14.6.7 lcp-max-configure パラメータの設定.....	240

14.6.8 lcp-max-failure パラメータの設定	240
14.6.9 Configure-Request をすぐに送信するか否かの設定	240
14.7 PAP 関連の設定	241
14.7.1 pap-restart パラメータの設定	241
14.7.2 pap-max-authreq パラメータの設定	241
14.8 CHAP 関連の設定	241
14.8.1 chap-restart パラメータの設定	241
14.8.2 chap-max-challenge パラメータの設定	241
14.9 IPCP 関連の設定	242
14.9.1 Van Jacobson Compressed TCP/IP 使用の設定	242
14.9.2 PP 側 IP アドレスのネゴシエーションの設定	242
14.9.3 ipcp-restart パラメータの設定	243
14.9.4 ipcp-max-terminate パラメータの設定	243
14.9.5 ipcp-max-configure パラメータの設定	243
14.9.6 ipcp-max-failure パラメータの設定	243
14.9.7 WINS サーバーの IP アドレスの設定	244
14.9.8 IPCP の MS 拡張オプションを使うか否かの設定	244
14.9.9 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	245
14.10 MSCBCP 関連の設定	245
14.10.1 mscbcpr-restart パラメータの設定	245
14.10.2 mscbcpr-maxretry パラメータの設定	245
14.11 CCP 関連の設定	246
14.11.1 全パケットの圧縮タイプの設定	246
14.11.2 ccp-restart パラメータの設定	246
14.11.3 ccp-max-terminate パラメータの設定	247
14.11.4 ccp-max-configure パラメータの設定	247
14.11.5 ccp-max-failure パラメータの設定	247
14.12 IPV6CP 関連の設定	248
14.12.1 IPV6CP を使用するか否かの設定	248
14.13 MP 関連の設定	248
14.13.1 MP を使用するか否かの設定	248
14.13.2 MP の制御方法の設定	248
14.13.3 MP のための負荷閾値の設定	249
14.13.4 MP の最大リンク数の設定	249
14.13.5 MP の最小リンク数の設定	250
14.13.6 MP のための負荷計測間隔の設定	250
14.13.7 MP のパケットを分割するか否かの設定	250
14.14 BACP 関連の設定	251
14.14.1 bacp-restart パラメータの設定	251
14.14.2 bacp-max-terminate パラメータの設定	251
14.14.3 bacp-max-configure パラメータの設定	251
14.14.4 bacp-max-failure パラメータの設定	251
14.15 BAP 関連の設定	252
14.15.1 bap-restart パラメータの設定	252
14.15.2 bap-max-retry パラメータの設定	252
14.16 PPPoE 関連の設定	252
14.16.1 PPPoE で使用する LAN インタフェースの指定	252
14.16.2 アクセスコンセントレータ名の設定	253
14.16.3 セッションの自動接続の設定	253
14.16.4 セッションの自動切断の設定	253
14.16.5 PADI パケットの最大再送回数の設定	254
14.16.6 PADI パケットの再送時間の設定	254
14.16.7 PADR パケットの最大再送回数の設定	254
14.16.8 PADR パケットの再送時間の設定	254
14.16.9 PPPoE セッションの切断タイマの設定	255
14.16.10 サービス名の指定	255
14.16.11 TCP パケットの MSS の制限の有無とサイズの指定	255
14.16.12 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	256
14.16.13 PPPoE フレームを中継するインターフェースの指定	256

第 15 章 : DHCP の設定	258
15.1 DHCP サーバー・リレーエージェント機能.....	258
15.1.1 DHCP の動作の設定.....	258
15.1.2 RFC2131 対応動作の設定.....	259
15.1.3 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.....	260
15.1.4 DHCP スコープの定義.....	261
15.1.5 DHCP 予約アドレスの設定.....	262
15.1.6 DHCP アドレス割り当て動作の設定.....	264
15.1.7 DHCP 割り当て情報を元にした予約設定の生成.....	265
15.1.8 DHCP オプションの設定.....	266
15.1.9 DHCP リース情報の手動追加.....	267
15.1.10 DHCP リース情報の手動削除.....	268
15.1.11 DHCP サーバーの指定の設定.....	268
15.1.12 DHCP リレーエージェント機能で使用する始点ポート番号の設定.....	269
15.1.13 DHCP サーバーの選択方法の設定.....	269
15.1.14 DHCP BOOTREQUEST パケットの中継基準の設定.....	269
15.1.15 インターフェース毎の DHCP の動作の設定.....	270
15.2 DHCP クライアント機能.....	270
15.2.1 DHCP クライアントのホスト名の設定.....	271
15.2.2 要求する IP アドレスリース期間の設定.....	272
15.2.3 IP アドレス取得要求の再送回数と間隔の設定.....	272
15.2.4 DHCP クライアント ID オプションの設定.....	273
15.2.5 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.....	274
15.2.6 リンクダウンした時に情報を解放するか否かの設定.....	275
第 16 章 : ICMP の設定	277
16.1 IPv4 の設定.....	277
16.1.1 ICMP Echo Reply を送信するか否かの設定.....	277
16.1.2 ICMP Echo Reply をリンクダウン時に送信するか否かの設定.....	277
16.1.3 ICMP Mask Reply を送信するか否かの設定.....	277
16.1.4 ICMP Parameter Problem を送信するか否かの設定.....	278
16.1.5 ICMP Redirect を送信するか否かの設定.....	278
16.1.6 ICMP Redirect 受信時の処理の設定.....	279
16.1.7 ICMP Time Exceeded を送信するか否かの設定.....	279
16.1.8 ICMP Timestamp Reply を送信するか否かの設定.....	280
16.1.9 ICMP Destination Unreachable を送信するか否かの設定.....	280
16.1.10 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.....	281
16.1.11 受信した ICMP のログを記録するか否かの設定.....	281
16.1.12 ステルス機能の設定.....	282
16.1.13 ARP による MTU 探索を行うか否かの設定.....	282
16.1.14 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.....	283
16.2 IPv6 の設定.....	283
16.2.1 ICMP Echo Reply を送信するか否かの設定.....	283
16.2.2 ICMP Echo Reply をリンクダウン時に送信するか否かの設定.....	284
16.2.3 ICMP Parameter Problem を送信するか否かの設定.....	284
16.2.4 ICMP Redirect を送信するか否かの設定.....	284
16.2.5 ICMP Redirect 受信時の処理の設定.....	285
16.2.6 ICMP Time Exceeded を送信するか否かの設定.....	285
16.2.7 ICMP Destination Unreachable を送信するか否かの設定.....	286
16.2.8 受信した ICMP のログを記録するか否かの設定.....	286
16.2.9 ICMP Packet-Too-Big を送信するか否かの設定.....	287
16.2.10 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.....	287
16.2.11 ステルス機能の設定.....	288
16.2.12 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.....	288
第 17 章 : トンネリング	290

17.1	トンネルインターフェースの使用許可の設定	290
17.2	トンネルインターフェースの使用不許可の設定	290
17.3	トンネルインターフェースの接続種別の設定	291
17.4	トンネルインターフェースの種別の設定	292
17.5	トンネルインターフェースの IPv4 アドレスの設定	292
17.6	トンネルインターフェースの相手側の IPv4 アドレスの設定	293
17.7	相手側トンネルインターフェースの端点 IP アドレスの設定	293
17.8	自分側トンネルインターフェースの端点 IP アドレスの設定	294
17.9	トンネルインターフェースの端点 IP アドレスの設定	294
17.10	トンネルの端点の名前の設定	295
17.11	マルチポイントトンネルのサーバーの設定	295
17.12	マルチポイントトンネルで使用する自分の名前の設定	296
17.13	マルチポイントトンネルで接続する相手の最大数の設定	296
17.14	トンネルインターフェースの MAP-E 種別の設定	297
17.15	トンネルインターフェースの変換種別の設定	297

第 18 章 : IPsec の設定.....299

18.1	IPsec の動作の設定	300
18.2	IKE バージョンの設定	300
18.3	IKE の認証方式の設定	301
18.4	事前共有鍵の登録	302
18.5	IKEv2 の認証に使用する PKI ファイルの設定	303
18.6	EAP-MD5 認証で使用する自分の名前とパスワードの設定	303
18.7	EAP-MD5 によるユーザ認証の設定	304
18.8	EAP-MD5 認証で証明書要求ペイロードを送信するか否かの設定	305
18.9	IKE の鍵交換を始動するか否かの設定	305
18.10	設定が異なる場合に鍵交換を拒否するか否かの設定	306
18.11	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	307
18.12	鍵交換の再送回数と間隔の設定	307
18.13	相手側のセキュリティ・ゲートウェイの名前の設定	308
18.14	相手側セキュリティ・ゲートウェイの IP アドレスの設定	309
18.15	相手側の ID の設定	310
18.16	自分側のセキュリティ・ゲートウェイの名前の設定	311
18.17	自分側セキュリティ・ゲートウェイの IP アドレスの設定	312
18.18	自分側の ID の設定	313
18.19	IKE キープアライブ機能の設定	313
18.20	IKE キープアライブに関する SYSLOG を出力するか否かの設定	315
18.21	IKE が用いる暗号アルゴリズムの設定	316
18.22	受信した IKE パケットを蓄積するキューの長さの設定	317
18.23	IKE が用いるグループの設定	318
18.24	IKE が用いるハッシュアルゴリズムの設定	319
18.25	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	319
18.26	IKE ペイロードのタイプの設定	320
18.27	IKEv1 鍵交換タイプの設定	321
18.28	IKE の情報ペイロードを送信するか否かの設定	322
18.29	PFS を用いるか否かの設定	322
18.30	XAUTH の設定	323
18.31	XAUTH 認証、EAP-MD5 認証に使用するユーザ ID の設定	323
18.32	XAUTH 認証、EAP-MD5 認証に使用するユーザ ID の属性の設定	324
18.33	XAUTH 認証、EAP-MD5 認証に使用するユーザグループの設定	325
18.34	XAUTH 認証、EAP-MD5 認証に使用するユーザグループの属性の設定	326
18.35	XAUTH によるユーザ認証の設定	327
18.36	内部 IP アドレスプールの設定	328
18.37	IKE XAUTH Mode-Cfg メソッドの設定	328
18.38	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	329
18.39	VPN クライアントの同時接続制限ライセンスの登録	330
18.40	VPN クライアントの同時接続制限ライセンスの適用	331
18.41	IKE のログの種類の設定	332
18.42	ESP を UDP でカプセル化して送受信するか否かの設定	332
18.43	折衝パラメーターを制限するか否かの設定	333

18.44 IKE のメッセージ ID 管理の設定.....	334
18.45 CHILD SA 作成方法の設定.....	335
18.46 鍵交換の始動パケットを受信するか否かの設定.....	335
18.47 SA 関連の設定.....	336
18.47.1 SA の寿命の設定.....	336
18.47.2 SA のポリシーの定義.....	337
18.47.3 SA の手動更新.....	339
18.47.4 ダングリング SA の動作の設定.....	340
18.47.5 IPsec NAT トラバーサルを利用するための設定.....	341
18.47.6 SA の削除.....	342
18.48 トンネルインタフェース関連の設定.....	343
18.48.1 IPsec トンネルの外側の IPv4 パケットに対するフラグメントの設定.....	343
18.48.2 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.....	343
18.48.3 使用する SA のポリシーの設定.....	344
18.48.4 IPComp によるデータ圧縮の設定.....	344
18.48.5 トンネルバックアップの設定.....	345
18.48.6 トンネルテンプレートの設定.....	346
18.49 トランスポートモード関連の設定.....	348
18.49.1 トランスポートモードの定義.....	348
18.49.2 トランスポートモードのテンプレートの設定.....	349
18.50 PKI 関連の設定.....	350
18.50.1 証明書ファイルの設定.....	350
18.50.2 CRL ファイルの設定.....	351
第 19 章 : L2TP 機能の設定.....	352
19.1 L2TP を動作させるか否かの設定.....	352
19.2 L2TP トンネル認証に関する設定.....	353
19.3 L2TP トンネルの切断タイマの設定.....	353
19.4 L2TP キープアライブの設定.....	354
19.5 L2TP キープアライブのログ設定.....	355
19.6 L2TP のコネクション制御の syslog を出力するか否かの設定.....	355
19.7 L2TPv3 の常時接続の設定.....	356
19.8 L2TP トンネルのホスト名の設定.....	356
19.9 L2TPv3 の Local Router ID の設定.....	357
19.10 L2TPv3 の Remote Router ID の設定.....	357
19.11 L2TPv3 の Remote End ID の設定.....	358
第 20 章 : PPTP 機能の設定.....	359
20.1 共通の設定.....	359
20.1.1 PPTP サーバーを動作させるか否かの設定.....	359
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.....	359
20.1.3 PPTP の動作タイプの設定.....	360
20.1.4 PPTP ホスト名の設定.....	360
20.1.5 PPTP ホスト名の設定.....	361
20.1.6 PPTP パケットのウィンドウサイズの設定.....	361
20.1.7 PPTP の動作モードの設定.....	361
20.1.8 PPTP 暗号鍵生成のための要求する認証方式の設定.....	362
20.1.9 PPTP 暗号鍵生成のための受け入れ可能な認証方式の設定.....	362
20.1.10 PPTP のコネクション制御の syslog を出力するか否かの設定.....	363
20.2 リモートアクセス VPN 機能.....	363
20.2.1 PPTP トンネルの出力切断タイマの設定.....	363
20.2.2 PPTP キープアライブの設定.....	363
20.2.3 PPTP キープアライブのログ設定.....	364
20.2.4 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.....	364
20.2.5 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.....	365
第 21 章 : IPIP トンネリング機能の設定.....	366
21.1 IPIP キープアライブの設定.....	366

21.2 IPIP キープアライブのログ設定.....	366
第 22 章 : クラウドサービスとの VPN 接続設定機能の設定.....	368
22.1 VPN 接続するクラウドサービスの指定.....	368
22.2 クラウドサービスとの VPN 接続設定に必要なパラメーターの設定.....	368
22.3 クラウドサービスとの VPN 接続設定の名称の設定.....	369
22.4 クラウドサービスとの VPN 接続を設定するトンネルインターフェースの指定.....	369
22.5 クラウドサービスとの VPN 接続設定に使用するオプションの設定.....	370
22.6 クラウドサービスとの VPN 接続設定の手動実行.....	370
22.7 クラウドサービスとの VPN 接続設定の状態の表示.....	371
22.8 クラウドサービス接続時の詳細情報を SYSLOG に表示.....	372
第 23 章 : SIP 機能の設定.....	373
23.1 共通の設定.....	373
23.1.1 SIP を使用するか否かの設定.....	373
23.1.2 SIP の session-timer 機能のタイマ値の設定.....	373
23.1.3 SIP による発信時に使用する IP プロトコルの選択.....	374
23.1.4 SIP による発信時に 100rel をサポートするか否かの設定.....	374
23.1.5 送信する SIP パケットに User-Agent ヘッダを付加する設定.....	375
23.1.6 SIP による着信時の INVITE に refresher 指定がない場合の設定.....	375
23.1.7 SIP による着信時に P-N-UAType ヘッダをサポートするか否かの設定.....	376
23.1.8 SIP による着信時のセッションタイマーのリクエストを設定.....	376
23.1.9 SIP 着信時にユーザー名を検証するか否かの設定.....	377
23.1.10 着信可能なポートがない場合に返す SIP のレスポンスコードの設定.....	377
23.1.11 SIP で使用する IP アドレスの設定.....	378
23.1.12 SIP メッセージのログを記録するか否かの設定.....	378
23.2 SIP サーバー毎の設定.....	378
23.2.1 SIP サーバーの設定.....	378
23.2.2 SIP サーバー毎の session-timer 機能のタイマ値の設定.....	379
23.2.3 SIP サーバー毎の代表 SIP アドレスの設定.....	380
23.2.4 SIP サーバー毎の先頭に付加された 184/186 の扱いの設定.....	380
23.2.5 SIP サーバー毎の発信時に使用する自己 SIP ディスプレイ名の設定.....	381
23.2.6 SIP サーバー毎の発信時の相手 SIP アドレスのドメイン名の設定.....	382
23.2.7 SIP サーバー毎の発信時に 100rel をサポートするか否かの設定.....	382
23.2.8 SIP サーバー毎の REGISTER リクエストの更新間隔の設定.....	383
23.2.9 SIP サーバー毎の REGISTER リクエストの Request-URI の設定.....	383
23.2.10 SIP サーバー毎の REGISTER リクエストの Contact ヘッダに付加する q 値の設定.....	384
23.2.11 SIP サーバへの発信に番号以外を使えないように制限する設定.....	384
23.2.12 自分自身の SIP アドレスへの発信を許可するかどうかの設定.....	385
23.3 NGN 機能の設定.....	385
23.3.1 NGN 網に接続するインタフェースの設定.....	385
23.3.2 NGN 網を介したトンネルインタフェースの切断タイマの設定.....	386
23.3.3 NGN 網を介したトンネルインタフェースの帯域幅の設定.....	386
23.3.4 NGN 網を介したトンネルインタフェースの着信許可の設定.....	387
23.3.5 NGN 網を介したトンネルインタフェースの発信許可の設定.....	388
23.3.6 NGN 網を介したトンネルインタフェースで使用する LAN インタフェースの設定.....	388
23.3.7 NGN 網を介したトンネルインタフェースで接続に失敗した場合に接続を試みる相手番号 の設定.....	389
23.3.8 NGN 電話番号を RADIUS で認証するか否かの設定.....	389
23.3.9 NGN 電話番号を RADIUS で認証するとき使用するパスワードの設定.....	390
23.3.10 NGN 網への発信時に RADIUS アカウンティングを使用するか否かの設定.....	390
23.3.11 NGN 網からの着信時に RADIUS アカウンティングを使用するか否かの設定.....	390
23.3.12 NGN 網を介したリナンバリング発生時に LAN インタフェースを一時的にリンクダウ ンするか否かの設定.....	391
23.3.13 NGN 網接続情報の表示.....	392
第 24 章 : SNMP の設定.....	393
24.1 SNMPv1 によるアクセスを許可するホストの設定.....	393

24.2 SNMPv1 の読み出し専用のコミュニティ名の設定	394
24.3 SNMPv1 の読み書き可能なコミュニティ名の設定	394
24.4 SNMPv1 トラップの送信先の設定	394
24.5 SNMPv1 トラップのコミュニティ名の設定	395
24.6 SNMPv2c によるアクセスを許可するホストの設定	395
24.7 SNMPv2c の読み出し専用のコミュニティ名の設定	396
24.8 SNMPv2c の読み書き可能なコミュニティ名の設定	396
24.9 SNMPv2c トラップの送信先の設定	396
24.10 SNMPv2c トラップのコミュニティ名の設定	397
24.11 SNMPv3 エンジン ID の設定	397
24.12 SNMPv3 コンテキスト名の設定	398
24.13 SNMPv3 USM で管理するユーザの設定	398
24.14 SNMPv3 によるアクセスを許可するホストの設定	399
24.15 SNMPv3 VACM で管理する MIB ビューファミリの設定	399
24.16 SNMPv3 VACM で管理するアクセスポリシーの設定	400
24.17 SNMPv3 トラップの送信先の設定	401
24.18 SNMP 送信パケットの始点アドレスの設定	401
24.19 sysContact の設定	402
24.20 sysLocation の設定	402
24.21 sysName の設定	402
24.22 SNMP 標準トラップを送信するか否かの設定	403
24.23 CPU 使用率監視機能による SNMP トラップを送信するか否かの設定	403
24.24 メモリ使用率監視機能による SNMP トラップを送信するか否かの設定	404
24.25 SNMP トラップの送信の遅延時間の設定	404
24.26 SNMP の linkDown トラップの送信制御の設定	405
24.27 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	406
24.28 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	406
24.29 スイッチの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	407
24.30 PP インタフェースのアドレスの強制表示の設定	407
24.31 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	407
24.32 電波強度トラップを送信するか否かの設定	408
24.33 スイッチへ静的に付与するインタフェース番号の設定	408
24.34 スイッチへ静的に付与するスイッチ番号の設定	409
24.35 スイッチの状態による SNMP トラップの条件の設定	409
24.36 スイッチで共通の SNMP トラップの条件の設定	410

第 25 章 : RADIUS の設定.....412

25.1 RADIUS による認証を使用するか否かの設定	412
25.2 RADIUS によるアカウントを使用するか否かの設定	412
25.3 RADIUS サーバーの指定	413
25.4 RADIUS 認証サーバーの指定	413
25.5 RADIUS アカウントサーバーの指定	413
25.6 RADIUS 認証サーバーの UDP ポートの設定	414
25.7 RADIUS アカウントサーバーの UDP ポートの設定	414
25.8 RADIUS シークレットの設定	415
25.9 RADIUS 再送信パラメータの設定	415

第 26 章 : NAT 機能.....416

26.1 NAT 機能の動作タイプの設定	416
26.2 インタフェースへの NAT ディスクリプタ適用の設定	416
26.3 NAT ディスクリプタの動作タイプの設定	417
26.4 NAT 処理の外側 IP アドレスの設定	418
26.5 NAT 処理の内側 IP アドレスの設定	419
26.6 静的 NAT エントリの設定	419
26.7 IP マスカレード使用時に rlogin,rcp と ssh を使用するかどうかの設定	420
26.8 静的 IP マスカレードエントリの設定	420
26.9 NAT の IP アドレスマップの消去タイマの設定	421
26.10 IP マスカレードテーブルの TTL 処理方式の設定	422
26.11 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	423

26.12 IP マスカレードで利用するポートの範囲の設定.....	423
26.13 FTP として認識するポート番号の設定.....	424
26.14 IP マスカレードで変換しないポート番号の範囲の設定.....	425
26.15 NAT のアドレス割当をログに記録するか否かの設定.....	425
26.16 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.....	426
26.17 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.....	426
26.18 IP マスカレードで変換するホスト毎のセッション数の設定.....	427
26.19 IP マスカレードで変換する合計セッション数の設定.....	427
第 27 章 : DNS の設定.....	429
27.1 DNS を利用するか否かの設定.....	429
27.2 DNS サーバーの IP アドレスの設定.....	429
27.3 DNS ドメイン名の設定.....	430
27.4 DNS サーバーを通知してもらう相手先情報番号の設定.....	431
27.5 DNS サーバーアドレスを取得するインタフェースの設定.....	432
27.6 DHCP/DHCPv6/IPCP MS 拡張で DNS サーバーを通知する順序の設定.....	433
27.7 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.....	434
27.8 DNS サーバーへの AAAA レコードの問い合わせを制限するか否かの設定.....	434
27.9 SYSLOG 表示で DNS により名前解決するか否かの設定.....	435
27.10 DNS 問い合わせの内容に応じた DNS サーバーの選択.....	435
27.11 静的 DNS レコードの登録.....	438
27.12 DNS 問い合わせパケットの始点ポート番号の設定.....	439
27.13 DNS サーバーへアクセスできるホストの設定.....	439
27.14 DNS キャッシュを使用するか否かの設定.....	440
27.15 DNS キャッシュの最大エントリ数の設定.....	441
27.16 DNS フォールバック動作をルーター全体で統一するか否かの設定.....	441
第 28 章 : NAT46/DNS46 機能.....	443
28.1 NAT46 機能で使用する IPv4 アドレスプールの設定.....	443
28.2 NAT46 機能で使用する IPv6 プレフィックスの設定.....	443
28.3 NAT46 機能で使用する宛先アドレスを静的に対応づける設定.....	444
28.4 NAT46 エントリーの表示.....	444
第 29 章 : 優先制御／帯域制御.....	446
29.1 インタフェース速度の設定.....	446
29.2 クラス分けのためのフィルター設定.....	447
29.3 キューイングアルゴリズムタイプの選択.....	450
29.4 MP インタリーブの設定.....	451
29.5 クラス分けフィルタの適用.....	452
29.6 クラス毎のキュー長の設定.....	453
29.7 第 2 階層クラスのキュー長の設定.....	454
29.8 デフォルトクラスの設定.....	454
29.9 第 2 階層のデフォルトクラスの設定.....	455
29.10 クラスの属性の設定.....	455
29.11 動的なクラス変更 (Dynamic Class Control) の設定.....	457
第 30 章 : 連携機能.....	460
30.1 連携動作を行うか否かの設定.....	460
30.2 連携動作で使用するポート番号の設定.....	460
30.3 帯域測定で連携動作を行う相手毎の動作の設定.....	461
30.4 負荷監視通知で連携動作を行う相手毎の動作の設定.....	462
30.5 負荷監視サーバーとしての動作トリガの設定.....	464
30.6 負荷監視クライアントとしての動作の設定.....	465
30.7 連携動作の手動実行.....	466
第 31 章 : OSPF.....	468

31.1 OSPF の有効設定.....	468
31.2 OSPF の使用設定.....	468
31.3 OSPF による経路の優先度設定.....	468
31.4 OSPF のルーター ID 設定.....	469
31.5 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.....	470
31.6 外部プロトコルによる経路導入.....	470
31.7 OSPF で受け取った経路をどう扱うかのフィルタの設定.....	471
31.8 外部経路導入に適用するフィルタ定義.....	472
31.9 OSPF エリア設定.....	474
31.10 エリアへの経路広告.....	474
31.11 スタブ的接続の広告.....	475
31.12 仮想リンク設定.....	476
31.13 指定インタフェースの OSPF エリア設定.....	477
31.14 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.....	480
31.15 スタブが存在する時のネットワーク経路の扱いの設定.....	481
31.16 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.....	481
31.17 インタフェースの状態変化時、OSPF に外部経路を反映させる時間間隔の設定.....	482

第 32 章 : BGP.....483

32.1 BGP の起動の設定.....	483
32.2 経路の集約の設定.....	483
32.3 経路を集約するためのフィルタの設定.....	483
32.4 AS 番号の設定.....	484
32.5 ルーター ID の設定.....	485
32.6 BGP による経路の優先度の設定.....	485
32.7 BGP で受信した経路に対するフィルタの適用.....	486
32.8 BGP で受信する経路に適用するフィルタの設定.....	487
32.9 BGP に導入する経路に対するフィルタの適用.....	488
32.10 BGP の設定の有効化.....	488
32.11 BGP に導入する経路に適用するフィルタの設定.....	489
32.12 BGP による接続先の設定.....	490
32.13 BGP で使用する TCP MD5 認証の事前共有鍵の設定.....	491
32.14 BGP のログの設定.....	491
32.15 BGP で強制的に経路を広告する.....	492
32.16 インタフェースの状態変化時、BGP に外部経路を反映させる時間間隔の設定.....	492
32.17 BGP の最適経路選択における MED 属性が付加されていない経路のデフォルトの MED 値の設定.....	493

第 33 章 : IPv6.....494

33.1 共通の設定.....	494
33.1.1 IPv6 パケットを扱うか否かの設定.....	494
33.1.2 IPv6 インタフェースのリンク MTU の設定.....	494
33.1.3 TCP セッションの MSS 制限の設定.....	495
33.1.4 TCP ウィンドウ・スケール・オプションを変更する.....	495
33.1.5 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.....	496
33.1.6 IPv6 ファストパス機能の設定.....	496
33.1.7 ICMPv6 でアドレス解決が完了するまでに送信を保留しておくことのできるパケット数の設定.....	497
33.1.8 近隣キャッシュの最大エントリ数の設定.....	497
33.1.9 IPv6 のフラグメントパケットを再構成するために保持しておく時間を設定.....	498
33.2 IPv6 アドレスの管理.....	498
33.2.1 インタフェースの IPv6 アドレスの設定.....	498
33.2.2 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.....	500
33.2.3 IPv6 プレフィックスに変化があった時にログに記録するか否かの設定.....	502
33.2.4 DHCPv6 の動作の設定.....	503
33.2.5 DAD(Duplicate Address Detection) の送信回数数の設定.....	504
33.2.6 自動的に設定される IPv6 アドレスの最大数の設定.....	504
33.2.7 始点 IPv6 アドレスを選択する規則の設定.....	505
33.3 近隣探索.....	505
33.3.1 ルーター広告で配布するプレフィックスの定義.....	505

33.3.2 ルーター広告で配布する RDNSS オプションの定義	507
33.3.3 ルーター広告の送信の制御	508
33.3.4 ルーター要請の再送機能の設定	510
33.4 経路制御	510
33.4.1 IPv6 の経路情報の追加	510
33.4.2 IPv6 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	512
33.5 RIPng	512
33.5.1 RIPng の使用の設定	512
33.5.2 インタフェースにおける RIPng の送信ポリシーの設定	513
33.5.3 インタフェースにおける RIPng の受信ポリシーの設定	513
33.5.4 RIPng の加算ホップ数の設定	514
33.5.5 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	514
33.5.6 RIPng で送受信する経路に対するフィルタリングの設定	515
33.5.7 回線接続時の PP 側の RIPng の動作の設定	515
33.5.8 回線接続時の PP 側の RIPng 送出の時間間隔の設定	516
33.5.9 回線切断時の PP 側の RIPng の動作の設定	516
33.5.10 回線切断時の PP 側の RIPng 送出の時間間隔の設定	517
33.5.11 RIPng による経路を回線切断時に保持するか否かの設定	517
33.5.12 RIPng による経路の優先度の設定	517
33.6 VRRPv3 の設定	518
33.6.1 インタフェース毎の VRRPv3 の設定	518
33.6.2 シャットダウントリガの設定	519
33.7 フィルタの設定	520
33.7.1 IPv6 フィルタの定義	520
33.7.2 IPv6 フィルタの適用	522
33.7.3 IPv6 動的フィルタの定義	523
33.8 IPv6 マルチキャストパケットの転送の設定	524
33.8.1 MLD の動作の設定	525
33.8.2 MLD の静的な設定	526
33.8.3 IPv6 マルチキャストの転送モードの設定	527
33.9 近隣要請	528
33.9.1 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	528

第 34 章 : OSPFv3.....529

34.1 OSPFv3 の有効設定	529
34.2 OSPFv3 の使用設定	529
34.3 OSPFv3 のルーター ID 設定	529
34.4 OSPFv3 エリア設定	530
34.5 エリアへの経路広告	531
34.6 指定インタフェースの OSPFv3 エリア設定	531
34.7 仮想リンク設定	533
34.8 OSPFv3 による経路の優先度設定	534
34.9 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	535
34.10 OSPFv3 で受け取った経路をどう扱うかのフィルタの設定	535
34.11 外部プロトコルによる経路導入	537
34.12 外部経路導入に適用するフィルタ定義	537
34.13 OSPFv3 のログ出力設定	539

第 35 章 : 状態メール通知機能.....540

35.1 状態メール通知機能の動作の設定	540
35.2 メールサーバーの設定	540
35.3 送信元のメールアドレスの設定	540
35.4 送信先メールアドレスの設定	541
35.5 サブジェクトの設定	541
35.6 送信タイムアウトの設定	541
35.7 通知内容の設定	542
35.8 状態メール通知の実行	542

第 36 章 : トリガによるメール通知機能.....	543
36.1 メール設定識別名の設定.....	543
36.2 SMTP メールサーバーの設定.....	543
36.3 POP メールサーバーの設定.....	544
36.4 メール処理のタイムアウト値の設定.....	545
36.5 メールの送信時に使用するテンプレートの設定.....	545
36.6 メール通知のトリガの設定.....	547
第 37 章 : HTTP サーバー機能.....	550
37.1 共通の設定.....	550
37.1.1 HTTP サーバー機能の有無の設定.....	550
37.1.2 HTTP サーバーへアクセスできるホストの設定.....	550
37.1.3 HTTP サーバーのセッションタイムアウト時間の設定.....	551
37.1.4 HTTP サーバー機能の listen ポートの設定.....	551
37.1.5 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.....	552
37.2 かんたん設定ページ用の設定.....	552
37.2.1 プロバイダ接続タイプの設定.....	552
37.2.2 プロバイダ情報の PP との関連付けと名前の設定.....	552
37.2.3 プロバイダ接続設定.....	553
37.2.4 プロバイダの DNS サーバーのアドレス設定.....	553
37.2.5 LAN インタフェースの DNS サーバーのアドレスの設定.....	554
37.2.6 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.....	554
37.2.7 フィルタ型ルーティングの形式の設定.....	554
37.2.8 LAN 側のプロバイダ名称の設定.....	555
37.2.9 NTP サーバーの設定.....	556
37.2.10 プロバイダの NTP サーバーのアドレス設定.....	556
37.2.11 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.....	556
37.2.12 かんたん設定ページで IPv6 接続を行うか否かの設定.....	557
37.2.13 LAN インタフェースのプロバイダ情報とトンネルとの関連付け.....	557
第 38 章 : ネットボランチ DNS サービスの設定.....	559
38.1 ネットボランチ DNS サービスの使用の可否.....	559
38.2 ネットボランチ DNS サーバーへの手動更新.....	559
38.3 ネットボランチ DNS サーバーからの削除.....	560
38.4 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.....	560
38.5 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.....	561
38.6 ホスト名の登録.....	561
38.7 通信タイムアウトの設定.....	562
38.8 ホスト名を自動生成するか否かの設定.....	563
38.9 シリアル番号を使ったホスト名登録コマンドの設定.....	564
38.10 ネットボランチ DNS サーバーの設定.....	564
38.11 ネットボランチ DNS サーバアドレス更新機能の ON/OFF の設定.....	565
38.12 ネットボランチ DNS サーバアドレス更新機能のポート番号の設定.....	565
38.13 自動更新に失敗した場合のリトライ間隔と回数の設定.....	565
38.14 ネットボランチ DNS 登録の定期更新間隔の設定.....	566
38.15 ネットボランチ DNS の自動登録に成功したとき設定を保存するファイルの設定.....	567
第 39 章 : UPnP の設定.....	568
39.1 UPnP を使用するか否かの設定.....	568
39.2 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.....	568
39.3 UPnP のポートマッピング用消去タイマのタイプの設定.....	569
39.4 UPnP のポートマッピングの消去タイマの設定.....	569
39.5 UPnP の syslog を出力するか否かの設定.....	570
第 40 章 : USB の設定.....	571

40.1 USB ホスト機能を使うか否かの設定.....	571
40.2 USB メモリに保存する SYSLOG ファイル名の指定.....	571
40.3 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.....	572
40.4 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.....	574
40.5 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.....	574
40.6 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.....	575
40.7 USB バスで過電流保護機能が働くまでの時間の設定.....	575
第 41 章 : スケジュール.....	576
41.1 スケジュールの設定.....	576
第 42 章 : VLAN の設定.....	579
42.1 VLAN ID の設定.....	579
42.2 スイッチングハブのポートが所属する VLAN の設定.....	579
第 43 章 : 生存通知機能.....	581
43.1 生存通知の共有鍵の設定.....	581
43.2 生存通知を受信するか否かの設定.....	581
43.3 生存通知の実行.....	582
第 44 章 : 生存通知機能 リリース 2.....	583
44.1 通知名称の設定.....	583
44.2 通知設定の定義.....	583
44.3 通知設定の有効化.....	584
44.4 通知間隔の設定.....	585
44.5 通知を送信した際にログを記録するか否かの設定.....	585
44.6 受信設定の定義.....	586
44.7 受信設定の有効化.....	586
44.8 受信間隔の監視設定.....	587
44.9 通知を受信した際にログを記録するか否かの設定.....	587
44.10 同時に保持できる生存情報の最大数の設定.....	588
44.11 生存通知の状態の表示.....	588
44.12 生存通知の状態のクリア.....	589
第 45 章 : SNMP サーバー機能.....	591
45.1 SNMP サーバー機能を有効にするか否かの設定.....	591
45.2 SNMP サーバーへのアクセスを許可するホストの設定.....	591
第 46 章 : 外部メモリ機能.....	593
46.1 microSD カードスロットを使うか否かの設定.....	593
46.2 外部メモリ用キャッシュメモリの動作モードの設定.....	594
46.3 ファイルアクセス高速化用キャッシュメモリのサイズの設定.....	594
46.4 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.....	595
46.5 外部メモリに保存する SYSLOG ファイル名の指定.....	597
46.6 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.....	599
46.7 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.....	599
46.8 ルーター起動時に外部メモリを検出するまでのタイムアウトを設定する.....	600
46.9 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.....	600
46.10 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.....	601
46.11 ファイル検索時のタイムアウトを設定する.....	603
46.12 バッチファイルを実行する.....	603

46.13 バッチファイルと実行結果ファイルの設定.....	603
46.14 外部メモリ性能測定コマンド.....	604
46.15 DOWNLOAD ボタンを押した時に実行する機能の設定.....	605
46.16 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.....	605
46.17 シグネチャーを保存する外部メモリのディレクトリーの設定.....	606

第 47 章 : HTTP アップロード機能.....607

47.1 HTTP アップロードするファイルの設定.....	607
47.2 HTTP アップロード先 URL の設定.....	608
47.3 HTTP アップロードを許可するか否かの設定.....	608
47.4 HTTP アップロードのタイムアウト時間の設定.....	609
47.5 HTTP アップロードのリトライの間隔と回数の設定.....	609
47.6 HTTP アップロードで使用するプロキシサーバーの設定.....	609
47.7 HTTP アップロードの実行.....	610
47.8 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.....	610

第 48 章 : モバイルインターネット接続機能.....611

48.1 新 JATE 番号の認識処理.....	611
48.2 携帯端末を使用するか否かの設定.....	611
48.3 携帯端末に入力する PIN コードの設定.....	612
48.4 モバイルインターネット接続機能の発信方式の設定.....	612
48.5 携帯端末に直接コマンドを発行する.....	613
48.6 指定した相手に対して発信制限を解除する.....	613
48.7 PP で使用するインタフェースの設定.....	614
48.8 携帯端末からの自動発信設定.....	615
48.9 携帯端末を切断するタイマの設定.....	615
48.10 携帯端末を入力がないときに切断するタイマの設定.....	615
48.11 携帯端末を出力がないときに切断するタイマの設定.....	616
48.12 発信先アクセスポイントの設定.....	616
48.13 携帯端末に指示する発信先の設定.....	616
48.14 パケット通信量制限の設定.....	617
48.15 パケット通信時間制限の設定.....	618
48.16 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.....	619
48.17 LCP の Async Control Character Map オプション使用の設定.....	619
48.18 発信者番号通知 (186) を付加するかどうかの設定.....	620
48.19 詳細な SYSLOG を出力するか否かの設定.....	620
48.20 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.....	621
48.21 接続毎パケット通信量制限の設定.....	621
48.22 接続毎パケット通信時間制限の設定.....	622
48.23 通信制限の累積期間の設定.....	622
48.24 携帯端末でパケット着信機能を使用するか否かの設定.....	623
48.25 モバイルインターネット機能の着信許可の設定.....	623
48.26 電波の受信レベルの取得.....	624
48.27 電波の受信レベル取得機能の設定.....	624
48.28 定期実行で取得した電波の受信レベルの表示.....	625
48.29 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.....	626
48.30 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.....	626
48.31 携帯端末のファームウェア更新.....	627
48.32 携帯端末のネットワーク事業者モードの設定.....	627
48.33 自分の名前とパスワードの設定.....	628
48.34 WAN で使用するインタフェースの設定.....	629
48.35 携帯端末からの自動発信設定.....	629
48.36 携帯端末を切断するタイマの設定.....	630
48.37 携帯端末を入力がないときに切断するタイマの設定.....	630
48.38 携帯端末を出力がないときに切断するタイマの設定.....	631
48.39 常時接続の設定.....	631
48.40 発信先アクセスポイントの設定.....	632
48.41 パケット通信量制限の設定.....	633
48.42 パケット通信時間制限の設定.....	634

48.43 接続毎パケット通信量制限の設定.....	635
48.44 接続毎パケット通信時間制限の設定.....	636
48.45 通信制限の累積期間の設定.....	636
第 49 章 : ブリッジインタフェース (ブリッジ機能).....	638
49.1 ブリッジインタフェースに収容するインタフェースを設定する.....	638
49.2 自動的なラーニングを行うか否かの設定.....	639
49.3 ブリッジがラーニングした情報の消去タイマーの設定.....	640
49.4 静的なラーニング情報の設定.....	640
第 50 章 : QAC/TM.....	642
50.1 QAC/TM 機能で使用するアンチウイルスソフトウェアの設定.....	642
50.2 アンチウイルスソフトウェアの管理サーバーの設定.....	642
50.3 有効なウイルスパターンファイルとウイルス検索エンジンのバージョン範囲の設定.....	643
50.4 警告画面に表示するクライアントインストール URL の設定.....	644
50.5 クライアント PC のアンチウイルスソフトウェアバージョン情報を取得するポート番号の設定.....	644
50.6 クライアント PC にインストールしているアンチウイルスソフトウェアのウイルスパターンファイルとウイルス検索エンジンの自動アップデートの設定.....	644
50.7 QAC/TM でチェックを行う HTTP のポート番号の設定.....	645
50.8 不適格クライアント PC のアクセス制御設定.....	645
50.9 アンチウイルスソフトウェア情報のチェックなしに認定されるクライアントの設定.....	646
50.10 QAC/TM で表示する警告画面の設定.....	646
50.11 管理サーバーのアンチウイルスソフトウェアパターンファイル情報を更新する.....	647
50.12 クライアント PC のアンチウイルスソフトウェアパターンファイル情報を更新する.....	647
50.13 QAC/TM の状態の表示.....	647
第 51 章 : Lua スクリプト機能.....	649
51.1 Lua スクリプト機能を有効にするか否かの設定.....	649
51.2 Lua スクリプトの実行.....	649
51.3 Lua コンパイラの実行.....	650
51.4 Lua スクリプトの走行状態の表示.....	650
51.5 Lua スクリプトの強制終了.....	652
51.6 Lua スクリプト機能に関連するアラーム音を鳴らすか否かの設定.....	652
第 52 章 : カスタム GUI.....	654
52.1 カスタム GUI を使用するか否かの設定.....	654
52.2 カスタム GUI を使用するユーザの設定.....	654
52.3 カスタム GUI の API を使用するか否かの設定.....	655
52.4 カスタム GUI の API にアクセスするためのパスワードの設定.....	655
第 53 章 : L2MS.....	657
53.1 共通の設定.....	657
53.1.1 L2MS の動作モードの設定.....	657
53.1.2 L2MS を使用するか否かの設定.....	658
53.1.3 エージェントの監視時間間隔の設定.....	659
53.1.4 端末情報の監視時間間隔の設定.....	659
53.1.5 スナップショット機能を使用するか否かの設定.....	660
53.1.6 スナップショットファイルを作成する.....	661
53.1.7 LAN マップの SYSLOG 出力の設定.....	661
53.1.8 LAN マップで使用する機器名の設定.....	662
53.2 スイッチの制御.....	662
53.2.1 スイッチの選択.....	662
53.2.2 スイッチが持つ機能の設定.....	663
53.2.3 スイッチが持つ機能の設定内容や動作状態の取得.....	663
53.2.4 スイッチに対して特定の動作を実行.....	664
53.2.5 スイッチの設定の削除.....	664

53.2.6	スイッチのファームウェアの更新.....	665
53.2.7	LAN ケーブル二重化機能の設定.....	665
53.2.8	スイッチの設定ファイルを格納するディレクトリの指定.....	666
53.2.9	スイッチの設定を保存するファイル名の指定.....	666
53.2.10	スイッチの設定の取得.....	667
53.2.11	スイッチの設定の復元.....	668
53.3	スイッチの機能.....	668
53.3.1	システム.....	668
53.3.2	ポート.....	673
53.3.3	MAC アドレステーブル.....	679
53.3.4	VLAN.....	681
53.3.5	QoS.....	686
53.3.6	ミラーリング.....	690
53.3.7	カウンタ.....	693
53.3.8	ループ検出.....	698
53.3.9	PoE 給電.....	703
53.4	アクセスポイントの制御.....	707
53.4.1	アクセスポイントの選択.....	707
53.4.2	アクセスポイントの設定ファイルを格納するディレクトリの指定.....	708
53.4.3	アクセスポイントの設定を保存するファイル名の指定.....	708
53.4.4	アクセスポイントの設定のバックアップ実行.....	708
53.4.5	アクセスポイントの設定の復元実行.....	709
53.4.6	アクセスポイントの設定の削除.....	709
53.4.7	アクセスポイント設定のゼロコンフィグ機能を使用するか否かの設定.....	710
53.4.8	アクセスポイントの HTTP リビジョンアップ機能の実行.....	710
53.4.9	アクセスポイント制御用の HTTP プロキシの使用.....	711
53.4.10	アクセスポイント制御用の HTTP プロキシのタイムアウト時間の設定.....	711
53.5	ルーターの制御.....	711
53.5.1	HTTP プロキシを経由での Web GUI へのアクセスを許可するか否かの設定.....	711

第 54 章 : YNO エージェント.....713

54.1	YN0 エージェント機能を使用するか否かの設定.....	713
54.2	YN0 マネージャー接続用のアクセスコードの設定.....	713
54.3	YN0 エージェント機能に関する追加の SYSLOG を出力するか否かの設定.....	714
54.4	YN0 マネージャーに表示される自身の機器説明の設定.....	714
54.5	YN0 で使用する HTTPS プロキシサーバーの設定.....	715
54.6	GUI Forwarder 接続のタイムアウト時間の設定.....	715
54.7	YN0 のゼロコンフィグの設定.....	716
54.8	YN0 エージェント機能の動作状態の表示.....	716
54.9	LAS (Log Analysis Service).....	718
54.9.1	SYSLOG 送信キューの長さの設定.....	718
54.9.2	LAS クライアントが送信したリクエストに対する LAS サーバーからの応答待ちがタイムアウトするまでの時間の設定.....	719
54.9.3	LAS クライアントがリクエストの送信を再試行する回数の設定.....	719
54.9.4	LAS サーバーとのコネクションに対するキープアライブの設定.....	719
54.9.5	LAS の動作状態の表示.....	720
54.10	XMPP サーバーとのキープアライブの時間間隔の設定.....	721

第 55 章 : 診断.....722

55.1	ポートの開閉状態の診断.....	722
55.2	ポートへ到達可能なアクセス範囲の診断.....	723
55.3	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.....	723
55.4	ポートの開閉状態の診断結果の履歴数の設定.....	724
55.5	ポートの開閉状態の診断結果の表示.....	724
55.6	ポートへ到達可能なアクセス範囲の診断結果の表示.....	724
55.7	ポートの開閉状態の診断結果の消去.....	724

第 56 章 : 統計.....725

56.1 統計機能を有効にするか否かの設定.....	725
第 57 章 : DPI.....	726
57.1 DPI を使用するか否かの設定.....	726
57.2 IPv4 の DPI フィルターの設定.....	726
57.3 IPv6 の DPI フィルタの設定.....	728
57.4 DPI のフィルターのインターフェースへの適用.....	729
57.5 DPI のアプリケーショングループの作成.....	730
57.6 シグネチャのダウンロードの手動実行.....	731
57.7 シグネチャのダウンロード先 URL の設定.....	732
57.8 アプリケーションの識別に関するログを出力するか否かの設定.....	732
57.9 DPI の統計情報の表示.....	733
57.10 DPI の統計情報のクリア.....	734
57.11 識別結果のキャッシュの表示.....	735
57.12 識別結果のキャッシュのクリア.....	735
57.13 アプリケーションを表すモニター一覧の表示.....	735
57.14 カテゴリーを表すモニター一覧の表示.....	736
57.15 DPI の動作状態、およびシグネチャの状態の表示.....	737
第 58 章 : ダッシュボード.....	739
58.1 ダッシュボードのデータを蓄積するか否かの設定.....	739
第 59 章 : 操作.....	740
59.1 相手先情報番号の選択.....	740
59.2 トンネルインタフェース番号の選択.....	740
59.3 設定に関する操作.....	741
59.3.1 管理ユーザへの移行.....	741
59.3.2 終了.....	741
59.3.3 設定内容の保存.....	741
59.3.4 設定ファイルの複製.....	742
59.3.5 ファームウェアファイルを内蔵フラッシュ ROM にコピー.....	744
59.3.6 設定ファイルの削除.....	745
59.3.7 実行形式ファームウェアファイルの削除.....	745
59.3.8 PKI ファイルの削除.....	745
59.3.9 デフォルト設定ファイルの設定.....	746
59.3.10 デフォルトファームウェアファイルの設定.....	746
59.3.11 シリアルポートのボーレートの設定.....	746
59.3.12 設定の初期化.....	747
59.3.13 遠隔地のルーターの設定.....	747
59.3.14 遠隔地のルーターからの設定に対する制限.....	748
59.4 動的情報のクリア操作.....	748
59.4.1 アカウントのクリア.....	748
59.4.2 PP アカウントのクリア.....	748
59.4.3 TUNNEL アカウントのクリア.....	749
59.4.4 携帯電話回線のアカウントのクリア.....	749
59.4.5 データコネクタのアカウントのクリア.....	749
59.4.6 ARP テーブルのクリア.....	750
59.4.7 IP の動的経路情報のクリア.....	750
59.4.8 ブリッジのラーニング情報のクリア.....	750
59.4.9 ログのクリア.....	750
59.4.10 InARP のクリア.....	751
59.4.11 DNS キャッシュのクリア.....	751
59.4.12 インタフェースのカウンター情報のクリア.....	751
59.4.13 PRI のステータス情報のクリア.....	752
59.4.14 NAT アドレステーブルのクリア.....	752
59.4.15 インタフェースの NAT アドレステーブルのクリア.....	753
59.4.16 IP マスカレードで管理しているセッションの統計情報のクリア.....	753
59.4.17 PPPoE パススルー機能がラーニングした情報のクリア.....	754

59.4.18 IPv6 の動的経路情報の消去.....	754
59.4.19 近隣キャッシュの消去.....	754
59.4.20 起動情報の履歴を削除する.....	755
59.4.21 外部メモリに保存された SYSLOG のクリアとバックアップファイルの削除.....	755
59.5 ファイル、ディレクトリの操作.....	755
59.5.1 ディレクトリの作成.....	755
59.5.2 ファイルまたはディレクトリの削除.....	755
59.5.3 ファイルまたはディレクトリの複製.....	756
59.5.4 ファイル名またはディレクトリ名の変更.....	756
59.6 その他の操作.....	757
59.6.1 相手先の使用許可の設定.....	757
59.6.2 相手先の使用不許可の設定.....	758
59.6.3 再起動.....	758
59.6.4 インタフェースの再起動.....	759
59.6.5 PP インタフェースの再起動.....	760
59.6.6 発信.....	760
59.6.7 切断.....	761
59.6.8 ping.....	762
59.6.9 ping6 の実行.....	763
59.6.10 traceroute.....	764
59.6.11 traceroute6 の実行.....	764
59.6.12 nslookup.....	765
59.6.13 SIP サーバーに対し手動で接続.....	765
59.6.14 SIP サーバーに対し手動で切断.....	766
59.6.15 IPv4 動的フィルタのコネクション管理情報の削除.....	766
59.6.16 TELNET クライアント.....	766
59.6.17 IPv6 動的フィルタのコネクション管理情報の削除.....	767
59.6.18 スイッチングハブ MAC アドレステーブルの消去.....	768
59.6.19 PRI のループバックの実行.....	768
59.6.20 PRI のループバック待ち受けの設定.....	769
59.6.21 Magic Packet の送信.....	770
59.6.22 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.....	771
59.6.23 入力遮断フィルタの状態のクリア.....	771
59.6.24 ポリシーフィルタの状態のクリア.....	772
59.6.25 URL フィルタの統計情報のクリア.....	772
59.6.26 外部データベース参照型 URL フィルタの統計情報のクリア.....	772
59.6.27 メール通知の実行.....	773
59.6.28 外部メモリに保存された SYSLOG ファイルのローテート (バックアップ).....	773
59.6.29 ライセンス認証の実行.....	774
59.6.30 ライセンス認証のリトライの間隔と回数設定.....	774
59.6.31 設定の一括更新.....	774
59.6.32 ロールバックタイマーの起動.....	775
59.6.33 設定の確認.....	776
59.6.34 ファイルをマクロとして実行する.....	776
59.6.35 echo.....	777

第 60 章 : 設定の表示.....778

60.1 機器設定の表示.....	778
60.2 すべての設定内容の表示.....	778
60.3 指定した AP の設定内容の表示.....	778
60.4 指定した PP の設定内容の表示.....	779
60.5 指定したスイッチの設定内容の表示.....	779
60.6 指定したトンネルの設定内容の表示.....	780
60.7 設定の差分の表示.....	780
60.8 設定ファイルの一覧.....	781
60.9 ファイル情報の一覧の表示.....	781
60.10 インタフェースに付与されている IPv6 アドレスの表示.....	782
60.11 マスタクロックを得ている回線の表示.....	783
60.12 SSH サーバー公開鍵の表示.....	783
60.13 指定したインタフェースのフィルタ内容の表示.....	784

60.14 指定したインターフェースの IPv6 フィルター内容の表示.....	784
60.15 ファームウェアファイルの一覧.....	785
60.16 環境変数の表示.....	785
60.17 エイリアスの表示.....	786
60.18 マクロの表示.....	786

第 61 章 : 状態の表示.....788

61.1 ARP テーブルの表示.....	788
61.2 インタフェースの状態の表示.....	788
61.3 各相手先の状態の表示.....	788
61.4 DLCI の表示.....	789
61.5 IP の経路情報テーブルの表示.....	789
61.6 RIP で得られた経路情報の表示.....	790
61.7 IPv6 の経路情報の表示.....	791
61.8 IPv6 の RIP テーブルの表示.....	791
61.9 近隣キャッシュの表示.....	791
61.10 ブリッジのラーニング情報の表示.....	792
61.11 IPsec の SA の表示.....	792
61.12 証明書の情報の表示.....	793
61.13 CRL ファイルの情報の表示.....	793
61.14 VRRP の情報の表示.....	794
61.15 動的 NAT ディスクリプタのアドレスマップの表示.....	794
61.16 動作中の NAT ディスクリプタの適用リストの表示.....	795
61.17 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.....	795
61.18 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.....	796
61.19 IP マスカレードで使用しているセッション数の表示.....	796
61.20 IP マスカレードで管理しているセッションの統計情報の表示.....	797
61.21 L2TP の状態の表示.....	797
61.22 PPTP の状態の表示.....	798
61.23 IPIP トンネリングの状態の表示.....	798
61.24 OSPF 情報の表示.....	798
61.25 BGP の状態の表示.....	799
61.26 DHCP サーバーの状態の表示.....	799
61.27 DHCP クライアントの状態の表示.....	800
61.28 DHCPv6 の状態の表示.....	800
61.29 バックアップ状態の表示.....	800
61.30 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.....	800
61.31 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.....	802
61.32 ネットワーク監視機能の状態の表示.....	803
61.33 侵入情報の履歴の表示.....	803
61.34 相手先ごとの接続時間情報の表示.....	804
61.35 PPPoE パススルー機能がラーニングした情報の表示.....	804
61.36 ネットボランチ DNS サービスに関する設定の表示.....	804
61.37 スイッチングハブ MAC アドレステーブルの表示.....	805
61.38 UPnP に関するステータス情報の表示.....	806
61.39 トンネルインタフェースの状態の表示.....	806
61.40 VLAN インタフェースの状態の表示.....	807
61.41 トリガによるメール通知機能の状態の表示.....	807
61.42 マルチキャストの経路情報の表示.....	807
61.43 IGMP のグループ管理情報の表示.....	808
61.44 PIM-SM によって管理される情報の表示.....	808
61.45 MLD のグループ管理情報の表示.....	809
61.46 IPv6 マルチキャストの経路情報の表示.....	809
61.47 ログインしているユーザー情報の表示.....	809
61.48 ログインしたユーザーのログイン履歴の表示.....	810
61.49 パケットバッファの状態の表示.....	810
61.50 QoS ステータスの表示.....	811
61.51 連携動作の状態の表示.....	812
61.52 OSPFv3 情報の表示.....	812
61.53 入力遮断フィルタの状態表示.....	813

61.54	ポリシーフィルタの状態表示	813
61.55	ポリシーフィルタの制御対象サービスの表示	814
61.56	URL フィルタの情報の表示	814
61.57	外部データベース参照型 URL フィルターの統計情報の表示	815
61.58	データベースのライセンス情報の表示	815
61.59	生存通知の状態の表示	816
61.60	USB ホスト機能の動作状態を表示	816
61.61	リモートセットアップ機能に関する接続情報の表示	816
61.62	技術情報の表示	817
61.63	microSD スロットの動作状態を表示	817
61.64	外部メモリの動作状態を表示	817
61.65	RTFS の状態の表示	818
61.66	起動情報を表示する	818
61.67	起動情報の履歴の詳細を表示する	818
61.68	起動情報の履歴の一覧を表示する	819
61.69	エージェント一覧の表示	819
61.70	LAN ケーブル二重化機能の動作状態を表示	820
61.71	DNS キャッシュの表示	821
61.72	ライセンス情報の表示	821
61.73	ライセンス認証の状態の表示	822
61.74	CPU スケジューリング(パケット転送)機能の状態の表示	822
61.75	STATUS LED の情報の表示	823
61.76	LAN マップの状態を表示する	823
61.77	コピーライトの表示	826
第 62 章	：ロギング	827
62.1	ログの表示	827
62.2	アカウントの表示	828
62.3	PP アカウントの表示	828
62.4	TUNNEL アカウントの表示	829
62.5	携帯電話回線のアカウントの表示	829
62.6	データコネクタのアカウントの表示	829
62.7	通信履歴の表示	830
62.8	コマンドヒストリーの表示	830
索引		831

序文

はじめに

- 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ようお願い致します。
- 本書に記載されている会社名、製品名は各社の登録商標あるいは商標です。

第 1 章

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.8.02.53, Rev.8.03.94, Rev.9.00.60, Rev.10.00.61, Rev.10.01.76, Rev.11.01.33, Rev.14.00.33, Rev.14.01.41, Rev.15.02.25, Rev.15.04.04 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 (<i>Italic face</i>) 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。
[設定例]	コマンドの具体例を示します。
[拡張ライセンス対応]	拡張ライセンスがインポートされているときに拡張される機能を示します。
[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。

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、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。

RTX5000、RTX3500、RTX1220、RTX1210、RTX1200、RTX830、RTX810 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, ...

インタフェースの種類	インタフェース名
LAN 分割機能の LAN	lan1.1, lan1.2, ...
LAN 分割機能の拡張機能の LAN	vlan1,vlan2, ...
メインモジュール上の BRI	bri1
1 つ目の BRI モジュール	bri1.1, bri1.2, ...
2 つ目の BRI モジュール	bri2.1, bri2.2, ...
1 つ目の PRI モジュール	pri1

また、Rev.8.03 系以降のファームウェア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

SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで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とスペースを含めて最大半角 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
?	\?, "?", "?"
#	\#, "#", "#"
	\ , " ", " "
>	\>, ">", ">"
\	\\
'	\', ""'
"	\", ""
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
RTX5000/RTX3500/RTX3000/RT250i	1-150
RTX1500/RTX1220/RTX1210/RTX1200	1-100
RTX1100/RTX830/RTX810/RT107e/SRT100	1-30

1.7 工場出荷設定値について

RTX1220、RTX1210、RTX1200、RTX830、RTX810、RT107e、SRT100 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
```

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。

以下の機種では **telnetd host lan** コマンドも設定されています。

機種	リビジョン
RTX1220	すべてのリビジョン
RTX830	Rev.15.02.03 以降
RTX1210	Rev.14.01.26 以降
RTX810	Rev.11.01.33 以降
RTX1200	Rev.10.01.76 以降

1.8 拡張ライセンスについて

拡張ライセンスはヤマハルーターの VPN、および外部接続に関する機能を拡張するためのライセンスです。

• インターフェース数の増加

以下のインターフェースの数が増加します。

- トンネル
- PP
- PP Anonymous

• 最大対地数の増加

以下の機能の最大対地数が増加します。

- IPsec
- IPIP
- L2TPv2, L2TPv3, L2TPv3/IPsec
- マルチポイントトンネル
- データコネクト

• マルチポイントトンネルサーバー機能の有効化

マルチポイントトンネルのサーバーとして利用できるようになります。

拡張ライセンスの詳細は技術資料を参照してください。

- <http://www.rtpro.yamaha.co.jp/RT/docs/ex-license/index.html>

以下の機種で拡張ライセンスに対応しています。

ライセンス名	機種	リビジョン
YSL-VPN-EX1	RTX830	Rev.15.02.22 以降

拡張ライセンスをインポートすると、コマンドのパラメーターの上限値などが拡張されます。

コマンド	拡張内容	ライセンス名	機種	ライセンスなし	ライセンスあり
トンネル番号を指定するコマンド(※1)	トンネル番号 (<i>tunnel_num</i>) の上限値が増加	YSL-VPN-EX1	RTX830	20	100
セキュリティゲートウェイ番号を指定するコマンド(※2)	セキュリティゲートウェイ番号 (<i>gateway_id</i>) の上限値が増加	YSL-VPN-EX1	RTX830	20	100
PP 番号を指定するコマンド(※3)	PP 番号 (<i>peer_num</i>) の上限値が増加	YSL-VPN-EX1	RTX830	30	100
bridge member	ブリッジインターフェースに収容できるインターフェース (<i>interface</i>) の最大個数が増加	YSL-VPN-EX1	RTX830	2	10
dhcp client client-identifier pooldhcp client hostname pooldhcp client option pool	アドレスプール番号 (<i>pool_num</i>) の上限値が増加	YSL-VPN-EX1	RTX830	32	101
ip pp remote address pool	プールできる IP アドレス (<i>ip_address</i>) の最大個数が増加	YSL-VPN-EX1	RTX830	32	101
ipsec transport template	ipsec transport コマンドの設定を展開できるトランスポート ID の最大個数が増加	YSL-VPN-EX1	RTX830	20	100
tunnel multipoint limit	tunnel multipoint limit コマンドが設定できるようになる	YSL-VPN-EX1	RTX830	設定不可	設定可能
tunnel type	point-to-multipoint トンネルのロール (<i>role</i>) にサーバー (<i>server</i>) が設定できるようになる	YSL-VPN-EX1	RTX830	設定不可	設定可能

(※1) **ip route**、**ipv6 route**、**pp bind**、**tunnel enable**、**tunnel select**、**tunnel template** など

(※2) **ipsec ike local address**、**ipsec ike pre-shared-key**、**ipsec ike remote address**、**ipsec sa policy** など

(※3) **ip route**、**ipv6 route**、**pp enable**、**pp select** など

第2章

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したりすることが可能です。

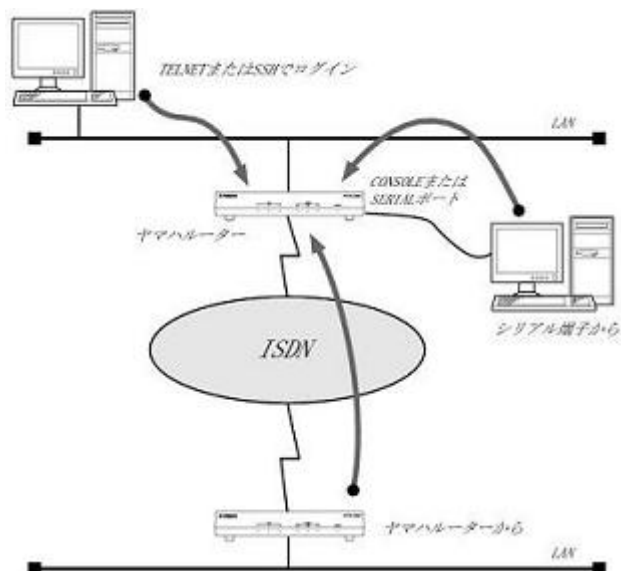
2.1 コンソールについて

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 をお使いの場合には、ターミナル機能のあるソフトウェアを用意してください。macOS をお使いの場合には、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 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. 一般ユーザーとしてログインした後、`administrator` コマンドで管理ユーザー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. 各種コマンドを使用して、相手先情報の内容を変更します。
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。

 **注:** 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 Ctrl 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ある一定時間無き時には、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。

新たに管理ユーザー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。

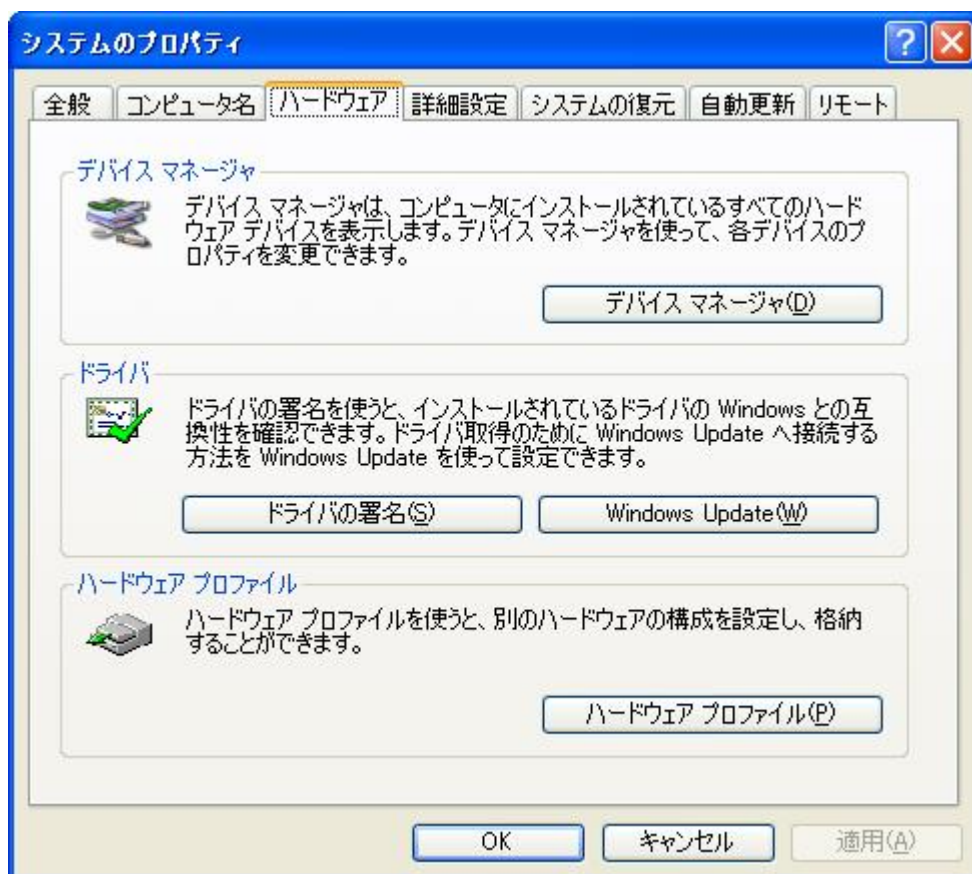
 **注意:** ご購入直後の起動や `cold start` 後にはログインパスワードも管理パスワードも設定されていません。セキュリティ上、ログインパスワードと管理パスワードの設定をお勧めします。なお SRT100 では、工場出荷状態でパスワードとして `doremi` が設定されています。

- 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ー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

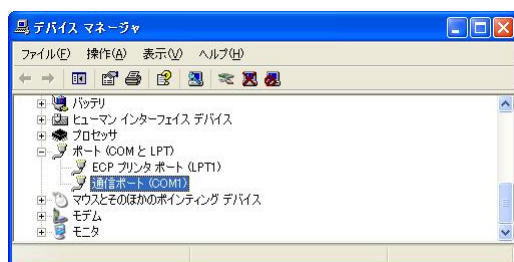
ここでは、Windows XP の『ハイパーターミナル』を使用する場合を例に説明します。シリアルケーブルの接続は事前にすませておきます。

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。



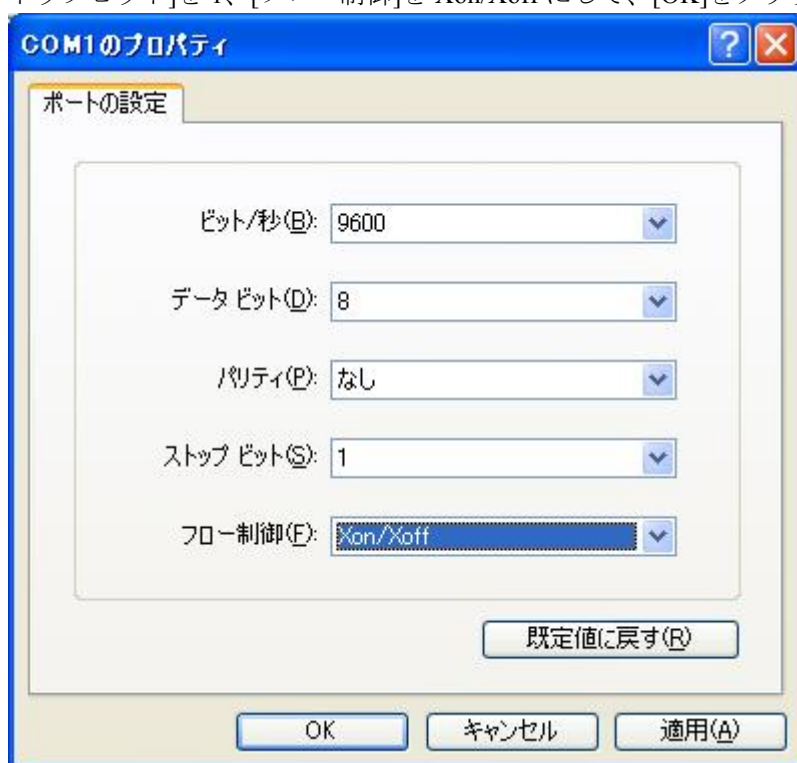
3. 「デバイスマネージャ」ウィンドウを閉じます。
4. [スタート]メニューから[すべてのプログラム]-[アクセサリ]-[通信]-[ハイパーターミナル]を選びます。「接続の設定」ウィンドウが開いたら、名前欄に適切な名前を入力して[OK]をクリックします。



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、RTX1200 にログインした場合の表示です。

```

test - ハイパーターミナル
ファイル(F) 編集(E) 表示(V) 通信(C) 転送(T) ヘルプ(H)
Password:
RTX1200 Rev.10.01.08 (build 4) (Fri Dec 12 10:15:18 2008)
Copyright (c) 1994-2008 Yamaha Corporation.
Copyright (c) 1991-1997 Regents of the University of California.
Copyright (c) 1995-2004 Jean-loup Gailly and Mark Adler.
Copyright (c) 1998-2000 Tokyo Institute of Technology.
Copyright (c) 2000 Japan Advanced Institute of Science and Technology, HOKURIK
U.
Copyright (c) 2002 RSA Security Inc. All rights reserved.
Copyright (c) 1997-2004 University of Cambridge. All rights reserved.
Copyright (C) 1997 - 2002, Makoto Matsumoto and Takuji Nishimura, All rights r
eserved.
Copyright (c) 1995 Tatu Ylonen , Espoo, Finland All rights reserved.
Copyright (c) 1998-2004 The OpenSSL Project. All rights reserved.
Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.
Copyright (c) 2006 Digital Arts Inc. All Rights Reserved.
00:a0:de:37:b5:04, 00:a0:de:37:b5:05, 00:a0:de:37:b5:06
Memory 128Mbytes, 3LAN, 1BRI
> -
接続 00236 自動検出 9600 8-N-1 SCROLL CAPS NUM キー 工口-800

```



注:

- **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。

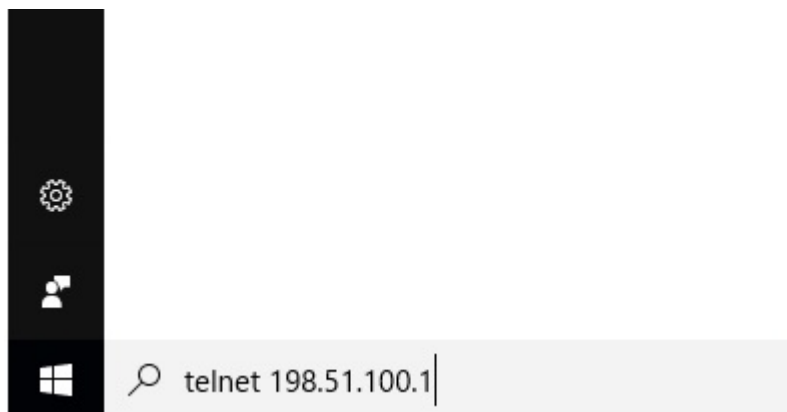
2.1.3 TELNET による設定

ここでは、Windows 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 198.51.100.1 とした場合の例です。

Windows では、あらかじめ次の方法で TELNET を有効にする必要があります。「コントロールパネル」-「プログラム」-「プログラムと機能」で、「Windows の機能の有効化または無効化」を選ぶと表示される「Windows の機能」画面で、「Telnet クライアント」にチェックを付けてから「OK」をクリックします。

1. [スタート]メニューから「telnet 198.51.100.1」と入力します。

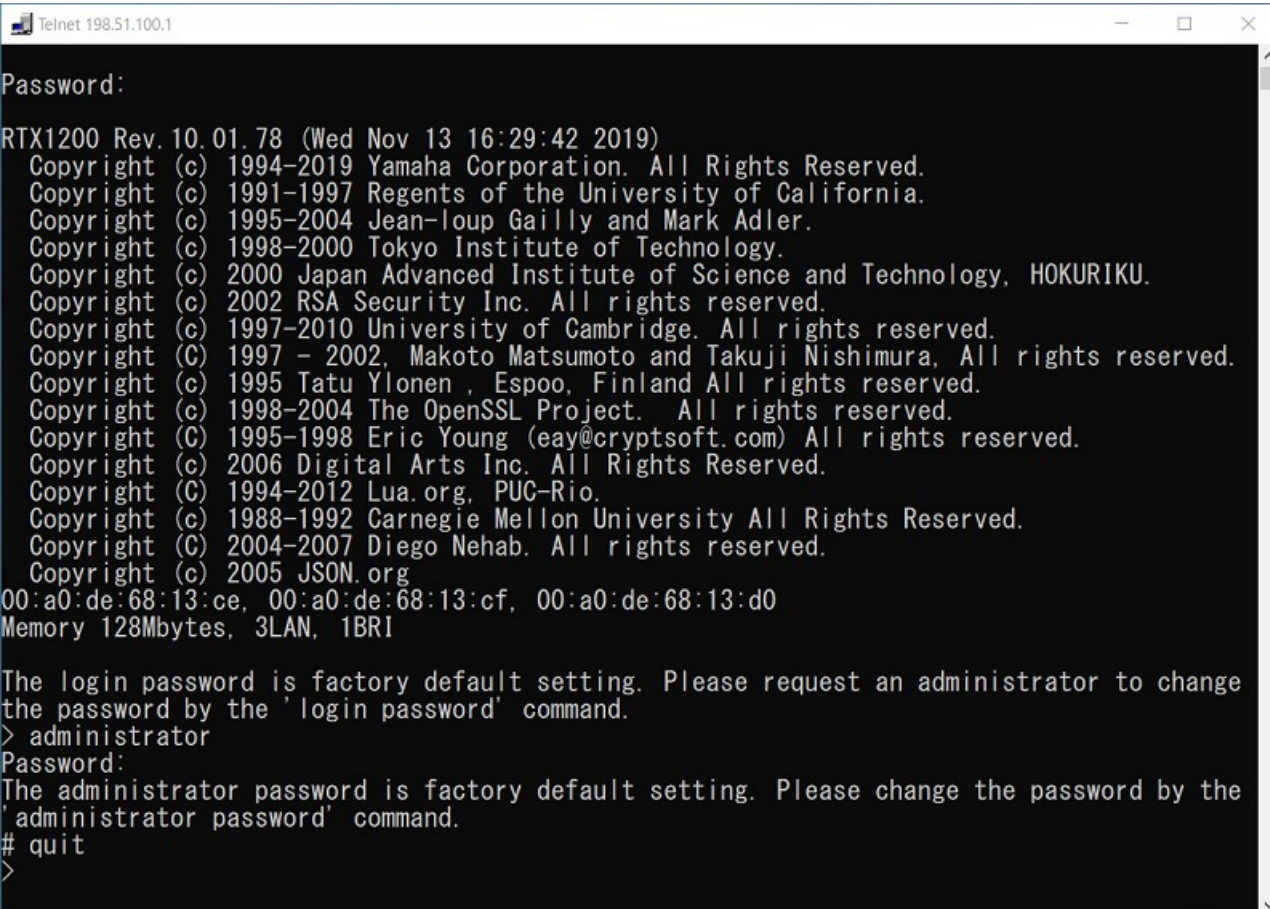
実際には「198.51.100.1」のかわりに本機に設定されている IP アドレスを入力します。



2. 「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ー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、ユーザー名の入力待ち状態となります。ここで、設定したユーザー名を入力して Enter キーを押し、続いてユーザー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。



```

Telnet 198.51.100.1
Password:
RTX1200 Rev. 10.01.78 (Wed Nov 13 16:29:42 2019)
Copyright (c) 1994-2019 Yamaha Corporation. All Rights Reserved.
Copyright (c) 1991-1997 Regents of the University of California.
Copyright (c) 1995-2004 Jean-loup Gailly and Mark Adler.
Copyright (c) 1998-2000 Tokyo Institute of Technology.
Copyright (c) 2000 Japan Advanced Institute of Science and Technology, HOKURIKU.
Copyright (c) 2002 RSA Security Inc. All rights reserved.
Copyright (c) 1997-2010 University of Cambridge. All rights reserved.
Copyright (C) 1997 - 2002, Makoto Matsumoto and Takuji Nishimura, All rights reserved.
Copyright (c) 1995 Tatu Ylonen , Espoo, Finland All rights reserved.
Copyright (c) 1998-2004 The OpenSSL Project. All rights reserved.
Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.
Copyright (c) 2006 Digital Arts Inc. All Rights Reserved.
Copyright (C) 1994-2012 Lua.org, PUC-Rio.
Copyright (c) 1988-1992 Carnegie Mellon University All Rights Reserved.
Copyright (C) 2004-2007 Diego Nehab. All rights reserved.
Copyright (c) 2005 JSON.org
00:a0:de:68:13:ce, 00:a0:de:68:13:cf, 00:a0:de:68:13:d0
Memory 128Mbytes, 3LAN, 1BRI

The login password is factory default setting. Please request an administrator to change
the password by the 'login password' command.
> administrator
Password:
The administrator password is factory default setting. Please change the password by the
'administrator password' command.
# quit
>

```

注:

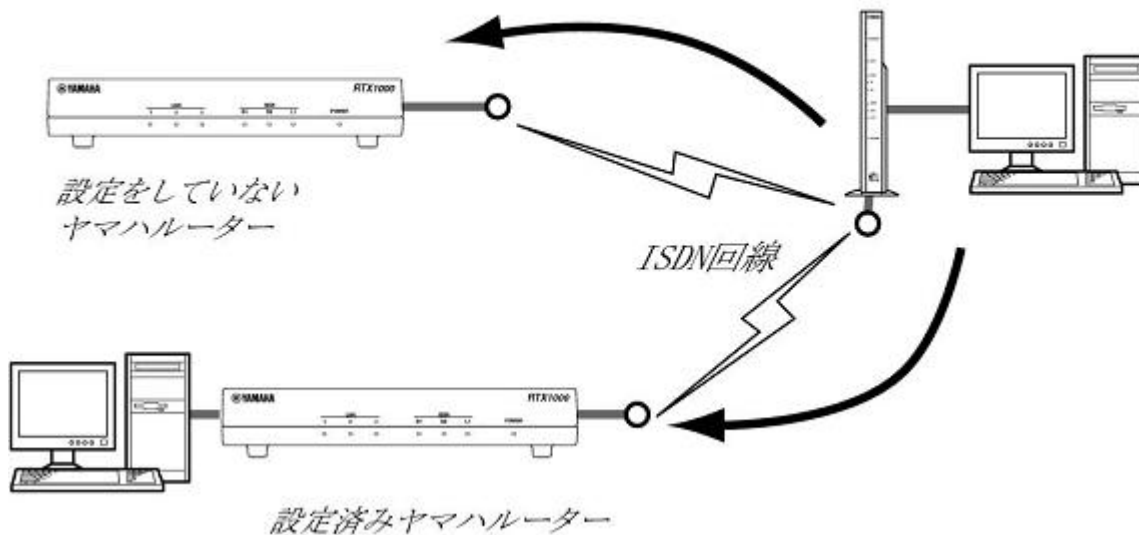
- **help** と入力してから Enter キーを押すと、キー操作の説明が表示されます。
- **show command** と入力してから Enter キーを押すと、コマンド一覧が表示されます。

3. **administrator** と入力してから、Enter キーを押します。
4. 「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。
5. コンソールコマンドを入力して、設定を行います
6. 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。
7. 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。
8. 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。

設定済みヤマハルーター



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。

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 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 SSH サーバー機能の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ー認証 (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)

※以下の機種およびファームウェアでは公開鍵認証をサポートしています。

- RTX5000 Rev.14.00.32 以降
- RTX3500 Rev.14.00.32 以降
- RTX1210 Rev.14.01.35 以降
- RTX830 Rev.15.02.14 以降
- RTX1220 すべてのリビジョン
- 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

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要となるため、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。

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

```

Telnet 198.51.100.1
> administrator
Password:
The administrator password is factory default setting. Please change the password by the 'administrator password' command.
# login user RTuser himitsu
Password Strength : Weak
# sshd host key generate
Update to new host key ? (Y/N)Y
Generating public/private dsa key pair ...
*****
Generating public/private rsa key pair ...
*****
# sshd service on
# save
Saving ... CONFIGO Done .
# quit
>

```

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 や macOS 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。

TFTP では、平文の設定ファイルと暗号化された設定ファイルを扱うことができます。対応している暗号化形式は、AES128 及び、AES256 です。パスワードを指定して暗号化されたファイルは利用できません。RT-Tftp Client では暗号化に対応していません。暗号化された設定ファイルを扱うことができるのは、Rev.10.01.11 以降のファームウェアです。



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ー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。

```

Telnet 198.51.100.1
> administrator
Password:
# tftp host 198.51.100.2
# save
Saving ... CONFIG0 Done .
# quit
>

```

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。
暗号化された設定ファイルを扱う場合は“バイナリ”、“binary”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。
- 起動中の設定ファイルを読み出したり書き込んだりする場合は、設定ファイル名は、“config”と指定します。

2.3.2 設定ファイルの読み出し

ここでは、Windows 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 198.51.100.1、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[Windows システム ツール]-[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 198.51.100.1 get config/himitsu OLDconfig.txt** と入力してから、Enter キーを押します。

設定ファイルを暗号化して読み出す場合は、ファイル名の後に“-encryption”オプションを指定します。暗号化形式を指定する場合は、“-encryption”の後に“-aes128”または“-aes256”をオプションを指定します。暗号化形式を省略した場合は、AES256 が暗号化形式として使用されます。暗号化形式を AES128 として設定ファイルを暗号化して読み出す場合は、

tftp -i 198.51.100.1 get config-encryption-aes128/himitsu OLDconfig.txt

と入力してから、Enter キーを押します

```

コマンドプロンプト
Microsoft Windows [Version 10.0.16299.1217]
(c) 2017 Microsoft Corporation. All rights reserved.

C:¥>cd YAMAHA

C:¥YAMAHA>tftp 198.51.100.1 get config/himitsu OLDconfig.txt
転送を正常に完了しました: 1 秒間に 2619 バイト、2619 バイト/秒

C:¥YAMAHA>

```

2.3.3 設定ファイルの書き込み

ここでは、Windows 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 198.51.100.1、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[Windows システム ツール]-[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 198.51.100.1 put NEWconfig.txt config/himitsu と入力してから、Enter キーを押します。

暗号化された設定されたファイル"NEWconfig.rtf"を設定ファイルに書き込む場合は、通常の設定ファイルの書き込みと同様に、

```
tftp -i 198.51.100.1 put NEWconfig.rtf config/himitsu
```

と入力してから、Enter キーを押します。

```

Microsoft Windows [Version 10.0.16299.1217]
(c) 2017 Microsoft Corporation. All rights reserved.

C:¥>cd YAMAHA

C:¥YAMAHA>tftp 198.51.100.1 put NEWconfig.txt config/himitsu
転送を正常に完了しました: 1 秒間に 2619 バイト、2619 バイト/秒

C:¥YAMAHA>
  
```

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 config tunnel**、**show config switch**、**show config ap**、**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 config tunnel**、**less config switch**、**less config ap**、**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	

キーボード操作	説明・備考
{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}行後ろに戻る
{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}半画面後ろに戻る
{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
{n} r	現在の画面の書き直し
{n} Ctrl-R	
{n} 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
```

[設定値及び初期値]

- -i: pattern 中の英大文字 / 小文字を区別せず検索する
 - [初期値]:-
- -v: pattern に一致しなかった行を表示する
 - [初期値]:-

- `-w`: *pattern* が単語に一致する時だけ表示する
 - [初期値]: -
- *pattern*
 - [設定値]: 検索パターン
 - [初期値]: -

[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'` などと一致する。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 回以上繰り返し返すパターンに一致する	ab*c	ac、abc、abbc、abbbbbbbbc
+	直前の文字が 1 回以上繰り返し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。

Rev.10.01.11 以降のリビジョンでは、コマンド実行時に "Searching ..." と表示され、対象文字列の検索中に `Ctrl + C` を入力すると表示を中止できる。

```
例 )
# show command | grep nat
Searching ...
clear nat descriptor dynamic: 動的な NAT 情報を削除します
^C
#
```

[設定例]

```
show config | grep ip | grep lan
show config | grep ip | less
```

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, 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、数値プレフィックスとコマンド文字を入力することで実行される。数値プレフィックスはオプションで省略できる。数値プレフィッ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 (数値プレフィックスを 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、数値プレフィッ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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, 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
```

```
show [...] >> name
```

[設定値及び初期値]

- *name*: ファイル名

- [設定値]:

設定値	説明
usb1:filename	USB メモリ内のファイル
sd1:filename	microSD カード内のファイル

- [初期値]:-

[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。

保存ファイルの暗号化には対応していない。

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。

```
# show log | grep IKE > usb1:log.txt
```

Rev.10.01.11 以降では、外部メモリの既存ファイルに対してリダイレクト記号 '>>' を使用することで、コマンドの実行結果を既存ファイルに追加できる。

```
# show log > usb1:log.txt          ... 新規ファイル
# show log >> usb1:(既存)log.txt ... ファイルの末尾に追加
```

また、リダイレクト記号 '>' を使用し、出力先ファイルに既存ファイル名を指定すると、ファイルを上書きしてよいかの確認メッセージが表示される。

```
# show log > usb1:(既存)log.txt
# 指定したファイルは既に存在しています。上書きしますか? (Y/N)
```

ただし、GUI のコマンド入力ページ、カスタム GUI、Lua の `rt.command` から実行した場合は確認メッセージが表示されず、強制的に上書きされる。

[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。リダイレクト記号 '>>' は、Rev.10.01.11 以降で使用可能

show 以外から始まるコマンド、**less** から始まるコマンドは適用外となる。

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。

SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降、および、Rev.11.01 系以降では、*filename* は半角 99 文字以内。上記以外の機種では、*filename* は半角 64 文字以内。

[設定例]

show log の内容を USB メモリに保存

```
# show log > usb1:log.txt
```

show techinfo の内容を microSD カードに保存

```
# show techinfo > sd1:techinfo.txt
```

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

第3章

ヘルプ

3.1 コンソールに対する簡易説明の表示

[書式]

help

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

3.2 コマンド一覧の表示

[書式]

show command

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

第 4 章

機器の設定

4.1 ログインパスワードの設定

[書式]

login password

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, 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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

4.3 管理パスワードの設定

[書式]

administrator password

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, 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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

4.5 一般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]
```

[設定値及び初期値]

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

[説明]

一般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、さもなければ **clear log** を実行するなどの操作を行うことが望ましい。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

4.6 ログイン時のパスワード認証に RADIUS を使用するか否かの設定

[書式]

```
login radius use use
no login radius use
```

[設定値及び初期値]

- *use*
 - [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: off

[説明]

ログイン時のパスワード認証に RADIUS を使用するか否かを設定する。

[ノート]

RADIUS 認証サーバーに関する以下のコマンドが正しく設定されている必要がある。

- **radius auth**
- **radius auth server**
- **radius auth port**
- **radius secret**

RTX1200 は Rev.10.01.36 以降で使用可能。

RTX810 は Rev.11.01.06 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

4.7 管理ユーザーへの移行時のパスワード認証に RADIUS を使用するか否かの設定

[書式]

administrator radius auth use

no administrator radius auth [*use*]

[設定値及び初期値]

- *use*
- [設定値]:

設定値	説明
on	ローカル認証と RADIUS 認証を併用する
only	RADIUS 認証のみ使用する
off	使用しない

- [初期値]: off

[説明]

administrator コマンドで管理ユーザーへ移行する際のパスワード認証に RADIUS を使用するか否かを設定する。

on の場合、最初に **administrator password** コマンドで設定された管理パスワードとの比較を行い、一致しなかった場合に RADIUS サーバーへの問い合わせを行う。only の場合、RADIUS サーバーへの問い合わせのみを行う。

[ノート]

RADIUS 認証サーバーに関する以下のコマンドが正しく設定されている必要がある。

- **radius auth**
- **radius auth server**
- **radius auth port**
- **radius secret**

RTX1200 は Rev.10.01.36 以降で使用可能。

RTX810 は Rev.11.01.06 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

4.8 拡張ライセンスの操作

4.8.1 拡張ライセンスのパスワードの設定

[書式]

ex-license password *password*

no ex-license password [*password*]

[設定値及び初期値]

- *password*
 - [設定値]: パスワード (半角 8 文字以上、64 文字以下)
 - [初期値]: -

[説明]

拡張ライセンスを使用するためのパスワードを設定する。

本コマンドの設定の変更、または削除によりインポート済みのライセンスが復号できなくなる場合、設定を保存してルーターを再起動したあとにライセンスが無効になる。

[ノート]

RTX830 は Rev.15.02.22 以降で使用可能。

[適用モデル]

RTX830

4.8.2 拡張ライセンスのインポート

[書式]

```
import ex-license key [key]
```

[設定値及び初期値]

- *key*: インポートするライセンスキー
 - [初期値]: -

[説明]

拡張ライセンスをインポートする。

ライセンスをインポートする前に **ex-license password** コマンドでパスワードを設定しておく必要がある。

key を省略した場合は、インポートするライセンスキーの入力を求められる。

このとき、インポートするライセンスの詳細が表示され、ライセンスのインポートを続行するか否かを選択することができる。

key を省略せずに入力した場合は、インポートを続行するか否かは問われず、正常なライセンスであれば自動的にインポートされる。

インポートしたライセンスは RTFS の `/yamaha_sys/ex-license_vpn.lic` に保存される。`yamaha_sys` ディレクトリがない場合は自動生成される。

[ノート]

RTX830 は Rev.15.02.22 以降で使用可能。

[適用モデル]

RTX830

4.8.3 拡張ライセンスの削除

[書式]

```
clear ex-license
```

[説明]

拡張ライセンスを削除する。

本コマンドを実行すると、削除するライセンスの詳細が表示され、ライセンスの削除を続行するか否かを選択することができる。ライセンスを削除するとルーターが再起動される。

[ノート]

RTX830 は Rev.15.02.22 以降で使用可能。

[適用モデル]

RTX830

4.9 ユーザーの属性を設定

[書式]

```
user attribute [user] attribute=value [attribute=value...]
```

```
no user attribute [user...]
```

[設定値及び初期値]

- *user*

- [設定値]:

設定値	説明
ユーザー名	登録されているユーザー名
*radius	RADIUS 認証でログインするすべてのユーザー
*	すべてのユーザー

- [初期値]: -

- *attribute=value*: ユーザー属性

- [設定値]:

- *administrator*: 管理者モードを使えるかどうかを示す属性

設定値	説明
on	administrator コマンドにより管理ユーザー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。管理者パスワードを用いて SFTP 接続を行うことができる。
off	administrator コマンドにより管理ユーザー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。管理者パスワードを用いて SFTP 接続を行うことができない。

- *connection*: ルーターへのアクセス方法を示す属性

設定値	説明
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。
sftp	SFTP 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。

- *gui-page*: ログインユーザーに対して閲覧を許可する GUI 画面の種別を示す属性

設定値	説明
all	ログインユーザーでアクセスできるすべての画面の閲覧を許可する。
dashboard	ダッシュボード画面の閲覧を許可する。
lan-map	LAN マップ画面の閲覧を許可する。
config	かんたん設定画面、詳細設定画面、管理画面、CONFIG 画面および TECHINFO 画面の閲覧を許可する。

- *host*: ルーターへのアクセスホストを指定する属性

設定値	説明
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 : 複数接続を許可するかどうかを示す属性

設定値	説明
on	同一ユーザー名による TELNET、SSH、HTTP での複数接続を許可する。
off	同一ユーザー名による TELNET、SSH、HTTP での複数接続を禁止する。

- login-timer : ログインタイマーの指定

設定値	説明
<ul style="list-style-type: none"> • 120..21474836 (Rev.10.00 系以降) • 30..21474836 (上記以外) 	キー入力がない場合に自動的にログアウトするまでの秒数。
clear	ログインタイマーを設定しない。

- [初期値]:
 - administrator=on
 - connection=serial,telnet,remote,ssh,sftp,http
 - gui-page=all
 - host=any
 - multi-session=on
 - login-timer=300

[説明]

ユーザーの属性を設定する。

user を省略した場合は、無名ユーザーの属性を設定する。

user に *radius を指定した場合は、RADIUS 認証でログインするすべてのユーザーの属性を設定する。

user にアスタリスク (*) を指定した場合は、すべてのユーザーに対して設定を有効にする。ただし、ユーザー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。

すでに管理ユーザーに昇格しているユーザーに対して、このコマンドで administrator 属性を off に変更しても、そのユーザーは exit コマンドにより一般ユーザーに降格するか、あるいはログアウトするまでは管理ユーザーで居続けることができる。

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。

すでに接続しているユーザーに対して、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、そのユーザーは切断するまでは接続を維持し続けることができる。

gui-page 属性では、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。本属性で設定した設定内容は、ログインユーザーとしてログインしたときのみ有効となる。管理ユーザーとしてログインした場合は、本属性の設定にかかわらず、常に GUI 上のすべての画面を閲覧する権限を持つ。すでに GUI に接続中のユーザーに対してこのコマンドで本属性の設定が変更された場合、次に GUI 上のページにアクセスした時点から新しい設定が反映される。

host 属性では、TELNET、SSH、SFTP 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、SSH、HTTP 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ー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ーに対して、このコマンドで multi-session 属性を off に変更しても、そのユーザーは切断するまでは接続を維持し続けることができる。

無名ユーザーに対しては SSH、SFTP による接続を許可することができない。

無名ユーザーに対しては TELNET での複数接続はできない。

TELNET、SSH、SFTP、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、タイム値は 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。

[ノート]

administrator 属性を **off** に設定して GUI の管理者ページへの接続を制限できるのは Rev.10.00 系以降のファームウェアである。

connection 属性に **http** を指定できるのは Rev.10.00 系以降のファームウェアである。 **sftp** を指定できるのは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.22 以降のファームウェア、および、Rev.11.01 系以降のファームウェアである。

gui-page 属性を設定できるのは、RTX1210 Rev.14.01.11 以降のファームウェア、および、RTX830、RTX1220 である。

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、すべてのユーザーの接続を禁止する、またはすべてのユーザーが管理ユーザー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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

4.10 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]
```

[設定値及び初期値]

- *user*
 - [設定値]: ユーザ名
 - [初期値]: -
- *connection*: 接続種別
 - [設定値]:

設定値	説明
telnet	TELNET による接続
serial	シリアルコンソールからの接続
remote	リモートセットアップによる接続
ssh	SSH による接続
sftp	SFTP による接続
http	GUI 設定画面への接続

- [初期値]: -
- *no*
 - [設定値]: 接続番号
 - [初期値]: -

[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。

sftp を指定できるのは Rev.10.01.22 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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

4.11 セキュリティクラスの設定

[書式]

```
security class level forget [telnet [ssh]]
```

```
no security class [level forget [telnet [ssh]]]
```

[設定値及び初期値]

- *level*

- [設定値]:

設定値	説明
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

- [初期値]: 1

- *forget*

- [設定値]:

設定値	説明
on	設定したパスワードの代わりに "w,lXlma" (ダブルユー、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

- [初期値]: on

- *telnet*

- [設定値]:

設定値	説明
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

- [初期値]: off

- *ssh*

- [設定値]:

設定値	説明
on	SSH クライアントとして ssh コマンドが使用できる
off	ssh コマンドは使用できない

- [初期値]: off

[説明]

セキュリティクラスを設定する。

ただし、本コマンドによる設定は Web GUI は対象外である。

[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。

SSH クライアント機能が実装されていないモデルでは、*ssh* キーワードは使用できない

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

4.12 タイムゾーンの設定

[書式]

timezone *timezone*

no timezone [*timezone*]

[設定値及び初期値]

- *timezone* : その地域と世界標準時との差

- [設定値] :

設定値	説明
jst	日本標準時 (+09:00)
utc	世界標準時 (+00:00)
任意の時刻 : 分	時刻 : 分 (-12:00..+11:59)

- [初期値] : jst

[説明]

タイムゾーンを設定する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

4.13 現在の日付けの設定

[書式]

date *date*

[設定値及び初期値]

- *date*
 - [設定値] : yyyy-mm-dd または yyyy/mm/dd
 - [初期値] : -

[説明]

現在の日付けを設定する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

4.14 現在の時刻の設定

[書式]

time *time*

[設定値及び初期値]

- *time*
 - [設定値] : hh:mm:ss
 - [初期値] : -

[説明]

現在の時刻を設定する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

4.15 リモートホストによる時計の設定

[書式]

rdate *host* [*syslog*]

[設定値及び初期値]

- *host*

- [設定値]:

設定値	説明
IP アドレス	リモートホストの IP アドレス (xxx.xxx.xxx.xxx(xxx は十進数))
名前	ホストの名称

- [初期値]:-

- *syslog*: 出力結果を SYSLOG へ出力することを示すキーワード

- [初期値]:-

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

4.16 NTP による時計の設定

[書式]

ntpdate *ntp_server* [*syslog*]

[設定値及び初期値]

- *ntp_server*

- [設定値]:

設定値	説明
IP アドレス	NTP サーバーの IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))
IPv6 アドレス	NTP サーバーの IPv6 アドレス (xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx.xxxx (xxx は十六進数))
名前	NTP サーバーの名称

- [初期値]:-

- *syslog*: 出力結果を SYSLOG へ出力することを示すキーワード

- [初期値]:-

[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、**rddate** 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を指定した方がよい。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。

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。

ntp_server に IPv6 アドレスを指定できるのは、RTX1100 / RTX1500 / RT107e Rev.8.03.92 以降、RTX3000 Rev.9.00.56 以降、SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.36 以降、RTX810 Rev.11.01.06 以降のファームウェア、および、Rev.14.00 系以降のすべてのファームウェアである。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

4.17 NTP パケットを送信するときの始点 IP アドレスの設定

[書式]

ntp local address *ip_address*

no ntp local address

[設定値及び初期値]

- *ip_address*
 - [設定値]: IP アドレス
 - [初期値]: -

[説明]

NTP パケットを送信するときの始点 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ときは、通常の UDP パケットの送信ルールに従い、出力インタフェースの IP アドレスを利用する。

[ノート]

RTX1100、RTX1500、RT107e は Rev.8.03.87 以降で使用可能。

RTX3000 は Rev.9.00.47 以降で使用可能。

SRT100 は Rev.10.00.48 以降で使用可能。

RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

4.18 Stratum 0 の NTP サーバーとの時刻同期を許可する設定

[書式]

ntp backward-compatibility *comp*

no ntp backward-compatibility [*comp*]

[設定値及び初期値]

- *comp*
 - [設定値]:

設定値	説明
accept-stratum-0	Stratum 0 の NTP サーバーとの時刻同期を許可する

- [初期値]: -

[説明]

Stratum 0 の NTP サーバーとの時刻同期を許可する。

[ノート]

外部クロックに同期した NTP サーバーでない限り、Stratum 0 にはならない。

RTX3000 は Rev.9.00.55 以降で使用可能。

SRT100 は Rev.10.00.61 以降で使用可能。

RTX1200 は Rev.10.01.42 以降で使用可能。

RTX810 は Rev.11.01.09 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

4.19 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*]

[設定値及び初期値]• *prompt*

- [設定値]: 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.8.02 系...16 文字以内)
- [初期値]: -

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

4.20 コンソールの言語とコードの設定

[書式]

console character *code*

no console character [*code*]

[設定値及び初期値]• *code*

- [設定値]:

設定値	説明
en.ascii (Rev.14.01 系以降)、ascii (左記以外)	英語で表示する、文字コードは ASCII
ja.sjis (Rev.14.01 系以降)、sjis (左記以外)	日本語で表示する、文字コードはシフト JIS
ja.euc (Rev.14.01 系以降)、euc (左記以外)	日本語で表示する、文字コードは EUC
ja.utf8 (Rev.14.01 系以降)	日本語で表示する、文字コードは UTF-8

- [初期値]:

- ja.sjis (Rev.14.01 系以降)
- sjis (上記以外)

[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。
Rev.14.01 系以降のファームウェアで UTF-8 の文字コードを使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

4.21 コンソールの表示文字数の設定

[書式]

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

[設定値及び初期値]

- *col*
 - [設定値]: コンソールの表示文字数
 - [設定値]:
 - 80..4096 (RTX830 Rev.15.02.14 以降、RTX1210 Rev.14.01.35 以降、RTX1220)
 - 80..200 (上記以外)
 - [初期値]: 80

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

4.22 コンソールの表示行数の設定

[書式]

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

[設定値及び初期値]

- *lines*
 - [設定値]:

設定値	説明
10..100	表示行数
infinity	スクロールを止めない

- [初期値]: 24

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

4.23 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]
```

[設定値及び初期値]

- *info*
 - [設定値]:

設定値	説明
on	表示する
off	表示しない

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

4.24 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]
```

[設定値及び初期値]

- *host*
 - [設定値]: 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)
 - [初期値]: -

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

4.25 SYSLOG ファシリティの設定

[書式]

```
syslog facility facility
no syslog facility [facility]
```

[設定値及び初期値]• *facility*

- [設定値]:

設定値	説明
0..23	facility 値
user	1
local0..local7	16..23

- [初期値]: user

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

4.26 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*]

[設定値及び初期値]• *notice*

- [設定値]:

設定値	説明
on	出力する
off	出力しない

- [初期値]: off

[説明]

各種フィルター機能等で検出したパケット情報を SYSLOG で出力するか否かを設定する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

4.27 INFO タイプの SYSLOG 出力の設定

[書式]

syslog info *info*

no syslog info [*info*]

[設定値及び初期値]• *info*

- [設定値]:

設定値	説明
on	出力する
off	出力する、ただし SYSLOG ホストへの送信は行わない

- [初期値]: on

[説明]

ルーターの動作状況に関する SYSLOG 出力の設定をする。

[ノート]

INFO タイプのログは *info* パラメータの on/off にかかわらずルーター内部に保持される。**syslog host** コマンドで設定するホストへの送信は、*info* パラメータが on の場合にのみ行われる。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

4.28 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]
```

[設定値及び初期値]

- *debug*
- [設定値]:

設定値	説明
on	出力する
off	出力しない

- [初期値]: off

[説明]

ルーターのデバッグ情報を 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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

4.29 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 address [address]
```

[設定値及び初期値]

- *address*
- [設定値]: 始点 IP アドレス
- [初期値]: -

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

4.30 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]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号 (1..65535)
 - [初期値]: 514

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

4.31 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*]

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
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

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

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

[書式]

packetdump *interface count*

packetdump pp *peer_num count*

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インターフェース名、WAN インターフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]:
 - 相手先情報番号
 - anonymous
 - [初期値]: -
- *count*
 - [設定値]:

設定値	説明
1..21474836	回数
off	ダンプを行わない
infinity	回数制限をかけない

- [初期値]: off

[説明]

`syslog debug on` が設定されている場合のみ、指定したインターフェースのパケットをダンプする。

[ノート]

本コマンドの設定は、`show config` コマンドで表示されない。

本コマンドの設定は、`save` コマンドで保存されない。電源再投入や再起動により、本コマンドの設定がクリアされる。

`count` パラメータを `infinity` にすると、大量のパケットダンプメッセージが出力されるため機器の負荷が高くなる。

すべてのパケットがダンプされるわけではない。パケットロスすることもある。

ファストパスで処理されたパケットは出力されない。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- `peer_num`

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

4.33 TELNET サーバー機能の ON/OFF の設定

[書式]

`telnetd service service`

`no telnetd service`

[設定値及び初期値]

- `service`
 - [設定値]:

設定値	説明
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

- [初期値]: on

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

4.34 TELNET サーバー機能の listen ポートの設定

[書式]

`telnetd listen port`

`no telnetd listen`

[設定値及び初期値]

- `port`
 - [設定値]: TELNET サーバー機能の待ち受け (listen) ポート番号 (1..65535)
 - [初期値]: 23

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

4.35 TELNET サーバーへアクセスできるホストの設定

[書式]

`telnetd host ip_range [ip_range...]`

`telnetd host any`

`telnetd host none`

`telnetd host lan`

`no telnetd host`

[設定値及び初期値]

- `ip_range` : TELNET サーバーへのアクセスを許可するホストの IP アドレスまたはニーモニック
 - [設定値] :

設定値	説明
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	指定したホストからのアクセスを許可する
lanN	LAN インターフェースからのアクセスを許可する
wan1	WAN インターフェースからのアクセスを許可する
bridge1	ブリッジインターフェースからのアクセスを許可する
vlanN	VLAN インターフェースからのアクセスを許可する
lanN/M	タグ VLAN インターフェースからのアクセスを許可する

- [初期値] :-
- `any`
 - [設定値] : すべてのホストからのアクセスを許可する
 - [初期値] : `any`
- `none`
 - [設定値] : すべてのホストからのアクセスを禁止する
 - [初期値] :-
- `lan`
 - [設定値] : すべての LAN 側ネットワーク内からのアクセスを許可する
 - [初期値] :-

[説明]

TELNET サーバーへのアクセスを許可するホストを設定する。

[ノート]

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は SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

WAN インタフェースは RTX1210 Rev.14.01.16 以降のファームウェア、および、RTX830、RTX1220 で指定可能。

lan キーワードは RTX1200 Rev.10.01.76 以降、RTX810 Rev.11.01.33 以降、RTX5000 / RTX3500 Rev.14.00.26 以降、RTX1210 Rev.14.01.16 以降のファームウェア、および、RTX830、RTX1220 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

4.36 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

[設定値及び初期値]

- *num*
 - [設定値]: 同時接続数 (1...8)
 - [初期値]: 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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

4.37 マスタクロック用インタフェースの設定

[書式]

line masterclock interface [interface]
no line masterclock

[設定値及び初期値]

- *interface*
 - [設定値]:

設定値	説明
BRI インタフェース名	マスタクロックを得る BRI インタフェースの選択
PRI インタフェース名	マスタクロックを得る PRI インタフェースの選択
auto	自動選択

- [初期値]: auto

[説明]

RTX3000 と RT250i 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。RTX5000 と RTX3500 では、各モジュール毎にそれぞれ 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。RTX5000 と RTX3500 では各モジュール毎にマスタクロックが必要なため、接続されているモジュールの数だけ *interface* を指定する必要がある。それ以外の機種では複数指定はできない。

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、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、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ならない。

[適用モデル]

RTX5000, RTX3500, RTX3000, RT250i

4.38 CPU 使用率の閾値の設定

[書式]

```
system cpu threshold cpu1 cpu2
no system cpu threshold [cpu1 [cpu2]]
```

[設定値及び初期値]

- *cpu1*
 - [設定値]: 警告を発する CPU 使用率の閾値の上限 (0..100 %)
 - [初期値]: -
- *cpu2*
 - [設定値]: 警告を発する CPU 使用率の閾値の下限 (0..100 %)
 - [初期値]: -

[説明]

CPU 使用率を監視して、*cpu1* 以上または *cpu2* 以下の使用率になると SYSLOG や SNMP トラップで警告を発する。SNMP トラップ送信するためには `snmp trap cpu threshold on` を設定する必要がある。

RTX5000、RTX3500 は Rev.14.00.29 以降で使用可能。RTX1210 は Rev.14.01.34 以降で使用可能。RTX830 は Rev.15.02.10 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

4.39 メモリ使用率の閾値の設定

[書式]

```
system memory threshold memory1 memory2
no system memory threshold [memory1 [memory2]]
```

[設定値及び初期値]

- *memory1*
 - [設定値]: 警告を発するメモリ使用率の閾値の上限 (0..100 %)
 - [初期値]: -
- *memory2*
 - [設定値]: 警告を発するメモリ使用率の閾値の下限 (0..100 %)
 - [初期値]: -

[説明]

メモリ使用率を監視して、*memory1* 以上または *memory2* 以下の使用率になると SYSLOG や SNMP トラップで警告を発する。

SNMP トラップ送信するためには `snmp trap memory threshold on` を設定する必要がある。

RTX5000、RTX3500 は Rev.14.00.29 以降で使用可能。RTX1210 は Rev.14.01.34 以降で使用可能。RTX830 は Rev.15.02.10 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

4.40 温度監視の閾値の設定

[書式]

```
system temperature threshold t1 t2
no system temperature threshold [t1 [t2]]
```

[設定値及び初期値]

- *t1*
 - [設定値]: 警告を発する温度 (0..100 °C)
 - [初期値]:
 - 65(RTX3000)
 - 70(RTX5000、RTX3500)
 - 75(RTX1200)
 - 80(上記以外の機種)
- *t2*
 - [設定値]: 警告を解除する温度 (0..100 °C)
 - [初期値]:
 - 60(RTX3000)
 - 65(RTX5000、RTX3500)
 - 70(RTX1200)
 - 75(上記以外の機種)

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RT250i

4.41 ファストパス機能の設定

[書式]

```
ip routing process process
no ip routing process
```

[設定値及び初期値]

- *process*
 - [設定値]:

設定値	説明
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

- [初期値]: fast

[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。

[適用モデル]

RTX5000, RTX3500, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

4.42 LAN インタフェースの動作設定

[書式]

```
lan shutdown interface [port...]
no lan shutdown interface [port...]
```

[設定値及び初期値]

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

[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。

RTX5000、RTX3500、RTX3000、RTX1220、RTX1210、RTX1200 は、このコマンドを実行すると、対象の lan インタフェースのみがリセットされる。

RTX1500、RTX1100 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。lan3 に対してこのコマンドを実行すると、lan3 インタフェースのみがリセットされる。

RTX830、RTX810、RT107e、SRT100 は、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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

4.43 HUB IC での受信オーバーフロー数を取得するか否かの設定

[書式]

lan count-hub-overflow *switch* [*interval*]

no lan count-hub-overflow [*switch* [*interval*]]

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	HUB IC での受信オーバーフロー数を定期的に取得する
off	HUB IC での受信オーバーフロー数を定期的に取得しない

- [初期値]: on
- *interval*
 - [設定値]: 受信オーバーフロー数を取得する時間間隔 [秒] (1..65535)
 - [初期値]: 120

[説明]

HUB IC での受信オーバーフロー数を定期的に取得するか否かを設定する。

[ノート]

interval に大きな値を設定するか、*switch* に off を設定することで HUB IC へのアクセスによる負荷を軽減することができる。

本コマンドの設定にかかわらず **show status lan** コマンド実行時に HUB IC での受信オーバーフロー数は取得される。

[適用モデル]

RTX810

4.44 LAN インタフェースのリンクアップ後の送信抑制時間の設定

[書式]

```
lan linkup send-wait-time interface time
no lan linkup send-wait-time interface [time]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *time*
 - [設定値]: 送信抑制秒数 (0..10)
 - [初期値]: 0 (抑制しない)

[説明]

リンクアップ後の送信抑制時間を設定し、パケットの送信を抑制する。送信を抑制されたパケットはキューに保存され、リンクアップから設定秒数の経過後に送信される。保存先のキュー長は **queue interface length** コマンドの設定に従う。

[ノート]

リンクアップ直後に Gratuitous ARP や IPv6 neighbor solicitation 等のパケットがルーターから送信されるが、その送信が早過ぎるために対向機器側で受信できない場合は、この抑制時間を適宜設定し送信を遅延させることで対向機器側で受信できるようになる。

RTX1100、RTX1500、RT107e は Rev.8.03.82 以降で使用可能。

RTX3000 は Rev.9.00.47 以降で使用可能。

SRT100 は Rev.10.00.46 以降で使用可能。

RTX1200 は Rev.10.01.11 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

4.45 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
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *mirror*
 - [設定値]: ミラーリングパケットを送出させるポート番号
 - [初期値]: -
- *direction*: 観測対象のパケットの方向
 - [設定値]:

設定値	説明
in	入る方向
out	出る方向

- [初期値]: -
- *port*
 - [設定値]: 観測対象とするポート番号
 - [初期値]: -

[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。

スニファ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スニファ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。

RTX5000、RTX3500 は、このコマンドを実行すると、対象の `lan` インタフェースのみがリセットされる。

RTX1220、RTX1210、RTX1200 は、このコマンドを実行すると、`lan1` インタフェースのみがリセットされる。

RTX1500、RTX1100、RTX830、RTX810、SRT100 は、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。

[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]

RTX5000, RTX3500, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, SRT100

4.46 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* [*option=value*...]

lan type *interface_without_swhub* *speed* [*option=value*...]

lan type *interface_without_swhub* *option=value* [*option=value*...]

no lan type *interface* [...]

[設定値及び初期値]

- *interface_with_swhub*
 - [設定値]: スイッチングハブを持つ LAN インタフェース名
 - [初期値]: -
- *interface_without_swhub*
 - [設定値]: スイッチングハブを持たない LAN インタフェース名
 - [初期値]: -
- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *speed*: LAN 速度および動作モード
 - [設定値]:

設定値	説明
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	省略時は auto

- [初期値]: auto
- *port*
 - [設定値]: スイッチングハブのポート番号

- [設定値]:
 - 省略時は全ポート
- [初期値]: -
- `option=value`: オプション機能
- [設定値]:
 - `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

設定値	説明
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

設定値	説明
秒数	エージング時間
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

設定値	説明
<code>divide-network</code>	LAN 分割機能を有効にする
<code>split-into-split_pattern</code>	ポート分離機能を有効にする(基本機能)
<code>X1,X2,X3,X4(X1..X4 は 1..4 の数字を羅列し末尾に"+"もしくは"-をつけたもの)</code>	ポート分離機能を有効にする(拡張機能)
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

設定値	説明
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

- `energy-saving`
 - 省電力機能

設定値	説明
on	省電力機能を有効にする
off	省電力機能を無効にする

- [初期値]:
 - `mtu=1500`
 - `auto-crossover=on`
 - `macaddress-aging=on` (秒数を指定できない機種)
 - `macaddress-aging=300` (秒数を指定できる機種)
 - `port-based-ks8995m/port-based-option=off`
 - `speed-downshift=on`
 - `energy-saving=on` (RTX1200)
 - `energy-saving=off` (RTX1220、RTX1210、RTX830)

[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
RTX5000、RTX3500	LAN1、LAN2、LAN3、LAN4	64~9578
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なくなる。

○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。

以下の機種では設定値に秒数を指定することができる。ただし、コマンドの設定値と実際に消去されるまでの時間に誤差が生じる場合がある。

RTX1220、RTX1210 では、設定した値からその 2 倍の時間までの間に消去される。

RTX830 では、13 秒未満の値を設定しても、実際に消去される時間が 13 秒より短くなることはない。

機種	設定範囲
RTX5000、RTX3500、RTX830	1~3825
RTX1220、RTX1210	10~630
RTX1200	1~86400
RTX810	1~3551

秒数を指定できる機種で **on** を入力すると初期値である 300 に変換される。

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
RTX5000、RTX3500、RTX1220、RTX1210、RTX1200、RTX830	8192
RTX1500、RTX1100、RTX810、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ングも可能になる。

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 個利用できるようになる。

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
RTX5000、RTX3500	vlan1-vlan4 (LAN1)、vlan5-vlan8 (LAN2)
RTX1220、RTX1210、RTX1200	vlan1-vlan8
RTX830、RTX810	vlan1-vlan4

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-vlan4 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。

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、ポート間での通信を制限することができる。

ポート分離機能には基本機能と拡張機能があり、基本機能ではポート間での通信を制限しつつ、ルーターを経由した通信が可能であり、拡張機能では指定ポートからのルーターを経由した通信も制限することができる。

拡張機能は Rev.11.01 系以降のファームウェアで利用できる。

基本機能では、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可能としつつ、他のグループのポートとは通信を制限できる。

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。

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

RTX1220、RTX1210、RTX1200 では、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_patt ern	ポ ー ト								説明
	1	2	3	4	5	6	7	8	
123:45678 (123)	←	→	↔	←	→	→	→	↔	ポート 1 -3 とそ その他
1:234:567 8 (1:234)	↔	←	→	↔	→	→	→	↔	ポート 1 とポート 2-4 とそ その他
12:34:56:7 8 (12:34:56)	←	→	←	→	←	→	↔	↔	ポート 1、 2、ポー ト 3、4、 ポート 5、 6 とそ 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。

拡張機能では、ポート毎に受信したパケットを転送するポートを指定することで、ポート間やルーター自身、ルーターを経由した通信を制限することができる。具体的には、以下のように設定する。

```
lan type lan1 port-based-option=X1,X2,X3,X4
```

Xn(n=1..4)にはポート n で受信したパケットを転送するポート番号を羅列し、ルーター自身との通信・ルーターを経由した通信を許可する場合は"+", 禁止する場合は "-" を末尾につける。ただし "+" は省略可能である。

"-" を指定した場合、そのポートで受信したパケットはルーティングされなくなる。またそのポートに接続された機器はルーターとの通信ができなくなる。

例えば以下の設定の場合、ポート 1 から 3 で受信したパケットはポート 4 とルーターに転送され、ポート 4 で受信したパケットはポート 1 から 3 に転送されるがルーターには転送されない。つまり、ポート 1 と 4、ポート 2 と 4、ポート 3 と 4 の 3 つのグループに分離された状態となり、ポート 1 から 3 はお互いのポートと通信できずポート 4

とのみ通信可能になる。また、ポート 1 から 3 はルーターと通信可能だが、ポート 4 は通信不可であり受信パケットもルーティングされない。

```
lan type lan1 port-based-option=4,4,4,123-
```

○速度ダウンシフト機能

on に設定すると 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。RTX5000、RTX3500、RTX1220、RTX1210、RTX1200、RTX830、RTX810 で利用可能。

○省電力機能

on に設定すると通信していない LAN ポートで消費電力を抑えることができる。

RTX1220、RTX1210、RTX1200、RTX830 で利用可能。

RTX1220、RTX1210、RTX830 は EEE(Energy Efficient Ethernet)に対応している。この機能を有効にするには、接続する機器も EEE をサポートしている必要がある。

RTX1200 は独自方式である。

[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。

RTX5000、RTX3500、RTX3000、RTX1220、RTX1210、RTX1200 は、このコマンドを実行すると、対象の lan インタフェースのみがリセットされる。

RTX1500、RTX1100 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。lan3 に対してこのコマンドを実行すると、lan3 インタフェースのみがリセットされる。

RTX830、RTX810、RT107e、SRT100 は、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。

RT250i は、lan1 インタフェースがリセットされる。

[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]

RTX5000、RTX3500、RTX3000、RTX1500、RTX1220、RTX1210、RTX1200、RTX1100、RTX830、RTX810、RT250i、RT107e、SRT100

4.47 スタティックリンクアグリゲーションの設定

[書式]

```
lan link-aggregation static link_id interface:port interface:port [interface:port ...]
no lan link-aggregation static link_id [interface:port ...]
```

[設定値及び初期値]

- *link_id*
 - [設定値]: リンク識別子 (1..10)
 - [初期値]: -
- *interface*
 - [設定値]: スイッチングハブを持つ LAN インタフェース名
 - [初期値]: -
- *port*
 - [設定値]: 集約対象のポート番号
 - [初期値]: -

[説明]

スイッチングハブを持つ LAN インタフェース内の複数のポートの物理リンクを集約し、一つの論理リンクを形成する。集約対象ポートに接続された複数の LAN ケーブルは、仮想的に 1 本の LAN ケーブルと見なされるようになる。なお、集約されたポートの中で実際にパケットが出力されるポートは、パケットの宛先 MAC アドレスと送信元 MAC アドレスを基に決められる。

同一の LAN インタフェースに属するポートを集約させることができる。一つのポートを複数の論理リンク (複数のリンク識別子) に従属させることはできない。

集約対象の各ポートで学習した MAC アドレスは同一の論理リンクに属する全ポートで共有され、常に一番大きいポート番号の MAC アドレステーブルに保持される。これは、一番大きいポート番号の物理リンクがダウンしている状態においても同じである。そのため、**show status switching-hub macaddress** コマンドでは常に一番大きいポート番号の欄にまとめて MAC アドレスが表示される。**show arp** コマンドや ARP ログで表示されるポート番号も同様に、MAC アドレスを学習したポートが集約対象になっている場合は常に一番大きいポート番号となる。

LAN 分割機能、ポート分離機能、ポートミラーリング機能との併用が可能である。ただし、LAN 分割機能またはポート分離機能と併用する場合は、分割または分離したスイッチポートと同一のセグメントに属するポートのみを集約させることができる。

[ノート]

パケットのループを避けるため、リンク相手機器の設定も含め、先にリンクアグリゲーションの設定を済ませてから LAN ケーブルを結線することに注意する。

RTX5000、RTX3500 は、このコマンドを実行すると、対象の lan インタフェースのみがリセットされる。

RTX1220、RTX1210 は、このコマンドを実行すると、lan1 インタフェースのみがリセットされる。

[設定例]

- LAN1 のポート 1 とポート 2 を集約する。

```
# lan link-aggregation static 1 lan1:1 lan1:2
```

- LAN1 のポート 3 とポート 4 を集約する。

```
# lan link-aggregation static 2 lan1:3 lan1:4
```

- LAN2 の 4 つのポートを集約する。

```
# lan link-aggregation static 3 lan2:1 lan2:2 lan2:3 lan2:4
```

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210

4.48 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
```

```
lan receive-buffer-size size
```

```
no lan receive-buffer-size interface [size]
```

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

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *size*
 - [設定値]: 受信パケットバッファサイズ
 - [設定値]:
 - 1..16384 (RTX5000、RTX3500)
 - 1..1000 (上記以外)
 - [初期値]:
 - 1024 (QoS 設定時は 128) (RTX5000、RTX3500)
 - 512 (RTX3000)
 - 128 (QoS 設定時は 20) (SRT100)

[説明]

LAN インタフェースの受信パケットバッファサイズ (受信キュー長) をパケットの個数で設定する。

RTX3000、SRT100 では LAN インタフェースごとの設定が必要であるため第 1 書式を使用する。RTX5000、RTX3500 では第 2 書式を使用する。RTX5000、RTX3500 では本コマンドで設定したサイズが全 CPU コアの受信処理に適用される。RTX5000、RTX3500 は 4 つの CPU コアで受信処理を行っており、各 CPU コアと LAN インタフェースは密接に結び付いていないため、LAN インタフェースごとの設定はできない。

RTX3000 以外の機種では QoS 設定の有無で初期値が変化したが、本コマンドを使用してサイズを明示的に設定している場合は、QoS 設定の有無に関係なく、常にその設定値が適用される。

[ノート]

RTX5000、RTX3500 は、Rev.14.00.18 以降で使用可能。

RTX3000 は、Rev.9.00.50 以降で使用可能。

SRT100 は、Rev.10.00.31 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, SRT100

4.49 ログインタイマの設定

[書式]

login timer *time*

no login timer [*time*]

[設定値及び初期値]

- *time*
 - [設定値]:

設定値	説明
120..21474836 (Rev.10.00 系以降)	キー入力がない場合に自動的にログアウトするまでの秒数
30..21474836 (上記以外)	
clear	ログインタイマを設定しない

- [初期値]: 300

[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、SSH、SFTP、HTTP で接続した場合、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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

4.50 TFTP によりアクセスできるホストの設定

[書式]

tftp host *ip_range* [*ip_range...*]

tftp host *any*

tftp host *none*

tftp host *lan*

no tftp host

[設定値及び初期値]

- *ip_range* : TFTP サーバーへのアクセスを許可するホストの IP アドレスまたはニーモニック
- [設定値] :

設定値	説明
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	指定したホストからのアクセスを許可する
lanN	LAN インターフェースからのアクセスを許可する
wan1	WAN インターフェースからのアクセスを許可する
bridge1	ブリッジインターフェースからのアクセスを許可する
vlanN	VLAN インターフェースからのアクセスを許可する
lanN/M	タグ VLAN インターフェースからのアクセスを許可する

- [初期値] :-
- *any*
 - [設定値] : すべてのホストからのアクセスを許可する
 - [初期値] :-
- *none*
 - [設定値] : すべてのホストからのアクセスを禁止する
 - [初期値] : none
- *lan*
 - [設定値] : すべての LAN 側ネットワーク内からのアクセスを許可する
 - [初期値] :-

[説明]

TFTP サーバーへのアクセスを許可するホストを設定する。

[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。

IP アドレスの範囲、複数キーワードの指定、LAN インターフェース、WAN インターフェース、ブリッジインターフェース、VLAN インターフェース、タグ VLAN インターフェース、lan キーワードは、RTX1210 Rev.14.01.16 以降のファームウェア、および、Rev.15.02 系以降のすべてのファームウェアで指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

4.51 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
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *relay*
 - [設定値]:

設定値	説明
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

- [初期値]: off

[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 MagicPacket 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ならない。

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。

SRT100 は、Rev.10.00.31 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, SRT100

4.52 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]
```

[設定値及び初期値]

- *id*
 - [設定値]: システム全体の説明を記述する場合の ID (1..21474836)
 - [初期値]: -
- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名、'pp'、'tunnel' のいずれか
 - [初期値]: -
- *description*

- [設定値]: 説明の文字列 (最大 64 文字/ASCII、32 文字/シフト JIS)
- [初期値]: -

[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]

RTX1100、RTX1500、RT107e、RT250i は 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、RTX1100 / RTX1500 / RT107e Rev.8.03.68 以降、RTX3000 Rev.9.00.31 以降、SRT100 Rev.10.00.31 以降のファームウェア、および、Rev.10.01 系以降のすべてのファームウェアで指定可能。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

4.53 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 [...]
```

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
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

- [初期値]: off
- *src_addr*: 始点アドレス
- [設定値]:
 - 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
 - , を区切りとして複数設定することができる。
 - FQDN

- 任意の文字列 (半角 255 文字以内。/ : は使用できない。 , は区切り文字として使われるため、使用できない)
- * から始まる FQDN は * より後ろの文字列を後方一致条件として判断する 例えば *.example.co.jp は www.example.co.jp 、 mail.example.co.jp などと一致する
- , を区切りとして複数設定することができる。
- *(すべての IP アドレス)
- [初期値]:-
- *dst_addr*: 終点アドレス
- [設定値]:
 - *src_addr* と同じ形式
 - 省略時は 1 個の * と同じ
- [初期値]:-
- *mask*: IP アドレスのビットマスク。*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。
- [設定値]:
 - "0xffffffff"のような 16 進表記
 - "/24"のようなビット数表記
 - 省略時は 0xffffffff と同じ
- [初期値]:-
- *tcpflag*: フィルタリングする TCP パケットの種類
- [設定値]:
 - 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*
 - *flag_value*, *flag_mask* は 16 進表記
 - 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
- [初期値]:-
- *src_port_list*: TCP のソースポート番号
- [設定値]:
 - ポート番号、タイプを表す 10 進数
 - ポート番号を表すニーモニック

ニーマモニツク	ポート番号
ftp	20,21
ftpdata	20
telnet	23
smtp	25
domain	53
gopher	70
finger	79
www	80
pop3	110
sunrpc	111
ident	113
ntp	123
nntp	119
snmp	161
syslog	514
printer	515
talk	517
route	520
uucp	540
submission	587

- 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
- [初期値]: -
- *dest_port_list*: TCP のデスティネーションポート番号
 - [設定値]: *src_port_list* と同じ形式
 - [初期値]: -

[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。

RTX1200 Rev.10.01.47 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで *src_port_list* または *dst_port_list* に *submission* を指定可能。

[ノート]

Rev.8.02.28 以降で使用可能。

src_addr および *dest_addr* への FQDN の指定は RTX5000 Rev.14.00.26 以降、RTX3500 Rev.14.00.26 以降、RTX1210 Rev.14.01.26 以降、RTX830 Rev.15.02.03 以降、RTX810 Rev.11.01.28 以降、RTX1220 で指定可能。

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

4.54 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]
```

[設定値及び初期値]

- *permit*
 - [設定値]:

設定値	説明
on	許可する
off	許可しない

- [初期値]: on

[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。

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。

RTX1500、RTX1100、RT107e は Rev.8.03.37 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

4.55 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]
```

[設定値及び初期値]

- *url*
 - [設定値]: ファームウェアが置いてある URL を設定する
 - [初期値]: `http://www.rtpro.yamaha.co.jp/firmware/revision-up/(機種名).bin`

[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。

[ノート]

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。

RTX1500、RTX1100、RT107e は Rev.8.03.37 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

4.56 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]]
```

[設定値及び初期値]

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

[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。

[ノート]

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。
RTX1500、RTX1100、RT107e は Rev.8.03.37 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

4.57 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]
```

[設定値及び初期値]

- *time*
 - [設定値]: タイムアウト時間 (秒)
 - [初期値]: 30

[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。

[ノート]

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。
RTX1500、RTX1100、RT107e は Rev.8.03.37 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

4.58 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]
```

[設定値及び初期値]

- *permit*
 - [設定値]:

設定値	説明
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

設定値	説明
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

- [初期値]: off

[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。

[ノート]

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

4.59 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]
```

[設定値及び初期値]

- *permit*
- [設定値]:

設定値	説明
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

- [初期値]: off

[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。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, RT107e, SRT100

4.60 リビジョンアップ実行のスケジュール

[書式]

```
http revision-up schedule period time1 time2
http revision-up schedule startup
no http revision-up schedule [period time1 time2]
no http revision-up schedule startup
```

[設定値及び初期値]

- *period*: ファームウェアのリビジョンアップを試みるスケジュールを設定する。
- [設定値]:

設定値	説明
daily	毎日

設定値	説明
weekly day	毎週 day は曜日を表す文字列で、以下のいずれか sun,mon,tue,wed,thu,fri,sat
monthly date	毎月 date は 1~31 の数字で月内の日を表す

- [初期値]:-
- *time1,time2*: リビジョンアップを試みる時間帯を設定する。
 - [設定値]: *time1,time2* は 24 時間制で、HH:MM 形式で指定する。
 - [初期値]:-

[説明]

ファームウェアのリビジョンアップを試みるスケジュールを設定する。

period ではリビジョンアップを試みる間隔を指定する。毎日、毎週、毎月の指定をそれぞれ、*daily*、*weekly*、*monthly* で指定する。*weekly*、*monthly* の場合はそれぞれ曜日、日の指定が必要になる。

monthly の場合で、指定した日とその月に存在しない場合には、その月にはリビジョンアップは試みられない。たとえば、'*monthly 31*' と指定した場合、31 日が存在しない 2 月、4 月、6 月、9 月、11 月にはリビジョンアップは試みられない。

time1、*time2* ではリビジョンアップを試みる時間帯を設定する。*time1* で指定した時刻から *time2* で指定した時刻の間のランダムな時刻に 1 回だけ、リビジョンアップを試みる。そこでリビジョンアップできなかった場合には、次の日/週/月までリビジョンアップは行われない。

time1 で指定した時刻が *time2* で指定した時刻より遅い場合には、*time2* は翌日の時刻と解釈される。

http revision-up schedule startup コマンドでは起動時に 1 回だけ、リビジョンアップを試みる。そこでリビジョンアップできなかった場合には、次の起動までリビジョンアップは行われない。

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、ファームウェアのリビジョンアップは行わない。

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。

[ノート]

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。

RTX1500、RTX1100、RT107e は Rev.8.03.80 以降で使用可能。

SRT100 は Rev.10.00.44 以降で使用可能。

RTX1200 は Rev.10.01.11 以降で使用可能。

startup は RTX5000、RTX3500 は Rev.14.00.29 以降、RTX1210 Rev.14.01.34 以降、RTX830 Rev.15.02.10 以降、RTX1220 のファームウェアで使用可能。

[設定例]

```
http revision-up schedule daily 23:00 02:00 # 毎日、23 時から翌日 2 時までの間
http revision-up schedule weekly sun 12:00 13:00 # 日曜日の昼 12 時から 13 時までの間
http revision-up schedule monthly 1 23:00 0:00 # 毎月 1 日の 23 時から 24 時までの間
http revision-up schedule startup # 起動時
```

[適用モデル]

RTX5000, RTX3500, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

4.61 SSH サーバー機能の ON/OFF の設定

[書式]

```
sshd service service
```

no sshd service [*service*]

[設定値及び初期値]

- *service*
 - [設定値]:

設定値	説明
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

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

4.62 SSH サーバー機能の listen ポートの設定

[書式]

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

[設定値及び初期値]

- *port*
 - [設定値]: SSH サーバー機能の待ち受け (listen) ポート番号 (1..65535)
 - [初期値]: 22

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

4.63 SSH サーバーへアクセスできるホストの設定

[書式]

sshd host *ip_range* [*ip_range...*]
sshd host *any*
sshd host *none*
sshd host *lan*
no sshd host

[設定値及び初期値]

- *ip_range*: SSH サーバーへのアクセスを許可するホストの IP アドレスまたはニーモニック
 - [設定値]:

設定値	説明
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	指定したホストからのアクセスを許可する
lanN	LAN インターフェースからのアクセスを許可する
wan1	WAN インターフェースからのアクセスを許可する

設定値	説明
bridge1	ブリッジインターフェースからのアクセスを許可する
vlanN	VLAN インターフェースからのアクセスを許可する
lanN/M	タグ VLAN インターフェースからのアクセスを許可する

- [初期値]: -
- *any*
 - [設定値]: すべてのホストからのアクセスを許可する
 - [初期値]: any
- *none*
 - [設定値]: すべてのホストからのアクセスを禁止する
 - [初期値]: -
- *lan*
 - [設定値]: すべての LAN 側ネットワーク内からのアクセスを許可する
 - [初期値]: -

[説明]

SSH サーバーへのアクセスを許可するホストを設定する。

[ノート]

設定後の新しい SSH 接続から適用される。

WAN インタフェースは RTX1210 Rev.14.01.16 以降のファームウェア、および、RTX830、RTX1220 で指定可能。ブリッジインタフェースは SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

lan キーワードは RTX5000 / RTX3500 Rev.14.00.32 以降、RTX1210 Rev.14.01.16 以降のファームウェア、および、RTX830、RTX1220 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

4.64 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]
```

[設定値及び初期値]

- *num*
 - [設定値]: 同時接続数 (1..8)
 - [初期値]: 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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

4.65 SSH サーバーホスト鍵の設定

[書式]

```
sshd host key generate [bit=bit]
no sshd host key generate [...]
```


[設定値及び初期値]

- *bit*
 - [設定値]: 鍵のビット長(1024, 2048)
 - [初期値]:
 - 1024(RTX5000、RTX3500、RTX1210、RTX1200、RTX810)
 - 2048(RTX1220、RTX830)

[説明]

SSH サーバーのホスト鍵を設定する。
bit パラメータによって、生成する鍵のビット数を指定できる。

[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。
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、1024 ビット鍵では数秒から 数分程度、2048 ビット鍵では数分から十数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 [bit=*bit*] KEY1 KEY2 KEY3** という形式で保存される。
KEY1 ~ KEY3 は、秘密鍵を機器固有の方式で暗号化した文字列である。

[ノート]

bit キーワードは、RTX1200 Rev.10.01.71 以降、RTX810 Rev.11.01.28 以降、RTX5000 / RTX3500 Rev.14.00.21 以降、RTX1210 Rev.14.01.11 以降のファームウェア、および、Rev.15.02 系以降のすべてのファームウェアで使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

4.66 SSH サーバーホスト鍵の表示

[書式]

```
show sshd host key [type=fingerprint [hash_algorithm]]
```

[設定値及び初期値]

- *fingerprint*: 鍵指紋を表示することを示すキーワード
 - [初期値]: -
- *hash_algorithm*: 鍵指紋を表示する際に使用するハッシュ関数のアルゴリズム
 - [設定値]:

設定値	説明
md5	MD5
sha256	SHA-256

- [初期値]: sha256

[説明]

SSH サーバーのホスト鍵を表示する。
fingerprint キーワードを指定した場合は、公開鍵の鍵長と鍵指紋を表示する。

[ノート]

RTX5000 は Rev.14.00.32 以降で使用可能。
RTX3500 は Rev.14.00.32 以降で使用可能。
RTX1210 は Rev.14.01.35 以降で使用可能。
RTX830 は Rev.15.02.14 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

4.67 SSH サーバーで利用可能な暗号アルゴリズムの設定

[書式]

sshd encrypt algorithm *algorithm* [*algorithm* ...]**no sshd encrypt algorithm** [...]

[設定値及び初期値]

- *algorithm* : 暗号アルゴリズム (空白で区切って複数指定可能)
- [設定値]:

設定値	説明
aes128-ctr	AES128-CTR
aes192-ctr	AES192-CTR
aes256-ctr	AES256-CTR
aes128-cbc	AES128-CBC
aes192-cbc	AES192-CBC
aes256-cbc	AES256-CBC
3des-cbc	3DES-CBC
blowfish-cbc	Blowfish-CBC (RTX1210 の Rev.14.01.34 以降、および、RTX830 の Rev.15.02.10 以降、RTX1220 では非対応)
cast128-cbc	CAST-128-CBC (RTX1210 の Rev.14.01.34 以降、および、RTX830 の Rev.15.02.10 以降、RTX1220 では非対応)
arcfour	Arcfour (RTX1210 の Rev.14.01.34 以降、および、RTX830 の Rev.15.02.10 以降、RTX1220 では非対応)

- [初期値] : aes128-ctr aes192-ctr aes256-ctr

[説明]

SSH サーバーで利用可能な暗号アルゴリズムを設定する。

algorithm で指定した暗号アルゴリズムのリストを SSH 接続時にクライアントへ提案する。

[ノート]

algorithm で指定した暗号アルゴリズムをクライアントがサポートしていない場合には、そのクライアントと SSH による接続ができない。

RTX1100、RTX1500、RT107e は Rev.8.03.82 以降で使用可能。

RTX3000 は Rev.9.00.47 以降で使用可能。

SRT100 は Rev.10.00.46 以降で使用可能。

RTX1200 は Rev.10.01.11 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

4.68 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* ...]

[設定値及び初期値]

- *switch*

- [設定値]:

設定値	説明
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

- [初期値]: off
- *interval*
 - [設定値]: 送信間隔の秒数 (1..2147483647)
 - [初期値]: 100
- *count*
 - [設定値]: 試行回数 (1..2147483647)
 - [初期値]: 3

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

4.69 SSH サーバー応答に含まれる OpenSSH のバージョン情報の非表示設定

[書式]

```
sshd hide openssh version use
```

```
no sshd hide openssh version [use]
```

[設定値及び初期値]

- *use*
 - [設定値]:

設定値	説明
on	SSH バージョン情報を表示しない
off	SSH バージョン情報を表示する

- [初期値]: off

[説明]

SSH 接続時のサーバー応答に含まれる OpenSSH のバージョン情報を表示するか否かを設定する。このコマンドはセキュリティ目的として OpenSSH のバージョン情報を隠したい場合に使用する。このコマンドを on に設定した場合は、"SSH-2.0-OpenSSH" と通知する。

[ノート]

このバージョン情報は、SSH 接続時にサーバーとクライアントのプロトコルの互換性を調整するために使用される。このコマンドを ON に設定することにより、クライアントソフトによっては、接続できなくなる可能性がある。その場合には、クライアントソフトを変更するか、このコマンドを OFF に設定する。

RTX1210 は Rev.14.01.09 以降で使用可能。

RTX5000、RTX3500 は Rev.14.00.18 以降で使用可能。

RTX810 は Rev.11.01.25 以降で使用可能。

RTX1200 は Rev.10.01.65 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

4.70 SSH サーバーで利用可能な認証方式の設定

[書式]

```
sshhd auth method all
sshhd auth method method [method]
no sshhd auth method [...]
```

[設定値及び初期値]

- *all*: パスワード認証、および、公開鍵認証を受け入れる
 - [初期値]: *all*
- *method*
 - [設定値]:

設定値	説明
password	パスワード認証を受け入れる
publickey	公開鍵認証を受け入れる

- [初期値]: -

[説明]

SSH サーバーで利用可能な認証方式を設定する。
パスワード認証より公開鍵認証が安全な認証方式である。

[ノート]

本コマンドが使用できないファームでは、**sshhd auth method password** 相当の動作となります。
RTX5000 は Rev.14.00.32 以降で使用可能。
RTX3500 は Rev.14.00.32 以降で使用可能。
RTX1210 は Rev.14.01.35 以降で使用可能。
RTX830 は Rev.15.02.14 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

4.71 SSH サーバーの公開鍵認証に用いる公開鍵情報を保存するファイルの設定

[書式]

```
sshhd authorized-keys filename [user] path=path
no sshhd authorized-keys filename [user] [path=path]
```

[設定値及び初期値]

- *user*: 登録されているユーザー名
 - [初期値]: -
- *path*: SSH クライアントの公開鍵を格納したファイル名
 - [初期値]:
 - /ssh/authorized_keys/ユーザー名 (登録されているユーザーの場合)
 - /ssh/authorized_keys/no.name (無名ユーザーの場合)

[説明]

SSH クライアントの公開鍵を格納したファイル (*authorized_keys* ファイル) を設定する。ユーザーが公開鍵認証する際に使用する。

本コマンドを設定する場合、無名ユーザー以外は事前に **login user** コマンドでユーザーを登録しておく必要がある。登録されていないユーザーに対して本コマンドを設定するとエラーになる。

user を省略した場合は、無名ユーザーに対する設定となる。

公開鍵認証を使用する場合は、あらかじめ許可する SSH クライアントの公開鍵をファイルに格納しておく必要がある。対応しているファイルのフォーマットは以下のとおり。

- 各行にひとつの公開鍵を格納する。

- 1つの公開鍵は、"(公開鍵の種類) (base64 エンコードされた鍵本体) (鍵のコメント)"の順に記載する。
- ファイルには 33 個まで公開鍵を登録できる。34 個目以降の公開鍵は無視する。
- 空行や#で始まる行は無視する。
- 1行の長さは、4094 文字 (改行コードを除く) まで対応する。4094 文字より長い行は無視する。
- 改行コードは、CR+LF、LF、CR に対応する。最終行の場合は改行がなくてもよい。
- ファイルの文字コードは、ASCII に対応する。
- 公開鍵の種類には、ecdsa-sha2-nistp256、ecdsa-sha2-nistp384、ecdsa-sha2-nistp521、ssh-ed25519、ssh-dss、ssh-rsa(※)を設定できる。
 - ※ssh-rsa の鍵長は、1024bit、2048bit、4096bit に対応する。
- OpenSSH の `authorized_keys` ファイルではオプションを指定できるが対応しない。オプションの記載を無視する。

[サンプル]

例:RSA 2048bit の公開鍵の場合

```
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEA3eK3sk60fhHP9zsRgI39tqAoNfljbnCNiJ7horhwu6
1ZyaKDKf8BiiCsKnvFsLI fSgcOejllflBtrFX3bN8iu+me2Ggh52vuIWDS/SUEQNWcYCalY0Ign8u80
zVxldx1QABzuAKEKA654gkhQA40iaCKbKD5RGp4zujqDA6p8Y9o06pC/Ns7GzkgegrMxg40feB+0hjs
+K2eY49uqqwqYUYCdNw6bTIJiH6nAgsXSUDjbo3N+b9CY/9/7txKBykt1zt04WCXepngxVRw2ss+JOV
kPisDmt10//Q7Xdi+MxiLKhjeZk3jppqrSHiLon6D30xU/5/FY0cwcRBwrj4Uuw== user1
```

例:ECDSA 256bit の公開鍵の場合

```
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBP211Vy
IP8Bg+r8rZhNmRq+ber0+sOaYCsVm5TN1CGt5WpCNkpwkV3c3rxwA6GAqGxuJsSn4J6Bo1mABhHg+YH
M= user2
```

login user コマンドで登録されていないユーザーから接続された場合は、無名ユーザーとして公開鍵認証を試みる。

[ノート]

RTX5000 は Rev.14.00.32 以降で使用可能。

RTX3500 は Rev.14.00.32 以降で使用可能。

RTX1210 は Rev.14.01.35 以降で使用可能。

RTX830 は Rev.15.02.14 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

4.72 SSH サーバーの公開鍵認証に用いる公開鍵の設定

[書式]

```
import sshd authorized-keys [user]
```

[設定値及び初期値]

- *user*
 - [設定値]: 登録されているユーザー名
 - [初期値]: -

[説明]

SSH クライアントの公開鍵を格納したファイル (`authorized_keys` ファイル) に設定を追加する。

本コマンドを実行する場合、無名ユーザー以外は事前に **login user** コマンドでユーザーを登録しておく必要がある。登録されていないユーザーに対して本コマンドを設定するとエラーになる。

user を省略した場合は、無名ユーザーに対する設定となる。

sshd authorized-keys filename コマンドで指定した `authorized_keys` ファイルに対して設定を追加する。

`authorized_keys` ファイルやディレクトリが存在しない場合は、新規に作成する。

コマンド入力後にプロンプトに応じて公開鍵を 1 つ入力する。入力した公開鍵が、`authorized_keys` ファイルに追加書き込みされる。公開鍵は、"(公開鍵の種類) (base64 エンコードされた鍵本体) (鍵のコメント)"の順に記載する。4094 文字まで入力できる。

公開鍵のフォーマットは、**sshd authorized-keys filename** コマンドと同様である。

`authorized_keys` ファイルを削除または初期化したいときは、**delete** コマンドを使用する。

[ノート]

RTX5000 は Rev.14.00.32 以降で使用可能。
 RTX3500 は Rev.14.00.32 以降で使用可能。
 RTX1210 は Rev.14.01.35 以降で使用可能。
 RTX830 は Rev.15.02.14 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

4.73 SSH サーバーの公開鍵認証に用いる公開鍵の表示

[書式]

```
show sshd authorized-keys [user] [type=fingerprint [hash_algorithm]]
show sshd authorized-keys * [type=fingerprint [hash_algorithm]]
```

[設定値及び初期値]

- *user* : 登録されているユーザー名
 - [初期値] : -
- *fingerprint* : 鍵指紋を表示することを示すキーワード
 - [初期値] : -
- *hash_algorithm* : 鍵指紋を表示する際に使用するハッシュ関数のアルゴリズム
 - [設定値] :

設定値	説明
md5	MD5
sha256	SHA-256

- [初期値] : sha256
- * : 全ユーザー
 - [初期値] : -

[説明]

SSH クライアントの公開鍵を格納したファイル (*authorized keys* ファイル) を表示する。

fingerprint を指定した場合は、公開鍵の鍵長と鍵指紋を表示する。

第 1 書式では、ユーザーに対応した *authorized_keys* ファイルを表示する。*user* を省略した場合は、無名ユーザーの情報を表示する。

第 2 書式では、全ユーザーの *authorized_keys* ファイルを表示する。

[ノート]

RTX5000 は Rev.14.00.32 以降で使用可能。
 RTX3500 は Rev.14.00.32 以降で使用可能。
 RTX1210 は Rev.14.01.35 以降で使用可能。
 RTX830 は Rev.15.02.14 以降で使用可能。

[設定例]

例: RSA 2048bit の公開鍵を表示する場合

```
# show sshd authorized-keys user1
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAp3eK3sk60fhHP9zsRgI39tqAoNfljbnCNiJ7horhwu6
1ZyaKDKf8BiiCsKnvFsLifSgcOejllflBtrFX3bN8iu+me2Ggh52vuIWDS/SUEQNWcYCaLY0Ign8u80
zVxldx1QABzuAKEKA654gkhQA40iaCKbKD5RGp4zujqDA6p8Y9o06pC/Ns7GzkgegrMxg40feB+0hjs
+K2eY49uqqwqYUYCdNw6bTlJiH6nAgsXSUDjbo3N+b9CY/9/7txKBykt1zt04WCXepngxVRw2ss+JOV
kPisDmtl0//Q7Xdi+MxiLKhjeZk3jppqrSHiLon6D30xU/5/FY0cwcRBwrj4Uuw== user1
```

例:RSA 2048bit の公開鍵の鍵指紋を SHA-256 で表示した場合

```
# show sshd authorized-keys user1 type=fingerprint sha256
2048 SHA256:uk2janKfeZXBsUniTmdNwL2fhdcAdfy0MsGSsCtpg8E user1 (RSA)
```

```

例:RSA 2048bit の公開鍵の鍵指紋を MD5 で表示した場合
# show sshd authorized-keys user1 type=fingerprint md5
2048 MD5:6e:fe:21:cc:d2:a4:55:78:07:7f:7f:f7:59:17:56:3a user1 (RSA)

例:全ユーザーを表示した場合
# 無名ユーザーと user1, user2, user3 が存在している。
# user2 は、sshd authorized-keys filename コマンドでファイルの置き場所を変更している。
# user3 は、authorized_keys ファイルが存在しない。

# show sshd authorized-keys * type=fingerprint sha256
(noname) /ssh/authorized_keys/no.name
2048 SHA256:fMlGwY5YlQvz9xEObkDXaO7TuvIlgFIAkmV0K2MGbyU (RSA)

user1 /ssh/authorized_keys/user1
2048 SHA256:uk2janKfeZXBsUniTmdNwL2fhdcAdfY0MsGSsCtpg8E user1 (RSA)

user2 /pub-key
2048 SHA256:Ul7sScopCUNPA5IndPWzHhkANqr3PkD2k3GMv0qS5NA user2 (RSA)

user3 /ssh/authorized_keys/user3
/ssh/authorized_keys/user3 : ファイルデータの読み込みに失敗しました。 : No such
file or directory
    
```

[適用モデル]
 RTX5000, RTX3500, RTX1220, RTX1210, RTX830

4.74 SFTP サーバーへアクセスできるホストの設定

[書式]

- sftpd host** *ip_range* [*ip_range...*]
- sftpd host** *any*
- sftpd host** *none*
- sftpd host** *lan*
- no sftpd host**

[設定値及び初期値]

- *ip_range* : SFTP サーバーへのアクセスを許可するホストの IP アドレスまたはニーモニック
 - [設定値]:

設定値	説明
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	指定したホストからのアクセスを許可する
lanN	LAN インターフェースからのアクセスを許可する
wan1	WAN インターフェースからのアクセスを許可する
bridge1	ブリッジインターフェースからのアクセスを許可する
vlanN	VLAN インターフェースからのアクセスを許可する
lanN/M	タグ VLAN インターフェースからのアクセスを許可する

- [初期値]: -
- *any*
 - [設定値]: すべてのホストからのアクセスを許可する
 - [初期値]: -
- *none*
 - [設定値]: すべてのホストからのアクセスを禁止する
 - [初期値]: none
- *lan*
 - [設定値]: すべての LAN 側ネットワーク内からのアクセスを許可する
 - [初期値]: -

[説明]

SFTP サーバーへのアクセスを許可するホストを設定する。

[ノート]

対象となるホストは **ssh host** コマンドでもアクセスが許可されていなければならない。

設定後の新しい SFTP 接続から適用される。

SRT100 は Rev.10.00.60 以降で使用可能。

RTX1200 は Rev.10.01.22 以降で使用可能。

WAN インタフェースは RTX1210 Rev.14.01.16 以降のファームウェア、および、RTX830、RTX1220 で指定可能。

ブリッジインタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

lan キーワードは RTX5000 / RTX3500 Rev.14.00.32 以降、RTX1210 Rev.14.01.16 以降のファームウェア、および、RTX830、RTX1220 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

4.75 SSH クライアント

[書式]

```
ssh [-p port] [-e escape] [user@]host
```

[設定値及び初期値]

- *port*
 - [設定値]: リモートホストのポート番号
 - [初期値]: 22
- *escape*
 - [設定値]: エスケープ文字の文字コード (0 ... 255)
 - [初期値]: 126 (~)
- *user*
 - [設定値]: リモートホストにログインする際に使用するユーザー名
 - [初期値]: -
- *host*
 - [設定値]: リモートホストのホスト名、または IP アドレス
 - [初期値]: -

[説明]

SSH を実行し、指定したホストにリモートログインする。

user を省略した場合、ルーターにログインした際に入力したユーザ名を使用して SSH サーバーへのアクセスを試みる。

host に IPv6 アドレスを指定する場合には、"**[**"、"**]**" で IP アドレスを囲む。

escape で指定したエスケープ文字は行頭に入力されたときだけ、エスケープ文字として認識される。エスケープ文字に続けてピリオド(.)が入力された場合、強制的に接続を閉じる。行頭からエスケープ文字を 2 回続けて入力した場合には、この文字が 1 回だけサーバに送られる。

実行例は以下の通り。

リモートホスト (192.168.1.1、ポート:10022) へアクセスする。

```
# ssh -p 10022 user@192.168.1.1
```

リモートホスト (2001:1::1) へアクセスする。

```
# ssh user@[2001:1::1]
```

[ノート]

RTX1200 は Rev.10.01.42 以降で使用可能。 RTX810 は Rev.11.01.12 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

4.76 SCP クライアント**[書式]**

```
scp [[user@]host:]file1 [[user@]host:]file2 [port]
```

[設定値及び初期値]

- *user*
 - [設定値]: リモートホストにログインする際に使用するユーザー名
 - [初期値]: -
- *host*
 - [設定値]: リモートホストのホスト名、または IP アドレス
 - [初期値]: -
- *file1*
 - [設定値]: 転送元ファイル名
 - [初期値]: -
- *file2*
 - [設定値]: 転送先ファイル名
 - [初期値]: -
- *port*
 - [設定値]: リモートホストのポート番号
 - [初期値]: 22

[説明]

SCP を実行する。

file1 または *file2* のどちらか一方はリモートホスト上のファイルを指定し、もう一方にはルータのファイルシステムにあるファイルを指定する。

file1、*file2* の両方にリモートホストのファイルを指定することはできない。

同様に *file1*、*file2* の両方にルータのファイルシステムにあるファイルを指定することはできない。

RTFS および外部メモリにあるファイルを指定する場合、*user* および *host* を省略し *file* のみを絶対パスで指定する。

ルータの設定ファイル (*config*、*config0*~*config4*) やファームウェア (*exec*、*exec0*、*exec1*) を指定する場合には、*file* に "config" や "exec0" のようにファイル名のみを指定する。

host に IPv6 アドレスを指定する場合には、"[", "]" で IP アドレスを囲む。

実行例は以下の通り。

リモートホスト (192.168.1.1) から、ルータの *exec0* にファイルをコピーする。

```
# scp user@192.168.1.1:rtx1200.bin exec0
```

ルータ上のファイル *usb1:/log.txt* を、リモートホスト (2001:1::1) へコピーする。

```
# scp usb1:/log.txt user@[2001:1::1]:log.txt
```

[ノート]

RTX1200 は Rev.10.01.42 以降で使用可能。 RTX810 は Rev.11.01.12 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

4.77 SSH クライアントで利用可能な暗号アルゴリズムの設定**[書式]**

```
ssh encrypt algorithm algorithm [algorithm...]
```

```
no ssh encrypt algorithm [algorithm...]
```

[設定値及び初期値]

- *algorithm*: 暗号アルゴリズム(空白で区切って複数指定可能)

- [設定値]:

設定値	説明
aes128-ctr	AES128-CTR
aes192-ctr	AES192-CTR
aes256-ctr	AES256-CTR
aes128-cbc	AES128-CBC
aes192-cbc	AES192-CBC
aes256-cbc	AES256-CBC
3des-cbc	3DES-CBC
blowfish-cbc	Blowfish-CBC (RTX1210 の Rev.14.01.34 以降、および、RTX830 の Rev.15.02.10 以降、RTX1220 では非対応)
cast128-cbc	CAST-128-CBC (RTX1210 の Rev.14.01.34 以降、および、RTX830 の Rev.15.02.10 以降、RTX1220 では非対応)
arcfour	Arcfour (RTX1210 の Rev.14.01.34 以降、および、RTX830 の Rev.15.02.10 以降、RTX1220 では非対応)

- [初期値]: aes128-ctr aes192-ctr aes256-ctr

[説明]

SCP クライアントで利用可能な暗号アルゴリズムを設定する。

algorithm で指定した暗号アルゴリズムのリストを SSH 接続時にサーバーに提案する。

[ノート]

algorithm で指定した暗号アルゴリズムをサーバーがサポートしていない場合には、そのサーバーと SSH による接続ができない。

RTX1200 は Rev.10.01.42 以降で使用可能。 RTX810 は Rev.11.01.12 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

4.78 SSH サーバーの公開鍵情報を保存するファイルの設定

[書式]

ssh known hosts *file*

no ssh known hosts [*file*]

[設定値及び初期値]

- *file*
 - [設定値]: SSH サーバーの公開鍵情報を保存するファイル名
 - [初期値]: /ssh/known_hosts

[説明]

SSH サーバーの公開鍵情報を保存するファイルを指定する。

[ノート]

RTX1200 は Rev.10.01.42 以降で使用可能。 RTX810 は Rev.11.01.12 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

4.79 パケットバッファのパラメータを変更する

[書式]

system packet-buffer *group* *parameter=value* [*parameter=value ...*]

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

[設定値及び初期値]

- *group* : パケットバッファのグループを指定する。
 - [設定値] : グループ名 (small, middle, large, jumbo, huge)
 - [初期値] : -
- *parameter* : 変更するパラメータを指定する。
 - [設定値] :

設定値	説明
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

- [初期値] : -
- *value*
 - [設定値] : 変更する値を指定する。
 - [初期値] :

RTX1100、RT107e、SRT100

group	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

RTX810

group	max-buffer	max-free	min-free	buffer-in-chunk	init-chunk
small	1248	468	31	312	1
middle	3332	1249	83	833	1
large	4992	1404	31	312	4
huge	20	0	0	1	0

RTX1220、RTX1210、RTX1200、RTX830

group	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

group	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

group	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

RTX5000、RTX3500

group	max-buffer	max-free	min-free	buffer-in-chunk	init-chunk
small	10000	3750	250	2500	1
middle	26664	9999	666	6666	1
large	40000	11250	250	2500	4
jumbo	40000	11250	250	2500	4
huge	20	0	0	1	0

[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。

- $\text{max-buffer} \geq \text{max-free}$
- $\text{max-free} > \text{min-free}$
- $\text{max_free} \geq \text{buffer-in-chunk}$
- $\text{max_free} \geq \text{buffer-in-chunk} \times \text{init-chunk}$

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。

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

4.80 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

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
on	鳴らす
off	鳴らさない

- [初期値]: on

[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。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

4.81 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

[設定値及び初期値]

- *switch*

- [設定値]:

設定値	説明
on	鳴らす
off	鳴らさない

- [初期値]: on

[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。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

4.82 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]

[設定値及び初期値]

- *switch*

- [設定値]:

設定値	説明
on	鳴らす
off	鳴らさない

- [初期値]: on

[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。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

4.83 バッチファイル実行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 batch switch

no alarm batch

[設定値及び初期値]

- *switch*

- [設定値]:

設定値	説明
on	鳴らす

設定値	説明
off	鳴らさない

- [初期値] : on

[説明]

バッチファイル実行機能に関連するアラーム音を鳴らすか否かを選択する。

[ノート]

RTX1200 は Rev.10.01.11 以降で使用可能

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

4.84 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*]

[設定値及び初期値]

- *switch*
 - [設定値] :

設定値	説明
on	鳴らす
off	鳴らさない

- [初期値] : off
- *pattern*
 - [設定値] : アラーム音のパターン (1...3、省略時は 1)
 - [初期値] : -

[説明]

起動時にアラーム音を鳴らすか否かを選択する。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

4.85 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*]

[設定値及び初期値]

- *switch*
 - [設定値] :

設定値	説明
on	鳴らす
off	鳴らさない

- [初期値] : on

[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。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

4.86 LED の輝度を調整する

[書式]

```
system led brightness mode
no system led brightness [mode]
```

[設定値及び初期値]

- *mode*
- [設定値]:

設定値	説明
0	明るい
1	暗い

- [初期値]: 0

[説明]

LED の輝度を調整する。

[適用モデル]

RTX1200, RTX810

4.87 環境変数の設定

[書式]

```
set name=value
no set name[=value]
```

[設定値及び初期値]

- *name*
 - [設定値]: 環境変数名
 - [初期値]: -
- *value*
 - [設定値]: 設定値
 - [初期値]: -

[説明]

ルーターの環境変数を設定する。

環境変数名の命名規則は次の通りである。

半角の英数字とアンダースコア '_' が使用でき、先頭は必ず英文字でなければならない。

変数名の長さには制限はないが、**set** コマンドはコマンドラインの最大長 (4095 文字) を超えて実行できない。

英文字の大文字、小文字を区別する。例えば、**abc** と **Abc** は別の環境変数として扱われる。

value に空白等の特殊文字を含む場合は、*value* 全体を引用符で囲む必要がある。

[ノート]

SRT100 は Rev.10.00.52 以降で使用可能。 RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

4.88 エイリアスの設定

[書式]

```
alias name=value
no alias name[=value]
```

[設定値及び初期値]

- *name*
 - [設定値]: エイリアス名
 - [初期値]: -

- *value*
 - [設定値]: 設定値
 - [初期値]: -

[説明]

エイリアスを設定する。

エイリアスの命名規則は次の通りである。

半角の英数字とアンダースコア '_' が使用でき、先頭は必ず英文字でなければならない。
英文字の大文字、小文字を区別する。例えば、`abc` と `Abc` は別のエイリアスとして扱われる。
value に空白等の特殊文字を含む場合は、*value* 全体を引用符で囲む必要がある。

[ノート]

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。

RTX1210 は Rev.14.01.26 以降で使用可能。

RTX830 は Rev.15.02.03 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

4.89 マクロの設定

[書式]

```
macro [-v] [-x] name <<eom
no macro [-v] [-x] name [<<eom]
```

[設定値及び初期値]

- *-v*
 - [設定値]: 展開前の内容を表示しながら実行する
 - [初期値]: -
- *-x*
 - [設定値]: 展開した後の行を表示しながら実行する
 - [初期値]: -
- *name*
 - [設定値]: マクロ名
 - [初期値]: -
- *eom*
 - [設定値]: マクロの終端文字列
 - [初期値]: -

[説明]

マクロを設定する。

このコマンド入力後はマクロ入力状態になるので、マクロの内容を入力していく。マクロの最後には、*eom* で指定した終端文字列だけを入力すれば、マクロ入力が終了する。

マクロ入力中でも、Ctrl-C を入力すればコマンドを中断できる。

-v オプションを指定すると、マクロを実行するときに実行する各行について、環境変数とエイリアスの展開前の内容を表示しながら実行する。

-x オプションは、環境変数とエイリアスを展開した後の行を表示しながらマクロを実行する。

name に使用できる文字は、半角の英大文字、英小文字、数字、アンダースコア (`_`) のみで、先頭は必ず英文字でなければならない。

実行例は以下の通り。

```
# macro sample <<EOM
show ip route
```



```
show ip connection
EOM
#
```

[ノート]

複数行からなるコマンドに対応していないため、**schedule at** コマンドからは実行できない。

Lua スクリプトの `rt.command()` で複数行からなるコマンドを実行する場合には、各行を改行文字（'\n'）で連結した文字列をコマンドとして渡す。改行文字は '\n' でなくてはならず、'\r' や '\r\n' ではエラーとなる。実行例は以下の通り。

```
rtn, err = rt.command("macro sample <<EOM\nnecho This is sample\nEOM")
```

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。

RTX1210 は Rev.14.01.26 以降で使用可能。

RTX830 は Rev.15.02.03 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

4.90 EMFS ファイルの作成、削除

[書式]

```
embedded file [-b] filename <<eof
no embedded file [-b] filename [<<eof]
```

[設定値及び初期値]

- *-b*
 - [設定値]: BASE64 形式を指定
 - [初期値]: -
- *filename*
 - [設定値]: ファイル名
 - [初期値]: -
- *eof*
 - [設定値]: 終端文字列
 - [初期値]: -

[説明]

EMFS 上のファイルを作成、削除する。

embedded file コマンドを投入すると、コンソールはファイルの内容を入力するモードとなる。*eof* で指定した EOF 文字列が入力されるまでが、ファイルの内容となる。**no embedded file** コマンドでファイルを削除できる。

-b オプションを指定した場合は、入力されたファイルの内容は BASE64 形式であるものとして処理される。BASE64 形式として不正な内容の場合はエラーとなる。バイナリーファイルを保存する場合は、BASE64 形式でなければならない。*-b* オプションが省略された場合は、入力された内容がそのままテキストファイルとして保存される。

EOF 文字列として利用できる文字種は、半角英数字 (A-Z、a-z、0-9) のみである。英大文字、小文字は区別される。

実行例は以下の通り。

```
# embedded file sample.txt <<EOF
show ip route
show ip connection
EOF
#
```

[ノート]

複数行からなるコマンドに対応していないため、**schedule at** コマンドからは実行できない。

Lua スクリプトの `rt.command()` で複数行からなるコマンドを実行する場合には、各行を改行文字（'\n'）で連結した文字列をコマンドとして渡す。改行文字は '\n' でなくてはならず、'\r' や '\r\n' ではエラーとなる。実行例は以下の通り。

```
rtn, err = rt.command("embedded file sample <<EOF\nnecho This is sample\nEOF")
```

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。

RTX1210 は Rev.14.01.26 以降で使用可能。

RTX830 は Rev.15.02.03 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

4.91 CPU スケジューリング方式の設定

[書式]

system packet-scheduling mode

no system packet-scheduling [*mode*]

[設定値及び初期値]

- *mode*: CPU スケジューリング方式
 - [設定値]:

設定値	説明
hash	ハッシュ方式
load-balance	ロードバランス方式
lan-based	LAN インターフェース方式

- [初期値]: hash

[説明]

CPU スケジューリング方式を設定する。

hash を選択した場合、受信パケットから算出されたハッシュ値を基にしてパケットの転送処理を実行する CPU コアが決まる。

load-balance を選択した場合、各 CPU コアの負荷が均等になるようにパケットの転送処理を実行する CPU コアがパケット単位で変化する。

lan-based を選択した場合、パケットを受信した LAN インターフェースによって転送処理を実行する CPU コアが次のように決まる。

受信 LAN インターフェース	CPU コア
LAN1	CPU0
LAN2	CPU1
LAN3	CPU2
LAN4	CPU3

[ノート]

BRI/PRI インターフェースで受信したパケットは、本コマンドの設定の対象にならない。

本コマンドを実行すると、すべての LAN インターフェースの初期化処理が実行されるため、すべての LAN インターフェースにおいて一時的にリンクダウンが発生する。

ノーマルパスの処理対象となるパケットは、本コマンドの設定に従って決定された CPU コアでは受信処理のみが実行され、転送処理は常に CPU1 で実行される。これは、**ip routing process** コマンドで **normal** が設定されている場合はすべてのパケットが対象となる。

CPU スケジューリング方式に `hash` を選択した場合、IPv4/IPv6 ヘッダを持たない受信パケットの転送処理は CPU0 で実行される。

CPU スケジューリング方式に `load-balance` を選択した場合、パケットの順番が入れ替わる可能性がある。パケットの順番が入れ替わると UDP を用いるアプリケーションで問題が発生する可能性がある。パケットの順番の入れ替わりは `system packet-scheduling filter` コマンドで該当パケットの転送処理を実行する CPU コアを固定することで抑制することができる。なお、TCP ではパケットの順番が入れ替わっても通常は問題は発生しない。

IPsec では、どの CPU スケジューリング方式であっても、ESP シーケンス番号の順序通りに ESP パケットが送信されないことがあるため、対向側ルーターの受信処理で ESP シーケンスエラーが発生し、ESP パケットが破棄される可能性がある。ESP シーケンスエラーは、対向側ルーターの `ipsec sa policy` コマンドで `anti-replay-check` を `off` にして、ESP シーケンス番号のチェックを行わないようにすることで回避できる。

RTX5000、RTX3500 の Rev.14.00.13 以降で使用可能。

[適用モデル]

RTX5000, RTX3500

4.92 CPU スケジューリングフィルターの設定

[書式]

```
system packet-scheduling filter filter_num cpu_num ip src_ipv4_address[/mask] [dest_ipv4_address[/mask]] [protocol [src_port [dest_port]]]
```

```
system packet-scheduling filter filter_num cpu_num ipv6 src_ipv6_address[/prefix_len] [dest_ipv6_address[/prefix_len]] [protocol [src_port [dest_port]]]
```

```
no system packet-scheduling filter filter_num [cpu_num ip src_ipv4_address[/mask] [dest_ipv4_address[/mask]] [protocol [src_port [dest_port]]]
```

```
no system packet-scheduling filter filter_num [cpu_num ipv6 src_ipv6_address[/prefix_len] [dest_ipv6_address[/prefix_len]] [protocol [src_port [dest_port]]]
```

[設定値及び初期値]

- `filter_num`
 - [設定値]: フィルター番号 (1..40)
 - [初期値]: -
- `cpu_num`
 - [設定値]: CPU 番号 (0..3)
 - [初期値]: -
- `src_ipv4_address`: IPv4 パケットの始点 IP アドレス
 - [設定値]:
 - A.B.C.D (A~D: 0~255 もしくは *)
 - 上記表記で A~D を * とすると、該当する 8 ビット分についてはすべての値に対応する
 - * (すべての IP アドレスに対応)
 - [初期値]: -
- `dest_ipv4_address`: IPv4 パケットの終点 IP アドレス
 - [設定値]:
 - `src_ipv4_address` と同じ形式
 - 省略した場合は一つの * と同じ
 - [初期値]: -
- `mask`: IP アドレスのネットマスク (`src_ipv4_address` および `dest_ipv4_address` がネットワークアドレスの場合のみ指定可)
 - [設定値]:
 - A.B.C.D (A~D: 0~255)
 - 0x に続く十六進数
 - マスクビット数
 - 省略時は 0xffffffff と同じ
 - [初期値]: -
- `src_ipv6_address`: IPv6 パケットの始点 IP アドレス
 - [設定値]:

- IPv6 アドレス
- * (すべての IP アドレスに対応)
- [初期値]:-
- *dest_ipv6_address*: IPv6 パケットの終点 IP アドレス
- [設定値]:
 - *src_ipv6_address* と同じ形式
 - 省略した場合は * と同じ
- [初期値]:-
- *prefix_len*: IP アドレスのプレフィックス長 (*src_ipv6_address* および *dest_ipv6_address* がネットワークアドレスの場合のみ指定可)
- [設定値]:
 - プレフィックス長
 - 省略時は 128 と同じ
- [初期値]:-
- *protocol*: スケジューリングするパケットの種類
- [設定値]:
 - 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 (一部)

ニーモニック	プロトコル番号
icmp	1 (IPv4 の場合)、58 (IPv6 の場合)
tcp	6
udp	17
gre	47
esp	50

- * (すべてのプロトコルに対応)
- 省略した場合は * と同じ。
- [初期値]:-
- *src_port*: UDP、TCP の送信元ポート番号
- [設定値]:
 - 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	21
ftpdata	20
telnet	23
smtp	25
domain	53
gopher	70
finger	79
www	80
pop3	110
sunrpc	111
ident	113
ntp	123
nntp	119
snmp	161

ニーモニック	ポート番号
syslog	514
printer	515
talk	517
route	520
uucp	540
submission	587

- * (すべてのポートに対応)
- 省略時は * と同じ
- [初期値]: -
- *dest_port*
 - [設定値]: *src_port* と同じ形式
 - [初期値]: -

[説明]

転送処理を実行する CPU コアを固定するためのフィルターを設定する。

フィルターに合致した受信パケットは、*cpu_num* で指定した CPU コアで転送処理が行われる。

[ノート]

BRI/PRI インターフェースで受信したパケットは、本コマンドの設定の対象にならない。

ノーマルパスの処理対象となるパケットは、本コマンドの設定に従って決定された CPU コアでは受信処理のみが実行され、転送処理は必ず CPU1 で実行される。これは、**ip routing process** コマンドで **normal** が設定されている場合はすべてのパケットが対象となる。

IPv4/IPv6 ヘッダを持たない受信パケットは、本コマンドの設定の対象にならない。

RTX5000、RTX3500 の Rev.14.00.13 以降で使用可能。

[設定例]

```
# system packet-scheduling filter 1 0 ip 192.168.100.1
# system packet-scheduling filter 2 1 ip 172.16.1.1 172.16.2.1 icmp
# system packet-scheduling filter 3 2 ip * * 6 21
# system packet-scheduling filter 4 3 ip 10.10.10.0/24 * udp * *
# system packet-scheduling filter 5 0 ip 192.168.*.*
# system packet-scheduling filter 6 1 ipv6 2001:240:10::1
# system packet-scheduling filter 7 2 ipv6 * 2001:240:100::
# system packet-scheduling filter 8 3 ipv6 2002::/32 * tcp
```

[適用モデル]

RTX5000, RTX3500

4.93 CPU スケジューリングフィルターの適用

[書式]

```
system packet-scheduling filter list filter_list
no system packet-scheduling filter list [filter_list]
```

[設定値及び初期値]

- *filter_list*
 - [設定値]: 空白で区切られた CPU スケジューリングフィルター番号の並び
 - [初期値]: -

[説明]

system packet-scheduling filter コマンドで設定したフィルターを適用する順番を設定する。

フィルターに合致した受信パケットは、フィルターで指定した CPU コアで転送処理が行われる。すべてのフィルターに合致しなかった受信パケットは、**system packet-scheduling** コマンドの設定に従って転送処理を実行する CPU コアが決まる。

[ノート]

RTX5000、RTX3500 の Rev.14.00.13 以降で使用可能。

[適用モデル]

RTX5000, RTX3500

第 5 章

ヤマハルーター用ファイルシステム RTFS

RTFS は、ルーターの内蔵フラッシュ ROM に構築されるファイルシステムです。一般的な PC のファイルシステムと同様、内蔵フラッシュ ROM に任意のデータを保存しファイル名を付けて管理することができます。またディレクトリ構造も実現されています。内蔵フラッシュ ROM にはファームウェア (exec) や設定ファイル (config) など様々なデータが保存されていますが、それらとは独立した特定の領域を RTFS として使用します。

ファイルやディレクトリを指定するコマンドでは、プレフィックスなしの "/" から始まるパスを入力すると RTFS 領域を参照することができます。

Lua スクリプト機能のスクリプトファイルやカスタム GUI の HTML ファイルなど、読み出し専用データを保存する用途として RTFS を使用してください。ログファイルの記録など、RTFS 領域への定期的な書き込みはフラッシュ ROM の消耗を早めます。頻繁に書き込みを行ったことが原因でフラッシュ ROM の故障に至った場合は、保証期間内であっても無償修理の保証対象外になります。

5.1 RTFS のフォーマット

[書式]

`rtfs format`

[説明]

内蔵フラッシュ ROM の RTFS 領域をフォーマットし、すべてのデータを削除する。工場出荷状態に戻した場合にもフォーマットが行われる。

[ノート]

フォーマットを実行するとデータは完全に削除され、復元することができない。

SRT100 は Rev.10.00.52 以降で使用可能。 RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

5.2 RTFS のガベージコレクト

[書式]

`rtfs garbage-collect`

[説明]

内蔵フラッシュ ROM の RTFS 領域にある不要なデータを削除し、空き容量を増やす。

ガベージコレクトは通常必要なときに自動で実行されるが、処理に数十秒かかるため、事前に行っておきたい場合にこのコマンドを実行する。

[ノート]

ガベージコレクトによってファイルが削除されたり上書きされたりすることはない。

SRT100 は Rev.10.00.52 以降で使用可能。 RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

第 6 章

ISDN 関連の設定

6.1 共通の設定

6.1.1 BRI 回線の種類の指定

[書式]

```
line type interface line [channels]
no line type interface line [channels]
```

[設定値及び初期値]

- *interface*
 - [設定値]: BRI インタフェース名
 - [初期値]: -
- *line*
 - [設定値]:

設定値	説明
isdn, isdn-ntt	ISDN 回線交換
164	デジタル専用線、64kbit/s
1128	デジタル専用線、128kbit/s

- [初期値]: isdn
- *channels*: *line* パラメータが *isdn*、*isdn-ntt* の場合のみ指定可
- [設定値]:

設定値	説明
1b	B チャンネルは 1 チャンネルだけ使用
2b	B チャンネルは 2 チャンネルとも使用する

- [初期値]: 2b

[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 チャンネルを確保したい場合は *channels* パラメータを 1b に設定する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

6.1.2 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
```

[設定値及び初期値]

- *interface*
 - [設定値]:
 - BRI インタフェース名
 - PRI インタフェース名
 - [初期値]: -
- *isdn_num*

- [設定値]: ISDN 番号
- [初期値]: -
- *sub_address*
 - [設定値]: ISDN サブアドレス (0x21 から 0x7e の ASCII 文字列)
 - [初期値]: -

[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ならないことがある

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

6.1.3 内蔵 DSU 使用の可否の設定

[書式]

```
isdn dsu interface switch
no isdn dsu interface [switch]
```

[設定値及び初期値]

- *interface*
 - [設定値]: BRI インタフェース名
 - [初期値]: -
- *switch*
 - [設定値]:

設定値	説明
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

- [初期値]: auto

[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

[適用モデル]

RTX1500

6.1.4 終端抵抗の設定

[書式]

```
isdn terminator interface terminator
no isdn terminator interface [terminator]
```

[設定値及び初期値]

- *interface*
 - [設定値]: BRI インタフェース名
 - [初期値]: -
- *terminator*

- [設定値]:

設定値	説明
on	終端抵抗を ON にする
off	終端抵抗を OFF にする

- [初期値]: on

[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]

ルーターを外部 DSU に直結する場合にはルーターの終端抵抗を必ず ON にする。DSU からのバス配線で接続する場合には、通常はバス配線に終端抵抗が配置されているので、ルーターの終端抵抗は OFF にする。ただし、ルーターがバス配線の終端にあり、バス配線内に終端抵抗が配置されていないときには、ルーターの終端抵抗を ON にしなければならない。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

6.1.5 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]
```

[設定値及び初期値]

- *interface*
 - [設定値]: BRI インタフェース名と BRI インタフェース名の並び
 - [初期値]: -

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

6.1.6 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]
```

[設定値及び初期値]

- *interface*
 - [設定値]:
 - BRI インタフェース名
 - PRI インタフェース名
 - [初期値]: -
- *yen*
 - [設定値]:

設定値	説明
円 (1..2147483647)	課金額
off	発信制限機能を使わない

- [初期値]: off

[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** を実行するようしておくこと、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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

6.1.7 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*]

[設定値及び初期値]

- *arrive*

- [設定値]:

設定値	説明
on	許可する
off	拒否する

- [初期値]: on

[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。

[適用モデル]

RTX3000, RTX1500, RTX1200, RTX1100

6.1.8 PIAFS 接続時の起動側の指定**[書式]**

isdn piafs control switch

no isdn piafs control

[設定値及び初期値]

- *switch*

- [設定値]:

設定値	説明
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

設定値	説明
arrive	自分が着信側の場合に PIAFS の起動側となる

- [初期値]: call

[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。

<i>switch</i> 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

[設定例]

```
# pp select 2
# isdn piafs control call
# pp enable 2
```

[適用モデル]

RTX3000, RTX1500, RTX1200, RTX1100

6.1.9 PIAFS の発信方式の設定

[書式]

```
isdn piafs call speed [64kmode]
no isdn piafs call [speed [64kmode]]
```

[設定値及び初期値]

- *speed*
- [設定値]:

設定値	説明
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

- [初期値]: off
- *64kmode*
- [設定値]:

設定値	説明
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

- [初期値]: -

[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。

[適用モデル]

RTX3000, RTX1500, RTX1200, RTX1100

6.1.10 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*]

[設定値及び初期値]

- *peer_num*

- [設定値]:

設定値	説明
番号	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

- [初期値]: none

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RT250i

6.2 相手側の設定

6.2.1 常時接続の設定

[書式]

pp always-on *switch* [*time*]

no pp always-on

[設定値及び初期値]

- *switch*

- [設定値]:

設定値	説明
on	常時接続する
off	常時接続しない

- [初期値]: off

- *time*

- [設定値]: 再接続を要求するまでの秒数 (60..21474836)

- [初期値]: -

[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、*time* は 60 になる。

以下のコマンドが設定されている場合、*switch* を on に設定した時点で接続処理が行われる。

- PPPoE 接続
 - **pppoe use**
 - **pp enable**
- ISDN 接続
 - **pp bind** BRI インタフェース名
 - **pp enable**
- モバイルインターネット接続 (携帯端末を PP (USB モデム) として制御するタイプ)
 - **pp bind** usb1
 - **pp enable**
 - **mobile use**

また、上記の設定に依らず、*switch* を off に設定した時点で切断処理が行われる。

[ノート]

PP 毎のコマンドである。

PP として専用線が使用される時、あるいは *anonymous* が選択された時には無効である。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

6.2.2 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]]
```

[設定値及び初期値]

- *call_arrive*
 - [設定値]:

設定値	説明
call	発着信用
arrive	着信専用

- [初期値]: -
- *isdn_num*
 - [設定値]: ISDN 番号
 - [初期値]: -
- *sub_address*
 - [設定値]: ISDN サブアドレス (0x21 から 0x7e の ASCII 文字)
 - [初期値]: -
- *isdn_num_list*
 - [設定値]: 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
 - [初期値]: -

[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ン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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

6.2.3 自動接続の設定

[書式]

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

[設定値及び初期値]

- *auto*

- [設定値]:

設定値	説明
on	自動接続する
off	自動接続しない

- [初期値]: on

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

6.2.4 相手への発信順序の設定

[書式]

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

[設定値及び初期値]

- *order*

- [設定値]:

設定値	説明
round	ラウンドロビン方式
serial	順次サーチ方式

- [初期値]: serial

[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ン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ン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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

6.2.5 着信許可の設定

[書式]

```
isdn arrive permit arrive [vrrp interface vrid[slave]]
```

```
no isdn arrive permit [arrive]
```

[設定値及び初期値]

- *arrive*

- [設定値]:

設定値	説明
on	許可する
off	許可しない

- [初期値]: on

- *interface*

- [設定値]: LAN インタフェース名
- [初期値]: -

- *vrid*

- [設定値]: VRRP グループ ID(1..255)
- [初期値]: -

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

6.2.6 発信許可の設定

[書式]

```
isdn call permit permit
```

```
no isdn call permit [permit]
```

[設定値及び初期値]

- *permit*

- [設定値]:

設定値	説明
on	許可する
off	許可しない

- [初期値]: on

[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、ISDN 回線経由では通信できない。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

6.2.7 再発信抑制タイマの設定

[書式]

```
isdn call block time time
no isdn call block time [time]
```

[設定値及び初期値]

- *time*
 - [設定値]: 秒数 (0..15.0)
 - [初期値]: 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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

6.2.8 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]
```

[設定値及び初期値]

- *time*
 - [設定値]: 秒数 (60..21474836.0)
 - [初期値]: 60

[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異なる。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

6.2.9 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]
```

[設定値及び初期値]

- *callback_request*
 - [設定値]:

設定値	説明
on	要求する
off	要求しない

- [初期値]: off

[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。

[ノート]

コールバックは、`backup` コマンドによる ISDN インタフェースへのバックアップとの併用はできません。バックアップと併用する場合は、ネットワークバックアップを使ってください。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

6.2.10 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]
```

[設定値及び初期値]

- *callback_permit*
 - [設定値]:

設定値	説明
on	応じる
off	応じない

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

6.2.11 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]
```

[設定値及び初期値]

- *type*
 - [設定値]:

設定値	説明
yamaha	ヤマハ方式
mscbcp	MS コールバック

- [初期値]: yamaha

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

6.2.12 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]]
```

[設定値及び初期値]

- *type1, type2*
 - [設定値]:

設定値	説明
yamaha	ヤマハ方式
mscbcp	MS コールバック

- [初期値]:
 - type1=yamaha
 - type2=mscbcp

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

6.2.13 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 mscbc user-specify specify
no no isdn callback mscbc user-specify [specify]
```

[設定値及び初期値]

- *specify*
 - [設定値]:

設定値	説明
on	許可する
off	拒否する

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

6.2.14 コールバックタイマの設定

[書式]

```
isdn callback response time type time
no isdn callback response time [type]
```

[設定値及び初期値]

- *type*
 - [設定値]:

設定値	説明
1b	1B でコールバックする

- [初期値]: -
- *time*
 - [設定値]: 秒数 (0..15.0)
 - [初期値]: 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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

6.2.15 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*]

[設定値及び初期値]

- *time*
 - [設定値]: 秒数 (1..60.0)
 - [初期値]: 60

[説明]

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

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

6.2.16 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*]

[設定値及び初期値]

- *type*
 - [設定値]:

設定値	説明
1	単純トラフィック監視方式
2	課金単位時間方式

- [初期値]: 1

[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。

[設定例]

```
# isdn disconnect policy 2
# isdn disconnect interval time 240 6 2
```

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

6.2.17 切断タイマの設定 (ノーマル)**[書式]**

isdn disconnect time *time*

no isdn disconnect time [*time*]

[設定値及び初期値]

- *time*
- [設定値]:

設定値	説明
1..21474836.0	秒数
off	タイマを設定しない

- [初期値]: 60

[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]

本コマンドを off に設定した場合には、**isdn disconnect input time** コマンドおよび **isdn disconnect output time** コマンドの設定にかかわらず切断されなくなる。

本コマンドの設定値を NORMAL 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。

NORMAL>IN または OUT>NORMAL のように設定した場合、設定値が大きい方が優先される。そのため、パケットの入力が観測されないと NORMAL 秒、パケットの出力が観測されないと OUT 秒で切断される。なお、パケットの入出力が観測されないと常に NORMAL 秒で切断される。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

6.2.18 切断タイマの設定 (ファスト)

[書式]

isdn fast disconnect time *time*

no no isdn fast disconnect time [*time*]

[設定値及び初期値]

- *time*
- [設定値]:

設定値	説明
1..21474836.0	秒数
off	タイマを設定しない

- [初期値]: 20

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

6.2.19 切断タイマの設定 (強制)

[書式]

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

[設定値及び初期値]

- *time*
- [設定値]:

設定値	説明
1..21474836.0	秒数
off	タイマを設定しない

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

6.2.20 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*]

[設定値及び初期値]

- *time*
- [設定値]:

設定値	説明
1..21474836.0	秒数
off	タイマを設定しない

- [初期値]: 120

[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。

isdn disconnect time コマンドを off に設定した場合には、本コマンドおよび **isdn disconnect output time** コマンドの設定にかかわらず切断されなくなる。

isdn disconnect time コマンドの設定値を NORMAL 秒、本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。

NORMAL>IN または OUT>NORMAL のように設定した場合、設定値が大きい方が優先される。そのため、パケットの入力が観測されないと NORMAL 秒、パケットの出力が観測されないと OUT 秒で切断される。なお、パケットの入出力が観測されないと常に NORMAL 秒で切断される。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

6.2.21 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]
```

[設定値及び初期値]

- *time*
- [設定値]:

設定値	説明
1..21474836.0	秒数
off	タイマを設定しない

- [初期値]: 120

[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、接続先を経由して外部から不正な UDP パケットを受信し続けるような場合、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。

isdn disconnect time コマンドを off に設定した場合には、**isdn disconnect input time** コマンドおよび本コマンドの設定にかかわらず切断されなくなる。

isdn disconnect time コマンドの設定値を NORMAL 秒、**isdn disconnect input time** コマンドの設定値を IN 秒、本コマンドの設定値を OUT 秒とする。

NORMAL>IN または OUT>NORMAL のように設定した場合、設定値が大きい方が優先される。そのため、パケットの入力が観測されないと NORMAL 秒、パケットの出力が観測されないと OUT 秒で切断される。なお、パケットの入出力が観測されないと常に NORMAL 秒で切断される。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

6.2.22 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]

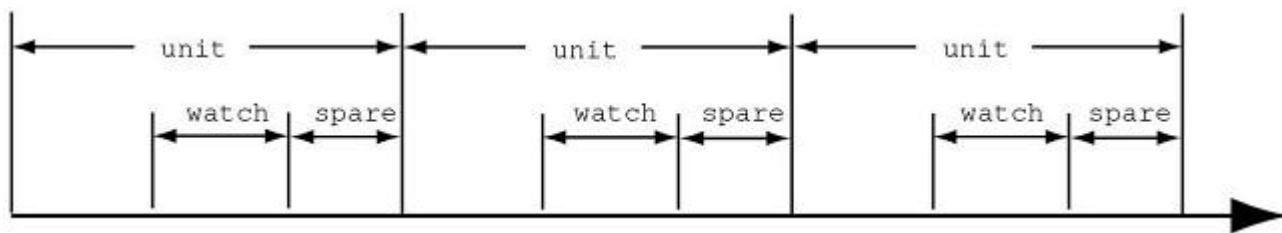
```
isdn disconnect interval time unit watch spare
no isdn disconnect interval time [unit watch spare]
```

[設定値及び初期値]

- *unit*: 課金単位時間
 - [設定値]:
 - 秒数 (1..21474836.0)
 - off
 - [初期値]: 180
- *watch*: 監視時間
 - [設定値]:
 - 秒数 (1..21474836.0)
 - off
 - [初期値]: 6
- *spare*: 切断余裕時間
 - [設定値]:
 - 秒数 (1..21474836.0)
 - off
 - [初期値]: 2

[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。

[設定例]

```
# isdn disconnect policy 2
# isdn disconnect interval time 240 6 2
```

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

第7章

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せん。

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。

※1 High level Data Link Control procedure

※2 Data Link Connection Identifier

※3 Permanent Virtual Circuit

※4 Local Management Interface

※5 Inverse Address Resolution Protocol; RFC1293

7.1 カプセル化の種類の設定

[書式]

pp encapsulation *type*

no pp encapsulation [*type*]

[設定値及び初期値]

- *type*

- [設定値]:

設定値	説明
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

- [初期値]: ppp

[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)

[適用モデル]

RTX3000, RTX1500, RTX1200, RTX1100, RT250i

7.2 DLCI の設定

[書式]

fr dlci *dlci_num*

no fr dlci [*dlci_num*]

[設定値及び初期値]

- *dlci_num*

- [設定値]:

設定値	説明
auto	DLCI を自動取得する
DLCI 値 (16..991)	DLCI 値を空白で区切って並べたもの (96 個以内)

- [初期値]: auto

[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、または主導設定する。

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 で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。

[設定例]

```
# fr dlci 16 17 18
```

[適用モデル]

RTX3000, RTX1500, RTX1200, RTX1100, RT250i

7.3 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*

[設定値及び初期値]

- *dcli_num*
 - [設定値]: DLCI 値 (16..991)
 - [初期値]: -
- *cir*
 - [設定値]: CIR 値 (bit/s 単位)
 - [初期値]: -
- *idle*
 - [設定値]:

設定値	説明
秒数 (1..2147483647)	スロースタート状態に戻るまでのアイドル時間
0	スロースタート動作を行わない

- [初期値]: 20
- *bc_size*
 - [設定値]: 認定バーストサイズ (ビット)
 - [初期値]: 7000
- *be_size*
 - [設定値]: 超過バーストサイズ (ビット)
 - [初期値]: 7000
- *step_count*
 - [設定値]: ステップカウント
 - [初期値]: $cir/bc_size/be_size$ から計算される値

[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。

[適用モデル]

RTX3000, RTX1500, RTX1200, RTX1100, RT250i

7.4 PVC 状態確認手順の設定

[書式]

fr lmi lmi

no fr lmi [lmi]

[設定値及び初期値]

- *lmi*
 - [設定値]:

設定値	説明
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

- [初期値]: q933

[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]

網との契約が LMI でない場合、**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。

[適用モデル]

RTX3000, RTX1500, RTX1200, RTX1100, RT250i

7.5 InARP 使用の設定

[書式]

```
fr inarp inarp
no fr inarp [inarp]
```

[設定値及び初期値]

- *inarp*
- [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: on

[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

[適用モデル]

RTX3000, RTX1500, RTX1200, RTX1100, RT250i

7.6 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]
```

[設定値及び初期値]

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

[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, RTX1500, RT250i

7.7 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]
```

[設定値及び初期値]

- *dlci_num*

- [設定値]:
 - DLCI 値 (16..991)
 - * (すべてのデータリンク)
- [初期値]: -
- *type*
- [設定値]:

設定値	説明
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

- [初期値]: none

[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。

[適用モデル]

RTX3000, RTX1500, RTX1200, RTX1100, RT250i

7.8 輻輳制御をするか否かの設定

[書式]

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

[設定値及び初期値]

- *control*
- [設定値]:

設定値	説明
on	輻輳制御を行う
off	輻輳制御を行わない

- [初期値]: off

[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。

[適用モデル]

RTX3000, RTX1500, RTX1200, RTX1100, RT250i

7.9 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*]

[設定値及び初期値]

- *type*
- [設定値]:

設定値	説明
serial	順次サーチ方式

設定値	説明
round-robin	ラウンドロビン方式

- [初期値]: round-robin

[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。

[適用モデル]

RTX3000, RTX1500, RTX1200, RTX1100, RT250i

7.10 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 dlcid=dlci_num filter_num_list
no fr de protocol filter dlcid=dlci_num [filter_num_list]
```

[設定値及び初期値]

- *protocol*
- [設定値]:

設定値	説明
ip	IP パケット
ipx	IPX パケット
bridge	ブリッジするパケット

- [初期値]: -
- *filter*: 固定のキーワード

- [初期値]: -
- *dlci_num*

- [設定値]:

設定値	説明
16..991	DLCI 値
*	すべてのデータリンク

- [初期値]: -
- *filter_num_list*
- [設定値]: 静的フィルタ番号 (1..100) の並び
- [初期値]: -

[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、bridge は指定できない。

[適用モデル]

RTX3000, RTX1500, RTX1200, RTX1100, RT250i

第 8 章

PRI 関連の設定

RTX5000、RTX3500、RTX3000、RT250i 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/YBA-1PRI-MB/YBA-1PRI-MC/YBC-1PRI-M)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)
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
RTX5000、RTX3500	YBC-1PRI-M	YBC-1PRI-M	YBC-1PRI-M

(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/YBA-1PRI-MB/YBA-1PRI-MC/YBC-1PRI-M: 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、情報チャンネル番号 (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
```

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を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。

8.1 PRI 回線の種類の設定

[書式]

line type interface line

no line type interface line

[設定値及び初期値]

- *interface*
 - [設定値]: PRI インタフェース名
 - [初期値]: -
- *line*
 - [設定値]:

設定値	説明
isdn、isdn-ntt	ISDN 回線交換
leased	デジタル専用線

- [初期値]: leased

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RT250i

8.2 情報チャン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]

[設定値及び初期値]

- *pri*
 - [設定値]: PRI 番号 (1..2)
 - [初期値]: -
- *info*
 - [設定値]: 情報チャンネル番号 (1...24)
 - [初期値]: -
- *timeslot_head*
 - [設定値]: 情報タイムスロット番号 (1...24)
 - [初期値]: -
- *timeslot_num*
 - [設定値]:
 - 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

- [初期値]: -

[説明]

指定した PRI 回線内の情報チャンネルを、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 の多重化非対応の PRI 拡張モジュール (YBA-1PRI-N) では、2 つ以上の情報チャンネルは設定できない。

[適用モデル]

RTX5000, RTX3500, RTX3000, RT250i

8.3 PP で使用するインタフェースの設定

[書式]

```
pp bind interface[/info] [interface[/info]]
no pp bind [interface/info]
```

[設定値及び初期値]

- *interface*
 - [設定値]: PRI インタフェース名
 - [初期値]: -
- *info*
 - [設定値]: 情報チャンネル番号
 - [初期値]: -

[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ンネル番号を、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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RT250i

第 9 章

IP の設定

9.1 インタフェース共通の設定

9.1.1 IP パケットを扱うか否かの設定

[書式]

```
ip routing routing
no ip routing [routing]
```

[設定値及び初期値]

- *routing*
 - [設定値]:

設定値	説明
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

- [初期値]: on

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.1.2 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]
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 interface address [dhcp]
no ip pp address [ip_address[/mask]]
no ip loopback address [ip_address[/mask]]
no ip bridge_interface address [ip_address/mask [broadcast broadcast_ip]]
no ip bridge_interface address [dhcp]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *loopback*
 - [設定値]: LOOPBACK インタフェース名
 - [初期値]: -
- *bridge_interface*
 - [設定値]: ブリッジインタフェース名
 - [初期値]: -

- *ip_address*
 - [設定値]: IP アドレス xxx.xxx.xxx.xxx(xxx は十進数)
 - [初期値]: -
- *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
 - [初期値]: -
- *mask*
 - [設定値]:
 - xxx.xxx.xxx.xxx(xxx は十進数)
 - 0x に続く十六進数
 - マスクビット数
 - [初期値]: -
- *broadcast_ip*
 - [設定値]: ブロードキャスト IP アドレス
 - [初期値]: -
- *switch*
 - [設定値]:

設定値	説明
on	AutoIP 機能を使う
off	AutoIP 機能を使わない

- [初期値]: off

[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 dhcp** コマンドで確認することができる。
 LOOPBACK インタフェースは Rev.8.03 系以降のすべてのファームウェアで指定可能。
 ブリッジインタフェースは SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。
 WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.1.3 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]**

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *ip_address*
 - [設定値]: セカンダリ IP アドレス xxx.xxx.xxx.xxx(xxx は十進数)
 - [初期値]: -
- *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
 - [初期値]: -
- *mask*
 - [設定値]:
 - xxx.xxx.xxx.xxx(xxx は十進数)
 - 0x に続く十六進数
 - マスクビット数
 - [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.1.4 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]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *mtu0,mtu1,mtu2*
 - [設定値]: MTU の値 (64..1500 ; RTX3000 の LAN1 / LAN2、および、RTX5000、RTX3500 の LAN インタフェースは 64..9578)
 - [初期値]:
 - *mtu0*=1500
 - *mtu1*=1500
 - *mtu2*=1280

[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。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.1.5 同一インタフェースに折り返すパケットを送信するか否かの設定

[書式]

```
ip interface rebound switch
ip pp rebound switch
ip tunnel rebound switch
no ip interface rebound [switch]
no ip pp rebound [switch]
no ip tunnel rebound [switch]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *switch*
 - [設定値]:

設定値	説明
on	折り返すパケットを送信する
off	折り返すパケットを送信しない

- [初期値]:
 - off (PP インタフェースの場合)
 - on (その他のインタフェースの場合)

[説明]

同一インタフェースに折り返すパケットを送信するか否かを設定する。折り返すパケットを送信しない場合にはそのパケットを廃棄し、送信元へ ICMP Destination Unreachable を送信する。

[ノート]

RTX1100、RTX1500、RT107e では、Rev.8.03.87 以降で使用可能。
 RTX3000 では、Rev.9.00.48 以降で使用可能。
 RTX1200 では、Rev.10.01.22 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e

9.1.6 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]
```

[設定値及び初期値]

- *service*
 - [設定値]:

設定値	説明
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

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.1.7 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...]
```

[設定値及び初期値]• *network*

• [設定値]:

設定値	説明
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)

• [初期値]:-

• *gateway1, gateway2*

• [設定値]:

• IP アドレス

- xxx.xxx.xxx.xxx (xxx は十進数)

- pp *peer_num* [*dci=dhci*]: PP インタフェースへの経路。"dci=dhci" 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

- pp anonymous name=*name*

設定値	説明
<i>name</i>	PAP/CHAP による名前

- dhcp *interface*

設定値	説明
<i>interface</i>	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、WAN インタフェース名、ブリッジインタフェース名

- 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

• [初期値]:-

- *parameter*: 以下のパラメータを空白で区切り複数設定可能

• [設定値]:

設定値	説明
filter <i>number</i> [<i>number..</i>]	フィルタ型経路の指定 <ul style="list-style-type: none"> • <i>number</i> <ul style="list-style-type: none"> • フィルタの番号 (1..21474836) (空白で区切り複数設定可能)
dpi <i>number</i> [<i>number..</i>]	フィルタ型経路の指定 <ul style="list-style-type: none"> • <i>number</i> <ul style="list-style-type: none"> • DPI フィルタの番号 (1..21474836) (空白で区切り複数設定可能)

設定値	説明
<code>metric metric</code>	メトリックの指定 <ul style="list-style-type: none"> • <i>metric</i> <ul style="list-style-type: none"> • メトリック値 (1..15) • 省略時は 1
<code>hide</code>	出力インターフェースが LAN インタフェース、または WAN インタフェース、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
<code>weight weight</code>	異なる経路間の比率を表す値 <ul style="list-style-type: none"> • <i>weight</i> <ul style="list-style-type: none"> • 経路への重み (0..2147483647) • 省略時は 1
<code>keepalive keepalive_id</code>	<code>gateway1</code> に到達性のあるときにだけ有効となる <ul style="list-style-type: none"> • <i>keepalive_id</i> <ul style="list-style-type: none"> • キープアライブの識別子 (1..100; RTX5000 は 1...3000; RTX3500、RTX3000 は 1...1000)

- [初期値] :-

[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。

[ノート]

既に存在する経路を上書きすることができる。

RT107e は、Rev.8.03.42 以降で `keepalive` オプションを指定可能。

ブリッジインタフェースは SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

`parameter` パラメータの `dpi` キーワードは RTX830 の Rev.15.02.13 以降のファームウェアで指定可能。

最初の `gateway` キーワードより後のキーワードとパラメーターは合計 129 個まで設定可能。

[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
```

- ソフトウェア更新関係のパケットは PP1 インターフェース経由で、その他は TUNNEL1 経由で送信する。

```
# dpi group set 100 name=sw_update
windows_update,apple_update,ios_ota_update,adobe_update
# ip dpi filter 1 pass * * 100
# ip route default gateway pp 1 dpi 1 gateway tunnel 1
```

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.1.8 DHCP で IP アドレスを取得したときにデフォルト経路を自動的に追加するか否かを設定**[書式]**

```
ip interface dhcp auto default-route-add switch
```

```
no ip interface dhcp auto default-route-add [switch]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インターフェース名、WAN インターフェース名、ブリッジインターフェース名
 - [初期値]: -
- *switch*
 - [設定値]:

設定値	説明
on	DHCP で IP アドレスを取得したときにデフォルト経路を自動的に追加する
off	DHCP で IP アドレスを取得したときにデフォルト経路を自動的に追加しない

- [初期値]: on

[説明]

指定したインターフェースを使用中、DHCP で IP アドレスを取得したときにデフォルト経路を自動的に追加するか

否かを設定する。

すでに DHCP で IP アドレスを取得しているインターフェースに対してこのコマンドの設定が変更された場合、次に DHCP で IP アドレスを取得した時点から新しい設定が反映される。

[ノート]

RTX1210 は Rev.14.01.28 以降で使用可能。 RTX830 は Rev.15.02.03 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830

9.1.9 DHCP で IP アドレスを取得したときに implicit 経路を自動的に追加するか否かを設定

[書式]

```
ip interface dhcp auto interface-route-add switch
no ip interface dhcp auto interface-route-add [switch]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インターフェース名、WAN インターフェース名、ブリッジインターフェース名
 - [初期値]: -
- *switch*
 - [設定値]:

設定値	説明
on	DHCP で IP アドレスを取得したときに implicit 経路を自動的に追加する
off	DHCP で IP アドレスを取得したときに implicit 経路を自動的に追加しない

- [初期値]: on

[説明]

指定したインターフェースを使用中、DHCP で IP アドレスを取得したときにアドレスを取得したインターフェースの implicit なネットワーク経路を自動的に追加するか否かを設定する。

すでに DHCP で IP アドレスを取得しているインターフェースに対してこのコマンドの設定が変更された場合、次に DHCP で IP アドレスを取得した時点から新しい設定が反映される。

[ノート]

RTX1210 は Rev.14.01.28 以降で使用可能。 RTX830 は Rev.15.02.03 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830

9.1.10 IP パケットのフィルターの設定

[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]
```

[設定値及び初期値]

- *filter_num*
 - [設定値]: 静的フィルター番号 (1..21474836)
 - [初期値]: -
- *pass_reject*
 - [設定値]:

設定値	説明
pass	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)

設定値	説明
pass-nolog	一致すれば通す (ログに記録しない)
reject	一致すれば破棄する (ログに記録する)
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	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 (破棄する場合のみログに記録する)
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)

- [初期値]: -
- *src_addr*: IP パケットの始点アドレス
 - [設定値]:
 - IP アドレス
 - A.B.C.D (A~D: 0~255 もしくは*)
 - 上記表記で A~D を*とすると、該当する 8 ビット分についてはすべての値に対応する
 - 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。
 - , を区切りとして複数設定することができる。
 - FQDN
 - 任意の文字列 (半角 255 文字以内。/ : は使用できない。 , は区切り文字として使われるため、使用できない)
 - * から始まる FQDN は * より後ろの文字列を後方一致条件として判断する 例えば *.example.co.jp は www.example.co.jp 、 mail.example.co.jp などと一致する
 - , を区切りとして複数設定することができる。
 - map-e
 - MAP-E のマッフルールにより生成されたグローバル IPv4 アドレスを表すキーワード
 - * (すべての IP アドレスに対応)
 - [初期値]: -
- *dest_addr*: IP パケットの終点アドレス
 - [設定値]:
 - *src_addr* と同じ形式
 - 省略した場合は一つの * と同じ
 - [初期値]: -
- *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)
 - [設定値]:
 - A.B.C.D (A~D: 0~255)
 - 0x に続く十六進数
 - マスクビット数
 - 省略時は 0xffffffff と同じ
 - [初期値]: -
- *protocol*: フィルタリングするパケットの種類
 - [設定値]:
 - 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

ニーモニック	十進数	説明
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
- 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
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
tcpflag=value/mask	TCP フラグの値と <i>mask</i> の値の論理積 (AND) が、 <i>value</i> に一致、または不一致である TCP パケット <i>value</i> と <i>mask</i> は 0x に続く十六進数で 0x0000~0xffff
tcpflag!=value/mask	
*	すべてのプロトコル

- 省略時は * と同じ。
- [初期値] :-
- *src_port_list* : *protocol* に、TCP(tcp/tcpsyn/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。
- [設定値] :
 - 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
ident	113
ntp	123

ニーモニック	ポート番号
nntp	119
snmp	161
syslog	514
printer	515
talk	517
route	520
uucp	540
submission	587

- 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。
- [初期値]: -
- *dest_port_list*
 - [設定値]: *protocol* に、TCP(*tcp/tcpsyn/tcpfin/teprst/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
 - [初期値]: -

[説明]

IP パケットのフィルターを設定する。本コマンドで設定されたフィルターは **ip filter directed-broadcast**、**ip filter dynamic**、**ip filter set**、**ip forward filter**、**ip fragment remove df-bit**、**ip interface rip filter**、**ip interface secure filter**、および **ip route** コマンドで用いられる。

[ノート]

restrict-log 及び **restrict-nolog** を使ったフィルターは、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 コードをフィルター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ぬ。また、*protocol* に 'icmp-error' や 'icmpinfo' 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ーが比較される。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ーと比較される。

Rev.10.00 系以降のすべてのファームウェアで *protocol* に 'tcpsyn' を指定可能。

RTX1200 Rev.10.01.47 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで *src_port_list* または *dest_port_list* に *submission* を指定可能。

RTX1500 / RTX1100 / RT107e Rev.8.03.68 以降、RTX3000 Rev.9.00.31 以降のファームウェア、および、Rev.10.00 系以降のすべてのファームウェアで ICMP のタイプとコードを指定可能。

src_addr および *dest_addr* は IP アドレス と FQDN と map-e を混合することも可能。

src_addr および *dest_addr* への FQDN の指定は RTX5000 Rev.14.00.26 以降、RTX3500 Rev.14.00.26 以降、RTX1210 Rev.14.01.26 以降、RTX830 Rev.15.02.03 以降、RTX810 Rev.11.01.28 以降、RTX1220 で指定可能。

src_addr および *dest_addr* に FQDN を指定することによって、固定 IP アドレスではないサーバーや 1 つの FQDN に対して複数の固定 IP アドレスを持つサーバーを対象にしたフィルタリングを行うことができる。FQDN を使用する場合、ルーター自身が DNS リカーシブサーバーとして動作し、ルーター配下の端末は DNS サーバーとして本機を指定する必要がある。

指定した FQDN に一致する通信が発生した場合、設定した FQDN に該当する IP アドレスの情報が保持される。保持

される期間は、**ip filter fqdn timer** コマンドで指定できる。

src_addr および *dest_addr* への **map-e** の指定は RTX5000 Rev.14.00.32 以降、RTX3500 Rev.14.00.32 以降、RTX1210 Rev.14.01.40 以降、RTX830 Rev.15.02.20 以降 で指定可能。

[設定例]

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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.1.11 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 ...]
```

[設定値及び初期値]

- *name*
 - [設定値]: フィルタセットの名前を表す文字列
 - [初期値]: -
- *direction*
 - [設定値]:

設定値	説明
in	入力方向のフィルタ
out	出力方向のフィルタ

- [初期値]: -
- *filter_list*
 - [設定値]: 空白で区切られたフィルタ番号の並び (1000 個以内)
 - [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.1.12 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]
```

[設定値及び初期値]

- *filter_out*
 - [設定値]:

設定値	説明
on	フィルタアウトする
off	フィルタアウトしない

- [初期値]: on

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.1.13 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
```

[設定値及び初期値]

- *filter_out*
 - [設定値]:

設定値	説明
on	フィルタアウトする
off	フィルタアウトしない

- [初期値]: on
- *filter_num*
 - [設定値]: 静的フィルタ番号 (1..21474836)
 - [初期値]: -

[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、**ip interface wol relay** コマンドのチェックの方が優先される。**ip interface 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。

SRT100 では、Rev.10.00.31 以降で第 2 書式を使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.1.14 動的フィルターの定義

[書式]

```
ip filter dynamic dyn_filter_num srcaddr[/mask] dstaddr[/mask] protocol [option ...]
ip filter dynamic dyn_filter_num srcaddr[/mask] dstaddr[/mask] filter filter_list [in filter_list] [out filter_list] [option...]
no ip filter dynamic dyn_filter_num
```

[設定値及び初期値]

- *dyn_filter_num*
 - [設定値]: 動的フィルター番号 (1..21474836)
 - [初期値]: -
- *srcaddr*: IP パケットの始点アドレス
 - [設定値]:
 - **ip filter** コマンドの *src_addr* と同じ形式
 - 省略した場合は一個の * と同じ
 - [初期値]: -
- *dstaddr*: IP パケットの終点アドレス
 - [設定値]:
 - *srcaddr* と同じ形式
 - 省略した場合は一個の * と同じ
 - [初期値]: -
- *mask*: IP アドレスのビットマスク (*srcaddr* および *dstaddr* がネットワークアドレスの場合のみ指定可)
 - [初期値]: -
- *protocol*: プロトコルのニーモニック
 - [設定値]:

- tcp/udp/ftp/tftp/domain/www/smtp/pop3/telnet/netmeeting

Rev.10.01 以降では以下が使用できます

- echo/discard/daytime/chargen/ftp/ssh/telnet/smtp/time/whois/dns/domain/
- tftp/gopher/finger/http/www/pop3/sunrpc/ident/nntp/ntp/ms-rpc/
- netbios_ns/netbios_dgm/netbios_ssn/imap/snmp/snmptrap/bgp/imap3/ldap/
- https/ms-ds/ike/rlogin/rwho/rsh/syslog/printer/rip/ripng/
- ms-sql/radius/l2tp/pptp/nfs/msblast/ipsec-nat-t/sip/
- ping/ping6/tcp/udp

Rev.10.01 以降では以下が設定できますが、動的フィルターとして動作しません

- dhcp/dhcps/dhcpv6c/dhcpv6s

Rev.10.01.47 以降、および、Rev.11.01 以降では以下が使用できます

- submission

- [初期値]: -
- *filter_list*
 - [設定値]: **ip filter** コマンドで登録されたフィルター番号のリスト
 - [初期値]: -

- *option*
 - [設定値]:
 - syslog=*switch*

設定値	説明
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*

設定値	説明
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

- [初期値]: syslog=on

[説明]

動的フィルターを定義する。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、ユーザー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ー番号を設定する。

filter キーワードの後に記述されたフィルターに該当するコネクション (トリガー) 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ー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ー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ー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。

[ノート]

srcaddr および dstaddr は IP アドレスと FQDN と map-e を混合することも可能。

srcaddr および dstaddr への FQDN の指定は RTX5000 Rev.14.00.26 以降、RTX3500 Rev.14.00.26 以降、RTX1210 Rev.14.01.26 以降、RTX830 Rev.15.02.03 以降、RTX810 Rev.11.01.28 以降、RTX1220 で指定可能。

srcaddr および dstaddr への map-e の指定は RTX5000 Rev.14.00.32 以降、RTX3500 Rev.14.00.32 以降、RTX1210 Rev.14.01.40 以降、RTX830 Rev.15.02.20 以降で指定可能。

[設定例]

```
# ip filter 10 pass * * udp * snmp
# ip filter dynamic 1 * * filter 10
```

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e

9.1.15 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=timeout...]
no ip filter dynamic timer
```

[設定値及び初期値]

- option : オプション名
- [設定値] :

設定値	説明
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

- [初期値] :
 - tcp-syn-timeout=30
 - tcp-fin-timeout=5
 - tcp-idle-time=3600
 - udp-idle-time=30
 - dns-timeout=5
- timeout
 - [設定値] : 待ち時間 (秒)
 - [初期値] : -

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e

9.1.16 FQDN フィルターで使用するキャッシュのタイマーの設定

[書式]

```
ip filter fqdn timer time [auto=switch]
```

```
no ip filter fqdn timer [time]
```

[設定値及び初期値]

- *time*
 - [設定値]: 秒数 (1..2147483647)
 - [初期値]: 600
- *switch*
 - [設定値]:

設定値	説明
on	自動設定を使用する
off	自動設定を使用しない

- [初期値]: on

[説明]

FQDN フィルターで使用するキャッシュのタイマーを設定する。

ip filter コマンド、および **ipv6 filter** コマンドで、始点アドレスおよび、終点アドレスに FQDN を設定している場合、指定した FQDN に一致する通信が発生したとき、タイマーが動作する。 *time* に指定した秒数の間、FQDN フィルターに一致する通信がない場合、FQDN と IP アドレスを対応づけるキャッシュを削除する。

auto=on の場合、タイマーには以下の値が設定される。

- ファストパスを使用する通信のとき、ファストパスのフローテーブルで使用されるタイマーの中で、最も大きい値が本タイマーの値として自動で設定される。
- ファストパスを使用しない通信のとき、*time* の値がタイマーとして設定される。

auto=off の場合は、常に *time* の値がタイマーとして設定される。

[ノート]

RTX5000 は Rev.14.00.26 以降、RTX3500 は Rev.14.00.26 以降、RTX1210 は Rev.14.01.26 以降、RTX830 は Rev.15.02.03 以降、RTX810 は Rev.11.01.28 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830, RTX810

9.1.17 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]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *direction*: 観察するパケット・接続の方向

- [設定値]:

設定値	説明
in	インタフェースの内向き
out	インタフェースの外向き

- [初期値]: -

- *type*: 観察するパケット・接続の種類

- [設定値]:

設定値	説明
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

- [初期値]: -

- *switch*

- [設定値]:

設定値	説明
on	実行する
off	実行しない

- [初期値]:

- TYPE を指定しないとき=off
- TYPE を指定したとき=on

- *option*

- [設定値]:

設定値	説明
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

- [初期値]: off

[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接続について異常を検知する。
type オプション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。

type オプションは Rev.8.03.46、Rev.9.00.15 以降のリビジョンで指定可能で、各パラメータは以下のリビジョン以降で指定可能となっている。

パラメータ	リビジョン
winny、default	Rev.8.03.46、Rev.9.00.15 以降のリビジョン

パラメータ	リビジョン
上記以外のパラメータ	Rev.10.00.38 以降のリビジョン

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.8.03.46、Rev.9.00.15 以降のリビジョンである。

Share については、バージョン 1.0 EX2 (ShareTCP 版) 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.10.00.38 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。
WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.1.18 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
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *frequency*
 - [設定値]: 頻度 (1...1000)
 - [初期値]: 1

[説明]

1 秒間に侵入検知情報を通知する頻度を設定する。

[ノート]

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

9.1.19 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
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *time*

- [設定値]: 秒数 (1..1000)
- [初期値]: 60

[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。

[ノート]

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

9.1.20 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

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *num*
 - [設定値]: 件数 (1..1000)
 - [初期値]: 50

[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。

[ノート]

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

9.1.21 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

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インターフェース名、WAN インターフェース名
 - [初期値]: -
- *type*: 閾値を設定する攻撃の種類
 - [設定値]:

設定値	説明
port-scan.	ポートスキャン

設定値	説明
syn-flood	SYN フラッド

- [初期値]:
 - port-scan=64
 - syn-flood=100
- *count*
 - [設定値]: 閾値 (1..65535)
 - [初期値]: -

[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。

<i>type</i>	<i>count</i> 値の意味
port-scan	同じホストに対して、1秒間に <i>count</i> 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 <i>count</i> 回以上検出したら SYN フラッドと判定する

[適用モデル]
RTX3000

9.1.22 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]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *mss*
 - [設定値]:

設定値	説明
536..1460	MSS の最大長
auto	自動設定
off	設定しない

- [初期値]:
 - auto(RTX1200 Rev.10.01.75 以降、RTX810 Rev.11.01.31 以降、RTX5000 / RTX3500 Rev.14.00.22 以降、RTX1210 Rev.14.01.26 以降、RTX830 Rev.15.02.03 以降、RTX1220)
 - off(上記以外)

[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。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.1.23 TCP ウィンドウ・スケール・オプションを変更する

[書式]

```
ip interface tcp window-scale sw
ip pp tcp window-scale sw
ip tunnel tcp window-scale sw
no ip interface tcp window-scale [...]
no ip pp tcp window-scale [...]
no ip tunnel tcp window-scale [...]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *sw*
 - [設定値]:

設定値	説明
off	何もしない
remove	TCP ウィンドウ・スケール・オプションを削除する

- [初期値]: off

[説明]

インターフェースを通過する TCP パケットのウィンドウ・スケール・オプションを強制的に変更する。remove を指定すると、ウィンドウ・スケール・オプションが有効になっていた場合には、無効にして転送する。

[ノート]

RTX5000、RTX3500 は Rev.14.00.21 以降で使用可能。

RTX1210 は Rev.14.01.16 以降で使用可能。

RTX810 は Rev.11.01.28 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830, RTX810

9.1.24 ルーターが端点となる TCP のセッション数の設定

[書式]

```
tcp session limit limit
no tcp session limit [limit]
```

[設定値及び初期値]

- *limit*: 制限値
- [設定値]:

設定値	説明
32~65535	セッション数
none	制限しない

- [初期値]:
 - 400 (SRT100 Rev.10.00.52 以前、RTX1200 Rev.10.01.22 以前)
 - 15000 (RTX5000 / RTX3500 Rev.14.00.12 以降、Rev.14.01 系以降)
 - 1000 (上記以外)

[説明]

ルーターが端点となる TCP のセッション数を制限する。

none を選択した場合には制限を設けない。

[ノート]

ルーターと直接通信しない場合にはこの制限は適用されない。

RT250i は Rev.8.02.51 以降で使用可能

RTX1100、RTX1500、RT107e は Rev.8.03.87 以降で使用可能

RTX3000 は Rev.9.00.48 以降で使用可能

SRT100 は Rev.10.00.49 以降で使用可能

RTX1200 は Rev.10.01.16 以降で使用可能

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.1.25 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

no ip route change log [log]

[設定値及び初期値]

- log
 - [設定値]:

設定値	説明
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

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.1.26 フィルタリングによるセキュリティーの設定

[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]
```

[設定値及び初期値]

- *interface*

- [設定値]: LAN インターフェース名、WAN インターフェース名、LOOPBACK インターフェース名、NULL インターフェース名、ブリッジインターフェース名
- [初期値]: -

- *direction*

- [設定値]:

設定値	説明
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

- [初期値]: -

- *filter_list*

- [設定値]: 空白で区切られたフィルター番号の並び (静的フィルターと動的フィルターの数の合計として RT250i、および、RT107e、RTX1500、RTX1100 は 128 個以内、RTX3000 の Rev.9.00.47 以降、および、RTX5000、RTX3500 は 300 個以内、他の機種は 129 個以内)
- [初期値]: -

- *set_name*

- [設定値]: フィルターセットの名前を表す文字列
- [初期値]: -

- *dynamic*: キーワード後に動的フィルターの番号を記述する

- [初期値]: -

[説明]

ip filter コマンドによるパケットのフィルターを組み合わせ、インター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ー列をフィルター番号で指定する。指定された番号のフィルターが順番に適用され、パケットにマッチするフィルターが見つければそのフィルターにより通過/破棄が決定する。それ以降のフィルターは調べられない。すべてのフィルターにマッチしないパケットは破棄される。

フィルターセットの名前を指定する書式では、指定されたフィルターセットが適用される。フィルター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ーセットの名前が指定された場合には、フィルターは設定されていないものとして動作する。

[ノート]

フィルターリストを走査して、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、最初のフィルター 1 で通過が決定してしまうため、フィルター 2 での検査は行われない。そのため、フィルター 2 は何も意味を持たない。フィルターリストを操作した結果、どのフィルター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ーセットを適用し、**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ーとして利用される。

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。動的フィルターは **ip policy filter** コマンドを使用する。

LOOPBACK インターフェースと NULL インターフェースでは動的フィルターは使用できない。

NULL インターフェースで *direction* に 'in' は指定できない。

LOOPBACK インターフェース、NULL インターフェースは Rev.8.03 系以降のすべてのファームウェアで指定可能。ブリッジインターフェースは SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

WAN インターフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.1.27 ルールに一致する 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 rule
no ip fragment remove df-bit [rule]
```

[設定値及び初期値]

- *rule*
- [設定値]:

設定値	説明
filter <i>filter_num</i>	<i>filter_num</i> は ip filter コマンドで登録されたフィルタ番号

- [初期値]:-

[説明]

フォワーディングする IP パケットの内、*rule* 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、経路の途中で 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。このような現象は、「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い。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.1.28 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]
```

[設定値及び初期値]

- *id*
 - [設定値]: 識別番号 (1..65535)
 - [初期値]:-
- *tos*
 - [設定値]:
 - 書き換える TOS 値 (0..15)
 - 以下のニーモニックが利用できる

ニーモニック	TOS 値
normal	0
min-monetary-cost	1

ニーモニック	TOS 値
max-reliability	2
max-throughput	4
min-delay	8

- [初期値]: -
- *precedence*
 - [設定値]:
 - precedence 値 (0..7)
 - precedence を省略した場合、PRECEDENCE 値は変更しない
 - [初期値]: -
- *filter_num*
 - [設定値]: 静的フィルタの番号 (1..21474836)
 - [初期値]: -
- *filter_num_list*
 - [設定値]: 静的フィルタの番号 (1..21474836) の並び
 - [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.1.29 代理 ARP の設定

[書式]

```
ip interface proxyarp proxyarp
ip interface proxyarp vrrp vrid
no ip interface proxyarp [proxyarp]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、ブリッジインタフェース名
 - [初期値]: -
- *proxyarp*
 - [設定値]:

設定値	説明
on	代理 ARP 動作をする
off	代理 ARP 動作をしない

- [初期値]: off
- *vrid*
 - [設定値]: VRRP グループ ID (1..255)
 - [初期値]: -

[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。ブリッジインタフェースを指定した時には、ブリッジインタフェースに收容された実 LAN インタフェースにおいて、代理 ARP 動作をするか否か設定する。この時利用する MAC アドレスは ARP を受信した実 LAN インタフェースの 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]

ブリッジインタフェースは SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.1.30 ARP エントリの寿命の設定

[書式]

```
ip arp timer timer [retry]
no ip arp timer [timer [retry]]
```

[設定値及び初期値]

- *timer*
 - [設定値]: ARP エントリの寿命秒数 (30..32767)
 - [初期値]: 1200
- *retry*
 - [設定値]: ARP リクエスト再送回数 (4..100)
 - [初期値]: 4

[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エントリは消される。ただし Rev.8.02 系以降でかつファストパス実装機種では、エントリが消される前に再度 ARP 手順が実行され、その ARP に応答が無い場合にエントリは消される。

retry パラメーターで ARP リクエストの再送回数を設定できる。ARP リクエストの再送間隔は初回は 2 秒、その後は 1 秒である。

retry パラメーターについては、通常は初期値から変更する必要はない。

retry パラメーターは、RTX1200 Rev.10.01.42 以降、RTX810 Rev.11.01.09 以降のファームウェア、および、Rev.14.00 系以降のすべてのファームウェアで指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.1.31 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[...]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *ip_address*
 - [設定値]: IP アドレス
 - [初期値]: -
- *mac_address*
 - [設定値]: MAC アドレス
 - [初期値]: -
- *mtu*

- [設定値]:

設定値	説明
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
64..9578 (RTX3000 の LAN1 / LAN2、および、RTX5000、RTX3500 の LAN インタフェース)	MTU 値
64..1500 (上記以外)	

- [初期値]:-

[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、RTX5000、RTX3500、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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.1.32 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]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]:-
- *len*
 - [設定値]: キュー長 (0..10000)
 - [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)

[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.8.02.28 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.1.33 ARP エントリの変化をログに残すか否かの設定**[書式]**

```
ip interface arp log switch
no ip interface arp log [switch]
```

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
on	記録する
off	記録しない

- [初期値]: off

[説明]

ARP エントリの変更をログに記録するか否かを設定する

[ノート]

show log | grep ARP: を実行することによって、過去の ARP エントリ履歴を確認することができる。
 RTX1500、RTX1100、RT107e は Rev.8.03.82 以降で使用可能。
 RTX3000 は Rev.9.00.47 以降で使用可能。
 SRT100 は Rev.10.00.46 以降で使用可能。
 RTX1200 は Rev.10.01.11 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

9.1.34 implicit 経路の優先度の設定**[書式]**

```
ip implicit-route preference preference
no ip implicit-route preference [preference]
```

[設定値及び初期値]

- *preference*
- [設定値]: implicit 経路の優先度 (1..2147483647)
- [初期値]: 10000

[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、数字が大きいくほど優先度が高い。

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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

9.1.35 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]****[設定値及び初期値]**

- *protocol* : 寿命を指定するプロトコル

- [設定値] :

設定値	説明
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

- [初期値] :

- tcp = 900
- udp = 30
- icmp = 30
- esp = 900 (RTX1500 のみ)
- slow = 30

- *time*

- [設定値] : 秒数 (1-21474836)
- [初期値] : -

[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]

Rev.8.03.75 以降、Rev.10.00.38 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

9.1.36 フローテーブルのエントリー数の設定

[書式]**ip flow limit limit****no ip flow limit [limit]****[設定値及び初期値]**

- *limit*

- [設定値] : 制限値 (10-131072)
- [初期値] : 131072

[説明]

IPv4 ファストパスまたは IPv6 ファストパスのそれぞれで使用可能なフローテーブルのエントリー数を設定する。ファストパス機能使用時でも本制限値を超える分のフローはノーマルパスで処理される。

[ノート]

RTX5000、RTX3500 は Rev.14.00.12 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

9.1.37 フラグメントパケットを再構成するために保持しておく時間を設定

[書式]

ip reassembly hold-time *time*
no ip reassembly hold-time [*time*]

[設定値及び初期値]

- *time*
- [設定値]:

設定値	説明
秒数 (1 .. 255)	フラグメントパケットを再構成するために保持しておく時間

- [初期値]: 15 秒

[説明]

IPv4 のフラグメントパケットを再構成するために保持しておく時間。
 設定した時間が経過しても再構成ができなかった場合、保持していたパケットは破棄される。
 コマンド実行時にすでに保持していたパケットについては変更しない。

[ノート]

RTX5000、RTX3500 は Rev.14.00.29 以降で使用可能。

RTX1210 は Rev.14.01.34 以降で使用可能。

RTX830 は Rev.15.02.10 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

9.2 PP 側の設定

9.2.1 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*]

[設定値及び初期値]

- *ip_address*
- [設定値]:

設定値	説明
IP アドレス	xxx.xxx.xxx.xxx (xxx は十進数)
dhcp	DHCP クライアントを利用することを示すキーワード

- [初期値]: -
- dhcpc: DHCP クライアントを利用することを示すキーワード
- [初期値]: -
- *interface*
- [設定値]:

- 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
- [初期値]:-

[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。

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。

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.2.2 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
```

[設定値及び初期値]

- *ip_address*
 - [設定値]: anonymous のためにプールする IP アドレス
 - [初期値]:-
- *ip_address-ip_address*
 - [設定値]: IP アドレスの範囲
 - [初期値]:-
- *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
 - [初期値]:-
- *dhcpc*: DHCP クライアントを利用することを示すキーワード
 - [初期値]:-
- *interface*
 - [設定値]:
 - 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
 - [初期値]:-

[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。

[ノート]

ip_address として設定できる数は下記の通り。

機種	ファームウェア	最大設定可能数
RTX5000	すべてのリビジョン	3104
RTX3500	すべてのリビジョン	1104
RTX3000	すべてのリビジョン	56
RTX1500	Rev.8.03.92 ~	136
	Rev.8.02.19 ~	76
	Rev.8.02.14 ~	88
RTX1220	すべてのリビジョン	101
RTX1210	すべてのリビジョン	103
RTX1200	Rev.10.01.32 ~	123
	Rev.10.01.07 ~	93
RTX1100	Rev.8.03.92 ~	74
	Rev.8.02.31 ~	44
RTX830	すべてのリビジョン	32
RTX810	すべてのリビジョン	18
RT250i	すべてのリビジョン	40
RT107e	Rev.8.03.92 ~	10
	Rev.8.03.15 ~	4
SRT100	Rev.10.00.60 ~	16
	Rev.10.00.52 ~	6
	Rev.10.00.08 ~	5

[拡張ライセンス対応]

拡張ライセンスをインポートすると、プールできる IP アドレス (*ip_address*) の最大個数が拡張される。

- *ip_address*

ライセンス名	拡張後の最大個数
YSL-VPN-EX1	101

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.2.3 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*]]

[設定値及び初期値]

- *interval*

- [設定値]: キープアライブパケットを送出する時間間隔[秒] (1..65535)
- [初期値]: 30
- *retry-interval*
 - [設定値]:
 - 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[秒] (1..65535)
 - 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
 - [初期値]: 1
- *count*
 - [設定値]: 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)
 - [初期値]: 6
- *time*
 - [設定値]:
 - 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[秒] ($(interval + 1) \cdot 65535$)
 - *count* パラメータとは同時には指定できない
 - [初期値]: -

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.2.4 PP 経路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
```

[設定値及び初期値]

- *lcp-echo*: LCP Echo Request/Reply を用いる
 - [初期値]: -
- *icmp-echo*: ICMP Echo/Reply を用いる
 - [初期値]: -
- *dest_ip*
 - [設定値]: キープアライブ確認先の IP アドレス
 - [初期値]: -
- *option=value* 列
 - [設定値]:

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)

option	value	説明
downwait	ミリ秒	ダウン検知のための許容応答時間 (1..10000)
disconnect	秒	無応答切断時間 (1..21474836)
length	バイト	ICMP Echo パケットの長さ (64-1500)

- [初期値]: -

[初期設定]

pp keepalive use off

[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、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.8.02.35 以降で指定可能である。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.2.5 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]

[設定値及び初期値]

- log
- [設定値]:

設定値	説明
on	ログをとる
off	ログをとらない

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.2.6 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*]

[設定値及び初期値]• *action*

- [設定値]:

設定値	説明
silent	何もしない
reset	ルーターを再起動する

- [初期値]: silent

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

9.3 RIP の設定**9.3.1 RIP を使用するか否かの設定****[書式]**

rip use *use*

no rip use [*use*]

[設定値及び初期値]• *use*

- [設定値]:

設定値	説明
on	RIP を使用する
off	RIP を使用しない

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.3.2 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* [*gateway*...]

ip pp rip trust gateway [except] *gateway* [*gateway*...]

ip tunnel rip trust gateway [except] *gateway* [*gateway*...]

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

no ip pp rip trust gateway [[except] *gateway* [*gateway*...]]

no ip tunnel rip trust gateway [[except] *gateway* [*gateway*...]]

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *gateway*
 - [設定値]: IP アドレス
 - [初期値]: -

[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。

`gateway` は 10 個まで指定可能。

[ノート]

RT250i には `ip tunnel rip trust gateway` コマンドはない。

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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.3.3 RIP による経路の優先度の設定**[書式]**

`rip preference preference [invalid-route-reactivate=switch]`

`no rip preference [preference [invalid-route-reactivate=switch]]`

[設定値及び初期値]

- *preference*
 - [設定値]: 1 以上の数値
 - [初期値]: 1000
- *switch*
 - [設定値]:

設定値	説明
on	無効となった RIP 由来の経路を削除しない
off	無効となった RIP 由来の経路を削除する

- [初期値]: off

[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。

RIP で他のルーターから経路を受信しているとき、スタティックや OSPF など RIP より優先度が高く設定されたルーティングプロトコルで同じ経路を受信した場合、通常 RIP により受信した経路は無効となって削除されるが、`invalid-route-reactivate` オプションを `on` で指定している場合、優先度が高い経路が消滅したときに無効になっていた RIP 由来の経路を再有効化する。

[ノート]

スタティック経路の優先度は 10000 で固定である。

`invalid-route-reactivate` オプションを `on` で指定しているとき、再有効化した経路を RIP の発信元が広告しなくなっても当該経路がルーティングテーブル上に残り続けることがあるため、`invalid-route-reactivate` オプションは `off` にする

ことが望ましい。

なお、上記のルーティングテーブルに残った経路は、RIP の使用を停止することで削除できる。

invalid-route-reactivate オプションは RTX3000 Rev.9.00.60 以降、SRT100 Rev.10.00.61 以降、RTX1200 Rev.10.01.47 以降、RTX810 Rev.11.01.19 以降のファームウェア、および、Rev.14.00 系以降のすべてのファームウェアで指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.3.4 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...]

[設定値及び初期値]

- *interface*

- [設定値]: LAN インタフェース名
- [初期値]: -

- *send*

- [設定値]:

設定値	説明
on	RIP パケットを送信する
off	RIP パケットを送信しない

- [初期値]:

- off (トンネルインタフェースの場合)
- on (その他のインタフェースの場合)

- *version*

- [設定値]: 送信する RIP のバージョン (1,2)
- [初期値]: 1 (トンネルインタフェース以外の場合)

- *broadcast*

- [設定値]: **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
- [初期値]: -

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.3.5 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...]

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *receive*
 - [設定値]:

設定値	説明
on	RIP パケットを受信する
off	RIP パケットを受信しない

- [初期値]:
 - off(トンネルインタフェースの場合)
 - on(その他のインタフェースの場合)
- *version*
 - [設定値]: 受信する RIP のバージョン (1,2)
 - [初期値]: 1 2 (トンネルインターフェース以外の場合)

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.3.6 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

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *direction*
 - [設定値]:

設定値	説明
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

- [初期値]: -
- *filter_list*
 - [設定値]: 空白で区切られた静的フィルタ番号の並び (100 個以内)
 - [初期値]: -

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.3.7 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
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *direction*
 - [設定値]:

設定値	説明
in	受信した RIP に加算する
out	送信する RIP に加算する

- [初期値]: -
- *hop*
 - [設定値]: 加算する値 (0..15)
 - [初期値]: 0

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.3.8 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]
```

[設定値及び初期値]

- *interface*

- [設定値]: LAN インタフェース名
- [初期値]: -
- *type*
 - [設定値]:

設定値	説明
text	テキスト型の認証を行う

- [初期値]: -

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.3.9 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
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *hex_key*
 - [設定値]: 十六進数の列で表現された認証キー
 - [初期値]: -
- *text_key*
 - [設定値]: 文字列で表現された認証キー
 - [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.3.10 RIP2 での広告動作モードの設定

[書式]

rip advertise mode *mode*

no rip advertise mode [*mode*]

[設定値及び初期値]

- *mode*

- [設定値]:

設定値	説明
1	RIP の送信インターフェースが属するネットワークアドレスと広告する経路の宛先ネットワークアドレスが一致し、サブネットマスクが異なる場合は、その経路を広告しない。
2	RIP の送信インターフェースが属するネットワークアドレスと広告する経路の宛先ネットワークアドレスが一致し、サブネットマスクが異なる場合は、その経路を広告する。

- [初期値]: 1

[説明]

RIP2 で RIP 送信インターフェースが属するネットワークアドレスと広告する経路の宛先ネットワークアドレスが一致し、サブネットマスクが異なる場合、当該経路の広告動作を *mode* の設定値によって変更する。

本コマンドに対応していないリビジョンでは、*mode* の設定値が 1 のときの動作をする。

RIP1 の動作には影響はない。

[ノート]

RTX5000 は Rev.14.00.32 以降で使用可能

RTX3500 は Rev.14.00.32 以降で使用可能

RTX1210 は Rev.14.01.36 以降で使用可能

RTX830 は Rev.15.02.15 以降で使用可能

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

9.3.11 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*]

[設定値及び初期値]

- *rip_hold*

- [設定値]:

設定値	説明
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

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.3.12 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]
```

[設定値及び初期値]

- *rip_action*
- [設定値]:

設定値	説明
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

- [初期値]: update

[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。

[設定例]

```
# ip pp rip connect interval 60
# ip pp rip connect send interval
```

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.3.13 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]
```

[設定値及び初期値]

- *time*
- [設定値]: 秒数 (30..21474836)
- [初期値]: 30

[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。

[設定例]

```
# ip pp rip connect interval 60
# ip pp rip connect send interval
```

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.3.14 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]
```

[設定値及び初期値]

- *rip_action*

- [設定値]:

設定値	説明
none	回線切断時に RIP を送出不しい
interval	ip pp rip disconnect interval コマンドで設定された時間間隔で RIP を送出手する
update	経路情報が変わった時にのみ RIP を送出手する

- [初期値]: none

[説明]

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

[設定例]

```
# ip pp rip disconnect interval 1800
# ip pp rip disconnect send interval
```

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.3.15 回線切断時の PP 側の RIP 送出手の時間間隔の設定

[書式]

```
ip pp rip disconnect interval time
no ip pp rip disconnect interval [time]
```

[設定値及び初期値]

- *time*
 - [設定値]: 秒数 (30..21474836)
 - [初期値]: 3600

[説明]

選択されている相手について回線切断時に RIP を送出手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。

[設定例]

```
# ip pp rip disconnect interval 1800
# ip pp rip disconnect send interval
```

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.3.16 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
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	切り替える
off	切り替えない

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.3.17 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]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *ip-address/netmask*
 - [設定値]: 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'
 - [初期値]: -
- *metric*
 - [設定値]: 広告する際のメトリック値 (1~15)
 - [初期値]: 1

[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 系以降

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

9.3.18 RIP2 でのフィルタの比較方法**[書式]**

```
rip filter rule rule
no rip filter rule [rule]
```

[設定値及び初期値]

- *rule*
- [設定値]:

設定値	説明
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

- [初期値]: address-only

[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	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、RIP エントリのアドレス、ネットマスクと一致するかどうかを比較する。
	RIP2	

[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

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

9.3.19 RIP のタイマーを調整する**[書式]**

```
rip timer update [invalid [holddown]]
no rip timer [update]
```

[設定値及び初期値]

- *update*
 - [設定値]: 定期的な広告の送信間隔 (10~60 (秒))
 - [初期値]: 30 秒
- *invalid*
 - [設定値]: 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))
 - [初期値]: update×6 (180 秒)
- *holddown*
 - [設定値]: 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))
 - [初期値]: update×4 (120 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。

$$\begin{aligned} update \times 3 &\leq invalid \leq update \times 6 \\ update \times 2 &\leq holddown \leq update \times 4 \end{aligned}$$

[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、各タイマーは以下ようになる。

<i>update</i>	T
<i>invalid</i>	T×6
<i>holddown</i>	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

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

9.4 VRRP の設定

9.4.1 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...]

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *vrid*
 - [設定値]: VRRP グループ ID (1..255)
 - [初期値]: -
- *ip_address*
 - [設定値]: 仮想ルーターの IP アドレス
 - [初期値]: -
- *priority*
 - [設定値]: 優先度 (1..254)
 - [初期値]: 100
- *preempt*: プリエンプトモード
 - [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: on

- *auth*
 - [設定値]: テキスト認証文字列 (8 文字以内)
 - [初期値]: -
- *time1*
 - [設定値]: VRRP 広告の送信間隔 (1..60 秒)
 - [初期値]: 1
- *time2*
 - [設定値]: マスターがダウンしたと判定するまでの時間 (3..180 秒)
 - [初期値]: 3

[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なくてはならない。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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.4.2 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 tunnel tunnel_num
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 tunnel tunnel_num
no ip interface vrrp shutdown trigger vrid route network
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *vrid*
 - [設定値]: VRRP グループ ID (1..255)
 - [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *dlci*
 - [設定値]: DLCI 番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: tunnel インターフェース 番号

- [初期値]:-
- *network*
 - [設定値]:
 - ネットワークアドレス
 - IP アドレス/マスク長
 - default
 - [初期値]:-
- *nexthop*
 - [設定値]:
 - インタフェース名
 - IP アドレス
 - [初期値]:-

[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。

形式	説明
LAN インタフェース形式	指定した LAN インタフェースがリンクダウンするか、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	<p>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。</p> <ul style="list-style-type: none"> • 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”<i>dlci=dlci</i>”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
tunnel 形式	<p>指定した tunnel インターフェースが以下の条件によりダウンした場合にシャットダウンする。</p> <ul style="list-style-type: none"> • IPsec トンネルで、ipsec ike keepalive use 設定によりダウンが検出された場合 • L2TP/IPsec、L2TPv3、L2TPv3/IPsec のいずれかのトンネルで、l2tp keepalive use 設定によりダウンが検出された場合 • PPTP トンネルで、pptp keepalive use 設定によりダウンが検出された場合 • IPIP トンネルで、ipip 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、 <i>nexthop</i> 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。 <i>nexthop</i> 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。

[ノート]

tunnel インターフェースは RTX5000 / RTX3500 Rev.14.00.32 以降、RTX1210 Rev.14.01.28 以降、RTX830 Rev.15.02.03 以降、RTX1220 のファームウェアで使用可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.5 バックアップの設定

9.5.1 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
```

[設定値及び初期値]

- none : バックアップ動作しない
 - [初期値] : none
- *peer_num*
 - [設定値] : 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
 - [初期値] : -
- *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
 - [設定値] :

設定値	説明
on	再構築する
off	再構築しない

- [初期値] : off
- *interface*
 - [設定値] : バックアップ先として使用する LAN インタフェース
 - [初期値] : -
- *ip_address*
 - [設定値] : ゲートウェイの IP アドレス
 - [初期値] : -
- *tunnel_num*
 - [設定値] : トンネルインタフェース番号
 - [初期値] : -

[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 use lcp-echo** コマンドを使用する。
RT107e は R ev.8.03.42 以降で使用可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e

9.5.2 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*]

[設定値及び初期値]

- *time*
- [設定値]:

設定値	説明
1..21474836	秒数
off	すぐに復帰

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e

9.5.3 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

[設定値及び初期値]

- none : バックアップ動作しない
 - [初期値]: none
- *interface*
 - [設定値]: バックアップ対象の LAN インタフェース名
 - [初期値]: -

- *peer_num*
 - [設定値]: バックアップとして **pp** を使用する場合は相手先情報番号
 - [初期値]: -
- *backup_interface*
 - [設定値]: バックアップとして使用する LAN インタフェース
 - [初期値]: -
- *ip_address*
 - [設定値]: ゲートウェイの IP アドレス
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -

[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。

[拡張ライセンス対応]

[拡張ライセンス](#) をインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e

9.5.4 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]

[設定値及び初期値]

- *interface*
 - [設定値]: バックアップ対象の LAN インタフェース名
 - [初期値]: -
- *time*
 - [設定値]:
 - 秒数 (1..21474836)
 - off
 - [初期値]: 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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e

9.5.5 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 [...]
```

[設定値及び初期値]

- *interface*
 - [設定値]: バックアップ対象の LAN インタフェース名
 - [初期値]: -
- *dest_ip*
 - [設定値]: キープアライブ確認先の IP アドレス
 - [初期値]: -
- *option = value 列*
 - [設定値]:

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)

- [初期値]: -

[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.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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e

9.5.6 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
```

[設定値及び初期値]

- *interface*

- [設定値]: バックアップ対象の LAN インタフェース名
- [初期値]: -
- *interval*
 - [設定値]: キープアライブパケットを送出する時間間隔 (1..65535)
 - [初期値]: 30
- *count*
 - [設定値]: ダウン検出を判定する回数 (3..100)
 - [初期値]: 6

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e

9.5.7 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
```

[設定値及び初期値]

- *interface*
 - [設定値]: バックアップ対象の LAN インタフェース名
 - [初期値]: -
- *log*
 - [設定値]:

設定値	説明
on	ログをとる
off	ログをとらない

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e

9.5.8 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
```

[設定値及び初期値]

- *num*
 - [設定値]: このコマンドの識別番号 (1..100; RTX5000 は 1...3000; RTX3500、RTX3000 は 1...1000)
 - [初期値]: -
- *kind*: 監視方式
 - [設定値]:

設定値	説明
icmp-echo	ICMP Echo を使用する

- [初期値]: -
- *interval*
 - [設定値]: キープアライブの送信間隔秒数 (1..65535)
 - [初期値]: -
- *count*
 - [設定値]: 到達性がないと判断するまでに送信する回数(3..100)
 - [初期値]: -
- *gateway*: 複数指定可 (10 個以内)
 - [設定値]:
 - IP アドレス
 - xxx.xxx.xxx.xxx (xxx は十進数)
 - *dhcp interface*
 - RTX1220、RTX1210、RTX1200、RTX830、RTX810、SRT100、RT107e と RTX5000 / RTX3500 Rev. 14.00.29 以降で指定可

設定値	説明
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 インタフェース名または WAN インタフェース名

- [初期値]: -
- *option=value 列*
- [設定値]:

<i>option</i>	<i>value</i>	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)
local-address	IP アドレス	始点 IP アドレス
ipsec-refresh	セキュリティ・ゲートウェイの識別子 (<i>gateway_id</i>)	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 (<i>gateway_id</i>)	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 (<i>gateway_id</i>)	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)

option	value	説明
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

- [初期値]:
 - log=off
 - upwait=5
 - downwait=5
 - length=64
 - gateway-selection-rule=head

[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]

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.8.02.35 以降、Rev.8.03 系以降で指定可能である。

local-address パラメータは、Rev.8.03.87 以降、Rev.9.00.47 以降、Rev.10.00.49 以降、Rev.10.01.16 以降、Rev.11.01 系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、Rev.8.03.68 以降、Rev.9.00.31 以降、Rev.10.00.31 以降、Rev.10.01 系以降で指定可能である。

gateway-selection-rule パラメータは、Rev.8.03.68 以降、Rev.9.00.24 以降、Rev.10.00.22 以降、Rev.10.01 系以降で指定可能である。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[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
```

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- gateway_id

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

9.6 IGMP の設定

9.6.1 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...]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *type*: IGMP の動作方式
 - [設定値]:

設定値	説明
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

- [初期値]: off
- *option*
 - [設定値]:
 - version=*version*
 - IGMP のバージョン

設定値	説明
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

設定値	説明
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

設定値	説明
on	ランダムな遅延後に転送する
off	即座に転送する

- [初期値]:
 - version=2,3
 - syslog=off
 - robust-variable=2

- delay-timer=on

[説明]

インタフェースの IGMP の動作を設定する。

[適用モデル]

RTX3000, RTX1500

9.6.2 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...]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *group*
 - [設定値]: グループのマルチキャストアドレス
 - [初期値]: -
- *filter_mode*: フィルタモード
 - [設定値]:

設定値	説明
include	IGMP の "INCLUDE" モード
exclude	IGMP の "EXCLUDE" モード

- [初期値]: -
- *source*

- [設定値]:

設定値	説明
IPv4 アドレス	マルチキャストパケットの送信元アドレス
省略	省略時はすべての送信元アドレスに対して同様に動作する

- [初期値]: -

[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。*source* を省略した場合は、全ての送信元からの要求を受信しない。

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。*source* を省略した場合は、全ての送信元からの要求を受信する。

[適用モデル]

RTX3000, RTX1500

9.7 PIM-SM の設定

9.7.1 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...]]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *switch*: PIM-SM が動作するか否か
 - [設定値]:

設定値	説明
off	動作しない
on	動作する

- [初期値]: off
- *option*
 - [設定値]:
 - dr-priority=*priority*
 - DR priority

設定値	説明
off	DR priority を送信しない
1..255	優先度

- 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

設定値	説明
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

- [初期値]:
 - dr-priority=1
 - register-checksum=header
 - holdtime=60

[説明]

インタフェースの PIM-SM の動作を設定する。

[適用モデル]

RTX3000, RTX1500

9.7.2 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
```

[設定値及び初期値]

- *group*
 - [設定値]: IP アドレス/マスク長 (マスク長は省略可)
 - [初期値]: -
- *rendezvous_point*

- [設定値]: RP の IP アドレス
- [初期値]: -
- *priority*
 - [設定値]: 優先度 (1-200)
 - [初期値]: -

[説明]

RP のグループの対応を静的に定義する。

[適用モデル]

RTX3000, RTX1500

9.7.3 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 ...]
```

[設定値及び初期値]

- *option*: 出力する詳細なログの種類を指定する
 - [設定値]:

設定値	説明
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

- [初期値]: -

[説明]

PIM-SM に関する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。

[適用モデル]

RTX3000, RTX1500

9.7.4 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]
```

[設定値及び初期値]

- *size*: register パケットの checksum 計算範囲
 - [設定値]:

設定値	説明
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

- [初期値]: header

[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。

[適用モデル]

RTX3000, RTX1500

9.7.5 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]
```

[設定値及び初期値]

- *cast*
- [設定値]:

設定値	説明
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

- [初期値]: unicast

[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。

[適用モデル]

RTX3000, RTX1500

9.7.6 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]
```

[設定値及び初期値]

- *sw*
- [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: on

[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。

[適用モデル]

RTX3000, RTX1500

9.8 受信パケット統計情報の設定**9.8.1 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]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *switch*
 - [設定値]:

設定値	説明
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

- [初期値]: off

[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。
RTX3000 の Rev.9.00.24 以降、および、RTX5000、RTX3500 で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000

9.8.2 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]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]: 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
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネル番号、省略時は選択されているトンネル番号
 - [初期値]: -

[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]
RTX5000, RTX3500, RTX3000

9.8.3 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]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]: 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
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネル番号、省略時は選択されているトンネル番号
 - [初期値]: -

[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]
RTX5000, RTX3500, RTX3000

9.8.4 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]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *value*
 - [設定値]: 統計情報に記録するパケットの最大分類数 (64..5000)
 - [初期値]: 64

[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。

RTX3000 の Rev.9.00.24 以降、および、RTX5000、RTX3500 で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000

9.9 パケット転送フィルターの設定

9.9.1 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]]
```

[設定値及び初期値]

- *id*
 - [設定値]: パケット転送フィルターの識別子 (1..255)
 - [初期値]: -
- *order*
 - [設定値]: 評価の順番 (1..255)
 - [初期値]: -
- *gateway*
 - [設定値]:

設定値	説明
IP アドレス	パケットを転送するゲートウェイの IP アドレス
wan1	WAN インタフェース
pp peer_num	PP インタフェース
tunnel tunnel_num	TUNNEL インタフェース

- [初期値]: -
- *filter_id*
 - [設定値]: **ip filter** コマンドの識別子
 - [初期値]: -
- *keepalive_id*
 - [設定値]: **ip keepalive** コマンドの識別子
 - [初期値]: -

[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]

RTX1500、RTX1100、RT107e は Rev.8.03.68 以降で使用可能。

RTX3000 は Rev.9.00.24 以降で使用可能。

WAN インタフェースは RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e

9.9.2 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]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *id*
 - [設定値]: **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)
 - [初期値]: -

[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。

WAN インタフェースは RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e

第 10 章

イーサネットフィルタの設定

10.1 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 ...]
```

[設定値及び初期値]

• num

- [設定値]:

設定値	説明
1..512 (RTX1210 Rev.14.01.16 以降、Rev.15.02 系以降)	静的フィルタの番号
1..100 (上記以外)	

- [初期値]: -

• kind

- [設定値]:

設定値	説明
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)

- [初期値]: -

• src_mac

- [設定値]:

- 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)

- [初期値]: -

• dst_mac

- [設定値]:

- 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

- [初期値]: -

• type

- [設定値]:

設定値	説明
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
dhcp-scope	指定された DHCP スコープでアドレスがリースされているホストを対象にする

設定値	説明
dhcp-not-scope	指定された DHCP スコープでアドレスがリースされていないホストを対象にする

- [初期値]: -
- *scope*
 - [設定値]:
 - 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
 - [初期値]: -
- *offset*
 - [設定値]: 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)
 - [初期値]: -
- *byte_list*
 - [設定値]:
 - 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)
 - [初期値]: -

[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、dhcp-not-bind 型のフィルタでは始点 MAC アドレスが DHCP スコープで予約されていないときに、dhcp-not-scope 型のフィルタでは始点 MAC アドレスが DHCP スコープでアドレスがリースされていないときにフィルタに合致するとみなす。

dhcp-bind、dhcp-not-bind、dhcp-scope、dhcp-not-scope 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、ルーター内部でイーサネットタイプとして 0x8100~0x810f の値を使用しているため、それらのイーサネットフレームをフィルタして送受信できないようにすると、LAN 分割機能を使用しているポートで通信できなくなるので注意が必要である。

dhcp-bind、dhcp-not-bind、dhcp-scope、dhcp-not-scope 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 の予約情報もしくはリースしたアドレスと一致することはない。

dhcp-bind、dhcp-scope 型フィルタは、予約もしくはアドレスがリース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、dhcp-not-scope 型フィルタは、予約もしくはアドレスがリース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ようになる。

dhcp-scope 型と dhcp-not-scope 型は SRT100 の Rev.10.00.44 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

10.2 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]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *dir*
 - [設定値]:

設定値	説明
in	LAN 側から入ってくるパケットのフィルタリング
out	LAN 側に出っていくパケットのフィルタリング

- [初期値]: -
- *list*
 - [設定値]:

設定値	説明
空白で区切られた静的フィルタ番号の並び	512 個以内 (Rev.14.01.16 以降)
	100 個以内 (上記以外)

- [初期値]: -

[説明]

LAN 側を通るパケットについて、**ethernet filter** コマンドによるパケットのフィルタを組み合わせ、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は、物理 LAN インタフェースおよび LAN 分割機能で使用するインタフェースを指定できる。Rev.10.01 系では、LAN 分割機能で使用するインタフェースとして VLAN インタフェースを指定できる。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

10.3 イーサネットフィルタの状態の表示

[書式]**show status ethernet filter type [scope]****[設定値及び初期値]**• *type*

- [設定値]:

設定値	説明
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
dhcp-scope	指定された DHCP スコープでアドレスがリースされているホスト

- [初期値]: -

• *scope*

- [設定値]: スコープ番号 (1-65535)

- [初期値]: -

[説明]

イーサネットフィルタの情報を表示する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

第 11 章

入力遮断フィルタの設定

11.1 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]]]]]
```

[設定値及び初期値]

- *id*
 - [設定値]: フィルタの識別子 (1..65535)
 - [初期値]: -
- *action*: 動作
 - [設定値]:

設定値	説明
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
 - [初期値]: -
- *src_address*: 始点アドレス
 - [設定値]:
 - 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。
 - [初期値]: -
- *dst_address*: 終点アドレス
 - [設定値]:
 - *src_address* と同じ形式
 - 省略時は 1 個の * と同じ。
 - [初期値]: -
- *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)
 - [設定値]:
 - 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
 - [初期値]: -
- *protocol*: プロトコル
 - [設定値]:
 - 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

ニーモニック	10 進数	説明
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
- [初期値]:-
- src_port: ソースポート番号
- [設定値]:
 - 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
ident	113
ntp	123
nntp	119

ニーマニツク	ポート番号
snmp	161
syslog	514
printer	515
talk	517
route	520
uucp	540
submission	587

- 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。
- [初期値]: -
- *dst_port*: デスティネーションポート番号
 - [設定値]:
 - 書式は *src_port* と同じ。
 - [初期値]: -

[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。

[ノート]

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* と *dst_port* 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と比較される。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* と *dst_port* の指定は存在しないものとしてフィルタと比較される。

[適用モデル]

SRT100

11.2 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 ...]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *id*
 - [設定値]: **ip/ipv6 inbound filter** コマンドで定義したフィルタの識別子

- [初期値]:-

[説明]

ip/ipv6 inbound filter コマンドによる設定を組み合わせ、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。

[ノート]

WAN インタフェースは Rev.10.00.60 以降で指定可能。ただし、**ipv6 inbound filter** コマンドでは、WAN インタフェースを指定できない。

[適用モデル]

SRT100

第 12 章

ポリシーフィルタの設定

12.1 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]]]
```

[設定値及び初期値]

- *id*
 - [設定値]: サービスの識別子 (1..65535)
 - [初期値]: -
- *service_name*
 - [設定値]: サービスの名前 (最大 16 文字まで)
 - [初期値]: -
- *protocol*
 - [設定値]: プロトコル (tcp,udp,icmp,ipv6,rsvp,gre,esp,ah,icmp6,icmpv6,ospf,pim)
 - [初期値]: -
- *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)
 - [設定値]:

設定値	説明
*	すべて
0..65535	番号
例 :6000-, 6000-6010、-6010	番号の範囲

- [初期値]: -
- *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)
 - [設定値]:
 - 書式は source_port と同じ。
 - [初期値]: -

[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。

[適用モデル]

SRT100

12.2 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 ...]
```

[設定値及び初期値]

- *id*

- [設定値]: インタフェースグループの識別子 (1..65535)
- [初期値]: -
- *name*
 - [設定値]: 名前 (半角 32 文字以内)
 - [初期値]: -
- *interface*: インタフェース
 - [設定値]:

設定値	説明
*	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
wan1	WAN インタフェース
ppN	PP インタフェース
ppanonymous	anonymous インタフェース
tunnelN	TUNNEL インタフェース
local	ルーター自身

- [初期値]: -
- *group_id*
 - [設定値]: 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)
 - [初期値]: -

[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。

[ノート]

WAN インタフェースは Rev.10.00.60 以降で指定可能。
 Rev.10.00.61 以降の SRT100 で *interface* に ppanonymous を指定可能となり、*や pp*を指定した場合は anonymous インタフェースも含まれる。

[適用モデル]
 SRT100

12.3 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 ...]
```

[設定値及び初期値]

- *id*
 - [設定値]: アドレスグループの識別子 (1..65535)
 - [初期値]: -

- *name*
 - [設定値]: 名前 (半角 32 文字以内)
 - [初期値]: -
- *address*: アドレス
 - [設定値]:

設定値	説明
*	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
qac-tm-server	QAC/TM の管理サーバ PC

- [初期値]: -
- *group_id*
 - [設定値]: 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)
 - [初期値]: -

[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。

[ノート]

'qac-tm-server' は、**ip policy address group** コマンドでのみ指定可能。

[適用モデル]

SRT100

12.4 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 ...]
```

[設定値及び初期値]

- *id*
 - [設定値]: サービスグループの識別子 (1..65535)
 - [初期値]: -
- *name*
 - [設定値]: 名前 (半角 32 文字以内)
 - [初期値]: -
- *service*: サービス
 - [設定値]:

設定値	説明
*	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
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

- [初期値]: -
- *group_id*

- [設定値]: 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)
- [初期値]: -

[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]
SRT100

12.5 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]]]]]]
```

[設定値及び初期値]

- *id*
 - [設定値]: ポリシーフィルタの識別子 (1..65535)
 - [初期値]: -
- *action*: 動作
 - [設定値]:

設定値	説明
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さ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

- [初期値]: -
- *source_interface*: 始点インタフェース
 - [設定値]:

設定値	説明
*	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)

設定値	説明
lanN	LAN インタフェース
wan1	WAN インタフェース
ppN	PP インタフェース
ppanonymous	anonymous 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

- [初期値]:-
- *dest_interface*: 終点インタフェース
 - [設定値]:
 - 書式は始点インタフェースと同じ
 - [初期値]:-
- *source_address*: 始点アドレス
 - [設定値]:

設定値	説明
*	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

- [初期値]:-
- *dest_address*: 終点アドレス
 - [設定値]:
 - 書式は始点アドレスと同じ
 - [初期値]:-
- *service*: サービス
 - [設定値]:

設定値	説明
*	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
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

- [初期値]:-

[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。
 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。

[ノート]

WAN インタフェースは Rev.10.00.60 以降で指定可能。
 Rev.10.00.61 以降の SRT100 で *source_interface*、*dest_interface* に *ppanonymous* を指定可能となり、*や *pp**を指定した場合は *anonymous* インタフェースも含まれる。

[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]

SRT100

12.6 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 ...]
```

[設定値及び初期値]

- *id*
 - [設定値]: ポリシーセットの識別子 (1..65535)
 - [初期値]: -
- *name*
 - [設定値]: 名前 (半角 32 文字以内)
 - [初期値]: -
- *filter_set*
 - [設定値]:
 - 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
 - [初期値]: -

[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。

[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]

SRT100

12.7 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]
```

[設定値及び初期値]

- *id*

- [設定値]: ポリシーセットの識別子 (1..65535)
- [初期値]: -

[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。

[適用モデル]

SRT100

12.8 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] [recoverytime=time]
ipv6 policy filter set switch original backup trigger trigger ... [count=count] [interval=interval] [recoverytime=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]]
```

[設定値及び初期値]

- *original*
 - [設定値]: 切り替え元のポリシーセットの番号 (1..65535)
 - [初期値]: -
- *backup*
 - [設定値]: 切り替え後のポリシーセットの番号 (1..65535)
 - [初期値]: -
- *trigger*: 切り替えのトリガ
 - [設定値]:

設定値	説明
winny	不正アクセス検知機能で Winny を検知したとき
share2	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

- [初期値]: -
- *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。
 - [設定値]:
 - 1..10
 - [初期値]: 1[回]
- *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。
 - [設定値]:
 - 秒数 (2..600)
 - [初期値]: 5[秒]
- *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
 - [設定値]:

設定値	説明
60..604800	秒数
infinity	ポリシーセットを元に戻さない

- [初期値]: 3600[秒]

[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 trigger winny**
- **ip policy filter set switch 1 3 trigger ethernet-filter**
- **ip policy filter set switch 1 4 trigger 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。

[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]

SRT100

12.9 タイマーの設定

[書式]

ip policy filter timer [*option=timeout ...*]

no ip policy filter timer

[設定値及び初期値]

- *option* : オプション名
- [設定値] :

設定値	説明
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

設定値	説明
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)

- [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
- *timeout*
 - [設定値]: タイムアウト時間 (秒)
 - [初期値]: -

[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。

[適用モデル]

SRT100

第 13 章

URL フィルタの設定

13.1 フィルタ定義の設定

[書式]

```
url filter id kind keyword [src_addr[/mask]]
```

```
no url filter id
```

[設定値及び初期値]

- *id*

- [設定値]: フィルタ番号 (1..65535)
- [初期値]: -

- *kind*

- [設定値]:

設定値	説明
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)

- [初期値]: -

- *keyword*

- [設定値]:

設定値	説明
任意の文字列	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

- [初期値]: -

- *src_addr*: IP パケットの始点 IP アドレス

- [設定値]:

設定値	説明
任意の IPv4 アドレス	1 個の IPv4 アドレス
範囲指定	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	省略時は * と同じ

- [初期値]: -

- *mask*

- [設定値]: 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)
- [初期値]: -

[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* をコマ (,) で区切って複数指定することができる。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

13.2 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 dir

no url pp filter dir

no url tunnel filter dir

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *dir*
 - [設定値]:

設定値	説明
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

- [初期値]: -
- *list*
 - [設定値]: 空白で区切られた URL フィルタ番号の並び (512 個以内...RTX5000/RTX3500/RTX3000, 128 個以内...他の機種)
 - [初期値]: -

[説明]

url filter コマンドで設定したフィルタを組み合わせ、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、RTX5000、RTX3500、RTX3000 では 512 個以内、他の機種では 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]

RTX1100、RT107e は Rev.8.03.60 以降で使用可能。

RTX3000 は Rev.9.00.31 以降で使用可能。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

13.3 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

[設定値及び初期値]

- *list*
 - [設定値]: 空白で区切られたポート番号の並び (4 個以内)
 - [初期値]: 80

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

13.4 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
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
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

- [初期値]: on

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

13.5 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]
```

[設定値及び初期値]

- *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
 - [初期値]: *redirect* (RTX5000、RTX3500、RTX3000 以外の場合)
- *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
 - [初期値]: *off* (RTX5000、RTX3500、RTX3000 の場合)
- *url*
 - [設定値]: 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)
 - [初期値]: -
- *action*
 - [設定値]:
 - *redirect*

- off
- [初期値]:-

[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、SRT100 ... Rev.10.00.38 以降、RTX3000 ... Rev.9.00.31 以降、RTX1100、RT107e ... Rev.8.03.75 以降で、その他の機種では初期リビジョンより使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

13.6 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
```

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
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

- [初期値]: on

[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`、`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

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

13.7 利用するデータベースの選択

[書式]

```
url filter external-database use [reputation reputation_name] [category category_name]
no url filter external-database use
```

[設定値及び初期値]

- *reputation_name*: Web レピュテーション機能で使用するデータベースの選択

- [設定値]:

設定値	説明
off	Web レピュテーション機能を使用しない
trendmicro	トレンドマイクロ株式会社のデータベースを使用する

- [初期値]: off
- *category_name*: カテゴリーチェック機能で使用するデータベースの選択
- [設定値]:

設定値	説明
off	カテゴリーチェック機能を使用しない
digitalarts	デジタルアーツ株式会社のデータベースを使用する (Rev.8.03.87 で無効)
digitalarts2	デジタルアーツ株式会社のデータベースを使用する (Rev.8.03.87 で有効)
netstar	ネットスター株式会社のデータベースを使用する
trendmicro	トレンドマイクロ株式会社のデータベースを使用する

- [初期値]: off

[説明]

外部データベース参照型 URL フィルターの各評価機能で利用するデータベースを選択する。

データベースを利用するためには、URL フィルタリングサービス事業者と契約を行う必要がある。

[ノート]

SRT100 Rev.10.00.52 以降、RTX1200 Rev.10.01.22 以降でトレンドマイクロ株式会社のデータベースが選択可能となる。また、同リビジョンより本コマンドの書式が変更され、旧書式での入力は受理されなくなる。ただし、それ以前のファームウェアからリビジョンアップした場合のみ、旧書式で保存されたコマンドは新書式に変換して継承される。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1200, RTX1100, RT107e, SRT100

13.8 データベースを持つサーバーアドレスの設定

[書式]

```
url filter external-database server address port
no url filter external-database server
```

[設定値及び初期値]

- *address*: サーバーのアドレス
 - [設定値]:
 - 1 個の IPv4 アドレス
 - FQDN
 - [初期値]: -
- *port*
 - [設定値]: ポート番号(1..65535)
 - [初期値]: -

[説明]

外部データベースを持つサーバーのアドレス、およびデータベースにアクセスするためのポート番号を設定する。

デジタルアーツ株式会社のデータベースを使用する場合にのみ有効である。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1200, RTX1100, RT107e, SRT100

13.9 Proxy サーバーの設定

[書式]

url filter external-database proxy server address [port]

no url filter external-database proxy server

[設定値及び初期値]

- *address* : Proxy サーバーのアドレス

- [設定値]:

- 1 個の IPv4 アドレス
- FQDN

- [初期値]: -

- *port*

- [設定値]:

- ポート番号(1..65535)
- 省略時は 80

- [初期値]: -

[説明]

外部データベースを持つサーバーにアクセスする時に使用する Proxy サーバーのアドレス、ポート番号を設定する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1200, RTX1100, RT107e, SRT100

13.10 チェックするカテゴリーの設定

[書式]

url filter external-database category num kind category_list [src_addr[/mask]]

no url filter external-database category num

[設定値及び初期値]

- *num*

- [設定値]: カテゴリーリスト番号(1..21474836)

- [初期値]: -

- *kind*

- [設定値]:

設定値	説明
pass	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)
pass-nolog	一致すれば通す (ログに記録しない)
reject	一致すれば破棄する (ログに記録する)
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)

- [初期値]: -

- *category_list*

- [設定値]:

- カテゴリー番号をコンマ(,)で区切った並び

- * ... すべてのカテゴリ番号
- [初期値]: -
- *src_addr*: IP パケットの始点 IP アドレス
 - [設定値]:
 - IPv4 アドレス
 - 間にハイフン(-)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
 - 上項目をコンマ(,)で区切った並び(RTX1100/RT107e Rev.8.03.75 以降、RTX3000 Rev.9.00.31 以降、SRT100 Rev.10.00.38 以降、および、Rev.11.01 系以降のファームウェア)
 - * ... すべての IP アドレス
 - 省略時は * と同じ
 - [初期値]: -
- *mask*
 - [設定値]: 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)
 - [初期値]: -

[説明]

URL フィルターでチェックするデータベースのカテゴリを設定する。本コマンドで設定されたフィルターは、**url interface filter** コマンドで用いられる。

どのカテゴリにも該当しない URL は、*category_list* で * を指定した場合の設定が適用される。指定できるカテゴリ番号は、使用する URL フィルタリングサービス事業者により異なる。

[ノート]

RTX1100/RT107e Rev.8.03.75 以降、RTX3000 Rev.9.00.31 以降、SRT100 Rev.10.00.38 以降、および、Rev.10.01 系以降のファームウェアで、*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]

RTX5000, RTX3500, RTX3000, RTX1200, RTX1100, RT107e, SRT100

13.11 Web レピュテーションによるフィルタの設定

[書式]

```
url filter external-database reputation num kind level_list [pharming_status] [src_addr[/mask]]
no url filter external-database reputation num
```

[設定値及び初期値]

- *num*
 - [設定値]: Web レピュテーションフィルター番号(1..21474836)
 - [初期値]: -
- *kind*
 - [設定値]:

設定値	説明
pass	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)
pass-nolog	一致すれば通す(ログに記録しない)
reject	一致すれば破棄する(ログに記録する)
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)

- [初期値]: -
- *level_list*
 - [設定値]:
 - マッチするセキュリティーレベル番号をコンマ(,)で区切った並び

- *...すべてのセキュリティレベルにマッチする
- [初期値]:-
- *pharming_status*
- [設定値]:

設定値	説明
pharmed	ファージングを検出した場合にマッチする
unpharmed	ファージングを検出しなかった場合にマッチする

- [初期値]:-
- *src_addr*: IP パケットの始点 IP アドレス
- [設定値]:
 - IPv4 アドレス
 - 間にハイフン(-)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
 - *...すべての IP アドレス
 - 省略時は*と同じ
- [初期値]:-
- *mask*
- [設定値]: 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)
- [初期値]:-

[説明]

URL フィルタの Web レピュテーション機能を使用したフィルターを定義する。本コマンドで設定されたフィルターは、**url interface filter** コマンドで用いられる。

指定できるセキュリティレベル番号とその定義については、URL フィルタリングサービス事業者によって異なる。

pharming_status パラメータは Web レピュテーションの評価と共にファージングの検出結果を利用したい場合に指定し、トレンドマイクロ株式会社のデータベースを使用する場合に評価される。

[ノート]

level_list と *pharming_status* は、どちらか一方にマッチすればマッチしたものと見なされる。

SRT100 は Rev.10.00.52 以降で使用可能。

RTX1200 は Rev.10.01.22 以降で使用可能。

[適用モデル]

RTX1200, SRT100

13.12 外部データベースへのアクセスに失敗したときにパケットを破棄するか否かの設定

[書式]

url filter external-database access failure type

no url filter external-database access failure

[設定値及び初期値]

- *type*
- [設定値]:

設定値	説明
pass	パケットを通す
reject	パケットを破棄する

- [初期値]: pass

[説明]

外部データベースへのアクセスに失敗したとき、パケットを破棄するか否かを設定する。

設定誤りによりデータベースを持つサーバーへアクセスできない、またはサーバーから応答がないなどの理由でサーバーから正常な応答が得られなかった場合に、本コマンドの設定にしたがってパケットが処理される。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1200, RTX1100, RT107e, SRT100

13.13 URL フィルター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 external-database reject redirect [url]
url filter external-database reject redirect url
url filter external-database reject redirect off
no url filter external-database reject
```

[設定値及び初期値]

- *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
 - [初期値]: *redirect* (RTX5000、RTX3500、RTX3000 以外の場合)
- *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
 - [初期値]: *off* (RTX5000、RTX3500、RTX3000 の場合)
- *url*
 - [設定値]: 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)
 - [初期値]: -

[説明]

URL フィルター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。

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。

- 使用している URL フィルタリング事業者名
- 該当したセキュリティーレベル番号、カテゴリー番号、もしくはエラー文字列
- アクセスを遮断した URL

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。

HTTP サーバー機能に対応していない機種で *redirect* を指定する場合、*url* を省略することはできない。

RTX1100/RT107e Rev.8.03.75 以降、RTX3000 Rev.9.00.31 以降、SRT100 Rev.10.00.38 以降、および、Rev.10.01 系以降のファームウェアで、*url* を指定できる。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1200, RTX1100, RT107e, SRT100

13.14 IP アドレスを直接指定した URL へのアクセスを許可するか否かの設定**[書式]**

```
url filter external-database ipaddress access type
no url filter external-database ipaddress access
```

[設定値及び初期値]

- *type*
- [設定値]:

設定値	説明
pass	パケットを通す
reject	パケットを破棄する

- [初期値]: pass

[説明]

http://(IP アドレス)/XXXX のように、IP アドレスを直接指定した URL へのアクセスを許可するか否かを設定する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1200, RTX1100, RT107e, SRT100

13.15 指定した拡張子の URL を評価するか否かの設定

[書式]

url filter external-database lookup specified extension *switch*

no url filter external-database lookup specified extension [*switch*]

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
on	指定した拡張子の URL を評価する
off	指定した拡張子の URL を評価しないで、通過させる

- [初期値]: off

[説明]

指定した拡張子の URL について評価するか否かを設定する。評価を行わない場合、その URL へのリクエストを通過させる。

初期設定として、以下の拡張子が登録されている。

jpg, gif, ico, png, bmp, jpeg, tif, tiff, swf, wav, wmv, wma, mp3, mpg, mpeg, mp4, asx, asf, wax, wvx, mov

url filter external-database lookup specified extension list コマンドで上記拡張子のリストに拡張子を追加または削除することができる。

[ノート]

使用する外部データベースによって対応するリビジョンが異なり、次のようになる。

- ネットスター株式会社
RTX1100/RT107e Rev.8.03.82 以降、RTX3000 Rev.9.00.47 以降、SRT100 Rev.10.00.44 以降、RTX1200 Rev.10.01.11 以降、および RTX3500/RTX5000 Rev.14.00.08 以降のファームウェアで有効。
- デジタルアーツ株式会社
RTX3000 Rev.9.00.47 以降、SRT100 Rev.10.00.46 以降、RTX1200 Rev.10.01.16 以降のファームウェアで有効。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1200, RTX1100, RT107e, SRT100

13.16 評価しない URL の拡張子の設定

[書式]

```
url filter external-database lookup specified extension list [+/-]extension [..]
```

```
no url filter external-database lookup specified extension list [..]
```

[設定値及び初期値]

- *extension*
 - [設定値]: 拡張子(半角 4 文字以内、64 個以内)
 - [初期値]: -

[説明]

url filter external-database lookup specified extension コマンドが off の設定の場合に、評価せずリクエストを通過させる URL の拡張子を設定する。

初期設定として、以下の拡張子が登録されており、このリストへの追加、削除する形で拡張子を設定する。

jpg, gif, ico, png, bmp, jpeg, tif, tiff, swf, wav, wmv, wma, mp3, mpg, mpeg, mp4, asx, asf, wax, wvx, mov

extension の前に+を置くか、あるいは何も置かない場合には上記初期設定のリストに *extension* を追加する。
extension の前に-を置く場合には上記初期設定のリストから *extension* を削除する。

[ノート]

使用する外部データベースによって対応するリビジョンが異なり、次のようになる。

- ネットスター株式会社
RTX1100/RT107e Rev.8.03.82 以降、RTX3000 Rev.9.00.47 以降、SRT100 Rev.10.00.44 以降、RTX1200 Rev.10.01.11 以降、および RTX3500/RTX5000 Rev.14.00.08 以降のファームウェアで有効。
- デジタルアーツ株式会社
RTX3000 Rev.9.00.47 以降、SRT100 Rev.10.00.46 以降、RTX1200 Rev.10.01.16 以降のファームウェアで有効。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1200, RTX1100, RT107e, SRT100

13.17 フィルター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 external-database log switch
```

```
no url filter external-database log
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	フィルターにマッチした際にログを出力する
off	フィルターにマッチした際にログを出力しない

- [初期値]: on

[説明]

フィルター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、pass-nolog、または reject-nolog を指定したフィルターにマッチした場合はログを出力しない。

RTX1100/RT107e Rev.8.03.75 以降、RTX3000 Rev.9.00.31 以降、SRT100 Rev.10.00.38 以降、および、Rev.10.01 系以降のファームウェアで使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1200, RTX1100, RT107e, SRT100

13.18 シリアル ID を登録する URL の設定

[書式]

`url filter external-database register url url`

`no url filter external-database register url`

[設定値及び初期値]

- *url*
 - [設定値]: シリアル ID を登録する URL(半角 255 文字以内)
 - [初期値]: <https://ars2s.daj.co.jp/register/add.php>

[説明]

シリアル ID を登録する URL を設定する。

デジタルアーツ株式会社のデータベースを使用する場合にのみ有効である。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1200, RTX1100, RT107e, SRT100

13.19 データベースへアクセスするためのシリアル ID の設定

[書式]

`url filter external-database id name [id]`

`no url filter external-database id name`

[設定値及び初期値]

- *name*
 - [設定値]:

設定値	説明
digitalarts	デジタルアーツ株式会社のデータベースへアクセスするためのシリアル ID を設定する
trendmicro	トレンドマイクロ株式会社のデータベースへアクセスするためのアクティベーションコードを設定する

- [初期値]: -
- *id*
 - [設定値]: シリアル ID(半角 255 文字以内)
 - [初期値]: -

[説明]

各サービス事業者のデータベースへアクセスするためのシリアル ID を設定する。

[ノート]

SRT100 Rev.10.00.52 以降、RTX1200 Rev.10.01.22 以降のファームウェアでは *name* パラメーターが新設され、指定が必須となる。ただし、それ以前のファームウェアからリビジョンアップした場合のみ、旧書式で保存されたコマンドは新書式に変換して継承される。ここで継承したコマンドはデジタルアーツ株式会社向けの設定と見なされる。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1200, RTX1100, RT107e, SRT100

13.20 URL フィルタリングサービス事業者にシリアル ID の登録

[書式]

```
url filter external-database id activate go [database]
```

[設定値及び初期値]

- *database*
- [設定値]:

設定値	説明
reputation	Web レピュテーションデータベースのサービス事業者にシリアル ID を登録する
category	カテゴリデータベースのサービス事業者にシリアル ID を登録する

- [初期値]:-

[説明]

url filter external-database use コマンドの設定に従い、URL フィルタリングサービス事業者にシリアル ID を登録する。

database パラメーターを指定することで、特定のデータベースのサービス事業者との契約状況のみを確認する。

[ノート]

本コマンドを実行する前に、**url filter external-database use** コマンドで、使用するデータベースを設定し、**url filter external-database id** コマンドで、シリアル ID を設定する必要がある。

トレンドマイクロ株式会社のデータベースを使用する場合にのみ有効である。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1200, RTX1100, RT107e, SRT100

13.21 URL フィルタリングサービス事業者との契約状況の確認

[書式]

```
url filter external-database id check go [database]
```

[設定値及び初期値]

- *database*
- [設定値]:

設定値	説明
reputation	Web レピュテーションデータベースのサービス事業者との契約状況を確認する
category	カテゴリデータベースのサービス事業者との契約状況を確認する

- [初期値]:-

[説明]

url filter external-database use コマンドの設定に従い、URL フィルタリングサービス事業者との契約状況を確認する。

database パラメーターを指定することで、特定のデータベースのサービス事業者との契約状況のみを確認する。また、*database* パラメーターを省略し、且つ複数のサービス事業者のデータベースを使用している場合は、それぞれの契約状況を確認する。

[ノート]

本コマンドを実行する前に、**url filter external-database use** コマンドで、使用するデータベースを設定する必要がある。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1200, RTX1100, RT107e, SRT100

13.22 データベース情報の更新

[書式]

url filter external-database update operation [*database*] [**prompt**]

[設定値及び初期値]

• *operation*

- [設定値]:

設定値	説明
check	更新の有無の確認のみ行う
go	更新の有無の確認を行い、更新があれば取得する

- [初期値]: -

• *database*

- [設定値]:

設定値	説明
reputation	Web レピュテーションデータベースのみを対象とする
category	カテゴリデータベースのみを対象とする

- [初期値]: -

- *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

- [初期値]: -

[説明]

url filter external-database use コマンドの設定に従い、データベースの更新情報の確認および取得を行う。

database パラメーターを指定することで、特定のデータベースの更新情報を確認する。また、*database* パラメーターを省略し、かつ複数のサービス事業者のデータベースを使用している場合は、それぞれの更新情報を確認する。

特定のデータベースとサービス事業者の組合せで発生する固有の動作については以下の通り。

- カテゴリデータベース×ネットスター株式会社

カテゴリチェックの追加モジュールの更新確認、ダウンロード、および保存を行う。追加モジュールは無名ユーザーのカスタム GUI として使用するため、ダウンロードした追加モジュール群の保存先は、無名ユーザーとして設定された **httpd custom-gui user** コマンドの PATH パラメーターのディレクトリとなる。従って、本コマンドにより追加モジュール群を保存するには無名ユーザーの **httpd custom-gui user** コマンドを事前に設定しておく必要がある。

[ノート]

本コマンドを実行する前に、**url filter external-database use** コマンドで、使用するデータベースを設定する必要がある。

SRT100 は Rev.10.00.60 以降で使用可能。

RTX1200 は Rev.10.01.36 以降で使用可能。

[適用モデル]

RTX1200, SRT100

13.23 ユーザー認証に失敗した場合の再送間隔と回数の設定

[書式]

```
url filter external-database auth retry interval [retry]
```

```
no url filter external-database auth retry
```

[設定値及び初期値]

- *interval*

- [設定値]:

設定値	説明
60 .. 300	再送間隔
auto	自動
off	再送しない

- [初期値]: auto

- *retry*

- [設定値]:

設定値	説明
1 .. 50	再送回数

- [初期値]: 10

[説明]

外部データベース参照型 URL フィルターでユーザー認証の自動実行に失敗した場合に、再度ユーザー認証を実行する間隔と回数を設定する。

interval に auto を設定した時に、ユーザー認証に失敗した場合には 30 秒から 90 秒の時間をおいて再度ユーザー認証を行う。それにも失敗した場合には、その後 60 秒間隔でユーザー認証を試みる。

interval に off を設定した時には、ユーザー認証に失敗した場合でも再送は行わない。

retry は *interval* に off 以外を設定した場合に指定できる。

[ノート]

url filter external-database id check go コマンドで、手動でユーザー認証を実行した場合には、本コマンドでの設定にかかわらずユーザー認証の再送は行われない。

ユーザー認証に失敗してから指定した時間までの間にユーザー認証を手動実行した場合には、その後の *interval* で指定した再送間隔でのユーザー認証は行わない。

RTX1100/RT107e Rev.8.03.75 以降、RTX3000 Rev.9.00.31 以降、SRT100 Rev.10.00.38 以降、および、Rev.10.01 系以降のファームウェアで使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1200, RTX1100, RT107e, SRT100

第 14 章

PPP の設定

14.1 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...]
```

[設定値及び初期値]

- *username*
 - [設定値]: 名前 (64 文字以内)
 - [初期値]: -
- *password*
 - [設定値]: パスワード (64 文字以内)
 - [初期値]: -
- *myname*: 自分側の設定を入力するためのキーワード
 - [初期値]: -
- *myname*
 - [設定値]: 自分側のユーザ名
 - [初期値]: -
- *mypass*
 - [設定値]: 自分側のパスワード
 - [初期値]: -
- *isdn1*
 - [設定値]: 相手の ISDN アドレス
 - [初期値]: -
- *clid*: 発番号認証を利用することを示すキーワード
 - [初期値]: -
- *isdn2*
 - [設定値]: 発番号認証に用いられる ISDN アドレス
 - [初期値]: -
- *mscbcp*: MS コールバックを許可することを示すキーワード
 - [初期値]: -
- *ip_address*
 - [設定値]: 相手に割り当てる IP アドレス
 - [初期値]: -
- *ip6_prefix*
 - [設定値]: ユーザに割り当てるプレフィックス
 - [初期値]: -

[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。

isdn2 は複数設定することができる。複数設定する場合は、まず先頭の ISDN アドレスで認証が行われ、認証に失敗すると次の ISDN アドレスが使われる。

mshcbp 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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.2 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]
```

[設定値及び初期値]

- *accept*

- [設定値]:

設定値	説明
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

- [初期値]: 認証を受け入れない

[説明]

相手からの PPP 認証要求を受け入れ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。

このコマンドで認証を受け入れる設定になっても、 **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。ただし、以下のリビジョンは mschap, mschap-v2 も指定が可能。

RTX5000, RTX3500 Rev.14.00.12 以降。

SRT100 Rev.10.00.61 以降。

RTX3000 Rev.9.00.60 以降。

RT107e Rev.8.03.94 以降。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.3 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]]
```

[設定値及び初期値]

- *auth*
- [設定値]:

設定値	説明
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

- [初期値]: -

[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。ただし、以下のリビジョンは mschap, mschap-v2 も指定が可能。

RTX5000, RTX3500 Rev.14.00.12 以降。

SRT100 Rev.10.00.61 以降。

RTX3000 Rev.9.00.60 以降。

RT107e Rev.8.03.94 以降。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.4 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]
```

[設定値及び初期値]

- *myname*
 - [設定値]: 名前 (64 文字以内)
 - [初期値]: -
- *password*
 - [設定値]: パスワード (64 文字以内)
 - [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.5 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]
```

[設定値及び初期値]

- *prohibit*
 - [設定値]:

設定値	説明
on	禁止する
off	禁止しない

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.6 LCP 関連の設定

14.6.1 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]
```

[設定値及び初期値]

- *acfc*
 - [設定値]:

設定値	説明
on	用いる
off	用いない

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.6.2 Magic Number オプション使用の設定**[書式]**

ppp lcp magicnumber *magicnumber*

no ppp lcp magicnumber [*magicnumber*]

[設定値及び初期値]

- *magicnumber*

- [設定値]:

設定値	説明
on	用いる
off	用いない

- [初期値]: on

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.6.3 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*]]

[設定値及び初期値]

- *mru*

- [設定値]:

設定値	説明
on	用いる
off	用いない

- [初期値]: on

- *length*: MRU の値

- [設定値]:

- 1500 または 1792 (RT250i)
- 1280..1792 (上記以外)

- [初期値]: 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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.6.4 Protocol Field Compression オプション使用の設定**[書式]**

```
ppp lcp pfc pfc
no ppp lcp pfc [pfc]
```

[設定値及び初期値]

- *pfc*
 - [設定値]:

設定値	説明
on	用いる
off	用いない

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.6.5 lcp-restart パラメータの設定**[書式]**

```
ppp lcp restart time
no ppp lcp restart [time]
```

[設定値及び初期値]

- *time*
 - [設定値]: ミリ秒 (20..10000)
 - [初期値]: 3000

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.6.6 lcp-max-terminate パラメータの設定**[書式]**

```
ppp lcp maxterminate count
no ppp lcp maxterminate [count]
```

[設定値及び初期値]

- *count*
 - [設定値]: 回数 (1..10)
 - [初期値]: 2

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.6.7 lcp-max-configure パラメータの設定**[書式]**

```
ppp lcp maxconfigure count
no ppp lcp maxconfigure [count]
```

[設定値及び初期値]

- *count*
 - [設定値]: 回数 (1..10)
 - [初期値]: 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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.6.8 lcp-max-failure パラメータの設定**[書式]**

```
ppp lcp maxfailure count
no ppp lcp maxfailure [count]
```

[設定値及び初期値]

- *count*
 - [設定値]: 回数 (1..10)
 - [初期値]: 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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.6.9 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]
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
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

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.7 PAP 関連の設定

14.7.1 pap-restart パラメータの設定

[書式]

```
ppp pap restart time
no ppp pap restart [time]
```

[設定値及び初期値]

- *time*
 - [設定値]: ミリ秒 (20..10000)
 - [初期値]: 3000

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.7.2 pap-max-authreq パラメータの設定

[書式]

```
ppp pap maxauthreq count
no ppp pap maxauthreq [count]
```

[設定値及び初期値]

- *count*
 - [設定値]: 回数 (1..10)
 - [初期値]: 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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.8 CHAP 関連の設定

14.8.1 chap-restart パラメータの設定

[書式]

```
ppp chap restart time
no ppp chap restart [time]
```

[設定値及び初期値]

- *time*
 - [設定値]: ミリ秒 (20..10000)
 - [初期値]: 3000

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.8.2 chap-max-challenge パラメータの設定

[書式]

```
ppp chap maxchallenge count
no ppp chap maxchallenge [count]
```

[設定値及び初期値]

- *count*
 - [設定値]: 回数 (1..10)
 - [初期値]: 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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.9 IPCP 関連の設定

14.9.1 Van Jacobson Compressed TCP/IP 使用の設定

[書式]

```
ppp ipcp vjc compression
no ppp ipcp vjc [compression]
```

[設定値及び初期値]

- *compression*
 - [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.9.2 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]
```

[設定値及び初期値]

- *negotiation*
 - [設定値]:

設定値	説明
on	ネゴシエーションする
off	ネゴシエーションしない

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.9.3 ipcp-restart パラメータの設定

[書式]

```
ppp ipcp restart time
no ppp ipcp restart [time]
```

[設定値及び初期値]

- *time*
 - [設定値]: ミリ秒 (20..10000)
 - [初期値]: 3000

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.9.4 ipcp-max-terminate パラメータの設定

[書式]

```
ppp ipcp maxterminate count
no ppp ipcp maxterminate [count]
```

[設定値及び初期値]

- *count*
 - [設定値]: 回数 (1..10)
 - [初期値]: 2

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.9.5 ipcp-max-configure パラメータの設定

[書式]

```
ppp ipcp maxconfigure count
no ppp ipcp maxconfigure [count]
```

[設定値及び初期値]

- *count*
 - [設定値]: 回数 (1..10)
 - [初期値]: 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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.9.6 ipcp-max-failure パラメータの設定

[書式]

```
ppp ipcp maxfailure count
no ppp ipcp maxfailure [count]
```

[設定値及び初期値]

- *count*
 - [設定値]: 回数 (1..10)
 - [初期値]: 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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.9.7 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]]
```

[設定値及び初期値]

- *server1*, *server2*
 - [設定値]: IP アドレス (xxx.xxx.xxx.xxx(xxx は十進数))
 - [初期値]: -

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.9.8 IPCP の MS 拡張オプションを使うか否かの設定

[書式]

```
ppp ipcp msxt msxt
no ppp ipcp msxt [msxt]
```

[設定値及び初期値]

- *msxt*
 - [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.9.9 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]
```

[設定値及び初期値]

- *sw*
- [設定値]:

設定値	説明
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

- [初期値]: on

[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]

RT250i は、Rev.8.02.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.10 MSCBCP 関連の設定

14.10.1 mscbcpr-restart パラメータの設定

[書式]

```
ppp mscbcpr restart time
no ppp mscbcpr restart [time]
```

[設定値及び初期値]

- *time*
- [設定値]: ミリ秒 (20..10000)
- [初期値]: 1000

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e

14.10.2 mscbcpr-maxretry パラメータの設定

[書式]

```
ppp mscbcpr maxretry count
no ppp mscbcpr maxretry [count]
```

[設定値及び初期値]

- *count*
- [設定値]: 回数 (1..30)

- [初期値]: 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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e

14.11 CCP 関連の設定

14.11.1 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]
```

[設定値及び初期値]

- *type*
- [設定値]:

設定値	説明
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

- [初期値]:
 - none(RT107e、SRT100)
 - stac(上記以外のモデル)

[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。

RTX5000、RTX3500、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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.11.2 ccp-restart パラメータの設定

[書式]

```
ppp ccp restart time  
no ppp ccp restart [time]
```

[設定値及び初期値]

- *time*
 - [設定値]: ミリ秒 (20..10000)
 - [初期値]: 3000

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.11.3 ccp-max-terminate パラメータの設定

[書式]

```
ppp ccp maxterminate count  
no ppp ccp maxterminate [count]
```

[設定値及び初期値]

- *count*
 - [設定値]: 回数 (1..10)
 - [初期値]: 2

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.11.4 ccp-max-configure パラメータの設定

[書式]

```
ppp ccp maxconfigure count  
no ppp ccp maxconfigure [count]
```

[設定値及び初期値]

- *count*
 - [設定値]: 回数 (1..10)
 - [初期値]: 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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.11.5 ccp-max-failure パラメータの設定

[書式]

```
ppp ccp maxfailure count  
no ppp ccp maxfailure [count]
```

[設定値及び初期値]

- *count*
 - [設定値]: 回数 (1..10)
 - [初期値]: 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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.12 IPV6CP 関連の設定

14.12.1 IPV6CP を使用するか否かの設定

[書式]

```
ppp ipv6cp use use
no ppp ipv6cp use [use]
```

[設定値及び初期値]

- `use`
- [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: on

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

14.13 MP 関連の設定

14.13.1 MP を使用するか否かの設定

[書式]

```
ppp mp use use
no ppp mp use [use]
```

[設定値及び初期値]

- `use`
- [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RT250i

14.13.2 MP の制御方法の設定

[書式]

```
ppp mp control type
```


no ppp mp control [*type*]

[設定値及び初期値]

- *type*
- [設定値]:

設定値	説明
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

- [初期値]: call

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RT250i

14.13.3 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*]

[設定値及び初期値]

- *call_load*
 - [設定値]: 発信負荷閾値 %(1..100)
 - [初期値]: 70
- *call_count*
 - [設定値]: 回数 (1..100)
 - [初期値]: 1
- *disc_load*
 - [設定値]: 切断負荷閾値 %(0..50)
 - [初期値]: 30
- *disc_count*
 - [設定値]: 回数 (1..100)
 - [初期値]: 2

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RT250i

14.13.4 MP の最大リンク数の設定

[書式]

ppp mp maxlink *number*

no ppp mp maxlink [*number*]

[設定値及び初期値]

- *number*
 - [設定値]: リンク数

- [初期値]: 2

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RT250i

14.13.5 MP の最小リンク数の設定

[書式]

```
ppp mp minlink number
no ppp mp minlink [number]
```

[設定値及び初期値]

- *number*
 - [設定値]: リンク数
 - [初期値]: 1

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RT250i

14.13.6 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]
```

[設定値及び初期値]

- *time*
 - [設定値]: 秒数 (1..21474836)
 - [初期値]: 10

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RT250i

14.13.7 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]
```

[設定値及び初期値]

- *divide*
 - [設定値]:

設定値	説明
on	分割する
off	分割しない

- [初期値]: on

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RT250i

14.14 BACP 関連の設定

14.14.1 bacp-restart パラメータの設定

[書式]

```
ppp bacp restart time
no ppp bacp restart [time]
```

[設定値及び初期値]

- *time*
 - [設定値]: ミリ秒 (20..10000)
 - [初期値]: 3000

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RT250i

14.14.2 bacp-max-terminate パラメータの設定

[書式]

```
ppp bacp maxterminate count
no ppp bacp maxterminate [count]
```

[設定値及び初期値]

- *count*
 - [設定値]: 回数 (1..10)
 - [初期値]: 2

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RT250i

14.14.3 bacp-max-configure パラメータの設定

[書式]

```
ppp bacp maxconfigure count
no ppp bacp maxconfigure [count]
```

[設定値及び初期値]

- *count*
 - [設定値]: 回数 (1..10)
 - [初期値]: 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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RT250i

14.14.4 bacp-max-failure パラメータの設定

[書式]

```
ppp bacp maxfailure count
no ppp bacp maxfailure [count]
```

[設定値及び初期値]

- *count*
 - [設定値]: 回数 (1..10)
 - [初期値]: 10

[説明]

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

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RT250i

14.15 BAP 関連の設定

14.15.1 bap-restart パラメータの設定

[書式]

```
ppp bap restart time
no ppp bap restart [time]
```

[設定値及び初期値]

- *time*
 - [設定値]: ミリ秒 (20..10000)
 - [初期値]: 1000

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RT250i

14.15.2 bap-max-retry パラメータの設定

[書式]

```
ppp bap maxretry count
no ppp bap maxretry [count]
```

[設定値及び初期値]

- *count*
 - [設定値]: 再送回数 (1..30)
 - [初期値]: 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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RT250i

14.16 PPPoE 関連の設定

14.16.1 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
```

[設定値及び初期値]

- *interface*

- [設定値]: LAN インタフェース名、VLAN インタフェース名、タグ VLAN インタフェース名
- [初期値]: -

[説明]

選択されている相手に対して、PPPoE で使用する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。

[ノート]

VLAN インターフェースは RTX5000、RTX3500、RTX1220、RTX1210、RTX1200、RTX830、RTX810 で指定可能。タグ VLAN インターフェースは RTX5000、RTX3500、RTX1220、RTX1210 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

14.16.2 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
```

[設定値及び初期値]

- *name*
 - [設定値]: アクセスコンセントレータの名前を表す文字列 (7bit US-ASCII)
 - [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

14.16.3 セッションの自動接続の設定

[書式]

```
pppoe auto connect switch
no pppoe auto connect
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	自動接続する
off	自動接続しない

- [初期値]: on

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

14.16.4 セッションの自動切断の設定

[書式]

```
pppoe auto disconnect switch
no pppoe auto disconnect
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	自動切断する
off	自動切断しない

- [初期値]: on

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

14.16.5 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
```

[設定値及び初期値]

- *times*
 - [設定値]: 回数 (1..10)
 - [初期値]: 5

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

14.16.6 PADI パケットの再送時間の設定

[書式]

```
pppoe padi restart time
no pppoe padi restart
```

[設定値及び初期値]

- *time*
 - [設定値]: ミリ秒 (20..10000)
 - [初期値]: 3000

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

14.16.7 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
```

[設定値及び初期値]

- *times*
 - [設定値]: 回数 (1..10)
 - [初期値]: 5

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

14.16.8 PADR パケットの再送時間の設定

[書式]

```
pppoe padr restart time
no pppoe padr restart
```

[設定値及び初期値]

- *time*
 - [設定値]: ミリ秒 (20..10000)
 - [初期値]: 3000

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

14.16.9 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
```

[設定値及び初期値]

- *time*
 - [設定値]:

設定値	説明
1..21474836	秒数
off	タイマを設定しない

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

14.16.10 サービス名の指定

[書式]

```
pppoe service-name name
no pppoe service-name
```

[設定値及び初期値]

- *name*
 - [設定値]: サービス名を表す文字列 (7bit US-ASCII、255 文字以内)
 - [初期値]: -

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

14.16.11 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
```

[設定値及び初期値]

- *length*
- [設定値]:

設定値	説明
1240..1452	データ長
auto	MSS を MTU の値に応じて制限する
off	MSS を制限しない

- [初期値]: auto

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

14.16.12 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
```

[設定値及び初期値]

- *sw*
- [設定値]:

設定値	説明
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

- [初期値]: on

[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.8.03.60 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

14.16.13 PPPoE フレームを中継するインターフェースの指定

[書式]

```
pppoe pass-through member interface interface [interface...]
no pppoe pass-through member [...]
```

[設定値及び初期値]

- *interface*
- [設定値]: LAN インターフェース名

- [初期値]:-

[説明]

PPPoE パススルー機能を使用するインターフェースを指定する。

指定したインターフェース間で PPPoE フレームが中継される。

LAN インターフェース名には、物理 LAN インターフェースおよび LAN 分割機能で使用するインターフェースを指定できる。

[ノート]

指定した LAN インターフェースはプロミスキャスモードで動作する。

RTX830 は Rev.15.02.03 以降で使用可能。

RTX1210 は Rev.14.01.26 以降で使用可能。

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。

設定できる *interface* の数は下記の通り。

機種	最大設定可能数
RTX1220	10
RTX830	5
RTX1210	10
RTX5000	10
RTX3500	10

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

第 15 章

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使用します。

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 dhcp** コマンドにより知ることができます。

(*1)Dynamic Host Configuration Protocol; RFC1541 , RFC2131

15.1 DHCP サーバー・リレーエージェント機能

15.1.1 DHCP の動作の設定

[書式]

```
dhcp service type
no dhcp service [type]
```

[設定値及び初期値]

- *type*
 - [設定値]:

設定値	説明
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

- [初期値]:-

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

15.1.2 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
```

[設定値及び初期値]

- *comp*

- [設定値]:

設定値	説明
on	RFC2131 準拠
off	RFC1541 準拠

- [初期値]: on

- *except*: 指定した機能以外が RFC2131 対応となるキーワード

- [初期値]: -

- *function*

- [設定値]:

設定値	説明
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

- [初期値]: -

[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 宛であれば 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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

15.1.3 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

[設定値及び初期値]

- *check1* : LAN 内を対象とするチェックの確認用待ち時間
- [設定値] :

設定値	説明
1..1000	ミリ秒
off	LAN 内を対象とするチェックを行わない

- [初期値] : 100
- *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
- [設定値] :

設定値	説明
1..3000	ミリ秒
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

- [初期値] : 500

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

15.1.4 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]]
```

[設定値及び初期値]

- *scope_num*
 - [設定値]: スコープ番号 (1..65535)
 - [初期値]: -
- *ip_address-ip_address*
 - [設定値]: 対象となるサブネットで割り当てる IP アドレスの範囲
 - [初期値]: -
- *netmask*
 - [設定値]:
 - xxx.xxx.xxx.xxx (xxx は十進数)
 - 0x に続く十六進数
 - マスクビット数
 - [初期値]: -
- *ex_ip*
 - [設定値]: 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)
 - [初期値]: -
- *gw_ip*
 - [設定値]: 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
 - [初期値]: -
- *time*: 時間
 - [設定値]:
 - expire time: DHCP クライアントからリース期間要求がない場合のリース期間
 - maxexpire time: DHCP クライアントからリース期間要求がある場合の許容最大リース期間

設定値	説明
1..21474836	分 (RTX5000 / RTX3500 Rev.14.00.26 以降、RTX1210 Rev.14.01.32 以降、RTX830 Rev.15.02.08 以降、RTX1220)
1..2147483647	分 (上記以外)
xx:xx	時間:分
infinity	無期限リース

- [初期値]:
 - expire time=72:00
 - maxexpire time=72:00

[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]

RTX5000 / RTX3500 Rev.14.00.26 以降、RTX1210 Rev.14.01.28 以降、RTX830 Rev.15.02.03 以降、RTX1220 では、同一ネットワークの DHCP スコープを複数設定できる。

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。

expire の設定値は maxexpire の設定値以下でなければならない。

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。

Rev.10.00 系以前、RTX1200 の Rev.10.01.71 以前、RTX810 の Rev.11.01.28 以前、RTX5000 / RTX3500 の Rev.14.00.21 以前、および、RTX1210 の Rev.14.01.20 以前では、**dhcp scope** コマンドを実行した場合に、同一のスコープ ID を持つ以下のコマンドの設定が消去される。

- **dhcp scope bind**
- **dhcp scope option**

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

15.1.5 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
dhcp scope bind scope_num ip_address-ip_address mac_address
no dhcp scope bind scope_num ip_address
no dhcp scope bind scope_num ip_address-ip_address
```

[設定値及び初期値]

- *scope_num*
 - [設定値]: スコープ番号 (1..65535)
 - [初期値]: -
- *ip_address*
 - [設定値]:

設定値	説明
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

- [初期値]: -
- *type*: Client-Identifier オプションの *type* フィールドを決定する
 - [設定値]:

設定値	説明
text	0x00
ethernet	0x01

- [初期値]: -
- *id*
 - [設定値]:

設定値	説明
<i>type</i> が ethernet の場合	MAC アドレス
<i>type</i> が text の場合	文字列

設定値	説明
<code>type</code> が省略された場合	2 桁十六進数の列で先頭は <code>type</code> フィールド

- [初期値]: -
- `mac_address`
- [設定値]:
 - `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
 - `xx:xx:xx:*` のように下位 3 オクテットをアスタリスク (*) にすることで、OUI(ベンダー ID) のみの指定となる
- [初期値]: -
- `ipcp`: IPCP でリモート側に与えることを示すキーワード
- [初期値]: -

[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。

`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` 機能を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-Identifier オプションで送られる値で予約し直す必要がある。

コマンドの第 2 書式で 1 つの OUI(ベンダー ID)を複数設定することができる。OUI(ベンダー ID)設定と MAC アドレス設定の両方がある場合、MAC アドレス設定を優先する。

OUI(ベンダー ID)設定は以下のファームウェアで指定可能。

RTX5000 / RTX3500 Rev.14.00.26 以降

RTX1210 Rev.14.01.28 以降

RTX830 Rev.15.02.03 以降

RTX1220 すべてのリビジョン

Rev.10.00 系以前、RTX1200 の Rev.10.01.71 以前、RTX810 の Rev.11.01.28 以前、RTX5000 / RTX3500 の Rev.14.00.21 以前、および、RTX1210 の Rev.14.01.20 以前では、**`dhcp scope`** コマンドを実行した場合に、同一のスコープ ID を持つ以下のコマンドの設定が消去される。

- **`dhcp scope bind`**
- **`dhcp scope option`**

[設定例]

```
A. # dhcp scope bind 1 192.168.100.2 ethernet 00:a0:de:01:23:45
B. # dhcp scope bind 1 192.168.100.2 text client01
C. # dhcp scope bind 1 192.168.100.2 01 00 a0 de 01 23 45 01 01 01
```

```
D. # dhcp scope bind 1 192.168.100.2 00:a0:de:01:23:45
E. # dhcp scope bind 1 192.168.100.2-192.168.100.19 00:a0:de:*
```

1. dhcp server rfc2131 compliant on あるいは use-clientid 機能を使用する設定の場合

- A. B. C. の書式では、クライアントの識別に Client-Identifier オプションを使用する。
- D. の書式では DHCP パケットの chaddr フィールドを使用する。ただし、Client-Identifier オプションが存在する場合、この設定は無視される。

DHCP サーバーは chaddr フィールドの値より Client-Identifier オプションの値の方が優先して使用される。

show status dhcp コマンドを実行して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。

- 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 オプションは使用していない
- リースしているクライアントとして十六進数の文字列、あるいは文字列が表示されていれば、Client-Identifier オプションが使われている Client-Identifier オプションを使うクライアントへの予約は、ここに表示される十六進数の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 機能を使用しない場合

- A. B. C. の書式では指定できない。Client-Identifier オプションは無視される。
- D. の書式では DHCP パケットの chaddr フィールドを使用する。

なお、クライアントとの相互動作に関して以下の留意点がある。

- 個々の機能を単独で用いるとクライアント側で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。
- ルーターの再起動やスコープの再設定によりリース情報が消去されている場合、アドレスの延長要求をした時やリース期間内のクライアントを再起動した時にクライアントが使用する IP アドレスは変わることがある。

これを防ぐためには **dhcp server rfc2131 compliant on** (あるいは remain-silent 機能を有効にする) 設定がある。この設定にすると、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 に対して DHCPNAK を返さず無視するようになる。

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 アドレスをリースすることができる。

E. の書式では、OUI(ベンダー ID)のみ指定し、その OUI(ベンダー ID)を持つ機器にのみ IP アドレスを割り当てることができる。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

15.1.6 DHCP アドレス割り当て動作の設定

[書式]

```
dhcp scope lease type scope_num type [qac-tm=switch fallback=fallback_scope_num]
```

```
dhcp scope lease type scope_num type [fallback=fallback_scope_num]
```

```
no dhcp scope lease type scope_num [type ...]
```

[設定値及び初期値]

- *scope_num, fallback_scope_num*
 - [設定値]: スコープ番号 (1-65535)
 - [初期値]: -
- *type*: 割り当ての動作
 - [設定値]:

設定値	説明
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

- [初期値]: bind-priority
- *switch*: QAC/TM 機能

- [設定値]:

設定値	説明
on	QAC/TM 機能を使用する
off	QAC/TM 機能を使用しない

- [初期値]:-

[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。
 - a. 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。
 - b. 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。

`qac-tm` オプションを `on` に設定している場合には、同時に `fallback` オプションでフォールバックスコープを指定する必要がある。この場合には以下の動作になる。

1. クライアントに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。
2. クライアントのアンチウイルスソフトウェアのバージョン情報を確認する。
3. アンチウイルスソフトウェアのバージョンが的確と認定されると、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。
4. アンチウイルスソフトウェアのバージョンが不適合と認定されると、フォールバックスコープの IP アドレスをリース延長する。

リース期間は DHCP スコープの定義に従う。

[ノート]

`qac-tm` オプションは SRT100 の Rev.10.00.44 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

15.1.7 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 [...]]
```

[設定値及び初期値]

- `scope_n`
 - [設定値]: スコープ番号 (1-65535)
 - [初期値]:-
- `idx`
 - [設定値]:

設定値	説明
番号	<code>show status dhcp summary</code> 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	省略時は all

- [初期値]:-

[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` で確認すべきである

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

15.1.8 DHCP オプションの設定

[書式]

`dhcp scope option scope_num option=value [option=value...]`

`no dhcp scope option scope_num [...]`

[設定値及び初期値]

- `scope_num`
 - [設定値]: スコープ番号 (1..65535)
 - [初期値]:-
- `option`
 - [設定値]:
 - オプション番号
 - 1..49,62..254(RTX1500/RTX1100/RT107e Rev.8.03.92 以降、RTX3000 Rev.9.00.56 以降、SRT100 Rev.10.00.61 以降、RTX1200 Rev.10.01.36 以降、RTX810 Rev.11.01.06 以降、および、Rev.14.00 系以降)
 - 1..49,64..76,85..87,128..254(上記以外)
 - 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

- [初期値]:-
- *value*: オプション値
- [設定値]:
 - 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..2147483647
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

- [初期値]:-

[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]

Rev.10.00 系以前、RTX1200 の Rev.10.01.71 以前、RTX810 の Rev.11.01.28 以前、RTX5000 / RTX3500 の Rev.14.00.21 以前、および、RTX1210 の Rev.14.01.20 以前では、**dhcp scope** コマンドを実行した場合に、同一のスコープ ID を持つ以下のコマンドの設定が消去される。

- **dhcp scope bind**
- **dhcp scope option**

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

15.1.9 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
```

[設定値及び初期値]

- *ip_address*
 - [設定値]: リースする IP アドレス
 - [初期値]:-
- *type*: Client-Identifier オプションの *type* フィールドを決定する
 - [設定値]:

設定値	説明
text	0x00
ethernet	0x01

- [初期値]:-

- *id*
- [設定値]:

設定値	説明
<i>type</i> が <i>text</i> の場合	文字列
<i>type</i> が <i>ethernet</i> の場合	MAC アドレス
<i>type</i> が省略された場合	2 桁十六進数の列で先頭は <i>type</i> フィールド

- [初期値]: -
- *mac_address*
 - [設定値]: 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
 - [初期値]: -
- *ipcp*: IPCP でリモート側に与えたものとするキーワード
 - [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

15.1.10 DHCP リース情報の手動削除

[書式]

```
dhcp manual release ip_address
```

[設定値及び初期値]

- *ip_address*
 - [設定値]: 解放する IP アドレス
 - [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

15.1.11 DHCP サーバーの指定の設定

[書式]

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

[設定値及び初期値]

- *host1..host4*
 - [設定値]: DHCP サーバーの IP アドレス
 - [初期値]: -

[説明]

DHCPBOOTREQUEST 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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

15.1.12 DHCP リレーエージェント機能で使用する始点ポート番号の設定

[書式]

```
dhcp relay srcport port
no dhcp relay srcport [port]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号 (1..65535)
 - [初期値]: 68

[説明]

DHCP リレーエージェント機能で使用する始点ポート番号を設定する。

[ノート]

RTX5000、RTX3500 は Rev.14.00.29 以降、RTX1210 Rev.14.01.36 以降、RTX830 Rev.15.02.15 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

15.1.13 DHCP サーバーの選択方法の設定

[書式]

```
dhcp relay select type
no dhcp relay select [type]
```

[設定値及び初期値]

- *type*
 - [設定値]:

設定値	説明
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

- [初期値]: hash

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

15.1.14 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]
```

[設定値及び初期値]

- *time*
 - [設定値]: 秒数 (0..65535)

- [初期値]: 0

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

15.1.15 インターフェース毎の DHCP の動作の設定

[書式]

```
ip interface dhcp service type [host1 [host2 [host3 [host4]]]]
```

```
no ip interface dhcp service
```

[設定値及び初期値]

- `interface`
 - [設定値]: LAN インタフェース名、ブリッジインタフェース名
 - [初期値]: -
- `type`
 - [設定値]:

設定値	説明
off	DHCP サーバーとしても DHCP リレーエージェントとしても機能しない
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

- [初期値]: -
- `host1..host4`
 - [設定値]: DHCP サーバーの IP アドレス
 - [初期値]: -

[説明]

インターフェース毎に DHCP の動作を設定する。

DHCP サーバーを設定した場合には、ネットワークアドレスが合致する DHCP スコープから IP アドレスを 1 つ割り当てる。

DHCP リレーエージェントを設定した場合には、HOST を設定する必要がある、この HOST へ DHCP DISCOVER パケットおよび DHCP REQUEST パケットを転送する。

off に設定した場合には、DHCP サーバーとしても DHCP リレーエージェントとしても動作しない。DHCP パケットは破棄されます。

本設定が無い場合は、`dhcp service` コマンドの設定に従う。`dhcp service` コマンドの設定と本設定の両方がある場合には、本設定が優先される。

[ノート]

RTX1200 は Rev.10.01.65 以降で使用可能。

RTX810 は Rev.11.01.25 以降で使用可能。

RTX5000、RTX3500 は Rev.14.00.18 以降で使用可能。

RTX1210 は Rev.14.01.09 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

15.2 DHCP クライアント機能

15.2.1 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]

```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名、ブリッジインタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]:
 - 相手先情報番号
 - anonymous
 - [初期値]: -
- *pool_num*
 - [設定値]: **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)
 - [初期値]: -
- *host*
 - [設定値]: DHCP クライアントのホスト名
 - [初期値]: -

[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は SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

WAN インタフェースを設定した時には、secondary は指定できない。

[拡張ライセンス対応]

[拡張ライセンス](#)をインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- *pool_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	101

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

15.2.2 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]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名、ブリッジインタフェース名
 - [初期値]: -
- *time*
 - [設定値]: 分数 (1..21474836)
 - [初期値]: -

[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は SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

15.2.3 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]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名、ブリッジインタフェース名
 - [初期値]: -
- *retry*
 - [設定値]:

設定値	説明
1..100	回数
infinity	無制限

- [初期値]: infinity
- *interval*
 - [設定値]: 秒数 (1..100)
 - [初期値]: 5

[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は SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

15.2.4 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
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名、ブリッジインタフェース名
 - [初期値]: -
- *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
 - [初期値]: -
- *type*
 - [設定値]: ID オプションの *type* フィールドの値
 - [初期値]: 1
- *id*
 - [設定値]:
 - ASCII 文字列で表した ID
 - 2 桁の十六進数列で表した ID
 - [初期値]: -
- *peer_num*
 - [設定値]:
 - 相手先情報番号
 - anonymous
 - [初期値]: -
- *pool_num*
 - [設定値]: **ip pp remote address pool dhcp** 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 dhcp** 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 dhcp** コマンドで取得できる IP アドレスの最大数)
 - [初期値]: -

[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は SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指

定可能。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

WAN インタフェースを設定した時には、secondary は指定できない。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- peer_num

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- pool_num

ライセンス名	拡張後の上限値
YSL-VPN-EX1	101

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

15.2.5 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]
```

[設定値及び初期値]

- interface
 - [設定値]: LAN インタフェース名、WAN インタフェース名、ブリッジインタフェース名
 - [初期値]: -
- option
 - [設定値]: オプション番号 (十進数)
 - [初期値]: -
- value
 - [設定値]: 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
 - [初期値]: -
- peer_num
 - [設定値]:
 - 相手先情報番号
 - anonymous
 - [初期値]: -
- pool_num
 - [設定値]: **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)
 - [初期値]: -

[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。

ブリッジインタフェースは SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

WAN インタフェースを設定した時には、secondary は指定できない。

[設定例]

- 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。)
```

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- peer_num

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- pool_num

ライセンス名	拡張後の上限値
YSL-VPN-EX1	101

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

15.2.6 リンクダウンした時に情報を解放するか否かの設定

[書式]

```
dhcp client release linkdown switch [time]
no dhcp client release linkdown [switch [time]]
```

[設定値及び初期値]

- switch
- [設定値]:

設定値	説明
on	インタフェースのリンクダウンが <i>time</i> 秒間継続すると、取得していた情報を解放する
off	インタフェースがリンクダウンしても情報は保持する

- [初期値]: off
- time
- [設定値]: 秒数 (0..259200)
- [初期値]: 3

[説明]

DHCP クライアントとして DHCP サーバーから IP アドレスを得ているインタフェースがリンクダウンした時に、DHCP サーバーから得ていた情報を解放するか否かを設定する。

リンクダウンするとタイマーが働き、*time* の秒数だけリンクダウン状態が継続すると情報を解放する。*time* が設定されていない場合には *time* は 3 秒となる。

情報が解放されると、次にリンクアップした時に情報の取得を試みる。

[ノート]

タイマーの値を長く設定すると、不安定なリンク状態の影響を避けることができる。
本コマンドの設定は、コマンド実行後に発生したリンクダウン以降で有効になる。
タイマーの満了前にリンクアップした場合にはタイマーはクリアされ、情報を解放しない。
タイマーの満了前に情報のリース期間が満了した場合には、タイマーはクリアされ、情報は解放される。
以下のコマンド実行時には、動作中のタイマーはクリアされる。

ip interface address, ip pp remote address, ip pp remote address pool, dhcp client release linkdown

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

第 16 章

ICMP の設定

16.1 IPv4 の設定

16.1.1 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]
```

[設定値及び初期値]

- *send*
- [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: on

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

16.1.2 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]
```

[設定値及び初期値]

- *send*
- [設定値]:

設定値	説明
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

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

16.1.3 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]
```

[設定値及び初期値]

- *send*
- [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: on

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

16.1.4 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]
```

[設定値及び初期値]

- *send*
- [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

16.1.5 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]
```

[設定値及び初期値]

- *send*
- [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: on

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

16.1.6 ICMP Redirect 受信時の処理の設定

[書式]

```
ip icmp redirect receive action
no ip icmp redirect receive [action]
```

[設定値及び初期値]

- *action*
 - [設定値]:

設定値	説明
on	処理する
off	無視する

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

16.1.7 ICMP Time Exceeded を送信するか否かの設定

[書式]

```
ip icmp time-exceeded send send [rebound=sw]
no ip icmp time-exceeded send [send rebound=sw]
```

[設定値及び初期値]

- *send*
 - [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: on

- *sw*
 - [設定値]:

設定値	説明
on	受信インターフェースから送信する
off	経路に従って送信する

- [初期値]: off

[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。

rebound オプションを on に設定した場合には、経路に関係なく元となるパケットを受信したインターフェースから送信する。

[ノート]

RTX3000 Rev.9.00.60 以降、RTX1200 Rev.10.01.59 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで rebound オプションを指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

16.1.8 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]
```

[設定値及び初期値]

- *send*
- [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: on

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

16.1.9 ICMP Destination Unreachable を送信するか否かの設定

[書式]

```
ip icmp unreachable send send [rebound=sw]
no ip icmp unreachable send [send rebound=sw]
```

[設定値及び初期値]

- *send*
- [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: on

- *sw*
- [設定値]:

設定値	説明
on	受信インターフェースから送信する
off	経路に従って送信する

- [初期値]: off

[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。

rebound オプションを on に設定した場合には、経路に関係なく元となるパケットを受信したインターフェースから送信する。

[ノート]

rebound オプションは RTX3000 Rev.9.00.60 以降、RTX1200 Rev.10.01.59 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定できる。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

16.1.10 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-decryptd-ipsec send switch
no ip icmp error-decryptd-ipsec send [switch]
```

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
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

- [初期値]: on

[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を設定する。

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

16.1.11 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]
```

[設定値及び初期値]

- *log*
- [設定値]:

設定値	説明
on	記録する
off	記録しない

- [初期値]: off

[説明]

受信した ICMP エラーを DEBUG レベルのログに記録するか否かを設定する。Echo Request や Echo Reply のログは記録しない。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

16.1.12 ステルス機能の設定**[書式]**

```
ip stealth all
ip stealth interface [interface...]
no ip stealth [...]
```

[設定値及び初期値]

- 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
 - [初期値] :-
- interface
 - [設定値] : 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
 - [初期値] :-

[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き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。

ブリッジインタフェースは SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

16.1.13 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]]
```

[設定値及び初期値]

- interface
 - [設定値] : LAN インタフェース名
 - [初期値] :-
- sw
 - [設定値] :

設定値	説明
on	ARP による MTU 探索を行う
off	ARP による MTU 探索を行わない

- [初期値] : on
- min_mtu

- [設定値]: 探索範囲の最低 MTU
- [初期値]: 4000

[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によって相手の MTU を探索します。

[適用モデル]

RTX5000, RTX3500, RTX3000

16.1.14 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]
```

[設定値及び初期値]

- *send*
- [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: on

[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 Destination unreachable (Fragmentation needed) 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。

[適用モデル]

RTX5000, RTX3500, RTX3000

16.2 IPv6 の設定

16.2.1 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]
```

[設定値及び初期値]

- *send*
- [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: on

[説明]

ICMP Echo Reply を送信するか否かを設定する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

16.2.2 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]
```

[設定値及び初期値]

- *send*
- [設定値]:

設定値	説明
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

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

16.2.3 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]
```

[設定値及び初期値]

- *send*
- [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: off

[説明]

ICMP Parameter Problem を送信するか否かを設定する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

16.2.4 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]
```

[設定値及び初期値]

- *send*
- [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: on

[説明]

ICMP Redirect を出すか否かを設定する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

16.2.5 ICMP Redirect 受信時の処理の設定

[書式]

ipv6 icmp redirect receive *action*
no ipv6 icmp redirect receive [*action*]

[設定値及び初期値]

- *action*
- [設定値]:

設定値	説明
on	処理する
off	無視する

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

16.2.6 ICMP Time Exceeded を送信するか否かの設定

[書式]

ipv6 icmp time-exceeded send *send* [rebound=*sw*]
no ipv6 icmp time-exceeded send [*send* rebound=*sw*]

[設定値及び初期値]

- *send*
- [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: on

- *sw*

- [設定値]:

設定値	説明
on	受信インターフェースから送信する
off	経路に従って送信する

- [初期値]: off

[説明]

ICMP Time Exceeded を出すか否かを設定する。

rebound オプションを on に設定した場合には、経路に関係なく元となるパケットを受信したインターフェースから送信する。

[ノート]

RTX3000 Rev.9.00.60 以降、RTX1200 Rev.10.01.59 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで rebound オプションを指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

16.2.7 ICMP Destination Unreachable を送信するか否かの設定

[書式]

```
ipv6 icmp unreachable send send [rebound=sw]
```

```
no ipv6 icmp unreachable send [send rebound=sw]
```

[設定値及び初期値]

- send

- [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: on

- sw

- [設定値]:

設定値	説明
on	受信インターフェースから送信する
off	経路に従って送信する

- [初期値]: off

[説明]

ICMP Destination Unreachable を出すか否かを設定する。

rebound オプションを on に設定した場合には、経路に関係なく元となるパケットを受信したインターフェースから送信する。

[ノート]

RTX3000 Rev.9.00.60 以降、RTX1200 Rev.10.01.59 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで rebound オプションを指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

16.2.8 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]
```

[設定値及び初期値]• *log*

- [設定値]:

設定値	説明
on	記録する
off	記録しない

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

16.2.9 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*]

[設定値及び初期値]• *send*

- [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: on

[説明]

ICMP Packet-Too-Big を出すか否かを設定する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

16.2.10 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*]

[設定値及び初期値]• *switch*

- [設定値]:

設定値	説明
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

- [初期値]: on

[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おり、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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

16.2.11 ステルス機能の設定

[書式]

ipv6 stealth all

ipv6 stealth interface [interface...]

no ipv6 stealth [...]

[設定値及び初期値]

- 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
 - [初期値] : -
- interface
 - [設定値] : 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
 - [初期値] : -

[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ことで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。

ブリッジインタフェースは SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

16.2.12 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]

[設定値及び初期値]

- send
 - [設定値] :

設定値	説明
on	送信する
off	送信しない

- [初期値] : on

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000

第 17 章

トンネリング

17.1 トンネルインターフェースの使用許可の設定

[書式]

```
tunnel enable tunnel_num [tunnel_num ...]
```

```
no tunnel enable tunnel_num
```

[設定値及び初期値]

- *tunnel_num*
- [設定値]:

設定値	説明
番号	トンネルインターフェース番号
番号 1-番号 2	番号 1 から番号 2 までのトンネルインターフェース番号
番号 1-	番号 1 以上のすべてのトンネルインターフェース番号
-番号 1	番号 1 以下のすべてのトンネルインターフェース番号
all	すべてのトンネルインターフェース

- [初期値]:-

[説明]

トンネルインター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ーフェースは `disable` 状態であり、使用する場合は本コマンドにより、インターフェースを有効にしなければならない。

複数指定した場合には、その全てで使用できる状態になる。複数指定は、RTX1200 Rev.10.01.75 以降、RTX810 Rev.11.01.31 以降、RTX5000 / RTX3500 Rev.14.00.26 以降、RTX1210 Rev.14.01.26 以降、RTX830 Rev.15.02.03 以降、RTX1220 で使用可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

17.2 トンネルインターフェースの使用不許可の設定

[書式]

```
tunnel disable tunnel_num
```

[設定値及び初期値]

- *tunnel_num*
- [設定値]:

設定値	説明
番号	トンネルインターフェース番号

設定値	説明
番号 1-番号 2	番号 1 から番号 2 までのトンネルインターフェース番号
番号 1-	番号 1 以上のすべてのトンネルインターフェース番号
-番号 1	番号 1 以下のすべてのトンネルインターフェース番号
all	すべてのトンネルインターフェース

- [初期値] :-

[説明]

トンネルインター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。
 複数指定した場合には、その全てで使用できない状態になる。複数指定は、RTX1200 Rev.10.01.75 以降、RTX810 Rev.11.01.31 以降、RTX5000 / RTX3500 Rev.14.00.26 以降、RTX1210 Rev.14.01.26 以降、RTX830 Rev.15.02.03 以降、RTX1220 で使用可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

17.3 トンネルインタフェースの接続種別の設定

[書式]

tunnel type *type* [*role*]

no tunnel type [*type* [*role*]]

[設定値及び初期値]

- *type*

- [設定値] :

設定値	説明
point-to-point	point-to-point トンネル
multipoint	point-to-multipoint トンネル

- [初期値] : point-to-point

- *role*

- [設定値] :

設定値	説明
server	サーバーの役割を割り当てる
client	クライアントの役割を割り当てる

- [初期値] : client

[説明]

トンネルインタフェースの接続種別を、接続先を 1 箇所だけ持つ point-to-point トンネル、もしくは、複数の接続先を持つ point-to-multipoint トンネル (マルチポイントトンネル) に設定する。

role オプションは *type* に multipoint を設定した場合のみ設定可能なオプションで、マルチポイントトンネルでは同一のトンネルに接続する複数のルーターの中から server と client をそれぞれ 1 台以上指定する必要がある。

[ノート]

マルチポイントトンネルはハブ・アンド・スポーク型の構成を基本構成とし、通常はハブ・ルーターの *role* オプションのみに *server* を指定する。なお、Rev.15.02.22 より前の RTX830 は、*server* を指定できない。

RTX1210 は、Rev.14.01.20 以降で使用可能。

RTX5000 / RTX3500 は Rev.14.00.26 以降で使用可能。

[拡張ライセンス対応]

RTX830 は、**拡張ライセンス (YSL-VPN-EX1)** がインポートされているときに *role* オプションに *server* を指定可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

17.4 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

[設定値及び初期値]

- *type*

- [設定値]:

設定値	説明
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
l2tp	L2TP/IPsec トンネル
l2tpv3-raw	L2TPv3 トンネル
l2tpv3	L2TPv3/IPsec トンネル
ipudp	IPUDP トンネル
map-e	MAP-E トンネル

- [初期値]: ipsec

[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。

L2TP/IPsec 機能を実装していないモデルでは、**l2tp** キーワードは使用できない。

L2TPv3 機能を実装していないモデルでは、**l2tpv3-raw** キーワードおよび **l2tpv3** キーワードは使用できない。

IPUDP トンネルは、データコネクタ接続以外では使用できない。

データコネクタ接続機能を実装していないモデルでは、**ipudp** キーワードは使用できない。

「v6 プラス」対応機能または OCN バーチャルコネクタサービス対応機能を実装していないモデルでは、**map-e** キーワードは使用できない。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

17.5 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]]
```

[設定値及び初期値]

- *ip_address*
 - [設定値]: IPv4 アドレス
 - [初期値]: -
- *mask*
 - [設定値]:
 - xxx.xxx.xxx.xxx(xxx は十進数)
 - 0x に続く十六進数
 - マスクビット数
 - [初期値]: -

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

17.6 トンネルインター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]
```

[設定値及び初期値]

- *ip_address*
 - [設定値]: IPv4 アドレス
 - [初期値]: -

[説明]

トンネルインター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ー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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

17.7 相手側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 remote address remote
no tunnel endpoint remote address [remote]
```

[設定値及び初期値]

- *remote*
 - [設定値]: 相手側のトンネルインタフェース端点の IP アドレス、またはホスト名(半角 64 文字以内)
 - [初期値]: -

[説明]

相手側のトンネルインタフェース端点の IP アドレス、またはホスト名を設定する。IP アドレスは IPv4/IPv6 いずれのアドレスも設定できる。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。

tunnel endpoint local address コマンドの設定がない場合、もしくは *local* と *remote* で IPv4/IPv6 の種別が異なる場合は、ローカルエンドポイントアドレスに適切なインタフェースの IP アドレスが利用される。また、本コマンドでホスト名を設定し、**tunnel endpoint local address** コマンドで IP アドレスを設定した場合、**tunnel endpoint local address** コマンドの IPv4/IPv6 種別に従ってホスト名の名前解決が行われる。

[ノート]

本コマンドにより設定した IP アドレスおよびホスト名が利用されるのは、**tunnel encapsulation** コマンドの設定値が `ipip` の場合である。本コマンドが設定されている場合、**tunnel endpoint address** コマンドおよび **tunnel endpoint name** コマンドの設定は利用されない。

RTX5000 / RTX3500 は Rev.14.00.22 以降で使用可能。

RTX1210 は Rev.14.01.20 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

17.8 自分側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 local address *local*

no tunnel endpoint local address [*local*]

[設定値及び初期値]

- *local*
 - [設定値]: 自分側のトンネルインタフェース端点の IP アドレス、またはホスト名(半角 64 文字以内)
 - [初期値]: -

[説明]

自分側のトンネルインタフェース端点の IP アドレス、またはホスト名を設定する。IP アドレスは IPv4/IPv6 いずれのアドレスも設定できる。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。

tunnel endpoint remote address コマンドの設定がない場合、もしくは *local* と *remote* で IPv4/IPv6 の種別が異なる場合は、本コマンドの設定は反映されない。また、本コマンドでホスト名を設定し、**tunnel endpoint remote address** コマンドで IP アドレスを設定した場合、**tunnel endpoint remote address** コマンドの IPv4/IPv6 種別に従ってホスト名の名前解決が行われる。

[ノート]

本コマンドにより設定した IP アドレスおよびホスト名が利用されるのは、**tunnel encapsulation** コマンドの設定値が `ipip` の場合である。

RTX5000 / RTX3500 は Rev.14.00.22 以降で使用可能。

RTX1210 は Rev.14.01.20 以降で使用可能。

IPv6 のダイナミックアドレスは RTX5000 Rev.14.00.26 以降、RTX3500 Rev.14.00.26 以降、RTX1210 Rev.14.01.33 以降、RTX830 Rev.15.02.08 以降、RTX1220 で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

17.9 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*]

[設定値及び初期値]

- *local*
 - [設定値]: 自分側のトンネルインタフェース端点の IP アドレス
 - [初期値]: -
- *remote*
 - [設定値]: 相手側のトンネルインタフェース端点の IP アドレス
 - [初期値]: -

[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いといけない。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*、*l2tp*、*l2tpv3-raw*、*l2tpv3*、*ipip* の場合である。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、L2TP/IPsec サーバーの *Anonymous* で受ける場合には設定する必要はない。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

17.10 トンネルの端点の名前の設定

[書式]

tunnel endpoint name [*local_name*] *remote_name* [*type*]

no tunnel endpoint name [*local_name remote_name type*]

[設定値及び初期値]

- *local_name*
 - [設定値]: 自分側端点
 - [初期値]: -
- *remote_name*
 - [設定値]: 相手側端点
 - [初期値]: -
- *type*: 名前の種類
 - [設定値]:

設定値	説明
fqdn	FQDN
tel	NGN 網電話番号

- [初期値]: fqdn

[説明]

トンネル端点の名前を指定する。

[ノート]

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。

このコマンドが利用されるのは、**tunnel encapsulation** コマンドの設定値が *pptp*、*l2tpv3-raw*、*l2tpv3*、*ipip*、*ipudp* の場合である。

pptp、*l2tpv3-raw*、*l2tpv3*、*ipip* トンネルの場合、名前にはドメイン名 (FQDN) を指定する。

ipudp トンネルの場合、名前には NGN 網電話番号を指定する。ハイフン無しで記述する。

データコネクタ接続機能を実装していないモデルでは、*type* パラメータは使用できない。

ipip トンネルの名前指定は、RTX5000 / RTX3500 Rev.14.00.22 以降、RTX1210 Rev.14.01.20 以降のファームウェア、および、Rev.15.02 系以降のすべてのファームウェアで使用可能。

RTX3000 は Rev.9.00.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810

17.11 マルチポイントトンネルのサーバーの設定

[書式]

```
tunnel multipoint server id ip_address
no tunnel multipoint server id [ip_address]
```

[設定値及び初期値]

- *id*
 - [設定値]: サーバー識別子 (1 .. 3)
 - [初期値]: -
- *ip_address*
 - [設定値]: IPv4 / IPv6 アドレスまたはホスト名
 - [初期値]: -

[説明]

マルチポイントトンネルにおいて、サーバーの役割が割り当てられているルーターのアドレスを設定する。本コマンドは **tunnel type** コマンドで接続種別に **multipoint**、**role** オプションに **client** が設定されているトンネルインタフェース（マルチポイントトンネルのクライアント側のトンネルインタフェース）で有効になる。

本コマンドを複数設定し、複数のサーバーを指定している場合は、接続可能なサーバーすべてに対してトンネルが接続される。最大で 3 台のサーバーを指定できる。

[ノート]

マルチポイントトンネルはハブ・アンド・スポーク型の構成を基本構成とし、通常はハブ・ルーターがサーバーとなる。

RTX1210 は Rev.14.01.20 以降で使用可能。

RTX5000 / RTX3500 は Rev.14.00.26 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

17.12 マルチポイントトンネルで使用する自分の名前の設定

[書式]

```
tunnel multipoint local name name
no tunnel multipoint local name [name]
```

[設定値及び初期値]

- *name*
 - [設定値]: 名前（半角で 64 文字以内、全角で 32 文字以内）
 - [初期値]: -

[説明]

マルチポイントトンネルで使用する自分の名前を設定する。

本コマンドで設定した名前はトンネル接続後に接続相手にも通知され、接続相手側でもトンネルの識別情報として SYSLOG 等で利用される。

[ノート]

RTX1210 は Rev.14.01.20 以降で使用可能。

RTX5000 / RTX3500 は Rev.14.00.26 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

17.13 マルチポイントトンネルで接続する相手の最大数の設定

[書式]

```
tunnel multipoint limit limit
no tunnel multipoint limit [limit]
```


[設定値及び初期値]

- *limit*
 - [設定値]: 最大数 (1 .. 100)
 - [初期値]: 100

[説明]

選択されているトンネルインタフェースで接続できる相手の最大数を設定する。本コマンドは **tunnel type** コマンドの接続種別に **multipoint**、**role** オプションに **server** が設定されているトンネルインタフェース（マルチポイントトンネルのサーバー側のトンネルインタフェース）で有効になる。

すべてのトンネルインタフェースの接続相手の合計数の上限は各機種ごとに定められているトンネル最大対地数となる。そのため、複数のトンネルインタフェースを使用する場合は、本コマンドで設定した最大数の制限だけでなく、各機種ごとのトンネル最大対地数の制限も受ける。接続相手の数が本コマンドで設定した最大数を下回っている場合でも、すべてのトンネルインタフェースの合計数が各機種ごとのトンネル最大対地数に達している場合は新たに接続することはできない。

[ノート]

RTX1210 は Rev.14.01.20 以降で使用可能。
 RTX5000 / RTX3500 は Rev.14.00.26 以降で使用可能。
 RTX830 は Rev.15.02.22 以降で使用可能。ただし、拡張ライセンスがインポートされていないときは使用不可。

[拡張ライセンス対応]

RTX830 は、[拡張ライセンス \(YSL-VPN-EX1\)](#) がインポートされているときに本コマンドを使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

17.14 トンネルインタフェースの MAP-E 種別の設定

[書式]

tunnel map-e type *type*
no tunnel map-e type [*type*]

[設定値及び初期値]

- *type*
 - [設定値]:

設定値	説明
v6plus	「v6 プラス」
ocn	OCN バーチャルコネク トサービス

- [初期値]: v6plus

[説明]

トンネルインタフェースの MAP-E 種別を設定する。
tunnel encapsulation コマンドを *map-e* に設定したときに、どの MAP-E サービスを利用するかを設定する。

[ノート]

RTX1210 は、Rev.14.01.34 以降で使用可能。
 RTX830 は、Rev.15.02.10 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830

17.15 トンネルインタフェースの変換種別の設定

[書式]

tunnel translation type
no tunnel translation [*type*]

[設定値及び初期値]

• *type*

• [設定値]:

設定値	説明
nat46	NAT46 トンネル

• [初期値]:-

[説明]

トンネルインタフェースの変換種別を設定する。

[ノート]

tunnel encapsulation コマンドとの併用はできず、後から入力したコマンドが有効となる。

RTX830 Rev.15.02.20 以降で使用可能。

RTX1220 Rev.15.04.04 以降で使用可能。

[適用モデル]

RTX1220, RTX830

第 18 章

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
<ul style="list-style-type: none"> • pp enable • pp disable • pp select 	<==>	<ul style="list-style-type: none"> • tunnel enable • tunnel disable • 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 に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。

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
RTX5000	1-3000	1-3000
RTX3500	1-1000	1-1000
RTX3000	1-1000	1-1000
RTX1500	1-100	1-100
RTX1220	1-100	1-100
RTX1210	1-100	1-100
RTX1200	1-100	1-100
RTX1100	1-30	1-30
RTX830	1-20	1-20
RTX810	1-6	1-6

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
RT250i	IPsec 非搭載	IPsec 非搭載
RT107e	1-6	1-6
SRT100	1-10	1-10

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。

18.1 IPsec の動作の設定

[書式]

```
ipsec use use
no ipsec use [use]
```

[設定値及び初期値]

- *use*
 - [設定値]:

設定値	説明
on	動作させる
off	動作させない

- [初期値]: on

[説明]

IPsec を動作させるか否かを設定する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.2 IKE バージョンの設定

[書式]

```
ipsec ike version gateway_id version
no ipsec ike version gateway_id [version]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *version*
 - [設定値]: 使用する IKE のバージョン
 - [設定値]:

設定値	説明
1	IKE バージョン 1
2	IKE バージョン 2

- [初期値]: 1

[説明]

セキュリティ・ゲートウェイで使用する IKE のバージョンを設定する。

[ノート]

version で指定したバージョン以外での接続以外は受け付けない。

RTX3000 は Rev.9.00.50 以降で使用可能。

RTX1200 は Rev.10.01.22 以降で使用可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

18.3 IKE の認証方式の設定

[書式]

`ipsec ike auth method gateway_id method`

`no ipsec ike auth method gateway_id [method]`

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *method*
 - [設定値]:

設定値	説明
auto	認証方式を自動的に選択する
pre-shared-key	事前共有鍵
certificate	デジタル署名
eap-md5	EAP-MD5

- [初期値]:
 - auto

[説明]

IKE の認証方式を設定する。

METHOD に auto を設定した場合、以下の条件にしたがって認証方式が決定される。

- 事前共有鍵方式
 - `ipsec ike pre-shared-key` コマンドが設定されている場合。
- デジタル署名方式

次の条件をすべて満たしている場合

 - `ipsec ike pki file` コマンドで指定した場所に証明書が保存されている。
 - `ipsec ike eap request` コマンドおよび `ipsec ike eap myname` コマンドが設定されていない。

- EAP-MD5 方式

次の条件をすべて満たしている場合

- `ipsec ike pki file` コマンドで指定した場所に証明書が保存されている。
- `ipsec ike eap request` コマンド、または `ipsec ike eap myname` コマンドが設定されていない。

上記、認証方式を決定する条件のうち、複数の条件に合致する場合、次の順番で認証方式が優先される。

1. 事前共有鍵方式
2. デジタル署名方式
3. EAP-MD5 方式

method に auto 以外を指定した場合、上記の認証方式を決定する条件にかかわらず、*method* に指定した方式で認証を行う。

[ノート]

本コマンドは IKEv2 でのみ有効であり、IKEv1 の動作に影響を与えない。

RTX3000 は Rev.9.00.50 以降で使用可能。

RTX1200 は Rev.10.01.22 以降で使用可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

18.4 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 [...]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *key*
 - [設定値]: 鍵となる 0x ではじまる十六進数列 (Rev.10.01.22 以降は 128 バイト以内、それ以外のリビジョンは 32 バイト以内)
 - [初期値]: -
- *text*
 - [設定値]: ASCII 文字列で表した鍵 (Rev.10.01.22 以降は 128 文字以内、それ以外のリビジョンは 32 文字以内)
 - [初期値]: -

[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。

[設定例]

```
ipsec ike pre-shared-key 1 text himitsu
ipsec ike pre-shared-key 8 0xCDEEEDC0CDEDCD
```

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.5 IKEv2 の認証に使用する PKI ファイルの設定

[書式]

```
ipsec ike pki file gateway_id certificate=cert_id [crl=crl_id]
no ipsec ike pki file gateway_id [...]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *cert_id*
 - [設定値]:

設定値	説明
1..2(RTX3000)	証明書ファイルの識別子
1..8(RTX3000 以外)	

- [初期値]: -
- *crl_id*
 - [設定値]:

設定値	説明
1..2(RTX3000)	CRL ファイルの識別子
1..8(RTX3000 以外)	

- [初期値]: -

[説明]

IKEv2 の認証に使用する PKI ファイルを設定する。

デジタル証明書方式の認証を行う場合、*cert_id* に使用する証明書が保存されているファイルの識別子を指定する。

EAP-MD5 認証を行う場合、始動側は相手の証明書を検証するために *cert_id* に自分の証明書が保存されているファイルの識別子を指定する。

[ノート]

本コマンドは IKEv2 でのみ有効であり、IKEv1 の動作に影響を与えない。

RTX3000 は Rev.9.00.50 以降で使用可能。

RTX1200 は Rev.10.01.22 以降で使用可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

18.6 EAP-MD5 認証で使用する自分の名前とパスワードの設定

[書式]

```
ipsec ike eap myname gateway_id name password
no ipsec ike eap myname gateway_id [...]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -

- *name*
 - [設定値]: 名前 (半角 256 文字以内)
 - [初期値]: -
- *password*
 - [設定値]: パスワード (半角 64 文字以内)
 - [初期値]: -

[説明]

EAP-MD5 認証を要求されたときに使用する名前とパスワードを設定する。

[ノート]

本コマンドは IKEv2 でのみ有効であり、IKEv1 の動作に影響を与えない。
 RTX3000 は Rev.9.00.50 以降で使用可能。
 RTX1200 は Rev.10.01.22 以降で使用可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

18.7 EAP-MD5 によるユーザ認証の設定

[書式]

```
ipsec ike eap request gateway_id sw group_id
no ipsec ike eap request gateway_id [...]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *sw*
 - [設定値]:

設定値	説明
on	要求する
off	要求しない

- [初期値]: off
- *group_id*
 - [設定値]: 認証に使用するユーザグループの識別番号
 - [初期値]: -

[説明]

IKEv2 で、EAP-MD5 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。

本コマンドによる設定はルーターが応答側として動作するときのみ有効であり、始動側のセキュリティゲートウェイから送信された IKE AUTH 交換に AUTH ペイロードが含まれない場合に EAP-MD5 によるユーザ認証を行う。

[ノート]

本コマンドは IKEv2 でのみ有効であり、IKEv1 の動作に影響を与えない。
 RTX3000 は Rev.9.00.50 以降で使用可能。
 RTX1200 は Rev.10.01.22 以降で使用可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

18.8 EAP-MD5 認証で証明書要求ペイロードを送信するか否かの設定

[書式]

```
ipsec ike eap send certreq gateway_id switch
no ipsec ike eap send certreq gateway_id [switch]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *switch*
 - [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: off

[説明]

EAP-MD5 認証方式の場合、始動側のセキュリティ・ゲートウェイから送信する IKE_AUTH 交換に、証明書要求 (CERTREQ) ペイロードを含めるか否かを設定する。

[ノート]

本コマンドは IKEv2 でのみ有効であり、IKEv1 の動作に影響を与えない。

RTX3000 は Rev.9.00.56 以降で使用可能。

RTX1200 は Rev.10.01.36 以降で使用可能。

RTX810 は Rev.11.01.06 以降で使用可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

18.9 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]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -

- *switch*
- [設定値]:

設定値	説明
on	鍵交換を始動する
off	鍵交換を始動しない

- [初期値]:
 - off (全体的な動作)
 - on (*gateway_id* 毎)

[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
```

[拡張ライセンス対応]

[拡張ライセンス](#) をインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.10 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
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *switch*
 - [設定値]:

設定値	説明
on	鍵交換を拒否する
off	鍵交換を受理する

- [初期値]: off

[説明]

IKEv1 として動作する際、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、同様の状態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

[ノート]

本コマンドは IKEv2 としての動作には影響を与えない。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.11 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
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *switch*
 - [設定値]:

設定値	説明
on	鍵交換を継続する
off	鍵交換を休止する

- [初期値]: off

[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。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.12 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]]
```

[設定値及び初期値]

- *count*
 - [設定値]: 再送回数 (1..50)
 - [初期値]: 10
- *interval*
 - [設定値]: 再送間隔の秒数 (1..100)
 - [初期値]: 5
- *max_session*
 - [設定値]: 同時に動作するフェーズ 1 の最大数 (1..5)
 - [初期値]: 3

[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、*max_session* パラメータは、IKEv1 において同時に動作するフェーズ 1 の最大数を指定する。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]

IKEv2 として動作する場合、*max_session* パラメータは効力を持たない。同じ相手側セキュリティ・ゲートウェイに対して始動する鍵交換セッションは、常に最大 1 セッションとなる。

相手側セキュリティ・ゲートウェイに掛かっている負荷が非常に高い場合、本コマンドの設定値を調整することで鍵交換が成功しやすくなる可能性がある。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.13 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 [type]
no ipsec ike remote name gateway [name]
```

[設定値及び初期値]

- *gateway*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *name*
 - [設定値]: 名前 (RTX3000 Rev.9.00.50 以降、RTX1200 Rev.10.01.22 以降、および、Rev.11.01 系以降は 256 文字以内、それ以外のリビジョンは 32 文字以内)
 - [初期値]: -
- *type*: id の種類
 - [設定値]:

設定値	説明
ipv4-addr	ID_IPV4_ADDR
fqdn	ID_FQDN
user-fqdn(もしくは rfc822-addr)	ID_USER_FQDN(ID_RFC822_ADDR)
ipv6-addr	ID_IPV6_ADDR

設定値	説明
key-id	ID_KEY_ID
tel	NGN 網電話番号(ID_IPV6_ADDR)
tel-key	NGN 網電話番号(ID_KEY_ID)

- [初期値]: -

[説明]

相手側のセキュリティ・ゲートウェイの名前と ID の種類を設定する。
 その他、動作する IKE のバージョンによって異なる、本コマンドの影響、注意点については以下の通り。

- IKEv1

このコマンドの設定は、フェーズ 1 のアグレッシブモードで使用され、メインモードでは使用されない。
 また、*type* パラメータは相手側セキュリティ・ゲートウェイの判別時に考慮されない。

- IKEv2

相手側セキュリティ・ゲートウェイの判別時には *name*、*type* パラメータの設定が共に一致している必要がある。
type パラメータが 'tel' の場合、相手側 IPv6 アドレス(ID_IPV6_ADDR)を相手側セキュリティ・ゲートウェイの判別に使用する。
type パラメータが 'tel-key' の場合、設定値を ID_KEY_ID として相手側セキュリティ・ゲートウェイの判別に使用する。
type パラメータが 'key-id' 以外の場合、*name* から相手側セキュリティ・ゲートウェイの IP アドレスの特定を試み、特定できれば、そのホストに対して鍵交換を始動する。この場合、**ipsec ike remote address** コマンドの設定は不要である。
 ただし、**ipsec ike remote address** コマンドが設定されている場合は、そちらの設定にしたがって始動時の接続先ホストが決定される。

[ノート]

type パラメータは、RTX3000 Rev.9.00.50 以降、RTX1200 Rev.10.01.22 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで指定できる。
 'tel'および'tel-key'は、RTX3000 Rev.9.00.50 以降、RTX1200 Rev.10.01.29 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで指定可能であり、データコネク ト拠点間接続機能で使用する。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.14 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]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *ip_address*
 - [設定値]:

設定値	説明
IP アドレス、またはホスト名	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(半角 255 文字以内)
any	自動選択

- [初期値]:-

[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。

その他、動作する IKE バージョンによって異なる、本コマンドの影響、注意点については以下の通り。

• IKEv1

応答側になる場合、本コマンドで指定したホストは相手側セキュリティ・ゲートウェイの判別に使用される。
'any' が設定された場合は、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鍵交換を受け付ける。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。例えば、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場合などに利用する。

• IKEv2

このコマンドで設定したホストは、鍵交換を始動する際の接続先としてのみ使用される。'any' は自分側から鍵交換を始動しないことを明示的に示す。

応答側となる場合、本コマンドの設定による相手側セキュリティ・ゲートウェイの判別は **ipsec ike remote name** コマンド等の設定によって行われる。

[ノート]

ホスト名を指定する場合には、**dns server** コマンドなどで必ず DNS サーバーを設定しておくこと。IPsec メインモード接続では、相手側セキュリティ・ゲートウェイの IP アドレスおよびホスト名を重複して設定しない。相手側セキュリティ・ゲートウェイの IP アドレスおよびホスト名を重複して設定した場合の動作は保証されない。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.15 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]]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *ip_address*
 - [設定値]: IP アドレス
 - [初期値]: -
- *mask*
 - [設定値]: ネットマスク
 - [初期値]: -

[説明]

IKEv1 のフェーズ 2 で用いる相手側の ID を設定する。

このコマンドが設定されていない場合は、フェーズ 2 で 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。

[ノート]

本コマンドは IKEv2 の動作には影響を与えない。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.16 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*]

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *name*
 - [設定値]: 名前 (RTX3000 Rev.9.00.50 以降、RTX1200 Rev.10.01.22 以降、および、Rev.11.01 系以降 は 256 文字以内、それ以外のリビジョンは 32 文字以内)
 - [初期値]: -
- *type*: id の種類
 - [設定値]:

設定値	説明
ipv4-addr	ID_IPV4_ADDR
fqdn	ID_FQDN
user-fqdn(もしくは rfc822-addr)	ID_USER_FQDN (ID_RFC822_ADDR)
ipv6-addr	ID_IPV6_ADDR
key-id	ID_KEY_ID
tel	NGN 網電話番号(ID_IPV6_ADDR)
tel-key	NGN 網電話番号(ID_KEY_ID)

- [初期値]: -

[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。

なお、IKEv1 として動作する際に *type* パラメータが 'ipv4-addr'、'ipv6-addr'、'tel'、'tel-key' に設定されていた場合は 'key-id' を設定したときと同等の動作となる。IKEv2 かつ *type* パラメータが 'tel' の場合、自分側 IPv6 アドレス (ID_IPV6_ADDR) を鍵交換に使用する。IKEv2 かつ *type* パラメータが 'tel-key' の場合、設定値を ID_KEY_ID として鍵交換に使用する。

[ノート]

'ipv4-addr'および'ipv6-addr'は、RTX3000 Rev.9.00.50 以降、RTX1200 Rev.10.01.22 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで指定できる。

'tel'および'tel-key'は、RTX3000 Rev.9.00.50 以降、RTX1200 Rev.10.01.29 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで指定可能であり、データコネク特拠点間接続機能で使用する。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.17 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 peer_num
no ipsec ike local address gateway_id [ip_address]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *ip_address*
 - [設定値]: 自分側セキュリティ・ゲートウェイの IP アドレス
 - [初期値]: -
- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *vrid*
 - [設定値]: VRRP グループ ID(1..255)
 - [初期値]: -
- *prefix*
 - [設定値]: プレフィックス
 - [初期値]: -
- *peer_num*
 - [設定値]: PP インタフェース番号
 - [初期値]: -

[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。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.18 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]]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *ip_address*
 - [設定値]: IP アドレス
 - [初期値]: -
- *mask*
 - [設定値]: ネットマスク
 - [初期値]: -

[説明]

IKEv1 のフェーズ 2 で用いる自分側の ID を設定する。

このコマンドが設定されていない場合には、フェーズ 2 で 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。

[ノート]

本コマンドは IKEv2 としての動作には影響を与えない。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.19 IKE キープアライブ機能の設定

[書式]

```
ipsec ike keepalive use gateway_id switch [down=disconnect] [send-only-new-sa=send]
ipsec ike keepalive use gateway_id switch heartbeat [interval count [upwait]] [down=disconnect] [send-only-new-sa=send]
ipsec ike keepalive use gateway_id switch icmp-echo ip_address [length=length] [interval count [upwait]]
[down=disconnect]
ipsec ike keepalive use gateway_id switch dpd [interval count [upwait]]
```

```
ipsec ike keepalive use gateway_id switch rfc4306 [interval count [upwait]]
no ipsec ike keepalive use gateway_id [switch ....]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *switch*: キープアライブの動作
 - [設定値]:

設定値	説明
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、rfc4306 でのみ有効)

- [初期値]: auto
- *ip_address*
 - [設定値]: ping を送信する宛先の IP アドレス (IPv4/IPv6)
 - [初期値]: -
- *length*
 - [設定値]: ICMP echo のデータ部の長さ (64..1500)
 - [初期値]: 64
- *interval*
 - [設定値]: キープアライブパケットの送信間隔秒数 (1..600)
 - [初期値]: 10
- *count*
 - [設定値]: 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)
 - [初期値]: 6
- *upwait*
 - [設定値]: 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)
 - [初期値]: 0
- *send*
 - [設定値]:

設定値	説明
on	新旧の SA が混在する場合、新しい SA のみに対してキープアライブパケットを送信する
off	新旧の SA が混在する場合、新旧 SA の両方に対してキープアライブパケットを送信する

- [初期値]: off

[説明]

IKE キープアライブの動作を設定する。

本コマンドは、動作する IKE のバージョンによって以下のように動作が異なる。

• IKEv1

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。第 1 書式は自動的に heartbeat 書式となる。

heartbeat 書式を利用するには第 1、第 2 書式を使用する。heartbeat 方式において *switch* パラメータが *auto* に設定されている場合は、相手から heartbeat パケットを受信したときだけ heartbeat パケットを送信する。従って、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。

ICMP Echo を利用するときには第 3 書式を使用し、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することができる。この方式では、*switch* パラメータが *auto* でも *on* の場合と同様に動作する。

DPD を利用するときには第 4 書式を使用する。この方式では *switch* パラメータが *auto* でも *on* の場合と同様に動作する。

その他、IKEv1 で対応していない方式 (書式) が設定されている場合は、代替方式として *heartbeat* で動作する。このとき、*switch*、*count*、*interval*、*upwait* パラメータは設定内容が反映される。

- IKEv2

キープアライブの方式として、RFC4306(IKEv2 標準)、ICMP Echo の 2 種類から選ぶことができる。第 1 書式は自動的に RFC4306 方式となる。

switch パラメータが *auto* の場合には、RFC4306 方式のキープアライブパケットを受信したときだけ応答パケットを送信する。なお、IKEv2 ではこの方式のキープアライブパケットには必ず応答しなければならないため、*switch* パラメータが *auto* でも *off* の場合でも同様に動作する。

ICMP Echo を利用するときには第 3 書式を使用し、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することができる。この方式では、*switch* パラメータが *auto* でも *on* の場合と同様に動作する。

その他、IKEv2 で対応していない方式 (書式) が設定されている場合は、代替方式として RFC4306 で動作する。このとき、*switch*、*count*、*interval*、*upwait* パラメータは設定内容が反映される。

[ノート]

相手先が PP インタフェースの先にある場合、*down* オプションを指定することができる。*down* オプションを指定すると、キープアライブダウン検出時と IKE の再送回数満了時に PP インタフェースの切断を行うことができる。網側の状態などで PP インタフェースの再接続によりトンネル確立状態の改善を望める場合に利用することができる。

キープアライブの方式として *heartbeat* を使用する場合、*send-only-new-sa* オプションを指定することができる。*send-only-new-sa* オプションに *on* を設定すると、鍵交換後の新旧の SA が混在するときに新しい SA のみに対してキープアライブパケットを送信するようになり、鍵交換時の負荷を軽減することができる。ただし、*send-only-new-sa* オプションに対応していないファームウェアとトンネルを構築する場合は、*send-only-new-sa* オプションを *off* に設定しておかなければトンネルがダウンする。

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。

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 は Rev.8.03 系以降のすべてのファームウェアで利用できる。

RFC4306 は RTX3000 Rev.9.00.50 以降、RTX1200 Rev.10.01.22 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで利用できる。

down オプションは RTX1200 Rev.10.01.16 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで利用できる。

send-only-new-sa オプションは RTX5000、RTX3500 Rev.14.00.29 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで利用できる。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.20 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]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -

- `log`
- [設定値]:

設定値	説明
on	出力する
off	出力しない

- [初期値]: on

[説明]

IKE キーペアライブに関する 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。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- `gateway_id`

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.21 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]
```

[設定値及び初期値]

- `gateway_id`
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- `algorithm`
 - [設定値]:

設定値	説明
3des-cbc	3DES-CBC
des-cbc	DES-CBC
aes-cbc	AES-CBC
aes256-cbc	AES256-CBC

- [初期値]:
 - 3des-cbc (RTX5000、RTX3500、RTX3000、RTX1220、RTX1210、RTX1200、RTX830、RTX810、SRT100)
 - des-cbc (上記以外の機種)

[説明]

IKE が用いる暗号アルゴリズムを設定する。

始動側として働く場合に、本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本コマンドの設定に関係なく、サポートされている任意のアルゴリズムを用いることができる。

ただし、IKEv1 で `ipsec ike negotiate-strictly` コマンドが on の場合は、応答側であっても設定したアルゴリズムしか利用できない。

[ノート]

aes256-cbc は、RTX3000 Rev.9.00.50 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで指定できる。

IKEv2 では、`ipsec ike proposal-limitation` コマンドが on に設定されているとき、本コマンドで設定されたアルゴリズムを提案する。`ipsec ike proposal-limitation` コマンドが off に設定されているとき、または、`ipsec ike proposal-limitation` コマンドに対応していない機種では、本コマンドの設定にかかわらず、サポートするすべてのアルゴリズム

ムを同時に提案し、相手側セキュリティ・ゲートウェイに選択させる。また応答側として働く場合は、提案されたものからより安全なアルゴリズムを選択する。

IKEv2 でサポート可能な暗号アルゴリズム及び応答時の選択の優先順位は以下の通り。

- AES256-CBC > AES192-CBC > AES128-CBC > 3DES-CBC > DES-CBC

※IKEv2 でのみ AES192-CBC をサポートする。ただし、コマンドで AES192-CBC を選択することはできない。

[設定例]

```
# ipsec ike encryption 1 aes-cbc
```

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- gateway_id

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.22 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]
```

[設定値及び初期値]

- length : キュー長
- [設定値] :

設定値	機種
3000...12000	RTX5000
1000...4000	RTX3500
1000...2000	RTX3000
100....200	RTX1220、RTX1210、RTX1200、RTX830 (Rev.15.02.22 以降)
20..40	RTX830
6..12	RTX810
10...20	SRT100
8...64	上記以外の機種

- [初期値] :
 - 6000 (RTX5000)
 - 2000 (RTX3500、RTX3000)
 - 200 (RTX1220、RTX1210、RTX1200、RTX830 (Rev.15.02.22 以降))
 - 40 (RTX830)
 - 12 (RTX810)
 - 20 (SRT100)
 - 8 (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ブアライブの応答が遅れ、トンネルの障害を間違え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]

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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.23 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]]
```

[設定値及び初期値]

- *gateway_id*: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *group*: グループ識別子
 - [設定値]:
 - modp768
 - modp1024
 - modp1536
 - modp2048
 - [初期値]:
 - modp768 (RTX1500, RTX1100, RT107e)
 - modp1024 (上記以外の機種)

[説明]

IKE で用いるグループを設定する。

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、サポート可能な任意のグループを用いることができる。

その他、動作する IKE のバージョンによって異なる本コマンドの影響、注意点については以下の通り。

- IKEv1

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。

また、 **ipsec ike negotiate-strictly** コマンドが on の場合は、応答側であっても設定したグループしか利用できない。
- IKEv2

常に 1 つ目に設定したグループのみが使用される。2 つ目に設定したグループは無視される。

また、始動側として提案したグループが相手に拒否され、別のグループを要求された場合は、そのグループで再度提案する (要求されたグループがサポート可能な場合)。以後、IPsec の設定を変更するか再起動するまで、同じ相手側セキュリティ・ゲートウェイに対しては再提案したグループが優先的に使用される。

[ノート]

以下の機種では、グループ識別子に modp768 と modp1024 しか指定できない。

- RTX1500, RTX1100, RT107e

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.24 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]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *algorithm*
 - [設定値]:

設定値	説明
md5	MD5
sha	SHA-1
sha256	SHA-256

- [初期値]:
 - sha (RTX5000、RTX3500、RTX3000、RTX1220、RTX1210、RTX1200、RTX830、RTX810、SRT100)
 - md5 (上記以外の機種)

[説明]

IKE が用いるハッシュアルゴリズムを設定する。

始動側として働く場合に、本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本コマンドの設定に関係なく、サポートされている任意のアルゴリズムを用いることができる。

ただし、IKEv1 で **ipsec ike negotiate-strictly** コマンドが on の場合は、応答側であっても設定したアルゴリズムしか利用できない。

[ノート]

sha256 は、RTX3000 Rev.9.00.50 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで指定できる。

IKEv2 では、IKEv1 のハッシュアルゴリズムに相当する折衝パラメーターとして、認証アルゴリズム (Integrity Algorithm) と PRF(Pseudo-Random Function)がある。IKEv2 で **ipsec ike proposal-limitation** コマンドが on に設定されているとき、本コマンドで設定されたアルゴリズムを提案する。**ipsec ike proposal-limitation** コマンドが off に設定されているとき、または、**ipsec ike proposal-limitation** コマンドに対応していない機種では、本コマンドの設定にかかわらず、サポートするすべてのアルゴリズムを同時に提案し、相手側セキュリティ・ゲートウェイに選択させる。また応答側として働く場合は、提案されたものからより安全なアルゴリズムを選択する。

IKEv2 でサポート可能な認証アルゴリズム及び応答時の選択の優先順位は以下の通り。

- HMAC-SHA2-256-128 > HMAC-SHA-1-96 > HMAC-MD5-96

※HMAC-SHA2-256-128 は、RTX3000 Rev.9.00.50 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで対応。

また、IKEv2 でサポート可能な PRF、及び応答選択時の優先順位は以下の通り。

- HMAC-SHA2-256 > HMAC-SHA-1 > HMAC-MD5

※HMAC-SHA2-256 は、RTX3000 Rev.9.00.50 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで対応。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.25 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
```

[設定値及び初期値]

- *switch*

- [設定値]:

設定値	説明
on	ログに出力する
off	ログに出力しない

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.26 IKE ペイロードのタイプの設定

[書式]

```
ipsec ike payload type gateway_id type1 [type2]
```

```
no ipsec ike payload type gateway_id [type1 ...]
```

[設定値及び初期値]

- *gateway_id*

- [設定値]: セキュリティ・ゲートウェイの識別子

- [初期値]: -

- *type1*: IKEv1 のメッセージのフォーマット

- [設定値]:

設定値	説明
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

- [初期値]: 2

- *type2*: IKEv2 のメッセージのフォーマット

- [設定値]:

設定値	説明
1	ヤマハルーターの IKEv2 のリリース 1 との互換性を保持する
2	鍵交換や鍵の使用方法を一部の実装に合わせる

- [初期値]: 2

[説明]

IKEv1 および IKEv2 のペイロードのタイプを設定する。
 IKEv1 でヤマハルーターの古いリビジョンと接続する場合には、*type1* パラメータを 1 に設定する必要がある。
 IKEv2 でヤマハルーターの以下のリビジョンと接続する場合には、*type2* パラメータを 1 に設定する必要がある。

機種	リビジョン
RTX3000	Rev.9.00.56 以前
RTX1200	Rev.10.01.45 以前
RTX810	Rev.11.01.06 以前
FWX120	Rev.11.03.02

[ノート]

type2 パラメータは、RTX3000 Rev.9.00.60 以降、RTX1200 Rev.10.01.47 以降、RTX810 Rev.11.01.09 以降のファームウェア、および、Rev.14.00 系以降のすべてのファームウェアで指定できる。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.27 IKEv1 鍵交換タイプの設定

[書式]

```
ipsec ike backward-compatibility gateway_id type
no ipsec ike backward-compatibility gateway_id [type]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *type*: IKEv1 で使用する鍵交換のタイプ
 - [設定値]:

設定値	説明
1	ヤマハルーターのリリース 1 (過去のリリース) との互換性を保持する
2	ヤマハルーターのリリース 2 (新リリース) に合わせる

- [初期値]: 1

[説明]

IKEv1 で使用する鍵交換のタイプを設定する。
 IKEv1 でヤマハルーターの古いリビジョンと接続する場合には、*type* パラメータを 1 に設定する必要がある。

[ノート]

RTX5000 は Rev.14.00.12 以降で使用可能。
 RTX3500 は Rev.14.00.12 以降で使用可能。
 RTX810 は Rev.11.01.19 以降で使用可能。

RTX1200 は Rev.10.01.53 以降で使用可能。
RTX3000 は Rev.9.00.60 以降で使用可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

18.28 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]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *info*
 - [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: on

[説明]

IKEv1 動作時に、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。

本コマンドは IKEv2 としての動作には影響を与えない。IKEv2 では常に、必要に応じて情報ペイロードの送受信を行う。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.29 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]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -

- *pfs*
- [設定値]:

設定値	説明
on	用いる
off	用いない

- [初期値]: off

[説明]

IKE の始動側として働く場合に、PFS(Perfect Forward Secrecy) を用いるか否かを設定する。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、相手側セキュリティ・ゲートウェイの PFS の使用有無に合わせて動作する。

ただし、IKEv1 として動作し、且つ **ipsec ike negotiate-strictly** コマンドが on の場合は、本コマンドの設定と相手側セキュリティ・ゲートウェイの PFS の使用有無が一致していなければならない。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.30 XAUTH の設定

[書式]

```
ipsec ike xauth myname gateway_id name password
no ipsec ike xauth myname gateway_id
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *name*
 - [設定値]: XAUTH で通知する名前 (32 文字以内)
 - [初期値]: -
- *password*
 - [設定値]: XAUTH で通知するパスワード (32 文字以内)
 - [初期値]: -

[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。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.31 XAUTH 認証、EAP-MD5 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 ...]
```

[設定値及び初期値]

- *userid*
 - [設定値]:
 - ユーザ識別番号

設定値	機種
1..3000	RTX5000
1..1000	RTX1500/RTX1100/RT107e Rev.8.03.92 以降、 RTX3000 Rev.9.00.56 以降、SRT100 Rev.10.00.61 以 降、RTX1200 Rev.10.01.42 以降、RTX810 Rev. 11.01.06 以降、RTX3500、RTX1210、RTX830、 RTX1220
1..500	上記以外

- [初期値]: -
- *username*

- [設定値]:
 - ユーザ名

設定値	機種
256 文字以内	RTX3000 Rev.9.00.50 以降、RTX1200 Rev.10.01.22 以 降、Rev.11.01 系以降
32 文字以内	上記以外

* 3 文字以上に設定してください。

- [初期値]: -
- *password*

- [設定値]:
 - パスワード

設定値	機種
64 文字以内	RTX3000 Rev.9.00.50 以降、RTX1200 Rev.10.01.22 以 降、Rev.11.01 系以降
32 文字以内	上記以外

* 3 文字以上に設定してください。

- [初期値]: -

[説明]

IKEv1 の XAUTH 認証、または IKEv2 の EAP-MD5 認証に使用するユーザ ID を設定する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.32 XAUTH 認証、EAP-MD5 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 ...]
```

[設定値及び初期値]

- *userid*
 - [設定値]:
 - ユーザ識別番号

設定値	機種
1..3000	RTX5000

設定値	機種
1..1000	RTX1500/RTX1100/RT107e Rev.8.03.92 以降、 RTX3000 Rev.9.00.56 以降、SRT100 Rev.10.00.61 以 降、RTX1200 Rev.10.01.42 以降、RTX810 Rev. 11.01.06 以降、RTX3500、RTX1210、RTX830、 RTX1220
1..500	上記以外

- [初期値]: -
- *attribute=value*
 - [設定値]: ユーザ属性
 - [初期値]: *xauth=off*

[説明]

IKEv1 の XAUTH 認証、または IKEv2 の EAP-MD5 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。

<i>attribute</i>	<i>value</i>	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
eap-md5	on	IKEv2 の EAP-MD5 認証にこの ID を 使用する
	off	IKEv2 の EAP-MD5 認証にこの ID を 使用しない

同じ属性が重複して指定されている場合はコマンドエラーとなる。

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.33 XAUTH 認証、EAP-MD5 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
```

[設定値及び初期値]

- *groupid*
 - [設定値]:
 - ユーザグループ識別番号

設定値	機種
1..3000	RTX5000
1..1000	RTX1500/RTX1100/RT107e Rev.8.03.92 以降、 RTX3000 Rev.9.00.56 以降、SRT100 Rev.10.00.61 以 降、RTX1200 Rev.10.01.42 以降、RTX810 Rev. 11.01.06 以降、RTX3500、RTX1210、RTX830、 RTX1220
1..500	上記以外

- [初期値]: -
- *userid*
 - [設定値]: 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)
 - [初期値]: -

[説明]

IKEv1 の XAUTH 認証、または IKEv2 の EAP-MD5 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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.34 XAUTH 認証、EAP-MD5 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 attribute=value [attribute=value ...]

no auth user group attribute groupid [attribute=value ...]

[設定値及び初期値]

- *groupid*
 - [設定値]:
 - ユーザグループ識別番号

設定値	機種
1..3000	RTX5000
1..1000	RTX1500/RTX1100/RT107e Rev.8.03.92 以降、 RTX3000 Rev.9.00.56 以降、SRT100 Rev.10.00.61 以 降、RTX1200 Rev.10.01.42 以降、RTX810 Rev. 11.01.06 以降、RTX3500、RTX1210、RTX830、 RTX1220
1..500	上記以外

- [初期値]: -
- *attribute=value*
 - [設定値]: ユーザグループ属性
 - [初期値]: xauth=off

[説明]

IKEv1 の XAUTH 認証、または IKEv2 の EAP-MD5 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
eap-md5	on	IKEv2 の EAP-MD5 認証にこの ID を使用する
	off	IKEv2 の EAP-MD5 認証にこの ID を使用しない

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]

同じ属性が重複して指定されている場合はコマンドエラーとなる。

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.35 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 ...]
```

[設定値及び初期値]

- gateway_id
 - [設定値]: セキュリティゲートウェイの識別子
 - [初期値]: -
- group_id
 - [設定値]: 認証に使用するユーザグループの識別番号
 - [初期値]: -
- auth
 - [設定値]:

設定値	説明
on	要求する
off	要求しない

- [初期値]: off

[説明]

IPsec の認証を行う際、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。

[ノート]

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う。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.36 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 ...]
```

[設定値及び初期値]

- *pool_id*
 - [設定値]: アドレスプール ID(1..65535)
 - [初期値]: -
- *ip_address*
 - [設定値]: IP アドレス (IPv6 アドレス可)
 - [初期値]: -
- *ip_address-ip_address*
 - [設定値]: IP アドレスの範囲 (IPv6 アドレス可)
 - [初期値]: -
- *mask*
 - [設定値]: ネットマスク (IPv6 アドレスの時はプレフィックス長)
 - [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.37 IKE XAUTH Mode-Cfg メソッドの設定

[書式]

```
ipsec ike mode-cfg method gateway_id method [option]  

no ipsec ike mode-cfg method gateway_id [method...]
```

[設定値及び初期値]

- *gateway_id*

- [設定値]: セキュリティゲートウェイの識別子
- [初期値]: -
- *method*
 - [設定値]:

設定値	説明
set	SET メソッド

- [初期値]: set
- *option*

- [設定値]:

設定値	説明
openswan	Openswan 互換モード

- [初期値]: -

[説明]

IKE XAUTH の Mode-Cfg でのアドレス割り当てメソッドを設定する。指定できるのは SET メソッドのみである。
option に 'openswan' を指定した場合には Openswan 互換モードとなり、Openswan と接続できるようになる。

[ノート]

ダイヤルアップ VPN の発呼側にヤマハルーターおよび YMS-VPN1 を利用するとき、
option を指定していると XAUTH では接続できない。
 RTX1500、RTX1100、RT107e は Rev.8.03.82 以降で使用可能。
 RTX3000 は Rev.9.00.47 以降で使用可能。
 SRT100 は Rev.10.00.44 以降で使用可能。
 RTX1200 は Rev.10.01.11 以降で使用可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.38 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]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティゲートウェイの識別子
 - [初期値]: -
- *pool_id*
 - [設定値]: アドレスプール ID
 - [初期値]: -

[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 にて行われるため、XAUTH 認証を行わない場合には通知は行われない。

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 認証を行うためには必ず内部 IP アドレスの通知を行う設定にしなければならない。

[拡張ライセンス対応]

[拡張ライセンス](#)をインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.39 VPN クライアントの同時接続制限ライセンスの登録

[書式]

```
ipsec ike license-key license_id key
no ipsec ike license-key license_id [...]
```

[設定値及び初期値]

- *license_id*
 - [設定値]: ルーターキーの識別番号 (1..500)
 - [初期値]: -
- *key*
 - [設定値]: ルーターキー (64 文字以内)
 - [初期値]: -

[説明]

VPN クライアントソフト (同時接続版) からの VPN 接続を受け入れるためのルーターキー (ライセンスキー) を設定する。

各ルーターキーには固有の同時接続数が付与されており、異なる複数のルーターキーを登録することで、各ルーターキーの合計分の最大同時接続数を確保することができる。このとき、VPN クライアントソフトは本コマンドで登録したルーターキーに対応するクライアントキーならばどれを使用してもよい。VPN クライアントソフトが使用するクライアントキーに関わらず、登録された各ルーターキーの合計の最大同時接続数を基に接続制限が施される。

[ノート]

RTX3000 は Rev.9.00.48 以降で使用可能。

RTX1200 は Rev.10.01.22 以降で使用可能。

RTX830 は Rev.15.02.15 以降で使用可能。

[設定例]

```
[YMS-VPN1-CP/YMS-VPN7-CP の場合]
# tunnel select 1
# tunnel template 2-20
# ipsec tunnel 1
# ipsec sa policy 1 1 esp aes-cbc sha-hmac
# ipsec ike log 1 payload-info
# ipsec ike remote address 1 any
# ipsec ike xauth request 1 on 11
# ipsec ike mode-cfg address 1 1
# ipsec ike license-key use 1 on
```

```
# tunnel enable 1
# ipsec ike license-key 1 abcdefg-10-hijklmno
# ipsec ike license-key 2 pqrstuvwxyz-10-wxyz0123
# ipsec ike mode-cfg address pool 1 172.16.0.1-172.16.0.20/32
# auth user 1 user1 pass1
# auth user 2 user2 pass2
:
# auth user 20 user20 pass20
# auth user group 11 1-20
# auth user group attribute 11 xauth=on xauth-dns=10.10.10.1
```

```
[YMS-VPN8-CP の場合]
# pp select anonymous
# pp bind tunnel1-tunnel20
# pp auth request mschap-v2
# pp auth username user1 pass1
# pp auth username user2 pass2
:
# pp auth username user20 pass20
# ppp ipcp ipaddress on
# ppp ipcp msexp on
# ip pp remote address pool 172.16.0.1-172.16.0.20
# ip pp mtu 1258
# pp enable anonymous
# tunnel select 1
# tunnel encapsulation l2tp
# ipsec tunnel 1
# ipsec sa policy 1 1 esp 3des-cbc sha-hmac
# ipsec ike keepalive use 1 off
# ipsec ike local address 1 172.16.0.254
# ipsec ike remote address 1 any
# ipsec ike license-key use 1 on
# l2tp tunnel disconnect time off
# ip tunnel tcp mss limit auto
# tunnel enable 1
:
# ipsec ike license-key 1 abcdefg-10-hijklmno
# ipsec ike license-key 2 pqrstuvwxyz-10-wxyz0123
# ipsec transport 1 1 udp 1701
# ipsec auto refresh on
# l2tp service on
```

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830

18.40 VPN クライアントの同時接続制限ライセンスの適用

[書式]

```
ipsec ike license-key use gateway_id sw
no ipsec ike license-key use gateway_id [...]
```

[設定値及び初期値]

- gateway_id
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- sw
 - [設定値]:

設定値	説明
on	ルーターキーの適用を許可する
off	ルーターキーの適用を許可しない

- [初期値]: off

[説明]

VPN クライアントソフト (同時接続版) からの VPN 接続を受け入れるためのルーターキー (ライセンスキー) の適用を許可するか否かを設定する。

ルーターキーの適用を許可されたゲートウェイが、対応するクライアントキーを持つ VPN クライアントソフトと接続可能になる。

[ノート]

RTX3000 は Rev.9.00.48 以降で使用可能。
 RTX1200 は Rev.10.01.22 以降で使用可能。
 RTX830 は Rev.15.02.15 以降で使用可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830

18.41 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]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *type*
 - [設定値]:

設定値	説明
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

- [初期値]: -

[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。

IKEv2 に対応した機種では、*gateway_id* パラメータを省略することができる。*gateway_id* パラメータを省略した設定は、応答側として働く際、セキュリティ・ゲートウェイが特定できない時点での通信に対して適用される。

[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。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.42 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
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *encap*
 - [設定値]:

設定値	説明
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

- [初期値]: off

[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。

[ノート]

ipsec ike nat-traversal コマンドとの併用はできない。

本コマンドは IKEv2 により確立された SA を伴う IPsec 通信には影響を与えない。

[拡張ライセンス対応]

[拡張ライセンス](#)をインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.43 折衝パラメーターを制限するか否かの設定

[書式]

```
ipsec ike proposal-limitation gateway_id switch
no ipsec ike proposal-limitation gateway_id [switch]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *switch*
 - [設定値]:

設定値	説明
on	折衝パラメーターを制限する
off	折衝パラメーターを制限しない

- [初期値]: off

[説明]

IKEv2 で鍵交換を始動するときに、SA を構築するための各折衝パラメーターを、特定のコマンド設定値に限定して

提案するか否かを設定する。このコマンドの設定が **off** のときは、サポート可能な折衝パラメーター全てを提案する。

このコマンドが適用されるパラメーターと対応するコマンドは以下の通りである。

パラメーター	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
暗号・認証アルゴリズム	ipsec sa policy ※CHILD SA 作成時

[ノート]

本コマンドは IKEv2 でのみ有効であり、IKEv1 の動作に影響を与えない。

RTX1210 は Rev.14.01.09 以降で使用可能。

RTX5000、RTX3500 は Rev.14.00.18 以降で使用可能。

RTX810 は Rev.11.01.21 以降で使用可能。

RTX1200 は Rev.10.01.59 以降で使用可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

18.44 IKE のメッセージ ID 管理の設定

[書式]

```
ipsec ike message-id-control gateway_id switch
no ipsec ike message-id-control gateway_id [switch]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *switch*
 - [設定値]:

設定値	説明
on	リクエストメッセージの送信をメッセージ ID で管理する
off	リクエストメッセージの送信をメッセージ ID で管理しない

- [初期値]: off

[説明]

自機から IKEv2 のリクエストメッセージを送信するときのメッセージ ID 管理方法を設定する。

on に設定しているとき、同じ IKE SA を使用して送信済みの IKE メッセージに対する全てのレスポンスメッセージを受信していない場合、新しい IKE メッセージは送信しない。

[ノート]

本コマンドは IKEv2 でのみ有効であり、IKEv1 の動作に影響を与えない。

RTX1210 は Rev.14.01.09 以降で使用可能。
 RTX5000、RTX3500 は Rev.14.00.18 以降で使用可能。
 RTX810 は Rev.11.01.21 以降で使用可能。
 RTX1200 は Rev.10.01.59 以降で使用可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

18.45 CHILD SA 作成方法の設定

[書式]

```
ipsec ike child-exchange type gateway_id type
no ipsec ike child-exchange type gateway_id [type]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *type*: IKEv2 の CHILD SA 作成方法のタイプ
 - [設定値]:

設定値	説明
1	ヤマハルーターの IKEv2 の従来動作との互換性を保持する
2	CREATE_CHILD_SA 交換を一部の実装にあわせる

- [初期値]: 1

[説明]

IKEv2 の CHILD SA 作成方法を設定する。
 このコマンドに対応する機種同士で接続する場合、*type* を同じ設定にして接続する必要がある。

[ノート]

本コマンドは IKEv2 でのみ有効であり、IKEv1 の動作に影響を与えない。
 RTX1210 は Rev.14.01.11 以降で使用可能。
 RTX5000、RTX3500 は Rev.14.00.18 以降で使用可能。
 RTX810 は Rev.11.01.28 以降で使用可能。
 RTX1200 は Rev.10.01.71 以降で使用可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

18.46 鍵交換の始動パケットを受信するか否かの設定

[書式]

```
ipsec ike negotiation receive gateway_id switch
no ipsec ike negotiation receive gateway_id [switch]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *switch*
 - [設定値]:

設定値	説明
on	鍵交換の始動パケットを受信する
off	鍵交換の始動パケットを受信しない

- [初期値]: on

[説明]

IKEv2 で、鍵交換の始動パケットを受信するか否かを設定する。
受信しないに設定した場合は、結果として受動側としては動作せず、必ず始動側として動作するようになる。

[ノート]

本コマンドは IKEv2 でのみ有効であり、IKEv1 の動作に影響を与えない。
off にする場合には、`ipsec ike remote address` または `ipsec ike remote name` を IP アドレスで設定しておく必要がある。
RTX1200 Rev.10.01.75 以降、RTX810 Rev.11.01.31 以降、RTX5000 Rev.14.00.26 以降、RTX3500 Rev.14.00.26 以降、
RTX1210 Rev.14.01.26 以降、RTX830 Rev.15.02.03 以降、RTX1220 で使用可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

18.47 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ならない。

18.47.1 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]]
```

[設定値及び初期値]

- *sa*
 - [設定値]:

設定値	説明
ipsec-sa (もしくは child-sa)	IPsec SA (CHILD SA)
isakmp-sa (もしくは ike-sa)	ISAKMP SA (IKE SA)

- [初期値]: -

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *second*
 - [設定値]: 秒数 (300..691200)
 - [初期値]: 28800 秒
- *kbytes*
 - [設定値]: キロ単位のバイト数 (100..100000)
 - [初期値]: -
- *rekey*: SA を更新するタイミング
 - [設定値]:

設定値	説明
70%-90%	パーセント
off	更新しない (<i>sa</i> パラメータで <i>isakmp-sa</i> (<i>ike-sa</i>) を指定したときのみ設定可能)

- [初期値]: 75%

[説明]

各 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* (*child-sa*) を指定したときのみ有効である。SA の更新は *kbytes* パラメータに設定したバイト数の 75% を処理したタイミングで行われる。

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% を指定した場合には、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*(*ike-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。このとき、IPsec SA (CHILD SA) を作る必要がない限り、ISAKMP SA (IKE SA) の更新を保留するので、ISAKMP SA (IKE SA) の生成を最小限に抑えることができる。

その他、動作する IKE のバージョンによって異なる、本コマンドの影響、注意点については以下の通り。

- IKEv1
 - 始動側として働く場合に、このコマンドで設定した寿命値が提案される。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相手側から提案された寿命値に合わせる。
 - また、ISAKMP SA に対する *rekey* パラメータを off に設定した場合、そ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。

- IKEv2
 - IKEv2 では SA 寿命値は折衝されず、各セキュリティ・ゲートウェイが独立して管理するものとなっている。従って、確立された SA には、常にこのコマンドで設定した寿命値がセットされる。ただし、相手側セキュリティ・ゲートウェイの方が SA 更新のタイミングが早ければ、SA はその分早く更新されることになる。
 - ISAKMP SA (IKE SA) の寿命が IPsec SA (CHILD SA) の寿命より先に尽きた場合は、ISAKMP SA (IKE SA) の寿命値を IPsec SA (CHILD SA) の寿命値に合わせる。

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。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.47.2 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=remote-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]
```

[設定値及び初期値]

- *policy_id*
 - [設定値]: ポリシー ID(1..2147483647)
 - [初期値]: -
- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *ah*: 認証ヘッダ (Authentication Header) プロトコルを示すキーワード
 - [初期値]: -
- *esp*: 暗号ペイロード (Encapsulating Security Payload) プロトコルを示すキーワード
 - [初期値]: -
- *ah_algorithm*: 認証アルゴリズム
 - [設定値]:

設定値	説明
md5-hmac	HMAC-MD5
sha-hmac	HMAC-SHA-1
sha256-hmac	HMAC-SHA2-256

- [初期値]:
 - sha-hmac (AH プロトコルの場合)
 - - (ESP プロトコルの場合)
- *esp_algorithm*: 暗号アルゴリズム
 - [設定値]:

設定値	説明
3des-cbc	3DES-CBC
des-cbc	DES-CBC
aes-cbc	AES128-CBC
aes256-cbc	AES256-CBC

- [初期値]:
 - aes-cbc (RTX3000 Rev.9.00.50 以降、RTX1200 Rev.10.01.22 以降、および、Rev.11.01 系以降)
 - - (上記以外の機種)

- *local-id*
 - [設定値]: 自分側のプライベートネットワーク
 - [初期値]: -
- *remote-id*
 - [設定値]: 相手側のプライベートネットワーク
 - [初期値]: -
- *check*
 - [設定値]:

設定値	説明
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

- [初期値]: on

[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。

local-id、*remote-id* には、カプセル化したいパケットの始点/終点アドレスの範囲をネットワークアドレスで記述する。これにより、1つのセキュリティ・ゲートウェイに対して、複数の IPsec SA を生成し、IP パケットの内容に応じて SA を使い分けることができるようになる。

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。

IKEv2 では、**ipsec ike proposal-limitation** コマンドが *on* に設定されているとき、本コマンドの *ah_algorithm*、および *esp_algorithm* パラメーターで設定されたアルゴリズムを提案する。**ipsec ike proposal-limitation** コマンドが *off* に設定されているとき、または、**ipsec ike proposal-limitation** コマンドに対応していない機種では、本コマンドの設定にかかわらず、サポートするすべてのアルゴリズムを同時に提案し、相手側セキュリティ・ゲートウェイに選択させる。また応答側として働く場合は受け取った提案から以下の優先順位でアルゴリズムを選択する。

- 認証アルゴリズム

HMAC-SHA2-256 > HMAC-SHA-1 > HMAC-MD5

※HMAC-SHA2-256 は、RTX3000 Rev.9.00.50 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで対応。

- 暗号アルゴリズム

AES256-CBC > AES192-CBC > AES128-CBC > 3DES-CBC > DES-CBC

※IKEv2 でのみ AES192-CBC をサポートする。ただし、コマンドで AES192-CBC を選択することはできない。

また、IKEv2 では *local-id*、*remote-id* パラメーターに関しても効力を持たない。

[ノート]

双方で設定する *local-id* と *remote-id* は一致している必要がある。

sha256-hmac および *aes256-cbc* は、RTX3000 Rev.9.00.50 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで指定できる。

ah_algorithm、および *esp_algorithm* パラメーターは、RTX3000 Rev.9.00.50 以降、RTX1200 Rev.10.01.22 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアでは省略可能であり、これら以外の機種では必ず指定する必要がある。

[設定例]

```
# ipsec sa policy 101 1 esp aes-cbc sha-hmac
```

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.47.3 SA の手動更新

[書式]

ipsec refresh sa

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.47.4 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]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *action*
 - [設定値]:

設定値	説明
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。

- [初期値]: auto

[説明]

このコマンドは IKEv1 のダングリング 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は、このコマンドにより動作を変更でき、それ以外では、ダングリング SA が発生しても何もせず通信を続ける。

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 IKESA が存在する IPsec SA で行われるようにしなくてはならない。

本コマンドは IKEv2 の動作には影響を与えない。IKEv2 では仕様として、ダングリング SA の存在を禁止している。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.47.5 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*] [force=*force_switch*] [type=*type*]

no ipsec ike nat-traversal gateway [*switch ...*]

[設定値及び初期値]

- *gateway*
 - [設定値]: セキュリティゲートウェイの識別子
 - [初期値]: -
- *switch*: 動作の有無
 - [設定値]:

設定値	説明
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

- [初期値]: off
- *interval*: NAT キープアライブの送信間隔
 - [設定値]:

設定値	説明
off	送信しない
30-100000	時間[秒]

- [初期値]: 300
- *force_switch*
 - [設定値]:

設定値	説明
on	通信経路上に NAT がなくても NAT トラバーサルを使用する
off	通信経路上に NAT がなければ NAT トラバーサルを使用しない

- [初期値]: off
- *type*
 - [設定値]:

設定値	説明
1	ヤマハルーターの従来の動作との互換性を保持する
2	NAT トラバーサル使用時に交換するペイロードを一部の実装に合わせる

- [初期値]: 1

[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

type に対応した機種同士で接続する場合、*type* を同じ設定にして接続する必要がある。また、*type* に 2 を指定した場合、*type* に対応していない機種との接続はできない。

IKEv2 では、イニシエータとして動作する場合のみ *switch* パラメータが影響する。このオプションは、通信経路上に NAT 処理がなくても NAT トラバーサル動作が必要な対向機器と接続する場合に使用する。なお、通常は 'off' にしておくことが望ましい。

[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。

IKEv1 では、メインモードおよび、アグレッシブモードの ESP トンネルでのみ利用できる。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。

ただし、L2TP/IPsec と L2TPv3 を用いた L2VPN で使用される IKEv1 では、メインモードかつトランスポートモードの ESP トンネルでも利用できる。

IKEv2 では、ESP トンネルを確立する場合のみ利用できる。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。

IKEv1 メインモードでの NAT トラバーサルは、RTX810 Rev.11.01.31 以降、RTX5000、RTX3500 Rev.14.00.22 以降、RTX1210 Rev.14.01.20 以降のファームウェア、および、Rev.15.02 系以降のすべてのファームウェアで利用できる。

force オプションは、RTX3000 Rev.9.00.50 以降、RTX1200 Rev.10.01.22 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで使用できる。

type オプションは、RTX810 Rev.11.01.31 以降、RTX5000、RTX3500 Rev.14.00.22 以降、RTX1210 Rev.14.01.20 以降のファームウェア、および、Rev.15.02 系以降のすべてのファームウェアで使用できる。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.47.6 SA の削除

[書式]

ipsec sa delete *id*

[設定値及び初期値]

- *id*
- [設定値]:

設定値	説明
番号	SA の ID
all	すべての SA

- [初期値]:-

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.48 トンネルインタフェース関連の設定

18.48.1 IPsec トンネルの外側の IPv4 パケットに対するフラグメントの設定

[書式]

```
ipsec tunnel fastpath-fragment-function follow df-bit switch
no ipsec tunnel fastpath-fragment-function follow df-bit [switch]
```

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
on	ESP パケットをフラグメントする必要がある場合に ESP パケットの DF ビットに従ってフラグメントするかを決定する
off	ESP パケットをフラグメントする必要がある場合に ESP パケットの DF ビットに関係なくフラグメントする

- [初期値]: off

[説明]

ESP パケットをフラグメントする必要がある場合に、DF ビットに従ってフラグメントするか否かを設定する。ipsec tunnel outer df-bit コマンドによって DF ビットがセットされた ESP パケットであっても本コマンドで off が設定されている場合はフラグメントされる。本コマンドは、トンネルインタフェースに対して設定し、ファストパスで処理される ESP パケットのみを対象とする。

[ノート]

RTX810 は Rev.11.01.09 以降で使用可能。
 RTX1200 は Rev.10.01.42 以降で使用可能。
 SRT100 は Rev.10.00.61 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

18.48.2 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]
```

[設定値及び初期値]

- *mode*
- [設定値]:

設定値	説明
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

- [初期値]: copy

[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ならない時には、このコマンドの設定に関わらず DF ビットは 0 になる。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.48.3 使用する SA のポリシーの設定**[書式]**

```
ipsec tunnel policy_id
no ipsec tunnel [policy_id]
```

[設定値及び初期値]

- *policy_id*
 - [設定値]: 整数 (1..2147483647)
 - [初期値]: -

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.48.4 IPComp によるデータ圧縮の設定**[書式]**

```
ipsec ipcomp type type
no ipsec ipcomp type [type]
```

[設定値及び初期値]

- *type*
 - [設定値]:

設定値	説明
deflate	deflate 圧縮でデータを圧縮する
none	データ圧縮を行わない

- [初期値]: none

[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、一定の効果を得られる。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、例えば本機の出カインタフェースが LAN であってもデータ圧縮効果を期待できる。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810

18.48.5 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
```

[設定値及び初期値]

- none : トンネルバックアップを使用しない
 - [初期値] : none
- interface
 - [設定値] : LAN インタフェース名
 - [初期値] : -
- ip_address
 - [設定値] : バックアップ先のゲートウェイの IP アドレス
 - [初期値] : -
- peer_num
 - [設定値] : バックアップ先の相手先情報番号
 - [初期値] : -
- tunnel_num
 - [設定値] : トンネルインタフェース番号
 - [初期値] : -
- 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
 - [設定値] :

設定値	説明
on	分ける
off	分けない

- [初期値] : off
- 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
 - [設定値] :

設定値	説明
on	作り直す
off	作り直さない

- [初期値] : on

[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。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- tunnel_num

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.48.6 トンネルテンプレートの設定

[書式]

tunnel template *tunnel_num* [*tunnel_num* ...]

no tunnel template

[設定値及び初期値]

- *tunnel_num*
 - [設定値]: トンネルインタフェース番号、または間にハイフン (-) をはさんでトンネルインタフェース番号を範囲指定したもの
 - [初期値]: -

[説明]

tunnel select コマンドにて選択されたトンネルインタフェースを展開元として、当該インタフェースに設定されているコマンドの展開先となるトンネルインタフェースを設定する。

展開元のトンネルインタフェースに設定することで、展開先のトンネルインタフェースにも適用されるコマンドは以下のとおりである。なお、末尾に (*1) または (*2) が付加されているコマンドについては [ノート] を参照のこと。

- **ipsec tunnel**
- **ipsec sa policy**
- **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** (引数にセキュリティ・ゲートウェイの識別子を指定する場合)
- **tunnel encapsulation (*1)**
- **tunnel ngn arrive permit (*1)**
- **tunnel ngn bandwidth (*1)**
- **tunnel ngn disconnect time (*1)**
- **tunnel ngn radius auth (*1)**
- **l2tp** で始まるコマンド (*2)
- **tunnel enable**

上記コマンドのうち以下のコマンドについては、特定のパラメータの値が展開元のトンネルインタフェース番号に一致する場合のみ、コマンドが展開される。その場合、当該パラメータの値は展開先のトンネルインタフェース番号に置換される。

コマンド	パラメータ
ipsec tunnel	ポリシー ID
ipsec sa policy	ポリシー ID
ipsec ike で始まるコマンド	セキュリティ・ゲートウェイの識別子
ipsec auto refresh	セキュリティ・ゲートウェイの識別子
tunnel enable	トンネルインタフェース番号

ipsec sa policy コマンドでは、セキュリティ・ゲートウェイの識別子が展開先のトンネルインタフェース番号に置換される。

ipsec ike remote name コマンドでは、相手側セキュリティ・ゲートウェイの名前の末尾に展開先のトンネルインタフェース番号が付加される。

展開元のトンネルインタフェースに設定されているコマンドと同じコマンドが、展開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、展開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が優先される。

コマンド展開後の、ルーターの動作時に参照される設定は **show config tunnel** コマンドに **expand** キーワードを指定することで確認できる。

[ノート]

トンネルインタフェースが選択されている時のみ使用できる。

本コマンドは Rev.8.03 系以降で使用可能である。なお、展開対象となるコマンドのうち、末尾に (*1) が付加されているコマンドについては、以下の機種、リビジョンで対応している。

機種	リビジョン
RTX5000、RTX3500	すべてのリビジョン
RTX3000	Rev.9.00.56 以降
RTX1220	すべてのリビジョン
RTX1210	すべてのリビジョン
RTX1200	Rev.10.01.42 以降
RTX830	すべてのリビジョン
RTX810	Rev.11.01.09 以降

展開対象となるコマンドのうち、末尾に (*2) が付加されているコマンドについては、以下の機種、リビジョンで対応している。

機種	リビジョン
RTX5000、RTX3500	Rev.14.00.12 以降
RTX3000	Rev.9.00.60 以降
RTX1220	すべてのリビジョン
RTX1210	すべてのリビジョン
RTX1200	Rev.10.01.59 以降
RTX830	すべてのリビジョン
RTX810	Rev.11.01.21 以降

[設定例]

展開先のトンネルインタフェースとして、番号の指定と範囲の指定を同時に記述することができる。

```
tunnel select 1
  tunnel template 8 10-20
tunnel select 2
  tunnel template 100 200-300 400
```

以下の2つの設定は同じ内容を示している。

```
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
```

```
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

```

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.49 トランスポートモード関連の設定

18.49.1 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]]]]

```

[設定値及び初期値]

- *id*
 - [設定値]: トランスポート ID(1..2147483647)
 - [初期値]: -
- *policy_id*
 - [設定値]: ポリシー ID(1..2147483647)
 - [初期値]: -
- *proto*
 - [設定値]: プロトコル
 - [初期値]: -
- *src_port_list*: UDP、TCP のソースポート番号列
 - [設定値]:
 - 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)
 - [初期値]: -
- *dst_port_list*: UDP、TCP のデスティネーションポート番号列
 - [設定値]:
 - 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)
 - [初期値]: -

[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]

- TELNET のデータをトランスポートモードで通信

```
# ipsec sa policy 101 1 esp aes-cbc sha-hmac
# ipsec transport 1 101 tcp * telnet
```

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

18.49.2 トランスポートモードのテンプレートの設定

[書式]

```
ipsec transport template id1 id2 [id2 ...]
no ipsec transport template id1 [id2 ...]
```

[設定値及び初期値]

- *id1*
 - [設定値]: 展開元のトランスポート ID
 - [初期値]: -
- *id2*
 - [設定値]: 展開先のトランスポート ID、または間にハイフン(-)をはさんでトランスポート ID を範囲指定したもの
 - [初期値]: -

[説明]

指定した **ipsec transport** コマンドの設定の展開先となるトランスポート ID を設定する。展開先のポリシー ID は展開先のトランスポート ID と同じ値が設定される。

展開先のトランスポート ID に対して既に設定が存在する場合、展開先の設定が優先される。

本コマンドによって VPN 対地数まで **ipsec transport** コマンドの設定を展開することができる。VPN 対地数を超える範囲に展開することはできない。

[ノート]

RTX5000 は Rev.14.00.12 以降で使用可能。
 RTX3500 は Rev.14.00.12 以降で使用可能。
 RTX810 は Rev.11.01.21 以降で使用可能。
 RTX1200 は Rev.10.01.59 以降で使用可能。
 RTX3000 は Rev.9.00.60 以降で使用可能。

[設定例]

展開先の設定としてトランスポート ID とトランスポート ID の範囲を同時に記述することができる。

```
ipsec transport 1 1 udp 1701 *
ipsec transport template 1 10 20-30
```

以下の 2 つの設定は同じ内容を示している。

```
ipsec transport 1 1 udp 1701 *
ipsec transport template 1 2 10-12
```

```
ipsec transport 1 1 udp 1701 *
ipsec transport 2 2 udp 1701 *
ipsec transport 10 10 udp 1701 *
ipsec transport 11 11 udp 1701 *
ipsec transport 12 12 udp 1701 *
```

[拡張ライセンス対応]

拡張ライセンスをインポートすると、**ipsec transport** コマンドの設定を展開するトランスポート ID (*id*) の最大個数が拡張される。

- *id*

ライセンス名	拡張後の最大個数
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX830, RTX810

18.50 PKI 関連の設定

18.50.1 証明書ファイルの設定

[書式]

```
pki certificate file cert_id file type [password]
```

```
no pki certificate file cert_id [file ...]
```

[設定値及び初期値]

- *cert_id*

- [設定値]:

設定値	説明
1..2(RTX3000)	証明書ファイルの識別子
1..8(RTX3000 以外)	

- [初期値]: -

- *file*

- [設定値]:

設定値	説明
内蔵フラッシュ ROM の証明書ファイル番号 (RTX3000)	証明書ファイルのファイル名
外部メモリ、RTFS 領域内のファイルを絶対パスまたは相対パスで指定する。(RTX3000 以外)	

- [初期値]: -

- *type*: ファイル形式

- [設定値]:

設定値	説明
pkcs12	PKCS#12 形式のファイル
x509-pem	X.509 PEM 形式のファイル

- [初期値]: -

- *password*

- [設定値]: ファイルを復号するためのパスワード(半角 64 文字以内)

- [初期値]: -

[説明]

証明書ファイルを設定する。

PKI ファイルを内蔵フラッシュ ROM の専用領域へ保存する機種と、外部メモリや RTFS 領域へ保存する機種によって *file* の指定形式が異なるので注意する必要がある。

内蔵フラッシュ ROM の専用領域へ保存する機種の場合、証明書ファイル番号は **show file list internal** コマンドで確認できる。

外部メモリや RTFS 領域が利用可能な機種で *file* に相対パスを指定する場合、**set** コマンドの環境変数 *pwd* で指定し

たディレクトリからの相対パスを指定する。

type に `pkcs12` を指定した場合、ファイルを復号するための *password* を指定する必要がある。

[ノート]

RTX3000 は Rev.9.00.50 以降で使用可能。

RTX1200 は Rev.10.01.22 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

18.50.2 CRL ファイルの設定

[書式]

`pki crl file crl_id file`

`no pki crl file crl_id [file]`

[設定値及び初期値]

- *crl_id*

- [設定値]:

設定値	説明
1..2(RTX3000)	CRL ファイルの識別子
1..8(RTX3000 以外)	

- [初期値]: -

- *file*

- [設定値]:

設定値	説明
内蔵フラッシュ ROM の CRL ファイル番号 (RTX3000)	CRL ファイルのファイル名
外部メモリ、RTFS 領域内のファイルを絶対パスまたは相対パスで指定する (RTX3000 以外)	

- [初期値]: -

[説明]

CRL ファイルを設定する。

PKI ファイルを内蔵フラッシュ ROM の専用領域へ保存する機種と、外部メモリや RTFS 領域へ保存する機種によって *file* の指定形式が異なるので注意する必要がある。

内蔵フラッシュ ROM の専用領域へ保存する機種の場合、CRL ファイル番号は `show file list internal` コマンドで確認できる。

外部メモリや RTFS 領域が利用可能な機種で *file* に相対パスを指定する場合、`set` コマンドの環境変数 *pwd* で指定したディレクトリからの相対パスを指定する。

[ノート]

RTX3000 は Rev.9.00.50 以降で使用可能。

RTX1200 は Rev.10.01.22 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

第 19 章

L2TP 機能の設定

L2TP/IPsec 機能

L2TP (Layer Two Tunneling Protocol) は、ネットワーク間での VPN (Virtual Private Network) 接続を実現するトンネリングプロトコルです。L2TP 自体は暗号化の仕組みを持ちませんが、IPsec を併用することでデータの機密性や完全性を確保した VPN 接続を実現する L2TP/IPsec があります。ヤマハルーターは、L2TP/IPsec を用いたリモートアクセス VPN のサーバーとして動作します。スマートフォンなどに搭載されている L2TP クライアントからインターネット越しにヤマハルーター配下のプライベートネットワーク内の端末とのセキュアな通信を可能にします。

ヤマハルーターでサポートする L2TP/IPsec には以下の制限があります。

- L2TP 単体での機能は提供しません。L2TP/IPsec のみサポートします。
- リモートアクセス VPN のサーバーとして動作します。クライアントとしては動作しません。
- LAN 間接続 VPN には対応していません。
- L2TP パケットの最初の待ち受けは UDP のポート番号 1701 が使用されます。変更することはできません。
- IKEv1 にのみ対応しており、IKEv2 は使用できません。

L2TPv3 機能

L2TPv3 (Layer 2 Tunneling Protocol version 3) は、データリンク層(L2)での VPN 接続 (L2VPN)を実現するトンネリングプロトコルです。L2 フレームを IP パケットとしてカプセル化することでルーター間での L2 フレーム転送を可能にし、複数の拠点で同一セグメントのネットワークを構築することができます。L2TPv3 自体は暗号化の仕組みを持ちませんが、IPsec と併用することでデータの機密性や完全性を確保した VPN 接続を実現する L2TPv3/IPsec があります。ヤマハルーターでは、L2TPv3 を用いた L2VPN および L2TPv3/IPsec を用いた L2VPN を構築することができます。

ヤマハルーターでサポートする L2TPv3 には以下の制限があります。

- L2 フレームのカプセル化方式として、UDP パケットとしてカプセル化する方法(L2TPv3 over UDP)にのみ対応しています。IP プロトコル番号 115 を使用して IP パケットとしてカプセル化する方法(L2TPv3 over IP)には対応していません。
- L2TPv3 パケットの受信には UDP のポート番号 1701 が使用されます。変更することはできません。
- L2TPv3 によってトンネリングできる L2 フレームは、イーサフレームのみです。
- L2TPv3/IPsec では、IKEv1 のトランスポートモードのみ対応しています。

19.1 L2TP を動作させるか否かの設定

[書式]

```
l2tp service service [version [version]]
no l2tp service [service [version [version]]]
```

[設定値及び初期値]

- *service*

- [設定値]:

設定値	説明
on	L2TP を有効にする
off	L2TP を無効にする

- [初期値]: off

- *version*

- [設定値]:

設定値	説明
l2tp	L2TP/IPsec を有効にする
l2tpv3	L2TPv3, L2TPv3/IPsec を有効にする

- [初期値]: -

[説明]

L2TP を動作させるか否かを設定する。

version によって動作する L2TP のバージョンを指定できる。version を指定しない場合には L2TPv2 と L2TPv3 の両方が動作する。

L2TP が有効になると UDP のポート番号 1701 を開き、L2TP コネクションの接続を待つ。

L2TP が無効になると UDP のポート番号 1701 を閉じ、接続中の L2TP コネクションはすべて切断される。

[ノート]

version は L2TPv3 機能が実装されたモデルでのみ指定可能。

RTX1500、RTX1100、RT107e は Rev.8.03.92 以降で使用可能。

RTX3000 は Rev.9.00.60 以降で使用可能。

SRT100 は Rev.10.00.60 以降で使用可能。

RTX1200 は Rev.10.01.32 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

19.2 L2TP トンネル認証に関する設定

[書式]

l2tp tunnel auth *switch* [*password*]

no l2tp tunnel auth [*switch* ...]

[設定値及び初期値]• *switch*

- [設定値]:

設定値	説明
on	L2TP トンネル認証を行う
off	L2TP トンネル認証を行わない

- [初期値]: off

• *password*

- [設定値]: L2TP トンネル認証に用いるパスワード(32 文字以内)
- [初期値]: -

[説明]

L2TP トンネル認証を行うか否かを設定する。

password を省略した場合には機種名がパスワードとして使用される。

RTX1200 の場合には "RTX1200" がパスワードとなる。大文字小文字の区別に注意してください。

[ノート]

RTX1500、RTX1100、RT107e は Rev.8.03.92 以降で使用可能。

RTX3000 は Rev.9.00.60 以降で使用可能

SRT100 は Rev.10.00.60 以降で使用可能。

RTX1200 は Rev.10.01.32 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

19.3 L2TP トンネルの切断タイマの設定

[書式]

l2tp tunnel disconnect time *time*

no l2tp tunnel disconnect time [*time*]

[設定値及び初期値]

- *time*
 - [設定値]:

設定値	説明
1..21474836	秒数
off	タイマを設定しない

- [初期値]: 60

[説明]

L2TP トンネルの切断タイマを設定する。

選択されている L2TP 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 L2TP トンネルを切断する時間を設定する。

L2TP 制御メッセージ以外はすべてデータパケットとなるため、PPP キープアライブを使用する場合などは切断タイマによる L2TP トンネルの切断は行われない場合がある。

トンネルインタフェースにのみ設定可能です。

[ノート]

RTX1500、RTX1100、RT107e は Rev.8.03.92 以降で使用可能。

RTX3000 は Rev.9.00.60 以降で使用可能。

SRT100 は Rev.10.00.60 以降で使用可能。

RTX1200 は Rev.10.01.32 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

19.4 L2TP キープアライブの設定

[書式]

l2tp keepalive use switch [*interval* [*count*]]

no l2tp keepalive use [*switch* ...]

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	L2TP キープアライブを使用する
off	L2TP キープアライブを使用しない

- [初期値]: on
- *interval*
 - [設定値]: キープアライブパケットを送出する時間間隔[秒] (1..600)
 - [初期値]: 10
- *count*
 - [設定値]: ダウン検出を判定する回数 (1..50)
 - [初期値]: 6

[説明]

L2TP キープアライブを使用するか否かを選択する。

キープアライブを行う場合は *interval* と *count* の設定値の応じて L2TP の Hello メッセージによるキープアライブが動作する。

トンネルインタフェースにのみ設定可能です。

[ノート]

RTX1500、RTX1100、RT107e は Rev.8.03.92 以降で使用可能。

RTX3000 は Rev.9.00.60 以降で使用可能。

SRT100 は Rev.10.00.60 以降で使用可能。

RTX1200 は Rev.10.01.32 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

19.5 L2TP キープアライブのログ設定

[書式]

l2tp keepalive log *log*

no l2tp keepalive log [*log*]

[設定値及び初期値]

- *log*

- [設定値]:

設定値	説明
on	L2TP キープアライブをログに出力する
off	L2TP キープアライブをログに出力しない

- [初期値]: off

[説明]

L2TP キープアライブのログを出力するか否かを設定する。

ログはすべて、**debug** レベルの **SYSLOG** に出力される。

トンネルインタフェースにのみ設定可能です。

[ノート]

RTX1500、RTX1100、RT107e は Rev.8.03.92 以降で使用可能。

RTX3000 は Rev.9.00.60 以降で使用可能。

SRT100 は Rev.10.00.60 以降で使用可能。

RTX1200 は Rev.10.01.32 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

19.6 L2TP の接続制御の syslog を出力するか否かの設定

[書式]

l2tp syslog *syslog*

no l2tp syslog [*syslog*]

[設定値及び初期値]

- *syslog*

- [設定値]:

設定値	説明
on	L2TP の接続制御に関するログを SYSLOG に出力する
off	L2TP の接続制御に関するログを SYSLOG に出力しない

- [初期値]: off

[説明]

L2TP の接続制御に関するログを SYSLOG に出力するか否かを設定する。
 L2TP のキープアライブに関するログは出力されない。
 ログはすべて、debug レベルの SYSLOG に出力される。
 トンネルインタフェースにのみ設定可能です。

[ノート]

RTX1500、RTX1100、RT107e は Rev.8.03.92 以降で使用可能。
 RTX3000 は Rev.9.00.60 以降で使用可能。
 SRT100 は Rev.10.00.60 以降で使用可能。
 RTX1200 は Rev.10.01.32 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

19.7 L2TPv3 の常時接続の設定

[書式]

```
l2tp always-on sw
no l2tp always-on [sw]
```

[設定値及び初期値]

- *sw*
 - [設定値]:

設定値	説明
on	常時接続する
off	常時接続しない

- [初期値]: on

[説明]

L2TPv3 の接続を常時接続するか否かを設定する。
 トンネルインタフェースにのみ設定可能です。

[ノート]

RTX5000 は Rev.14.00.12 以降で使用可能。
 RTX3500 は Rev.14.00.12 以降で使用可能。
 RTX810 は Rev.11.01.21 以降で使用可能。
 RTX1200 は Rev.10.01.53 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

19.8 L2TP トンネルのホスト名の設定

[書式]

```
l2tp hostname hostname
no l2tp hostname [name]
```

[設定値及び初期値]

- *name*
 - [設定値]: ホスト名 (32 文字以内)
 - [初期値]: 機種名

[説明]

接続相手に通知するホスト名を設定する。
 show status l2tp コマンドで出力される L2TP トンネル情報に表示される。
 本コマンドを設定しない場合には機種名がホスト名として使用される。
 トンネルインターフェースのみ設定可能です。

[ノート]

RTX5000 は Rev.14.00.12 以降で使用可能。
 RTX3500 は Rev.14.00.12 以降で使用可能。
 RTX810 は Rev.11.01.21 以降で使用可能。
 RTX1200 は Rev.10.01.53 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

19.9 L2TPv3 の Local Router ID の設定

[書式]

```
l2tp local router-id ipv4_address  

no l2tp local router-id [ipv4_address]
```

[設定値及び初期値]

- *ipv4_address*
 - [設定値]: IPv4 アドレス
 - [初期値]: 0.0.0.0

[説明]

L2TPv3 の接続相手に通知する Router ID を設定する。
 接続相手の Remote Router ID と同じ IPv4 アドレスを設定します。
 ルーターに設定されている IPv4 アドレスを使用する必要はない。
 トンネルインターフェースにのみ設定可能です。

[ノート]

RTX5000 は Rev.14.00.12 以降で使用可能。
 RTX3500 は Rev.14.00.12 以降で使用可能。
 RTX810 は Rev.11.01.21 以降で使用可能。
 RTX1200 は Rev.10.01.53 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

19.10 L2TPv3 の Remote Router ID の設定

[書式]

```
l2tp remote router-id ipv4_address  

no l2tp remote router-id [ipv4_address]
```

[設定値及び初期値]

- *ipv4_address*
 - [設定値]: IPv4 アドレス
 - [初期値]: 0.0.0.0

[説明]

L2TPv3 の接続相手の Router ID を設定する。
 接続相手の Local Router ID と同じ IPv4 アドレスを設定する。

ルーターに設定されている IPv4 アドレスを使用する必要はない。
トンネルインターフェースにのみ設定可能です。

[ノート]

RTX5000 は Rev.14.00.12 以降で使用可能。
RTX3500 は Rev.14.00.12 以降で使用可能。
RTX810 は Rev.11.01.21 以降で使用可能。
RTX1200 は Rev.10.01.53 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

19.11 L2TPv3 の Remote End ID の設定

[書式]

l2tp remote end-id *end-id*

no l2tp remote end-id [*end-id*]

[設定値及び初期値]

- *end-id*
 - [設定値]: 任意文字列(32 文字以内)
 - [初期値]: なし

[説明]

L2TPv3 の Remote End ID を設定する。
接続相手の Remote End ID と同じ文字列を設定する。
トンネルインターフェースにのみ設定可能です。

[ノート]

RTX5000 は Rev.14.00.12 以降で使用可能。
RTX3500 は Rev.14.00.12 以降で使用可能。
RTX810 は Rev.11.01.21 以降で使用可能。
RTX1200 は Rev.10.01.53 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

第 20 章

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`、`tunnel endpoint name`、`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 ptp service [service]
```

[設定値及び初期値]

- `service`
- [設定値]:

設定値	説明
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

- [初期値]: off

[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]

off に設定すると 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。

[適用モデル]

RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810

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 interface [interface ...]
no pp bind [interface]
```

[設定値及び初期値]

- `interface`
- [設定値]:

設定値	説明
tunnelN	TUNNEL インターフェース名 (N はインターフェース番号 (<code>tunnel_num</code>))
tunnelN-tunnelM	TUNNEL インターフェースの範囲 (N、M はインターフェース番号 (<code>tunnel_num</code>))

- [初期値]: -

[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。
`anonymous` インタフェースに対してのみ、複数のトンネルインタフェースが指定できる。
 また、連続している複数のトンネルインタフェースの場合は、インタフェース範囲指定が可能である。

[ノート]

PPTP または L2TP/IPsec は PP 毎に設定する。

tunnel encapsulation コマンドで **pptp** または **l2tp** 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 または L2TP/IPsec で通信することを可能にする。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, 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]
```

[設定値及び初期値]

- *type*

- [設定値]:

設定値	説明
server	サーバーとして動作
client	クライアントとして動作

- [初期値]: server

[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。

[適用モデル]

RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810

20.1.4 PPTP ホスト名の設定

[書式]

```
pptp hostname name
```

```
no pptp hostname [name]
```

[設定値及び初期値]

- *name*

- [設定値]: ホスト名 (64 バイト以下)

- [初期値]:

- なし (RTX1200 Rev.10.01.76 以降、RTX810 Rev.11.01.33 以降、RTX1210 Rev.14.01.26 以降、RTX830 Rev.15.02.03 以降、RTX1220)
- 機種名(上記以外)

[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。
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。

[適用モデル]

RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810

20.1.5 PPTP ホスト名の設定

[書式]

```
pptp vendorname name
no pptp vendorname [name]
```

[設定値及び初期値]

- *name*
 - [設定値]: ベンダー名 (最大 64 文字/半角、32 文字/全角)
 - [初期値]: -

[説明]

PPTP ベンダー名を設定する。

[ノート]

本コマンドで設定した値が Start-Control-Connection-Request と Start-Control-Connection-Reply のベンダー名にセットされる。
本コマンドが設定されていないときはベンダー名に空文字がセットされる。

RTX1200 Rev.10.01.76 以降、RTX810 Rev.11.01.33 以降、RTX1210 Rev.14.01.26 以降、RTX830 Rev.15.02.03 以降、RTX1220 のファームウェアで使用可能。
それ以外のファームウェアではベンダー名に"YAMAHA Corporation"がセットされる。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

20.1.6 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]
```

[設定値及び初期値]

- *size*
 - [設定値]: パケットサイズ (1..128)
 - [初期値]: 32

[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。

[適用モデル]

RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810

20.1.7 PPTP の動作モードの設定

[書式]

```
pptp call-id mode mode
no pptp call-id mode [mode]
```

[設定値及び初期値]

- *mode*
 - [設定値]:

設定値	説明
normal	通常モード
backward-compatibility	Rev.4.06.16 互換モード

- [初期値] : normal

[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。

[適用モデル]

RTX1500, RTX1100

20.1.8 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*]

[設定値及び初期値]

- *auth*
- [設定値] :

設定値	説明
pap	PAP
chap	CHAP
mschap	MSCHAP
mschap-v2	MSCHAP-Version2
chap-pap	CHAP と PAP 両方

- [初期値] : -

[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。

[適用モデル]

RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810

20.1.9 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*]

[設定値及び初期値]

- *auth*
- [設定値] :

設定値	説明
pap	PAP
chap	CHAP
mschap	MSCHAP
mschap-v2	MSCHAP-Version2

- [初期値] : -

[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 および Windows Vista、Windows 7 をクライアントとして使用する場合は mschap-v2 を用いる。

[適用モデル]

RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810

20.1.10 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]
```

[設定値及び初期値]

- *syslog*
- [設定値]:

設定値	説明
on	出力する
off	出力しない

- [初期値]: off

[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。

[適用モデル]

RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810

20.2 リモートアクセス VPN 機能**20.2.1 PPTP トンネルの出力切断タイマの設定****[書式]**

```
pptp tunnel disconnect time time
no pptp tunnel disconnect time [time]
```

[設定値及び初期値]

- *time*
- [設定値]:

設定値	説明
1..21474836	秒数
off	タイマを設定しない

- [初期値]: 60

[説明]

選択されている PPTP トンネルに対して、データパケット無送信の場合、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。

[適用モデル]

RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810

20.2.2 PPTP キープアライブの設定

[書式]

```
pptp keepalive use use
no pptp keepalive use [use]
```

[設定値及び初期値]

- *use*
- [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: on

[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。

[適用モデル]

RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810

20.2.3 PPTP キープアライブのログ設定

[書式]

```
pptp keepalive log log
no pptp keepalive log [log]
```

[設定値及び初期値]

- *log*
- [設定値]:

設定値	説明
on	ログにとる
off	ログにとらない

- [初期値]: off

[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。

[適用モデル]

RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810

20.2.4 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]
```

[設定値及び初期値]

- *interval*
 - [設定値]: インターバル (1..65535)
 - [初期値]: 30
- *count*
 - [設定値]: カウント (3..100)
 - [初期値]: 6

[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。

[適用モデル]

RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810

20.2.5 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]
```

[設定値及び初期値]

- *mode*

- [設定値]:

設定値	説明
reject	暗号化なしでは接続拒否
accept	暗号化なしでも接続許可

- [初期値]: accept

[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。

[適用モデル]

RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810

第 21 章

IPIP トンネリング機能の設定

IPIP トンネリング機能

IPIP トンネリング (IP over IP) は、IP パケットにさらに IP ヘッダを付加してカプセル化することでネットワーク間での VPN (Virtual Private Network) 接続を実現するトンネリングプロトコルです。IPIP トンネリングには認証や暗号化の仕組みは無いため、閉域網サービスなど安全な通信が提供されている環境で利用します。

ヤマハルーターでは独自仕様の IPIP キープアライブを使用することができます。IPIP キープアライブを使用すると、以下のようなメリットがあります。

- 対向ルーターの応答を確認してからトンネルを確立することで、確実に対向ルーターにパケットを送信することができます。
- トンネル端点をホスト名で指定している場合に、ホスト名に対応する IP アドレスが変わっても、切断検知後に再度名前解決を行うことで自動的に復旧することができます。

21.1 IPIP キープアライブの設定

[書式]

```
ipip keepalive use switch [interval [count]]
no ipip keepalive use [switch ...]
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	IPIP キープアライブを使用する
off	IPIP キープアライブを使用しない

- [初期値]: off
- *interval*
 - [設定値]: キープアライブパケットを送出する時間間隔[秒] (1..600)
 - [初期値]: 10
- *count*
 - [設定値]: ダウンと見なすまでのキープアライブパケット送信回数 (1..50)
 - [初期値]: 6

[説明]

IPIP キープアライブを使用するか否かを選択する。

キープアライブを行う場合は *interval* と *count* の設定値に応じて独自仕様の IPIP キープアライブが動作する。トンネルインタフェースにのみ設定可能。

キープアライブ有効時に、*count* 回連続してキープアライブの応答が確認できなければ接続性がないと見なしてトンネルをダウンする。

また、トンネル端点を名前指定している場合は、*count* 回キープアライブを送信しても応答がない場合、再度名前解決を実行する。

[ノート]

RTX5000 / RTX3500 は Rev.14.00.22 以降で使用可能。

RTX1210 は Rev.14.01.20 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

21.2 IPIP キープアライブのログ設定

[書式]

ipip keepalive log *log*

no ipip keepalive log [*log*]

[設定値及び初期値]

- *log*

- [設定値]:

設定値	説明
on	IPIP キープアライブをログに出力する
off	IPIP キープアライブをログに出力しない

- [初期値]: off

[説明]

IPIP キープアライブのログを出力するか否かを設定する。
ログはすべて、`debug` レベルの `SYSLOG` に出力される。
トンネルインタフェースにのみ設定可能。

[ノート]

RTX5000 / RTX3500 は Rev.14.00.22 以降で使用可能。
RTX1210 は Rev.14.01.20 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

第 22 章

クラウドサービスとの VPN 接続設定機能の設定

クラウドサービスと VPN 接続するためのヤマハルーターの設定を、かんたんに行うための機能です。本機能を利用することで、インターネットのゲートウェイにしているヤマハルーターと、クラウドサービスの仮想ネットワークとをかんたんに VPN 接続することができます。

本機能を使用するためには、事前にクラウドサービス側の設定をしておく必要があります。

接続するクラウドサービスとして選べるサービスは以下の URL を参照してください。

- http://www.rtpro.yamaha.co.jp/RT/docs/cloud_vpn/

22.1 VPN 接続するクラウドサービスの指定

[書式]

```
cloud vpn service id service_name
no cloud vpn service id [service_name]
```

[設定値及び初期値]

- *id*
 - [設定値]: クラウド設定番号 (1..3)
 - [初期値]: -
- *service_name*
 - [設定値]:

設定値	説明
amazon-api	API を用いた Amazon VPC との接続設定

- [初期値]: -

[説明]

VPN 接続するクラウドサービスを指定する。

[ノート]

RTX1210 は Rev.14.01.20 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830

22.2 クラウドサービスとの VPN 接続設定に必要なパラメーターの設定

[書式]

```
cloud vpn parameter id parameter [parameter [parameter]]
no cloud vpn parameter id [parameter ...]
```

[設定値及び初期値]

- *id*
 - [設定値]: クラウド設定番号 (1..3)
 - [初期値]: -
- *parameter*
 - [設定値]: パラメーター (半角 256 文字以内)
 - [初期値]: -

[説明]

クラウドサービスとの VPN 接続設定に必要なパラメーターを設定する。

Amazon VPC との VPN 接続を行う場合、次の順番で *parameter* に指定する。これらの情報は、事前に AWS の管理画面で設定しておく必要がある。

1. アクセスキー ID
2. シークレットアクセスキー
3. VPN ID

[ノート]

RTX1210 は Rev.14.01.20 以降で使用可能。

[設定例]

Amazon VPC との VPN 接続を行う場合

```
cloud vpn parameter 1 abcdefghij ABCDEFGHIJKLM vpn-01234567
```

[適用モデル]

RTX1220, RTX1210, RTX830

22.3 クラウドサービスとの VPN 接続設定の名称の設定

[書式]

```
cloud vpn name id name
```

```
no cloud vpn name id [name]
```

[設定値及び初期値]

- *id*
 - [設定値]: クラウド設定番号 (1..3)
 - [初期値]: -
- *name*
 - [設定値]: クラウド設定の名称 (半角 32 文字以内)
 - [初期値]: -

[説明]

クラウドサービスとの VPN 接続設定の名称を設定する。

name に指定した名称は、設定を取得したときに自動的に設定される **tunnel description** コマンドの文字列に反映される。

[ノート]

RTX1210 は Rev.14.01.20 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830

22.4 クラウドサービスとの VPN 接続を設定するトンネルインターフェースの指定

[書式]

```
cloud vpn bind id tunnel_if1 [tunnel_if2]
```

```
no cloud vpn bind id [tunnel_if1 ...]
```

[設定値及び初期値]

- *id*
 - [設定値]: クラウド設定番号 (1..3)
 - [初期値]: -
- *tunnel_if1, tunnel_if2*
 - [設定値]: トンネルインターフェース番号
 - [初期値]: -

[説明]

クラウドサービスとの VPN 接続を設定するトンネルインターフェースを指定する。

本コマンドを事前に設定した場合、指定したトンネルインターフェースにクラウドサービスとの VPN 接続を設定する。

Amazon VPC との VPN 接続設定を行う場合、トンネルインターフェースを 2 つ指定する必要がある。

本コマンドを設定していない状態で、クラウドサービスから設定値を取得した場合、使用していないトンネルインターフェースを検索して自動的に設定する。

[ノート]

RTX1210 は Rev.14.01.20 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830

22.5 クラウドサービスとの VPN 接続設定に使用するオプションの設定

[書式]

```
cloud vpn option id option=value
```

```
no cloud vpn option id [option=value]
```

[設定値及び初期値]

- *id*
 - [設定値]: クラウド設定番号 (1..3)
 - [初期値]: -
- *option=value*
 - [設定値]:

<i>option</i>	<i>value</i>	説明
region	リージョン	Amazon VPC のインスタンスを生成したリージョン (半角 32 文字以内)

- [初期値]:
 - region=ap-northeast-1

[説明]

クラウドサービスとの VPN 接続設定に使用するオプションを設定する。

region には、Amazon VPC のインスタンスを生成したリージョンを設定する。初期値は *ap-northeast-1* で、アジアパシフィック (東京) のリージョンである。Amazon VPC のリージョン名、およびリージョンについては以下の URL を参照のこと。

- http://www.rtpro.yamaha.co.jp/RT/docs/cloud_vpn/amazon-vpc_api.html

[ノート]

RTX1210 は Rev.14.01.20 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830

22.6 クラウドサービスとの VPN 接続設定の手動実行

[書式]

```
cloud vpn set go id [option]
```

[設定値及び初期値]

- *id*
 - [設定値]: クラウド設定番号 (1..3)
 - [初期値]: -
- *option*
 - [設定値]:

設定値	説明
save	生成した CONFIG を保存する
no-save	生成した CONFIG を保存しない

- [初期値]: -

[説明]

クラウドサービスとの VPN 接続設定を実行する。
 クラウドサービスから取得した設定値を基に、クラウドサービスとの VPN 接続を行うための CONFIG を生成し、VPN 接続する。
option を省略した場合、クラウドサービスとの VPN 接続設定が完了すると、設定を保存するか否か (Y/N) の問い合わせを表示する。Y を入力すると設定を保存し、N を入力すると設定を保存しない。
 Web GUI でのコマンド実行やスケジュール実行、Lua スクリプトなど、対話型の入力ができない場合、*option* は必ず指定する必要がある。

[ノート]

本コマンドを実行して手動で設定値を取得する場合、リトライは行わない。
 RTX1210 は Rev.14.01.20 以降で使用可能。

[設定例]

```
# cloud vpn set go 1
.....
クラウドサービスとの VPN 接続設定が完了しました。
設定を保存しますか？ (Y/N)
```

[適用モデル]

RTX1220, RTX1210, RTX830

22.7 クラウドサービスとの VPN 接続設定の状態の表示

[書式]

show status cloud vpn [id]

[設定値及び初期値]

- *id*
 - [設定値]: クラウド設定番号 (1..3)
 - [初期値]: -

[説明]

クラウドサービスとの VPN 接続設定の状態を表示する。

- 設定名
- ステータス (設定取得状況)
- CONFIG の更新日時
- 設定情報の最終取得日時
- トンネルの接続状態

ID を省略すると、設定されているすべてのクラウドサービスとの VPN 接続設定の状態を表示する。

[ノート]

RTX1210 は Rev.14.01.20 以降で使用可能。

[表示例]

```
# show status cloud vpn 1
クラウド設定 [1]
サービス名: Amazon (API 方式)
設定名: yamaha # cloud vpn name コマンドの設定値
ステータス: 設定済み
```

```

最終取得日時:          2017/01/25 10:11:22
CONFIG の更新日時:     2017/01/24 12:00:00
TUNNEL の接続状態:
  TUNNEL[01]: 接続されています
  TUNNEL[02]: 接続されています

```

[適用モデル]

RTX1220, RTX1210, RTX830

22.8 クラウドサービス接続時の詳細情報を SYSLOG に表示**[書式]****cloud vpn syslog *sw*****no cloud vpn syslog [*sw*]****[設定値及び初期値]**

- *sw*

- [設定値]:

設定値	説明
on	クラウドサービス接続時の詳細情報を SYSLOG に表示する
off	クラウドサービス接続時の詳細情報を SYSLOG に表示しない

- [初期値]: off

[説明]

クラウドサービス接続時の詳細情報を SYSLOG に表示する。

[ノート]

RTX1210 は Rev.14.01.34 以降で使用可能。

RTX830 は Rev.15.02.10 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830

第 23 章

SIP 機能の設定

23.1 共通の設定

23.1.1 SIP を使用するか否かの設定

[書式]

`sip use use`

`no sip use`

[設定値及び初期値]

- `use`

- [設定値]:

設定値	説明
off	使用しない
on	使用する

- [初期値]: off

[説明]

SIP プロトコルを使用するか否かを設定する。

[ノート]

on から off への設定の変更は再起動後有効となる。

RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

23.1.2 SIP の session-timer 機能のタイマ値の設定

[書式]

`sip session timer time [update=update] [refresher=refresher]`

`no sip session timer`

[設定値及び初期値]

- `time`

- [設定値]:

設定値	説明
秒数 (60..540)	
0	session-timer 機能を利用しない

- [初期値]: 0

- `update`

- [設定値]:

設定値	説明
on	UPDATE メソッドを使用する
off	UPDATE メソッドを使用しない

- [初期値]: off

- `refresher`

- [設定値]:

設定値	説明
none	refresher パラメータを設定しない
uac	refresher パラメータに uac を設定する
uas	refresher パラメータに uas を設定する

- [初期値]: uac

[説明]

SIP の session-timer 機能のタイマ値を設定する。

SIP の通話中に相手が停電などにより突然落ちた場合にタイマにより自動的に通話を切断する。

update を on に設定すれば、発信時に session-timer 機能において UPDATE メソッドを使用可能とする。

refresher を none に設定した時は refresher パラメータを設定せず、uac/uas を設定した時はそれぞれのパラメータ値で発信する。

[ノート]

RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX830, RTX810

23.1.3 SIP による発信時に使用する IP プロトコルの選択

[書式]

sip ip protocol *protocol*

no sip ip protocol

[設定値及び初期値]

- *protocol*

- [設定値]:

設定値	説明
udp	UDP を使用
tcp	TCP を使用

- [初期値]: udp

[説明]

SIP による発信時の呼制御に使用する IP プロトコルを選択する。

[ノート]

着信した場合は、この設定に関わらず、受信したプロトコルで送信を行なう。

RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX830, RTX810

23.1.4 SIP による発信時に 100rel をサポートするか否かの設定

[書式]

sip 100rel *switch*

no sip 100rel

[設定値及び初期値]

- *switch*

- [設定値]:

設定値	説明
on	100rel をサポートする

設定値	説明
off	100rel をサポートしない

- [初期値] : off

[説明]

SIP の発信時に 100rel(RFC3262) をサポートするか否かを設定する。

[ノート]

RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX830, RTX810

23.1.5 送信する SIP パケットに User-Agent ヘッダを付加する設定

[書式]

sip user agent sw [*user-agent*]

no sip user agent

[設定値及び初期値]

- *sw*
- [設定値] :

設定値	説明
on	付加する
off	付加しない

- [初期値] : off
- *user-agent*
- [設定値] : ヘッダに記述する文字列
- [初期値] : -

[説明]

送信する SIP パケットに User-Agent ヘッダを付加することができる。

付加する文字列は、*user-agent* パラメータにて設定することが可能であるが、64 文字以内で ASCII 文字のみ設定可能である。

[ノート]

RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

23.1.6 SIP による着信時の INVITE に refresher 指定がない場合の設定

[書式]

sip arrive session timer refresher *refresher*

no sip arrive session timer refresher

[設定値及び初期値]

- *refresher*
- [設定値] :

設定値	説明
uac	refresher=uac と指定する
uas	refresher=uas と指定する

- [初期値] : uac

[説明]

SIP による着信時の INVITE が refresher を指定していない場合に UAC/UAS を指定できる。

[ノート]

RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

23.1.7 SIP による着信時に P-N-UAType ヘッダをサポートするか否かの設定

[書式]

sip arrive ringing p-n-uatype switch

no sip arrive ringing p-n-uatype

[設定値及び初期値]

- *switch*

- [設定値]:

設定値	説明
on	P-N-UAType ヘッダを付加する
off	P-N-UAType ヘッダを付加しない

- [初期値]: off

[説明]

SIP による着信時に送信する Ringing レスポンスに、P-N-UAType ヘッダを付加するか否かを設定する。

[ノート]

設定はすべての着信に適用される。

RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX830, RTX810

23.1.8 SIP による着信時のセッションタイマーのリクエストを設定

[書式]

sip arrive session timer method *method*

no sip arrive session timer method [*method*]

[設定値及び初期値]

- *method*

- [設定値]:

設定値	説明
auto	自動的に判断する
invite	INVITE のみを使用する

- [初期値]: auto

[説明]

SIP による着信時にセッションタイマー機能で使用するリクエストを設定する。

auto に設定した場合には UPDATE, INVITE とともに使用でき、発信側またはサーバで UPDATE に対応していれば UPDATE を使用する。

invite に設定した場合には、発信側またはサーバで UPDATE に対応していてもこれを使用せずに動作する。

UPDATE のみを使用する設定はできない。

また、サーバ毎に設定することできないため、全ての着信でこの設定が有効となる。

発信の場合は、**sip server session timer** または **sip session timer** の *update* オプションで設定できる。

[ノート]

RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

23.1.9 SIP 着信時にユーザー名を検証するか否かの設定

[書式]

sip arrive address check *switch*

no sip arrive address check

[設定値及び初期値]

- *switch*

- [設定値]:

設定値	説明
on	ユーザ名を検証する
off	ユーザ名を検証しない

- [初期値]: on

[説明]

SIP サーバーの設定をした場合に、着信時の Request-URI が送信した REGISTER の Contact ヘッダの内容と一致するかを検証するか否かを設定する。

SIP を利用した VoIP 機能において、SIP サーバーを利用する設定と Peer to Peer で利用する設定を併用する場合は off にする。

また、SIP サーバーに RTV01 を利用する場合にも off にする。

[ノート]

この検証は **sip server** 設定がある場合に有効となる。

RTX3000 は Rev.9.00.50 以降で使用可能。

RTX1200 は Rev.10.01.32 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

23.1.10 着信可能なポートがない場合に返す SIP のレスポンスコードの設定

[書式]

sip response code busy *code*

no sip response code busy

[設定値及び初期値]

- *code*: レスポンスコード

- [設定値]:

設定値	説明
486	486 を返す
503	503 を返す

- [初期値]: 486

[説明]

SIP 着信時に、ビジーで着信できない場合に返すレスポンスコードを設定する。

[ノート]

RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

23.1.11 SIP で使用する IP アドレスの設定

[書式]**sip outer address *ipaddress*****no sip outer address****[設定値及び初期値]**

- *ipaddress*

- [設定値]:

設定値	説明
auto	自動設定
IP アドレス	IP アドレス

- [初期値]: auto

[説明]

SIP で使用する IP アドレスを設定する。RTP/RTCP もこの値が使用される。

[ノート]

初期設定のまま使用する事を推奨する。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830, RTX810

23.1.12 SIP メッセージのログを記録するか否かの設定

[書式]**sip log *switch*****no sip log****[設定値及び初期値]**

- *switch*

- [設定値]:

設定値	説明
on	SIP メッセージのログを記録する
off	SIP メッセージのログを記録しない

- [初期値]: off

[説明]

SIP メッセージのログを DEBUG レベルのログに記録するか否かを設定する。

[ノート]

RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

23.2 SIP サーバー毎の設定

23.2.1 SIP サーバーの設定

[書式]**sip server number *address type protocol sip_uri* [*username* [*password*]]****no sip server number**

[設定値及び初期値]

- *number*
 - [設定値]: SIP サーバーの登録番号 (1..65535)
 - [初期値]: -
- *address*
 - [設定値]: SIP サーバーの IP アドレス
 - [初期値]: -
- *type*
 - [設定値]:
 - register
 - no-register
 - [初期値]: -
- *protocol*
 - [設定値]:

設定値	説明
tcp	TCP プロトコル
udp	UDP プロトコル

- [初期値]: -
- *sip_url*
 - [設定値]: SIP アドレス
 - [初期値]: -
- *username*
 - [設定値]: ユーザ名
 - [初期値]: -
- *password*
 - [設定値]: パスワード
 - [初期値]: -

[説明]

SIP サーバー設定を追加または削除する。

[ノート]

RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000

23.2.2 SIP サーバー毎の session-timer 機能のタイマ値の設定**[書式]**

```
sip server session timer number time [update=update] [refresher=refresher]
```

```
no sip server session timer number
```

[設定値及び初期値]

- *number*
 - [設定値]: SIP サーバーの登録番号 (1..65535)
 - [初期値]: -
- *time*
 - [設定値]:
 - 秒数(60..540)
 - 0 ... session-timer 機能を利用しない
 - [初期値]: -
- *update*
 - [設定値]:

設定値	説明
on	UPDATE メソッドを使用する
off	UPDATE メソッドを使用しない

- [初期値]: -
- *refresher*
- [設定値]:

設定値	説明
none	refresher パラメータを設定しない
uac	refresher パラメータに uac を設定する
uas	refresher パラメータに uas を設定する

- [初期値]: -

[説明]

SIP サーバー毎の *session-timer* 機能のタイマ値を設定する。

SIP の通話中に相手が停電などにより突然落ちた場合にタイマにより自動的に通話を切断する。

サーバーが *session-timer* に対応していれば、端末が 2 台同時に突然落ちてもサーバーでの呼の持ち切りを防ぐことができる。

update を on に設定すれば、発信時に *session-timer* 機能において UPDATE メソッドを使用可能とする。

refresher を none に設定した時は *refresher* パラメータを設定せず、*uac/uas* を設定した時はそれぞれのパラメータ値で発信する。

[ノート]

RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000

23.2.3 SIP サーバー毎の代表 SIP アドレスの設定

[書式]

sip server pilot address number sipaddress

no sip server pilot address number

[設定値及び初期値]

- *number*
 - [設定値]: SIP サーバーの登録番号 (1..65535)
 - [初期値]: -
- *sipaddress*
 - [設定値]: 代表 SIP アドレス
 - [初期値]: -

[説明]

SIP サーバー経由の発信時に、INVITE リクエストの P-Preferred-Identity ヘッダに設定した代表 SIP アドレスを入れて発信する。

[ノート]

RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000

23.2.4 SIP サーバー毎の先頭に付加された 184/186 の扱いの設定

[書式]

sip server privacy number switch [pattern]
no sip server privacy number switch [pattern]

[設定値及び初期値]

- *number*
 - [設定値]: SIP サーバーの登録番号 (1..65535)
 - [初期値]: -
- *switch*
 - [設定値]:

設定値	説明
off	ダイヤルされたそのままの番号で発信する
always-off	ダイヤルされた番号から 184 / 186 を取り除き、常に「通知」で発信する
always-on	ダイヤルされた番号から 184 / 186 を取り除き、常に「非通知」で発信する
default-off	ダイヤルされた番号から 184 / 186 を取り除き、184 が付加されている場合には「非通知」で、それ以外の場合には「通知」で発信する。
default-on	ダイヤルされた番号から 184 / 186 を取り除き、186 が付加されている場合には「通知」で、それ以外の場合には「非通知」で発信する。

- [初期値]: off
- *pattern*
 - [設定値]:

設定値	説明
sip-privacy	draft-ietf-sip-privacy-01 に従って発信者番号の通知 / 非通知を行なう。
rfc3325	RFC3325 に従って発信者番号の通知 / 非通知を行なう。
as-is	ダイヤルされた番号に 184 / 186 を付加して発信する。

- [初期値]: -

[説明]

ダイヤルされた番号の先頭に付加された 184 / 186 をどのように取り扱うかを指定する。各 *pattern* パラメータで指定した方式に従って、ダイヤルされた番号を処理する。*pattern* パラメータを省略した場合は、draft-ietf-sip-privacy-01 に従って、ダイヤルされた番号を処理する。

[ノート]

RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000

23.2.5 SIP サーバー毎の発信時に使用する自己 SIP ディスプレイ名の設定

[書式]

sip server display name *number displayname*
no sip server display name *number*

[設定値及び初期値]

- *number*
 - [設定値]: SIP サーバーの登録番号 (1..65535)
 - [初期値]: -
- *displayname*
 - [設定値]: ディスプレイ名
 - [初期値]: -

[説明]

SIP サーバー毎の発信時に使用される自己 SIP ディスプレイ名を設定する。

[ノート]

空白を含むディスプレイ名を設定する場合、" " で囲む必要がある。
漢字を設定する場合は、シフト JIS コードで設定を行なう。
RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000

23.2.6 SIP サーバー毎の発信時の相手 SIP アドレスのドメイン名の設定

[書式]

```
sip server call remote domain number domain
no sip server call remote domain number
```

[設定値及び初期値]

- *number*
 - [設定値]: SIP サーバーの登録番号 (1..65535)
 - [初期値]: -
- *domain*
 - [設定値]: ドメイン名
 - [初期値]: -

[説明]

SIP サーバー経由の発信時に、相手の SIP アドレスの **host** 部分を設定したドメイン名にして発信する。
ドメイン名の長さは 58 文字まで設定できる。
なお、ドメイン名として使用可能な文字は、アルファベット、数字、ハイフン、ピリオド、コロン、カッコ [] のみである。
ドメイン名を設定しない場合には、**sip server** コマンドの SIP-URI の **host** 部分と同じドメイン名にして発信する。

[ノート]

RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000

23.2.7 SIP サーバー毎の発信時に 100rel をサポートするか否かの設定

[書式]

```
sip server 100rel number switch
no sip server 100rel number
```

[設定値及び初期値]

- *number*
 - [設定値]: SIP サーバーの登録番号 (1..65535)
 - [初期値]: -
- *switch*
 - [設定値]:

設定値	説明
on	100rel をサポートする
off	100rel をサポートしない

- [初期値]: off

[説明]

SIP サーバー経由の発信時に 100rel(RFC3262) をサポートするか否かを設定する。

[ノート]

RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000

23.2.8 SIP サーバー毎の REGISTER リクエストの更新間隔の設定

[書式]

```
sip server register timer server=number OK_time NG_time
```

```
no sip server register timer server=number
```

[設定値及び初期値]

- *number*
 - [設定値]: SIP サーバーの登録番号 (1..65535)
 - [初期値]: -
- *OK_time*
 - [設定値]: 通常時更新間隔 (10..120 (分))
 - [初期値]: 30
- *NG_time*
 - [設定値]: 異常時更新間隔 (1..60 (分))
 - [初期値]: 5

[説明]

SIP サーバーに REGISTER リクエストを送信する間隔を設定する。

正常に更新されている場合には通常時更新間隔毎に更新する。サーバーからエラーが返されたり、サーバーから応答が無い場合には、異常時更新間隔毎に更新する。また、この時の Expires ヘッダは通常時更新間隔を 2 倍して秒に直した値で送信する。しかし、サーバーから Expires の指定があった場合はその値に従って、指定された値の半分の時間で通常時の更新を行なう。

[ノート]

RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000

23.2.9 SIP サーバー毎の REGISTER リクエストの Request-URI の設定

[書式]

```
sip server register request-uri number sip_address
```

```
no sip server register request-uri number
```

[設定値及び初期値]

- *number*
 - [設定値]: SIP サーバーの登録番号 (1..65535)
 - [初期値]: -
- *sip_address*
 - [設定値]: Request-URI

- [初期値]: -

[説明]

SIP サーバーに送信する REGISTER リクエストの Request-URI を設定する。
設定しない場合は、**sip server** コマンドで設定した SIP-URI の host 部分を入れて REGISTER リクエストを送信する。

[ノート]

RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000

23.2.10 SIP サーバー毎の REGISTER リクエストの Contact ヘッダに付加する q 値の設定

[書式]

sip server qvalue number value

no sip server qvalue number

[設定値及び初期値]

- *number*
 - [設定値]: SIP サーバーの登録番号 (1..65535)
 - [初期値]: -
- *value*
 - [設定値]:

設定値	説明
q 値 (0.001..1.000)	
0	q 値を付加しない

- [初期値]: 0

[説明]

SIP サーバーへ接続する時に送信する REGISTER リクエストの Contact ヘッダに付加する q 値を設定する。0.001 単位で設定可能。

同じアカウントで同時に複数の端末から接続が許されている SIP サーバーを利用する時に、この設定により着信する優先順位を SIP サーバーに通知することが可能となる。数値が大きい方が優先される。

[ノート]

RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000

23.2.11 SIP サーバへの発信に番号以外を使えないように制限する設定

[書式]

sip server dial number-only server=number sw

no sip server dial number-only server=number

[設定値及び初期値]

- *number*
 - [設定値]: SIP サーバーの登録番号 (1..65535)
 - [初期値]: -
- *sw*
 - [設定値]:

設定値	説明
on	制限する
off	制限しない

- [初期値]: off

[説明]

SIP サーバ経由での VoIP 発信時に * など番号以外をダイヤルして発信しようとした場合に番号が正しくないとして発信しないように制限する。

[ノート]

RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]
RTX3000

23.2.12 自分自身の SIP アドレスへの発信を許可するかどうかの設定

[書式]

```

sip server call own permit server=number sw
no sip server call own permit server=number

```

[設定値及び初期値]

- *number*
 - [設定値]: SIP サーバーの登録番号 (1..65535)
 - [初期値]: -
- *sw*
 - [設定値]:

設定値	説明
on	許可する
off	許可しない

- [初期値]: off

[説明]

To, From が同じ SIP アドレスとなるような発信を許可するか否かを設定する。

この機能を利用して正常に発信ができるのは、Call-ID や tag 等の乱数値を発信側と着信側で別の値を付加して管理する SIP サーバーを利用する場合だけである。

そのため、通常は off で運用する。

[ノート]

RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]
RTX5000, RTX3500, RTX3000

23.3 NGN 機能の設定

データコネクタを利用して拠点間接続を行うにはトンネルインタフェースを利用します。トンネリングの章や IPsec の設定の章を参照してください。

23.3.1 NGN 網に接続するインタフェースの設定

[書式]

```

ngn type interface type
no ngn type interface [type]

```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース
 - [初期値]: -
- *type*
 - [設定値]:

設定値	説明
off	NGN 網のサービスを使用しない
ntt	NTT 東日本または NTT 西日本が提供する NGN 網を使用する

- [初期値]: off

[説明]

NGN 網に接続するインタフェースを設定する。

[ノート]

RTX1500、RTX1100、RT107e は Rev.8.03.92 以降で使用可能。

RTX3000 は Rev.9.00.50 以降で使用可能。

SRT100 は Rev.10.00.60 以降で使用可能。

RTX1200 は Rev.10.01.24 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

23.3.2 NGN 網を介したトンネルインタフェースの切断タイマの設定

[書式]

```
tunnel ngn disconnect time time
no tunnel ngn disconnect time [time]
```

[設定値及び初期値]

- *time*
 - [設定値]:

設定値	説明
1..21474836	秒数
off	タイマを設定しない

- [初期値]: 60

[説明]

NGN 網を介したトンネルインタフェース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。off に設定した場合は切断しない。

[ノート]

通信中の変更は無効。

RTX3000 は Rev.9.00.50 以降で使用可能。

RTX1200 は Rev.10.01.29 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

23.3.3 NGN 網を介したトンネルインタフェースの帯域幅の設定

[書式]

```
tunnel ngn bandwidth bandwidth [arrivepermit=switch]
no tunnel ngn bandwidth [bandwidth arrivepermit=switch]
```

[設定値及び初期値]• *bandwidth*

- [設定値]:

設定値	説明
64k	64kbps
512k	512kbps
1m	1Mbps
1k..1000m	帯域

- [初期値]: 1m

• *switch*

- [設定値]:

設定値	説明
on	帯域の設定と一致しない着信も許可する
off	帯域の設定と一致した着信のみ許可する

- [初期値]: on

[説明]

NGN 網を介したトンネルインタフェースの帯域幅を設定した値にする。

帯域の設定が一致しない着信について、arrivepermit オプションが off の場合は着信せず、on の場合は着信する。

[ノート]

通信中の変更は無効。

RTX3000 は Rev.9.00.50 以降で使用可能。

RTX1200 は Rev.10.01.29 以降で使用可能。

arrivepermit オプションは、RTX3000 Rev.9.00.56 以降、RTX1200 Rev.10.01.36 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで指定可能。

bandwidth は、RTX1200 Rev.10.01.71 以降、RTX810 Rev.11.01.28 以降、RTX5000 / RTX3500 Rev.14.00.21 以降、RTX1210 Rev.14.01.16 以降のファームウェア、および、Rev.15.02 系以降のすべてのファームウェアで任意の数値を設定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

23.3.4 NGN 網を介したトンネルインタフェースの着信許可の設定**[書式]**

tunnel ngn arrive permit *permit*

no tunnel ngn arrive permit [*permit*]

[設定値及び初期値]• *permit*

- [設定値]:

設定値	説明
on	許可する
off	許可しない

- [初期値]: on

[説明]

選択されている相手からの着信を許可するか否かを設定する。

[ノート]

tunnel ngn arrive permit、**tunnel ngn call permit** コマンドとも **off** を設定した場合は通信できない。
 RTX3000 は Rev.9.00.50 以降で使用可能。
 RTX1200 は Rev.10.01.29 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

23.3.5 NGN 網を介したトンネルインタフェースの発信許可の設定

[書式]

tunnel ngn call permit *permit*
no tunnel ngn call permit [*permit*]

[設定値及び初期値]

- *permit*
- [設定値]:

設定値	説明
on	許可する
off	許可しない

- [初期値]: on

[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]

tunnel ngn arrive permit、**tunnel ngn call permit** コマンドとも **off** を設定した場合は通信できない。
 RTX3000 は Rev.9.00.50 以降で使用可能。
 RTX1200 は Rev.10.01.29 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

23.3.6 NGN 網を介したトンネルインタフェースで使用する LAN インタフェースの設定

[書式]

tunnel ngn interface *lan*
no tunnel ngn interface [*lan*]

[設定値及び初期値]

- *lan*
- [設定値]:

設定値	説明
auto	自動設定
LAN インタフェース名	LAN ポート

- [初期値]: auto

[説明]

NGN 網を介したトンネルインタフェースで使用する LAN インタフェースを設定する。

auto に設定した時はトンネルインタフェースで設定した電話番号を利用して、使用する LAN インタフェースを決定する。

追加番号を使用する場合や HGW 配下で使用する場合に設定する。

[ノート]

通信中の変更は無効。

RTX3000 は Rev.9.00.50 以降で使用可能。

RTX1200 は Rev.10.01.32 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

23.3.7 NGN 網を介したトンネルインタフェースで接続に失敗した場合に接続を試みる相手番号の設定

[書式]

```
tunnel ngn fallback remote_tel ...
```

```
no tunnel ngn fallback [remote_tel ...]
```

[設定値及び初期値]

- *remote_tel*
 - [設定値]: 相手電話番号
 - [初期値]: -

[説明]

NGN 網を介したトンネルインタフェースで使用する相手番号は、**ipsec ike remote name** コマンドや **tunnel endpoint name** コマンドで設定した番号に対して発信するが、これが何らかの原因で接続できなかった場合に、設定された番号に対して発信する。

設定は最大 7 個まで可能で、接続に失敗すると設定された順番に次の番号を用いて接続を試みる。

[ノート]

RTX3000 は Rev.9.00.56 以降で使用可能。

RTX1200 は Rev.10.01.42 以降で使用可能。

RTX810 は Rev.11.01.06 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

23.3.8 NGN 電話番号を RADIUS で認証するか否かの設定

[書式]

```
tunnel ngn radius auth use
```

```
no tunnel ngn radius auth
```

[設定値及び初期値]

- *use*
 - [設定値]:

設定値	説明
on	認証する
off	認証しない

- [初期値]: off

[説明]

データコネクタを利用した拠点間接続において、着信を受けたときに発信元の NGN 電話番号を RADIUS で認証するか否かを設定する。

[ノート]

トンネルインタフェースが選択されている時のみ使用できる。

トンネルに相手の電話番号が設定されている場合は RADIUS 認証を行わない。

以下のコマンドが正しく設定されている必要がある。

- **radius account**
- **radius account server**
- **radius account port**
- **radius secret**
- **ngn radius auth password**

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

23.3.9 NGN 電話番号を RADIUS で認証するときに使用するパスワードの設定

[書式]

```
ngn radius auth password password
no ngn radius auth password
```

[設定値及び初期値]

- *password*
 - [設定値]: パスワード
 - [初期値]: -

[説明]

NGN 電話番号を RADIUS で認証するときに使用するパスワードを設定する。NGN 電話番号をユーザー名、当コマンドで設定した文字列をパスワードとして RADIUS サーバーに問い合わせを行う。

PASSWORD 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) で、文字列の長さは 0 文字以上 64 文字以下となる。

[ノート]

当コマンドが設定されていない場合は、NGN 電話番号を RADIUS で認証することができない。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

23.3.10 NGN 網への発信時に RADIUS アカウンティングを使用するか否かの設定

[書式]

```
ngn radius account caller use
no ngn radius account caller
```

[設定値及び初期値]

- *use*
 - [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: off

[説明]

NGN 網への発信時に RADIUS アカウンティングを使用するか否かを設定する。

[ノート]

RADIUS アカウンティングサーバーに関する以下のコマンドが正しく設定されている必要がある。

- **radius account**
- **radius account server**
- **radius account port**
- **radius secret**

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

23.3.11 NGN 網からの着信時に RADIUS アカウンティングを使用するか否かの設定

[書式]

ngn radius account callee use

no ngn radius account callee

[設定値及び初期値]

- *use*
- [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: off

[説明]

NGN 網からの着信時に RADIUS アカウンティングを使用するか否かを設定する。

[ノート]

RADIUS アカウンティングサーバーに関する以下のコマンドが正しく設定されている必要がある。

- **radius account**
- **radius account server**
- **radius account port**
- **radius secret**

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

23.3.12 NGN 網を介したリナンバリング発生時に LAN インターフェースを一時的にリンクダウンするか否かの設定

[書式]

ngn renumbering link-refresh switch

no ngn renumbering link-refresh [switch]

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
on	リナンバリング発生時、LAN インターフェースを一時的にリンクダウンする
off	リナンバリング発生時、取得したプレフィックスに変更がない場合は、LAN インターフェースをリンクダウンしない

- [初期値]: on

[説明]

NGN 網を介したリナンバリングが発生した時、LAN インターフェースを一時的にリンクダウンするか否かを設定する。

LAN インターフェースを一時的にリンクダウンさせることにより、DHCPv6-PD/RA プロキシの配下のより多くの端末に対して、IPv4/IPv6 アドレスの再取得を促し、リナンバリング後も通信を継続できるようにする。

このコマンドを on に設定した場合は、NGN 網を介したリナンバリングの発生時、取得したプレフィックスに変更がないときでも LAN インターフェースを一時的にリンクダウンする。off に設定した場合は、取得したプレフィックスに変更がないときはリンクダウンしない。

[ノート]

RTX1210 は Rev.14.01.16 以降で使用可能。
RTX5000、RTX3500 は Rev.14.00.21 以降で使用可能。
RTX1200 は Rev.10.01.71 以降で使用可能。
RTX810 は Rev.11.01.28 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

23.3.13 NGN 網接続情報の表示

[書式]

show status ngn

[説明]

NGN 網への接続状態を表示する。

[ノート]

RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

第 24 章

SNMP の設定

SNMP (Simple Network Management Protocol) 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ますようになります。このときヤマハルーターは SNMP エージェントとなります。

ヤマハルーターは SNMPv1、SNMPv2c、SNMPv3 による通信に対応しています。また 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 については以下の URL から参照することができます。

- YAMAHA private MIB: <http://www.rtpro.yamaha.co.jp/RT/docs/mib/>

SNMPv1 および SNMPv2c では、コミュニティと呼ばれるグループの名前を相手に通知し、同じコミュニティに属するホスト間でのみ通信します。このとき、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に対して別々にコミュニティ名を設定することができます。

このようにコミュニティ名はある種のパスワードとして機能しますが、その反面、コミュニティ名は必ず平文でネットワーク上を流れるという特性があり、セキュリティ面では脆弱と言えます。よりセキュアな通信が必要な場合は SNMPv3 の利用を推奨します。

SNMPv3 では通信内容の認証、および暗号化に対応しています。SNMPv3 はコミュニティの概念を廃し、新たに USM (User-based Security Model) と呼ばれるセキュリティモデルを利用することで、より高度なセキュリティを確保しています。

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。ヤマハルーターでは SNMP 標準トラップの他にも、一部機能で特定のイベントを通知するため独自のトラップを送信することがあります。なお、これらの独自トラップはプライベート MIB として定義されています。

トラップの送信先ホストについては、各 SNMP バージョン毎に複数のホストを設定することができます。

SNMPv1 および SNMPv2c で利用する読み出し専用と送信トラップ用のコミュニティ名は、共に初期値が "public" となっています。SNMP 管理ソフトウェア側も "public" がコミュニティ名である場合が多いため、当該バージョンの通信でセキュリティを考慮する場合は適切なコミュニティ名に変更してください。ただし、上述の通りコミュニティ名はネットワーク上を平文で流れますので、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決して使用しないよう注意してください。

工場出荷状態では、各 SNMP バージョンにおいてアクセスが一切できない状態となっています。また、トラップの送信先ホストは設定されておらず、どこにもトラップを送信しません。

24.1 SNMPv1 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]
```

[設定値及び初期値]

- *host*: SNMPv1 によるアクセスを許可するホスト

- [設定値]:

設定値	説明
<i>ip_address</i>	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)
<i>lanN</i>	LAN インターフェース名
<i>bridgeN</i>	ブリッジインターフェース名
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

- [初期値]: none
- *ro_community*
 - [設定値]: 読み出し専用のコミュニティ名 (16 文字以内)
 - [初期値]: -
- *rw_community*

- [設定値]: 読み書き可能なコミュニティ名 (16 文字以内)
- [初期値]: -

[説明]

SNMPv1 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 SNMPv1 によるアクセスを許可する。

IP アドレスや lanN、bridgeN でホストを指定した場合には、同時にコミュニティ名も設定できる。rw_community パラメータを省略した場合には、アクセスモードが読み書き可能であるアクセスが禁止される。ro_community パラメータも省略した場合には、snmp community read-only コマンド、および snmp community read-write コマンドの設定値が用いられる。

[ノート]

HOST パラメーターに IP アドレスの範囲や lanN、bridgeN を指定できるのは RTX1200 Rev.10.01.59 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.18 以降のファームウェア、および、Rev.14.01 系以降のファームウェアである。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

24.2 SNMPv1 の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
```

[設定値及び初期値]

- name
 - [設定値]: コミュニティ名 (16 文字以内)
 - [初期値]: public

[説明]

SNMPv1 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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

24.3 SNMPv1 の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
```

[設定値及び初期値]

- name
 - [設定値]: コミュニティ名 (16 文字以内)
 - [初期値]: -

[説明]

SNMPv1 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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

24.4 SNMPv1 トラップの送信先の設定

[書式]

```
snmp trap host host [community]
no snmp trap host host
```

[設定値及び初期値]

- *host*
 - [設定値]: SNMPv1 トラップの送信先ホストの IP アドレス (IPv4/IPv6)
 - [初期値]: -
- *community*
 - [設定値]: コミュニティ名 (16 文字以内)
 - [初期値]: -

[説明]

SNMPv1 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名にはこのコマンドの *community* パラメータが用いられるが、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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

24.5 SNMPv1 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
```

[設定値及び初期値]

- *name*
 - [設定値]: コミュニティ名 (16 文字以内)
 - [初期値]: public

[説明]

SNMPv1 トラップを送信する際のコミュニティ名を設定する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

24.6 SNMPv2c によるアクセスを許可するホストの設定

[書式]

```
snmpv2c host host [ro_community [rw_community]]
no snmpv2c host [host]
```

[設定値及び初期値]

- *host*: SNMPv2c によるアクセスを許可するホスト
 - [設定値]:

設定値	説明
<i>ip_address</i>	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)
<i>lanN</i>	LAN インターフェース名
<i>bridgeN</i>	ブリッジインターフェース名
<i>any</i>	すべてのホストからのアクセスを許可する
<i>none</i>	すべてのホストからのアクセスを禁止する

- [初期値]: none
- *ro_community*
 - [設定値]: 読み出し専用のコミュニティ名 (16 文字以内)
 - [初期値]: -
- *rw_community*
 - [設定値]: 読み書き可能なコミュニティ名 (16 文字以内)

- [初期値]:-

[説明]

SNMPv2c 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 SNMPv2c によるアクセスを許可する。

IP アドレスや `lanN`、`bridgeN` でホストを指定した場合には、同時にコミュニティ名も設定できる。`rw_community` パラメータを省略した場合には、アクセスモードが読み書き可能であるアクセスが禁止される。`ro_community` パラメータも省略した場合には、**snmpv2c community read-only** コマンド、および **snmpv2c community read-write** コマンドの設定値が用いられる。

[ノート]

HOST パラメーターに IP アドレスの範囲や `lanN`、`bridgeN` を指定できるのは RTX1200 Rev.10.01.59 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.18 以降のファームウェア、および、Rev.14.01 系以降のファームウェアである。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

24.7 SNMPv2c の読み出し専用のコミュニティ名の設定

[書式]

snmpv2c community read-only name

no snmpv2c community read-only

[設定値及び初期値]

- *name*
 - [設定値]: コミュニティ名 (16 文字以内)
 - [初期値]: public

[説明]

SNMPv2c 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。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

24.8 SNMPv2c の読み書き可能なコミュニティ名の設定

[書式]

snmpv2c community read-write name

no snmpv2c community read-write

[設定値及び初期値]

- *name*
 - [設定値]: コミュニティ名 (16 文字以内)
 - [初期値]: -

[説明]

SNMPv2c 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。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

24.9 SNMPv2c トラップの送信先の設定

[書式]

snmpv2c trap host host [type [community]]

no snmpv2c trap host host

[設定値及び初期値]

- *host*
 - [設定値]: SNMPv2c トラップの送信先ホストの IP アドレス (IPv4/IPv6)
 - [初期値]: -

- *type*: メッセージタイプ
- [設定値]:

設定値	説明
trap	トラップを送信する
inform	Inform リクエストを送信する

- [初期値]: trap
- *community*
 - [設定値]: コミュニティ名 (16 文字以内)
 - [初期値]: -

[説明]

SNMPv2c 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名にはこのコマンドの *community* パラメータが用いられるが、省略されている場合には **snmpv2c trap community** コマンドの設定値が用いられる。

type パラメータで 'inform' を指定した場合は、送信先からの応答があるまで、5 秒間隔で最大 3 回再送する。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

24.10 SNMPv2c トラップのコミュニティ名の設定

[書式]

```
snmpv2c trap community name
no snmpv2c trap community
```

[設定値及び初期値]

- *name*
 - [設定値]: コミュニティ名 (16 文字以内)
 - [初期値]: public

[説明]

SNMPv2c トラップを送信する際のコミュニティ名を設定する。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

24.11 SNMPv3 エンジン ID の設定

[書式]

```
snmpv3 engine id engine_id
no snmpv3 engine id
```

[設定値及び初期値]

- *engine_id*
 - [設定値]: SNMP エンジン ID (27 文字以内)
 - [初期値]: LAN1 の MAC アドレス

[説明]

SNMP エンジンを識別するためのユニークな ID を設定する。SNMP エンジン ID は SNMPv3 通信で相手先に通知される。

相手先に通知されるフォーマットは以下。

- *engine_id* が初期値の場合
「8000049e03」 + (LAN1 の MAC アドレス)
- *engine_id* に任意の値を設定した場合
「8000049e04」 + 設定値の ASCII 文字列

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

24.12 SNMPv3 コンテキスト名の設定

[書式]

snmpv3 context name *name*

no snmpv3 context name

[設定値及び初期値]

- *name*
 - [設定値]: SNMP コンテキスト名 (16 文字以内)
 - [初期値]: -

[説明]

SNMP コンテキストを識別するための名前を設定する。SNMP コンテキスト名は SNMPv3 通信で相手先に通知される。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

24.13 SNMPv3 USM で管理するユーザの設定

[書式]

snmpv3 usm user *user_id name* [**group** *group_id*] [*auth auth_pass* [*priv priv_pass*]]

no snmpv3 usm user *user_id*

[設定値及び初期値]

- *user_id*
 - [設定値]: ユーザ番号 (1..65535)
 - [初期値]: -
- *name*
 - [設定値]: ユーザ名 (32 文字以内)
 - [初期値]: -
- *group_id*
 - [設定値]: ユーザグループ番号 (1..65535)
 - [初期値]: -
- *auth*: 認証アルゴリズム
 - [設定値]:

設定値	説明
md5	HMAC-MD5-96
sha	HMAC-SHA1-96

- [初期値]: -
- *auth_pass*
 - [設定値]: 認証パスワード (8 文字以上、32 文字以内)
 - [初期値]: -
- *priv*: 暗号アルゴリズム
 - [設定値]:

設定値	説明
des-cbc	DES-CBC
aes128-cfb	AES128-CFB

- [初期値]: -
- *priv_pass*
 - [設定値]: 暗号パスワード (8 文字以上、32 文字以内)
 - [初期値]: -

[説明]

SNMPv3 によるアクセスが可能なユーザ情報を設定する。

ユーザグループ番号を指定した場合は VACM によるアクセス制御の対象となる。指定しない場合、そのユーザはすべての MIB オブジェクトにアクセスできる。

SNMPv3 では通信内容の認証および暗号化が可能であり、本コマンドでユーザ名と共にアルゴリズムおよびパスワードを設定して使用する。なお、認証を行わず暗号化のみを行うことはできない。

認証や暗号化の有無、アルゴリズムおよびパスワードは、対向となる SNMP マネージャ側のユーザ設定と一致させておく必要がある。

[ノート]

group オプションは、RTX1200 Rev.10.01.29 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで指定可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

24.14 SNMPv3 によるアクセスを許可するホストの設定

[書式]

```
snmpv3 host host user user_id ...
```

```
snmpv3 host none
```

```
no snmpv3 host [host]
```

[設定値及び初期値]

- *host* : SNMPv3 によるアクセスを許可するホスト

- [設定値]:

設定値	説明
<i>ip_address</i>	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)
<i>lanN</i>	LAN インターフェース名
<i>bridgeN</i>	ブリッジインターフェース名
any	すべてのホストからのアクセスを許可する

- [初期値]: -
- none : すべてのホストからのアクセスを禁止する
 - [初期値]: none
- *user_id* : ユーザ番号
 - [設定値]:
 - 1 個の数字、または間に - をはさんだ数字 (範囲指定)、およびこれらを任意に並べたもの (128 個以内)
 - [初期値]: -

[説明]

SNMPv3 によるアクセスを許可するホストを設定する。

host パラメータに 'any' を設定した場合は任意のホストからの SNMPv3 によるアクセスを許可する。なお、アクセスのあったホストが *host* パラメータに合致していても、*user_id* パラメータで指定したユーザに合致しなければアクセスはできない。

[ノート]

HOST パラメーターに IP アドレスの範囲や *lanN*、*bridgeN* を指定できるのは RTX1200 Rev.10.01.59 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.18 以降のファームウェア、および、Rev.14.01 系以降のファームウェアである。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

24.15 SNMPv3 VACM で管理する MIB ビューファミリの設定

[書式]

```
snmpv3 vacm view view_id type oid [type oid ...]
```

```
no snmpv3 vacm view view_id
```

[設定値及び初期値]

- *view_id*
 - [設定値]: ビュー番号 (1..65535)
 - [初期値]: -
- *type*
 - [設定値]:

設定値	説明
include	指定したオブジェクト ID を管理対象にする
exclude	指定したオブジェクト ID を管理対象から除外する

- [初期値]: -
- *oid*
 - [設定値]: MIB オブジェクト ID (サブ ID の数は 2 個以上、128 個以下)
 - [初期値]: -

[説明]

VACM による管理で使用する MIB ビューファミリを設定する。MIB ビューファミリとは、アクセス権を許可する際に指定する MIB 変数の集合である。

type パラメータと *oid* パラメータの組は、指定のオブジェクト ID 以降の MIB サブツリーを管理対象とする／しないことを意味する。また複数の組を指定した際に、それぞれ指定したオブジェクト ID の中で包含関係にあるものは、より下位の階層まで指定したオブジェクト ID に対応する *type* パラメータが優先される。128 組まで指定可能。

[ノート]

RTX1200 は Rev.10.01.29 以降で使用可能。

[設定例]

- inetnet サブツリー (1.3.6.1) 以降を管理対象とする。ただし enterprises サブツリー (1.3.6.1.4.1) 以降は管理対象から除外する

```
# snmpv3 vacm view 1 include 1.3.6.1 exclude 1.3.6.1.4.1
```

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

24.16 SNMPv3 VACM で管理するアクセスポリシーの設定

[書式]

```
snmpv3 vacm access group_id read read_view write write_view
```

```
no snmpv3 vacm access group_id
```

[設定値及び初期値]

- *group_id*
 - [設定値]: グループ番号 (1..65535)
 - [初期値]: -
- *read_view*
 - [設定値]:

設定値	説明
<i>view_id</i>	読み出し可能なアクセス権を設定するビュー番号
none	読み出し可能なビューを設定しない

- [初期値]: -
- *write_view*

- [設定値]:

設定値	説明
<i>view_id</i>	書き込み可能なアクセス権を設定するビュー番号
none	書き込み可能なビューを設定しない

- [初期値]:-

[説明]

ユーザグループに対してアクセスできる MIB ビューファミリを設定する。このコマンドで設定された MIB ビューファミリに含まれない MIB 変数へのアクセスは禁止される。

[ノート]

RTX1200 は Rev.10.01.29 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

24.17 SNMPv3 トラップの送信先の設定

[書式]

```
snmpv3 trap host host [type] user user_id
no snmpv3 trap host host
```

[設定値及び初期値]

- *host*
 - [設定値]: SNMPv3 トラップの送信先ホストの IP アドレス (IPv4/IPv6)
 - [初期値]:-
- *type*: メッセージタイプ
 - [設定値]:

設定値	説明
trap	トラップを送信する
inform	Inform リクエストを送信する

- [初期値]: trap
- *user_id*
 - [設定値]: ユーザ番号
 - [初期値]:-

[説明]

SNMPv3 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。トラップ送信時のユーザ設定は **snmpv3 usm user** コマンドで設定したユーザ設定が用いられる。

type パラメータで 'inform' を指定した場合は、送信先からの応答があるまで、5 秒間隔で最大 3 回再送する。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

24.18 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
```

[設定値及び初期値]

- *ip_address*
 - [設定値]: IP アドレス (IPv4/IPv6)
 - [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

[説明]

SNMP 送信パケットの始点 IP アドレスを設定する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

24.19 sysContact の設定

[書式]

snmp syscontact *name*

no snmp syscontact

[設定値及び初期値]

- *name*
 - [設定値]: sysContact として登録する名称 (255 文字以内)
 - [初期値]: -

[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。

[設定例]

```
# snmp syscontact "RT administrator"
```

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

24.20 sysLocation の設定

[書式]

snmp syslocation *name*

no snmp syslocation

[設定値及び初期値]

- *name*
 - [設定値]: sysLocation として登録する名称 (255 文字以内)
 - [初期値]: -

[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。

[設定例]

```
# snmp syslocation "RT room"
```

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

24.21 sysName の設定

[書式]

snmp sysname *name*

no snmp sysname

[設定値及び初期値]

- *name*
 - [設定値]: sysName として登録する名称 (255 文字以内)

- [初期値]:-

[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。

[設定例]

```
# snmp sysname "RTX3000 with BRI module"
```

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

24.22 SNMP 標準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
```

[設定値及び初期値]

- `trap` : 標準トラップの種類

- [設定値]:

設定値	説明
coldstart	電源投入時
warmstart	再起動時
linkdown	リンクダウン時
linkup	リンクアップ時
authenticationfailure	認証失敗時

- [初期値]:-

- `all` : 全ての標準トラップを送信する

- [初期値]:-

[初期設定]

```
snmp trap enable snmp all
```

[説明]

SNMP 標準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、すべての標準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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

24.23 CPU 使用率監視機能による SNMP トラップを送信するか否かの設定

[書式]

snmp trap cpu threshold *switch*

no snmp trap cpu threshold

[設定値及び初期値]

- *switch*

- [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: off

[説明]

system cpu threshold により設定した警告を発する CPU 使用率の閾値の上限を超える、または、閾値の下限を下回った際に SNMP トラップを送信するか否かの設定

[ノート]

RTX5000、RTX3500 は Rev.14.00.29 以降で使用可能。 RTX1210 は Rev.14.01.34 以降で使用可能。 RTX830 は Rev. 15.02.10 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

24.24 メモリ使用率監視機能による SNMP トラップを送信するか否かの設定

[書式]

snmp trap memory threshold *switch*

no snmp trap memory threshold

[設定値及び初期値]

- *switch*

- [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: off

[説明]

system memory threshold により設定した警告を発するメモリ使用率の閾値の上限を超える、または、閾値の下限を下回った際に SNMP トラップを送信するか否かの設定

[ノート]

RTX5000、RTX3500 は Rev.14.00.29 以降で使用可能。 RTX1210 は Rev.14.01.34 以降で使用可能。 RTX830 は Rev. 15.02.10 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

24.25 SNMP トラップの送信の遅延時間の設定

[書式]

snmp trap delay-timer [*wait*]

snmp trap delay-timer off

no snmp trap delay-timer [*wait*]

[設定値及び初期値]

- *wait*

- [設定値]: SNMP トラップを送信するまでの遅延時間の秒数(1 .. 21474836)
- [初期値]: -

[説明]

SNMP トラップを送信するイベントが発生してからトラップを送信するまでの間隔を指定する。off を設定した場合、即座に SNMP トラップを送信する。設定する遅延時間は最低限保証する値であり、設定値以上遅延する場合もある。

[ノート]

RTX5000 は Rev.14.00.26 以降で使用可能。
 RTX3500 は Rev.14.00.26 以降で使用可能。
 RTX1210 は Rev.14.01.28 以降で使用可能。
 RTX830 は Rev.15.02.03 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

24.26 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
no snmp trap send linkdown tunnel tunnel_num
```

[設定値及び初期値]

- *interface*
 - [設定値]:
 - LAN インタフェース名
 - WAN インタフェース名
 - BRI インタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -
- *switch*
 - [設定値]:

設定値	説明
on	送信する
off	送信しない
 - [初期値]: on

[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。

[ノート]

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

24.27 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
```

[設定値及び初期値]

- *switch*

- [設定値]:

設定値	説明
on	MIB 変数 yrIfPpDisplayAtMib2 を "enabled(1)" とする
off	MIB 変数 yrIfPpDisplayAtMib2 を "disabled(2)" とする

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

24.28 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
```

[設定値及び初期値]

- *switch*

- [設定値]:

設定値	説明
on	MIB 変数 yrIfTunnelDisplayAtMib2 を "enabled(1)" とする
off	MIB 変数 yrIfTunnelDisplayAtMib2 を "disabled(2)" とする

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

24.29 スイッチの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 yrifswitchdisplayatmib2 switch
no snmp yrifswitchdisplayatmib2
```

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
on	MIB 変数 yrIfSwitchDisplayAtMib2 を "enabled(1)" とする
off	MIB 変数 yrIfSwitchDisplayAtMib2 を "disabled(2)" とする

- [初期値]: on

[説明]

MIB 変数 yrIfSwitchDisplayAtMib2 の値をセットする。この MIB 変数は、スイッチのインタフェースを MIB2 の範囲で表示するかどうかを決定する。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

24.30 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
```

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
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

- [初期値]: off

[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、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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

24.31 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
```

[設定値及び初期値]

- *interface*
 - [設定値]: スイッチングハブを持つ LAN インタフェース名
 - [初期値]: -
- *switch*
 - [設定値]:

設定値	説明
on	トラップを送信する
off	トラップを送信しない

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

24.32 電波強度トラップを送信するか否かの設定

[書式]

```
snmp trap mobile signal-strength switch [level]
no snmp trap mobile signal-strength [switch [level]]
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	トラップを送信する
off	トラップを送信しない

- [初期値]: off
- *level*: アンテナ本数の閾値
 - [設定値]:

設定値	説明
0..3	アンテナ本数
省略	省略時は圏外

- [初期値]: -

[説明]

モバイル端末の電波強度トラップを送信するか否かを設定する。自動/手動に関わらず、ルータが電波強度を取得した時にトラップ送信が許可されており、電波強度のアンテナ本数が閾値以下であった場合にトラップが送信される。

[ノート]

トラップは `yrIfMobileStatusTrap` が送信される。

RTX1200 は Rev.10.01.29 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

24.33 スイッチへ静的に付与するインタフェース番号の設定

[書式]

```
snmp ifindex switch static index index switch
no snmp ifindex switch static index index [switch]
```

[設定値及び初期値]

- *index*
 - [設定値]: オブジェクト ID のインデックス(100000000 .. 199999999)
 - [初期値]: -
- *switch*: MAC アドレス、あるいはポート番号の組
 - [初期値]: -

[説明]

スイッチのインタフェースを示すオブジェクト ID のインデックスの先頭を静的に指定する。

[ノート]

オブジェクト ID が重複した場合の動作は保証されない。

静的にオブジェクト ID のインデックスの先頭を指定した場合、スイッチのインタフェースを示すオブジェクト ID のインデックスは動的に割り当てられない。

snmp yrswindex switch static index コマンドが設定された場合、**snmp yrswindex switch static index** コマンドで指定されたスイッチのみインデックスが割り当てられる。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

24.34 スイッチへ静的に付与するスイッチ番号の設定

[書式]

```
snmp yrswindex switch static index index switch
no snmp yrswindex switch static index index [switch]
```

[設定値及び初期値]

- *index*
 - [設定値]: オブジェクト ID のインデックス(1 .. 2147483647)
 - [初期値]: -
- *switch*: MAC アドレス、あるいはポート番号の組
 - [初期値]: -

[説明]

スイッチのオブジェクト ID のインデックスを静的に指定する。

[ノート]

静的にオブジェクト ID のインデックスを指定した場合、スイッチのオブジェクト ID のインデックスは動的に割り当てられない。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

24.35 スイッチの状態による SNMP トラップの条件の設定

[書式]

```
snmp trap enable switch switch trap [trap...]
snmp trap enable switch switch all
snmp trap enable switch switch none
no snmp trap enable switch switch
```

[設定値及び初期値]

- *switch*: default、MAC アドレス、あるいはポート番号の組

- [初期値]: -
- *trap*: トラップの種類
- [設定値]:

設定値	説明
linkup	リンクアップ時
linkdown	リンクダウン時
fanlock	ファン異常時
loopdetect	ループ検出時
poesupply	給電開始
poetermine	給電停止
oversupply	給電能力オーバー
overtemp	温度異常
powerfailure	電源異常

- [初期値]: -
- *all*: 全てのトラップを送信する
- [初期値]: -
- *none*: 全てのトラップを送信しない
- [初期値]: -

[初期設定]

```
snmp trap enable switch default all
```

[説明]

選択されたスイッチの監視状態に応じてトラップを送信する条件を設定する。*default* を指定して設定した場合は、個別のスイッチについて SNMP トラップの条件の設定がない場合の動作を決定する。

all を設定した場合には、すべてのトラップを送信する。*none* を設定した場合には、すべてのトラップを送信しない。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。

リンクアップ・リンクダウントラップは標準 MIB のトラップであり、送信するには **snmp trap enable snmp** コマンドでもトラップ送信が許可されている必要がある。

ループ検出のトラップを送信するにはスイッチ側に **switch control function set loopdetect-linkdown linkdown** コマンドあるいは **switch control function set loopdetect-linkdown linkdown-recovery** コマンドが設定されている必要がある。

給電開始、給電停止、給電能力オーバー、温度異常、電源異常のトラップを設定した場合、SWX2200-8PoE 以外のスイッチではトラップは送信されない。

[ノート]

給電開始、給電停止、給電能力オーバー、温度異常、電源異常のトラップは RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.19 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

24.36 スイッチで共通の SNMP トラップの条件の設定

[書式]

```
snmp trap enable switch common trap [trap...]
snmp trap enable switch common all
snmp trap enable switch common none
no snmp trap enable switch common
```

[設定値及び初期値]

- *trap*: トラップの種類
- [設定値]:

設定値	説明
find-switch	スイッチが監視下に入った時
detect-down	スイッチが監視から外れた時

- [初期値]: -
- all: 全てのトラップを送信する
 - [初期値]: -
- none: 全てのトラップを送信しない
 - [初期値]: -

[初期設定]

```
snmp trap enable switch common all
```

[説明]

スイッチの監視状態に応じてトラップを送信する条件を設定する。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

第 25 章

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。

25.1 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]
```

[設定値及び初期値]

- *auth*
- [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

25.2 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]
```

[設定値及び初期値]

- *account*
- [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

25.3 RADIUS サーバーの指定

[書式]

```
radius server ip1 [ip2]
no radius server [ip1 [ip2]]
```

[設定値及び初期値]

- *ip1*
 - [設定値]: RADIUS サーバー(正)の IP アドレス (IPv6 アドレス可)
 - [初期値]: -
- *ip2*
 - [設定値]: RADIUS サーバー(副)の IP アドレス (IPv6 アドレス可)
 - [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

25.4 RADIUS 認証サーバーの指定

[書式]

```
radius auth server ip1 [ip2]
no radius auth server [ip1 [ip2]]
```

[設定値及び初期値]

- *ip1*
 - [設定値]: RADIUS 認証サーバー(正)の IP アドレス (IPv6 アドレス可)
 - [初期値]: -
- *ip2*
 - [設定値]: RADIUS 認証サーバー(副)の IP アドレス (IPv6 アドレス可)
 - [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

25.5 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]]
```

[設定値及び初期値]

- *ip1*
 - [設定値]: RADIUS アカウントサーバー(正)の IP アドレス (IPv6 アドレス可)
 - [初期値]: -
- *ip2*
 - [設定値]: RADIUS アカウントサーバー(副)の IP アドレス (IPv6 アドレス可)
 - [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

25.6 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]
```

[設定値及び初期値]

- *port_num*
 - [設定値]: UDP ポート番号
 - [初期値]: 1645

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

25.7 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]
```

[設定値及び初期値]

- *port_num*
 - [設定値]: UDP ポート番号
 - [初期値]: 1646

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

25.8 RADIUS シークレットの設定

[書式]

radius secret *secret*

no radius secret [*secret*]

[設定値及び初期値]

- *secret*
 - [設定値]: シークレット文字列 (16 文字以内)
 - [初期値]: -

[説明]

RADIUS シークレットを設定する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

25.9 RADIUS 再送信パラメータの設定

[書式]

radius retry *count time*

no radius retry [*count time*]

[設定値及び初期値]

- *count*
 - [設定値]: 再送回数 (1..10)
 - [初期値]: 4
- *time*
 - [設定値]: ミリ秒 (20..10000)
 - [初期値]: 3000

[説明]

RADIUS パケットの再送回数とその時間間隔を設定する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

第 26 章

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。

26.1 NAT 機能の動作タイプの設定

[書式]

```
nat descriptor backward-compatibility type
```

```
no nat descriptor backward-compatibility [type]
```

[設定値及び初期値]

- *type*

- [設定値]:

設定値	説明
1	Rev.14 系以前の動作タイプ (ポートセービング IP マスカレード機能を無効にする)
2	Rev.14.01 系以降の動作タイプ (ポートセービング IP マスカレード機能を有効にする)

- [初期値]:

- 1 (RTX5000、RTX3500)
- 2 (上記以外)

[説明]

NAT 機能全体の動作タイプを設定する。

RTX5000 / RTX3500 Rev.14.00.32 以降、および、Rev.14.01 系以降の機種では、ポートセービング IP マスカレード機能に対応しており、IP マスカレードにおいて同一のポート番号を使用して複数の接続先とのセッションを確立できる。本コマンドは、ポートセービング IP マスカレード機能をサポートしていない Rev.14 系以前の機種との互換性維持のために用意されており、*type* パラメータを 1 に設定した場合の NAT 機能の動作は、Rev.14 系以前の NAT 機能の動作と同等となる。*type* パラメータを 2 に設定して動作させた場合に問題が生じる場合は、*type* パラメータを 1 にして NAT 機能を使用する必要がある。

[ノート]

本コマンドによる設定の変更を反映するには、ルーターの再起動が必要となる。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

26.2 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]]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *nat_descriptor_list*
 - [設定値]: 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)
 - [初期値]: -

[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 は Rev.8.03 系以降のすべてのファームウェアで指定可能。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

26.3 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 [hairpin=sw]
no nat descriptor type nat_descriptor [type [hairpin=sw]]
```

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]: NAT ディスクリプタ番号 (1..2147483647)
 - [初期値]: -
- *type*
 - [設定値]:

設定値	説明
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

- [初期値]: none
- *sw*

- [設定値]:

設定値	説明
on	ヘアピン NAT 機能を利用する
off	ヘアピン NAT 機能を利用しない

- [初期値]: off

[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 個利用可能な場合は先勝ちで 15 個 NAT 変換され、残りは IP マスカレード変換される。

hairpin オプションは、RTX830 Rev.15.02.24 以降、RTX1220 Rev.15.04.04 以降 のファームウェアで指定可能。また、*type* に none を指定したときは、hairpin オプションは指定できない。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

26.4 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]
```

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]: NAT ディスクリプタ番号 (1..2147483647)
 - [初期値]: -
- *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
 - [設定値]:

設定値	説明
IP アドレス	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
map-e	MAP-E で自動的に生成された IP アドレス

- [初期値]: ipcp

[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	○	×	×

適用インタフェース	LAN	PP	トンネル
secondary	○	×	×
IP アドレス	○	○	○
map-e	×	×	○

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

26.5 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]
```

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]: NAT ディスクリプタ番号 (1..2147483647)
 - [初期値]: -
- *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
 - [設定値]:

設定値	説明
IP アドレス	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

- [初期値]: auto

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

26.6 静的 NAT エントリの設定

[書式]

```
nat descriptor static nat_descriptor id outer_ip=inner_ip [count]
nat descriptor static nat_descriptor id outer_ip=inner_ip/netmask
no nat descriptor static nat_descriptor id [outer_ip=inner_ip [count]]
```

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]: NAT ディスクリプタ番号 (1..2147483647)
 - [初期値]: -
- *id*
 - [設定値]: 静的 NAT エントリの識別情報 (1..2147483647)
 - [初期値]: -
- *outer_ip*
 - [設定値]: 外側 IP アドレス (1 個)
 - [初期値]: -
- *inner_ip*
 - [設定値]: 内側 IP アドレス (1 個)
 - [初期値]: -
- *count*

- [設定値]:
 - 連続設定する個数
 - 省略時は 1
- [初期値]: -
- *netmask*
 - [設定値]:
 - xxx.xxx.xxx.xxx(xxx は十進数)
 - 0x に続く十六進数
 - マスクビット数 (16...32)
 - [初期値]: -

[説明]

NAT 変換で固定割り付けする IP アドレスの組み合わせを指定する。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。

ネットマスクによる範囲指定方式は、RTX1200 Rev.10.01.42 以降、RTX810 Rev.11.01.09 以降のファームウェア、および、Rev.14.00 系以降のすべてのファームウェアで使用可能である。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

26.7 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]
```

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]: NAT ディスクリプタ番号 (1..2147483647)
 - [初期値]: -
- *use*
 - [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

26.8 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]
```

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]: NAT ディスクリプタ番号 (1..2147483647)
 - [初期値]: -
- *id*
 - [設定値]: 静的 IP マスカレードエントリの識別情報 (1 以上の数値)
 - [初期値]: -
- *inner_ip*
 - [設定値]: 内側 IP アドレス (1 個)
 - [初期値]: -
- *protocol*
 - [設定値]:

設定値	説明
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

- [初期値]: -
- *outer_port*
 - [設定値]: 固定する外側ポート番号 (ニーモニック)
 - [初期値]: -
- *inner_port*
 - [設定値]: 固定する内側ポート番号 (ニーモニック)
 - [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

26.9 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_descriptor 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_descriptor tcpfin [time2]
```

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]: NAT ディスクリプタ番号 (1..2147483647)
 - [初期値]: -
- *time*
 - [設定値]: 消去タイマの秒数 (30..21474836)
 - [初期値]: 900
- *time2*
 - [設定値]: TCP/FIN 通過後の消去タイマの秒数 (1-21474836)
 - [初期値]: 60
- *protocol*
 - [設定値]: プロトコル
 - [初期値]: -
- *port_range*
 - [設定値]: 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
 - [初期値]: -

[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。DNS の場合、このコマンドでの設定値にかかわらず、応答パケットが通過してから約 10 秒でセッション情報を削除する。

[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 系以降

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

26.10 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
```

[設定値及び初期値]

- *type*
 - [設定値]:

設定値	説明
auto	自動認識可能なアプリケーションの接続の制御チャンネルとデータチャンネルの TTL を同期させる
all	同じホストによるすべての TCP 接続を対象
ftp	FTP の制御チャンネルのみを対象

- [初期値]: auto

[説明]

制御チャンネルとデータチャンネルからなるアプリケーションにおいて、データチャンネル上でのデータ転送中に、対応する制御チャン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、制御チャンネルとデータチャンネルの両 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。

[適用モデル]

RTX1500, RTX1100, RT250i, RT107e

26.11 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
```

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]: NAT ディスクリプタ番号 (1..2147483647)
 - [初期値]: -
- *action*
 - [設定値]:

設定値	説明	
	TCP/0~1023 宛てのパケット	左記以外
through	破棄して、RST を返す	変換せずに通す
reject	破棄して、RST を返す	破棄して、何も返さない
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	

- [初期値]: reject
- *ip_address*
 - [設定値]: 転送先の IP アドレス
 - [初期値]: -

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

26.12 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 [port_range4]]]
no nat descriptor masquerade port range nat_descriptor [port_range1 [port_range2 [port_range3 [port_range4]]]]
```

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]: NAT ディスクリプタ番号 (1..2147483647)
 - [初期値]: -

- *port_range1*, *port_range2*, *port_range3*, *port_range4*

- [設定値]: 間に - をはさんだポート番号の範囲

- [初期値]:

Rev.14.00 系以前では IP マスカレードの最大使用ポート数によって以下のように設定されている

- 4096 : *port_range1*=60000-64095
- 10000 : *port_range1*=60000-64095, *port_range2*=54096-59999
- 20000 : *port_range1*=60000-64095, *port_range2*=49152-59999, *port_range3*=44096-49151
- 40000 : *port_range1*=60000-64095, *port_range2*=49152-59999, *port_range3*=24096-49151
- 65534 : *port_range1*=49152-65534, *port_range2*=30000-49151, *port_range3*=10000-29999, *port_range4*=1024-9999

Rev.14.01 系以降では機種ごとに以下のように設定されている

- RTX1220 / RTX1210 / RTX830 : *port_range1*=60000-64095, *port_range2*=49152-59999, *port_range3*=44096-49151 (初期設定ポート数は 20000)

[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。このように、*port_range1* から *port_rangeN* の範囲まで、小さい番号のポート範囲から順番にポート番号が利用される。

RTX5000 / RTX3500 は NAT の最大同時セッション数が 65534 であるが、初期設定ではウェルノウンポートを除いた 64511 個のポートしか使用できないため、同時セッション数を 65534 まで拡張する場合は、本コマンドで 65534 個のポートを使用できるようにポート範囲を広げる、あるいは `nat descriptor backward-compatibility` コマンドで *type* パラメーターを 2 に設定する必要がある。

RTX5000 / RTX3500 Rev.14.00.32 以降、および、Rev.14.01 系以降では、同一のポート番号を使用して複数の接続先とのセッションを確立できるため、本コマンドで設定したポート数を超えるセッションの確立が可能である。

RTX5000 / RTX3500 Rev.14.00.32 以降、および、Rev.14.01 系以降では、最大セッション数は `nat descriptor masquerade session limit total` コマンドで設定する。ただし RTX5000 / RTX3500 Rev.14.00.32 以降、および、Rev.14.01 系以降においても、`nat descriptor backward-compatibility` コマンドで *type* パラメーターを 1 に変更した場合は、最大セッション数は本コマンドで設定したポート数と同等となるため、最大セッション数を変更する場合は本コマンドの設定を変更する必要がある。

[ノート]

機種ごとの最大使用ポート数と利用可能なポート範囲の個数を下表に示す。

機種	最大使用ポート数	ポート範囲の個数
RTX1210 Rev.14.01.34 以降、RTX830 Rev.15.02.10 以降、RTX1220	65534	64
RTX1210 Rev.14.01.26 以降、RTX830 Rev.15.02.03 以降	65534	16
RTX1210 Rev.14.01.20 以前、RTX830 Rev.15.02.01	65534	4
RTX5000, RTX3500 Rev.14.00.32 以降	65534	64
RTX5000, RTX3500 Rev.14.00.29 以前	65534	4
RTX3000	40000	3
RTX1200	20000	3
RTX810	10000	2
上記以外	4096	1

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

26.13 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...]

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]: NAT ディスクリプタ番号 (1..2147483647)
 - [初期値]: -
- *port*
 - [設定値]: ポート番号 (1..65535)
 - [初期値]: 21

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

26.14 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]

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]: NAT ディスクリプタ番号 (1..2147483647)
 - [初期値]: -
- *protocol*
 - [設定値]:

設定値	説明
tcp	TCP
udp	UDP

- [初期値]: -
- *port*
 - [設定値]: ポート番号の範囲
 - [初期値]: -

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

26.15 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

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	記録する
off	記録しない

- [初期値]: off

[説明]

NAT のアドレス割当をログに記録するか否かを設定する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

26.16 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*

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]: NAT ディスクリプタ番号 (1..2147483647)
 - [初期値]: -
- *sip*
 - [設定値]:

設定値	説明
on	変換する
off	変換しない
auto	sip use コマンドの設定値に従う

- [初期値]:
 - auto (auto が指摘できる機種・リビジョン)
 - on (上記以外)

[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.8.02.35 で初期値を off から on に変更した。

auto は RTX3000 Rev.9.00.50 以降、RTX1200 Rev.10.01.24 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

26.17 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*]

[設定値及び初期値]

- *remove*
 - [設定値]:

設定値	説明
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

- [初期値]: on

[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ならない。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。そうすると、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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

26.18 IP マスカレードで変換するホスト毎の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
```

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]: NAT ディスクリプタ番号 (1..2147483647)
 - [初期値]: -
- *id*
 - [設定値]: セッション数設定の識別番号 (1)
 - [初期値]: -
- *limit*
 - [設定値]:
 - 制限値 (1..65534)(RTX5000、RTX3500、RTX1210、RTX830、RTX1220)
 - 制限値 (1..40000)(RTX3000)
 - 制限値 (1..20000)(RTX1200)
 - 制限値 (1..10000)(RTX810)
 - 制限値 (1..4096) (上記以外)
 - [初期値]:
 - 65534(RTX5000、RTX3500、RTX1210、RTX830、RTX1220)
 - 40000(RTX3000)
 - 20000(RTX1200)
 - 10000(RTX810)
 - 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]

RTX1500、RTX1100、RT107e は Rev.8.03.68 以降で使用可能。

RTX3000 は Rev.9.00.31 以降で使用可能。

SRT100 は Rev.10.00.27 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

26.19 IP マスカレードで変換する合計セッション数の設定

[書式]

nat descriptor masquerade session limit total *nat_descriptor limit*

no nat descriptor masquerade session limit total *nat_descriptor*

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]: NAT ディスクリプタ番号 (1..2147483647)
 - [初期値]: -
- *limit*
 - [設定値]:
 - 制限値 (1..2147483647)
 - [初期値]:
 - 65534

[説明]

ひとつの NAT ディスクリプターにおいて、IP マスカレードで変換するセッション数の最大数を設定する。**nat descriptor masquerade session limit** コマンドとは異なり、すべてのホストのセッション数の合計が対象となる。

[ノート]

本コマンドの設定は、**nat descriptor backward-compatibility** コマンドで、*type* パラメータを 2 に設定した場合のみ有効となる。

[適用モデル]

RTX1220, RTX1210, RTX830

第 27 章

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** 等の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。**dns cache max entry** コマンドで設定した件数 (初期値 = 256) 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** 等のコマンドで、問い合わせ先 DNS サーバー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。問い合わせ先 DNS サーバーを設定するコマンドは複数存在しますが、これらのうち複数のコマンドで問い合わせ先 DNS サーバーが設定されている場合、利用できる中で最も優先順位の高いコマンドの設定が使用されます。各コマンドによる設定の優先順位は、高い順に以下の通りです。

1. **dns server select** コマンド
2. **dns server** コマンド
3. **dns server pp** コマンド
4. **dns server dhcp** コマンド

なお、これらのコマンドで問い合わせ先 DNS サーバーが全く設定されていない場合でも、DHCP サーバーから取得した DNS サーバーが存在すれば、そちらが自動的に使用されます。

27.1 DNS を利用するか否かの設定

[書式]

```
dns service service
no dns service [service]
```

[設定値及び初期値]

- *service*
- [設定値] :

設定値	説明
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

- [初期値] : recursive

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

27.2 DNS サーバーの IP アドレスの設定

[書式]

```
dns server ip_address [edns=sw] [nat46=tunnel_num] [ip_address [edns=sw] [nat46=tunnel_num]...]
no dns server [ip_address [edns=sw] [nat46=tunnel_num]...]
```

[設定値及び初期値]

- *ip_address*

- [設定値]: 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)
- [初期値]: -
- *sw*
- [設定値]:

設定値	説明
on	対象の DNS サーバーへの通信を EDNS で行う
off	対象の DNS サーバーへの通信を DNS で行う

- [初期値]: off
- *tunnel_num*
- [設定値]: トンネルインターフェース番号
- [初期値]: -

[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。
他のコマンドでも DNS サーバーが設定されている場合は、最も優先順位の高いコマンドの設定が使用される。DNS サーバーを設定する各種コマンドの優先順位は、本章冒頭の説明を参照。

edns オプションを省略、または edns=off を指定すると、対象の DNS サーバーへの名前解決は DNS で通信を行う。edns=on を指定すると、対象の DNS サーバーへの名前解決は EDNS で通信を行う。
edns=on で名前解決ができない場合、edns=off に変更すると名前解決できる場合がある。
EDNS はバージョン 0 に対応。

nat46 オプションを指定すると DNS46 機能が有効になり、この DNS サーバー宛ての A レコードの問い合わせを AAAA レコードの問い合わせに変換する。
また、DNS サーバーからの応答に含まれる AAAA レコードを、**nat46 ip address pool** コマンドの設定値を使用して A レコードに変換する。変換した A レコードは、DNS キャッシュに登録する。
tunnel_num には、**tunnel translation nat46** コマンドを設定したトンネルインターフェースの番号を指定する。

[ノート]

edns オプションは以下の機種およびリビジョンで使用可能。
RTX5000、RTX3500 は Rev.14.00.29 以降。
RTX830 は Rev.15.02.14 以降。
RTX1210 は Rev.14.01.35 以降。
RTX1220 はすべてのリビジョン。

nat46 オプションは以下の機種およびリビジョンで使用可能。
RTX830 Rev.15.02.20 以降で使用可能。
RTX1220 Rev.15.04.04 以降で使用可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

27.3 DNS ドメイン名の設定

[書式]

dns domain *domain_name*

no dns domain [*domain_name*]

[設定値及び初期値]

- *domain_name*
 - [設定値]: DNS ドメインを表す文字列
 - [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

27.4 DNS サーバーを通知してもらおう相手先情報番号の設定

[書式]

dns server pp *peer_num* [edns=sw]

no dns server pp [*peer_num* [edns=sw]]

[設定値及び初期値]

- *peer_num*
 - [設定値]: DNS サーバーを通知してもらおう相手先情報番号
 - [初期値]: -
- *sw*
 - [設定値]:

設定値	説明
on	対象の DNS サーバーへの通信を EDNS で行う
off	対象の DNS サーバーへの通信を DNS で行う

- [初期値]: off

[説明]

DNS サーバーを通知してもらお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 IPCPMS 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つたり、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ぬ。

他のコマンドでも DNS サーバーが設定されている場合は、最も優先順位の高いコマンドの設定が使用される。DNS サーバーを設定する各種コマンドの優先順位は、本章冒頭の説明を参照。

edns オプションを省略、または edns=off を指定すると、対象の DNS サーバーへの名前解決は DNS で通信を行う。

edns=on を指定すると、対象の DNS サーバーへの名前解決は EDNS で通信を行う。

edns=on で名前解決ができない場合、edns=off に変更すると名前解決できる場合がある。

EDNS はバージョン 0 に対応。

[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 msextn on** の設定が必要である。

edns オプションは以下の機種およびリビジョンで使用可能。

RTX5000、RTX3500 は Rev.14.00.29 以降。

RTX830 は Rev.15.02.14 以降。

RTX1210 は Rev.14.01.35 以降。

RTX1220 はすべてのリビジョン。

[設定例]

```
# pp select 2
pp2# ppp ipcp msexp on
pp2# dns server pp 2
```

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

27.5 DNS サーバーアドレスを取得するインタフェースの設定

[書式]

```
dns server dhcp interface [edns=sw] [nat46=tunnel_num]
no dns server dhcp
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名、ブリッジインタフェース名
 - [初期値]: -
- *sw*
 - [設定値]:

設定値	説明
on	対象の DNS サーバーへの通信を EDNS で行う
off	対象の DNS サーバーへの通信を DNS で行う

- [初期値]: off
- *tunnel_num*
 - [設定値]: トンネルインターフェース番号
 - [初期値]: -

[説明]

DNS サーバーアドレスを取得するインタフェースを設定する。このコマンドで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。

他のコマンドでも DNS サーバーが設定されている場合は、最も優先順位の高いコマンドの設定が使用される。DNS サーバーを設定する各種コマンドの優先順位は、本章冒頭の説明を参照。

edns オプションを省略、または edns=off を指定すると、対象の DNS サーバーへの名前解決は DNS で通信を行う。

edns=on を指定すると、対象の DNS サーバーへの名前解決は EDNS で通信を行う。

edns=on で名前解決ができない場合、edns=off に変更すると名前解決できる場合がある。

EDNS はバージョン 0 に対応。

nat46 オプションを指定すると DNS46 機能が有効になり、この DNS サーバー宛ての A レコードの問い合わせを AAAA レコードの問い合わせに変換する。

また、DNS サーバーからの応答に含まれる AAAA レコードを、**nat46 ip address pool** コマンドの設定値を使用して A レコードに変換する。変換した A レコードは、DNS キャッシュに登録する。

tunnel_num には、**tunnel translation nat46** コマンドを設定したトンネルインターフェースの番号を指定する。

[ノート]

この機能は指定したインタフェースが 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は SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

edns オプションは以下の機種およびリビジョンで使用可能。

RTX5000、RTX3500 は Rev.14.00.29 以降。

RTX830 は Rev.15.02.14 以降。

RTX1210 は Rev.14.01.35 以降。

RTX1220 はすべてのリビジョン。

nat46 オプションは RTX830 Rev.15.02.20 以降で使用可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

27.6 DHCP/DHCPv6/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]]

[設定値及び初期値]

- *protocol*

- [設定値]:

設定値	説明
dhcp	DHCP による通知
dhcpv6	DHCPv6 による通知
msex	IPCP MS 拡張による通知

- [初期値]: dhcp、dhcpv6 および msex

- *server*

- [設定値]:

設定値	説明
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、 <i>protocol</i> に dhcpv6 を指定した場合に DHCPv6 で割り当てられたサーバー群

- [初期値]:

- me server (*protocol* が dhcp または msex の場合)
- me (*protocol* が dhcpv6 の場合)

[説明]

DHCP や DHCPv6、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。

server に none を設定した場合、他の設定に関わらず DNS サーバーの通知を行わなくなる。

server に *me* を設定した場合、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 に *server* を設定した場合、*protocol* に *dhcp* または *msect* を指定したときは **dns server** コマンドに設定したサーバー群を通知し、*protocol* に *dhcpv6* を指定したときは、IPv6 網から DHCPv6 で通知された DNS サーバー群を通知する。

protocol に *dhcpv6* を指定したときは、IPv6 網と連動できない環境では、*server* の設定値にかかわらず、ルーターが IPv6 DNS サーバーアドレスを一切通知しない。

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。

[ノート]

dhcpv6 パラメーターは、RTX1210 は、Rev.14.01.35 以降、RTX830 は、Rev.15.02.14 以降、RTX1220 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

27.7 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]
```

[設定値及び初期値]

- *spoof*
- [設定値]:

設定値	説明
on	処理する
off	処理しない

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

27.8 DNS サーバーへの AAAA レコードの問い合わせを制限するか否かの設定

[書式]

```
dns service aaaa filter switch
no dns service aaaa filter [switch]
```

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
on	AAAA レコードの問い合わせを制限する
off	AAAA レコードの問い合わせを制限しない

- [初期値]: off

[説明]

DNS サーバーへの AAAA レコードの問い合わせを制限するか否かを設定する。

IPv6 での接続環境がないのに AAAA レコードが引けてしまうことで、接続に失敗するような場合は、このコマンドにより AAAA レコードの問い合わせに対して、AAAA レコードを回答しないようにする。

本機が DNS リレーサーバーになっている通信及び本機発の通信が影響を受ける。

[ノート]

RTX830 は Rev.15.02.03 以降で使用可能。
 RTX1210 は Rev.14.01.26 以降で使用可能。
 RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

27.9 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]
```

[設定値及び初期値]

- *resolv*
- [設定値]:

設定値	説明
on	解決する
off	解決しない

- [初期値]: off

[説明]

SYSLOG 表示で DNS により名前解決するか否かを設定する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

27.10 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 [edns=sw] [nat46=tunnel_num] [server2 [edns=sw]] [nat46=tunnel_num] [type] query [original-sender] [restrict pp connection-pp]
dns server select id pp peer_num [edns=sw] [default-server [edns=sw]] [type] query [original-sender] [restrict pp connection-pp]
dns server select id dhcp interface [edns=sw] [nat46=tunnel_num] [default-server [edns=sw]] [nat46=tunnel_num] [type] query [original-sender] [restrict pp connection-pp]
dns server select id reject [type] query [original-sender]
no dns server select id
```

[設定値及び初期値]

- *id*
 - [設定値]: DNS サーバー選択テーブルの番号
 - [初期値]: -
- *server*
 - [設定値]: プライマリ DNS サーバーの IP アドレス
 - [初期値]: -
- *server2*
 - [設定値]: セカンダリ DNS サーバーの IP アドレス
 - [初期値]: -
- *type*: DNS レコードタイプ
 - [設定値]:

設定値	説明
a	ホストの IP 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
any	すべてのタイプにマッチする
省略	省略時は a

- [初期値]: -
- *query*: DNS 問い合わせの内容
- [設定値]:

設定値	説明
<i>type</i> が a、aaaa、mx、ns、cname の場合	<i>query</i> 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、 <i>rtpro.yamaha.co.jp</i> 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。
<i>type</i> が ptr の場合	<i>query</i> は IP アドレス (<i>ip_address[/masklen]</i>) であり、 <i>masklen</i> を省略したときは IP アドレスにのみマッチし、 <i>masklen</i> 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 <i>.in-addr.arpa</i> 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	<i>query</i> 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、 <i>NetVolante.jp</i> 、 <i>NetVolante.rupro.yamaha.co.jp</i> などにマッチする。また、後方一致では、"*yamaha.co.jp" と記述する。

- [初期値]: -
- *original-sender*
 - [設定値]: DNS 問い合わせの送信元の IP アドレスの範囲
 - [初期値]: -
- *connection-pp*
 - [設定値]: 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
 - [初期値]: -
- *peer_num*
 - [設定値]: 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
 - [初期値]: -
- *interface*
 - [設定値]: DHCP サーバーより取得する DNS サーバーを使う場合の LAN インターフェース名または WAN インターフェース名またはブリッジインターフェース名
 - [初期値]: -
- *default-server*
 - [設定値]: *peer_num* パラメーター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
 - [初期値]: -
- *sw*
 - [設定値]:

設定値	説明
on	対象の DNS サーバーへの通信を EDNS で行う
off	対象の DNS サーバーへの通信を DNS で行う

- [初期値]: off
- *tunnel_num*
 - [設定値]: トンネルインターフェース番号
 - [初期値]: -

[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、他のコマンドで指定された DNS サーバーを用いる。DNS サーバーを設定する各種コマンドの優先順位は、本章冒頭の説明を参照。

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を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。

edns オプションを省略、または *edns=off* を指定すると、対象の DNS サーバーへの名前解決は DNS で通信を行う。*edns=on* を指定すると、対象の DNS サーバーへの名前解決は EDNS で通信を行う。*edns=on* で名前解決ができない場合、*edns=off* に変更すると名前解決できる場合がある。EDNS はバージョン 0 に対応。

nat46 オプションを指定すると DNS46 機能が有効になり、この DNS サーバー宛ての A レコードの問い合わせを AAAA レコードの問い合わせに変換する。また、DNS サーバーからの応答に含まれる AAAA レコードを、*nat46 ip address pool* コマンドの設定値を使用して A レコードに変換する。変換した A レコードは、DNS キャッシュに登録する。*tunnel_num* には、*tunnel translation nat46* コマンドを設定したトンネルインターフェースの番号を指定する。

[ノート]

ブリッジインタフェースは SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

edns オプションは以下の機種およびリビジョンで使用可能。
 RTX5000、RTX3500 は Rev.14.00.29 以降。
 RTX830 は Rev.15.02.14 以降。
 RTX1210 は Rev.14.01.35 以降。
 RTX1220 はすべてのリビジョン。

nat46 オプションは以下の機種およびリビジョンで使用可能。
 RTX830 Rev.15.02.20 以降で使用可能。
 RTX1220 Rev.15.04.04 以降で使用可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

27.11 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*]

[設定値及び初期値]

- *type* : 名前のタイプ

- [設定値] :

設定値	説明
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

- [初期値] :-

- *name*、*value*

- [設定値] :

type パラメータによって以下のように意味が異なる

<i>type</i> パラメータ	<i>name</i>	<i>value</i>
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

- [初期値] :-

- *fqdn*

- [設定値] : ドメイン名を含んだホスト名

- [初期値] :-

- *ttl*

- [設定値] : 秒数 (1~4294967295)

- [初期値] :-

[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。
- Answer セクションに回答となる DNS レコードが 1 つセットされるだけで、Authority/Additional セクションには DNS レコードがセットされない
- MX レコードの *preference* フィールドは 0 にセットされる

[設定例]

```
# ip host pc1.rtpro.yamaha.co.jp 133.176.200.1
# dns static ptr 133.176.200.2 pc2.yamaha.co.jp
# dns static cname mail.yamaha.co.jp mail2.yamaha.co.jp
```

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

27.12 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]]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号 (1..65535)
 - [初期値]:
 - 53 (Rev.10.00 以前)
 - 10000-10999 (Rev.10.01 以降)

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

27.13 DNS サーバーへアクセスできるホストの設定

[書式]

```
dns host ip_range [ip_range...]
dns host any
dns host none
dns host lan
no dns host
```

[設定値及び初期値]

- *ip_range*: DNS サーバーへのアクセスを許可するホストの IP アドレスまたはニーモニック
 - [設定値]:

設定値	説明
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	指定したホストからのアクセスを許可する
lanN	LAN インターフェースからのアクセスを許可する
wan1	WAN インターフェースからのアクセスを許可する
bridge1	ブリッジインターフェースからのアクセスを許可する
vlanN	VLAN インターフェースからのアクセスを許可する
lanN/M	タグ VLAN インターフェースからのアクセスを許可する

- [初期値]: -
- *any*
 - [設定値]: すべてのホストからのアクセスを許可する
 - [初期値]: *any*
- *none*
 - [設定値]: すべてのホストからのアクセスを禁止する
 - [初期値]: -
- *lan*
 - [設定値]: すべての LAN 側ネットワーク内からのアクセスを許可する
 - [初期値]: -

[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]

RTX1210 Rev.14.01.11 以降のファームウェア、および、Rev.15.02 系以降のすべてのファームウェアで IP アドレスとニーモニックの混在指定および複数のニーモニックの指定が可能。
それ以外のファームウェアでは、IP アドレスのみ複数指定可能。

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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

27.14 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 use [*switch*]

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
on	DNS キャッシュを利用する
off	DNS キャッシュを利用しない

- [初期値]: on

[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。

[ノート]

RT250i は、Rev.8.02.48 以降で使用可能。

RTX1100, RTX1500 は、Rev.8.03.77 以降で使用可能。

RT107e は、Rev.8.03.78 以降で使用可能。

RTX3000 は、Rev.9.00.40 以降で使用可能。

SRT100 は、Rev.10.00.40 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

27.15 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]

[設定値及び初期値]

- *num*
 - [設定値]: 最大エントリ数 (1...1024)
 - [初期値]: 256

[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。

[ノート]

RT250i は、Rev.8.02.48 以降で使用可能。

RTX1100, RTX1500 は、Rev.8.03.77 以降で使用可能。

RT107e は、Rev.8.03.78 以降で使用可能。

RTX3000 は、Rev.9.00.40 以降で使用可能。

SRT100 は、Rev.10.00.40 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

27.16 DNS フォールバック動作をルーター全体で統一するか否かの設定

[書式]

```
dns service fallback switch
```

```
no dns service fallback [switch]
```

[設定値及び初期値]

- *switch*

- [設定値]:

設定値	説明
on	DNS フォールバック動作を IPv6 優先に統一する
off	DNS フォールバック動作は機能ごとにまちまちである

- [初期値]: off

[説明]

DNS フォールバック動作をルーターのすべての機能で統一するか否かを設定する。

DNS でホスト名を IP アドレスに変換する場合、IPv4/IPv6 いずれかを DNS サーバーに先に問い合わせ、アドレスが解決できない場合に他方のアドレスを問い合わせる動作を、DNS フォールバックと呼ぶ。ルーター自身が問い合わせる場合、IPv4 を優先するか IPv6 を優先するかは機能ごとにまちまちであった。具体的には、以下の機能では DNS フォールバック動作では IPv6 が優先されるが、その他の機能では IPv4 が優先されている。

- HTTP リビジョンアップ機能
- HTTP アップロード機能

このコマンドを on に設定すると、ルーターのすべての機能で IPv6 が優先されるようになる。

[ノート]

DNS リカーシブサーバーとして、LAN 内の PC 等の問い合わせを上位の DNS サーバーに転送する際には、PC 等の問い合わせ内容をそのまま上位サーバーに転送するため、DNS フォールバックの動作も PC 等の実装がそのまま反映され、このコマンドの設定には影響を受けない。

RTX1100、RTX1500、RT107e は Rev.8.03.91 以降で使用可能。

SRT100 は Rev.10.00.61 以降で使用可能。

RTX1200 は Rev.10.01.36 以降で使用可能。

RTX810 は Rev.11.01.06 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

第 28 章

NAT46/DNS46 機能

NAT46/DNS46 機能とは、IPv4 パケットを IPv6 パケットに変換して転送する機能です。

本来、IP バージョンが異なるネットワークにあるホスト同士では、通信ができません。しかし、本機能を利用すると、LAN が IPv4 ネットワーク、WAN が IPv6 ネットワークという構成において、LAN にある PC から WAN にあるサーバーへのアクセスが可能になります。

既に IPv4 アドレスで構築された LAN を変更することなく、IPv6 アドレスで提供されているサービスを利用できます。

28.1 NAT46 機能で使用する IPv4 アドレスプールの設定

[書式]

```
nat46 ip address pool ipaddress_list  
no nat46 ip address pool [ipaddress_list]
```

[設定値及び初期値]

- *ipaddress_list*
 - [設定値]: 1 個の IPv4 アドレスまたは間に - をはさんだ IPv4 アドレス (範囲指定)、または、IPv4 ネットワークアドレス、および、これらを任意に並べたもの
 - [初期値]: -

[説明]

NAT46 機能で IPv4 アドレスを IPv6 アドレスに変換するために使用する IPv4 アドレスのプールを設定する。

DNS46 機能が AAAA レコードを A レコードに変換するとき、AAAA レコードの IPv6 アドレスを当コマンドで設定した範囲内の IPv4 アドレスに変換する。

DNS46 機能で行われた IPv4 アドレスと IPv6 アドレスとの対応づけは、以降の通信において NAT46 機能が IP ヘッダーを変換する際に使用する。

ipaddress_list は 8 個まで設定可能。ただし、*ipaddress_list* に含まれる IPv4 アドレスの合計が 254 個を超えた場合はコマンドエラーとなる。

[ノート]

tunnel translation コマンドで変換種別として nat46 を選択した場合だけ有効である。

RTX830 Rev.15.02.20 以降で使用可能。

RTX1220 Rev.15.04.04 以降で使用可能。

[適用モデル]

RTX1220, RTX830

28.2 NAT46 機能で使用する IPv6 プレフィックスの設定

[書式]

```
nat46 ipv6 prefix prefix_id  
no nat46 ipv6 prefix [prefix_id]
```

[設定値及び初期値]

- *prefix_id*
 - [設定値]: プレフィックス番号 (1..4294967295)
 - [初期値]: -

[説明]

NAT46 機能で送信元 IPv4 アドレスを送信元 IPv6 アドレスに変換するために使用するプレフィックスを設定する。

ipv6 prefix コマンドで設定したプレフィックス番号を指定する。

[ノート]

本コマンドで指定する `ipv6 prefix` コマンドのプレフィックスは以下の条件を満たす必要がある。

- プレフィックス長が /96 であること
- XXXX:XXXX:XXXX:XXXX:YYXX:XXXX:0000:0000/96 : 64 ~ 71 ビット目 (YY) が 0 であること

RTX830 Rev.15.02.20 以降で使用可能。

RTX1220 Rev.15.04.04 以降で使用可能。

[設定例]

LAN2 で受信した /64 の RA のプレフィックスから、NAT46 機能で使用する IPv6 プレフィックスを設定する。

RA で配られる プレフィックス(/64) : XXXX:XXXX:XXXX:XXXX:0000:0000:0000:0000/64

IPv4 アドレスに付与するプレフィックス : XXXX:XXXX:XXXX:XXXX:0000:0000:0000:0000/96

IPv6 アドレスに変換された IPv4 アドレス : XXXX:XXXX:XXXX:XXXX:0000:0000:YYY.YYY.YYY.YYY

```
# ipv6 prefix 1 ra-prefix@lan2::/96
# nat46 ipv6 prefix 1
```

[適用モデル]

RTX1220, RTX830

28.3 NAT46 機能で使用する宛先アドレスを静的に対応づける設定

[書式]

```
nat46 static id ipv4_address ipv6_address
```

```
no nat46 static id [ipv4_address] ipv6_address
```

[設定値及び初期値]

- *id*
 - [設定値]: 識別情報 (1..2147483647)
 - [初期値]: -
- *ipv4_address*
 - [設定値]: IPv4 アドレス (1 個)
 - [初期値]: -
- *ipv6_address*
 - [設定値]: IPv6 アドレス (1 個)
 - [初期値]: -

[説明]

NAT46 機能で使用する宛先の IPv6 アドレスに対応する IPv4 アドレスを静的に設定する。

宛先にホスト名ではなく IPv4 アドレスを指定してアクセスする場合 (DNS46 機能で名前解決させずに NAT46 機能を使用する場合) に設定する。

[ノート]

`nat46 ip address pool` コマンドで設定している IPv4 アドレスとは異なるアドレスを設定する必要がある。

RTX830 Rev.15.02.20 以降で使用可能。

RTX1220 Rev.15.04.04 以降で使用可能。

[適用モデル]

RTX1220, RTX830

28.4 NAT46 エントリーの表示

[書式]

```
show status nat46 table [tunnel tunnel_num] [type]
```

[設定値及び初期値]

- *tunnel_num* : トンネルインターフェース番号
 - [初期値] : -
- *type*
 - [設定値] :

設定値	説明
static	静的エントリーの情報を表示する
dynamic	動的エントリーの情報を表示する
all	静的エントリーと動的エントリーの情報を表示する

- [初期値] : all

[説明]

NAT46 エントリーを表示する。TYPE を省略した場合は、静的エントリーと動的エントリーの情報を表示する。

[ノート]

RTX830 Rev.15.02.20 以降で使用可能。
RTX1220 Rev.15.04.04 以降で使用可能。

[拡張ライセンス対応]

[拡張ライセンス](#)をインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX1220, RTX830

第 29 章

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。RTX5000、RTX3500、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
RTX5000、RTX3500、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。

RTX5000、RTX3500、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。

29.1 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]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *speed*
 - [設定値]: インタフェース速度 (bit/s)
 - [初期値]: 0 (PP インタフェースの場合)

[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。

RTX5000、RTX3500、RTX1220、RTX1210、RTX830 では、**queue interface type** コマンドで優先制御および帯域制御の設定が必要。

帯域制御で CBQ を利用する時にはパラメータ計算に用いられるので、物理的な速度と一致しているのが望ましい。その場合、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。

RTX830、RTX810、RT107e、SRT100 では **speed pp** コマンドは使用できない。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

29.2 クラス分けのためのフィルター設定

[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[/class2] [cos=cos] ipv6 src_addr [dest_addr [protocol [src_port [dest_port]]]]
queue class filter num precedence [mapping=prec:class [,prec:class...]] [cos=cos] ip src_addr [dest_addr [protocol
[src_port [dest_port]]]]
queue class filter num precedence [mapping=prec:class [,prec:class...]] [cos=cos] ipv6 src_addr [dest_addr [protocol
[src_port [dest_port]]]]
queue class filter num dscp [cos=cos] ip src_addr [dest_addr [protocol [src_port [dest_port]]]]
queue class filter num dscp [cos=cos] ipv6 src_addr [dest_addr [protocol [src_port [dest_port]]]]
queue class filter num class1 ip dpi src_addr [dest_addr [application]]
queue class filter num class1 ipv6 dpi src_addr [dest_addr [application]]
queue class filter num precedence [mapping=prec:class [,prec:class...]] [cos=cos] ip dpi src_addr [dest_addr
[application]]
queue class filter num precedence [mapping=prec:class [,prec:class...]] [cos=cos] ipv6 dpi src_addr [dest_addr
[application]]
queue class filter num class1 ip dpi src_addr [dest_addr [group_num]]
queue class filter num class1 ipv6 dpi src_addr [dest_addr [group_num]]
queue class filter num precedence [mapping=prec:class [,prec:class...]] [cos=cos] ip dpi src_addr [dest_addr
[group_num]]
queue class filter num precedence [mapping=prec:class [,prec:class...]] [cos=cos] ipv6 dpi src_addr [dest_addr
[group_num]]
no queue class filter num [...]
    
```

[設定値及び初期値]

- num
 - [設定値]: クラスフィルターの識別番号
 - [初期値]: -
- class1
 - [設定値]:

設定値	説明
1..100 (RTX5000、RTX3500、RTX3000)	クラス
1..16 (上記以外)	

- [初期値]: -
- class2
 - [設定値]: 第2階層クラス (1..4)
 - [初期値]: -
- prec
 - [設定値]: precedence 値 (0..7)
 - [初期値]: -
- cos
 - [設定値]:

設定値	説明
0-7	CoS 値
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

- [初期値]: -
- src_addr: IP パケットの始点アドレス

- [設定値]:
 - IP アドレス
 - A.B.C.D (A~D: 0~255 もしくは*)
 - 上記表記で A~D を*とすると、該当する 8 ビット分についてはすべての値に対応する
 - IPv6 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。
 - , を区切りとして複数設定することができる。
 - FQDN
 - 任意の文字列 (半角 255 文字以内。/ : は使用できない。 , は区切り文字として使われるため、使用できない)
 - * から始まる FQDN は * より後ろの文字列を後方一致条件として判断する 例えば *.example.co.jp は www.example.co.jp 、 mail.example.co.jp などと一致する
 - , を区切りとして複数設定することができる。
 - * (すべての IP アドレスまたは IPv6 アドレスに対応)
- [初期値]: -
- *dest_addr*: IP パケットの終点アドレス
 - [設定値]:
 - *src_addr* と同じ形式
 - 省略した場合は一個の * と同じ
 - [初期値]: -
- *protocol*: フィルタリングするパケットの種類
 - [設定値]:
 - 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
- [初期値]: -
- *src_port*: UDP、TCP のソースポート番号
 - [設定値]:
 - 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
submission	587

- 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。
- [初期値]: -
- *dest_port*: UDP、TCP のディスティネーションポート番号
 - [設定値]: *src_port* と同じ形式
 - [初期値]: -
- *application*: フィルタリング対象とするアプリケーション、またはカテゴリー
 - [設定値]:
 - アプリケーションを表すニーモニック
 - "@" で始まるカテゴリーを表すニーモニック
 - 上記文字列をカンマで区切った並び (10 個以内、アプリケーションとカテゴリーの混在が可能)
 - 省略時は 1 つの * と同じ
 - [初期値]: -
- *group_num*: グループ ID
 - [設定値]: **dpi group set** コマンドでグループ化したアプリケーションのグループ ID
 - [初期値]: -

[説明]

クラス分けのためのフィルターを設定する。

precedence 形式の場合、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。 *precedence* 値からクラスへの変換は、*mapping* オプションにより指定できる。例えば、以下の例では *precedence* 値=1 をクラス 8 に、 *precedence* 値=4 をクラス 3 に変換する。

`queue class filter 1 precedence mapping=1:8,4:3 ip *`

mapping オプション全体を省略した場合、あるいは *mapping* オプションは指定しているものの、その中で記述しなかった *precedence* 値については以下の表のような変換が行われる。

precedence 値	0	1	2	3	4	5	6	7
クラス	1	2	3	4	5	6	7	8

precedence 形式は RTX5000、RTX3500、RTX3000、RTX1500、RTX1220、RTX1210、RTX1200、RTX1100、RTX830、RTX810、SRT100 で指定可能である。 *mapping* オプションは RTX5000、RTX3500、RTX3000、RTX1220、RTX1210、RTX1200、RTX1100、RTX830、RTX810、SRT100 で指定可能である。

dscp 形式の場合、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。RTX5000、RTX3500、RTX3000、RTX1500、RTX1220、RTX1210、RTX1200 で指定可能である。

cos=cos 指定を行うと、フィルター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 RTX5000、RTX3500、RTX3000、RTX1500、RTX1220、RTX1210、RTX1200、RTX1100、RTX830、RTX810、RT107e 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、各インターフェースにおける **queue interface class filter list** コマンドで設定する。

`application`、または、`group_num` を指定した場合、DPI のアプリケーション識別結果を利用したクラス分けが行われる。アプリケーションの識別が完了したパケットは、直ちに指定のクラスに分類されるようになる。識別処理中のパケットや DPI がアクティベーション中で識別されなかったパケットは、DPI のフィルタにはマッチせず、通常の設定に従ってクラスに分類される。

`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 RTX5000、RTX3500、RTX3000 で指定可能。

RTX1200 Rev.10.01.47 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで `src_port` または `dest_port` に `submission` を指定可能。

[ノート]

RTX1500 は Rev.8.03 系で `dscp` パラメータを指定可能。

RTX1200 は Rev.10.01.29 以降で `dscp` パラメータを指定可能。

IPv6 アドレスは RTX1100 / RT107e Rev.8.03.92 以降、RTX3000 Rev.9.00.56 以降、SRT100 Rev.10.00.61 以降、RTX1200 Rev.10.01.42 以降、RTX810 Rev.11.01.09 以降のファームウェア、および、Rev.14.00 系以降のすべてのファームウェアで指定可能。

`application` パラメータ、および `group_num` パラメータは、RTX830 の Rev.15.02.13 以降で指定可能。

`src_addr` および `dest_addr` への FQDN の指定は RTX5000 Rev.14.00.26 以降、RTX3500 Rev.14.00.26 以降、RTX1210 Rev.14.01.26 以降、RTX830 Rev.15.02.03 以降、RTX810 Rev.11.01.28 以降、RTX1220 で指定可能。

[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
# queue class filter 12 4 ip dpi * * @audio_video
```

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

29.3 キューイングアルゴリズムタイプの選択

[書式]

queue interface type type [shaping-level=level]

queue pp type type

no queue interface type [type]

no queue pp type [type]

[設定値及び初期値]

- `interface`
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- `type`
 - [設定値]:

設定値	説明
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

設定値	説明
wfq	Weighted Fair Queue 形式のキューイング
shaping	帯域制御

- [初期値]: fifo
- *level*: 帯域速度の計算を行うレイヤー
- [設定値]:

設定値	説明
1	レイヤー 1
2	レイヤー 2

- [初期値]: 2

[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。

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。**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。PP インタフェースにだけ設定できる。

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、設定がいらぬということである。設定するところがないため、優先制御や帯域制御に比べて細かい調整はできないが、簡単にフロー間での帯域のバランスを図ることができる。PP インタフェースにだけ設定できる。

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。

shaping-level オプションは *TYPE* パラメーターに *priority* および *shaping* を指定しているときのみ指定可能。*shaping-level* に 1 を設定した場合、帯域速度の計算をブリアンブル、SFD(Start Frame Delimiter)、IFG(Inter Frame Gap)を含んだフレームサイズでおこなう。

[ノート]

RT107e	<i>type</i> パラメータに <i>fifo</i> 、 <i>priority</i> を指定することができる。
RT250i	<i>type</i> パラメータに <i>fifo</i> 、 <i>priority</i> 、 <i>cbq</i> 、 <i>wfq</i> を指定することができる。
RTX1220、RTX1210、RTX830、RTX810、SRT100	<i>type</i> パラメータに <i>fifo</i> 、 <i>priority</i> 、 <i>shaping</i> を指定することができる。
上記以外の機種	<i>type</i> パラメータに <i>fifo</i> 、 <i>priority</i> 、 <i>cbq</i> 、 <i>wfq</i> 、 <i>shaping</i> を指定することができる。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

shaping-level オプションは RTX1200 Rev.10.01.59 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.18 以降、RTX1210 Rev.14.01.09 以降のファームウェア、および、Rev.15.02 系以降のすべてのファームウェアで指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

29.4 MP インタリーブの設定

[書式]

```
ppp mp interleave [delay] switch
no ppp mp interleave [[delay] switch]
```

[設定値及び初期値]

- *delay*
 - [設定値]: 遅延 (ミリ秒)
 - [初期値]: 30
- *switch*
 - [設定値]:

設定値	説明
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

- [初期値]: off

[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
```

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RT250i

29.5 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]
```

[設定値及び初期値]

- *interface*

- [設定値]: LAN インタフェース名、WAN インタフェース名
- [初期値]: -
- *filter_list*
 - [設定値]: 空白で区切られたクラスフィルタの並び
 - [初期値]: -

[説明]

指定した LAN インタフェース、WAN 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。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

29.6 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...]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *len1..lenN*
 - [設定値]:
 - クラス 1 からクラス 16 のキュー長 (1..10000; RTX1500 の場合は 1..2000)
 - RTX5000、RTX3500、RTX3000 の場合はクラス 1 からクラス 100 のキュー長 (1..10000)
 - [初期値]:
 - 600 (RTX5000、RTX3500)
 - 200 (RTX3000、RTX1220、RTX1210、RTX1200、RTX830、RTX810)
 - 40 (上記以外)
- *len1..len16*
 - [設定値]: クラス 1 からクラス 16 のキュー長 (1..10000; RTX1500 の場合は 1..2000)
 - [初期値]: 20
- *dthreshold-mid*
 - [設定値]: 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%)
 - [初期値]: 75%
- *dthreshold-high*
 - [設定値]: 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%)
 - [初期値]: 50%

[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、RTX5000、RTX3500、RTX3000、RTX1500、RTX1220、RTX1210、RTX1200 で指定可能である。

[ノート]

dthreshold-mid、*dthreshold-high* パラメータは RTX5000、RTX3500、RTX3000、RTX1210、RTX1220、および、Rev. 8.03 系以降の RTX1500、Rev.10.01.29 系以降の RTX1200 で指定可能。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

RTX5000、RTX3500、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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

29.7 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...]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *primary_class*
 - [設定値]:
 - 第 1 階層クラス (1..100)
 - 省略時、すべての第 1 階層クラスに從属する第 2 階層クラスのキュー長を一律に指定する
 - [初期値]: -
- *len1...len4*
 - [設定値]: クラス 1 からクラス 4 のキュー長 (1..10000)
 - [初期値]:
 - 600 (RTX5000、RTX3500)
 - 200 (上記以外)

[説明]

インタフェースに対して、指定した第 1 階層クラスに從属する第 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。

[適用モデル]

RTX5000, RTX3500, RTX3000

29.8 デフォルトクラスの設定

[書式]

```
queue interface default class class
```

```
queue pp default class class
```

```
queue tunnel default class class
```

```
no queue interface default class [class]
```

```
no queue pp default class [class]
```

```
no queue tunnel default class [class]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名

- [初期値]: -
- *class*
 - [設定値]: クラス (1..16; RTX5000、RTX3500、RTX3000 の場合は 1..100)
 - [初期値]: 2

[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。

[ノート]

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

第 3、第 6 書式は RTX5000 / RTX3500 は Rev.14.00.32 以降、RTX1210 は Rev.14.01.40 以降、RTX830 は Rev.15.02.20 以降のファームウェア、および、RTX1220 で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

29.9 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
queue tunnel default class secondary [primary=primary_class] class
no queue interface default class secondary [primary=primary_class...]
no queue tunnel default class secondary [primary=primary_class...]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *primary_class*
 - [設定値]:
 - 第 1 階層クラス (1..100)
 - 省略時、すべての第 1 階層クラスに從属する第 2 階層クラスのデフォルトクラスを一律に指定する
 - [初期値]: -
- *class*
 - [設定値]: クラス (1..4)
 - [初期値]: 2

[説明]

指定した第 1 階層クラスに從属する第 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。

[ノート]

第 2、第 4 書式は RTX5000 / RTX3500 は Rev.14.00.32 以降のファームウェアで使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000

29.10 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] [packetize=packetize]
no queue interface class property class [...]
no queue pp class property class [bandwidth=bandwidth...]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *class*
 - [設定値]: クラス (1..16; RTX5000、RTX3500、RTX3000 の場合は 1..100)
 - [初期値]: -
- *bandwidth*
 - [設定値]:
 - 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。
 - 'ngn' を設定した場合はデータコネク ト拠点間接続の接続時に決めた帯域に設定される。
 - [初期値]: -
- *parent*
 - [設定値]: 親クラスの番号 (0..16)
 - [初期値]: 0
- *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
 - [設定値]:

設定値	説明
on	借りる
off	借りない

- [初期値]: on
- *maxburst*
 - [設定値]: 連続送信できる最大バイト数 (1..10000)
 - [初期値]: 20
- *minburst*
 - [設定値]: 安定送信中に連続送信できる最大バイト数 (1..10000)
 - [初期値]: maxburst/10
- *packetize*
 - [設定値]: クラスで流れるパケットの平均パケット長 (1..10000)
 - [初期値]: 512
- *type*
 - [設定値]:

設定値	説明
priority	優先制御クラスとして使用することを明示する。

- [初期値]: -

[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。'ngn' を指定した場合は、データコネク ト拠点間接続で接続時に決まる帯域に自動的 に設定される。複数のデータコネク ト拠点間接続を利用する場合は、トンネルインタフェース毎にクラスを分ける 必要がある。また、**tunnel ngn interface** コマンドで使用する LAN インタフェースを設定する必要がある。 *bandwidth* パラメータに 'ngn' を指定できるのは、RTX3000 Rev.9.00.56 以降、RTX1200 Rev.10.01.42 以降、RTX810 Rev.11.01.09 以降のファームウェア、および、Rev.14.00 系以降のすべてのファームウェアである。

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ません。Dynamic Traffic Control は RTX5000、RTX3500、RTX3000、RTX1500、RTX1220、RTX1210、RTX1200、RTX1100、RTX830、RTX810、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 RTX5000、RTX3500、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ならない。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 では **queue pp class property** は指定できない。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, SRT100

29.11 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...*]

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *class*
 - [設定値]: DCC を有効にするクラス (1..16; RTX5000、RTX3500 の場合は 1..100)
 - [初期値]: -
- *ip_address*
 - [設定値]:

設定値	説明
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)

- [初期値]: -
- *option = value 列*
 - [設定値]:

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	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)
	10..604800	
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	制御されていないことを通知しない

- [初期値]:
 - watch=source
 - threshold=70%,30
 - time=600
 - mode=forced
 - notice=on

[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越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ませんが、**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.10.01 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.10.01 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、かつ、Web GUI 機能を搭載している機種で使用可能。

[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。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

第 30 章

連携機能

30.1 連携動作を行うか否かの設定

[書式]

cooperation *type* *role* *sw*

no cooperation *type* *role* [*sw*]

[設定値及び初期値]

- *type* : 連携動作タイプ

- [設定値] :

設定値	説明
bandwidth-measuring	回線帯域検出
load-watch	負荷監視通知

- [初期値] : -

- *role* : 連携動作での役割

- [設定値] :

設定値	説明
server	サーバー側動作
client	クライアント側動作

- [初期値] : -

- *sw*

- [設定値] :

設定値	説明
on	機能を有効にする
off	機能を無効にする

- [初期値] : すべての連携動作で off

[説明]

連携動作の機能毎の動作を設定する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

30.2 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*]

[設定値及び初期値]

- *port*

- [設定値] : ポート番号

- [初期値] : 59410

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

30.3 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]]

[設定値及び初期値]

- *id*
 - [設定値]: 相手先 ID 番号 (1..100)
 - [初期値]: -
- *role*: 連携動作での相手側の役割
 - [設定値]:

設定値	説明
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

- [初期値]: -
- *address*
 - [設定値]: 連携動作の相手側 IP アドレス、FQDN または 'any'
 - [初期値]: -
- *option*: オプション
 - [設定値]:

設定値	説明
apply	測定結果を LAN インタフェースまたは WAN 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 インタフェースまたは WAN 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

- [初期値]:
 - apply=on
 - port=59410
 - initial-speed=10000000
 - interval=3600
 - retry-interval=3600
 - sensitivity=high
 - syslog=off
 - number=30

[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、または WAN インタフェースの `speed wan1` 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、または `queue wan1 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。

`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。 WAN インタフェースが設定されている場合には、`speed wan1` 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 wan1 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。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

30.4 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]]
```

[設定値及び初期値]

- `id`
 - [設定値]: 相手先 ID 番号 (1..100)
 - [初期値]: -
- `role`: 連携動作での相手側の役割
 - [設定値]:

設定値	説明
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

- [初期値]: -
- `address`

- [設定値]: 連携動作の相手側 IP アドレス、FQDN または 'any'
- [初期値]: -
- *option*: オプション
- [設定値]:

設定値	説明
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

- [初期値]:
 - port=59410
 - syslog=off
 - apply=on
 - register=off
 - register-interval=1200
 - register-time=3600

[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]

role パラメータで *client* を設定する場合のみ *trigger* オプションを利用でき、*client* を設定する場合は *trigger* オプションの設定は必須である。また、*server* を設定する場合のみ *control* オプションを利用でき、*server* を設定する場合は *control* オプションの設定は必須である。

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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

30.5 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=value*]**no cooperation load-watch trigger** *id* [*point* high=*high* [, *count*] low=*low* [, *count*] [*option=value*]]

[設定値及び初期値]

• *id*

- [設定値]: 相手先 ID 番号 (1-100)

- [初期値]: -

• *point*: 負荷監視対象ポイント

- [設定値]:

• *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

<i>interface</i>	インタフェース名 (LAN, TUNNEL (tunnel <i>tunnel_num</i>), PP (pp <i>peer_num</i>))
------------------	--

• *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を監視する。値は発生回数で指定する

<i>interface</i>	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

<i>interface</i>	インタフェース名 (LAN, TUNNEL (tunnel <i>tunnel_num</i>), PP (pp <i>peer_num</i>))
<i>class</i>	クラス番号 (LAN インタフェースの場合)

- [初期値]: -

• *high*

- [初期値]: 高負荷検出閾値

• *low*

- [設定値]: 負荷減少検出閾値

- [初期値]: -

• *count*

- [設定値]: 通知を送出するに至る検出回数 (1-100)、省略時は 3

- [初期値]: -

• *option*: オプション

- [設定値]:

設定値	説明
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'

- [初期値]: -

[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。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

30.6 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] [option=value]
```

```
no cooperation load-watch control id [high=high [raise=raise] low=low [lower=lower] [option=value]]
```

[設定値及び初期値]

- *id*
 - [設定値]: 相手先 ID 番号 (1-100)
 - [初期値]: -
- *high*
 - [設定値]: bit/sec、帯域上限値
 - [初期値]: -
- *raise*
 - [設定値]:
 - %, 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%
 - [初期値]: -
- *low*
 - [設定値]: bit/sec、帯域下限値
 - [初期値]: -
- *lower*
 - [設定値]:

- %、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%
- [初期値]:-
- *option* : オプション
- [設定値]:

設定値	説明
interval	帯域を増加させる間隔(1-65535)[sec]、省略時は 10[sec]
interface	帯域を変化させる LAN インタフェース
class	帯域を変化させるクラス

- [初期値]:-

[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。

帯域制御機能が実装されている機種でのみ *option* に *class* を指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

30.7 連携動作の手動実行

[書式]

cooperation bandwidth-measuring go id

cooperation load-watch go id type

[設定値及び初期値]

- bandwidth-measuring : 回線帯域検出
 - [初期値]:-
- load-watch : 負荷監視通知
 - [初期値]:-
- *id*
 - [設定値]: 相手先 ID 番号 (1-100)
 - [初期値]:-
- *type* : パケットタイプ
 - [設定値]:

設定値	説明
lower	負荷減少検出パケット
raise	高負荷検出パケット

- [初期値]:-

[説明]

手動で連携動作を実行する。

[ノート]

bandwidth-measuring を指定した場合、測定結果がログに表示される。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、指定した相手先に対して負荷監視のトリガで送出されるパケットと同じパケットが送出される。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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

第 31 章

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。

31.1 OSPF の有効設定

[書式]

```
ospf configure refresh
```

[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ならない。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

31.2 OSPF の使用設定

[書式]

```
ospf use use
```

```
no ospf use [use]
```

[設定値及び初期値]

- use

- [設定値]:

設定値	説明
on	OSPF を使用する
off	OSPF を使用しない

- [初期値]: off

[説明]

OSPF を使用するか否かを設定する。

[ノート]

以下のファームウェアではセカンダリアドレスを割り当てたインタフェースで OSPF を使用しても正しく経路変換ができない。

RT250i では全てのリビジョン

RTX1500、RTX1100、RT107e では Rev.8.03.90、およびそれ以前

RTX3000 では Rev.9.00.48、およびそれ以前

SRT100 では Rev.10.00.56、およびそれ以前

RTX1200 では Rev.10.01.29、およびそれ以前

以下の機能はまだサポートされていない。

- NSSA (RFC1587)
- OSPF over demand circuit (RFC1793)
- OSPF MIB

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

31.3 OSPF による経路の優先度設定

[書式]

```
ospf preference preference
no ospf preference [preference]
```

[設定値及び初期値]

- *preference*
 - [設定値]: OSPF による経路の優先度 (1 以上の数値)
 - [初期値]: 2000

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

31.4 OSPF のルーター ID 設定

[書式]

```
ospf router id router-id
no ospf router id [router-id]
```

[設定値及び初期値]

- *router_id*
 - [設定値]: IP アドレス
 - [初期値]: -

[説明]

OSPF のルーター ID を指定する。

[ノート]

ルーター ID が本コマンドで設定されていないときは、以下のインタフェースに付与されているプライマリ IPv4 アドレスのいずれかが自動的に選択され、ルーター ID として使用させれる。

- LAN インタフェース
- LOOPBACK インタフェース
- PP インタフェース

なお、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。意図しない IP アドレスがルーター ID として使用されることを防ぐため、本コマンドにより明示的にルーター ID を指定することが望ましい。

OSPF と BGP-4 とを併用する場合、本コマンドか `bgp router id` コマンドのいずれか一方を設定する。以下のファームウェアでは、本コマンドと `bgp router id` コマンドの両方を設定することができるが、必ず同一のルーター ID を指定する必要がある。

機種	リビジョン
RTX1220	すべてのリビジョン
RTX1210	Rev.14.01.16
RTX5000	Rev.14.00.21
RTX3500	Rev.14.00.21

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

31.5 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...]
```

[設定値及び初期値]

- *filter_num*
 - [設定値]: **ospf export filter** コマンドのフィルタ番号
 - [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

[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または **filter** キーワード以降を省略した場合には、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]

フィルタ番号は 100 個まで設定できる。

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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

31.6 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...]
```

[設定値及び初期値]

- *protocol*: OSPF の経路テーブルに導入する外部プロトコル
 - [設定値]:

設定値	説明
static	静的経路
rip	RIP
bgp	BGP

- [初期値]: -
- *filter_num*
 - [設定値]: フィルタ番号
 - [初期値]: -

[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

[ノート]

フィルタ番号は、RTX3000 Rev.9.00.47 以降、および、RTX5000、RTX3500 は 300 個、他の機種は 100 個まで設定できる。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

31.7 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 [...]
```

[設定値及び初期値]

- filter_num
 - [設定値]: フィルタ番号
 - [初期値]: -
- nr: フィルタの解釈の方法
 - [設定値]:

設定値	説明
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	フィルタに該当した経路を導入する

- [初期値]: -
- kind: フィルタ種別
 - [設定値]:

設定値	説明
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

- [初期値]: -
- ip_address/mask
 - [設定値]: 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
 - [初期値]: -

[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 ospf** 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
```

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

31.8 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...*]]

[設定値及び初期値]

- *filter_num*
 - [設定値]: フィルタ番号
 - [初期値]: -
- *nr*: フィルタの解釈の方法
 - [設定値]:

設定値	説明
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	フィルタに該当した経路を広告する

- [初期値]: -
- *kind*
 - [設定値]:

設定値	説明
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

- [初期値]: -
- *ip_address/mask*
 - [設定値]: 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
 - [初期値]: -
- *parameter*: 外部経路を広告する場合のパラメータ
 - [設定値]:

設定値	説明
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)

- [初期値]: -

[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まらないため、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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

31.9 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]]
```

[設定値及び初期値]

- *area*

- [設定値]:

設定値	説明
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

- [初期値]: -

- *auth*

- [設定値]:

設定値	説明
text	プレーンテキスト認証
md5	MD5 認証

- [初期値]: 認証は行わない

- *stub*: スタブエリアであることを指定する。

- [初期値]: スタブエリアではない

- *cost*

- [設定値]: 1 以上の数値

- [初期値]: -

[説明]

OSPF エリアを設定する。

cost は 1 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ぬ。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

31.10 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]
```

[設定値及び初期値]

- *area*
 - [設定値]:

設定値	説明
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

- [初期値]: -
- *network*
 - [設定値]: IP アドレス
 - [初期値]: -
- *mask*
 - [設定値]: ネットマスク長
 - [初期値]: -

[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、*network/mask* で指定したネットワーク範囲内の個々の経路を *network/mask* に要約して広告する。*restrict* キーワードを指定した場合は、*network/mask* の範囲内の経路は要約した経路も含めて一切他のエリアに広告しなくなる。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

31.11 スタブ的接続の広告

[書式]

```
ospf area stubhost area host [cost cost]
no ospf area stubhost area host
```

[設定値及び初期値]

- *area*
 - [設定値]:

設定値	説明
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

- [初期値]: -
- *host*
 - [設定値]: IP アドレス
 - [初期値]: -
- *cost*
 - [設定値]: 1 以上の数値
 - [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

31.12 仮想リンク設定**[書式]**

```
ospf virtual-link router_id area [parameters...]
no ospf virtual-link router_id [area [parameters...]]
```

[設定値及び初期値]

- *router_id*
 - [設定値]: 仮想リンクの相手のルーター ID
 - [初期値]: -
- *area*
 - [設定値]:

設定値	説明
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

- [初期値]: -
- *parameters*
 - [設定値]: NAME=VALUE の列
 - [初期値]:
 - 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

[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。(1..)
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。(1..)
hello-interval	秒数	HELLO パケットの送信間隔を秒単位で設定する。(1..)
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。(1..)
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。(8 文字以内)

NAME	VALUE	説明
md5key	"(ID),(KEY)"	MD5 認証の認証鍵を表す ID と鍵文字列 KEY 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 OSPFHELLO 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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

31.13 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...]]
```

[設定値及び初期値]

- interface
 - [設定値]: LAN インタフェース名、LOOPBACK インタフェース名
 - [初期値]: -
- area
 - [設定値]:

設定値	説明
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

- [初期値]: インタフェースは OSPF エリアに属していない
- parameters
 - [設定値]: NAME=VALUE の列
 - [初期値]:

- type=broadcast(LAN インタフェース設定時)
- type=point-to-point(PP または TUNNEL インタフェース設定時)
- type=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)
- hello-interval=10 秒 (point-to-point 設定時)
- hello-interval=30 秒 (non-broadcast 設定時)
- hello-interval=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

[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-multipoint	ポイント・マルチポイント
	non-broadcast	NBMA
passive		インタフェースに対して、OSPF パケットを送信しない。該当インタフェースに他の OSPF ルーターがない場合に設定する。
cost	コスト	<p>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)</p> <ul style="list-style-type: none"> • COST=100000/S <p>TUNNEL インタフェースの場合は、1562 がデフォルト値となる。</p>
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。(1..)

NAME	VALUE	説明
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。(1..)
hello-interval	秒数	HELLO パケットの送信間隔を秒単位で設定する。(1..)
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。(1..)
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。(1..)
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。(8 文字以内)
md5key	"(ID),(KEY)"	MD5 認証の認証鍵を表す ID と鍵文字列 KEY 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

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、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 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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

31.14 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]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *ip_address*
 - [設定値]: 近隣ルーターの IP アドレス
 - [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

31.15 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

[設定値及び初期値]

- *merge*
- [設定値]:

設定値	説明
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

- [初期値]: on

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

31.16 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...]

[設定値及び初期値]

- *log*
- [設定値]:

設定値	説明
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

- [初期値]: OSPF のログは記録しない。

[説明]

指定した種類のログを INFO レベルで記録する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

31.17 インタフェースの状態変化時、OSPF に外部経路を反映させる時間間隔の設定

[書式]

ospf reric interval *time*

no ospf reric interval [*time*]

[設定値及び初期値]

- *time*
 - [設定値]: 秒数 (1 以上の数値)
 - [初期値]: 1

[説明]

ルーターのインタフェースの状態が変化したとき、OSPF に外部経路を反映させる時間の間隔を設定する。

OSPF ではインタフェースの状態変化を 1 秒間隔で監視し、変化があれば最新の外部経路を自身に反映させるが、インタフェースの状態変化が連続して発生するときは、複数の外部経路の反映処理が *time* で指定した秒数の間隔でまとめて行われるようになる。

[ノート]

複数のトンネルが一斉にアップすることがあるような環境では、本コマンドの値を適切に設定することで、OSPF や BGP の外部経路の導入によるシステムへの負荷を軽減することができる。

本コマンドの設定値は、BGP への外部経路の反映にも影響する。本コマンドと **bgp reric interval** コマンドの設定値が食い違う場合には、本コマンドの設定値が優先して適用される。

本コマンドの設定は、経路の変化や IP アドレスの変化に対する OSPF や BGP の動作には関係しない。また本コマンドの設定値は、**ospf configure refresh** コマンドを実行しなくても即時反映される。

RTX1210 は Rev.14.01.16 以降で使用可能。

RTX5000、RTX3500 は Rev.14.00.21 以降で使用可能。

RTX1200 は Rev.10.01.71 以降で使用可能。

RTX810 は Rev.11.01.28 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

第 32 章

BGP

32.1 BGP の起動の設定

[書式]

```
bgp use use
no bgp use [use]
```

[設定値及び初期値]

- *use*
 - [設定値]:

設定値	説明
on	起動する
off.	起動しない

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

32.2 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... ]
```

[設定値及び初期値]

- *ip_address/mask*
 - [設定値]: IP アドレス/ネットマスク
 - [初期値]: -
- *filter_num*
 - [設定値]: フィルタ番号 (1..2147483647)
 - [初期値]: -

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

32.3 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 ...]
```

[設定値及び初期値]

- *filter_num*

- [設定値]: フィルタ番号 (1..2147483647)
- [初期値]: -
- *protocol*
 - [設定値]:

設定値	説明
static	静的経路
rip	RIP
ospf	OSPF
bgp	BGP
all	すべてのプロトコル

- [初期値]: -
- *kind*
 - [設定値]:

設定値	説明
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

- [初期値]: -
- *ip_address/mask*
 - [設定値]: IP アドレス/ネットマスク
 - [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

32.4 AS 番号の設定

[書式]

```
bgp autonomous-system as
no bgp autonomous-system [as]
```

[設定値及び初期値]

- *as*
 - [設定値]: AS 番号 (1..65535)
 - [初期値]: -

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

32.5 ルーター ID の設定**[書式]**

```
bgp router id ip_address
no bgp router id [ip_address]
```

[設定値及び初期値]

- *ip_address*
 - [設定値]: IP アドレス
 - [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。

[説明]

ルーター ID を設定する。

[ノート]

ルーター ID が本コマンドで設定されていないときは、以下のインタフェースに付与されているプライマリ IPv4 アドレスのいずれかが自動的に選択され、ルーター ID として使用させれる。

- LAN インタフェース
- LOOPBACK インタフェース
- PP インタフェース

なお、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。意図しない IP アドレスがルーター ID として使用されることを防ぐため、本コマンドにより明示的にルーター ID を指定することが望ましい。

OSPF と BGP-4 とを併用する場合、本コマンドか `ospf router id` コマンドのいずれか一方を設定する。以下のファームウェアでは、本コマンドと `ospf router id` コマンドの両方を設定することができるが、必ず同一のルーター ID を指定する必要がある。

機種	リビジョン
RTX1220	すべてのリビジョン
RTX1210	Rev.14.01.16
RTX5000	Rev.14.00.21
RTX3500	Rev.14.00.21

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

32.6 BGP による経路の優先度の設定**[書式]**

```
bgp preference preference
no bgp preference [preference]
```

[設定値及び初期値]

- *preference*
 - [設定値]: 優先度 (1..2147483647)
 - [初期値]: 500

[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

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

32.7 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_regex" filter filter_num ...
no bgp export remote_as [filter filter_num ...]
no bgp export aspath seq ["aspath_regex" [filter filter_num ...]]

```

[設定値及び初期値]

- *remote_as*
 - [設定値]: 相手の AS 番号 (1..65535)
 - [初期値]: -
- *seq*
 - [設定値]: AS パスを指定したときの評価順序 (1..65535)
 - [初期値]: -
- *aspath_regex*
 - [設定値]: 正規表現
 - [初期値]: -
- *filter_num*
 - [設定値]: フィルタ番号 (1..2147483647)
 - [初期値]: -

[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_regex 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_regex* 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_regex 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_regex* 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。

フィルタ番号は、100 個まで設定できる。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

32.8 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]]
```

[設定値及び初期値]

- filter_num*
 - [設定値]: フィルタ番号 (1..2147483647)
 - [初期値]: -
- kind*
 - [設定値]:

設定値	説明
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

- [初期値]: -
- ip_address/mask*
 - [設定値]:

設定値	説明
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

- [初期値]: -
- parameter* : TYPE=VALUE の組
 - [設定値]:

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

- [初期値]: 0

[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。

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

32.9 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 ...]
```

[設定値及び初期値]

- *remote_as*
 - [設定値]: 相手の AS 番号 (1..65535)
 - [初期値]: -
- *protocol*
 - [設定値]:

設定値	説明
static	静的経路
rip	RIP
ospf	OSPF
bgp	BGP
aggregate	集約経路

- [初期値]: -
- *from_as*
 - [設定値]: 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)
 - [初期値]: -
- *filter_num*
 - [設定値]: フィルタ番号 (1..2147483647)
 - [初期値]: -

[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。

[ノート]

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。
 フィルタ番号は、100 個まで設定できる。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

32.10 BGP の設定の有効化

[書式]

bgp configure refresh

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

32.11 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 ...]*]

[設定値及び初期値]

- *filter_num*
 - [設定値]: フィルタ番号 (1..2147483647)
 - [初期値]: -
- *kind*
 - [設定値]:

設定値	説明
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

- [初期値]: -
- *ip_address/mask*

- [設定値]:

設定値	説明
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

- [初期値]: -
- *parameter*: TYPE=VALUE の組
- [設定値]:

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)
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

- [初期値]:
 - preference=100

[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。

[ノート]

`preference` は、RTX3000 Rev.9.00.56 以降、RTX1200 Rev.10.01.42 以降、RTX810 Rev.11.01.09 以降のファームウェア、および、Rev.14.00 系以降のすべてのファームウェアで使用可能。それ以外の機種、リビジョンでは指定できない。

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

32.12 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* *remote_address* [*parameter...*]]

[設定値及び初期値]

- *neighbor_id*
 - [設定値]: 近隣ルーターの番号 (1..2147483647)
 - [初期値]: -
- *remote_as*
 - [設定値]: 相手の AS 番号 (1..65535)
 - [初期値]: -
- *remote_address*
 - [設定値]: 相手の IP アドレス
 - [初期値]: -
- *parameter*: TYPE=VALUE の組
 - [設定値]:

TYPE	VALUE	説明
hold-time	off、秒数	キープアライブの送信間隔 (3..28,800 秒)
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
ignore-capability	on または off	capability を無視するか否か

- [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
 - ignore-capability=off

[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` では、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。

RTX3000 Rev.9.00.56 以降、RTX1200 Rev.10.01.36 以降、RTX810 Rev.11.01.06 以降のファームウェア、および、Rev.14.00 系以降のすべてのファームウェアでは、本コマンドは最大で 32 個までしか設定することはできない。

RT250i では `local-address` は指定できない。

`ignore-capability` は RTX810 Rev.11.01.19 以降のファームウェア、および、Rev.14.00 系以降のすべてのファームウェアで指定できる。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

32.13 BGP で使用する TCP MD5 認証の事前共有鍵の設定

[書式]

```
bgp neighbor pre-shared-key neighbor_id text text_key
no bgp neighbor pre-shared-key neighbor_id [text text_key]
```

[設定値及び初期値]

- `neighbor_id`
 - [設定値]: 近隣ルーターの番号 (1...2147483647)
 - [初期値]: -
- `text_key`
 - [設定値]: ASCII 文字列で表した鍵 (80 文字以内)
 - [初期値]: -

[説明]

BGP で使用する TCP MD5 認証の事前共有鍵を設定する。設定した事前共有鍵が一致するピア間のみ、BGP のコネクションが成立する。

[ノート]

RTX1210 は Rev.14.01.11 以降で使用可能。

RTX5000、RTX3500 は Rev.14.00.18 以降で使用可能。

RTX810 は Rev.11.01.28 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830, RTX810

32.14 BGP のログの設定

[書式]

```
bgp log log [log]
no bgp log [log ...]
```

[設定値及び初期値]

- `log`
 - [設定値]:

設定値	説明
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

- [初期値]: ログを記録しない。

[説明]

指定した種類のログを INFO レベルで記録する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

32.15 BGP で強制的に経路を広告する**[書式]**

```
bgp force-to-advertise remote_as ip_address/mask [parameter ...]
no bgp force-to-advertise remote_as ip_address/mask [parameter ...]
```

[設定値及び初期値]

- *remote_as*
 - [設定値]: 相手の AS 番号
 - [初期値]: -
- *ip_address/mask*
 - [設定値]: IP アドレス/ネットマスク
 - [初期値]: -
- *parameter*
 - [設定値]:
 - 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
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

- [初期値]: preference=100

[説明]

本コマンドで設定した経路がルーティングテーブルに存在しない場合でも、指定された AS 番号のルーターに対して BGP 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。設定したコマンドは bgp configure refresh コマンドを実行したときに有効になる。

[ノート]

RTX5000、RTX3500 は Rev.14.00.18 以降で使用可能。

RTX1210 は Rev.14.01.11 以降で使用可能。

RTX810 は Rev.11.01.25 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830, RTX810

32.16 インタフェースの状態変化時、BGP に外部経路を反映させる時間間隔の設定**[書式]**

```
bgp reric interval time
no bgp reric interval [time]
```

[設定値及び初期値]

- *time*
 - [設定値]: 秒数 (1 以上の数値)
 - [初期値]: 1

[説明]

ルーターのインタフェースの状態が変化するとき、**bgp** に外部経路を反映させる時間の間隔を設定する。

BGP ではインタフェースの状態変化を 1 秒間隔で監視し、変化があれば最新の外部経路を自身に反映させるが、インタフェースの状態変化が連続して発生するときは、複数の外部経路の反映処理が *time* で指定した秒数の間隔でまとめて行われるようになる。

[ノート]

複数のトンネルが一斉にアップすることがあるような環境では、本コマンドの値を適切に設定することで、OSPF や BGP の外部経路の導入によるシステムへの負荷を軽減することができる。
本コマンドの設定値は、OSPF への外部経路の反映にも影響する。本コマンドと **ospf reric interval** コマンドの設定値が食い違う場合には、**ospf reric interval** コマンドの設定値が優先して適用される。
本コマンドの設定は、経路の変化や IP アドレスの変化に対する OSPF や BGP の動作には関係しない。また本コマンドの設定値は、**bgp configure refresh** コマンドを実行しなくても即時反映される。

RTX1210 は Rev.14.01.16 以降で使用可能。
RTX5000、RTX3500 は Rev.14.00.21 以降で使用可能。
RTX1200 は Rev.10.01.71 以降で使用可能。
RTX810 は Rev.11.01.28 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

32.17 BGP の最適経路選択における MED 属性が付加されていない経路のデフォルトの MED 値の設定

[書式]

```
bgp default med med
no bgp default med [med]
```

[設定値及び初期値]

- *med*
 - [設定値]: MED 値 (1..2147483647)
 - [初期値]: 2147483647

[説明]

BGP の最適経路選択で、MED 属性が付加されていない経路に対するデフォルトの MED 値を設定する。
本コマンドが設定されていない場合、MED 属性が付加されていない経路は最大の MED 値(2147483647)を持つことになり、優先度は最低となる。
本コマンドの設定は、MED 属性が付加されている経路には影響しない。

[ノート]

RTX5000、RTX3500 は Rev.14.00.32 以降で使用可能。
RTX1210 は Rev.14.01.36 以降で使用可能。
RTX830 は Rev.15.02.15 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

第 33 章

IPv6

33.1 共通の設定

33.1.1 IPv6 パケットを扱うか否かの設定

[書式]

```
ipv6 routing routing
no ipv6 routing [routing]
```

[設定値及び初期値]

- *routing*
 - [設定値]:

設定値	説明
on	処理対象として扱う
off	処理対象として扱わない

- [初期値]: on

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

33.1.2 IPv6 インタフェースのリンク MTU の設定

[書式]

```
ipv6 interface mtu mtu0
ipv6 pp mtu mtu1
ipv6 tunnel mtu mtu2
no ipv6 interface mtu [mtu0]
no ipv6 pp mtu [mtu1]
no ipv6 tunnel mtu [mtu2]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *mtu*
 - [設定値]: MTU の値 (1280..1500 ; RTX3000 の LAN1 / LAN2、および、RTX5000、RTX3500 の LAN インタフェースは 1280..9578)
 - [初期値]:
 - mtu0=1500
 - mtu1=1500
 - mtu2=1280

[説明]

IPv6 インタフェースの MTU の値を設定する

[ノート]

ipv6 tunnel mtu コマンドは RTX5000 / RTX3500 Rev.14.00.29 以降、RTX1210 Rev.14.01.34 以降、RTX830 Rev.15.02.10 以降、RTX1220 で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

33.1.3 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]
```

[設定値及び初期値]

- interface
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- mss
 - [設定値]:

設定値	説明
536..1440	MSS の最大長
auto	自動設定
off	設定しない

- [初期値]:
 - auto(RTX1200 Rev.10.01.75 以降、RTX810 Rev.11.01.31 以降、RTX1210 Rev.14.01.26 以降、RTX830 Rev.15.02.03 以降、RTX1220)
 - off(上記以外)

[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、ipv6 tunnel tcp mss limit コマンドはない。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

33.1.4 TCP ウィンドウ・スケール・オプションを変更する

[書式]

```
ipv6 interface tcp window-scale sw
ipv6 pp tcp window-scale sw
ipv6 tunnel tcp window-scale sw
no ipv6 interface tcp window-scale [...]
```

```
no ipv6 pp tcp window-scale [...]
no ipv6 tunnel tcp window-scale [...]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *sw*
 - [設定値]:

設定値	説明
off	何もしない
remove	TCP ウィンドウ・スケール・オプションを削除する

- [初期値]: off

[説明]

インターフェースを通過する TCP パケットのウィンドウ・スケール・オプションを強制的に変更する。
remove を指定すると、ウィンドウ・スケール・オプションが有効になっていた場合には、無効にして転送する。

[ノート]

RTX5000、RTX3500 は Rev.14.00.21 以降で使用可能。
RTX1210 は Rev.14.01.16 以降で使用可能。
RTX810 は Rev.11.01.28 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830, RTX810

33.1.5 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
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	破棄する
off	破棄しない

- [初期値]: on

[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]

RTX3000 は、Rev.9.00.24 以降で使用可能。
RT250i は、Rev.8.02.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

33.1.6 IPv6 ファストパス機能の設定

[書式]

```
ipv6 routing process process
```


no ipv6 routing process

[設定値及び初期値]

- *process*
 - [設定値]:

設定値	説明
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

- [初期値]: fast

[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。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

33.1.7 ICMPv6 でアドレス解決が完了するまでに送信を保留しておくことのできるパケット数の設定

[書式]

ipv6 interface icmp-nd queue length len
no ipv6 interface icmp-nd queue length [len]

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インターフェース名
 - [初期値]: -
- *len*
 - [設定値]: キュー長 (0..10000)
 - [初期値]: 200

[説明]

ICMPv6 の Neighbor Discovery のアドレス解決が完了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、アドレス解決が完了するかタイムアウトにより解決できないことが確定するまで、インター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。

[ノート]

RTX5000 は Rev.14.00.26 以降、RTX3500 は Rev.14.00.26 以降、RTX1210 は Rev.14.01.33 以降、RTX830 は Rev.15.02.09 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

33.1.8 近隣キャッシュの最大エントリ数の設定

[書式]

ipv6 interface neighbor cache max entry num
no ipv6 interface neighbor cache max entry [num]

[設定値及び初期値]

- *interface*

- [設定値]: LAN インタフェース名
- [初期値]: -
- *num*
 - [設定値]: 最大エントリー数 (256...20480)
 - [初期値]:
 - 1024

[説明]

インタフェースごとに近隣キャッシュの最大エントリー数を設定する。
近隣キャッシュのエントリー数が、設定した最大エントリー数に達した場合は、古い近隣キャッシュを削除する。
本コマンド実行時、現在の近隣キャッシュのエントリー数が最大エントリー数を超える場合は、古い近隣キャッシュを削除する。

[ノート]

RTX5000、RTX3500 は Rev.14.00.32 以降で使用可能。
RTX1210 は Rev.14.01.40 以降で使用可能。
RTX830 は Rev.15.02.20 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

33.1.9 IPv6 のフラグメントパケットを再構成するために保持しておく時間を設定

[書式]

```
ipv6 reassembly hold-time sec
no ipv6 reassembly hold-time [sec]
```

[設定値及び初期値]

- *sec*
 - [設定値]:

設定値	説明
秒数 (1 .. 60)	フラグメントパケットを再構成するために保持しておく時間

- [初期値]: 60 秒

[説明]

IPv6 のフラグメントパケットを再構成するために保持しておく時間。
設定した時間が経過しても再構成ができなかった場合、保持していたパケットは破棄される。
コマンド実行時にすでに保持していたパケットについては変更しない。

[ノート]

RTX5000、RTX3500 は Rev.14.00.32 以降で使用可能。
RTX1210 は Rev.14.01.40 以降で使用可能。
RTX830 は Rev.15.02.20 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

33.2 IPv6 アドレスの管理

33.2.1 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 [address_type]
ipv6 interface address auto
```

```

ipv6 interface address dhcp
ipv6 interface address proxy
ipv6 pp address ipv6_address/prefix_len [address_type]
ipv6 pp address auto
ipv6 pp address dhcp
ipv6 pp address proxy
ipv6 tunnel address ipv6_address/prefix_len [address_type]
ipv6 tunnel address auto
ipv6 tunnel address dhcp
ipv6 tunnel address proxy
no ipv6 interface address ipv6_address/prefix_len [address_type]
no ipv6 interface address auto
no ipv6 interface address dhcp
no ipv6 interface address proxy
no ipv6 pp address ipv6_address/prefix_len [address_type]
no ipv6 pp address auto
no ipv6 pp address dhcp
no ipv6 pp address proxy
no ipv6 tunnel address ipv6_address/prefix_len [address_type]
no ipv6 tunnel address auto
no ipv6 tunnel address dhcp
no ipv6 tunnel address proxy
    
```

[設定値及び初期値]

- *interface*
 - [設定値]: 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
 - [初期値]: -
- *ipv6_address*
 - [設定値]: IPv6 アドレス部分
 - [初期値]: -
- *prefix_len*
 - [設定値]: IPv6 プレフィックス長
 - [初期値]: -
- *address_type*
 - [設定値]:

設定値	説明
unicast	ユニキャスト
anycast	エニーキャスト

- [初期値]: unicast
- *auto*: RA で取得したプレフィックスとインタフェースの MAC アドレスから IPv6 アドレスを生成することを示すキーワード
 - [初期値]: -
- *dhcp*: DHCPv6 で取得したプレフィックスとインタフェースの MAC アドレスから IPv6 アドレスを生成することを示すキーワード
 - [初期値]: -
- *proxy*: プロキシ
 - [設定値]:
 - *prefix_type@prefix_interface*[*interface_id/prefix_len*]
 - *prefix_type*

設定値	説明
dhcp-prefix	DHCPv6 プロキシ

設定値	説明
ra-prefix	RA プロキシ

- *prefix_interface*

設定値	説明
<i>prefix_interface</i>	転送元のインタフェース名

- *interface_id*

設定値	説明
<i>interface_id</i>	インタフェース ID

- *prefix_len*

設定値	説明
<i>prefix_len</i>	IPv6 プレフィックス長

- [初期値]:-

[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 インタフェースでアドレスを自動で設定する機能を利用することができる。

具体的には、RA で取得したプレフィックスとインタフェース ID から IPv6 アドレスを生成する機能と、DHCPv6 で取得したプレフィックスとインタフェース ID から IPv6 アドレスを生成する機能が利用できる。

これらを設定する場合、デフォルト経路は最後に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 以降のリリースである。

LOOPBACK インタフェースを指定した場合は、**auto**、**dhcp**、**address_type**、**proxy** は指定できない。

prefix_interface には LOOPBACK インタフェースは指定できない。

ブリッジインタフェースは SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

dhcp は RTX1500 / RTX1100 / RT107e Rev.8.03.92 以降、RTX3000 Rev.9.00.50 以降、SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.24 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで指定可能。

address_type は RTX1200 Rev.10.01.32 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで指定可能。

dhcp-prefix は RTX1500 / RTX1100 / RT107e Rev.8.03.92 以降、RTX3000 Rev.9.00.50 以降、SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.24 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで指定可能。

[設定例]

- LAN2 で受信した RA のプレフィックスに::1 を付け足して IPv6 アドレスを作り、それを LAN1 に付与する

```
# ipv6 lan1 address ra-prefix@lan2::1/64
```

- LAN2 が DHCPv6 で取得した /56 のプレフィックス (XXXX:XXXX:XXXX:XX00::/56) を分割し、LAN1 と LAN3 に異なる /64 のプレフィックスの IPv6 アドレスを付与する

```
LAN1 に付与する IPv6 アドレス : XXXX:XXXX:XXXX:XX01::1/64
```

```
LAN3 に付与する IPv6 アドレス : XXXX:XXXX:XXXX:XX02::1/64
```

```
# ipv6 lan1 address dhcp-prefix@lan2::1:0:0:0:1/64
```

```
# ipv6 lan3 address dhcp-prefix@lan2::2:0:0:0:1/64
```

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

33.2.2 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 proxy
ipv6 pp prefix ipv6_prefix/prefix_len
ipv6 pp prefix proxy
ipv6 tunnel prefix ipv6_prefix/prefix_len
ipv6 tunnel prefix proxy
no ipv6 interface prefix ipv6_prefix/prefix_len
no ipv6 interface prefix proxy
no ipv6 pp prefix ipv6_prefix/prefix_len
no ipv6 pp prefix proxy
no ipv6 tunnel prefix ipv6_prefix/prefix_len
no ipv6 tunnel prefix proxy

```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、ブリッジインタフェース名
 - [初期値]: -
- *ipv6_prefix*
 - [設定値]: IPv6 プレフィックスのアドレス部分
 - [初期値]: -
- *prefix_len*
 - [設定値]: IPv6 プレフィックス長
 - [初期値]: -
- *proxy*: プロキシ
 - [設定値]:
 - *prefix_type@prefix_interface[interface_id/prefix_len]*

設定値	説明
dhcp-prefix	DHCPv6 プロキシ
ra-prefix	RA プロキシ

- *prefix_interface*

設定値	説明
<i>prefix_interface</i>	転送元のインタフェース名

- *interface_id*

設定値	説明
<i>interface_id</i>	インタフェース ID

- *prefix_len*

設定値	説明
<i>prefix_len</i>	IPv6 プレフィックス長

- [初期値]: -

[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。

[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。

RT250i では **ipv6 tunnel prefix** コマンドは使用できない。

prefix_interface には LOOPBACK インタフェースは指定できない。

ブリッジインタフェースは SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

dhcp-prefix は RTX1500 / RTX1100 / RT107e Rev.8.03.92 以降、RTX3000 Rev.9.00.50 以降、SRT100 Rev.10.00.60 以降、RTX1200 10.01.24 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで指定可能。

[設定例]

- LAN2 で受信した RA のプレフィックスを LAN1 に付与する

```
# ipv6 lan1 prefix ra-prefix@lan2::/64
```

- LAN2 が DHCPv6 で取得した /56 のプレフィックス (XXXX:XXXX:XXXX:XX00::/56) を分割し、LAN1 と LAN3 に異なる /64 のプレフィックスを付与する

```
LAN1 に付与するプレフィックス : XXXX:XXXX:XXXX:XX01::/64
```

```
LAN3 に付与するプレフィックス : XXXX:XXXX:XXXX:XX02::/64
```

```
# ipv6 lan1 prefix dhcp-prefix@lan2::1:0:0:0:1/64
```

```
# ipv6 lan3 prefix dhcp-prefix@lan2::2:0:0:0:1/64
```

(注 : 内部動作の関係上「dhcp-prefix@lan2::1:0:0:0:0/64」ではなく、「dhcp-prefix@lan2::1:0:0:0:1/64」と設定してください。)

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

33.2.3 IPv6 プレフィックスに変化があった時にログに記録するか否かの設定

[書式]

```
ipv6 interface prefix change log log
```

```
ipv6 pp prefix change log log
```

```
ipv6 tunnel prefix change log log
```

```
no ipv6 interface prefix change log log
```

```
no ipv6 pp prefix change log log
```

```
no ipv6 tunnel prefix change log log
```

[設定値及び初期値]

- interface**
 - [設定値]: LAN インタフェース名、ブリッジインタフェース名
 - [初期値]: -
- log**
 - [設定値]:

設定値	説明
on	IPv6 プレフィックスの変化をログに記録する
off	IPv6 プレフィックスの変化をログに記録しない

- [初期値]: off

[説明]

IPv6 プレフィックス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。

同じプレフィックスに対するアドレスを複数設定した場合、同じログが複数回表示される。

[ノート]

SRT100 は Rev.10.00.61 以降で使用可能。

RTX1200 は Rev.10.01.42 以降で使用可能。

RTX810 は Rev.11.01.06 以降で使用可能。

ブリッジインタフェースは SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

33.2.4 DHCPv6 の動作の設定

[書式]

```

ipv6 interface dhcp service type
ipv6 interface dhcp service client [ir=value]
ipv6 pp dhcp service type
ipv6 pp dhcp service client [ir=value]
ipv6 tunnel dhcp service type
ipv6 tunnel dhcp service client [ir=value]
no ipv6 interface dhcp service
no ipv6 pp dhcp service
no ipv6 tunnel dhcp service
    
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *type*
 - [設定値]:

設定値	説明
off	DHCPv6 を使わない
client	クライアント
server	サーバー

- [初期値]: off
- *value*

- [設定値]:

設定値	説明
on	クライアントとして動作する時、Inform-Request を送信する
off	クライアントとして動作する時、Solicit を送信する

- [初期値]: off

[説明]

各インタフェースにおける DHCPv6 の動作を設定する。

[ノート]

RTX1500、RTX1100、RT107e は Rev.8.03.92 以降で使用可能。

RTX3000 は Rev.9.00.50 以降で使用可能。

SRT100 は Rev.10.00.60 以降で使用可能。

RTX1200 は Rev.10.01.24 以降で使用可能。

`ir=value` オプションは、RTX1500 / RTX1100 / RT107e Rev.8.03.92 以降、RTX3000 Rev.9.00.56 以降、SRT100 Rev.10.00.61 以降、RTX1200 Rev.10.01.36 以降、RTX810 Rev.11.01.06 以降のファームウェア、および、Rev.14.00 系以降のすべてのファームウェアで使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

33.2.5 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]`

[設定値及び初期値]

- `interface`
 - [設定値]: LAN インタフェース名、ブリッジインタフェース名
 - [初期値]: -
- `count`
 - [設定値]: 選択したインタフェースでの DAD の再送回数 (0..10)
 - [初期値]: 1

[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.8.02.28 以降で使用可能。

ブリッジインタフェースは SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

33.2.6 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]`

[設定値及び初期値]

- `max`
 - [設定値]: 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)
 - [初期値]: 16

[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]

RT250i は、Rev.8.02.50 以降で使用可能。

RTX1100, RTX1500, RT107e は、Rev.8.03.80 以降で使用可能。

RTX3000 は、Rev.9.00.43 以降で使用可能。

SRT100 は、Rev.10.00.38 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

33.2.7 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*]

[設定値及び初期値]

- *rule* : 始点 IPv6 アドレスを選択する規則

- [設定値] :

設定値	説明
prefix	プレフィックスの最長一致
lifetime	寿命の長い方を優先

- [初期値] : prefix

[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 アドレスと始点 IPv6 アドレス候補とを比較して、先頭から一致している部分 (プレフィックス) 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' を設定しておけばよいが、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。

RTX1100, RTX1500, RT107e は、Rev.8.03.80 以降で使用可能。

RTX3000 は、Rev.9.00.43 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

33.3 近隣探索**33.3.1 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*]

ipv6 prefix *prefix_id proxy* [preferred_lifetime=*time*] [valid_lifetime=*time*] [l_flag=*switch*] [a_flag=*switch*]

no ipv6 prefix *prefix_id*

[設定値及び初期値]

- *prefix_id*

- [設定値] : プレフィックス番号

- [初期値] : -

- *prefix*

- [設定値] : プレフィックス

- [初期値] : -

- *prefix_len*

- [設定値] : プレフィックス長

- [初期値] : -

- *proxy* : プロキシ

- [設定値] :

- `prefix_type@prefix_interface[interface_id/prefix_len]`

- `prefix_type`

設定値	説明
dhcp-prefix	DHCPv6 プロキシ
ra-prefix	RA プロキシ

- `prefix_interface`

設定値	説明
<code>prefix_interface</code>	転送元のインタフェース名

- `interface_id`

設定値	説明
<code>interface_id</code>	インタフェース ID

- `prefix_len`

設定値	説明
<code>prefix_len</code>	IPv6 プレフィックス長

- [初期値]: -

- `preferred_lifetime`: プレフィックスの推奨寿命

- [設定値]:

- | 設定値 | 説明 |
|---------------|-----------------|
| 0..4294967295 | Rev.10.01.32 以降 |
| 60..15552000 | 上記以外 |

- [初期値]: 604800

- `valid_lifetime`: プレフィックスの有効寿命

- [設定値]:

- | 設定値 | 説明 |
|---------------|-----------------|
| 0..4294967295 | Rev.10.01.32 以降 |
| 60..15552000 | 上記以外 |

- [初期値]: 2592000

- `time`: 時間設定

- [設定値]:

- `yyyy-mm-dd[,hh:mm[:ss]]`

設定値	説明
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)

- [初期値]: -

- `l_flag`: on-link フラグ

- [初期値]: on

- `a_flag`: autonomous address configuration フラグ

- [初期値]: on

- `switch`

- [設定値]:
 - on
 - off
- [初期値]:-

[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 (Rev.10.01.32 以降では 0 以上 4294967295 以下、それ以外のリビジョンでは 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。

prefix_interface には LOOPBACK インタフェースは指定できない。

ブリッジインタフェースは SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

dhcp-prefix は RTX1500 / RTX1100 / RT107e Rev.8.03.92 以降、RTX3000 Rev.9.00.50 以降、SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.24 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで指定可能。

[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。

[設定例]

- LAN2 で受信した RA を LAN1 に転送する

```
# ipv6 prefix 1 ra-prefix@lan2::/64
# ipv6 lan1 rtadv send 1
```

- LAN2 が DHCPv6 で取得した /56 のプレフィックス (XXXX:XXXX:XXXX:XX00::/56) を分割し、LAN1 と LAN3 から異なる /64 のプレフィックスをルーター広告で配布する

```
LAN1 のルーター広告で配布するプレフィックス : XXXX:XXXX:XXXX:XX01::/64
LAN3 のルーター広告で配布するプレフィックス : XXXX:XXXX:XXXX:XX02::/64
```

```
# ipv6 prefix 1 dhcp-prefix@lan2::1:0:0:0:1/64
# ipv6 prefix 2 dhcp-prefix@lan2::2:0:0:0:1/64
# ipv6 lan1 rtadv send 1
# ipv6 lan3 rtadv send 2
```

(注 : 内部動作の関係上「dhcp-prefix@lan2::1:0:0:0:0/64」ではなく、「dhcp-prefix@lan2::1:0:0:0:1/64」と設定してください。)

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

33.3.2 ルーター広告で配布する RDNSS オプションの定義

[書式]

```
ipv6 nd ra-rdnss rdns_id dns_ipv6_address [dns_ipv6_address...] [option=value]
no ipv6 nd ra-rdnss rdns_id [...]
```

[設定値及び初期値]

- *rdns_id*
 - [設定値]: RDNSS オプション番号 (1..21474836)
 - [初期値]:-
- *dns_ipv6_address*
 - [設定値]:

設定値	説明
dhcpv6	DHCPv6 で通知された DNS サーバーの IPv6 アドレス
ipv6_address	任意の DNS サーバーの IPv6 アドレス

- [初期値]: -
- *option=value* : NAME=VALUE の列
- [設定値]:

NAME	VALUE	説明
lifetime	秒数、infinity	DNS サーバーの有効時間 (0.4294967294 秒)。infinity は DNS サーバーを無期限で使用できることを示す。

- [初期値]:
 - `lifetime = ipv6 interface rtadv send` コマンドのルーター広告を送信する最大間隔 (max-rtr-adv-interval) の 3 倍

[説明]

ルーター広告で配布する RDNSS オプションを定義する。実際に広告するためには、`ipv6 interface rtadv send` コマンドの `rdnss=` オプションの設定が必要である。

`dns_ipv6_address` は最大 3 つまで指定可能。

[ノート]

RTX1210 Rev.14.01.41 以降、RTX830 Rev.15.02.24 以降、RTX1220 Rev.15.04.04 以降のファームウェアで使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830

33.3.3 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 [...]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *prefix_id*
 - [設定値]: プレフィックス番号
 - [初期値]: -
- *option=value* : NAME=VALUE の列
- [設定値]:

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。

NAME	VALUE	説明
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。
prf_flag	high、medium、low	default router preference フラグ。ルーター広告の優先度を示す設定。
max-rtr-adv-interval	秒数	ルーター広告を送信する最大間隔 (4-1,800 秒)
min-rtr-adv-interval	秒数	ルーター広告を送信する最小間隔 (3-1,350 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)
adv-retrans-time	ミリ秒数	ルーター広告を再送する間隔 (0-4,294,967,295 ミリ秒)
adv-cur-hop-limit	ホップ数	ルーター広告の限界ホップ数 (0-255)
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。
rdnss	rdnss、off、dhcpv6、RDNSS オプション番号	ルーター広告に RDNSS オプションを含めるか否かと、含める場合の値の設定。rdnss の場合は RA の RDNSS オプションで割り当てられたサーバー群を通知する。

• [初期値] :

- m_flag = off
- o_flag = off
- prf_flag = medium
- max-rtr-adv-interval = 600
- min-rtr-adv-interval = 200
- adv-default-lifetime = 1800
- adv-reachable-time = 0
- adv-retrans-time = 0
- adv-cur-hop-limit = 64
- mtu=auto
- rdnss=rdnss

[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]

prf_flag= オプションは、RTX5000、RTX3500 Rev.14.00.32 以降、RTX1210 Rev.14.01.41 以降、RTX830 Rev.15.02.22 以降、RTX1220 Rev.15.04.04 以降のファームウェアで指定可能。

adv-retrans-time= オプションと adv-cur-hop-limit= オプションは、RTX1200 Rev.10.01.32 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで指定可能。

RT107e では、`mtu`= オプションは指定できない。

`rdnss`= オプションは、RTX5000、RTX3500 Rev.14.00.32 以降、RTX1210 Rev.14.01.40 以降、RTX830 Rev.15.02.20 以降のファームウェア、および、Rev.15.04 系以降のすべてのファームウェアで指定可能。

`rdnss`= オプションの RDNSS オプション番号の指定は、RTX1210 Rev.14.01.41 以降、RTX830 Rev.15.02.24 以降、RTX1220 Rev.15.04.04 以降のファームウェアで指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

33.3.4 ルーター要請の再送機能の設定

[書式]

```
ipv6 interface rtsol max-retransmit mrt=MRT mrd=MRD mrc=MRC
```

```
ipv6 pp rtsol max-retransmit mrt=MRT mrd=MRD mrc=MRC
```

```
no ipv6 interface rtsol max-retransmit [...]
```

```
no ipv6 pp rtsol max-retransmit [...]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *MRT*
 - [設定値]: 最大再送間隔(4..3600(秒))
 - [初期値]: 3600
- *MRD*
 - [設定値]: 最大再送継続時間(4..2147483647(秒)または infinity)
 - [初期値]: infinity
- *MRC*
 - [設定値]: 最大再送回数(0..2147483647 または infinity)
 - [初期値]: infinity

[説明]

再送間隔は初期値 4 秒から 2 倍ずつ増加していく。初期値は+10%幅、倍率は±10%幅でランダムな値を取る。MRD と MRC の両方を infinity 以外に設定している場合は、MRD と MRC のどちらかの条件が満たされたら再送はストップする。

MRC を 0 に設定している場合は再送を行わない。

[ノート]

RTX5000 は Rev.14.00.26 以降で使用可能。

RTX3500 は Rev.14.00.26 以降で使用可能。

RTX1210 は Rev.14.01.33 以降で使用可能。

RTX830 は Rev.15.02.09 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

33.4 経路制御

33.4.1 IPv6 の経路情報の追加

[書式]

```
ipv6 route network gateway gateway [parameter] [gateway gateway [parameter]]
```

```
no ipv6 route network [gateway...]
```

[設定値及び初期値]

- *network*
 - [設定値]:

設定値	説明
IPv6 アドレス/プレフィックス長	送り先のホスト
default	デフォルト経路

- [初期値]: -
- *gateway*: ゲートウェイ
- [設定値]:
 - 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*

設定値	説明
<i>name</i>	PAP/CHAP による名前

- *dhcp interface*

設定値	説明
<i>interface</i>	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
- [初期値]: -
- *parameter*: 以下のパラメータを空白で区切り複数設定可能
- [設定値]:

設定値	説明
<i>metric metric</i>	メトリックの指定 <ul style="list-style-type: none"> • <i>metric</i> <ul style="list-style-type: none"> • メトリック値 (1..15) • 省略時は 1
<i>hide</i>	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、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

- [初期値]: -

[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。

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。

[ノート]

RTX1220、RTX1210、RTX830、RTX810、RT107e、SRT100 では、PP インタフェースの *dlci=* オプションは指定できない。*gateway* に *dhcp* を指定できるのは、RTX1500 / RTX1100 / RT107e Rev.8.03.92 以降、RTX3000 Rev.9.00.50 以降、SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.24 以降、および、Rev.11.01 系以降のすべてのファームウェアである。ブリッジインタフェースは SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、

RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

33.4.2 IPv6 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]

```
ipv6 route change log log
no ipv6 route change log [log]
```

[設定値及び初期値]

- *log*
 - [設定値]:

設定値	説明
on	IPv6 経路の変化をログに記録する
off	IPv6 経路の変化をログに記録しない

- [初期値]: off

[説明]

IPv6 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]

RTX1220 Rev.15.04.04 以降のファームウェアで使用可能。

[適用モデル]

RTX1220

33.5 RIPng

33.5.1 RIPng の使用の設定

[書式]

```
ipv6 rip use use
no ipv6 rip use
```

[設定値及び初期値]

- *use*
 - [設定値]:

設定値	説明
on	RIPng を使う

設定値	説明
off	RIPng を使わない

- [初期値] : off

[説明]

RIPng を使うか否かを設定する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

33.5.2 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

[設定値及び初期値]

- *interface*
 - [設定値] : LAN インタフェース名
 - [初期値] : -
- *send*
 - [設定値] :

設定値	説明
on	RIPng を送信する
off	RIPng を送信しない

- [初期値] : on

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

33.5.3 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

[設定値及び初期値]

- *interface*
 - [設定値] : LAN インタフェース名
 - [初期値] : -
- *receive*
 - [設定値] :

設定値	説明
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

- [初期値]: on

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

33.5.4 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

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *direction*
 - [設定値]:

設定値	説明
in	受信時に加算する
out	送信時に加算する

- [初期値]: -
- *hop*
 - [設定値]: 加算ホップ数 (0..15)
 - [初期値]: 0

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

33.5.5 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 [[except] gateway [gateway...]]

no ipv6 pp rip trust gateway [[except] gateway [gateway...]]

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *gateway*
 - [設定値]: IPv6 アドレス

- [初期値]: -

[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。

gateway は 10 個まで指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

33.5.6 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

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *direction*
 - [設定値]:

設定値	説明
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

- [初期値]: -
- *filter_list*
 - [設定値]: フィルタ番号
 - [初期値]: -

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

33.5.7 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

[設定値及び初期値]

- *action*
 - [設定値]:

設定値	説明
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

- [初期値]: update

[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。

[設定例]

```
# ipv6 pp rip connect interval 60
# ipv6 pp rip connect send interval
```

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

33.5.8 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
```

[設定値及び初期値]

- *time*
 - [設定値]: 秒数 (30..21474836)
 - [初期値]: 30

[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。

[設定例]

```
# ipv6 pp rip connect interval 60
# ipv6 pp rip connect send interval
```

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

33.5.9 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
```

[設定値及び初期値]

- *action*
 - [設定値]:

設定値	説明
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 を送信する

- [初期値]: none

[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。

[設定例]

```
# ipv6 pp rip disconnect interval 1800
# ipv6 pp rip disconnect send interval
```

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

33.5.10 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
```

[設定値及び初期値]

- *time*
 - [設定値]: 秒数 (30..21474836)
 - [初期値]: 3600

[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。

[設定例]

```
# ipv6 pp rip disconnect interval 1800
# ipv6 pp rip disconnect send interval
```

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

33.5.11 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
```

[設定値及び初期値]

- *hold*
 - [設定値]:

設定値	説明
on	保持する
off	保持しない

- [初期値]: off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

33.5.12 RIPng による経路の優先度の設定**[書式]**

```
ipv6 rip preference preference
no ipv6 rip preference [preference]
```

[設定値及び初期値]

- *preference*
 - [設定値]: RIPng による経路の優先度 (1-2147483647)
 - [初期値]: 1000

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

33.6 VRRPv3 の設定

33.6.1 インタフェース毎の VRRPv3 の設定

[書式]

```
ipv6 interface vrrp vrid ipv6_address [priority=priority] [preempt=preempt] [auth=auth] [advertise-interval=time1] [down-interval=time2]
```

```
no ipv6 interface vrrp vrid [vrid...]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *vrid*
 - [設定値]: VRRPv3 グループ ID (1..255)
 - [初期値]: -
- *ipv6_address*
 - [設定値]: 仮想ルーターの IPv6 アドレス
 - [初期値]: -
- *priority*
 - [設定値]: 優先度 (1..254)
 - [初期値]: 100
- *preempt*: プリエンプトモード
 - [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: on
- *auth*
 - [設定値]: テキスト認証文字列 (8 文字以内)
 - [初期値]: -
- *time1*
 - [設定値]: VRRPv3 広告の送信間隔 (1..60 秒)
 - [初期値]: 1
- *time2*
 - [設定値]: マスターがダウンしたと判定するまでの時間 (3..180 秒)
 - [初期値]: 3

[説明]

指定した VRRPv3 グループを利用することを設定する。

同じ VRRPv3 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 IPv6 アドレスを一致させておか

なくてはならない。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 VRRPv3 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 VRRPv3 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 IPv6 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。

RTX1200 Rev.10.01.59 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.18 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

33.6.2 シャットダウントリガの設定

[書式]

```

ipv6 interface vrrp shutdown trigger vrid interface
ipv6 interface vrrp shutdown trigger vrid pp peer_num [dlsi=dlsi]
ipv6 interface vrrp shutdown trigger vrid tunnel tunnel_num
ipv6 interface vrrp shutdown trigger vrid route network [nexthop]
no ipv6 interface vrrp shutdown trigger vrid interface
no ipv6 interface vrrp shutdown trigger vrid pp peer_num [...]
no ipv6 interface vrrp shutdown trigger vrid tunnel tunnel_num
no ipv6 interface vrrp shutdown trigger vrid route network

```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *vrid*
 - [設定値]: VRRPv3 グループ ID (1..255)
 - [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *dlsi*
 - [設定値]: DLCI 番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: tunnel インターフェース 番号
 - [初期値]: -
- *network*
 - [設定値]:
 - IPv6 プレフィックス/プレフィックス長
 - default
 - [初期値]: -
- *nexthop*
 - [設定値]:
 - インタフェース名
 - IPv6 アドレス
 - [初期値]: -

[説明]

設定した VRRPv3 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。

形式	説明
LAN インタフェース形式	指定した LAN インタフェースがリンクダウンするか、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。 <ul style="list-style-type: none"> 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”dldci=dldci”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
tunnel 形式	指定した tunnel インターフェースが以下の条件によりダウンした場合にシャットダウンする。 <ul style="list-style-type: none"> IPsec トンネルで、ipsec ike keepalive use 設定によりダウンが検出された場合 L2TP/IPsec、L2TPv3、L2TPv3/IPsec のいずれかのトンネルで、l2tp keepalive use 設定によりダウンが検出された場合 PPTP トンネルで、pptp keepalive use 設定によりダウンが検出された場合 IPIP トンネルで、ipip 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 IPv6 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に向いていても存在する限りはシャットダウンしない。

[ノート]

RTX1200 Rev.10.01.59 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.18 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで使用可能。
tunnel インターフェースは RTX5000 / RTX3500 Rev.14.00.32 以降、RTX1210 Rev.14.01.28 以降、RTX830 Rev.15.02.03 以降、RTX1220 のファームウェアで使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

33.7 フィルタの設定

33.7.1 IPv6 フィルターの定義

[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]
```

[設定値及び初期値]

- filter_num*

- [設定値]: 静的フィルター番号 (1..21474836)
- [初期値]: -
- *pass_reject*
 - [設定値]: フィルターのタイプ (**ip filter** コマンドに準ずる)
 - [初期値]: -
- *src_addr*: IPv6 パケットの始点 IPv6 アドレス
 - [設定値]:
 - IPv6 アドレス
 - 静的または動的 IPv6 アドレス
 - , を区切りとして複数設定することができる。
 - FQDN
 - 任意の文字列 (半角 255 文字以内。 / : は使用できない。 , は区切り文字として使われるため、使用できない)
 - * から始まる FQDN は * より後ろの文字列を後方一致条件として判断する 例えば *.example.co.jp は www.example.co.jp 、 mail.example.co.jp などと一致する
 - , を区切りとして複数設定することができる。
 - map-e
 - MAP-E のマッピングルールにより生成され、MAP-E トンネルに設定されたグローバル IPv6 アドレスを表すキーワード
 - * (すべての IPv6 アドレスに対応)
 - [初期値]: -
- *prefix_len*
 - [設定値]: プレフィックス長
 - [初期値]: -
- *dest_addr*: IPv6 パケットの終点 IPv6 アドレス
 - [設定値]:
 - *src_addr* と同じ形式
 - 省略した場合は一個の * と同じ
 - [初期値]: -
- *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)
 - [設定値]:

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)
icmp4	ICMPv4 パケットの指定を示すキーワード
icmp	ICMPv6 パケットの指定を示すキーワード
icmp6	

- [初期値]: -
- *src_port_list*
 - [設定値]: 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)
 - [初期値]: -
- *dest_port_list*
 - [設定値]: 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
 - [初期値]: -

[説明]

IPv6 のフィルターを定義する。

[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 は Rev.8.03.68 以降
- RTX3000 は Rev.9.00.31 以降

フィルタリングするパケットの種類に `icmp4` を指定できるのは、

- RTX1500、RTX1100、RT107e は Rev.8.03.87 以降
- RTX3000 は Rev.9.00.48 以降
- RTX1200 は Rev.10.01.22 以降

`src_addr` および `dest_addr` は IPv6 アドレス と FQDN と `map-e` を混合することも可能。

`src_addr` および `dest_addr` への FQDN の指定は RTX5000 Rev.14.00.32 以降、RTX3500 Rev.14.00.32 以降、RTX1210 Rev.14.01.41 以降、RTX830 Rev.15.02.24、RTX1220 Rev.15.04.04 以降で指定可能。

`src_addr` および `dest_addr` に FQDN を指定することによって、固定 IP アドレスではないサーバーや 1 つの FQDN に対して複数の固定 IP アドレスを持つサーバーを対象にしたフィルタリングを行うことができる。FQDN を使用する場合、ルーター自身が DNS リカーシブサーバーとして動作し、ルーター配下の端末は DNS サーバーとして本機を指定する必要がある。

指定した FQDN に一致する通信が発生した場合、設定した FQDN に該当する IPv6 アドレスの情報が保持される。保持される期間は、`ip filter fqdn timer` コマンドで指定できる。

`src_addr` および `dest_addr` への `map-e` の指定は RTX5000 Rev.14.00.32 以降、RTX3500 Rev.14.00.32 以降、RTX1210 Rev.14.01.40 以降、RTX830 Rev.15.02.20 以降で指定可能。

[設定例]

PP 1 で送受信される IPv6 Packet Too Big を記録する

```
# pp select 1
# ipv6 pp secure filter in 1 100
# ipv6 pp secure filter out 1 100
# pp enable 1
# ipv6 filter 1 pass-log * * icmp6 2
# ipv6 filter 100 pass * *
```

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

33.7.2 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*

[設定値及び初期値]

- *interface*
 - [設定値]: 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
 - [初期値]: -
- *direction*
 - [設定値]:

設定値	説明
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

- [初期値]:-
- *filter_list*
 - [設定値]: 空白で区切られたフィルタ番号の並び (静的フィルタと動的フィルタの数の合計として 128 個以内)
 - [初期値]:-
- *dynamic*: キーワード後に動的フィルタの番号を記述する
 - [初期値]:-

[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 インタフェースは Rev.8.03 系以降のすべてのファームウェアで指定可能。

ブリッジインタフェースは SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、

RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

33.7.3 IPv6 動的フィルターの定義

[書式]

```
ipv6 filter dynamic dyn_filter_num srcaddr[/prefix_len] dstaddr[/prefix_len] protocol [option ...]
```

```
ipv6 filter dynamic dyn_filter_num srcaddr[/prefix_len] dstaddr[/prefix_len] filter filter_list [in filter_list] [out filter_list] [option ...]
```

```
no ipv6 filter dynamic dyn_filter_num [srcaddr ...]
```

[設定値及び初期値]

- *dyn_filter_num*
 - [設定値]: 動的フィルター番号 (1..21474836)
 - [初期値]:-
 - *srcaddr*: IPv6 パケットの始点 IPv6 アドレス
 - [設定値]:
 - **ipv6 filter** コマンドの *src_addr* と同じ形式
 - 省略した場合は一個の * と同じ
 - [初期値]:-
 - *prefix_len*
 - [設定値]: プレフィックス長
 - [初期値]:-
 - *dstaddr*: IPv6 パケットの終点 IPv6 アドレス
 - [設定値]:
 - *srcaddr* と同じ形式
 - 省略した場合は一個の * と同じ
 - [初期値]:-
 - *protocol*: プロトコルのニーモニック
 - [設定値]:
 - tcp/udp/ftp/tftp/domain/www/smtp/pop3/telnet
- Rev.10.01 以降では以下が設定できます
- echo/discard/daytime/chargen/ftp/ssh/telnet/smtp/time/whois/dns/domain/dhcps/
 - dhcpc/tftp/gopher/finger/http/www/pop3/sunrpc/ident/nntp/ntp/ms-rpc/

- netbios_ns/netbios_dgm/netbios_ssn/imap/snmp/snmptrap/bgp/imap3/ldap/
- https/ms-ds/ike/rlogin/rwho/rsh/syslog/printer/rip/ripng/
- dhcpv6c/dhcpv6s/ms-sql/radius/l2tp/pptp/nfs/msblast/ipsec-nat-t/sip/
- ping/ping6/tcp/udp
- [初期値]: -
- *filter_list*
 - [設定値]: **ipv6 filter** コマンドで登録されたフィルター番号のリスト
 - [初期値]: -
- *option*
 - [設定値]:
 - syslog=*switch*

設定値	説明
on	接続の通信履歴を syslog に残す
off	接続の通信履歴を syslog に残さない

- timeout=*time*

設定値	説明
time	データが流れなくなったときに接続情報を解放するまでの秒数

- [初期値]:
 - syslog=on
 - timeout=60

[説明]

IPv6 の動的フィルターを定義する。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、ユーザー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ー番号を設定する。

filter キーワードの後に記述されたフィルターに該当する接続 (トリガー) 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ーに該当する接続を通過させる。*in* キーワードはトリガー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ー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。

[ノート]

srcaddr および *dstaddr* は IPv6 アドレスと FQDN と map-e を混合することも可能。

srcaddr および *dstaddr* への FQDN の指定は RTX5000 Rev.14.00.32 以降、RTX3500 Rev.14.00.32 以降、RTX1210 Rev.14.01.41 以降、RTX830 Rev.15.02.24 以降、RTX1220 Rev.15.04.04 以降で指定可能。

srcaddr および *dstaddr* への map-e の指定は RTX5000 Rev.14.00.32 以降、RTX3500 Rev.14.00.32 以降、RTX1210 Rev.14.01.40 以降、RTX830 Rev.15.02.20 以降で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e

33.8 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-mldv2-07.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。

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(MulticastListenerDiscovery) 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 (FilterMode) とソースリスト (SourceList) 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。

33.8.1 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 ...]]
    
```

[設定値及び初期値]

- *interface*
 - [設定値] : LAN インタフェース名
 - [初期値] : -
- *type* : MLD の動作方式
 - [設定値] :

設定値	説明
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

- [初期値] : off
- *option* : オプション
 - [設定値] :
 - version=*version*
 - MLD のバージョン

設定値	説明
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

設定値	説明
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。
- `report-link-local-group=switch`
 - リンクローカルスコープのグループを処理するか否か

設定値	説明
on	MLD ルーターとして動作しているとき、リンクローカルスコープのグループのレポート受信を有効にする。MLD ホストとして動作しているとき、リンクローカルスコープのグループのレポート送信を有効にする。
off	リンクローカルスコープのグループのレポート送受信を無効にする。

- [初期値]:
 - `version=1,2`
 - `syslog=off`
 - `robust-variable=2`
 - `report-link-local-group=off`

[説明]

インタフェースの MLD の動作を設定する。

[ノート]

`report-link-local-group` オプションは、RTX1200 Rev.10.01.71 以降、RTX810 Rev.11.01.28 以降、RTX5000 / RTX3500 Rev.14.00.21 以降、RTX1210 Rev.14.01.16 以降のファームウェア、および、Rev.15.02 系以降のすべてのファームウェアで指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e

33.8.2 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...]

```

[設定値及び初期値]

- `interface`
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- `group`

- [設定値]: グループのマルチキャストアドレス
- [初期値]: -
- *filter_mode*: フィルタモード
 - [設定値]:

設定値	説明
include	MLD の "INCLUDE" モード
exclude	MLD の "EXCLUDE" モード

- [初期値]: -
- *source*

- [設定値]:

設定値	説明
IPv6 アドレス	マルチキャストパケットの送信元アドレス
省略	省略時はすべての送信元アドレスに対して同様に動作する

- [初期値]: -

[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くなるときに設定する。*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。*source* を省略した場合は、全ての送信元からの要求を受信しない。*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。*source* を省略した場合は、全ての送信元からの要求を受信する。

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e

33.8.3 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
```

[設定値及び初期値]

- *mode*
 - [設定値]:

設定値	説明
fast	ファストパスで処理する
normal	ノーマルパスで処理する

- [初期値]: fast

[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。

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。

[適用モデル]
RTX1100, RT107e

33.9 近隣要請

33.9.1 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 [...]
```

[設定値及び初期値]

- on
 - [設定値]: 近隣要請を行う
 - [初期値]: -
- off
 - [設定値]: 近隣要請を行わない
 - [初期値]: -
- *option=value* 列: MLD の動作方式
 - [設定値]:

<i>option</i>	<i>value</i>	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

- [初期値]: na-proxy=all

[初期設定]

```
ipv6 nd ns-trigger-dad off
```

[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.8.02.50 以降、Rev.8.03.75 以降、Rev.10.00.38 以降、Rev.10.01 系以降

[適用モデル]

RTX5000, RTX3500, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

第 34 章

OSPFv3

34.1 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。

RTX1200 は Rev.10.01.53 以降で使用可能。

RTX810 は Rev.11.01.21 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

34.2 OSPFv3 の使用設定

[書式]

```
ipv6 ospf use use
no ipv6 ospf use [use]
```

[設定値及び初期値]

- *use*
- [設定値]:

設定値	説明
on	OSPFv3 を使用する
off	OSPFv3 を使用しない

- [初期値]: off

[説明]

OSPFv3 を使用するか否かを設定する。

[ノート]

RTX1200 は Rev.10.01.53 以降で使用可能。

RTX810 は Rev.11.01.21 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

34.3 OSPFv3 のルーター ID 設定

[書式]

```
ipv6 ospf router id router-id
no ipv6 ospf router id [router-id]
```

[設定値及び初期値]

- *router_id*
 - [設定値]: IPv4 アドレス表記 (0.0.0.0 は不可)
 - [初期値]: -

[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、以下の順序でインタフェースに付与されているプライマリ IPv4 アドレスを探索して 最初に見つかった IPv4 アドレスをルーター ID として使用する。

- LAN インタフェース(若番順)
- LOOPBACK インタフェース(若番順、RTX3000 では Rev.9.00.56 以降で対応する)

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。

RTX1200 は Rev.10.01.53 以降で使用可能。

RTX810 は Rev.11.01.21 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

34.4 OSPFv3 エリア設定

[書式]

```
ipv6 ospf area area [stub [cost=cost]]
no ipv6 ospf area area [stub [cost=cost]]
```

[設定値及び初期値]

- *area*
 - [設定値]:

設定値	説明
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

- [初期値]: -
- *cost*
 - [設定値]: デフォルト経路のコスト (0~16777215)
 - [初期値]: 0

[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。

[ノート]

RTX1200 は Rev.10.01.53 以降で使用可能。

RTX810 は Rev.11.01.21 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

34.5 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]
```

[設定値及び初期値]

- *area*
- [設定値]:

設定値	説明
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

- [初期値]: -
- *ipv6_prefix/prefix_len*
 - [設定値]: IPv6 プレフィクス
 - [初期値]: サブネットの範囲は設定されていない

[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。

[ノート]

RTX1200 は Rev.10.01.53 以降で使用可能。

RTX810 は Rev.11.01.21 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

34.6 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...]]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *area*
 - [設定値]:

設定値	説明
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

- [初期値]: インタフェースは OSPF エリアに属していない

- *parameters*
 - [設定値]: NAME=VALUE の列
 - [初期値]:
 - type=broadcast(LAN インタフェース設定時)
 - type=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)
 - passive=インタフェースは passive ではない
 - cost=1(LAN 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

[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	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。

[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。dead-interval を指定しなかった場合には、hello-interval の 4 倍の値が設定される。

- 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。

RTX1200 は Rev.10.01.53 以降で使用可能。
RTX810 は Rev.11.01.21 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

34.7 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...]]
```

[設定値及び初期値]

- router_id
 - [設定値]: 仮想リンクの相手のルーター ID
 - [初期値]: -
- area : 経由するエリア
 - [設定値]:

設定値	説明
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

- [初期値]: -
- parameters
 - [設定値]: NAME=VALUE の列
 - [初期値]:
 - retransmit-interval=5 秒

- transmit-delay=1 秒
- hello-interval=10 秒
- dead-interval=40 秒

[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。

RTX1200 は Rev.10.01.53 以降で使用可能。

RTX810 は Rev.11.01.21 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

34.8 OSPFv3 による経路の優先度設定

[書式]

```
ipv6 ospf preference preference
no ipv6 ospf preference [preference]
```

[設定値及び初期値]

- *preference*
 - [設定値]: OSPFv3 による経路の優先度 (1...2147483647)
 - [初期値]: 2000

[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。

RTX1200 は Rev.10.01.53 以降で使用可能。

RTX810 は Rev.11.01.21 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

34.9 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...]
```

[設定値及び初期値]

- *filter_num*
 - [設定値]: **ipv6 ospf export filter** コマンドのフィルタ番号 (1...2147483647)
 - [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

[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。

RTX1200 は Rev.10.01.53 以降で使用可能。

RTX810 は Rev.11.01.21 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

34.10 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[...]
```

[設定値及び初期値]

- *filter_num*
 - [設定値]: フィルタ番号 (1...2147483647)
 - [初期値]: -
- *nr*: フィルタの解釈の方法
 - [設定値]:

設定値	説明
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

- [初期値]: -
- *kind*: IPv6 プレフィクスの解釈の方法
 - [設定値]:

設定値	説明
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

- [初期値]:-
- `ipv6_prefix/prefix_len`
 - [設定値]: IPv6 プレフィクス
 - [初期値]:-

[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まらないため、`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
```

RTX1200 は Rev.10.01.53 以降で使用可能。

RTX810 は Rev.11.01.21 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

34.11 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...]
```

[設定値及び初期値]

- *protocol* : OSPFv3 の経路テーブルに導入する外部プロトコル

- [設定値] :

設定値	説明
static	静的経路
rip	RIPng

- [初期値] : -
- *filter_num*
 - [設定値] : **ipv6 ospf import filter** コマンドのフィルタ番号 (1...2147483647)
 - [初期値] : -

[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

[ノート]

RTX1200 は Rev.10.01.53 以降で使用可能。

RTX810 は Rev.11.01.21 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

34.12 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...]]
```

[設定値及び初期値]

- *filter_num*
 - [設定値] : フィルタ番号 (1...2147483647)
 - [初期値] : -
- *nr* : フィルタの解釈の方法
 - [設定値] :

設定値	説明
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

- [初期値] : -

- *kind*: IPv6 プレフィックスの解釈の方法

- [設定値]:

設定値	説明
include	指定した IPv6 プレフィックスに含まれる経路 (IPv6 プレフィックス自身を含む)
refines	指定した IPv6 プレフィックスに含まれる経路 (IPv6 プレフィックス自身を含まない)
equal	指定した IPv6 プレフィックスに一致する経路

- [初期値]: -

- *ipv6_prefix/prefix_len*

- [設定値]: IPv6 プレフィックス
- [初期値]: -

- *parameters*: 外部経路を広告する場合のパラメータ

- [設定値]:

設定値	説明
<i>metric = metric</i>	メトリック値 (1 ~ 16777215)
<i>type = type</i>	メトリックのタイプ (1 または 2)

- [初期値]: -

[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 プレフィックスを指定する。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 プレフィックスと一致する経路および、IPv6 プレフィックスに含まれる経路が該当
refines	IPv6 プレフィックスに含まれる経路が該当するが、IPv6 プレフィックスと一致する経路は該当しない
equal	IPv6 プレフィッ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 プレフィッ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 プレフィッ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 プレフィッ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は決定しないため、**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
```

RTX1200 は Rev.10.01.53 以降で使用可能。

RTX810 は Rev.11.01.21 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

34.13 OSPFv3 のログ出力設定

[書式]

```
ipv6 ospf log log ...
```

```
no ipv6 ospf log [log...]
```

[設定値及び初期値]

- *log*

- [設定値]:

設定値	説明
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

- [初期値]: いずれの種類ログも出力しない

[説明]

OSPFv3 に関わるログ出力の種類を設定する。

[ノート]

RTX1200 は Rev.10.01.53 以降で使用可能。

RTX810 は Rev.11.01.21 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

第 35 章

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。

35.1 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
```

[設定値及び初期値]

- *use*
- [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: on

[説明]

状態メール通知機能を使用するか否かを設定する。

[適用モデル]

RTX3000, RTX1500, RTX1100

35.2 メールサーバーの設定

[書式]

```
mail-notify status server server
```

```
no mail-notify status server
```

[設定値及び初期値]

- *server*
- [設定値]: SMTP サーバーの IP アドレスまたはドメイン名
- [初期値]: -

[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。

[適用モデル]

RTX3000, RTX1500, RTX1100

35.3 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
```

[設定値及び初期値]

- *address*
- [設定値]: 送信元メールアドレス
- [初期値]: -

[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。

[適用モデル]
RTX3000, RTX1500, RTX1100

35.4 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*

[設定値及び初期値]

- *id*
 - [設定値]: 識別子 (1..4)
 - [初期値]: -
- *address*
 - [設定値]: 送信先メールアドレス
 - [初期値]: -
- *option*
 - [設定値]:

設定値	説明
alert	警告のみを送信する

- [初期値]: -

[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。

[適用モデル]
RTX3000, RTX1500, RTX1100

35.5 サブジェクトの設定

[書式]

mail-notify status subject *subject*
no mail-notify status subject

[設定値及び初期値]

- *subject*
 - [設定値]: メールのサブジェクト
 - [初期値]: -

[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。

[適用モデル]
RTX3000, RTX1500, RTX1100

35.6 送信タイムアウトの設定

[書式]

mail-notify status timeout *timeout*
no mail-notify status timeout

[設定値及び初期値]

- *timeout*
 - [設定値]: タイムアウト秒数 (1..180)
 - [初期値]: 30

[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。

[適用モデル]

RTX3000, RTX1500, RTX1100

35.7 通知内容の設定

[書式]**mail-notify status type info [info...]****no mail-notify status type****[設定値及び初期値]**

- *info* : 通知する情報
- [設定値]:

設定値	説明
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	ファイアウォールの情報を通知
config-log	設定情報とログを通知

- [初期値]: all

[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。

[適用モデル]

RTX3000, RTX1500, RTX1100

35.8 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。

[適用モデル]

RTX3000, RTX1500, RTX1100

第 36 章

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検出したトリガの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。

36.1 メール設定識別名の設定

[書式]

mail server name *id name*

no mail server name *id [name]*

[設定値及び初期値]

- *id*
 - [設定値]: メールサーバー設定 ID (1..10)
 - [初期値]: -
- *name*
 - [設定値]: 識別名
 - [初期値]: -

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, SRT100

36.2 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] [smtps]*

no mail server smtp *id [...]*

[設定値及び初期値]

- *id*
 - [設定値]: メールサーバー設定 ID (1..10)
 - [初期値]: -
- *address*
 - [設定値]: サーバーの IP アドレスまたはホスト名 (半角 1 文字以上 64 文字以内)
 - [初期値]: -
- *port*
 - [設定値]: サーバーのポート番号 (省略時は 25、または、465)
 - [初期値]: -
- *username*
 - [設定値]: 認証用ユーザ名
 - [初期値]: -
- *password*
 - [設定値]: 認証用パスワード
 - [初期値]: -
- *auth_protocol*: SMTP-AUTH 認証プロトコル

- [設定値]:

設定値	説明
cram-md5	CRAM-MD5
digest-md5	DIGEST-MD5
plain	PLAIN 認証

- [初期値]: -
- pop-before-smtp
 - [設定値]: POP before SMTP の使用
 - [初期値]: -
- smtps
 - [設定値]: SMTPS の使用
 - [初期値]: -

[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。

smtps パラメーターが設定されている場合、SMTPS を使用してメールを送信する。*smtps* パラメーターと *pop-before-smtp* パラメーターは同時に設定できない。

port パラメーターを省略した場合、*smtps* パラメーターの設定によって、メールサーバーのポート番号として使用する値が変わる。*smtps* パラメーターの設定と、メールサーバーのポート番号の対応は以下のとおり。

<i>smtps</i> パラメーター	使用するポート番号
設定しない (省略)	25
設定する	465

[ノート]

Rev.8.03 系以降のすべてのリビジョンで使用可能。

smtps パラメーターは RTX5000 Rev.14.00.26 以降、RTX3500 Rev.14.00.26 以降、RTX1210 Rev.14.01.26 以降、RTX830 Rev.15.02.03 以降、RTX1220 のファームウェアで指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, SRT100

36.3 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 [...]
```

[設定値及び初期値]

- *id*
 - [設定値]: メールサーバー設定 ID (1..10)
 - [初期値]: -
- *address*
 - [設定値]: サーバーの IP アドレスまたはホスト名
 - [初期値]: -
- *port*

- [設定値]: サーバーのポート番号 (省略時は 110)
- [初期値]: -
- *protocol*
 - [設定値]:

設定値	説明
pop3	POP3
apop	APOP

- [初期値]: -
- *username*
 - [設定値]: 認証用ユーザ名
 - [初期値]: -
- *password*
 - [設定値]: 認証用パスワード
 - [初期値]: -

[説明]

メール受信に使用するサーバー情報を設定する。

mail server smtp コマンドで *pop-before-smtp* パラメータを設定したときに必要な設定である。

[ノート]

Rev.8.03 系以降のすべてのリビジョンで使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, SRT100

36.4 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]

[設定値及び初期値]

- *id*
 - [設定値]: メールサーバー設定 ID (1..10)
 - [初期値]: -
- *timeout*
 - [設定値]: タイムアウト値 (1..600 秒)
 - [初期値]: 60

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, SRT100

36.5 メールを送信時に使用するテンプレートの設定

[書式]

mail template template_id mailserv_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* [...]

[設定値及び初期値]

- *template_id*
 - [設定値]: メールテンプレート ID (1..10)
 - [初期値]: -
- *mailserver_id*
 - [設定値]: このテンプレートで使用するメールサーバー ID (1..10)
 - [初期値]: -
- *from_address*
 - [設定値]: 送信元メールアドレス
 - [初期値]: -
- *to_address*
 - [設定値]: 宛先メールアドレス
 - [初期値]: -
- *subject*
 - [設定値]: 送信時の件名
 - [初期値]: Backup Info/Route Change Info/Filter Info/Status Info/Intrusion Info/QAC/TM Info
- *date*
 - [設定値]: メールのヘッダに表示する時刻
 - [初期値]: 送信時の時刻
- *mime_version*
 - [設定値]: メールのヘッダに表示する MIME-Version
 - [初期値]: 1.0
- *content_type*
 - [設定値]: メールのヘッダに表示する Content-Type
 - [初期値]: text/plain;charset=iso-2022-jp
- *switch*
 - [設定値]:

設定値	説明
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

 - [初期値]: off
- *sec*
 - [設定値]: 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 (1..86400 秒)
 - [初期値]: 30

[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。

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, SRT100

36.6 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 route6 route6 [route6 ...]
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 ...]
mail notify id template_id trigger qac-tm qac_type
mail notify id template_id trigger lan-map
no mail notify id [...]
```

[設定値及び初期値]

- *id*
 - [設定値]: 設定番号 (1..10)
 - [初期値]: -
- *template_id*
 - [設定値]: テンプレート ID (1..10)
 - [初期値]: -
- *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
 - [設定値]:

設定値	説明
pp	PP バックアップ
lanN	LAN バックアップ
tunnel	TUNNEL バックアップ

- [初期値]: -
- *range_b*
 - [設定値]:
 - インタフェース番号および範囲指定
 - pp,tunnel のみ (*,xx-yy,zz etc)
 - [初期値]: -
- *route*
 - [設定値]:
 - ネットマスク付きの経路
 - default
 - [初期値]: -
- *route6*
 - [設定値]:
 - プレフィックス長付きの経路

- default
- [初期値]: -
- *if_f*
 - [設定値]: メール通知を行うイーサネットフィルタの設定された LAN インタフェース
 - [初期値]: -
- *dir_f*: フィルタ設定の方向
 - [設定値]:

設定値	説明
in	受信方向
out	送信方向

- [初期値]: -
- *type*: メール通知で通知する情報
 - [設定値]:

設定値	説明
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

- [初期値]: -
- *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)
 - [設定値]:

設定値	説明
pp	PP インタフェース
lanN(N,M,N/M)	LAN インタフェース
wan1	WAN 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

- [初期値]: -
- *range_i*
 - [設定値]:
 - 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)
 - [初期値]: -
- *dir_i*: 不正アクセス検知設定の方向 (Rev10.00.27 以降で利用可)
 - [設定値]:

設定値	説明
in	受信方向
out	送信方向
in/out	受信/送信方向

- [初期値]: -

- `qac_type` : QAC/TM 機能 (Rev10.00.44 以降で利用可)

- [設定値]:

設定値	説明
server-error	管理サーバー情報更新失敗時
unqualified	不適格 PC 接続時

- [初期値]:-

[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、イーサネットフィルタのログ表示、**mail notify status exec** コマンド実行時、および不正アクセス検知時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 (IPv4)	ip route コマンド
経路に対するバックアップ (IPv6)	ipv6 route コマンド

イーサネット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。

QAC/TM 機能については以下の条件が対象となる。

- 管理サーバー情報の更新に失敗したとき
- クライアント PC の接続時の認定で不適格と判定したとき

LAN マップによる異常検知については **switch control use interface** コマンドが設定された LAN インターフェースが対象となる。スナップショット機能による異常を含める場合は **lan-map snapshot use interface** コマンドを設定する必要がある。

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 route6` は RTX1220 Rev.15.04.04 以降のファームウェアで使用可能。

`trigger status` は Rev.10.00 系以降で使用可能。

`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 系以降

`trigger qac-tm` は、Rev.10.00.44 以降の SRT100 で使用可能。

`trigger lan-map` は、Rev.14.01.09 以降で使用可能。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[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 route6 1000::1/64
mail notify 4 1 trigger filter ethernet lan1 in
mail notify 5 1 trigger status all
mail notify 6 1 trigger intrusion lan1 in/out pp * in tunnel 1-3,5 out
mail notify 7 1 trigger lan-map
```

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, SRT100

第 37 章

HTTP サーバー機能

37.1 共通の設定

37.1.1 HTTP サーバー機能の有無の設定

[書式]

```
httpd service switch
no httpd service
```

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
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

- [初期値]: on

[説明]

HTTP サーバーを有効にするか否かを選択する。

[適用モデル]

RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

37.1.2 HTTP サーバーへアクセスできるホストの設定

[書式]

```
httpd host ip_range [ip_range...]
httpd host any
httpd host none
httpd host lan
no httpd host
```

[設定値及び初期値]

- *ip_range*: HTTP サーバーへのアクセスを許可するホストの IP アドレスまたはニーモニック
- [設定値]:

設定値	説明
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	指定したホストからのアクセスを許可する
lanN	LAN インターフェースからのアクセスを許可する
wan1	WAN インターフェースからのアクセスを許可する
bridge1	ブリッジインターフェースからのアクセスを許可する
vlanN	VLAN インターフェースからのアクセスを許可する
lanN/M	タグ VLAN インターフェースからのアクセスを許可する

- [初期値]: -
- *any*
- [設定値]: すべてのホストからのアクセスを許可する
- [初期値]: -

- *none*
 - [設定値]: すべてのホストからのアクセスを禁止する
 - [初期値]: -
- *lan*
 - [設定値]: すべての LAN 側ネットワーク内からのアクセスを許可する
 - [初期値]: lan

[説明]

HTTP サーバー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 インター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 インター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.14.01 系以降のすべてのファームウェアで IP アドレスとニーモニックの混在指定が可能。

ブリッジインターフェースは SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

WAN インターフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

37.1.3 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]
```

[設定値及び初期値]

- *time*
 - [設定値]: 秒数 (1..180)
 - [初期値]: 5

[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。

[適用モデル]

RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

37.1.4 HTTP サーバー機能の listen ポートの設定

[書式]

```
httpd listen port
no httpd listen
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号 (1..65535)
 - [初期値]: 80

[説明]

HTTP サーバーの待ち受けるポートを設定する。

[適用モデル]

RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

37.1.5 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
```

[設定値及び初期値]

- *name*
 - [設定値]: 名前 (64 文字以内)
 - [初期値]: -

[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 (RTX810、RT107e) と WWW ブラウザ設定支援機能 (左記以外) でのみ用いられる。

[適用モデル]

RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

37.2 かんたん設定ページ用の設定

本節のコマンドは、RTX810 および 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。

37.2.1 プロバイダ接続タイプの設定

[書式]

```
provider type provider_type
no provider type [provider_type]
```

[設定値及び初期値]

- *provider_type*
 - [設定値]:

設定値	説明
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

- [初期値]: none

[説明]

プロバイダの接続タイプを設定する。

[適用モデル]

RTX810, RT107e

37.2.2 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]
```

[設定値及び初期値]

- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *name*
 - [設定値]: 名前 (32 文字以内)
 - [初期値]: -

[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]

RTX810, RT107e

37.2.3 プロバイダ接続設定

[書式]

```
provider select peer_num
no provider select peer_num
```

[設定値及び初期値]

- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -

[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]

RTX810, RT107e

37.2.4 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..]
```

[設定値及び初期値]

- *peer_num*
 - [設定値]: 相手先情報番号

- [初期値]:-
- *ip_address*
 - [設定値]: DNS サーバーの IP アドレス (最大 4 つ)
 - [初期値]:-

[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]

RTX810, RT107e

37.2.5 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 server [ip_address [ip_address]]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]:-
- *ip_address*
 - [設定値]: DNS サーバーの IP アドレス (最大 2 つ)
 - [初期値]:-

[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。

[適用モデル]

RTX810, RT107e

37.2.6 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]
```

[設定値及び初期値]

- *peer_num*
 - [設定値]: 相手先情報番号 (1..30)
 - [初期値]:-
- *dns_peer_num*
 - [設定値]: DNS 通知相手先情報番号 (1..30)
 - [初期値]:-

[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]

RTX810, RT107e

37.2.7 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]

[設定値及び初期値]

- *type* : フィルタ型ルーティングの形式
 - [設定値] :

設定値	説明
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

- [初期値] : off

[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。

[適用モデル]

RTX810, RT107e

37.2.8 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]

[設定値及び初期値]

- *interface*
 - [設定値] : LAN インタフェース名
 - [初期値] : -
- *protocol*
 - [設定値] :

設定値	説明
ipv4	IPv4 アドレスを用いたプロバイダ設定の名称
ipv6	IPv6 アドレスを用いたプロバイダ設定の名称

- [初期値] : -
- *type*
 - [設定値] : プロバイダ情報の識別情報 ("PRV" など)
 - [初期値] : -
- *name*
 - [設定値] : ユーザが設定したプロバイダの名称など
 - [初期値] : -

[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。
protocol オプションは省略可能。省略した場合は、IPv4 アドレスを用いたプロバイダ設定の名称とする。

[ノート]

protocol オプションは RTX810 Rev.11.01.06 以降で使用可能。

[適用モデル]

RTX810, RT107e

37.2.9 NTP サーバーの設定

[書式]

```
provider ntpdate server_name
no provider ntpdate [server_name]
```

[設定値及び初期値]

- *server_name*
 - [設定値]: NTP サーバー名 (IP アドレスまたは FQDN)
 - [初期値]: -

[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]

RTX810, RT107e

37.2.10 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]
```

[設定値及び初期値]

- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *ip_address*
 - [設定値]: NTP サーバーの IP アドレス
 - [初期値]: -

[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]

RTX810, RT107e

37.2.11 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]
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	自動接続しない

設定値	説明
off	自動接続する

- [初期値]: off

[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。

[適用モデル]

RTX810, RT107e

37.2.12 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]
```

[設定値及び初期値]

- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *connect*
 - [設定値]:

設定値	説明
on	接続する
off	接続しない

- [初期値]: off

[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。

[適用モデル]

RTX810, RT107e

37.2.13 LAN インタフェースのプロバイダ情報とトンネルとの関連付け

[書式]

```
provider interface bind tunnel_num...
no provider interface bind [tunnel_num...]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -

[説明]

LAN インタフェースのプロバイダ情報とトンネルとの関連付けを設定します。

[適用モデル]
RTX810

第 38 章

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ます。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。

38.1 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]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *switch*
 - [設定値]:

設定値	説明
auto	自動更新する
off	自動更新しない

- [初期値]: auto

[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。

[ノート]

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

38.2 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
```

[設定値及び初期値]

- *interface*

- [設定値]: LAN インタフェース名、WAN インタフェース名
- [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -

[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。

[ノート]

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[拡張ライセンス対応]

[拡張ライセンス](#)をインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

38.3 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]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *host*
 - [設定値]: ホスト名
 - [初期値]: -

[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。

[ノート]

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[拡張ライセンス対応]

[拡張ライセンス](#)をインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

38.4 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]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号 (1..65535)
 - [初期値]: 2002

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

38.5 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
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- all: すべてのインタフェース
 - [初期値]: -

[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。

[ノート]

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[拡張ライセンス対応]

[拡張ライセンス](#)をインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

38.6 ホスト名の登録

[書式]

```
netvolante-dns hostname host interface [server=server_num] host [duplicate]
netvolante-dns hostname host pp [server=server_num] host [duplicate]
netvolante-dns hostname host interface [server=server_num] host ipv6 address [ipv6_address] [duplicate]
netvolante-dns hostname host pp [server=server_num] host ipv6 address [ipv6_address] [duplicate]
netvolante-dns hostname host interface [server=server_num] host ipv6 prefix [ipv6_prefix] [duplicate]
netvolante-dns hostname host pp [server=server_num] host ipv6 prefix [ipv6_prefix] [duplicate]
```

```
no netvolante-dns hostname host interface [server=server_num] [host [duplicate]]
```

```
no netvolante-dns hostname host pp [server=server_num] [host [duplicate]]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *server_num*
 - [設定値]:

設定値	説明
1 または 2	サーバ番号
省略	省略時は 1 が指定されたものとみなす

- [初期値]: -
- *host*
 - [設定値]: ホスト名 (63 文字以内)
 - [初期値]: -
- *ipv6_address*
 - [設定値]: IPv6 アドレス
 - [初期値]: -
- *ipv6_prefix*
 - [設定値]: IPv6 プレフィックス
 - [初期値]: -

[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。

[ノート]

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

ipv6 address および ipv6 prefix は RTX5000 / RTX3500 Rev.14.00.26 以降、RTX1210 Rev.14.01.33 以降、RTX830 Rev.15.02.09 以降、RTX1220 で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

38.7 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]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *time*
 - [設定値]: タイムアウト秒数 (1..180)

- [初期値]: 90

[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。

[ノート]

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

38.8 ホスト名を自動生成するか否かの設定

[書式]

```
netvolante-dns auto hostname interface [server=server_num] switch
netvolante-dns auto hostname interface [server=server_num] ipv6 address [ipv6_address]
netvolante-dns auto hostname interface [server=server_num] ipv6 prefix [ipv6_prefix]
netvolante-dns auto hostname pp [server=server_num] switch
netvolante-dns auto hostname pp [server=server_num] ipv6 address [ipv6_address]
netvolante-dns auto hostname pp [server=server_num] ipv6 prefix [ipv6_prefix]
no netvolante-dns auto hostname interface [switch]
no netvolante-dns auto hostname pp [switch]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インターフェース名、WAN インターフェース名
 - [初期値]: -
- *server_num*
 - [設定値]:

設定値	説明
1 または 2	サーバ番号
省略	省略時は 1 が指定されたものとみなす

- [初期値]: -

- *switch*

- [設定値]:

設定値	説明
on	自動生成する
off	自動生成しない

- [初期値]: off
- *ipv6_address*
 - [設定値]: IPv6 アドレス
 - [初期値]: -
- *ipv6_prefix*
 - [設定値]: IPv6 プレフィックス
 - [初期値]: -

[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、MAC アドレス上 6 桁が "00:a0:de" のときは、『'y'+(MAC アドレス下 6 桁).auto.netvolante.jp』という形になる。MAC アドレス上 6 桁が "00:a0:de" 以外の場合は、『'y'+(MAC アドレス全 12 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。

[ノート]

MAC アドレス上 6 桁が "00:a0:de" 以外の製品に対するホスト名の自動生成には RTX810 Rev.11.01.28 以降、RTX5000 / RTX3500 Rev.14.00.21 以降、RTX1210 Rev.14.01.16 以降のファームウェア、および、Rev.15.02 系以降のすべてのファームウェアで対応している。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

ipv6 address および ipv6 prefix は RTX5000 / RTX3500 Rev.14.00.26 以降、RTX1210 Rev.14.01.33 以降、RTX830 Rev.15.02.09 以降、RTX1220 で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

38.9 シリアル番号を使ったホスト名登録コマンドの設定

[書式]

```
netvolante-dns set hostname interface serial
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名あるいは "pp"
 - [初期値]: -

[説明]

機器のシリアル番号を使ったホスト名を利用するためのコマンドを自動設定する。

本コマンドを実行すると、**netvolante-dns hostname host** コマンドが設定される。

例えば機器のシリアル番号が D000ABCDE の場合、**netvolante-dns set hostname pp serial** を実行すると、**netvolante-dns hostname host pp server=1 SER-D000ABCDE** が設定される。

[ノート]

サブドメインをユーザが指定することはできない。

RTX1100、RTX1500、RT107e は Rev.8.03.82 以降で使用可能。

RTX3000 は Rev.9.00.47 以降で使用可能。

SRT100 は Rev.10.00.46 以降で使用可能。

RTX1200 は Rev.10.01.11 以降で使用可能。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

38.10 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]
```

[設定値及び初期値]

- *ip_address*
 - [設定値]: IP アドレス
 - [初期値]: -
- *name*
 - [設定値]: ドメイン名
 - [初期値]: netvolante-dns.netvolante.jp

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

38.11 ネットボランチ DNS サーバアドレス更新機能の ON/OFF の設定

[書式]

netvolante-dns server update address use [server=*server_num*] *switch*

no netvolante-dns server update address use [server=*server_num*]

[設定値及び初期値]

- *server_num*

- [設定値]:

設定値	説明
1 または 2	サーバ番号
省略	省略時は 1 が指定されたものとみなす

- [初期値]: -

- *switch*

- [設定値]:

設定値	説明
on	サーバアドレスの更新機能を有効にする
off	サーバアドレスの更新機能を停止させる

- [初期値]: on

[説明]

ネットボランチ DNS サーバからの IP アドレスの変更通知を受け取り、設定を自動更新するか否かを設定する。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

38.12 ネットボランチ DNS サーバアドレス更新機能のポート番号の設定

[書式]

netvolante-dns server update address port [server=*server_num*] *port*

no netvolante-dns server update address port [server=*server_num*]

[設定値及び初期値]

- *server_num*

- [設定値]:

設定値	説明
1 または 2	サーバ番号
省略	省略時は 1 が指定されたものとみなす

- [初期値]: -

- *port*

- [設定値]: ポート番号 (1..65535)

- [初期値]: 2002

[説明]

ネットボランチ DNS サーバの IP アドレス更新通知の待ち受けポート番号を設定する。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

38.13 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]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *interval*
 - [設定値]:
 - auto
 - 秒数 (60-300)
 - [初期値]: auto
- *count*
 - [設定値]: 回数 (1-50)
 - [初期値]: 10

[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。WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

38.14 ネットボランチ DNS 登録の定期更新間隔の設定

[書式]

```
netvolante-dns register timer [server=server_num] time
no netvolante-dns register timer [server=server_num]
```

[設定値及び初期値]

- *server_num*
 - [設定値]:

設定値	説明
1 または 2	サーバ番号
省略	省略時は 1 が指定されたものとみなす

- [初期値]: -
- *time*

- [設定値]:

設定値	説明
3600 ... 2147483647	秒数
off	ネットボランチ DNS 登録の定期更新を行わない

- [初期値]: off

[説明]

ネットボランチ DNS 登録を定期的に更新する間隔を指定する。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

38.15 ネットボランチ DNS の自動登録に成功したとき設定を保存するファイルの設定

[書式]

```
netvolante-dns auto save [server=server_num] file
```

```
no netvolante-dns auto save [server=server_num]
```

[設定値及び初期値]

- *server_num*

- [設定値]:

設定値	説明
1 または 2	サーバ番号
省略	省略時は 1 が指定されたものとみなす

- [初期値]: -

- *file*

- [設定値]:

設定値	説明
off	設定の自動保存を行わない
auto	デフォルト設定ファイルに自動保存を行う
番号	自動保存を行うファイル名

- [初期値]: auto

[説明]

ネットボランチ DNS の自動登録に成功したとき、およびネットボランチ DNS サーバからのアドレス通知を受け取ったとき、設定を自動保存するかどうか、および自動保存する場合は保存先のファイル名を指定する。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

第 39 章

UPnP の設定

39.1 UPnP を使用するか否かの設定

[書式]

upnp use *use*

no upnp use

[設定値及び初期値]

- *use*
- [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: off

[説明]

UPnP 機能を使用するか否かを設定する。

[適用モデル]

RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

39.2 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*]

[設定値及び初期値]

- *interface*
- [設定値]:

設定値	説明
LAN インタフェース名	指定した LAN インタフェースの IP アドレスを取得する
WAN インタフェース名	指定した WAN インタフェースの IP アドレスを取得する
default	デフォルトルートのインタフェース

- [初期値]: default
- *peer_num*
- [設定値]:
 - 相手先情報番号
 - anonymous
- [初期値]: -

[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]

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

39.3 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 mapping timer type

[設定値及び初期値]

- *type*

- [設定値]:

設定値	説明
normal	ARP 情報を参照しない
arp	ARP 情報を参照する

- [初期値]: arp

[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消去タイマ値は 3600 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。

[適用モデル]

RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

39.4 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

[設定値及び初期値]

- *time*

- [設定値]:

設定値	説明
600..21474836	秒数
off	消去しない

- [初期値]: 3600

[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、このコマンドを設定する。

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 timertype normal** に設定するようにする。

[適用モデル]

RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

39.5 UPnP の syslog を出力するか否かの設定

[書式]

upnp syslog *syslog*

no upnp syslog

[設定値及び初期値]

- *syslog*

- [設定値]:

設定値	説明
on	UPnP の syslog を出力する
off	UPnP の syslog を出力しない

- [初期値]: off

[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。

[適用モデル]

RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

第 40 章

USB の設定

40.1 USB ホスト機能を使うか否かの設定

[書式]

```
usbhost use switch
no usbhost use [switch]
```

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
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

- [初期値]: on

[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。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

40.2 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]
```

[設定値及び初期値]

- *name*: SYSLOG ファイル名
- [設定値]:

設定値	説明
usb1:filename	USB メモリ内のファイル (<i>filename</i> 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)

- [初期値]: -
- *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
- [設定値]:

設定値	説明
aes128	AES128 で暗号化する。
aes256	AES256 で暗号化する。

- [初期値]: -
- *password*
- [設定値]: 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)
- [初期値]: -

[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

外部メモリに暗号化して保存したファイルは、PC 上で RT-FileGuard を使用して復号することができる。

Rev.10.00.60 以降では、*filename* は半角 99 文字以内。

[適用モデル]

SRT100

40.3 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]]
```

[設定値及び初期値]

- *prefix* : ファイル名のプレフィックス (英数字のみ、15 文字以内)

- [設定値]:

設定値	説明
usb1: <i>filename</i>	ファイル名のプレフィックス

- [初期値]: -

- *term* : 1 つのファイルに含めるデータの期間

- [設定値]:

設定値	説明
monthly	月ごと
daily	日ごと

- [初期値]: monthly

- *crypto* : 暗号アルゴリズムの選択

- [設定値]:

設定値	説明
aes128	AES128 で暗号化する。
aes256	AES256 で暗号化する。

- [初期値]: -
- *password*
 - [設定値]: 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)
 - [初期値]: -

[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

外部メモリに暗号化して保存したファイルは、PC 上で RT-FileGuard を使用して復号することができる。

Rev.10.00.60 以降では、*prefix* に指定可能な文字数は"usb1:"などのプレフィックスを含めずに半角 15 文字以内。上記以外では、*prefix* に指定可能な文字数は"usb1:"などのプレフィックスを含めて半角 15 文字以内。

[適用モデル]
SRT100

40.4 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*]

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
on	許可する
off	許可しない

- [初期値]: on

[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。

[適用モデル]
SRT100

40.5 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*]

[設定値及び初期値]

- *from*
- [設定値]:

設定値	説明
usb1: <i>filename</i>	USB メモリ内の設定ファイル名 (<i>filename</i> は 64 文字以内)

- [初期値]: usb1:config.txt
- *to*
- [設定値]:
 - 内蔵フラッシュ ROM の設定ファイル番号 (0~4)
- [初期値]: 0
- *password*
- [設定値]: 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)
- [初期値]: -

[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 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。

Rev.10.00.60 以降では、*filename* は半角 99 文字以内。

[適用モデル]

SRT100

40.6 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*]

[設定値及び初期値]

• *from*

- [設定値]:

設定値	説明
usb1: <i>filename</i>	USB メモリ内の実行形式ファームウェアファイル名 (<i>filename</i> は 64 文字以内)

- [初期値]: usb1:srt100.bin

• *to*

- [設定値]:
 - 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
- [初期値]: 0

[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。

[ノート]

Rev.10.00.60 以降では、*filename* は半角 99 文字以内。

[適用モデル]

SRT100

40.7 USB バスで過電流保護機能が働くまでの時間の設定

[書式]

usbhost overcurrent duration *duration*

no usbhost overcurrent duration [*duration*]

[設定値及び初期値]

• *duration*

- [設定値]: 時間 (5..100、1 単位が 10 ミリ秒)
- [初期値]: 5 (50 ミリ秒)

[説明]

過電流保護機能が働くまでの時間を設定する。ここで設定した時間、連続して過電流が検出されたら、過電流保護機能が働く。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

第 41 章

スケジュール

41.1 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...
schedule at id [date] time switch switch command...
schedule at id +timer * command...
schedule at id +timer pp peer_num command...
schedule at id +timer tunnel tunnel_num command...
schedule at id +timer switch switch command...
no schedule at id [[date]...]

```

[設定値及び初期値]

- *id*
 - [設定値]: スケジュール番号
 - [初期値]: -
- *date*: 日付 (省略可)
 - [設定値]:
 - 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

- [初期値]: -
- *time*: 時刻
- [設定値]:

設定値	説明
hh:mm[:ss]	時 (0..23 または *): 分 (0..59 または *): 秒 (0..59)、秒は省略可
startup	起動時
usb-attached	USB デバイス認識時
sd-attached	microSD デバイス認識時

- [初期値]: -
- *timer*: *command* を実行するまでの時間 (秒、1..3600)
 - [初期値]: -
- *peer_num*
 - [設定値]:
 - 相手先情報番号
 - anonymous
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェースの番号
 - [初期値]: -
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -
- *command*
 - [設定値]: 実行するコマンド (制限あり)
 - [初期値]: -

[説明]

time で指定した時刻、または *timer* で指定した時間後に、*command* で指定されたコマンドを実行する。

第2、第3、第4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/スイッチでの、**pp select/tunnel select/switch 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。

time は hh:mm 形式で指定されたときは秒指定なしとみなされ、hh:mm:ss 形式で指定されたときは秒指定ありとみなされる。秒数に "-" を用いた範囲指定や "*" による全指定をすることはできない。

以下のコマンドは指定できない。

administrator、**administrator password**、**administrator password encrypted**、**ap select** (※)、**auth user**、**auth user group**、**bgp configure refresh**、**cold start**、**confirm**、**console info** と **console prompt** を除く **console** で始まるコマンド、**copy**、**copy exec**、**date**、**delete**、**echo**、**embedded file**、**exit**、**external-memory performance-test go**、**help**、**http revision-up go**、**http revision-up schedule**、**interface reset**、**ipsec transport template**、**ipv6 bgp configure refresh**、**ipv6 ospf configure refresh**、**less** で始まるコマンド、**load**、**login password**、**login password encrypted**、**login timer**、**login user**、**luac**、**macro**、**make directory**、**nslookup**、**ospf configure refresh**、**packetdump**、**ping**、**ping6**、**pp select** (※)、**quit**、**remote setup**、**rename**、**rollback timer**、**rtfs format**、**rtfs garbage collect**、**save**、**schedule at**、**scp**、**show** で始まるコマンド、**ssh**、**sshd host key generate**、**sshd session**、**switch control function get FUNCTION**、**switch select** (※)、**system packet-buffer**、**telnet**、**telnetd session**、**time**、**timezone**、**traceroute**、**traceroute6**、**tunnel select** (※)、**tunnel template**、**user attribute**

- (※) のコマンドは RTX5000、RTX3500 Rev.14.00.26 以降、RTX1210 Rev.14.01.26 以降、および RTX830 Rev.15.02.03 以降、RTX1220 で指定可能。
- **load** コマンドは RTX1210 Rev.14.01.28 以降、RTX830 Rev.15.02.03 以降、RTX1220 で指定可能。

[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わぬが、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。

第 4 書式は RTX1220、RTX1210、RTX1200、RTX830、RTX810 で使用できる。

usb-attached を指定できるのは Rev.10.01 系以降である。

time パラメータでの秒指定は RTX1200 Rev.10.01.16 以降、および、Rev.11.01 系以降で利用できる。

第 5 ～ 8 書式は RTX5000 / RTX3500 Rev.14.00.32 以降、および、RTX1210 Rev.14.01.41 以降、RTX830 Rev.15.02.03 以降、RTX1220 Rev.15.04.04 以降 で利用できる。

[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
```

- 毎日 12 時から 13 時の間だけ 20 秒間隔で Lua スクリプトを実行する

```
# schedule at 1 12:*:00 * lua script.lua
# schedule at 2 12:*:20 * lua script.lua
# schedule at 3 12:*:40 * lua script.lua
```

- 毎日 3 時にスイッチを再起動する

```
# schedule at 1 */* 03:00 switch 00:a0:de:01:02:03 switch control function execute restart
# schedule at 2 */* 03:00 switch lan1:4 switch control function execute restart
```

- コマンド設定時から 10 分後に再起動する

```
# schedule at 1 +600 * restart
```

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

第 42 章

VLAN の設定

42.1 VLAN ID の設定

[書式]

```
vlan interface/sub_interface 802.1q vid=vid [name=name]
no vlan interface/sub_interface 802.1q
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *sub_interface*
 - [設定値]: 1-32 (RTX5000、RTX3500、RTX3000、RTX1220、RTX1210、RTX1200、RTX830)、1-8 (左記以外の機種)
 - [初期値]: -
- *vid*
 - [設定値]: VLAN ID (IEEE802.1Q タグの VID フィールド格納値) (2 -4094)
 - [初期値]: -
- *name*
 - [設定値]: VLAN に付ける任意の名前 (最大 127 文字)
 - [初期値]: -

[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に設定できる数は以下の通り。

設定できる数	機種
32 個	RTX5000、RTX3500、RTX3000、RTX1220、RTX1210、RTX1200、RTX830
8 個	上記以外の機種

[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い場合は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/port-based-option** オプション) との併用はできない (Rev.10.01 系以前のファームウェアでは "port-based-ks8995m"、Rev.10.01 系以降のファームウェアでは "port-based-option")。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。

RTX1100、RT107e は Rev.8.02.28 以降で使用可能。

[適用モデル]

RTX5000、RTX3500、RTX3000、RTX1500、RTX1220、RTX1210、RTX1200、RTX1100、RTX830、RTX810、RT107e、SRT100

42.2 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]
```

[設定値及び初期値]

- *sw_port*

- [設定値]: スイッチングハブのポート (lan1.1 - lan1.N、lan2.1 - lan2.N)
- [初期値]: -
- *vlan_interface*
 - [設定値]: VLAN インタフェース名 (vlan1 - vlanN)
 - [初期値]: -

[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 / lan2.N を使用する。lan2.N はスイッチインタフェースが 2 個ある機種で指定可能である。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。

RTX5000、RTX3500 では、lan1.N のポートに対して vlan1 ~ vlan4 をマッピングすることができ、lan2.N のポートに対しては vlan5 ~ vlan8 をマッピングすることができる。

スイッチインタフェースが 1 個の機種の初期状態のマッピングは、lan1.N = vlanN となる。

RTX5000、RTX3500 の初期状態のマッピングを下表に示す。

ポート	VLAN
LAN1.1	vlan1
LAN1.2	vlan2
LAN1.3	vlan3
LAN1.4	vlan4
LAN2.1	vlan5
LAN2.2	vlan6
LAN2.3	vlan7
LAN2.4	vlan8

[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。

[設定例]

```
# vlan port mapping lan1.3 vlan2
# vlan port mapping lan1.4 vlan2
```

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

第 43 章

生存通知機能

43.1 生存通知の共有鍵の設定

[書式]

heartbeat pre-shared-key *key*

no heartbeat pre-shared-key

[設定値及び初期値]

- *key*
 - [設定値]: ASCII 文字列で表した鍵 (32 文字以内)
 - [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

43.2 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*]

[設定値及び初期値]

- *switch*
 - [設定値]:
- [初期値]: off
- *option=value*
 - [設定値]:

設定値	説明
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

<i>option</i>	<i>value</i>	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。

- [初期値]:

- log=off
- monitor=off

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

43.3 生存通知の実行

[書式]

```
heartbeat send dest_addr [log=switch]
```

[設定値及び初期値]

- `dest_addr`
 - [設定値]: 送信先ルーターの IPv4 アドレスまたは FQDN
 - [初期値]: -
- `switch`: `syslog` の出力
 - [設定値]:

設定値	説明
on	syslog を出力する
off	syslog を出力しない

- [初期値]: off

[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]

本コマンドを設定する前に、**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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

第 44 章

生存通知機能 リリース 2

生存通知機能とは、ネットワークに接続しているルーターから他拠点のルーターへ、自分の名前と IP アドレスを含めたパケットを送り、通信できる状態であることを通知する機能です。通知パケットを受信したルーターは、通知された名前と IP アドレスをログに出力し、保存します。WAN の IP アドレスが不定となる拠点のルーターから他拠点のルーターへ通信可能であることを知らせる手段として本機能を利用することができます。

リリースについて

前章で説明する従来の生存通知機能はリリース 1、本章で説明する生存通知機能はリリース 2 と区別します。両者の機能概念は同じですが、コマンド体系、動作には互換性がありませんので注意してください。

リリース 2 の特徴

- 生存通知パケットとして UDP / 8512 番ポートを使用します (始点 / 終点ともに)。
- 生存通知を受信したルーターでは、通知された名前によって送信元のルーターを識別します。そのため、生存通知を送信するルーター毎に固有の名前を設定する必要があります。
- 送信側ルーター、受信側ルーターで共通の暗号鍵、および認証鍵を持つことにより、通知情報の暗号化や改竄の検出が可能となります。
- 多対地通信における運用管理を容易にするため、送信 / 受信設定はそれぞれ識別子を指定することで複数設定できるようになっています。ここで、ペアとなる送信側の送信設定と受信側の受信設定は、それぞれ同じ識別子を指定する必要があります。この設定識別子を通知パケットに含めることにより、受信側は任意の通知パケットに対して使用する受信設定を一意に決定します。
- 従来、**schedule** コマンドと組み合わせることで実現していた通知の定期送信は、送信設定コマンドのみで実施できるようになります。
- 通知する IP アドレスは原則として生存通知パケットの送出インタフェースに設定されている IP アドレスとなります。ここで、当該インタフェースに NAT や IP マスカレードが設定されていれば、送出する通知パケットに NAT / IP マスカレード設定を適用した場合の IP アドレスが使用されます。ただし、**unnumbered** 接続の回線を使用して生存通知パケットを送信する場合は、IP アドレスが設定されている LAN インタフェースの中で、若番のインタフェースから優先的に IP アドレスを選択して通知します (通知パケットの IP ヘッダの始点アドレスと同期)。
- 受信した生存通知の情報を **show status heartbeat2** コマンドで表示することができます。

44.1 通知名称の設定

[書式]

```
heartbeat2 myname name
no heartbeat2 myname
```

[設定値及び初期値]

- *name*
 - [設定値]: 生存通知で使用する名称 (1~64 文字/ASCII、1~32 文字/シフト JIS)
 - [初期値]: -

[説明]

生存通知で通知する本機の名前を設定する。

name 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、他の設定では意図した通りに処理されない場合がある。

[ノート]

RTX1100, RTX1500, RT107e は、Rev.8.03.80 以降で使用可能。

RTX3000 は Rev.9.00.43 以降で使用可能。

SRT100 は Rev.10.00.46 以降で使用可能。

RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

44.2 通知設定の定義

[書式]

```
heartbeat2 transmit trans_id [crypto crypto_key] auth auth_key dest_addr ...
no heartbeat2 transmit trans_id
```

[設定値及び初期値]

- *trans_id*
 - [設定値]: 通知設定の識別子 (1..65535)
 - [初期値]: -
- *crypto_key*
 - [設定値]: ASCII 文字列で表した暗号鍵 (1~32 文字)
 - [初期値]: -
- *auth_key*
 - [設定値]: ASCII 文字列で表した認証鍵 (1~32 文字)
 - [初期値]: -
- *dest_addr*
 - [設定値]: 送信先ルーターの IPv4 アドレス、または FQDN(空白で区切って 4 つまで指定可能)
 - [初期値]: -

[説明]

生存通知の定期的な送信設定を定義する。本コマンドで設定した *auth_key* を元に、通知パケットには認証情報が付与される。また、*crypto_key* を指定した場合は更に通知内容が暗号化される。

対応する受信側の設定として **heartbeat2 receive** コマンドを設定する際には、*recv_id* が本コマンドの *trans_id* と一致していなければならない。また同様に、*crypto_key*、*auth_key* も一致させる必要がある。

本コマンドは送信に最低限必要なパラメータを *trans_id* に紐付けて定義するためのものである。実際に送信処理を有効にするには **heartbeat2 transmit enable** コマンドを設定する必要がある。

なお、複数の通知設定による送信負荷を分散させるため、通知設定が有効になってから最初に通知パケットを送信するまでの時間は、通知設定/宛先毎にランダムとなる (ただし 30 秒以内)。

[ノート]

RTX1100, RTX1500, RT107e は Rev.8.03.80 以降で使用可能。

RTX3000 は Rev.9.00.43 以降で使用可能。

SRT100 は Rev.10.00.46 以降で使用可能。

RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

44.3 通知設定の有効化

[書式]

```
heartbeat2 transmit enable [one-shot] trans_id_list
no heartbeat2 transmit enable
```

[設定値及び初期値]

- *trans_id_list*: 有効にしたい通知設定の識別子のリスト
 - [設定値]:
 - 1 個の数字、または間に - をはさんだ数字 (範囲指定)、およびこれらを任意に並べたもの (128 個以内)
 - [初期値]: -

[説明]

定義した通知設定から実際に有効にしたいものを指定する。

識別子のリストは空白で区切って 128 個まで指定することができる。

'one-shot' キーワードを指定した場合は、*trans_id_list* で指定された各設定の通知処理を 1 回だけ実行する。なお、この形式で入力したコマンドは保存できない。

[ノート]

RTX1100, RTX1500, RT107e は Rev.8.03.80 以降で使用可能。

RTX3000 は Rev.9.00.43 以降で使用可能。

SRT100 は Rev.10.00.46 以降で使用可能。

RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

44.4 通知間隔の設定

[書式]

heartbeat2 transmit interval *time*

heartbeat2 transmit interval *trans_id* *time*

no heartbeat2 transmit interval [*time*]

no heartbeat2 transmit interval *trans_id* *time*

[設定値及び初期値]

- *trans_id*
 - [設定値]: 通知設定の識別子
 - [初期値]: -
- *time*
 - [設定値]: 通知間隔秒数 (30..65535)
 - [初期値]: 30

[説明]

trans_id に対応する通知設定の送信間隔を指定する。

trans_id を省略した場合は全ての通知設定が適用対象となる。

ただし、*trans_id* を個別に指定した設定の方が優先して適用される。

[ノート]

RTX1100, RTX1500, RT107e は Rev.8.03.80 以降で使用可能。

RTX3000 は Rev.9.00.43 以降で使用可能。

SRT100 は Rev.10.00.46 以降で使用可能。

RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

44.5 通知を送信した際にログを記録するか否かの設定

[書式]

heartbeat2 transmit log [*trans_id*] *sw*

no heartbeat2 transmit log [*trans_id*]

[設定値及び初期値]

- *trans_id*
 - [設定値]: 通知設定の識別子
 - [初期値]: -
- *sw*
 - [設定値]:

設定値	説明
on	送信した内容を syslog に出力する
off	送信した内容を syslog に出力しない

- [初期値]: off

[説明]

trans_id に対応する通知設定のログ出力に関する設定を行う。sw を 'on' にした場合、生存通知を送信する際に INFO レベルの syslog を出力する。

trans_id を省略した場合は全ての通知設定が適用対象となる。ただし、*trans_id* を個別に指定した設定の方が優先して適用される。

[ノート]

RTX1100, RTX1500, RT107e は Rev.8.03.80 以降で使用可能。

RTX3000 は Rev.9.00.43 以降で使用可能。

SRT100 は Rev.10.00.46 以降で使用可能。

RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

44.6 受信設定の定義

[書式]

```
heartbeat2 receive recv_id [crypto crypto_key] auth auth_key
no heartbeat2 receive recv_id
```

[設定値及び初期値]

- *recv_id*
 - [設定値]: 受信設定の識別子
 - [初期値]: -
- *crypto_key*
 - [設定値]: ASCII 文字列で表した暗号鍵 (1~32 文字)
 - [初期値]: -
- *auth_key*
 - [設定値]: ASCII 文字列で表した認証鍵 (1~32 文字)
 - [初期値]: -

[説明]

生存通知の受信設定を定義する。受信処理を行う際は、通知パケットに含まれる送信側の設定識別子 (*trans_id*) を元に、同じ *recv_id* を持つ本コマンドの設定を使用して復号化、認証チェックが行われる。

対応する送信側の設定として **heartbeat2 transmit** コマンドを設定する際には、*trans_id* が本コマンドの *recv_id* と一致していなければならない。また同様に、*crypto_key*、*auth_key* も一致させる必要がある。

本コマンドは受信に最低限必要なパラメータを *recv_id* に紐付けて定義するためのものである。実際に受信処理を有効にするには **heartbeat2 receive enable** コマンドを設定する必要がある。

[ノート]

RTX1100, RTX1500, RT107e は Rev.8.03.80 以降で使用可能。

RTX3000 は Rev.9.00.43 以降で使用可能。

SRT100 は Rev.10.00.46 以降で使用可能。

RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

44.7 受信設定の有効化

[書式]

```
heartbeat2 receive enable recv_id_list
no heartbeat2 receive enable
```

[設定値及び初期値]

- *recv_id_list* : 有効にしたい受信設定の識別子のリスト
 - [設定値]:
 - 1 個の数字、または間に - をはさんだ数字 (範囲指定)、およびこれらを任意に並べたもの (128 個以内)
 - [初期値]: -

[説明]

定義した受信設定から実際に有効にしたいものを指定する。
識別子のリストは空白で区切って 128 個まで指定することができる。

[ノート]

RTX1100, RTX1500, RT107e は Rev.8.03.80 以降で使用可能。
RTX3000 は Rev.9.00.43 以降で使用可能。
SRT100 は Rev.10.00.46 以降で使用可能。
RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

44.8 受信間隔の監視設定

[書式]

```
heartbeat2 receive monitor time
heartbeat2 receive monitor recv_id time
no heartbeat2 receive monitor [time]
no heartbeat2 receive monitor recv_id time
```

[設定値及び初期値]

- *recv_id*
 - [設定値]: 受信設定の識別子
 - [初期値]: -
- *time* : 監視時間
 - [設定値]:

設定値	説明
30..21474836	秒数
off	受信間隔を監視しない

- [初期値]: off

[説明]

recv_id に対応する受信設定における受信間隔の監視設定を行う。監視が有効な場合は、指定した時間内に生存通知が届かないとき INFO レベルの syslog を出力して SNMP トラップを送出する。

recv_id を省略した場合は全ての受信設定が適用対象となる。ただし、*recv_id* を個別に指定した設定の方が優先して適用される。

[ノート]

RTX1100, RTX1500, RT107e は Rev.8.03.80 以降で使用可能。
RTX3000 は Rev.9.00.43 以降で使用可能。
SRT100 は Rev.10.00.46 以降で使用可能。
RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

44.9 通知を受信した際にログを記録するか否かの設定

[書式]

```
heartbeat2 receive log [recv_id] sw
```

```
no heartbeat2 receive log [recv_id]
```

[設定値及び初期値]

- *recv_id*
 - [設定値]: 受信設定の識別子
 - [初期値]: -
- *sw*
 - [設定値]:

設定値	説明
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

- [初期値]: off

[説明]

recv_id に対応する受信設定のログ出力に関する設定を行う。sw を 'on' にした場合、生存通知を送信する際に INFO レベルの syslog を出力する。

recv_id を省略した場合は全ての受信設定が適用対象となる。ただし、*recv_id* を個別に指定した設定の方が優先して適用される。

[ノート]

RTX1100, RTX1500, RT107e は Rev.8.03.80 以降で使用可能。

RTX3000 は Rev.9.00.43 以降で使用可能。

SRT100 は Rev.10.00.46 以降で使用可能。

RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

44.10 同時に保持できる生存情報の最大数の設定

[書式]

```
heartbeat2 receive record limit num
```

```
no heartbeat2 receive record limit
```

[設定値及び初期値]

- *num*
 - [設定値]: 生存情報の最大保持数 (RTX5000、RTX3500、RTX3000 : 64..10000、それ以外の機種 : 64..1000)
 - [初期値]: 64

[説明]

受信した生存情報を同時に保持できる最大数を設定する。生存情報数が最大に達した状態では新規の情報を取り込むことができない。そのような場合は **clear heartbeat2** コマンドで不要な情報を削除する必要がある。

[ノート]

RTX1500、RTX1100、RT107e は Rev.8.03.80 以降で使用可能。

RTX3000 は Rev.9.00.43 以降で使用可能。

SRT100 は Rev.10.00.46 以降で使用可能。

RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

44.11 生存通知の状態の表示

[書式]

```
show status heartbeat2
show status heartbeat2 id recv_id
show status heartbeat2 name string
```

[設定値及び初期値]

- *recv_id*
 - [設定値]: 受信設定の識別子
 - [初期値]: -
- *string*
 - [設定値]: 文字列 (1~64 文字/ASCII、1~32 文字/シフト JIS)
 - [初期値]: -

[説明]

受信した生存通知の情報を表示する。

第 1 書式では保持している全ての情報を表示する。

第 2 書式では指定の受信設定により受信した情報のみ表示する。

第 3 書式では指定の文字列が通知名称に含まれる情報のみ表示する。

string 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動作し、他の設定では誤動作する可能性がある。

[ノート]

RTX1100, RTX1500, RT107e は Rev.8.03.80 以降で使用可能。

RTX3000 は Rev.9.00.43 以降で使用可能。

SRT100 は Rev.10.00.46 以降で使用可能。

RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

44.12 生存通知の状態のクリア

[書式]

```
clear heartbeat2
clear heartbeat2 id recv_id
clear heartbeat2 name string
```

[設定値及び初期値]

- *recv_id*
 - [設定値]: 受信設定の識別子
 - [初期値]: -
- *string*
 - [設定値]: 文字列 (1~64 文字/ASCII、1~32 文字/シフト JIS)
 - [初期値]: -

[説明]

受信した生存通知の情報をクリアする。

第 1 書式では保持している全ての情報をクリアする。

第 2 書式では指定の受信設定により受信した情報のみクリアする。

第 3 書式では指定の文字列が通知名称に含まれる情報のみクリアする。

string 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動作し、他の設定では誤動作する可能性がある。

[ノート]

RTX1100, RTX1500, RT107e は Rev.8.03.80 以降で使用可能。

RTX3000 は Rev.9.00.43 以降で使用可能。

SRT100 は Rev.10.00.46 以降で使用可能。

RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

第 45 章

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。

45.1 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
```

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
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

- [初期値]: on

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

45.2 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 ip_range [ip_range...]
sntpd host any
sntpd host none
sntpd host lan
no sntpd host
```

[設定値及び初期値]

- *ip_range*: SNTP サーバーへのアクセスを許可するホストの IP アドレスまたはニーモニック
- [設定値]:

設定値	説明
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	指定したホストからのアクセスを許可する
lanN	LAN インターフェースからのアクセスを許可する
wan1	WAN インターフェースからのアクセスを許可する
bridge1	ブリッジインターフェースからのアクセスを許可する

設定値	説明
vlanN	VLAN インターフェースからのアクセスを許可する
lanN/M	タグ VLAN インターフェースからのアクセスを許可する

- [初期値]: -
- *any*
 - [設定値]: すべてのホストからのアクセスを許可する
 - [初期値]: -
- *none*
 - [設定値]: すべてのホストからのアクセスを禁止する
 - [初期値]: -
- *lan*
 - [設定値]: すべての LAN 側ネットワーク内からのアクセスを許可する
 - [初期値]: lan

[説明]

SNTP サーバー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。

WAN インタフェース、ブリッジインタフェースは RTX1210 Rev.14.01.16 以降のファームウェア、RTX1220、RTX830 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

第 46 章

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 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>

46.1 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*]

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
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

- [初期値]: on

[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 カードをカードスロットに差し込んでも認識されない。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

46.2 外部メモリ用キャッシュメモリの動作モードの設定

[書式]

external-memory cache mode *mode*

no external-memory cache mode [*mode*]

[設定値及び初期値]

- *mode*

- [設定値]:

設定値	説明
write-through	ライトスルーモード
copy-back1	コピーバックモード 1
copy-back2	コピーバックモード 2

- [初期値]: copy-back1

[説明]

外部メモリ用キャッシュメモリの動作モードを設定する。ライトスルーモード、コピーバックモード 1、及びコピーバックモード 2 の 3 種類の動作モードをサポートしており、各モードによって FAT、DIR、FILE の各キャッシュ上のデータを外部メモリへ書き出すタイミングが異なる。

各動作モードについて、以下に説明する。

write-through を指定した場合、FAT、DIR、FILE に割り当てられていたキャッシュは、ライトスルーモードで動作し、常に外部メモリへ書き出される。最も安全性が高い。

copy-back1 を指定した場合、FAT と DIR キャッシュはコピーバックモードで動作し、FILE キャッシュは、ライトスルーモードで動作する。ライトスルーモードより高速に動作させることができる。

copy-back2 を指定した場合、FAT、DIR、FILE キャッシュがコピーバックモードで動作する。この設定では、外部メモリへの書き出しが抑制されるので、最も高速に動作する。しかし、外部メモリへ書き出しが完了していない状態が続く為、予期しない電源断が発生すると外部メモリのファイルシステムがダメージを受ける可能性が高くなる。

FAT : File Allocation Table の略

DIR : Directory Entry の略

[ノート]

本コマンドの変更は、外部メモリを接続した時に反映される。外部メモリが既に接続されている状態でコマンドを入力した場合は、一旦、取り外した後に再接続する必要がある。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830, RTX810

46.3 ファイルアクセス高速化用キャッシュメモリのサイズの設定

[書式]

external-memory accelerator cache size *interface size*

no external-memory accelerator cache size *interface* [*size*]

[設定値及び初期値]

- *interface*

- [設定値]:

設定値	説明
usb1	USB ポート 1

設定値	説明
sd1	microSD カードスロット

- [初期値]: -
- *size*
- [設定値]:

設定値	説明
1-5	キャッシュメモリのサイズ (数値が大きいほどメモリサイズが大きい)
off	ファイルアクセス高速化機構を使用しない

- [初期値]: 1

[説明]

ファイルアクセスを高速化するために使用するキャッシュメモリのサイズを設定する。

size に数値を指定した場合は、ファイルアクセスを高速化するための機構が働き、特にディレクトリ数やファイル数の多い構成での外部メモリへのアクセス性能が向上する。アクセス性能が向上しない場合は、*size* を大きくすることで向上することがある。ただし、*size* が大きいほど、外部メモリを接続してから使用可能になるまでの時間が長くなる可能性がある。

size に off を指定した場合は、ファイルアクセスを高速化するためのキャッシュメモリは確保されない。

なお、すべてのインタフェースに対して *size* に最大値を設定した状態で、同時にすべてのインタフェースに外部メモリを接続して使用すると、システム全体の性能に影響を与える可能性があるため、本コマンドを設定してファイルアクセスを高速化するインタフェースは一つに限定することを推奨する。

[ノート]

本コマンドの変更は、外部メモリを接続した時に反映される。外部メモリが既に接続されている状態でコマンドを入力した場合は、一旦、取り外した後に再接続する必要がある。

また、本コマンドで、*size* を大きくしてもアクセス性能が向上しない場合は、下記に示す操作を行うことで、改善されることがある。

- 可能であれば、外部メモリ内のディレクトリやファイルを減らす
- 外部メモリ内の総ディレクトリ数を 2,000 個以内となるように調整する
- 頻繁にアクセスするディレクトリ内の総ファイル数 (ディレクトリ含む) を 20,000 個以内となるように調整する
- ファイル名やディレクトリ名をなるべく短くする (32 文字以内を推奨)

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830, RTX810

46.4 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*]

external-memory statistics filename prefix *prefix* [*crypto password*] [**max-filenum**=*filenum*] [**interval**=*minute*]

no external-memory statistics filename prefix [*prefix* [*term*] [*crypto password*]]

no external-memory statistics filename prefix [*prefix* [*crypto password*] [**max-filenum**=*filenum*] [**interval**=*minute*]]

[設定値及び初期値]

- *prefix*: ファイル名のプレフィックス (半角英数字のみ)
- [設定値]:

設定値	説明
usb1: <i>filename</i>	ファイル名のプレフィックス
sd1: <i>filename</i>	ファイル名のプレフィックス

- [初期値]: -
- *term*: 1 つのファイルに含めるデータの期間
- [設定値]:

設定値	説明
monthly	月ごと
daily	日ごと

- [初期値]: monthly
- *crypto*: 暗号化して保存するときの暗号アルゴリズム
- [設定値]:

設定値	説明
aes128	AES128 で暗号化する
aes256	AES256 で暗号化する

- [初期値]: -
- *password*
 - [設定値]: 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)
 - [初期値]: -
- *filenum*: 外部メモリーに保存する統計情報のファイル数の上限
- [設定値]:

設定値	説明
100 ... 2147483647	外部メモリーに保存する統計情報のファイル数の上限
infinity	外部メモリーに保存する統計情報のファイル数を制限しない

- [初期値]: infinity
- *minute*: 統計情報を外部メモリーに書き出す間隔
- [設定値]:

設定値	説明
2 ... 120	統計情報を外部メモリーに書き出す間隔 (分)

- [初期値]: 12

[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。

[ノート]

term パラメータを指定できる機種では、*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。

term パラメータを指定できない機種では、上限を超えた場合、各種別・インターフェースの統計情報のファイルで最も古いファイルを削除して新しいファイルを作成する。

アプリケーションのトラフィック情報に関しては、*crypto* パラメータの有無にかかわらず、暗号化されない。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	動的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
application	アプリケーションのトラフィック情報

- *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

外部メモリに暗号化して保存したファイルは、PC 上で RT-FileGuard を使用して復号することができる。
 アプリケーションのトラフィック情報は、暗号化して保存することはできない。

Rev.10.01.32 以降では、*prefix* に指定可能な文字数は"usb1:"などのプレフィックスを含めずに半角 15 文字以内。
 上記以外では、*prefix* に指定可能な文字数は"usb1:"などのプレフィックスを含めて半角 15 文字以内。

max-filenum オプションで制限するファイル数は、すべての種別・インターフェースの統計情報を書き出したファイルの合計数となる。

アプリケーションのトラフィック情報に関しては、*interval* の設定によらず 1 分ごとに統計情報が書き出される。

第 1 書式、および第 3 書式は RTX1200 で使用可能。

第 2 書式、および第 4 書式は RTX1200 は使用不可。

第 2 書式、および第 4 書式は RTX1210 は Rev.14.01.34 以降、RTX830 は Rev.15.02.10 以降、RTX1220 で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830

46.5 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] [limit=size] [backup=num] [interval=interval] [line=line]
no external-memory syslog filename [name]
```

[設定値及び初期値]

- *name* : SYSLOG ファイル名
 - [設定値]:

設定値	説明
usb1:filename	USB メモリ内のファイル名 (.bak 拡張子を含む名前は指定できない)
sd1:filename	microSD カード内のファイル名 (.bak 拡張子を含む名前は指定できない)

- [初期値]: -
- *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
- [設定値]:

設定値	説明
aes128	AES128 で暗号化する
aes256	AES256 で暗号化する

- [初期値]: -
- *password*
 - [設定値]: 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)
 - [初期値]: -
- *size*
 - [設定値]: SYSLOG ファイルの上限サイズ (1 - 1024 単位:MB)
 - [初期値]: 10
- *num*
 - [設定値]: バックアップファイルの上限数 (1 - 100)
 - [初期値]: 10
- *interval*
 - [設定値]: SYSLOG を外部メモリに書き出す間隔 (2 - 86400 単位:秒)
 - [初期値]: 2
- *line*
 - [設定値]: SYSLOG を外部メモリに書き出す行数 (1000 - N 単位:行) N ... 各機種のログ記憶容量
 - [初期値]: 1000

[説明]

外部メモリ内に保存する SYSLOG ファイル名を指定する。

name に .bak 拡張子を含むファイル名は指定できない。また、暗号化しない場合、*name* に .rtfg 拡張子を含むファイル名は指定できない。

crypto および *password* を指定した場合、SYSLOG は暗号化してから外部メモリに書き込まれる。暗号化する場合、*name* 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 拡張子が追加される。

SYSLOG ファイルが上限サイズに達すると、SYSLOG ファイルのバックアップが行われる。このとき作成されるバックアップファイルの名前はファームウェアによって異なる。

Rev.11.01 系以降では、バックアップファイル名は *name* で指定されたファイル名の後にバックアップが行われた日時を表す `_yyyymmdd_hhmmss` 形式の文字列が付加されたものとなる。

- yyyy ... 西暦 (4 桁)
- mm ... 月 (2 桁)
- dd ... 日 (2 桁)
- hh ... 時 (2 桁)
- mm ... 分 (2 桁)
- ss ... 秒 (2 桁)

バックアップファイル数が *num* で指定される上限数に達した場合、もしくは外部メモリに空き容量がなくなった場合は、最も古いバックアップファイルを削除してから新しいバックアップファイルが作成される。

RTX1200 では、オプションの *size* や *num* の指定はできない。各パラメータは固定となっており、それぞれ、*size* は、1,024(MB)、*num* は、1 として動作する。また、バックアップファイル名は以下の規則に従って決定される。

name に拡張子が含まれている場合

- 暗号化しないで保存する ... 拡張子を .bak に置き換える
- 暗号化して保存する ... 拡張子の前に _bak を追加する

name に拡張子が含まれていない場合bak という拡張子を追加する

interval で指定した時間が経過した場合、もしくは *line* で指定した行数だけ SYSLOG が出力された場合に、外部メモリに SYSLOG を書き出す。 *line* で指定可能な各機種のログ記憶容量は以下のとおり。

- RTX5000 ... 20000
- RTX3500 ... 20000
- RTX1220 / RTX1210 / RTX830 ... 10000
- RTX810 ... 3000

本コマンドが設定されていないときは SYSLOG は外部メモリに書き込まれない。

[ノート]

以下の変更を行う場合、*name* 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

外部メモリに暗号化して保存したファイルは、PC 上で RT-FileGuard を使用して復号することができる。

RTX1200 Rev.10.01.32 以降、および、Rev.11.01 系以降では、*name* は半角 99 文字以内。
上記以外のリビジョンでは、*name* は半角 64 文字以内。

interval オプションと *line* オプションは、RTX810 Rev.11.01.21 以降のファームウェア、RTX5000/RTX3500 Rev.14.00.18 以降のファームウェアおよび、Rev.14.01 系以降のすべてのファームウェアで使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

46.6 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]
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	許可する
off	許可しない

- [初期値]: on

[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。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

46.7 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]
```

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
on	許可する
off	許可しない

- [初期値]: on

[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。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

46.8 ルーター起動時に外部メモリを検出するまでのタイムアウトを設定する

[書式]

```
external-memory boot timeout time
no external-memory boot timeout [time]
```

[設定値及び初期値]

- *time*
- [設定値]: タイムアウト秒数 (1..30)
- [初期値]: 1

[説明]

ルーター起動時に外部メモリを検出するまでのタイムアウト時間を設定する。

external-memory boot permit on コマンドによって、外部メモリ内のファイルからの起動を許可するに設定されている場合に有効である。

接続認識が遅いデバイスの場合、タイムアウト時間を大きくすることで認識されるようになることがある。

[ノート]

外部メモリ性能測定コマンドで、**boot device attach** で表示される時間を目安にして設定するとよい。

[適用モデル]

RTX830, RTX810

46.9 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]
```

[設定値及び初期値]

- *from*: 外部メモリとファームウェアファイル名
- [設定値]:

設定値	説明
<code>usb1:filename</code>	USB メモリ内のファームウェアファイル名
<code>sd1:filename</code>	microSD カード内のファームウェアファイル名
<code>*:filename</code>	USB メモリおよび microSD カード内のファームウェアファイル名

- [初期値]:
 - *: (機種名).bin (RTX1220、RTX1210、RTX1200、RTX830、RTX810)
 - sd1: (機種名).bin (RTX5000、RTX3500)
- `to`: コピー先ファイル名
- [設定値]:

設定値	説明
0~1	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 (省略時は 0)

- [初期値]: 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 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。

RTX1200 Rev.10.01.32 以降、および、Rev.11.01 系以降のファームウェアでは、`filename` は半角 99 文字以内。上記以外では、`filename` は半角 64 文字以内。

[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 exec 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 exec filename sd1:/test/rtx1200.bin
```

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

46.10 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]

[設定値及び初期値]

- *from* : 外部メモリと設定ファイル名

- [設定値]:

設定値	説明
usb1: <i>filename</i>	USB メモリ内の設定ファイル名
sd1: <i>filename</i>	microSD カード内の設定ファイル名
*: <i>filename</i>	USB メモリおよび microSD カード内の設定ファイル名

- [初期値]:

- *:config.rtfg,*:config.txt (RTX1220、RTX1210、RTX1200、RTX830、RTX810)
- sd1:config.rtfg,sd1:config.txt (RTX5000、RTX3500)

- *to* : コピー先ファイル名

- [設定値]:

設定値	説明
0~4	内蔵フラッシュ ROM の設定ファイル番号 (省略時は 0)

- [初期値]: 0

- *password*

- [設定値]: 復号パスワード (ASCII 文字列で半角 8 文字以上、32 文字以内)

- [初期値]: -

[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 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。

外部メモリに暗号化して保存したファイルは、PC 上で RT-FileGuard を使用して復号することができる。

RTX1200 Rev.10.01.32 以降、および、Rev.11.01 系以降のファームウェアでは、*filename* は半角 99 文字以内。上記以外では、*filename* は半角 64 文字以内。

[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]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

46.11 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]
```

[設定値及び初期値]

- *time*
 - [設定値]:
 - 秒数 (1..600)
 - [初期値]: 300

[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。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

46.12 バッチファイルを実行する

[書式]

```
execute batch
```

[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]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

46.13 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]]
```

[設定値及び初期値]

- *batchfile*: バッチファイル名
 - [設定値]:

設定値	説明
usb1: <i>filename</i>	USB メモリ内のバッチファイル名
sd1: <i>filename</i>	microSD カード内のバッチファイル名
*: <i>filename</i>	USB メモリおよび microSD カード内のバッチファイル名

- [初期値]:
 - *:command.txt (RTX1220, RTX1210, RTX1200, RTX830, RTX810)
 - sd1:command.txt (RTX5000, RTX3500)
- *logfile*
 - [設定値]:

設定値	説明
<i>filename</i>	実行結果ファイル名

- [初期値] : `command-log.txt`

[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。

[ノート]

RTX1200 Rev.10.01.32 以降、および、Rev.11.01 系以降のファームウェアでは、*batchfile* に指定可能な文字数は *logfile* を指定した場合は、半角 99 文字以内。*logfile* を省略した場合は、拡張子を除いて半角 91 文字以内。*filename* に指定可能な文字数は半角 99 文字以内。

上記以外では、*batchfile* に指定可能な文字数は半角 64 文字以内。*filename* に指定可能な文字数は半角 64 文字以内。

[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]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

46.14 外部メモリ性能測定コマンド

[書式]

```
external-memory performance-test go interface
```

[設定値及び初期値]

- *interface*
- [設定値] :

設定値	説明
usb1	USB インタフェース
sd1	microSD インタフェース

- [初期値] :-

[説明]

外部メモリ機能の使用に耐えうる性能を持つメモリであるか否かを確認する。

外部メモリの認識に要する時間やデータの読み書き速度を確認し、一連のテスト終了後、使用に耐えうる性能を持つと判断されれば、

- OK:succeeded

そうでないものは

- NG:failed

と表示する。

[ノート]

外部メモリはフォーマット直後の状態のものを対象とする。

本機能は他の機能を使用していない状態で実行する必要がある。

本コマンド実行中は **syslog debug on**、**no syslog host** が設定される。そのため、**syslog debug off** にしていても DEBUG タイプの SYSLOG が出力されることがある。また、**syslog host** コマンドを設定していても SYSLOG サーバーにログが転送されない。

ヤマハルーターの外部メモリ機能を利用する際に外部メモリに求められる最低限の性能を確認するものであり、本機能の結果はその外部メモリの全ての動作を保証するものではない。
外部メモリ機能を使用する際は、**show status external-memory** コマンドで外部メモリへの書き込みエラーなどが発生していないことを定期的に確認することを推奨する。

RTX1200 は Rev.10.01.11 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

46.15 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* [*script_file* [*args* ...]]

no operation button function download [*function* [*script_file* [*args* ...]]]

[設定値及び初期値]

- *function* : DOWNLOAD ボタンを押した時に実行する機能
 - [設定値] :

設定値	説明
http revision-up	HTTP リビジョンアップ
execute batch	バッチファイルの実行
mobile signal-strength	携帯端末の電波の受信レベルの取得
execute lua	Lua スクリプトの実行

- [初期値] : http revision-up
- *script_file*
 - [設定値] : スクリプトファイル名またはバイトコードファイル名を絶対パスもしくは相対パスで指定する
 - [初期値] : -
- *args*
 - [設定値] : *script_file* に渡す可変個引数
 - [初期値] : -

[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。

function に execute lua を設定した場合、*script_file* を必ず指定する必要がある。*script_file* に相対パスを指定した場合、環境変数 PWD を基点としたパスと解釈される。PWD は **set** コマンドで変更可能であり、初期値は "/" である。

[ノート]

Lua スクリプトを実行させる場合、環境変数 LUA_INIT が設定されていれば *script_file* よりも先に LUA_INIT のスクリプトが実行される。

function パラメータへの mobile signal-strength の指定は Rev.10.01.11 以降で使用可能。

function パラメータへの execute lua の指定は、Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

46.16 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*]

[設定値及び初期値]

- *permit*
- [設定値]:

設定値	説明
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

- [初期値]: off

[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。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

46.17 シグネチャーを保存する外部メモリのディレクトリーの設定

[書式]

```
external-memory dpi signature directory path
no external-memory dpi signature directory [path]
```

[設定値及び初期値]

- *path*
- [設定値]: ディレクトリーのパス(半角 99 文字以内)
- [初期値]: -

[説明]

シグネチャーを保存する外部メモリのディレクトリーを指定する。

DPI が有効になったとき、本コマンドが設定されており、かつ本コマンドで指定されている外部メモリ上のディレクトリーにシグネチャーが存在する場合には、ネットワーク経由のシグネチャーのダウンロードは行わず、外部メモリ上のシグネチャーを使用する。

シグネチャーをダウンロードしたとき、*path* に指定した外部メモリ上のディレクトリーが存在しなければ、ディレクトリーを自動生成して、シグネチャーを保存する。*path* に指定したディレクトリーを含む外部メモリが接続されていない場合、その間にダウンロードしたシグネチャーは保存できない。その後外部メモリが接続された場合には、次のシグネチャー更新時にダウンロードしたシグネチャーが保存される。

次の更新を待たずに外部メモリにシグネチャーをダウンロードしたい場合には、**dpi signature download go** コマンドを **force** オプションを付けて実行すると、シグネチャーの更新がなくとも直ちにダウンロード、および外部メモリへの保存が可能となる。*path* で指定したディレクトリーに以前保存したシグネチャーが存在する場合には、新たにダウンロードしたシグネチャーを既存のシグネチャーに上書きして保存する。

[ノート]

シグネチャーは "rt_dpi_(機種名).ysig" というファイル名で保存される。例えば、RTX830 の場合には、"rt_dpi_rtx830.ysig" となる。*path* に RTFS 上のディレクトリーを指定することはできない。

RTX830 は Rev.15.02.13 以降で使用可能。

[設定例]

- microSD カードの dpi/signature ディレクトリーにシグネチャーを保存する。

```
# external-memory dpi signature directory sd:/dpi/signature
```

[適用モデル]

RTX830

第 47 章

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
```

47.1 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 type [...]
```

[設定値及び初期値]

- *type*
 - [設定値]: 'config' or 'log'
 - [初期値]: -
- *config_no*
 - [設定値]: 0-4.2
 - [初期値]: -
- *directory*
 - [設定値]: 出力先のディレクトリ名
 - [初期値]: -
- *filename*
 - [設定値]: 出力先のファイル名
 - [初期値]: -

[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)。

Rev.10.01.16 以降のバージョンでは、ディレクトリ名、ファイル名に以下を指定することもできる。

文字列	意味
%y	年 (yyyy)

文字列	意味
%m	月 (mm)
%d	日 (dd)
%H	時 (hh)
%M	分 (mm)
%S	秒 (ss)
%n	シリアル番号
%a	LAN1 の MAC アドレス
%P	機種名

ディレクトリ、ファイル名に '%' を含む文字列を指定する場合は、 '%' を続けて指定する必要がある。
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。

[設定例]

「(機種名)/(シリアル番号)/(LAN1 の MAC アドレス)/20100101/120000.txt」というディレクトリとファイルをアップロードする

```
# http upload config %P/%n/%a/%y%m%d/%H%M%S.txt
```

「%config.txt」というファイルをアップロードする

```
# http upload config %%config.txt
```

[適用モデル]

RTX1220, RTX1210, RTX1200

47.2 HTTP アップロード先 URL の設定

[書式]

```
http upload url url
```

```
no http upload url [url]
```

[設定値及び初期値]

- *url*
 - [設定値]: アップロード先の URL
 - [初期値]: -

[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。

[適用モデル]

RTX1220, RTX1210, RTX1200

47.3 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]
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
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

- [初期値]: off

[説明]

HTTP アップロードを許可するか否かを設定する。

[適用モデル]

RTX1220, RTX1210, RTX1200

47.4 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*]

[設定値及び初期値]

- *time*
 - [設定値]: 1-180[秒]
 - [初期値]: 30

[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。

[適用モデル]

RTX1220, RTX1210, RTX1200

47.5 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 [..]

[設定値及び初期値]

- *interval*
 - [設定値]: 1-60[秒]
 - [初期値]: 30
- *count*
 - [設定値]: 1-10
 - [初期値]: 5

[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。

[適用モデル]

RTX1220, RTX1210, RTX1200

47.6 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 [..]

[設定値及び初期値]

- *proxy*
 - [設定値]: プロキシサーバー
 - [初期値]: -
- *port*
 - [設定値]: 1-65535

- [初期値]: 80

[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。

[適用モデル]

RTX1220, RTX1210, RTX1200

47.7 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]

RTX1220, RTX1210, RTX1200

47.8 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*]

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	鳴らす
off	鳴らさない

- [初期値]: on

[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。

[適用モデル]

RTX1220, RTX1210, RTX1200

第 48 章

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 で接続するものだけとなります。この場合、携帯端末を PP(USB モデム)として制御、又は WAN(ネットワークアダプタ)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 U 等)

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。これらの上限值は、PP(USB モデム)として制御する場合には **mobile access limit length** および **mobile access limit time** コマンドで、WAN(ネットワークアダプタ)として制御する場合には **wan access limit time** および **wan access limit length** コマンドで変更することができます。

48.1 新 JATE 番号の認識処理

[書式]

```
jate number
no jate number
```

[説明]

SRT100 では、モバイルインターネット機能を使用するにあたり、JATE の認定番号が新しいものへと変更となるため、認識処理が必要となる。本コマンドの実行を済ませないと **mobile use** コマンドを設定できず、モバイルインターネット機能を使用することはできない。2 回目以降の実行では新しい JATE 認定番号の表示だけを行う。

[ノート]

mobile use コマンドは本コマンド実行後に入力できるようになるので、TFTP や外部メモリの config ファイルなどでは、**mobile use** コマンドよりも前に記述する必要がある。

[適用モデル]

SRT100

48.2 携帯端末を使用するか否かの設定

[書式]

```
mobile use interface use [first-connect-wait-time=time]
no mobile use interface [use]
```

[設定値及び初期値]

- *interface*
 - [設定値]:

設定値	説明
usb1	USB1 をモバイルインターネット接続に使用

- [初期値]: -
- *use*
 - [設定値]:

設定値	説明
on	携帯端末を使用する
off	携帯端末を使用しない

- [初期値]: off
- *time*
- [設定値]:

設定値	説明
0-300	携帯端末アタッチ後の発信抑制秒数

- [初期値]: 0

[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。

first-connect-wait-time オプションは、携帯端末のアタッチ後の発信抑制時間を設定し、網への接続を抑制する。

mobile auto connect コマンドや、**wan1 auto connect** コマンド、**pp always-on** コマンド、**wan1 always-on** コマンドで on が設定されている場合の網への接続要求も、このコマンドで設定された発信抑制秒数のあいだは、発信が抑制される。

[ノート]

first-connect-wait-time オプションは、RTX1200 Rev.10.01.59 以降、RTX810 Rev.11.01.21 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.3 携帯端末に入力する PIN コードの設定

[書式]

```
mobile pin code interface pin
no mobile pin code interface [pin]
```

[設定値及び初期値]

- *interface*
- [設定値]:

設定値	説明
usb1	USB1 インタフェース

- [初期値]: -
- *pin*
- [設定値]: PIN コード
- [初期値]: -

[説明]

USB インタフェースに接続する携帯端末の使用に PIN コードを必要とする場合に、用いる PIN コードを設定する。携帯端末が PIN コードを必要としない場合には、本コマンドの設定に関係なく携帯端末を使用することができる。

[ノート]

PIN コードを利用する場合は、予め携帯端末の接続ユーティリティ等を使用して SIM カードに PIN コードを登録する必要がある。ルーターでは SIM カードに PIN コードを登録することはできない。

SIM カードに登録された PIN コードと本コマンドの設定が一致せず、3 回連続して失敗すると、携帯端末は自動的にロック (PIN ロック) される。PIN ロックがかかるとルーターでは解除できない。携帯端末の接続ユーティリティにて PIN ロック解除コードを入力する必要がある。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.4 モバイルインターネット接続機能の発信方式の設定

[書式]

mobile call type *type*
no mobile call type [*type*]

[設定値及び初期値]

- *type*
 - [設定値]:

設定値	説明
1	発信方式 1
2	発信方式 2

- [初期値]: 1

[説明]

モバイルインターネット接続機能で、発信動作を行うときの方式を設定する。

[ノート]

モバイルインターネット接続機能で接続失敗する場合、本コマンドの設定値を変更することにより接続できるようになる可能性がある。

RTX830 は Rev.15.02.09 以降で使用可能。

RTX1210 は Rev.14.01.33 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830

48.5 携帯端末に直接コマンドを発行する

[書式]

execute at-command *interface command*

[設定値及び初期値]

- *interface*
 - [設定値]:
 - usb1
 - [初期値]: -
- *command*
 - [設定値]:
 - AT コマンド
 - [初期値]: -

[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>,"IP","mopera.net\"
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]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.6 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]
```

[設定値及び初期値]

- *interface*
- [設定値]:

設定値	説明
usb1	USB インタフェース
wan1	WAN インタフェース

- [初期値]: -
- *peer_num*

- [設定値]:

設定値	説明
相手先情報番号	省略時は現在選択している相手先

- [初期値]: -

[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。

[ノート]

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[拡張ライセンス対応]

[拡張ライセンス](#)をインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.7 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]
```

[設定値及び初期値]

- *interface*
- [設定値]:

設定値	説明
usb1	usb1 を使用する

- [初期値]: -

[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。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.8 携帯端末からの自動発信設定

[書式]

mobile auto connect *auto*

no mobile auto connect [*auto*]

[設定値及び初期値]

- *auto*

- [設定値]:

設定値	説明
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

- [初期値]: off

[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。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.9 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*]

[設定値及び初期値]

- *time*

- [設定値]:

設定値	説明
1-21474836	秒数
off	タイマを設定しない

- [初期値]: 60

[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。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.10 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*]

[設定値及び初期値]

- *time*

- [設定値]:

設定値	説明
1-21474836	秒数
off	タイマを設定しない

- [初期値]: 120

[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。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.11 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*]

[設定値及び初期値]

• *time*

- [設定値]:

設定値	説明
1-21474836	秒数
off	タイマを設定しない

- [初期値]: 120

[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。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.12 発信先アクセスポイントの設定

[書式]

mobile access-point name *apn* *cid=cid* [*pdp=type*]**no mobile access-point name** [*apn cid=cid*]

[設定値及び初期値]

• *apn*

- [設定値]: パケット通信に対応したアクセスポイント名 (Access Point Name)
- [初期値]: -

• *cid*

- [設定値]:

設定値	説明
1-10	CID 番号

- [初期値]: -

• *type*

- [設定値]:

設定値	説明
ppp	PDP type を PPP とする
ip	PDP type を IP とする

- [初期値]: -

[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、PDP タイプの割り当てを設定する。なお *pdp=type* を省略すると、通常は *ip* となる。

[設定例]

```
mobile access-point name mopera.net cid=3 (mopera U の場合 )
```

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.13 携帯端末に指示する発信先の設定

[書式]

mobile dial number *dial_string*
no mobile dial number [*dial_string*]

[設定値及び初期値]

- *dial_string*
 - [設定値]: 発信先を指定する文字列
 - [初期値]: -

[説明]

選択されている相手について、携帯端末に ATD に続いて発行する発信先を設定する。

[ノート]

設定がない場合、**mobile access-point name** コマンドで設定された *cid* 番号 [CID] を使って「ATD*99***[CID]#」を発行する。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.14 パケット通信量制限の設定

[書式]

mobile access limit length *length* [alert=*alert*[,*alert_cancel*]]
no mobile access limit length [*length*]

[設定値及び初期値]

- *length*
 - [設定値]:
- | 設定値 | 説明 |
|-----------------------|--------------------------|
| 1-9223372036854775807 | バイト数、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 |
- [初期値]:
 - 50M(RTX1210 Rev.14.01.20 以降、Rev.15.02 系以降)
 - 200000(上記以外)
 - *alert*
 - [設定値]: 警告値、データ長あるいは[%]指定
 - [初期値]: -
 - *alert_cancel*
 - [設定値]: 警告解除値、データ長あるいは[%]指定
 - [初期値]: -

[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。

累積値は、

- **clear mobile access limitation** コマンドの発行
- **mobile access limit duration** コマンドの再設定
- システムの再起動

でクリアされ、発信制限が解除される。

show status pp コマンドで、現在までの累積パケットデータ長を確認できる。

alert で警告値を設定すると、その警告値を上回った時にログに表示することができる。

また **mobile access limit duration** コマンドで累積期間を設定している場合には、*alert_cancel* で指定した警告解除値を

下回った時にログに表示することができる。

警告解除値を指定しない場合は、期間累積のデータ長が 0 になるまで警告を解除しない。

[ノート]

警告値は上限値よりも小さく、警告解除値は警告値よりも小さくなければならない。

携帯端末の packets 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もある。

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。

off を設定したときは警告が表示される。

RTX1200 は Rev.10.01.11 以降で使用可能。

length, *alert*, *alert_cancel* パラメータへの 2147483647 より大きな値の設定は、RTX830 Rev.15.02.03 以降、および RTX1220 で指定可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.15 パケット通信時間制限の設定

[書式]

mobile access limit time *time* [*alert*=*alert*[,*alert_cancel*]] [*unit*=*unit*]

no mobile access limit time [*time*]

[設定値及び初期値]

- time*

- [設定値]:

設定値	説明
1-2147483647	累積通信秒数の上限値
off	タイマを設定しない

- [初期値]: 3600

- alert*

- [設定値]: 警告値、秒数あるいは[%]指定

- [初期値]: -

- alert_cancel*

- [設定値]: 警告解除値、秒数あるいは[%]指定

- [初期値]: -

- unit*

- [設定値]: 単位、second 又は minute

- [初期値]: second

[説明]

選択されている相手について、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。

累積値は、

- **clear mobile access limitation** コマンドの発行
- **mobile access limit duration** コマンドの再設定
- システムの再起動

でクリアされ、発信制限が解除される。

show status pp コマンドで、現在までの累積通信時間を確認できる。

alert で警告値を設定すると、その警告値を上回った時にログに表示することができる。

また **mobile access limit duration** コマンドで累積期間を設定している場合には、**alert_cancel** で指定した警告解除値を下回った時にログに表示することができる。

累積通信時間が警告値に達している間は再接続できない。警告解除値を下回ると再接続できる。

警告解除値を指定しない場合は、期間累積の接続時間が 0 になるまで警告を解除しない。

unit で minute を指定すると、接続時間を分単位で算出する。秒単位は切り上げられる。

[ノート]

警告値は上限値よりも小さく、警告解除値は警告値よりも小さくなければならない。

mobile access limit duration が設定されている場合、**unit=minute** を指定しても、期間内累積時間は、秒単位で加算される。

off を設定したときは警告が表示される。

Rev.10.01.11 以降で使用可能。

unit パラメータは Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.16 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*]

[設定値及び初期値]

- *count*

- [設定値]:

設定値	説明
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

- [初期値]: 5

[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 accept / no pp auth request / 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。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.17 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*]

[設定値及び初期値]

- *accm*

- [設定値]:

設定値	説明
on	用いる
off	用いない

- [初期値]: off

[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。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.18 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 switch
no mobile display caller id [switch]

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
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)

- [初期値]: off

[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。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.19 詳細な SYSLOG を出力するか否かの設定

[書式]

mobile syslog switch
no mobile syslog [switch]

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
on	詳細な SYSLOG を出力する
off	詳細な SYSLOG を出力しない

- [初期値]: off

[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で記録され、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。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.20 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*]

[設定値及び初期値]

- *switch*

- [設定値]:

設定値	説明
on	鳴らす
off	鳴らさない

- [初期値]: on

[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。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.21 接続毎パケット通信量制限の設定

[書式]

mobile access limit connection length length [*alert=alert*]

no mobile access limit connection length [*length*]

[設定値及び初期値]

- *length*

- [設定値]:

設定値	説明
1-9223372036854775807	バイト数、送受信するパケットデータ長の上限值
off	制限しない

- [初期値]: off

- *alert*

- [設定値]: 警告値、データ長あるいは[%]指定

- [初期値]: -

[説明]

選択されている相手について、1 回の接続で送受信するパケットのデータ長の上限值を設定する。上限に達した場合は通信を強制的に切断する。

alert を指定して上限に達する前に警告を発生させることができる。警告はログに表示される。

[ノート]

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もある。
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。

Rev.10.01.11 以降で使用可能。

length, *alert* パラメータへの 2147483647 より大きな値の設定は、RTX830 Rev.15.02.03 以降、および RTX1220 で指定可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.22 接続毎パケット通信時間制限の設定

[書式]

mobile access limit connection time *time* [*alert*=*alert*]

no mobile access limit connection time [*time*]

[設定値及び初期値]

- *time*

- [設定値]:

設定値	説明
1-2147483647	秒数、通信秒数の上限値
off	タイマを設定しない

- [初期値]: off

- *alert*

- [設定値]: 警告値、秒数あるいは[%]指定

- [初期値]: -

[説明]

選択されている相手について、1回の接続の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。

alert を指定して上限に達する前に警告を発生させることができる。警告はログに表示される。

[ノート]

Rev.10.01.11 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.23 通信制限の累積期間の設定

[書式]

mobile access limit duration *duration*

no mobile access limit duration [*duration*]

[設定値及び初期値]

- *duration*

- [設定値]:

設定値	説明
1-2592000(RTX1210 Rev.14.01.20 以降、Rev.15.02 系以降), 1-604800(それ以外)	秒数、通信制限の累積対象の過去の期間
off	過去の全期間を対象とする

- [初期値]: off

[説明]

選択されている相手について、通信制限を行う場合に累積対象となる過去の期間を設定する。

[ノート]

Rev.10.01.11 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.24 携帯端末でパケット着信機能を使用するか否かの設定

[書式]

```
mobile arrive use interface use
no mobile arrive use interface [use]
```

[設定値及び初期値]

- interface*

- [設定値]:

設定値	説明
usb1	USB1 インターフェース

- [初期値]: -

- use*

- [設定値]:

設定値	説明
on	携帯端末でパケット着信機能を使用する
off	携帯端末でパケット着信機能を使用しない

- [初期値]: -

[説明]

指定したインターフェースに接続された携帯端末でモバイルインターネット接続のパケット着信機能を使用するか否かを設定する。

[ノート]

パケット着信機能に対応している携帯端末を使用する場合は、本コマンドを **on** か **off** に必ず設定してください。本コマンドが設定されていない場合は、アタッチされた時点における携帯端末本体のパケット着信機能の設定値が使用されます。

パケット着信機能の詳細は携帯端末の取扱説明書などを参照のこと。

また、パケット着信機能を使用することが可能な携帯端末については以下の URL を参照のこと。

- <http://www.rtpo.yamaha.co.jp/RT/docs/mobile-internet/>

RTX1210 は Rev.14.01.11 以降で使用可能。

RTX810 は Rev.11.01.28 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830, RTX810

48.25 モバイルインターネット機能の着信許可の設定

[書式]

```
mobile arrive permit arrive
no mobile arrive permit [arrive]
```

[設定値及び初期値]

- use*

- [設定値]:

設定値	説明
on	許可する
off	許可しない

- [初期値]: off

[説明]

モバイルインターネット機能で、相手からの着信を許可するか否かを設定する。
on に設定すると、相手からのパケット着信を受けたときに自動接続されるようになる。

[ノート]

mobile arrive use コマンドによって、携帯端末の設定が、"パケット着信機能を使用する"となっている場合に有効である。

RTX1210 は Rev.14.01.11 以降で使用可能。

RTX810 は Rev.11.01.28 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830, RTX810

48.26 電波の受信レベルの取得

[書式]

mobile signal-strength go

[説明]

電波の受信レベルを取得する。

[ノート]

Rev.10.01.11 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.27 電波の受信レベル取得機能の設定

[書式]

mobile signal-strength switch [*option=value*]

no mobile signal-strength [...]

[設定値及び初期値]

- *switch*: 電波の受信レベルの取得を許可するか否か
 - [設定値]:

設定値	説明
on	許可する
off	許可しない

- [初期値]: on
- *option=value*: 取得時のオプション
 - [設定値]:
 - interface
 - 電波の受信レベルを取得するインタフェース
 - syslog
 - 取得結果を INFO レベルで SYSLOG に出力するか否か

設定値	説明
on	出力する

設定値	説明
off	出力しない
trans	圏内、圏外の遷移が発生したときだけ出力する

- interval
 - 定期的に電波の受信レベルを取得する間隔及び回数
 - 間隔

設定値	説明
1..3600	秒数
off	定期的に取得しない

- 回数

設定値	説明
1..1000	回数
infinity	無期限

- [初期値]:
 - interface=usb1
 - syslog=on
 - interval=off

[説明]

電波の受信レベルを取得する際の諸設定を行う。

GUI への表示、**mobile signal-strength go** コマンドや DOWNLOAD ボタンの押下による取得では、本コマンドの設定が適用される。

また、**interval** オプションでは、秒数及び回数をカンマで区切って指定することができる。

interval オプションで秒数及び回数を指定した場合は本コマンド設定後、指定回数に応じて定期的を取得する。

定期的に取得した結果は **show status mobile signal-strength** コマンドで確認できる。

なお、データ通信の開始直前と終了直後は本コマンドの設定に関係なく取得される。

定期的に電波の受信レベルを取得する場合、**syslog** オプションに **trans** を指定していると、電波レベルが圏外から圏内、または圏内から圏外へと遷移したときだけ **SYSLOG** に出力する。

on を指定した場合には、取得した受信レベルを毎回 **SYSLOG** に出力し、それに加えて、電波レベルが圏外、圏内への遷移が発生したときも出力する。

[ノート]

一部の携帯端末では、「網に接続しているとき」あるいは「網から切断されているとき」のみ電波の受信レベルが取得できるものがある。

Rev.10.01.11 以降で使用可能。

interval オプションの回数は RTX1200 Rev.10.01.16 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで指定可能。

syslog オプションの **trans** は RTX810 Rev.11.01.21 以降のファームウェア、および、RTX830 で指定可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.28 定期実行で取得した電波の受信レベルの表示

[書式]

show status mobile signal-strength [reverse]

[設定値及び初期値]

- reverse : 取得時刻の新しいものから順に結果を表示する
 - [初期値]: -

[説明]

mobile signal-strength コマンドの設定で定期的に電波の受信レベルを取得した場合、取得結果を最大 256 件表示する。256 件を超えた場合は古い情報から削除される。このコマンドでは、通常は取得時刻の古いものから順に結果を表示するが、**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。

[ノート]

携帯端末が接続されている状態で USB ボタンを 2 秒以上押し続け、端末とルーターの接続を解除すると、この履歴はクリアされる。

Rev.10.01.11 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

48.29 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
```

[設定値及び初期値]

- *interface* : インタフェース名
 - [設定値]:
 - usb1
 - [初期値]:-
- *command*
 - [設定値]: AT コマンド文字列 (最大 64 文字)
 - [初期値]:-
- *command_list*
 - [設定値]: AT コマンド文字列を空白で区切った並び
 - [初期値]:-

[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 を使ったり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]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.30 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
```

[設定値及び初期値]

- *interface* : インタフェース名
 - [設定値]:
 - usb1
 - [初期値]:-
- *sw*

- [設定値]:

設定値	説明
on	フロー制御を行う
off	フロー制御を行わない

- [初期値]:

- on (下記以外)
- off (Rev.10.01.11 以降)

[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り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。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.31 携帯端末のファームウェア更新

[書式]

mobile firmware update go interface

[設定値及び初期値]

- interface

- [設定値]:

設定値	説明
usb1	USB1 インターフェース

- [初期値]: -

[説明]

指定したインターフェースに接続された携帯端末のファームウェアを更新する。

[ノート]

ソフトウェア更新機能の詳細は携帯端末の取扱説明書などを参照のこと。

また、本コマンドによりファームウェアを更新することが可能な携帯端末については以下の URL を参照のこと。

- <http://www.rtpro.yamaha.co.jp/RT/docs/mobile-internet/>

RTX1210 は Rev.14.01.11 以降で使用可能。

RTX810 は Rev.11.01.28 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830, RTX810

48.32 携帯端末のネットワーク事業者モードの設定

[書式]

mobile carrier mode interface mode

no mobile carrier mode interface [mode]

[設定値及び初期値]

- interface

- [設定値]:

設定値	説明
usb1	USB1 インターフェース

- [初期値]: -

- *mode*
- [設定値]:

設定値	説明
0	工場出荷時の設定
1	ネットワーク事業者モード 1
2	ネットワーク事業者モード 2
3	ネットワーク事業者モード 3

- [初期値]: -

[説明]

指定したインターフェースに接続された携帯端末のネットワーク事業者モードを設定する。

[ノート]

ネットワーク事業者モードを設定することが可能な携帯端末を使用する場合は、本コマンドを設定する必要がある。本コマンドが設定されていない場合は、アタッチされた時点における携帯端末本体のネットワーク事業者モードの設定値が使用される。

すでにアタッチされている携帯端末に対してこのコマンドの設定が変更された場合、次に携帯端末がアタッチされた時点から新しい設定が反映される。

また、本コマンドによりネットワーク事業者モードを設定することが可能な携帯端末については以下の URL を参照のこと。

- <http://www.rtpro.yamaha.co.jp/RT/docs/mobile-internet/>

RTX830 は Rev.15.02.03 以降で使用可能。

RTX1210 は Rev.14.01.26 以降で使用可能。

RTX810 は Rev.11.01.31 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830, RTX810

48.33 自分の名前とパスワードの設定

[書式]

```
wan auth myname myname password
```

```
no wan auth myname [myname password]
```

[設定値及び初期値]

- *wan*
- [設定値]:

設定値	説明
wan1	WAN インタフェース名

- [初期値]: -
- *myname*
 - [設定値]: 名前 (64 文字以内)
 - [初期値]: -
- *password*
 - [設定値]: パスワード (64 文字以内)
 - [初期値]: -

[説明]

モバイルインターネットで、接続時に送信する自分の名前とパスワードを設定する。

[ノート]

SRT100 は Rev.10.00.60 以降で使用可能。
 RTX1200 は Rev.10.01.32 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.34 WAN で使用するインタフェースの設定

[書式]

wan bind interface

no wan bind [*interface*]

[設定値及び初期値]

• *wan*

- [設定値]:

設定値	説明
wan1	WAN インタフェース名

- [初期値]: -

• *interface*

- [設定値]:

設定値	説明
usb1	USB インタフェース名

- [初期値]: -

[説明]

指定した WAN インタフェースについて実際に使用するインタフェースを設定する。

[ノート]

SRT100 は Rev.10.00.60 以降で使用可能。
 RTX1200 は Rev.10.01.32 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.35 携帯端末からの自動発信設定

[書式]

wan auto connect auto

no wan auto connect [*auto*]

[設定値及び初期値]

• *wan*

- [設定値]:

設定値	説明
wan1	WAN インタフェース名

- [初期値]: -

• *auto*

- [設定値]:

設定値	説明
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

- [初期値]: off

[説明]

指定した WAN インタフェースについて自動接続するか否かを設定する。

[ノート]

SRT100 は Rev.10.00.60 以降で使用可能。

RTX1200 は Rev.10.01.32 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.36 携帯端末を切断するタイマの設定

[書式]

wan disconnect time *time*

no wan disconnect time [*time*]

[設定値及び初期値]

- *wan*

- [設定値]:

設定値	説明
wan1	WAN インタフェース名

- [初期値]: -

- *time*

- [設定値]:

設定値	説明
1-21474836	秒数
off	タイマを設定しない

- [初期値]: 60

[説明]

指定した WAN インタフェースについて、送受信がない場合の切断までの時間を設定する。

[ノート]

SRT100 は Rev.10.00.60 以降で使用可能。

RTX1200 は Rev.10.01.32 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.37 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]

wan disconnect input time *time*

no wan disconnect input time [*time*]

[設定値及び初期値]

- *wan*

- [設定値]:

設定値	説明
wan1	WAN インタフェース名

- [初期値]: -

- *time*

- [設定値]:

設定値	説明
1-21474836	秒数
off	タイマを設定しない

- [初期値]: 120

[説明]

指定した WAN インタフェースについて、データ受信がない場合の切断までの時間を設定する。

[ノート]

SRT100 は Rev.10.00.60 以降で使用可能。
 RTX1200 は Rev.10.01.32 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.38 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]

```
wan disconnect output time time
no wan disconnect output time [time]
```

[設定値及び初期値]

- wan

- [設定値]:

設定値	説明
wan1	WAN インタフェース名

- [初期値]: -

- time

- [設定値]:

設定値	説明
1-21474836	秒数
off	タイマを設定しない

- [初期値]: 120

[説明]

指定した WAN インタフェースについて、データ送信がない場合の切断までの時間を設定する。

[ノート]

SRT100 は Rev.10.00.60 以降で使用可能。
 RTX1200 は Rev.10.01.32 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.39 常時接続の設定

[書式]

```
wan always-on switch [time]
no wan always-on
```

[設定値及び初期値]

- wan

- [設定値]:

設定値	説明
wan1	WAN インタフェース名

- [初期値]: -
- *switch*
- [設定値]:

設定値	説明
on	常時接続する
off	常時接続しない

- [初期値]: off
- *time*
- [設定値]: 再接続を要求するまでの秒数 (60..21474836)
- [初期値]: -

[説明]

指定した WAN インタフェースについて、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する。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]

SRT100 は Rev.10.00.60 以降で使用可能。

RTX1200 は Rev.10.01.32 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.40 発信先アクセスポイントの設定

[書式]

wan access-point name apn

no *wan access-point name [apn]*

[設定値及び初期値]

- *wan*
- [設定値]:

設定値	説明
wan1	WAN インタフェース名

- [初期値]: -
- *apn*
- [設定値]: モバイルインターネット通信に対応したアクセスポイント名 (Access Point Name)
- [初期値]: -

[説明]

指定した WAN インタフェースについてアクセスポイント名 (APN) の割り当てを設定する。

[ノート]

SRT100 は Rev.10.00.60 以降で使用可能。

RTX1200 は Rev.10.01.32 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.41 パケット通信量制限の設定

[書式]

`wan access limit length length [alert=alert[,alert_cancel]]`

`no wan access limit length [length]`

[設定値及び初期値]

• *wan*

• [設定値]:

設定値	説明
wan1	WAN インタフェース名

• [初期値]: -

• *length*

• [設定値]:

設定値	説明
1-9223372036854775807	バイト数、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

• [初期値]:

- 50M(RTX1210 Rev.14.01.20 以降、Rev.15.02 系以降)
- 200000(上記以外)

• *alert*

• [設定値]: 警告値、データ長あるいは[%]指定

• [初期値]: -

• *alert_cancel*

• [設定値]: 警告解除値、データ長あるいは[%]指定

• [初期値]: -

[説明]

指定した WAN インタフェースについて、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。

累積値は、

- **clear mobile access limitation** コマンドの発行
- **wan access limit duration** コマンドの再設定
- システムの再起動

でクリアされ、発信制限が解除される。

show status wan1 コマンドで、現在までの累積パケットデータ長を確認できる。

alert で警告値を設定すると、その警告値を上回った時にログに表示することができる。

また **wan access limit duration** コマンドで累積期間を設定している場合には、*alert_cancel* で指定した警告解除値を下回った時にログに表示することができる。

警告解除値を指定しない場合は、期間累積のデータ長が 0 になるまで警告を解除しない。

[ノート]

警告値は上限値よりも小さく、警告解除値は警告値よりも小さくなければならない。

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もある。

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。

off を設定したときは警告が表示される。

SRT100 は Rev.10.00.60 以降で使用可能。

RTX1200 は Rev.10.01.32 以降で使用可能。

length, *alert*, *alert_cancel* パラメータへの 2147483647 より大きな値の設定は、RTX830 Rev.15.02.03 以降、および RTX1220 で指定可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.42 パケット通信時間制限の設定

[書式]

```
wan access limit time time [alert=alert[,alert_cancel]] [unit=unit]
```

```
no wan access limit time [time]
```

[設定値及び初期値]

• wan

- [設定値]:

設定値	説明
wan1	WAN インタフェース名

- [初期値]: -

• time

- [設定値]:

設定値	説明
1-2147483647	累積通信秒数の上限値
off	タイマを設定しない

- [初期値]: 3600

• alert

- [設定値]: 警告値、秒数あるいは[%]指定

- [初期値]: -

• alert_cancel

- [設定値]: 警告解除値、秒数あるいは[%]指定

- [初期値]: -

• unit

- [設定値]: 単位、second 又は minute

- [初期値]: second

[説明]

指定した WAN インタフェースについて、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 **wan disconnect time** コマンドとは独立して動作する。

累積値は、

- **clear mobile access limitation** コマンドの発行
- **wan access limit duration** コマンドの再設定
- システムの再起動

でクリアされ、発信制限が解除される。

show status wan1 コマンドで、現在までの累積通信時間を確認できる。

alert で警告値を設定すると、その警告値を上回った時にログに表示することができる。

また **wan access limit duration** コマンドで累積期間を設定している場合には、*alert_cancel* で指定した警告解除値を下回った時にログに表示することができる。

累積通信時間が警告値に達している間は再接続できない。警告解除値を下回ると再接続できる。

警告解除値を指定しない場合は、期間累積の接続時間が 0 になるまで警告を解除しない。
unit で **minute** を指定すると、接続時間を分単位で算出する。秒単位は切り上げられる。

[ノート]

警告値は上限値よりも小さく、警告解除値は警告値よりも小さくなければならない。
wan access limit duration が設定されている場合、*unit=minute* を指定しても、期間内累積時間は、秒単位で加算される。
off を設定したときは警告が表示される。

SRT100 は Rev.10.00.60 以降で使用可能。
 RTX1200 は Rev.10.01.32 以降で使用可能。

[適用モデル]
 RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.43 接続毎パケット通信量制限の設定

[書式]

wan access limit connection length *length* [*alert=alert*]
no wan access limit connection length [*length*]

[設定値及び初期値]

- *wan*
- [設定値]:

設定値	説明
wan1	WAN インタフェース名

- [初期値]: -
- *length*

- [設定値]:

設定値	説明
1-9223372036854775807	バイト数、送受信するパケットデータ長の上限值
off	制限しない

- [初期値]: off
- *alert*
- [設定値]: 警告値、データ長あるいは[%]指定
- [初期値]: -

[説明]

指定した WAN インタフェースについて、1 回の接続で送受信するパケットのデータ長の上限值を設定する。上限に達した場合は通信を強制的に切断する。
alert を指定して上限に達する前に警告を発生させることができる。警告はログに表示される。

[ノート]

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もある。
 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。

SRT100 は Rev.10.00.60 以降で使用可能。
 RTX1200 は Rev.10.01.32 以降で使用可能。

length, *alert* パラメータへの 2147483647 より大きな値の設定は、RTX830 Rev.15.02.03 以降、および RTX1220 で指定可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.44 接続毎パケット通信時間制限の設定

[書式]

wan access limit connection time time [alert=alert]

no wan access limit connection time [time]

[設定値及び初期値]

- *wan*

- [設定値]:

設定値	説明
wan1	WAN インタフェース名

- [初期値]: -

- *time*

- [設定値]:

設定値	説明
1-2147483647	秒数、通信秒数の上限値
off	タイマを設定しない

- [初期値]: off

- *alert*

- [設定値]: 警告値、秒数あるいは[%]指定

- [初期値]: -

[説明]

指定した WAN インタフェースについて、1 回の接続の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する。

本コマンドは **wan disconnect time** コマンドとは独立して動作する。

alert を指定して上限に達する前に警告を発生させることができる。警告はログに表示される。

[ノート]

SRT100 は Rev.10.00.60 以降で使用可能。

RTX1200 は Rev.10.01.32 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

48.45 通信制限の累積期間の設定

[書式]

wan access limit duration duration

no wan access limit duration [duration]

[設定値及び初期値]

- *wan*

- [設定値]:

設定値	説明
wan1	WAN インタフェース名

- [初期値]: -

• *duration*

- [設定値]:

設定値	説明
1-2592000(RTX1210 Rev.14.01.20 以降、Rev.15.02 系以降), 1-604800(それ以外)	秒数、通信制限の累積対象の過去の期間
off	過去の全期間を対象とする

- [初期値]: off

[説明]

指定した WAN インタフェースについて、通信制限を行う場合に累積対象となる過去の期間を設定する。

[ノート]

SRT100 は Rev.10.00.60 以降で使用可能。

RTX1200 は Rev.10.01.32 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

第 49 章

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收容し、收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。

收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。

49.1 ブリッジインタフェースに收容する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 ...]
```

[設定値及び初期値]

- *bridge_interface*
 - [設定値]: ブリッジインタフェース名
 - [初期値]: -
- *interface*
 - [設定値]:

設定値	説明
lanN	LAN インタフェース名
lanN.M	LAN 分割 インタフェース名
vlanN	VLAN インタフェース名
tunnelN	TUNNEL インタフェース名
tunnelN-tunnelM	TUNNEL インタフェースの範囲

- [初期値]: -

[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收容するインタフェースを指定する。

收容したインタフェース間でブリッジ動作が行われる。

トンネルインタフェースを收容した場合、L2TPv3 トンネルが確立しているトンネルインタフェースでのみブリッジ動作が行われる。

[ノート]

- 收容する LAN インタフェースについて
收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。
收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。
收容する 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收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收容することはできない。
收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。
VLAN インタフェース名を指定できるのは LAN 分割機能の拡張機能に対応した機種のみである。

・収容するトンネルインタフェースについて
 収容するトンネルインタフェースの MTU は無効となり、トンネルインタフェースでフラグメントは行われず、カプセル化されたパケットの送信インタフェースの MTU に従ってフラグメントが発生する。
 いずれかのブリッジインタフェースに収容したインタフェースは、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としてトンネルインタフェースを設定できるのは L2TPv3 機能が実装されているモデルのみである。

・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 インタフェースまたはトンネル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。

RTX830、RTX810 では、トンネルインタフェースの範囲指定に対応していない。

RTX5000 は Rev.14.00.12 以降で使用可能。
 RTX3500 は Rev.14.00.12 以降で使用可能。
 RTX810 は Rev.11.01.21 以降で使用可能。
 RTX1200 は Rev.10.01.53 以降で使用可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、ブリッジインターフェースに収容できるインターフェース (*interface*) の最大個数が拡張される。

- *interface*

ライセンス名	拡張後の最大個数
YSL-VPN-EX1	10

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

49.2 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]
```

[設定値及び初期値]

- *bridge_interface*
 - [設定値]: ブリッジインタフェース名
 - [初期値]: -
- *switch*
 - [設定値]:

設定値	説明
on	ラーニングする
off	ラーニングしない

- [初期値]: on

[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。

RTX5000 は Rev.14.00.12 以降で使用可能。

RTX3500 は Rev.14.00.12 以降で使用可能。

RTX810 は Rev.11.01.21 以降で使用可能。

RTX1200 は Rev.10.01.53 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

49.3 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]

[設定値及び初期値]

- *bridge_interface*
 - [設定値]: ブリッジインタフェース名
 - [初期値]: -
- *time*
 - [設定値]:

設定値	説明
30..32767	秒数
off	タイマを設定しない

- [初期値]: 300

[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。

[ノート]

RTX5000 は Rev.14.00.12 以降で使用可能。

RTX3500 は Rev.14.00.12 以降で使用可能。

RTX810 は Rev.11.01.21 以降で使用可能。

RTX1200 は Rev.10.01.53 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

49.4 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]
```

[設定値及び初期値]

- *bridge_interface*
 - [設定値]: ブリッジインタフェース名
 - [初期値]: -
- *mac_address*
 - [設定値]: MAC アドレス
 - [初期値]: -
- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -

[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* に收容された 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* に收容されていない場合、登録した情報は無視される。

RTX5000 は Rev.14.00.12 以降で使用可能。

RTX3500 は Rev.14.00.12 以降で使用可能。

RTX810 は Rev.11.01.21 以降で使用可能。

RTX1200 は Rev.10.01.53 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

第 50 章

QAC/TM

QAC/TM 機能は、LAN 配下の PC におけるアンチウイルスクライアントソフトウェアのインストール状況やウイルスパターンファイルならびにウイルス検索エンジンのバージョンを確認して、その結果に応じて PC がアクセスできるネットワークを制御します。

クライアントソフトウェアがインストールされていて最新のウイルスパターンファイルとウイルス検索エンジンを使用している PC (以下、適格 PC) には LAN 側と WAN 側の全てのネットワークへのアクセスを許可し、クライアントがインストールされていなかったり古いウイルスパターンファイルもしくはウイルス検索エンジンを使っている PC (以下、不適格 PC) に対しては L3 ルーティングでのセグメント越えを禁止して LAN 側の特定ネットワークへのアクセスのみに制限するなど、適格 PC と不適格 PC で異なるアクセス権を与えることができます。

適格 PC と不適格 PC に異なるアクセス権を与えるしくみには DHCP 認証機能を応用します。適格 PC に対してはプライマリネットワークに対応する IP アドレスを、不適格 PC にはセカンダリネットワークに対応する IP アドレスを割り当て、イーサネットフィルター機能やポリシーフィルター機能を組み合わせてアクセスを制御します。

対応しているアンチウイルスソフトウェアおよびバージョン

- トレンドマイクロ株式会社
 - ウイルスバスター コーポレートエディション 8.0 以上
 - Trend Micro ビジネスセキュリティ 5.0 以上

50.1 QAC/TM 機能で使用するアンチウイルスソフトウェアの設定

[書式]

```
qac-tm use type
no qac-tm use
```

[設定値及び初期値]

- *type*: 使用するアンチウイルスソフトウェア
- [設定値]:

設定値	説明
off	QAC/TM 機能を使用しない
biz	Trend Micro ビジネスセキュリティ
corp	ウイルスバスター コーポレートエディション

- [初期値]: off

[説明]

QAC/TM 機能で使用するアンチウイルスソフトウェアを設定する。

[ノート]

SRT100 は、Rev.10.00.44 以降で使用可能。

[適用モデル]

SRT100

50.2 アンチウイルスソフトウェアの管理サーバーの設定

[書式]

```
qac-tm server ip_address port [protocol=protocol]
no qac-tm server
```

[設定値及び初期値]

- *address*
- [設定値]:

設定値	説明
IP アドレス	管理サーバ PC の IP アドレス

設定値	説明
url	管理サーバ PC の URL

- [初期値]: -
- *port*
 - [設定値]: 管理サーバ PC へアクセスするポート番号
 - [初期値]: -
- *protocol*: サーバ情報を取得するときに使用するプロトコル
 - [設定値]:

設定値	説明
http	http を使用する
https	https を使用する

- [初期値]: http

[説明]

アンチウイルスソフトウェア管理サーバ PC の IP アドレスとポート番号を設定する。

[ノート]

HTTPS は、Rev.10.00.46 以降で使用可能。

[適用モデル]

SRT100

50.3 有効なウイルスパターンファイルとウイルス検索エンジンのバージョン範囲の設定

[書式]

```
qac-tm version margin pattern [engine] [os=os]  
no qac-tm version margin
```

[設定値及び初期値]

- *pattern*: 有効なウイルスパターンファイルと判定するバージョン範囲
 - [設定値]:
 - 0 - 100(世代)
 - 0.001.00 - 99.999.99
 - [初期値]: 3
- *engine*: 有効なウイルス検索エンジンと判定するバージョン範囲
 - [設定値]:

設定値	説明
all	すべて有効
recent	最新のみ有効
範囲	0.001.0000 - 99.999.9999

- [初期値]: recent
- *os*: 優先して判定するアンチウイルスソフトウェアの OS バージョン
 - [設定値]:

設定値	説明
32bit	32bitOS 用
64bit	64bitOS 用

- [初期値]: 32bit

[説明]

ウイルスパターンファイルとウイルス検索エンジンが有効と判定するバージョン範囲を設定する。

os オプションを設定することで、ウイルスパターンファイルとウイルス検索エンジンのバージョン確認を優先して行う OS のバージョンを指定することができる。

[ノート]

管理サーバー及びクライアントから取得できるアンチウイルスソフトウェア情報からは、使用している OS が 32 ビットバージョンか 64 ビットバージョンかを判定できないため、*os* オプションで指定した OS バージョンを判定に使用する。

SRT100 は、Rev.10.00.44 以降で使用可能。

[適用モデル]

SRT100

50.4 警告画面に表示するクライアントインストール URL の設定

[書式]

qac-tm redirect *url*

no qac-tm redirect

[設定値及び初期値]

- *url*
 - [設定値]: 管理サーバー Web コンソールのクライアントインストール画面の URL
 - [初期値]: 規定のクライアントインストール画面の URL

[説明]

警告画面に表示する管理サーバー Web コンソールのクライアントインストール画面の URL を設定する。ポート番号を指定するときは URL にポート番号を含めて設定する。

[ノート]

SRT100 は、Rev.10.00.44 以降で使用可能。

[適用モデル]

SRT100

50.5 クライアント PC のアンチウイルスソフトウェアバージョン情報を取得するポート番号の設定

[書式]

qac-tm client_port *port* [*port*...]

no qac-tm client_port

[設定値及び初期値]

- *port*
 - [設定値]: 空白で区切られたポート番号の並び (10 個以内)
 - [初期値]: -

[説明]

クライアント PC にインストールしているアンチウイルスソフトウェアのバージョン情報を取得するポート番号を設定する。

[ノート]

SRT100 は、Rev.10.00.44 以降で使用可能。

Rev.10.00.46 以降で複数のポート番号を設定可能。

[適用モデル]

SRT100

50.6 クライアント PC にインストールしているアンチウイルスソフトウェアのウイルスパターンファイルとウイルス検索エンジンの自動アップデートの設定

[書式]

qac-tm client update *sw*[*port*]

no qac-tm client update**[設定値及び初期値]**

- *sw*

- [設定値]:

設定値	説明
on	自動アップデートを行う
off	自動アップデートを行わない

- [初期値]: off

- *port*: 自動アップデート指示を送信する UDP ポート番号

- [設定値]:

- 1 - 65535

- [初期値]: 52225

[説明]

本機能を使用する場合は、クライアント PC にエージェント (QAC/TM エージェント) をインストールしている必要がある

[ノート]

SRT100 は、Rev.10.00.46 以降で使用可能。

[適用モデル]

SRT100

50.7 QAC/TM でチェックを行う HTTP のポート番号の設定**[書式]**

```
qac-tm port port [port...]
```

```
no qac-tm port
```

[設定値及び初期値]

- *port*

- [設定値]: 空白で区切られたポート番号の並び (4 個以内)

- [初期値]: 80

[説明]

QAC/TM でチェックを行う HTTP のポート番号を設定する。

[ノート]

SRT100 は、Rev.10.00.44 以降で使用可能。

[適用モデル]

SRT100

50.8 不適格クライアント PC のアクセス制御設定**[書式]**

```
qac-tm unqualified client access control type [server-error=server_error_type] [dhcp-not-bind=dhcp_not_bind_type]
```

```
no qac-tm unqualified client access control
```

[設定値及び初期値]

- *type*

- [設定値]:

設定値	説明
pass	Web アクセスを許可する
reject	Web アクセスを禁止する

- [初期値]: reject

- *server_error_type*

- [設定値]:

設定値	説明
pass	Web アクセスを許可する
reject	Web アクセスを禁止する

- [初期値]: pass
- *dhcp_not_bind_type*

- [設定値]:

設定値	説明
pass	Web アクセスを許可する
reject	Web アクセスを禁止する

- [初期値]: pass

[説明]

QAC/TM により不適格 PC とされたクライアントの Web アクセス制御を本コマンドの設定にしたがって処理する。
server-error=pass の場合、設定誤りにより管理サーバーへアクセスできないとき、または管理サーバーから応答が得られなかったときはパケットを通過させる。

dhcp-not-bind=pass の場合、DHCP による IP アドレス割り当てをされていないクライアントのパケットを通過させる。

[ノート]

SRT100 は、Rev.10.00.44 以降で使用可能。

[適用モデル]

SRT100

50.9 アンチウイルスソフトウェア情報のチェックなしに認定されるクライアントの設定

[書式]

```
qac-tm client permit mac_address
no qac-tm client permit mac_address
```

[設定値及び初期値]

- *mac_address*: クライアントの MAC アドレス
 - [設定値]:
 - xx:xx:xx:xx:xx:xx (xx は 16 進数)
 - [初期値]: -

[説明]

アンチウイルスソフトウェアのバージョン情報のチェックを行わずに認定されるクライアント PC を設定する。

[ノート]

SRT100 は、Rev.10.00.44 以降で使用可能。

[適用モデル]

SRT100

50.10 QAC/TM で表示する警告画面の設定

[書式]

```
qac-tm warning url url
no qac-tm warning url
```

[設定値及び初期値]

- *url*
 - [設定値]: 不適格 PC の Web アクセスで表示する警告画面の URL
 - [初期値]: ルーターが用意する警告画面の URL

[説明]

不適格 PC からの Web アクセス時に表示する警告画面の URL を設定する。

[ノート]

SRT100 は、Rev.10.00.46 以降で使用可能。

[適用モデル]

SRT100

50.11 管理サーバーのアンチウイルスソフトウェアパターンファイル情報を更新する

[書式]

```
qac-tm server refresh go
```

[説明]

管理サーバーで管理しているアンチウイルスソフトウェアのウイルスパターンファイル及びウイルス検索エンジンのバージョン情報の更新を行う。

[ノート]

SRT100 は、Rev.10.00.44 以降で使用可能。

[適用モデル]

SRT100

50.12 クライアント PC のアンチウイルスソフトウェアパターンファイル情報を更新する

[書式]

```
qac-tm client refresh go ip_address [prompt]
```

[設定値及び初期値]

- *ip_address*
 - [設定値]:

設定値	説明
all	すべてのクライアント PC
IP アドレス	更新するクライアント PC の IP アドレス (xxx.xxx.xxx.xxx(xxx は十進数))

- [初期値]: -
- *prompt*
 - [設定値]: コマンド実行後すぐにプロンプトを表示する
 - [初期値]: -

[説明]

クライアント PC のアンチウイルスソフトウェアのウイルスパターンファイル及びウイルス検索エンジンのバージョン情報の更新を行う。

管理サーバーの情報を更新した場合、または、クライアント PC のウイルスパターンファイル及び検索エンジンのアップデートを行った場合にルーター内の情報を最新の状態へ更新する。

[ノート]

SRT100 は、Rev.10.00.46 以降で使用可能。

[適用モデル]

SRT100

50.13 QAC/TM の状態の表示

[書式]

```
show status qac-tm
show status qac-tm server
show status qac-tm client
show status qac-tm qualified
```

show status qac-tm unqualified

[説明]

QAC/TM の状態を表示する。

[ノート]

SRT100 は、Rev.10.00.44 以降で使用可能。

[適用モデル]

SRT100

第 51 章

Lua スクリプト機能

Lua 言語で記述されたスクリプトを実行する機能です。Lua スクリプトにヤマハルーター専用 API を埋め込むことで、ルーターの状態に応じて、ルーターの設定変更やアクションをプログラミングすることが可能になります。

51.1 Lua スクリプト機能を有効にするか否かの設定

[書式]

```
lua use switch
no lua use [switch]
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	有効にする
off	無効にする

- [初期値]: on

[説明]

Lua スクリプト機能を有効にするか否かを設定をする。

Lua スクリプトの走行中に当コマンドで Lua スクリプト機能を無効にした場合、走行中のすべての Lua スクリプトは強制終了される。

[ノート]

SRT100 は Rev.10.00.52 以降で使用可能。

RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

51.2 Lua スクリプトの実行

[書式]

```
lua [-e stat] [-l module] [-v] [--] [script_file [args ...]]
```

[設定値及び初期値]

- *stat*
 - [設定値]: スクリプト文字列
 - [初期値]: -
- *module*
 - [設定値]: ロード (require する) モジュール名
 - [初期値]: -
- *script_file*
 - [設定値]: スクリプトファイル名またはバイトコードファイル名を絶対パスもしくは相対パスで指定する
 - [初期値]: -
- *args*
 - [設定値]: *script_file* に渡す可変個引数
 - [初期値]: -

[説明]

Lua スクリプトを実行する。

基本的な文法は Lua 標準の **lua** コマンドと同じであるが、標準入力 (stdin) をスクリプトの入力対象とする **-i/-** オプションと、パラメータなしの実行には対応していない。**-v** オプションはバージョン情報を出力する。**--** オプションは記述したポイントでオプション処理を終了することを表し、*script_file* や *args* に "-" で始まるファイル名および文字列を指定できるようになる。なお、**-e/-l/-v** の各オプションは繰り返して複数個指定できるが *script_file* よりも後に指定することはできない。*script_file* は 1 つしか指定できず、*script_file* を記述したポイント以降のパラメータはすべて無視される。このとき、エラーメッセージは出力されない。

script_file に相対パスを指定した場合、環境変数 **PWD** を基点としたパスと解釈される。**PWD** は **set** コマンドで変更可能であり、初期値は "/" である。

[ノート]

環境変数 **LUA_INIT** が設定されている場合は、そのスクリプトが最初に実行される。

script_file にバイトコードファイルを指定する場合、ルーター上で生成したバイトコードだけが実行可能であり、Lua をインストールした PC 等で生成したバイトコードは実行できない。

SRT100 は Rev.10.00.52 以降で使用可能。

RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

51.3 Lua コンパイラの実行

[書式]

```
luac [-l] [-o output_file] [-p] [-s] [-v] [--] script_file [script_file ..]
```

[設定値及び初期値]

- *output_file*
 - [設定値]: バイトコードの出力先のファイル名を絶対パスもしくは相対パスで指定する
 - [初期値]: luac.out (相対パス)
- *script_file*
 - [設定値]: コンパイル対象のスクリプトファイル名を絶対パスもしくは相対パスで指定する
 - [初期値]: -

[説明]

Lua コンパイラを実行し、バイトコードを生成する。

基本的な文法は Lua 標準の **luac** コマンドと同じであるが、**-** オプションは指定できない。**-l** オプションは生成したバイトコードをリスト表示する。**-p** オプションは構文解析のみを行う。**-s** オプションはコメント等のデバッグ情報を取り除く。**-v** オプションはバージョン情報を出力する。**--** オプションは記述したポイントでオプション処理を終了することを表し、*script_file* に "-" で始まるファイル名を指定できるようになる。なお、*script_file* を複数指定して、一つのバイトコードファイルにまとめることもできる。

script_file/output_file に相対パスを指定した場合、環境変数 **PWD** を基点としたパスと解釈される。**PWD** は **set** コマンドで変更可能であり、初期値は "/" である。

[ノート]

SRT100 は Rev.10.00.52 以降で使用可能。

RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

51.4 Lua スクリプトの走行状態の表示

[書式]

`show status lua [info]`

[設定値及び初期値]

- `info` : 表示する情報の種類
- [設定値] :

設定値	説明
running	走行中のスクリプトに関する情報
history	過去に走行したスクリプトに関する情報
省略	すべての情報を表示する

- [初期値] :-

[説明]

現在の Lua スクリプトの走行状態や過去の走行履歴を表示する。この情報は `lua use` コマンドで Lua スクリプト機能を無効にするとクリアされる。

- Lua のバージョン情報
- 走行中のスクリプト[running]
 - Lua タスク番号
 - 走行状態

RUN	走行中
SLEEP	スリープ中
WATCH	SYSLOG 監視中 (Lua タスクはスリープしている)
COMMUNICATE	通信中
TERMINATE	強制終了中

- トリガ
 - `lua` コマンド
 - `luac` コマンド
 - スケジュール
 - DOWNLOAD ボタン
- コマンドライン
- スクリプトファイル名
- 監視文字列 (SYSLOG 監視中のとき)
- 開始日時/走行時間
- 過去に走行したスクリプト[history] (最新 10 種類まで新しい順に表示)
 - トリガ
 - `lua` コマンド
 - `luac` コマンド
 - スケジュール
 - DOWNLOAD ボタン
 - コマンドライン
 - スクリプトファイル名
 - 走行回数/エラー発生回数/エラー履歴 (最新 5 回分まで新しい順に表示)
 - 前回の開始日時/終了時間/走行結果

[ノート]

SRT100 は Rev.10.00.52 以降で使用可能。

RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

51.5 Lua スクリプトの強制終了

[書式]

```
terminate lua task_id
```

```
terminate lua file script_file
```

[設定値及び初期値]

- *task_id*: 強制終了する Lua タスクの番号

- [設定値]:

設定値	説明
all	すべての Lua タスク番号
1..10 (DOWNLOAD ボタン非搭載の機種では 1..9)	Lua タスクの番号

- [初期値]: -

- *script_file*

- [設定値]: 強制終了するスクリプトファイル名またはバイトコードファイル名を絶対パスもしくは相対パスで指定する

- [初期値]: -

[説明]

指定した Lua タスク、または、Lua スクリプトを強制終了する。

第 1 書式では、*task_id* で指定された Lua タスクを強制終了する。Lua タスクの番号や実行しているスクリプトについては **show status lua** コマンドで確認できる。

第 2 書式では、*script_file* で指定されたパスとファイル名が完全に一致するスクリプトを実行しているすべての Lua タスクを強制終了する。*script_file* に相対パスを指定した場合、環境変数 PWD を基点とする絶対パスに置換された後で対象の Lua タスクの検索が行われる。

lua コマンドの **-e** オプションを使用して、スクリプトファイルを使用せずに実行されているような Lua スクリプトを強制終了させる場合は、第 1 書式を使用する。

[ノート]

SRT100 は Rev.10.00.52 以降で使用可能

RTX1200 は Rev.10.01.16 以降で使用可能

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

51.6 Lua スクリプ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 lua switch
```

```
no alarm lua [switch]
```

[設定値及び初期値]

- *switch*

- [設定値]:

設定値	説明
on	鳴らす
off	鳴らさない

- [初期値]: on

[説明]

Lua スクリプ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。

[ノート]

本コマンドでは、DOWNLOAD ボタンによる Lua スクリプトの実行に関するアラーム音を鳴らすか否かの設定ができる。ハードウェアライブラリでの制御によるアラーム音を鳴らすか否かは、**alarm entire** コマンドの設定に従う。

RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

第 52 章

カスタム GUI

カスタム GUI とは、ルーターの設定を行うための GUI (WWW ブラウザに対応するユーザインタフェース) をユーザが独自に設計し組み込むことができる機能です。ルーターにはホストから HTTP で設定を転送するためのインタフェースが用意されており、ユーザは JavaScript を使用して GUI を作成します。

ヤマハルーターには WWW ブラウザ設定支援機能が搭載されていますが、ユーザごとに設定画面を変更することはできませんでした。本機能では、カスタム GUI を複数組み込み、ログインするユーザによって画面を切り替えることが可能です。

52.1 カスタム GUI を使用するか否かの設定

[書式]

```
httpd custom-gui use use
no httpd custom-gui use [use]
```

[設定値及び初期値]

- *use*
- [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: off

[説明]

カスタム GUI を使用するか否かを設定する。

[ノート]

SRT100 は Rev.10.00.52 以降で使用可能。 RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

52.2 カスタム GUI を使用するユーザの設定

[書式]

```
httpd custom-gui user [user] directory=path [index=name]
no httpd custom-gui user [user...]
```

[設定値及び初期値]

- *user*
 - [設定値]: ユーザー名
 - [初期値]: -
- *path*
 - [設定値]: 基点となるディレクトリの絶対パスまたは相対パス
 - [初期値]: -
- *name*
 - [設定値]: スラッシュ '/' 止めの URL でアクセスした場合に出力するファイル名
 - [初期値]: index.html

[説明]

カスタム GUI を使用するユーザを設定する。 `http://(ルーターの IP アドレス)/` にアクセスし、本コマンドで登録されているユーザ名でログインすると `http://(ルーターの IP アドレス)/custom/user/` にリダイレクトされる。

user を省略した場合には無名ユーザに対する設定となる。この場合の URL は `http://(ルーターの IP アドレス)/custom/anonymous.user/` となる。

path には基点となるディレクトリを絶対パス、もしくは相対パスで指定する。相対パスで指定した場合、環境変数 PWD を基点としたパスと解釈される。PWD は `set` コマンドで変更可能であり、初期値は "/" である。

name にはブラウザから '/' 止めの URL でアクセスした場合に表示するファイル名を指定する。

[ノート]

本コマンドを設定する場合、無名ユーザ以外は事前に `login user` コマンドでユーザを登録しておく必要がある。登録されていないユーザに対して本コマンドを設定するとエラーになる。

RTX1200 の外部メモリにおいて自動検索機能は使用できない。また、*name* にスラッシュ '/' を含む文字列を指定することはできない。

本コマンドが設定されているユーザは、ルーターに内蔵されている通常の GUI にアクセスすることができない。

SRT100 は Rev.10.00.52 以降で使用可能。 RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

52.3 カスタム GUI の API を使用するか否かの設定

[書式]

```
httpd custom-gui api use use
no httpd custom-gui api use [use]
```

[設定値及び初期値]

- *use*
- [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: off

[説明]

API 用の URL "http://(ルーターの IP アドレス)/custom/api" に対する POST リクエストを受け付けるか否かを設定する。

[ノート]

API 用の URL を使用するには、本コマンドに加えて `httpd custom-gui use on` が設定されている必要がある。

本コマンドを on にしても `httpd custom-gui api password` コマンドを設定しなければ API 用の URL を使用することはできない。

SRT100 は Rev.10.00.52 以降で使用可能。 RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

52.4 カスタム GUI の API にアクセスするためのパスワードの設定

[書式]

```
httpd custom-gui api password password
no httpd custom-gui api password [password]
```

[設定値及び初期値]

- *password*
- [設定値]: パスワード
- [初期値]: -

[説明]

API 用の URL へ POST リクエストを送信する際のパスワードを設定する。32 文字以内で半角英数字を使用することができる。

例えば、本コマンドでパスワードとして `doremi` を設定した場合、URL は `http://(ルーターの IP アドレス)/custom/api?password=doremi` となる。

[ノート]

SRT100 は Rev.10.00.52 以降で使用可能。 RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

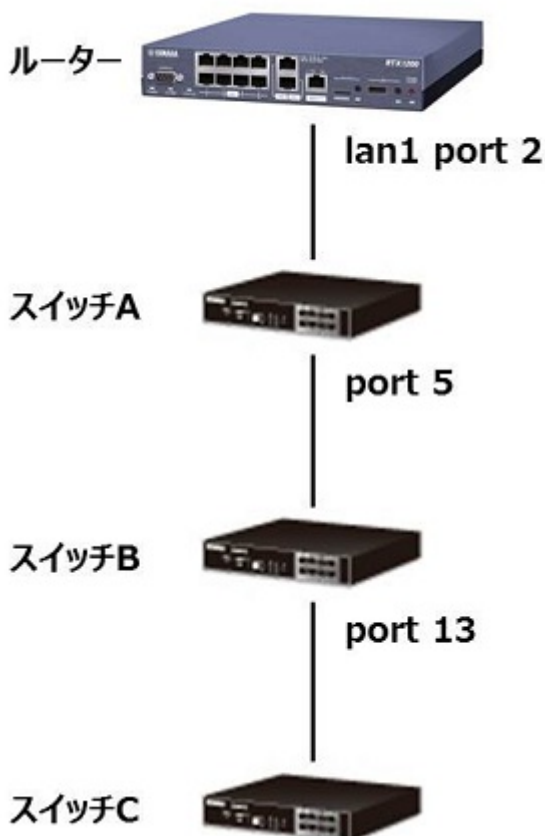
第 53 章

L2MS

L2MS とは、ヤマハネットワーク機器 (スイッチ、無線 LAN アクセスポイント、ルーター) をルーターから制御するための機能です。L2MS では制御を行う機器をマネージャー、マネージャーから制御される機器をエージェントと呼びます。エージェントの制御を行うためには、共通の設定の他に、それぞれの機器に対応する制御コマンドを参照してください。

当機能の各コマンドでスイッチまたはアクセスポイントを指定する場合、MAC アドレスによる指定と経路による指定の 2 つの方法があります。

経路による指定方法では、ルーターを基点として途中にある各スイッチのポート番号を順に記述します。



上図のような構成でスイッチ C を指定する場合の表記は "lan1:2-5-13" となります。

- 最初にルーターの LAN インターフェースを指定します。
- LAN インターフェースがスイッチングハブである場合、ポート番号を指定します。LAN インターフェース名とポート番号の間はコロン ":" で区切ります。
- LAN インターフェースがスイッチングハブでない場合、ポート番号の指定は不要です。
- ルーターとスイッチ C の間にある各スイッチのポート番号をルーターに近い方から順に指定します。各ポート番号はハイフン "-" で区切ります。

L2MS によって制御できる機器の種類や対応ファームウェアリビジョンの詳細については、以下に示す、L2MS の技術資料をご覧ください。

<http://www.rtpro.yamaha.co.jp/RT/docs/swctl/>

53.1 共通の設定

53.1.1 L2MS の動作モードの設定

[書式]

```
switch control mode mode
no switch control mode [mode]
```

[設定値及び初期値]

- mode

- [設定値]:

設定値	説明
manager	L2MS のマネージャーとして動作する
agent	L2MS のエージェントとして動作する
off	L2MS を使用しない

- [初期値]: master

[説明]

L2MS の動作モードを設定する。*mode* が **manager** である場合は L2MS のマネージャーとして動作する。*mode* が **agent** である場合は L2MS のエージェントとして動作する。

[ノート]

RTX1210 は Rev.14.01.20 以降で使用可能。

manager オプションと **agent** オプションは RTX1210 Rev.14.01.41 以降、RTX830 Rev.15.02.24 以降、RTX1220 Rev.15.04.04 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830

53.1.2 L2MS を使用するか否かの設定

[書式]

switch control use interface use [terminal=terminal]

no switch control use interface use [use [terminal=terminal]]

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インターフェース名、ブリッジインターフェース名
 - [初期値]: -
- *use*
 - [設定値]:

設定値	説明
on	L2MS を使用する
off	L2MS を使用しない

- [初期値]: off
- *terminal*
 - [設定値]:

設定値	説明
on	端末情報の取得を行う
off	端末情報の取得を行わない

- [初期値]: off

[説明]

L2MS を使用するか否かをインターフェースごとに設定する。*use* が **on** であるインターフェースで L2MS を使用する。L2MS は **switch control use** コマンドの設定にしたがって動作する。L2MS のマネージャーとして動作している場合は、L2MS に対応したエージェントを制御するための通信を行う。また、*terminal* オプションが **on** に設定されたインターフェースでは端末情報の取得も行う。L2MS を使用しないインターフェースでは *use* を **off** に設定することで不要なパケットの送出手を抑制することができる。L2MS のエージェントとして動作している場合は、マネージャーからの探索パケットに対して応答パケットを返す。

[ノート]

switch control mode コマンドで *mode* に **off** が設定されている場合、本コマンドの設定は反映されない。

LAN 分割機能が有効になっているインターフェースでは本コマンドを設定することができない。

ポート分離機能が有効になっているインターフェースで本コマンドを設定できるのは、RTX1200 Rev.10.01.42 以降、RTX810 Rev.11.01.06 以降のファームウェア、および、Rev.14.01 系以降のファームウェアである。

bridge member コマンドで LAN インターフェースが収容されていない場合、本コマンドのブリッジインターフェースへの設定は反映されない。また、ブリッジインターフェースとブリッジインターフェースに収容されている LAN インターフェースで *use* に **on** を設定している場合、ブリッジインターフェースへの設定のみ反映される。ブリッジインターフェースで本コマンドを設定できるのは、RTX1210 Rev.14.01.20 以降のファームウェア、および、Rev.15.02 系以降のすべてのファームウェアである。

use が **off** に設定されたインターフェースでは *terminal* オプションが **on** であっても端末情報の取得は行わない。また、L2MS のエージェントとして動作している場合、*terminal* オプションの設定は L2MS の動作に反映されない。*terminal* オプションは Rev.14.01 系以降のファームウェアで使用できる。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.1.3 エージェントの監視時間間隔の設定

[書式]

switch control watch interval time [*count*]

no switch control watch interval

[設定値及び初期値]

- *time*
 - [設定値]: 秒数 (2 .. 10)
 - [初期値]: 3
- *count*
 - [設定値]: 回数 (2 .. 10)
 - [初期値]: 3

[説明]

エージェントを探索するパケットの送信時間間隔、およびエージェントからの応答パケットを受信せずダウンしたと判断するまでの探索パケット送信回数を設定する。

time を大きな値に設定した場合、探索パケットの送信頻度は減るが、エージェントを接続してからマネージャーが認識するまでの時間が長くなる。*time* を小さな値に設定した場合はその逆となり、探索パケットの送信頻度は増えるが、エージェントを接続してからマネージャーが認識するまでの時間が短くなる。

探索パケットを *count* で設定した回数送信してもエージェントから応答パケットを受信しない場合、当該のエージェントはダウンしたと判断する。

[ノート]

switch control mode コマンドで *mode* に **manager** が設定されていない場合、本コマンドの設定は L2MS の動作に反映されない。

エージェントを接続しているイーサネットケーブルを抜いた場合は、当コマンドの設定よりも早いタイミングでエージェントがダウンしたと判断することがある。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.1.4 端末情報の監視時間間隔の設定

[書式]

lan-map terminal watch interval time1 [*time2*]

no lan-map terminal watch interval [*time1* [*time2*]]

[設定値及び初期値]

- *time1*
 - [設定値]: マネージャー/エージェント配下の端末情報を取得する間隔 (秒) (1800 .. 86400)
 - [初期値]: 1800
- *time2*
 - [設定値]: 端末の接続/切断を即時通知できないエージェント配下の端末情報を取得する間隔 (秒) (10 .. 86400)
 - [初期値]: 60

[説明]

LAN マップで管理しているネットワークの端末情報の定期取得を行う間隔を設定する。

マネージャーは、各エージェントからの端末の接続/切断の即時通知を契機に取得する端末情報と、指定の間隔で各エージェントに対して行う定期取得処理を契機に取得する端末情報を基に LAN マップの端末情報を更新している。ただし、端末の接続/切断を即時通知できるエージェントと、端末の接続/切断を即時通知できないエージェントがあり、それぞれで定期取得処理の実行間隔と目的が以下のように異なる。

- 定期取得 1

マネージャー、および端末の接続/切断を即時通知できるエージェントを対象機器として、*time1* に設定した時間が経過する度に端末情報を取得する。定期取得 1 は端末情報の補正を目的としている。端末の接続/切断を即時通知できるエージェント配下の端末の接続/切断は、*time1* の経過を待たずに LAN マップに即時に反映される。しかし、端末からの通信がなく、エージェントの MAC アドレステーブルに端末が登録されていなかった場合やパケットロスにより端末情報を受信できなかった場合、端末の接続は LAN マップに即時に反映されない。このような場合は、*time1* が経過する度に行う定期取得により、端末情報が取得できたときに LAN マップに反映される。

- 定期取得 2

端末の接続/切断を即時通知できないエージェントを対象機器として、*time2* に設定した時間が経過する度に端末情報を取得する。端末の接続/切断を即時通知できないエージェント配下の端末の接続/切断は、LAN マップに即時に反映されず、*time2* の間隔で反映される。

[ノート]

端末の接続/切断を即時通知できないエージェントは以下の無線 AP である。

- WLX202
- WLX302
- WLX313
- WLX402 (Rev.17.00.09 より前のファームウェア)

他のエージェントは端末の接続/切断の即時通知が可能である。

switch control mode コマンドで *mode* に *manager* が設定されていない場合、本コマンドの設定は L2MS の動作に反映されない。

switch control use コマンドで *terminal* オプションに *on* が設定されていない場合、本コマンドの設定に関わらず、端末情報の補正、および更新は行わない。

RTX1210 は Rev.14.01.09 以降で *time2* オプションを使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830

53.1.5 スナップショット機能を使用するか否かの設定

[書式]

```
lan-map snapshot use interface use [terminal=terminal]
no lan-map snapshot use interface [use [terminal=terminal]]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インターフェース名、ブリッジインターフェース名
 - [初期値]: -
- *use*
 - [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: off
- *terminal*
 - [設定値]:

設定値	説明
on	端末情報を含める
off	端末情報を含めない
wired-only	有線接続された端末情報のみ含める

- [初期値]: off

[説明]

LAN マップのスナップショット機能を使用するか否かをインターフェースごとに設定する。 *terminal* オプションが on に設定されたインターフェースでは、端末情報がスナップショット機能の対象に含まれるようになる。 *terminal* オプションが *wired-only* に設定されたインターフェースでは、有線接続された端末情報のみがスナップショット機能の対象に含まれるようになる。無線接続された端末情報はスナップショット機能の対象には含まれない。

[ノート]

switch control mode コマンドで *mode* に *manager* が設定されていない場合、本コマンドの設定は L2MS の動作に反映されない。

switch control use コマンドで *terminal* オプションが on に設定されていない場合、本コマンドの設定に関わらず、端末情報はスナップショット機能の対象に含まれない。

ブリッジインターフェースは RTX1210 Rev.14.01.20 以降のファームウェア、および、Rev.15.02 系以降のすべてのファームウェアで指定可能。

wired-only は RTX1210 Rev.14.01.09 以降のファームウェア、および、Rev.15.02 系以降のすべてのファームウェアで指定可能。

[適用モデル]

RTX1220, RTX1210, RTX830

53.1.6 スナップショットファイルを作成する

[書式]

take lan-map snapshot interface [update]

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インターフェース名、ブリッジインターフェース名
 - [初期値]: -
- *update*: ネットワークの接続状態を更新した後、スナップショットファイルを作成する
 - [初期値]: -

[説明]

LAN マップのスナップショット機能でベースとなるスナップショットファイルを作成する。 *update* オプションが含まれない場合、現在マネージャーが保持しているネットワークの状態をスナップショットファイルとして保存する。 *update* オプションが含まれる場合、ネットワークの接続状態の情報を最新に更新した後、スナップショットファイルとして保存する。

[ノート]

switch control mode コマンドで *mode* に *manager* が設定されている場合、本コマンドを使用できる。

スナップショットファイルの作成を開始すると、以下の SYSLOG が出力される。

```
[LANMAP] SnapShot(LAN1): Take snapshot files: Start.
```

スナップショットファイルの作成が完了すると、以下の SYSLOG が出力される。

```
[LANMAP] SnapShot(LAN1): Take snapshot files: Complete.
```

update オプションが含まれる場合、ネットワークの接続状態の情報を最新に更新するが、ネットワークの構成によっては更新が完了するまでに時間がかかる場合がある。

ブリッジインターフェースは RTX1210 Rev.14.01.20 以降のファームウェア、および、Rev.15.02 系以降のすべてのファームウェアで指定可能。

[適用モデル]

RTX1220, RTX1210, RTX830

53.1.7 LAN マップの SYSLOG 出力の設定

[書式]

```
lan-map log sw
no lan-map log [sw]
```

[設定値及び初期値]

- *sw*
- [設定値]:

設定値	説明
on	出力する
off	出力しない

- [初期値]: off

[説明]

LAN マップに関する SYSLOG 出力の設定をする。

[適用モデル]

RTX1220, RTX1210, RTX830

53.1.8 LAN マップで使用する機器名の設定

[書式]

```
lan-map sysname name
no lan-map sysname [name]
```

[設定値及び初期値]

- *name*
- [設定値]: 機器名 (半角 1 文字以上、32 文字以下)
- [初期値]: (製品名称)_(シリアル番号)

[説明]

LAN マップで表示する機器名を設定をする。*name* に使用できる文字は、半角英数字、ハイフン (-)、アンダーバー (_)、および半角スペース ()。半角スペースを含ませるためには、*name* 全体をダブルクォーテーション (")、またはシングルクォーテーション (') で囲む。

[ノート]

RTX1210 は Rev.14.01.20 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830

53.2 スイッチの制御

53.2.1 スイッチの選択

[書式]

```
switch select switch
no switch select
```

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
スイッチ	MAC アドレスもしくは経路
none	スイッチを選択しない

- [初期値]: -

[説明]

対象とするスイッチを選択する。以降プロンプトには `console prompt` で設定した文字列と選択したスイッチが続けて表示される。

`switch select none` または `no switch select` を実行すると、プロンプトにスイッチを表示しなくなる。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.2.2 スイッチが持つ機能の設定

[書式]

`switch control function set function [index ...] value`

`no switch control function set function [index ...]`

[設定値及び初期値]

- *function*
 - [設定値]: 機能の名前
 - [初期値]: -
- *index*
 - [設定値]: インデックス
 - [初期値]: -
- *value*
 - [設定値]: 設定値
 - [初期値]: -

[説明]

スイッチが持つ機能について設定を行う。設定したい機能の名前とその機能に対する設定値をパラメータとして指定する。複数の設定対象が存在する機能ではインデックスを指定する。

コマンド実行中に Ctrl-C 押下で中断することができる。ただし、実行後に同期処理が開始された場合は中断できない。

[ノート]

本コマンドを実行する前に `switch select` でスイッチを指定しておく必要がある。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.2.3 スイッチが持つ機能の設定内容や動作状態の取得

[書式]

`switch control function get function [index ...] [switch]`

[設定値及び初期値]

- *function*
 - [設定値]: 機能の名前
 - [初期値]: -
- *index*
 - [設定値]: インデックス
 - [初期値]: -
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

スイッチが持つ機能の設定内容や動作状態を取得する。取得したい機能の名前をパラメータとして指定する。複数の取得対象が存在する機能ではインデックスを指定する。

コマンド実行中に Ctrl-C 押下で中断することができる。

[ノート]

switch を指定しない場合は、本コマンドを実行する前に **switch select** でスイッチを指定しておく必要がある。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.2.4 スイッチに対して特定の動作を実行

[書式]

```
switch control function execute function [index ...] [switch]
```

[設定値及び初期値]

- *function*
 - [設定値]: 機能の名前
 - [初期値]: -
- *index*
 - [設定値]: インデックス
 - [初期値]: -
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

スイッチに対して特定の動作を実行させる。実行したい動作に対応する機能の名前をパラメータとして指定する。複数の実行対象が存在する機能ではインデックスを指定する。

コマンド実行中に Ctrl-C 押下で中断することができる。

[ノート]

switch を指定しない場合は、本コマンドを実行する前に **switch select** でスイッチを指定しておく必要がある。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.2.5 スイッチの設定の削除

[書式]

```
switch control function default [both] [switch]
```

[設定値及び初期値]

- *both*: 対象のスイッチに対して適用可能な設定をすべて削除する
 - [初期値]: -
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

選択したスイッチに対するルーター上の設定を削除する。同時に、ルーターがスイッチを制御している場合は同期処理を行う。

both オプションを指定しない場合、スイッチに対して適用可能な他の設定が存在すれば、その設定でスイッチを同期する。例えば、MAC アドレス指定と経路指定の設定が存在する状態で、MAC アドレス指定の設定を選択して本コマンドを実行した場合、MAC アドレス指定の設定が削除された後、スイッチは経路指定の設定で同期される。

both オプションを指定する場合、スイッチに対して適用可能な他の設定が存在すれば、その設定も同時に削除する。上記の例では、MAC アドレス指定と経路指定の両方の設定が削除される。

すなわち、スイッチを確実に初期化したい場合は *both* オプションを指定する。

[ノート]

switch を指定しない場合は、本コマンドを実行する前に **switch select** でスイッチを指定しておく必要がある。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.2.6 スイッチのファームウェアの更新

[書式]

```
switch control firmware upload go file [switch]
```

[設定値及び初期値]

- *file*
 - [設定値]: ファームウェアのファイルへの相対パスまたは絶対パス
 - [初期値]: -
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

スイッチのファームウェアを更新する。ファームウェアのファイルはフラッシュ ROM や外部メモリへ事前に保存しておき、*file* にパスを指定する。ファームウェアの書き換えに成功すると、スイッチは自動的に再起動する。

コマンド実行中に Ctrl-C 押下で中断することができる。

file に相対パスを指定した場合、環境変数 PWD を基点としたパスと解釈される。PWD は **set** コマンドで変更可能であり、初期値は "/" である。

[ノート]

switch を指定しない場合は、本コマンドを実行する前に **switch select** でスイッチを指定しておく必要がある。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.2.7 LAN ケーブル二重化機能の設定

[書式]

```
switch control route backup route port
```

```
no switch control route backup route
```

[設定値及び初期値]

- *route*
 - [設定値]: メイン経路
 - [初期値]: -
- *port*
 - [設定値]: バックアップ経路として使用するポート番号
 - [初期値]: -

[説明]

LAN ケーブル二重化機能を動作させるメイン経路とバックアップ経路を設定する。

route で指定した経路をメイン経路、*port* に接続される先の経路をバックアップ経路として、LAN ケーブル二重化機能が動作する。

[ノート]

以下のポートを *port* に設定することはできない

- *route* でメイン経路として指定したポート
- 既に LAN ケーブル二重化機能が設定されているポート

ルーターのスイッチングハブに対して本コマンドを設定した場合、設定した LAN インタフェースで **switch control use** コマンドが on に設定されているときのみ、LAN ケーブル二重化機能が動作する。

スイッチに対して本コマンドを設定した場合、当該ポートが一時的にリンクダウンする。

LAN ケーブル二重化機能の動作状態は **show status switch control route backup** コマンドで確認できる。
スイッチに本機能が実装されていない場合はコマンドエラーとなる。

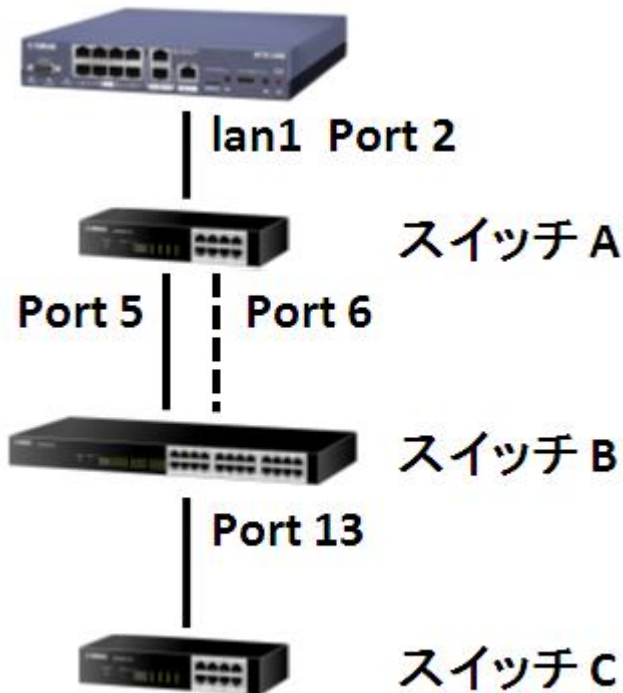
RTX1200 は Rev.10.01.45 以降で使用可能。

RTX810 は Rev.11.01.12 以降で使用可能。

[設定例]

下図のようにスイッチ A のポート 5 をメイン経路、ポート 6 をバックアップ経路とする場合の設定

```
switch control route backup lan1:2-5 6
```



[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.2.8 スイッチの設定ファイルを格納するディレクトリの指定

[書式]

```
switch config directory path
```

```
no switch config directory [path]
```

[設定値及び初期値]

- *path*
 - [設定値]: 相対パスまたは絶対パス (半角 256 文字以下、全角 128 文字以下)
 - [初期値]: /sw_config

[説明]

スイッチの設定ファイル(config)を格納するディレクトリを指定する。

相対パスを指定した場合、環境変数 PWD を起点としたパスと解釈される。

PWD は **set** コマンドで変更可能であり、初期値は "/" である。

path が RTFS 領域となる場合には、*path* にマルチバイト文字を使用することはできない。

[ノート]

RTX1210 は Rev.14.01.28 以降で使用可能。

RTX830 は Rev.15.02.03 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830

53.2.9 スイッチの設定を保存するファイル名の指定

[書式]

```
switch config filename name
no switch config filename [name]
```

[設定値及び初期値]

- *name*
 - [設定値]: config ファイル名 (半角 99 文字以下、全角 49 文字以下)
 - [初期値]: -

[説明]

スイッチの設定を保存するファイル名を指定する。

このコマンドが省略された場合は、**switch select** で指定された文字列に .conf を付けたものをファイル名とする。

ただし:(コロン)は_(アンダースコア)に置き換えられる。

複数の **switch select** コマンドで同じファイル名を指定することができる。

switch config directory コマンドで指定したディレクトリが RTFS 領域である場合は、ファイル名にマルチバイト文字を使用することはできない。

本コマンドを実行する前に **switch select** コマンドでスイッチを指定しておく必要がある。

[ノート]

RTX1210 は Rev.14.01.28 以降で使用可能。

RTX830 は Rev.15.02.03 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830

53.2.10 スイッチの設定の取得

[書式]

```
switch control config get [switch]
switch control config get [[interface] all]
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
MAC アドレスもしくは経路	選択したスイッチのみ
all	全てのスイッチ

- [初期値]: -
- *interface*
 - [設定値]: LAN インターフェース名、ブリッジインターフェース名
 - [初期値]: -

[説明]

スイッチの設定ファイルを取得して保存する。

switch パラメータに MAC アドレスもしくは経路を指定した場合は、指定したスイッチの設定ファイルを取得する。

all を指定すると、マネージャーが認識している全てのスイッチの設定ファイルを取得する。

interface パラメータを指定すると、指定のインターフェースにつながっているスイッチを対象とする。

interface パラメータを省略した場合は、all を指定した時と同様になる。

[ノート]

スイッチの設定ファイルの名前には、**switch config filename** コマンドで指定したファイル名を使用する。

スイッチの設定ファイルは **switch config directory** コマンドで指定したディレクトリに保存される。

schedule at コマンドで指定することができる。

RTX1210 は Rev.14.01.28 以降で使用可能。
 RTX830 は Rev.15.02.03 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830

53.2.11 スイッチの設定の復元

[書式]

switch control config set [*switch*]

switch control config set [[*interface*] all]

[設定値及び初期値]

- *switch*

- [設定値]:

設定値	説明
MAC アドレスもしくは経路	選択したスイッチのみ
all	全てのスイッチ

- [初期値]:-

- *interface*

- [設定値]: LAN インターフェース名、ブリッジインターフェース名
- [初期値]:-

[説明]

マネージャーに保存されているスイッチの設定ファイルを使用して、スイッチの設定を復元する。
switch パラメータに MAC アドレスもしくは経路を指定した場合は、指定したスイッチの設定を復元する。
 all を指定すると、マネージャーが認識している全てのスイッチの設定を復元する。
interface パラメータを指定すると、指定のインターフェースにつながっているスイッチを対象とする。
interface パラメータを省略した場合は、all を指定した時と同様になる。

[ノート]

復元に使用するスイッチの設定ファイルには、**switch config filename** コマンドで指定した設定ファイルを使用する。
 スイッチの設定ファイルは **switch config directory** コマンドで指定したディレクトリに保存されている必要がある。
schedule at コマンドで指定することができる。
 RTX1210 は Rev.14.01.28 以降で使用可能。
 RTX830 は Rev.15.02.03 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830

53.3 スイッチの機能

53.3.1 システム

53.3.1.1 BootROM バージョンの取得

[書式]

switch control function get boot-rom-version [*switch*]

[設定値及び初期値]

- *switch*: スイッチ

- [設定値]:
 - MAC アドレス
 - 経路
- [初期値]:-

[説明]

BootROM バージョンを取得する。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.1.2 ファームウェアリビジョンの取得**[書式]**

switch control function get firmware-revision [*switch*]

[設定値及び初期値]

- *switch* : スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

ファームウェアリビジョンを取得する。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.1.3 シリアル番号の取得**[書式]**

switch control function get serial-number [*switch*]

[設定値及び初期値]

- *switch* : スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

シリアル番号を取得する。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.1.4 製品名称の取得**[書式]**

switch control function get model-name [*switch*]

[設定値及び初期値]

- *switch* : スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

製品名称を取得する。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.1.5 MAC アドレスの取得**[書式]**

switch control function get system-macaddress [*switch*]

[設定値及び初期値]

- *switch* : スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

MAC アドレスを取得する。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.1.6 機器の名前の設定**[書式]**

```
switch control function set system-name name
no switch control function set system-name
switch control function get system-name [switch]
```

[設定値及び初期値]

- *name*
 - [設定値]: 機器の名前 (1 文字以上、64 文字以下)
 - [初期値]: (製品名称)_(シリアル番号)
- *switch* : スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

機器の名前を設定する。*name* 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 (_)

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.1.7 省電力機能を使用するか否かの設定**[書式]**

```
switch control function set energy-saving mode
no switch control function set energy-saving
switch control function get energy-saving [switch]
```

[設定値及び初期値]

- *mode*
 - [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: off
- *switch* : スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

LAN ポートの省電力機能を使用するか否かを設定する。

[ノート]

本機能の設定を変更すると、全てのポートが一時的にリンクダウンする。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.1.8 LED の輝度の調整

[書式]

```
switch control function set led-brightness mode
no switch control function set led-brightness
switch control function get led-brightness [switch]
```

[設定値及び初期値]

- mode
- [設定値]:

設定値	説明
normal	明るい
economy	暗い

- [初期値]: normal
- switch: スイッチ
- [設定値]:
 - MAC アドレス
 - 経路
- [初期値]: -

[説明]

LED の輝度を調整する。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830

53.3.1.9 LED の表示モードの取得

[書式]

```
switch control function get status-led-mode [switch]
```

[設定値及び初期値]

- switch: スイッチ
- [設定値]:
 - MAC アドレス
 - 経路
- [初期値]: -

[説明]

LAN ポートごとの LED の現在の表示モードを取得する。

表示モード	説明
link/act	各ポートのリンク状態を表示する。 <ul style="list-style-type: none"> • 緑色で点灯: リンク確立状態 • 緑色で点滅: データ転送中 • 消灯: リンク喪失状態
speed	各ポートの接続速度を表示する。 <ul style="list-style-type: none"> • 緑色で点灯: 1000BASE-T で接続 • 橙色で点灯: 100BASE-TX で接続 • 消灯: 10BASE-T で接続

表示モード	説明
duplex	各ポートの接続状態 (全二重/半二重) を表示する。 <ul style="list-style-type: none"> 緑色で点灯: 全二重で接続 橙色で点灯: 半二重で接続
status	機器の状態を表示。 <ul style="list-style-type: none"> 橙色で点灯: ループを検出 SWX2200-24G でファンの故障を検知した場合は、モード LED 下側が橙色で点滅する。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.1.10 ファンの状態の取得**[書式]****switch control function get status-fan** [*switch*]**[設定値及び初期値]**

- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

ファンの状態を取得する。

状態	説明
normal	正常
lock	異常

[ノート]

SWX2200-24G、SWX2200-8PoE でのみ使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.1.11 ファンの回転数の取得**[書式]****switch control function get status-fan-rpm** *FAN* [*switch*]**[設定値及び初期値]**

- *FAN*
 - [設定値]: ファン番号
 - [初期値]: -
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

ファンの回転数を取得する。

[ノート]

SWX2200-8PoE でのみ使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.1.12 再起動

[書式]

switch control function execute restart [*switch*]

[設定値及び初期値]

- *switch* : スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

機器を再起動する。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.1.13 起動してからの時間の取得

[書式]

switch control function get system-uptime [*switch*]

[設定値及び初期値]

- *switch* : スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

起動してからの時間を取得する。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.2 ポート

53.3.2.1 リンクアグリゲーションのタイプの取得

[書式]

switch control function get lag-type [*switch*]

[設定値及び初期値]

- *switch* : スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

リンクアグリゲーションのタイプを取得する。

状態	説明
Not bundle	リンクアグリゲーションが設定されていない
Type-A	グループ#1: ポート 21, 22
Type-B	グループ#1: ポート 21, 22 グループ#2: ポート 23, 24
Type-C	グループ#1: ポート 21, 22, 23, 24

[ノート]

SWX2100-24G でのみ使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830, RTX810

53.3.2.2 ポートの通信速度および動作モードの設定**[書式]**

```
switch control function set port-speed port speed
no switch control function set port-speed port
switch control function get port-speed port [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]: -
- *speed*: 通信速度および動作モード
 - [設定値]:

設定値	説明
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

- [初期値]: auto
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

ポートの通信速度および動作モードを設定する。

[ノート]

本機能の設定を変更すると、当該ポートが一時的にリンクダウンする。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.2.3 ポートを使用するか否かの設定**[書式]**

```
switch control function set port-use port mode
no switch control function set port-use port
switch control function get port-use port [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]: -
- *mode*
 - [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: on
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

ポートを使用するか否かを設定する。本機能を off に設定すると、当該ポートに LAN ケーブルを接続してもリンクアップしなくなる。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.2.4 オートクロスオーバー機能を使用するか否かの設定**[書式]**

```
switch control function set port-auto-crossover port mode
no switch control function set port-auto-crossover port
switch control function get port-auto-crossover port [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]: -
- *mode*
 - [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: on
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

オートクロスオーバー機能を使用するか否かを設定する。

オートクロスオーバー機能とは、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である。本機能を on に設定すると、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なくなる。

[ノート]

本機能の設定を変更すると、当該ポートが一時的にリンクダウンする。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.2.5 速度ダウンシフト機能を使用するか否かの設定**[書式]**

```
switch control function set port-speed-downshift port mode
no switch control function set port-speed-downshift port
switch control function get port-speed-downshift port [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号

- [初期値]: -
- *mode*
- [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: on
- *switch*: スイッチ
- [設定値]:
 - MAC アドレス
 - 経路
- [初期値]: -

[説明]

速度ダウンシフト機能を使用するか否かを設定する。

速度ダウンシフト機能とは、例えば 1000BASE-T で使用できない LAN 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]

本機能の設定を変更すると、当該ポートが一時的にリンクダウンする。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.2.6 フロー制御を使用するか否かの設定

[書式]

```
switch control function set port-flow-control port mode
no switch control function set port-flow-control port
switch control function get port-flow-control port [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]: -
- *mode*
 - [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: off
- *switch*: スイッチ
- [設定値]:
 - MAC アドレス
 - 経路
- [初期値]: -

[説明]

フロー制御を使用するか否かを設定する。

本機能を on に設定すると、受信側と送信側の両方でフロー制御が有効になる。全二重でリンクアップしている場合は IEEE802.3x、半二重の場合はバックプレッシャ方式による制御がそれぞれ行われる。

[ノート]

本機能の設定を変更すると、当該ポートが一時的にリンクダウンする。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.2.7 L2MS パケットを遮断するか否かの設定**[書式]**

```
switch control function set port-blocking-control-packet port mode
no switch control function set port-blocking-control-packet port
switch control function get port-blocking-control-packet port [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]: -
- *mode*
 - [設定値]:

設定値	説明
on	制御パケットを遮断する
off	制御パケットを遮断しない

- [初期値]: off
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

L2MS パケットを遮断するか否かを設定する。本機能を on に設定すると、当該ポートでスイッチを制御するための通信が行われなくなる。

[ノート]

ヤマハスイッチに本機能が実装されていない場合はコマンドエラーとなる。

RTX1200 は Rev.10.01.45 以降で使用可能。

RTX810 は Rev.11.01.12 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.2.8 L2MS パケット以外のデータパケットを遮断するか否かの設定**[書式]**

```
switch control function set port-blocking-data-packet port mode
no switch control function set port-blocking-data-packet port
switch control function get port-blocking-data-packet port [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]: -
- *mode*
 - [設定値]:

設定値	説明
on	データパケットを遮断する
off	データパケットを遮断しない

- [初期値]: off

- *switch* : スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]:-

[説明]

L2MS パケット以外のデータパケットを遮断するか否かを設定する。本機能を on に設定すると、当該ポートでスイッチを制御するための通信以外のデータ通信が行われなくなる。

[ノート]

ヤマハスイッチに本機能が実装されていない場合はコマンドエラーとなる。

RTX1200 は Rev.10.01.45 以降で使用可能。

RTX810 は Rev.11.01.12 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.2.9 コンボポートの使用状況の取得**[書式]**

```
switch control function get status-combo-port port [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]:-
- *switch* : スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]:-

[説明]

ポートが SFP と Ethernet のどちらで使用されているかを取得する。

状態	説明
disable	ポートが使用されていない
sfp	SFP ポートとして使用されている
ethernet	イーサポートとして使用されている

[ノート]

SWX2100-24G でのみ使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830, RTX810

53.3.2.10 ポートの受光レベルの取得**[書式]**

```
switch control function get status-port-sfp-rx-power port [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]:-
- *switch* : スイッチ
 - [設定値]:
 - MAC アドレス

- 経路
- [初期値]:-

[説明]

SFP ポートの受光レベルを取得する。

状態	説明
normal	正常
low	受光レベルが下限閾値を下回っている
high	受光レベルが上限閾値を超えている

[ノート]

SWX2100-24G でのみ使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830, RTX810

53.3.2.11 ポートのリンク状態の取得

[書式]

switch control function get status-port-speed *port* [*switch*]

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]:-
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]:-

[説明]

ポートの現在のリンク状態を取得する。

状態	説明
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
down	リンクダウン

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.3 MAC アドレステーブル

ヤマハスイッチの MAC アドレステーブルの大きさは以下の通りです。

機種	最大エントリ数
SWX2200-24G	8192
SWX2200-8G、SWX2200-8PoE	

53.3.3.1 MAC アドレスエイジング機能を使用するか否かの設定

[書式]

switch control function set macaddress-aging *mode*

```
no switch control function set macaddress-aging
switch control function get macaddress-aging [switch]
```

[設定値及び初期値]

- *mode*
 - [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: on
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

MAC アドレスエージング機能を使用するか否かを設定する。

MAC アドレスエージング機能とは、スイッチが持つ 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である。本機能を off に設定すると、一度スイッチが学習した MAC アドレスは自動的に消去されない。

消去する時間間隔は **macaddress-aging-timer** で設定する。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.3.2 MAC アドレスエージングの時間間隔の設定

[書式]

```
switch control function set macaddress-aging-timer time
no switch control function set macaddress-aging-timer
switch control function get macaddress-aging-timer [switch]
```

[設定値及び初期値]

- *time*
 - [設定値]: 秒数 (10 .. 64800)
 - [初期値]: 300

[説明]

MAC アドレスエージング機能において、スイッチが学習した MAC アドレスを消去する時間間隔を設定する。

スイッチが MAC アドレスを学習してからエントリを消去するまでの時間は、最短で本機能で設定した秒数、最長でその 2 倍の秒数となる。例えば設定値が 300 秒だった場合、最短 300 秒、最長 600 秒となる。

なお、一度学習した MAC アドレスからのフレームを再度受信した場合、当該エントリが消去されるまでの時間はリセットされる。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.3.3 MAC アドレスをキーにした MAC アドレステーブルの検索

[書式]

```
switch control function get status-macaddress-addr mac_address [switch]
```

[設定値及び初期値]

- *mac_address*
 - [設定値]: MAC アドレス
 - [初期値]: -
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス

- 経路
- [初期値]:-

[説明]

MAC アドレスをキーにして MAC アドレステーブルを検索し、当該 MAC アドレスを学習したポート番号を取得する。同一の MAC アドレスを異なる VLAN で学習している場合は、ポート番号が複数表示されることがある。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.3.4 ポート番号をキーにした MAC アドレステーブルの検索**[書式]**

```
switch control function get status-macaddress-port port [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]:-
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]:-

[説明]

ポート番号をキーにして MAC アドレステーブルを検索し、当該ポートで学習した MAC アドレスを取得する。同一の MAC アドレスを異なる VLAN で学習している場合は、複数のポートで同一の MAC アドレスが表示される場合がある。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.3.5 MAC アドレステーブルのエントリの消去**[書式]**

```
switch control function execute clear-macaddress-table [switch]
```

[設定値及び初期値]

- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]:-

[説明]

MAC アドレステーブルの全エントリを消去する。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.4 VLAN

ヤマハスイッチでポート VLAN/タグ VLAN の設定を行う場合、コマンドでは VLAN ID を直接入力せず、VLAN 登録番号を指定します。VLAN 登録番号と VLAN ID の紐付けは **vlan-id** で行います。例えば以下のような設定を行った場合、ポート 2 の VLAN ID は 4 になります。

```
switch control function set vlan-id 10 4
switch control function set vlan-access 2 10
```

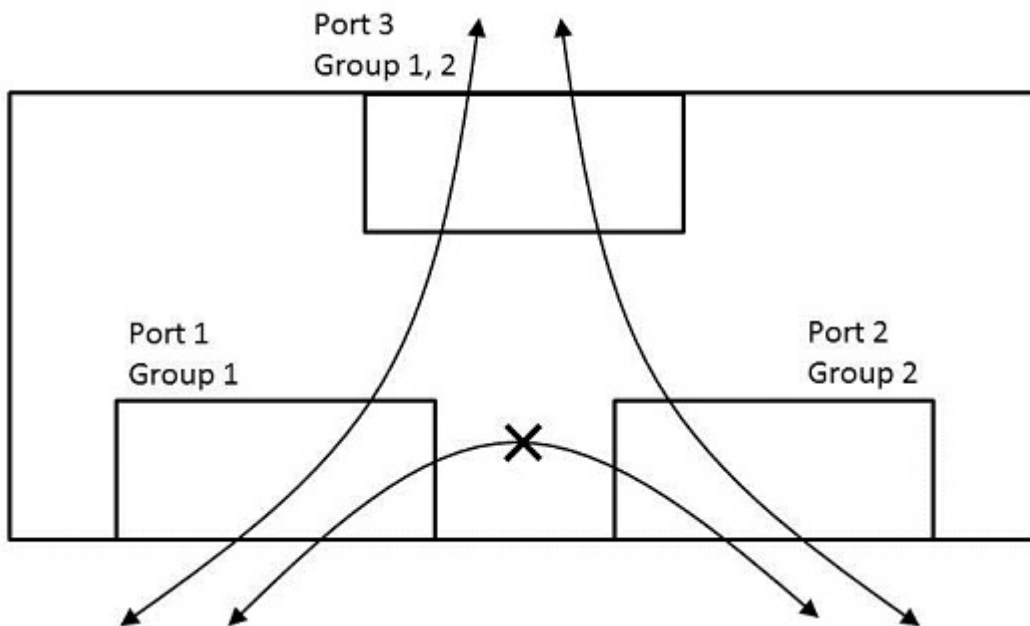
スイッチで受信したパケットは、VLAN タグの有無に関わらずいずれかの VLAN ID に分類され、その情報に基づいて転送処理が行われます。ポートの VLAN 動作モードは **vlan-port-mode** で設定します。

vlan-port-mode	受信時の動作	送信時の動作
access	VLAN タグ無しのパケットのみ受信します。VLAN ID の分類は vlan-access の設定に基づいて行われます。	受信時に、送信するポートの VLAN ID (vlan-access) に分類されたパケットを VLAN タグ無しで送信します。
trunk	VLAN タグ付きのパケットのみ受信します。ただし、VLAN タグ中の VLAN ID にポートが参加している必要があります。ポートが参加する VLAN ID は vlan-trunk で設定します。VLAN ID の分類は VLAN タグの情報に基づいて行われます。	受信時に、送信するポートが参加する VLAN ID (vlan-trunk) に分類されたパケットを VLAN タグ付きで送信します。
hybrid	VLAN タグ付き、VLAN タグ無し、両方のパケットを受信します。VLAN タグ無しのパケットを受信した場合は、アクセスポートと同様の動作をします。VLAN タグ付きのパケットを受信した場合は、トランクポートと同様の動作をします。	受信時に、送信するポートの VLAN ID (vlan-access) に分類されたパケットを VLAN タグ無しで送信します。また、受信時に、送信するポートが参加する VLAN ID (vlan-trunk) に分類されたパケットを VLAN タグ付きで送信します。どちらにも該当する場合は、VLAN タグ無しで送信します。

マルチプル VLAN は、1つのスイッチにおいてポートをグループに分けて、グループ間の通信を禁止する機能です。

vlan-multiple-use で機能を有効にした後、**vlan-multiple** でポートが所属するグループ番号を指定します。1つのポートを複数のグループに所属させることができます。あるポートで受信したパケットは、当該ポートと同じグループ番号に所属する他のポートから送信されます。

例として、以下のような設定を行った場合を考えます。



```
switch control function set vlan-multiple-use on
switch control function set vlan-multiple 1 1 join
switch control function set vlan-multiple 2 2 join
switch control function set vlan-multiple 3 1 join
switch control function set vlan-multiple 3 2 join
```

- ポート 1 で受信したパケットはポート 3 からのみ送信されます。
- ポート 2 で受信したパケットはポート 3 からのみ送信されます。
- ポート 3 で受信したパケットはポート 1 とポート 2 から送信されます。

マルチプル VLAN はネットワークを分割するものではないので、異なるグループ間でも同一のネットワークアドレスが割り振られます。

ポート VLAN/タグ VLAN とマルチプル VLAN を併用する場合、マルチプル VLAN において同一のグループに所属するポート間であっても、ポート VLAN/タグ VLAN において同一の VLAN に所属していない場合は通信することができません。

53.3.4.1 VLAN ID の設定

[書式]

```
switch control function set vlan-id vlan_register_num vid
no switch control function set vlan-id vlan_register_num
switch control function get vlan-id vlan_register_num [switch]
```

[設定値及び初期値]

- *vlan_register_num*
 - [設定値]: VLAN 登録番号 (1 .. 256)
 - [初期値]: -
- *vid*
 - [設定値]: VLAN ID (1 .. 4094)
 - [初期値]: VLAN 登録番号と同じ値
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

VLAN 登録番号に対して VLAN ID を設定する。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.4.2 ポートの VLAN 動作モードの設定

[書式]

```
switch control function set vlan-port-mode port mode
no switch control function set vlan-port-mode port
switch control function get vlan-port-mode port [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]: -
- *mode*: VLAN 動作モード
 - [設定値]:

設定値	説明
access	アクセスポート
trunk	トランクポート
hybrid	ハイブリッドポート

- [初期値]: access
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

ポートの VLAN 動作モードを設定する。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.4.3 アクセスポートの設定

[書式]

```
switch control function set vlan-access port vlan_register_num
no switch control function set vlan-access port
switch control function get vlan-access port [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]: -
- *vlan_register_num*
 - [設定値]: VLAN 登録番号 (1 .. 256)
 - [初期値]: 1
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

vlan-port-mode が **access** または **hybrid** であるポートについて、ポートの VLAN ID を設定する。VLAN ID は VLAN 登録番号を用いて指定する。

[ノート]

vlan-port-mode が **trunk** であるポートにおいて、本機能の設定を変更しても動作に影響はない。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.4.4 トランクポートの設定

[書式]

```
switch control function set vlan-trunk port vlan_register_num mode
no switch control function set vlan-trunk port vlan_register_num
switch control function get vlan-trunk port vlan_register_num [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]: -
- *vlan_register_num*
 - [設定値]: VLAN 登録番号 (1 .. 256)
 - [初期値]: -
- *mode*
 - [設定値]:

設定値	説明
join	参加する
leave	参加しない

- [初期値]: leave
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

vlan-port-mode が trunk もしくは hybrid であるポートにおいて、参加する VLAN ID を設定する。VLAN ID は VLAN 登録番号を用いて指定する。

[ノート]

vlan-port-mode が access であるポートにおいて、本機能の設定を変更しても動作に影響はない。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.4.5 マルチプル VLAN を使用するか否かの設定

[書式]

```
switch control function set vlan-multiple-use mode
no switch control function set vlan-multiple-use
switch control function get vlan-multiple-use [switch]
```

[設定値及び初期値]

- *mode*
 - [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: off
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

マルチプル VLAN を使用するか否かを設定する。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.4.6 マルチプル VLAN のグループ設定

[書式]

```
switch control function set vlan-multiple port group_num mode
no switch control function set vlan-multiple port group_num
switch control function get vlan-multiple port group_num [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]: -
- *group_num*: グループ番号
 - [設定値]:

機種	範囲
SWX2200-24G	1 .. 24
SWX2200-8G、SWX2200-8PoE	1 .. 8

- [初期値]: -
- *mode*
 - [設定値]:

設定値	説明
join	参加する
leave	参加しない

- [初期値]: leave
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

ポートが所属するマルチプル VLAN のグループ番号を設定する。

[ノート]

vlan-multiple-use が off の場合、本機能の設定を変更しても動作に影響はない。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.5 QoS

DSCP リマーキングは、IP ヘッダの DS フィールド中の 6 ビットの DSCP 値を書き換える機能です。書き換える値は、パケットを受信したポートのクラス (**qos-dscp-remark-class**) と送信するポートの書き換え方式 (**qos-dscp-remark-type**) により決定されます。具体的には以下ようになります。

qos-dscp-remark-type	qos-dscp-remark-class	DSCP 値	PHB
af	class1	001100	AF12
	class2	010100	AF22
	class3	011100	AF32
	class4	100100	AF42
cs	class1	000000	default
	class2	001000	Class Selector
	class3	010000	
	class4	011000	

53.3.5.1 DSCP リマーキングの書き換え方式の設定

[書式]

```
switch control function set qos-dscp-remark-type port type
no switch control function set qos-dscp-remark-type port
switch control function get qos-dscp-remark-type port [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]: -
- *type*: 書き換え方式
 - [設定値]:

設定値	説明
off	書き換えを行わない
af	AF (Assured Forwarding) で書き換えを行う
cs	CS (Class Selector) で書き換えを行う

- [初期値]: off

- *switch* : スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

スイッチから送信する IP パケットの DSCP 値を書き換える際の方式を設定する。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.5.2 受信パケットのクラス分けの設定

[書式]

```
switch control function set qos-dscp-remark-class port class
no switch control function set qos-dscp-remark-class port
switch control function get qos-dscp-remark-class port [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]: -
- *class*
 - [設定値]:

設定値	説明
off	分類しない
class1	クラス 1 に分類する
class2	クラス 2 に分類する
class3	クラス 3 に分類する
class4	クラス 4 に分類する

- [初期値]: off
- *switch* : スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

DSCP リマーキングにおいて、スイッチが受信したパケットのクラス分けを行う。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.5.3 帯域制限を行う際の速度単位の設定

[書式]

```
switch control function set qos-speed-unit unit
no switch control function set qos-speed-unit
switch control function get qos-speed-unit [switch]
```

[設定値及び初期値]

- *unit* : 速度単位
 - [設定値]:
 - 128k
 - 1m
 - 10m

- 32m
- [初期値]: 32m
- *switch*: スイッチ
- [設定値]:
 - MAC アドレス
 - 経路
- [初期値]: -

[説明]

受信トラフィックのポリシングおよび送信トラフィックのシェーピングを行う際の速度単位を設定する。

[ノート]

SWX2200-24G でのみ使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.5.4 受信トラフィックのポリシングを行うか否かの設定**[書式]**

```
switch control function set qos-policing-use port mode
no switch control function set qos-policing-use port
switch control function get qos-policing-use port [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]: -
- *mode*
 - [設定値]:

設定値	説明
on	行う
off	行わない

- [初期値]: off
- *switch*: スイッチ
- [設定値]:
 - MAC アドレス
 - 経路
- [初期値]: -

[説明]

受信トラフィックのポリシングを行うか否かを設定する。

[ノート]

SWX2200-24G でのみ使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.5.5 受信トラフィックの帯域幅の設定**[書式]**

```
switch control function set qos-policing-speed port level
no switch control function set qos-policing-speed port
switch control function get qos-policing-speed port [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]: -

- *level*
 - [設定値]: 帯域幅 (1 .. 31)
 - [初期値]: 1
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

受信トラフィックのポリシングを行う際の帯域幅を設定する。**qos-speed-unit** の設定値に *level* を掛けた値が実際の帯域幅となる。

[ノート]

SWX2200-24G でのみ使用可能。

qos-policing-use が off の場合、本機能の設定を変更しても動作に影響はない。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.5.6 送信トラフィックのシェーピングを行うか否かの設定

[書式]

```
switch control function set qos-shaping-use port mode
no switch control function set qos-shaping-use port
switch control function get qos-shaping-use port [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]: -
- *mode*
 - [設定値]:

設定値	説明
on	行う
off	行わない

- [初期値]: off
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

送信トラフィックのシェーピングを行うか否かを設定する。

[ノート]

SWX2200-24G でのみ使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.5.7 送信トラフィックの帯域幅の設定

[書式]

```
switch control function set qos-shaping-speed port level
no switch control function set qos-shaping-speed port
switch control function get qos-shaping-speed port [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]: -
- *level*
 - [設定値]: 帯域幅 (1 .. 31)
 - [初期値]: 1
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

送信トラフィックのシェーピングを行う際の帯域幅を設定する。**qos-speed-unit** の設定値に *level* を掛けた値が実際の帯域幅となる。

[ノート]

SWX2200-24G でのみ使用可能。

qos-shaping-use が off の場合、本機能の設定を変更しても動作に影響はない。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

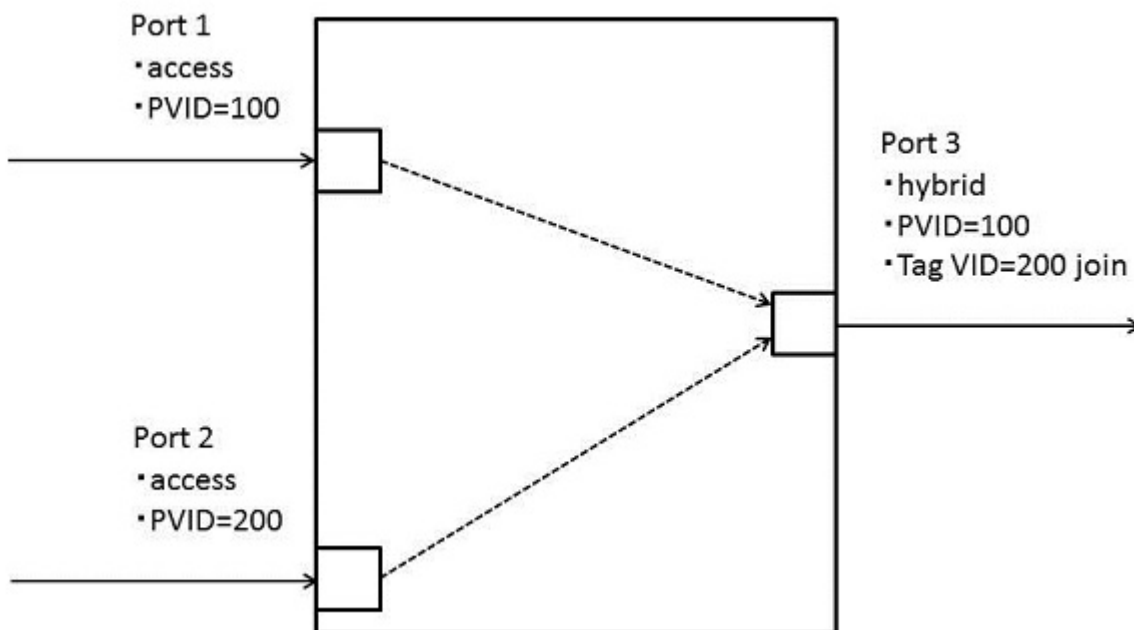
53.3.6 ミラーリング

ミラーリングは、特定ポートでの通信を他のポートで観測できる機能です。

ミラーリングとポートブロッキング機能(**port-blocking-control-packet** および **port-blocking-data-packet**)は併用できません。

ミラーリングとポート VLAN/タグ VLAN、マルチプル VLAN を併用する場合、ミラーリングを行うポート (**mirroring-src-rx** および **mirroring-src-tx**) とミラーリングパケットを送出するポート (**mirroring-dest**) が同一の VLAN、グループ番号に所属するようにしてください。

ミラーリングパケットと元のパケットで VLAN タグの有無に違いが生じることがあります。ミラーリングパケットに VLAN タグが付くか否かは、ミラーリングパケットを送出するポートの VLAN 動作モードに依存します。例えば以下の設定があるとします。



- ポート 1 はアクセスポートで VLAN ID=100
- ポート 2 はアクセスポートで VLAN ID=200
- ポート 3 はハイブリッドポートで、アクセスポートの VLAN ID=100、タグ VLAN で VLAN ID=200 に参加。
- ポート 1 とポート 2 で受信したパケットをポート 3 でミラーリングする。

```

switch control function set vlan-port-mode 3 hybrid
switch control function set vlan-access 1 100
switch control function set vlan-access 2 200
switch control function set vlan-access 3 100
switch control function set vlan-trunk 3 200 join
switch control function set mirroring-use on
switch control function set mirroring-dest 3
switch control function set mirroring-src-rx 1 on
switch control function set mirroring-src-rx 2 on

```

- ポート 1 で受信したパケットをポート 3 でミラーリングする場合、パケットに VLAN タグは付加されません。
- ポート 2 で受信したパケットをポート 3 でミラーリングする場合、パケットに VLAN ID=200 の VLAN タグが付加されます。

53.3.6.1 ミラーリング機能を使用するか否かの設定

[書式]

```

switch control function set mirroring-use mode
no switch control function set mirroring-use
switch control function get mirroring-use [switch]

```

[設定値及び初期値]

- *mode*
 - [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: off
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

ミラーリング機能を使用するか否かを設定する。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.6.2 ミラーリングパケットを送出するポートの設定

[書式]

```

switch control function set mirroring-dest port
no switch control function set mirroring-dest
switch control function get mirroring-dest [switch]

```

[設定値及び初期値]

- *port*
 - [設定値]: ミラーリングパケットを送出するポート番号
 - [初期値]:

機種	ポート番号
SWX2200-24G	24
SWX2200-8G、SWX2200-8PoE	8

- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路

- [初期値]:-

[説明]

ミラーリングパケットを送出するポートを設定する。

[ノート]

mirroring-use が off の場合、本機能の設定を変更しても動作に影響はない。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.6.3 受信したパケットをミラーリングするか否かの設定

[書式]

```
switch control function set mirroring-src-rx port mode
no switch control function set mirroring-src-rx port
switch control function get mirroring-src-rx port [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]:-
- *mode*
 - [設定値]:

設定値	説明
on	受信したパケットをミラーリングする
off	受信したパケットをミラーリングしない

- [初期値]: off
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]:-

[説明]

受信したパケットをミラーリングするか否かを設定する。

[ノート]

mirroring-dest に設定しているポートにおいて当機能を on にしても、ミラーリングは行われない。

mirroring-use が off の場合、本機能の設定を変更しても動作に影響はない。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.6.4 送信するパケットをミラーリングするか否かの設定

[書式]

```
switch control function set mirroring-src-tx port mode
no switch control function set mirroring-src-tx port
switch control function get mirroring-src-tx port [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]:-
- *mode*
 - [設定値]:

設定値	説明
on	送信するパケットをミラーリングする
off	送信するパケットをミラーリングしない

- [初期値]: off
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

送信するパケットをミラーリングするか否かを設定する。

[ノート]

mirroring-dest に設定しているポートにおいて当機能を on にしても、ミラーリングは行われぬ。

mirroring-use が off の場合、本機能の設定を変更しても動作に影響はない。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.7 カウンタ

ポートごとにフレームカウンタとオクテットカウンタがあり、それぞれ受信と送信で個別にカウントすることができます。フレームカウンタでは同時に複数の種類のパケットをカウントすることができます。

フレームカウンタを使用する場合、事前に **counter-frame-rx-type** または **counter-frame-tx-type** でカウントするパケットの種類を設定します。カウンタの値は **status-counter-frame-rx** または **status-counter-frame-tx** で取得します。

オクテットカウンタの値は **status-counter-octet-rx** または **status-counter-octet-tx** で取得します。

フレームカウンタでカウントするパケットの種類のうち class-0~class-3 は DSCP リマーカーキングによるクラス分け (**qos-dscp-remark-class**) に対応しています。対応関係は以下の通りです。

DSCP によるクラス分け	送信キューまたは受信キューのクラス
class1	class-0
class2	class-1
class3	class-2
class4	class-3
クラス分け無し (off)	

スイッチで受信したパケットを送信するとき、受信キューと送信キューのクラスは常に同一となります。

53.3.7.1 受信フレームカウンタでカウントするフレームの種類の設定

[書式]

```
switch control function set counter-frame-rx-type port counter type
no switch control function set counter-frame-rx-type port counter
switch control function get counter-frame-rx-type port counter [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]: -
- *counter*: カウンタ番号
 - [設定値]:

機種	範囲
SWX2200-24G	1 .. 5
SWX2200-8G、SWX2200-8PoE	1 .. 3

- [初期値]: -
- *type*: カウントするパケットの種類
- [設定値]:

設定値	説明
packets	全てのパケット
broadcast-and-multicast-packets	ブロードキャストパケットとマルチキャストパケット
total-error-packets	CRC エラー、アライメントエラー、フレームサイズエラーを含むパケット
broadcast-packets	ブロードキャストパケット
multicast-packets	マルチキャストパケット
packets-64-octets	64 オクテットのパケット
packets-65-to-127-octets	65～127 オクテットのパケット
packets-128-to-255-octets	128～255 オクテットのパケット
packets-256-to-511-octets	256～511 オクテットのパケット
packets-512-to-1023-octets	512～1023 オクテットのパケット
packets-1024-to-1526-octets	1024～1526 オクテットのパケット
pause	PAUSE パケット
fifo-drops	受信バッファのオーバーフローで破棄されたパケット
total-good-packets	正常に受信したパケット
class-0	受信キュー class-0 に振り分けられたパケット
class-1	受信キュー class-1 に振り分けられたパケット
class-2	受信キュー class-2 に振り分けられたパケット
class-3	受信キュー class-3 に振り分けられたパケット
backward-drops	バッファが輻輳しているために破棄されたパケット
classifier-drops	送信元もしくは送信先 MAC アドレスが 00:00:00:00:00:00 のパケット、アクセスポートで受信した VLAN タグ付きパケット、トランクポートで受信した VLAN タグ無しパケット
crc-align-errors	CRC エラー、アライメントエラー、物理層でのエラーを検出したパケット
under-size-packets	64 バイト未満で CRC は正常であるパケット
over-size-packets	1519 バイト以上 (VLAN タグ無し) もしくは 1523 バイト以上 (VLAN タグ付き) で CRC は正常であるパケット
fragments	64 バイト未満で CRC が異常であるパケット
jabbers	1519 バイト以上 (VLAN タグ無し) もしくは 1523 バイト以上 (VLAN タグ付き) で CRC が異常であるパケット
control-packets	イーサネットタイプが 0x8808 であるパケット

- [初期値]:

機種	カウンタ番号	種類
SWX2200-24G	1	packets
	2	total-good-packets
	3	total-error-packets
	4	fifo-drops
	5	crc-align-errors
SWX2200-8G、SWX2200-8PoE	1	packets
	2	total-good-packets
	3	total-error-packets

- *switch* : スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

受信フレームカウンタでカウントするフレームの種類を設定する。カウンタの値は **status-counter-frame-rx** で取得する。

[ノート]

本機能の設定を変更すると、当該ポートにおけるすべてのカウンタ (送信、受信、フレーム、オクテット) がリセットされる。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.7.2 送信フレームカウンタでカウントするフレームの種類の設定

[書式]

```
switch control function set counter-frame-tx-type port counter type
no switch control function set counter-frame-tx-type port counter
switch control function get counter-frame-tx-type port counter [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]: -
- *counter* : カウンタ番号
 - [設定値]:

機種	範囲
SWX2200-24G	1 .. 5
SWX2200-8G、SWX2200-8PoE	1 .. 3

- [初期値]: -
- *type* : カウントするパケットの種類
 - [設定値]:

設定値	説明
packets	全てのパケット
broadcast-and-multicast-packets	ブロードキャストパケットとマルチキャストパケット
total-error-packets	パケットの送信時にエラーが発生して送信を中断した回数
broadcast-packets	ブロードキャストパケット

設定値	説明
multicast-packets	マルチキャストパケット
packets-64-octets	64 オクテットのパケット
packets-65-to-127-octets	65～127 オクテットのパケット
packets-128-to-255-octets	128～255 オクテットのパケット
packets-256-to-511-octets	256～511 オクテットのパケット
packets-512-to-1023-octets	512～1023 オクテットのパケット
packets-1024-to-1526-octets	1024～1526 オクテットのパケット
pause	PAUSE パケット
fifo-drops	送信バッファのオーバーフローで破棄されたパケット
total-good-packets	正常に送信されたパケット
class-0	送信キュー class-0 から送信されたパケット
class-1	送信キュー class-1 から送信されたパケット
class-2	送信キュー class-2 から送信されたパケット
class-3	送信キュー class-3 から送信されたパケット
drops	コリジョンの多発、レイトコリジョン、送信バッファへの長時間滞留のいずれかの理由により破棄されたパケット
collisions	コリジョンが発生した回数
cfi-drop	CFI ビットが 1 であるために破棄したパケット (CFI ビットが 1 であるパケットを受信し、当該パケットをタグ無しで送信しようとした場合は破棄される)

- [初期値]:

機種	カウンタ番号	種類
SWX2200-24G	1	packets
	2	total-good-packets
	3	total-error-packets
	4	fifo-drops
	5	collisions
SWX2200-8G、SWX2200-8PoE	1	packets
	2	total-good-packets
	3	total-error-packets

- *switch*: スイッチ

- [設定値]:
 - MAC アドレス
 - 経路
- [初期値]: -

[説明]

送信フレームカウンタでカウントするフレームの種類を設定する。カウンタの値は **status-counter-frame-tx** で取得する。

[ノート]

本機能の設定を変更すると、当該ポートにおけるすべてのカウンタ (送信、受信、フレーム、オクテット) がリセットされる。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.7.3 受信フレームカウンタの値の取得**[書式]****switch control function get status-counter-frame-rx port counter [switch]****[設定値及び初期値]**

- *port*
 - [設定値]: ポート番号
 - [初期値]: -
- *counter*: カウンタ番号
 - [設定値]:

機種	範囲
SWX2200-24G	1 .. 5
SWX2200-8G、SWX2200-8PoE	1 .. 3

- [初期値]: -
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

受信フレームカウンタの値を取得する。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.7.4 送信フレームカウンタの値の取得**[書式]****switch control function get status-counter-frame-tx port counter [switch]****[設定値及び初期値]**

- *port*
 - [設定値]: ポート番号
 - [初期値]: -
- *counter*: カウンタ番号
 - [設定値]:

機種	範囲
SWX2200-24G	1 .. 5
SWX2200-8G、SWX2200-8PoE	1 .. 3

- [初期値]: -
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

送信フレームカウンタの値を取得する。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.7.5 受信オクテットカウンタの値の取得

[書式]

```
switch control function get status-counter-octet-rx port [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]: -
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

受信オクテットカウンタの値を取得する。当カウンタは **counter-frame-rx-type** の設定によらず、受信したすべてのパケットについてオクテット数をカウントする。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.7.6 送信オクテットカウンタの値の取得

[書式]

```
switch control function get status-counter-octet-tx port [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]: -
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

送信オクテットカウンタの値を取得する。当カウンタは **counter-frame-tx-type** の設定によらず、送信したすべてのパケットについてオクテット数をカウントする。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.7.7 カウンタのクリア

[書式]

```
switch control function execute clear-counter [switch]
```

[設定値及び初期値]

- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

全てのカウンタ (全ポート、送信、受信、フレーム、オクテット) をクリアする。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.8 ループ検出

ヤマハスイッチは、MACアドレスの移動を監視する方法と L2MS パケットを監視する方法の 2 種類の方法でネットワークのループを検出します。

MACアドレスの移動とは、同一の MAC アドレスが異なるポートにおいて学習されることです。スイッチは、1 秒あたりの MAC アドレス移動回数を監視しています。移動回数が **loopdetect-count** で指定した閾値を超えている状態が、**loopdetect-time** で設定した時間継続した場合にループが発生したと判断します。

L2MS パケットを監視する方法では、スイッチ自身が送信した制御パケットを受信した回数を監視しています。自身が送信した制御パケットを受信した回数が **loopdetect-count** で指定した閾値を越えている状態が、**loopdetect-time** で設定した時間継続した場合にループが発生したと判断します。

どちらの方法で検出した場合でも、ループが発生したポートでは LED が橙色で点灯します。

ループ検出機能を使用するポートでは、**loopdetect-port-use** を on に設定します。

ループ発生後の動作は **loopdetect-linkdown** で設定します。**loopdetect-linkdown** が linkdown または linkdown-recovery の場合、ループが発生しているポートのうち番号の大きいものから順に、ループが停止するまでリンクダウンしていきます。ループ発生時にもルーターと通信できるようにしておくため、アップリンクポートはポート 1 を使用することが推奨されます。

なお、ループの発生によってリンクダウンしたポートの LED は橙色で点滅します。

53.3.8.1 1 秒あたりのループが発生したと判断する閾値の設定

[書式]

```
switch control function set loopdetect-count count
no switch control function set loopdetect-count count
switch control function get loopdetect-count [switch]
```

[設定値及び初期値]

- *count*
 - [設定値]: 1 秒あたりのループが発生したと判断する閾値 (3 .. 65535)
 - [初期値]: 3
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

1 秒あたりのループが発生したと判断する閾値を設定する。MAC アドレス移動回数またはスイッチ自身が送信した制御パケットを受信した回数が本機能で設定した閾値を越えた状態が、**loopdetect-time** で設定した時間継続した場合にループが発生したと判断する。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.8.2 ループが発生したと判断するまでの時間の設定

[書式]

```
switch control function set loopdetect-time time
no switch control function set loopdetect-time
switch control function get loopdetect-time [switch]
```

[設定値及び初期値]

- *time*
 - [設定値]: 秒数 (2 .. 60)
 - [初期値]: 3
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

1 秒あたりの MAC アドレス移動回数またはスイッチ自身が送信した制御パケットを受信した回数が **loopdetect-count** で設定した閾値以上である状態が継続し、ループが発生したと判断するまでの時間を設定する。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.8.3 ループ発生時の動作の設定**[書式]**

```
switch control function set loopdetect-linkdown action
no switch control function set loopdetect-linkdown
switch control function get loopdetect-linkdown [switch]
```

[設定値及び初期値]

- *action*
- [設定値]:

設定値	説明
none	何も行わない
linkdown	ループが発生したポートをリンクダウンする
linkdown-recovery	ループが発生したポートをリンクダウンした後、一定時間経過後に復帰させる

- [初期値]: none
- *switch*: スイッチ
- [設定値]:
 - MAC アドレス
 - 経路
- [初期値]: -

[説明]

ループ発生時の動作を設定する。

action が linkdown または linkdown-recovery の場合、ループが発生しているポートのうち番号の大きいものから順に、ループが停止するまでリンクダウンしていく。リンクダウンしたポートを復帰させるには **reset-loopdetect** を実行するか、MODE ボタンを押下する。

action が linkdown-recovery の場合、ポートをリンクダウンしてから **loopdetect-recovery-timer** で設定した時間経過後に自動的に復帰させる。

[ノート]

loopdetect-port-use が off に設定されているポートでは、実際にループが発生してもそのことを検出しないため、当機能で設定された動作は行わない。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.8.4 ポートをリンクダウンしてから復帰させるまでの時間の設定**[書式]**

```
switch control function set loopdetect-recovery-timer time
no switch control function set loopdetect-recovery-timer
switch control function get loopdetect-recovery-timer [switch]
```

[設定値及び初期値]

- *time*
- [設定値]: 秒数 (1 .. 86400)
- [初期値]: 300
- *switch*: スイッチ
- [設定値]:
 - MAC アドレス
 - 経路

- [初期値]: -

[説明]

loopdetect-linkdown の設定が linkdown-recovery の場合に、リンクダウンしてから復帰させるまでの時間を設定する。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.8.5 ループ検出機能を使用するか否かの設定

[書式]

```
switch control function set loopdetect-port-use port mode
no switch control function set loopdetect-port-use port
switch control function get loopdetect-port-use port [switch]
```

[設定値及び初期値]

- port
 - [設定値]: ポート番号
 - [初期値]: -
- mode
 - [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: on
- switch: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

ループ検出機能を使用するか否かを設定する。当機能が on に設定されているポートと off に設定されているポートでループが発生した場合は、on に設定されているポートでループを検出する。off に設定されているポートのみでループが発生した場合は、検出しない。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.8.6 L2MS パケットを用いたループ検出を行うか否かの設定

[書式]

```
switch control function set loopdetect-use-control-packet mode
no switch control function set loopdetect-use-control-packet
switch control function get loopdetect-use-control-packet [switch]
```

[設定値及び初期値]

- mode
 - [設定値]:

設定値	説明
on	制御パケットによるループ検出を行う
off	制御パケットによるループ検出を行わない

- [初期値]: on
- switch: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路

- [初期値]:-

[説明]

L2MS パケットを用いたループ検出を行うか否かを設定する。本機能を on に設定すると、スイッチ自身が送信した制御パケットを受信した場合にループが発生したと判断する。

[ノート]

スイッチ配下のハブやスイッチにて輻輳等が発生し、制御パケットが転送されない場合は、ループを検出できないことがある

ヤマハスイッチに本機能が実装されていない場合はコマンドエラーとなる。

RTX1200 は Rev.10.01.45 以降で使用可能。

RTX810 は Rev.11.01.12 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.8.7 ループ検出機能に関するポートの状態の取得

[書式]

```
switch control function get status-loopdetect-port port [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]:-
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]:-

[説明]

ループ検出機能に関するポートの状態を取得する。

状態	説明
normal	正常
loopdetect	ループが発生している
linkdown	ループが発生したため、リンクダウンした

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.8.8 リンクダウンしている状態から復帰するまでの残り時間の取得

[書式]

```
switch control function get status-loopdetect-recovery-timer port [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]:-
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]:-

[説明]

ループ発生によってリンクダウンしている状態から復帰するまでの残り時間を取得する。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.8.9 ループ発生によってリンクダウンしているポートの復帰**[書式]****switch control function execute reset-loopdetect** [*switch*]**[設定値及び初期値]**

- *switch* : スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]:-

[説明]

ループ発生によってリンクダウンしている全てのポートを復帰させる。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.9 PoE 給電**53.3.9.1 各ポートで給電可能なクラスの上限の設定****[書式]**

```
switch control function set poe-class port class
no switch control function set poe-class port class
switch control function get poe-class port [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]:-
- *class*
 - [設定値]:

設定値	説明
none	給電しない
class3	15.4W までの機器まで給電する
class4	30W までの機器まで給電する

- [初期値]:
 - class4(1、3、5、7ポート)
 - class3(2、4、6、8ポート)
- *switch* : スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]:-

[説明]

各ポート毎に給電する上限を設定する。スイッチの上段ポート(1、3、5、7ポート)は、クラス 4(30W)を上限に設定できる。下段ポート(2、4、6、8ポート)はクラス 3(15.4W)が上限となる。給電は上下のポートを対として、上段のポートにクラス 4(30W)の機器を接続すると、その直下に位置するポートへの給電を停止する。

[ノート]

SWX2200-8PoE でのみ使用可能。

設定したクラス以上の機器を接続した場合、実際に使用する電力が設定したクラス以下であっても給電は行われない。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.9.2 各ポートの給電状態の取得

[書式]

switch control function get status-poe-state port [switch]

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]: -
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

状態	説明	備考
none	給電していない	-
terminate	給電停止	-
supply-class0, supply-class1, supply-class2, supply-class3, supply-class4	給電中(給電中のクラス)	-
overcurrent	過電流による給電停止	-
class-failure	電力クラス設定より大きなクラスを認識したことによる給電停止	SWX2200-8PoE でのみ発生
over-supply	供給電力が最大給電能力を超えたことによる給電停止	-
over-temperature	内部温度が 60°C を超えたことによる給電停止	SWX2200-8PoE でのみ発生
fan-lock	ファン停止による給電停止	SWX2200-8PoE でのみ発生
forced-terminate	Class3(15.4W)を給電していたポートに Class4(30W)給電が給電されたことによる給電停止	SWX2200-8PoE でのみ発生
power-failure	電源故障による給電停止	-

[ノート]

SWX2200-8PoE、SWX2100-10PoE、SWX2100-5PoE で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.9.3 各ポートに接続された機器のクラスの取得

[書式]

switch control function get status-poe-detect-class port [switch]

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]: -
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路

- [初期値]:-

[説明]

ポートに接続された機器のクラスを取得する。

[ノート]

SWX2200-8PoE、SWX2100-10PoE、SWX2100-5PoE でのみ使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.9.4 スイッチの内部温度の取得

[書式]

switch control function get status-poe-temperature [*switch*]

[設定値及び初期値]

- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]:-

[説明]

スイッチの内部温度を取得する。

[ノート]

SWX2200-8PoE でのみ使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.9.5 各ポートの供給電力の取得

[書式]

switch control function get status-poe-supply port [*switch*]

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]:-
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]:-

[説明]

各ポートの現在の供給電力を取得する。

[ノート]

SWX2200-8PoE、SWX2100-10PoE、SWX2100-5PoE で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.3.9.6 各ポートの詳細な供給電力の取得

[書式]

switch control function get status-poe-supply-detail port [*switch*]

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]:-

- *switch* : スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]:-

[説明]

各ポートの詳細な現在の供給電力を取得する。

[ノート]

SWX2100-10PoE、SWX2100-5PoE で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830, RTX810

53.3.9.7 スイッチの総供給電力の取得**[書式]**

switch control function get status-poe-supply-total [*switch*]

[設定値及び初期値]

- *switch* : スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]:-

[説明]

スイッチの総供給電力を取得する。単位は W (ワット)。

[ノート]

SWX2100-10PoE、SWX2100-5PoE で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830, RTX810

53.3.9.8 給電復帰**[書式]**

switch control function execute restart-poe-supply [*switch*]

[設定値及び初期値]

- *switch* : スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]:-

[説明]

給電を復帰させる。なお、何らかの異常により給電を停止している場合には、電源異常による給電停止の場合は、本コマンドでの給電復帰はできない。

[ノート]

SWX2200-8PoE でのみ使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830

53.3.9.9 各ポートへの給電を開始**[書式]**

switch control function execute start-poe-supply port [*switch*]

[設定値及び初期値]

- *port*

- [設定値]: ポート番号
- [初期値]: -
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

各ポートへの給電を開始する。

[ノート]

SWX2100-10PoE、SWX2100-5PoE で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830, RTX810

53.3.9.10 各ポートへの給電を停止**[書式]**

```
switch control function execute stop-poe-supply port [switch]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号
 - [初期値]: -
- *switch*: スイッチ
 - [設定値]:
 - MAC アドレス
 - 経路
 - [初期値]: -

[説明]

各ポートへの給電を停止する。

[ノート]

SWX2100-10PoE、SWX2100-5PoE で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830, RTX810

53.4 アクセスポイントの制御

53.4.1 アクセスポイントの選択

[書式]

```
ap select ap
no ap select
```

[設定値及び初期値]

- *ap*
 - [設定値]:

設定値	説明
MAC アドレスもしくは経路	アクセスポイントを選択する
none	アクセスポイントを選択しない
 - [初期値]: -

[説明]

対象とするアクセスポイントを選択する。以降プロンプトには console prompt で設定した文字列と ap パラメータにより選択したアクセスポイントが続けて表示される。

ap select none または **no ap select** を実行すると、プロンプトにアクセスポイントが表示されなくなる。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.4.2 アクセスポイントの設定ファイルを格納するディレクトリの指定

[書式]

ap config directory *path*

no ap config directory [*path*]

[設定値及び初期値]

- *path*

- [設定値]: 相対パスまたは絶対パス (半角 256 文字以下、全角 128 文字以下 (RTX1210 Rev.14.01.28 以降、RTX830 Rev.15.02.03 以降、RTX1220))
- [初期値]: /ap_config

[説明]

アクセスポイントの設定ファイル(config)を格納するディレクトリを指定する。

相対パスを指定した場合、環境変数 PWD を起点としたパスと解釈される。

PWD は **set** コマンドで変更可能であり、初期値は "/" である。

RTX1210 Rev.14.01.28 以降、および、RTX830 Rev.15.02.03 以降、RTX1220 では、*path* が RTFS 領域となる場合には、*path* にマルチバイト文字を使用することはできない。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.4.3 アクセスポイントの設定を保存するファイル名の指定

[書式]

ap config filename *name*

no ap config filename [*name*]

[設定値及び初期値]

- *name*

- [設定値]: config ファイル名 (半角 99 文字以下、全角 49 文字以下 (RTX1210 Rev.14.01.28 以降、および、RTX830 Rev.15.02.03 以降、RTX1220))
- [初期値]: -

[説明]

アクセスポイントの設定を保存するファイル名を指定する。

このコマンドが省略された場合は、**ap select** で指定された文字列に .conf を付けたものをファイル名とする。

ただし:(コロン)は_(アンダースコア)に置き換えられる。

複数の **ap select** コマンドで同じファイル名を指定することができる。

RTX1210 Rev.14.01.28 以降、および、RTX830 Rev.15.02.03 以降、RTX1220 では、**ap config directory** コマンドで指定したディレクトリが RTFS 領域である場合は、ファイル名にマルチバイト文字を使用することはできない。

本コマンドを実行する前に **ap select** コマンドでスイッチを指定しておく必要がある。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.4.4 アクセスポイントの設定のバックアップ実行

[書式]

ap control config get [*ap*]

ap control config get [[*interface*] all]

[設定値及び初期値]

- *ap*

- [設定値]:

設定値	説明
MAC アドレスもしくは経路	選択したアクセスポイントのみ
all	全てのアクセスポイント

- [初期値]:-
- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]:-

[説明]

アクセスポイントの設定のバックアップ動作を実行する。

ap パラメータを使用した場合は、対象となるアクセスポイントのみバックアップを行う。
all を指定すると、ヤマハルーターが認識している全てのアクセスポイントのコンフィグを保存する。
LAN インタフェースを指定すると、LAN インタフェースにつながっているアクセスポイントだけを対象とする。
パラメータを省略した場合は、*all* を指定した時と同様になる。

[ノート]

schedule at コマンドで指定することができる。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.4.5 アクセスポイントの設定の復元実行

[書式]

```
ap control config set [ap]
ap control config set [[interface] all]
```

[設定値及び初期値]

- *ap*
 - [設定値]:

設定値	説明
MAC アドレスもしくは経路	選択したアクセスポイントのみ
all	全てのアクセスポイント

- [初期値]:-
- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]:-

[説明]

アクセスポイントの設定の復元動作を実行する。

ap パラメータを使用した場合は、対象となるアクセスポイントのみ復元を行う。
all を指定すると、ヤマハルーターが認識している全てのアクセスポイントのコンフィグを復元する。
LAN インタフェースを指定すると、LAN インタフェースにつながっているアクセスポイントだけを対象とする。
パラメータを省略した場合は、*all* を指定した時と同様になる。

[ノート]

schedule at コマンドで指定することができる。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.4.6 アクセスポイントの設定の削除

[書式]

ap control config delete [*ap*]

[設定値及び初期値]

- *ap*
- [設定値]:

設定値	説明
MAC アドレスもしくは経路	選択したアクセスポイントのみ
all	全てのアクセスポイント

- [初期値]:-

[説明]

アクセスポイントの設定の削除を実行する。

ap パラメータを使用した場合は、対象となるアクセスポイントのみ削除を行う。

ap パラメータを省略した場合は、全てのアクセスポイントの削除を行う。

[ノート]

schedule at コマンドで指定することができる。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.4.7 アクセスポイント設定のゼロコンフィグ機能を使用するか否かの設定

[書式]

ap control config-auto-set use *use*

no ap control config-auto-set use [*use*]

[設定値及び初期値]

- *use*
- [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: on

[説明]

アクセスポイント設定のゼロコンフィグ機能を使用するか否かを設定する。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.4.8 アクセスポイントの HTTP リビジョンアップ機能の実行

[書式]

ap control firmware update go [*ap*]

[設定値及び初期値]

- *ap*
- [設定値]:

設定値	説明
MAC アドレスもしくは経路	選択したアクセスポイントのみ
all	全てのアクセスポイント

- [初期値]:-

[説明]

アクセスポイントに対してファームウェアの更新を要求する。

ap パラメータを省略した場合は、全てのアクセスポイントに対して本コマンドを実行する。

[ノート]

schedule at コマンドで指定することができる。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.4.9 アクセスポイント制御用の HTTP プロキシの使用**[書式]**

```
ap control http proxy use use
```

```
no ap control http proxy use [use]
```

[設定値及び初期値]

- *use*

- [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: on

[説明]

アクセスポイント制御用の HTTP プロキシ機能を使用するか否かを設定する。

use を on に設定した場合、ルーター経由でアクセスポイントの GUI にアクセスすることができる。

[ノート]

L2MS においてルーターの管理下におかれているアクセスポイントに対してのみ、HTTP プロキシ機能を利用することができる。

また、アクセスポイントに IP アドレスが割り当てられている必要がある。

アクセスポイント毎に認証情報を入力する必要がなく、ルーターを経由することで、遠隔拠点から VPN や静的 IP マスカレードなどを使わずともアクセスポイントの設定ができる。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.4.10 アクセスポイント制御用の HTTP プロキシのタイムアウト時間の設定**[書式]**

```
ap control http proxy timeout time
```

```
no ap control http proxy timeout [time]
```

[設定値及び初期値]

- *time*

- [設定値]: タイムアウトの秒数
- [初期値]: 60

[説明]

アクセスポイント制御用の HTTP プロキシ機能のタイムアウト時間を設定する。

プロキシ経由でアクセスポイントの GUI にアクセスする際、アクセスポイントから指定時間以内に応答がなければタイムアウトになる。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

53.5 ルーターの制御

53.5.1 HTTP プロキシ経由での Web GUI へのアクセスを許可するか否かの設定

[書式]

```
httpd proxy-access l2ms permit permit
no httpd proxy-access l2ms permit [permit]
```

[設定値及び初期値]

- *permit*
- [設定値]:

設定値	説明
on	HTTP プロキシ経由での Web GUI へのアクセスを許可する
off	HTTP プロキシ経由での Web GUI へのアクセスを許可しない

- [初期値]: off

[説明]

HTTP プロキシ経由での Web GUI へのアクセスを許可するか否かを設定する。*permit* が on である場合は、マネージャの Web GUI から本機の Web GUI を表示するときに HTTP プロキシ経由でアクセスする。

[ノート]

switch control mode コマンドで *mode* に *agent* が設定されていない場合、本コマンドの設定は反映されない。

RTX1210 は Rev.14.01.20 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830

第 54 章

YNO エージェント

YNO エージェントは、ヤマハネットワーク機器を「Yamaha Network Organizer (YNO)」で遠隔管理するための機能です。YNO エージェント機能を有効にしたヤマハネットワーク機器はインターネット経由で YNO マネージャーへ接続し、必要に応じて以下の処理を実施します。

- ヤマハネットワーク機器動作状態の YNO マネージャーへの通知
- CONFIG の送信・適用・保存
- ファームウェアの更新
- コマンドの実行
- GUI Forwarder によるヤマハネットワーク機器 GUI の表示
- ゼロコンフィグによる CONFIG の自動適用

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.rtpo.yamaha.co.jp/RT/docs/yno/agent/>

54.1 YNO エージェント機能を使用するか否かの設定

[書式]

```
yno use sw
no yno use sw
```

[設定値及び初期値]

- *sw*
- [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: off

[説明]

YNO エージェント機能を使用するか否かを設定する。

[ノート]

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。
 RTX1210 は Rev.14.01.14 以降で使用可能。
 RTX810 は Rev.11.01.28 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830, RTX810

54.2 YNO マネージャー接続用のアクセスコードの設定

[書式]

```
yno access code operator_id access_code
no yno access code [operator_id [access_code]]
```

[設定値及び初期値]

- *operator_id*
 - [設定値]: オペレーター ID (半角 4 文字以上 かつ 半角 64 文字以内)
 - [初期値]: -
- *access_code*
 - [設定値]: アクセスコード (半角 8 文字以上 かつ 半角 64 文字以内)
 - [初期値]: -

[説明]

YNO エージェント機能が YNO マネージャーへ接続する際に使用するアクセスコードを設定する。

ヤマハネットワーク機器は `operator_id` で指定したオペレーターの管理対象となる。同一オペレーターが管理するすべてのヤマハネットワーク機器には、同一のオペレーター ID およびアクセスコードを設定する必要がある。

`yno zero-config id` コマンドが設定されているときは、本コマンドは設定できない。

[ノート]

YNO マネージャーでアクセスコードを変更すると、管理対象のヤマハネットワーク機器で新しいアクセスコードを含んだ本コマンドが自動で実行・保存される。

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。

RTX1210 は Rev.14.01.14 以降で使用可能。

RTX810 は Rev.11.01.28 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830, RTX810

54.3 YNO エージェント機能に関する追加の SYSLOG を出力するか否かの設定

[書式]

```
yno log type [type...]
```

```
no yno log [type...]
```

[設定値及び初期値]

- `type`

- [設定値]:

設定値	説明
action-read	ヤマハネットワーク機器の動作状態や CONFIG の読み出しに関する SYSLOG を出力する
inform	YNO マネージャーとの定期通信に関する SYSLOG を出力する

- [初期値]: -

[説明]

YNO エージェント機能に関する追加の SYSLOG を出力するか否かを設定する。

[ノート]

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。

RTX1210 は Rev.14.01.14 以降で使用可能。

RTX810 は Rev.11.01.28 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830, RTX810

54.4 YNO マネージャーに表示される自身の機器説明の設定

[書式]

```
description yno description
```

```
no description yno [description]
```

[設定値及び初期値]

- `description`

- [設定値]: 説明の文字列 (最大 32 文字/半角、16 文字/全角)
- [初期値]: 空文字列

[説明]

YNO マネージャーに表示されるヤマハネットワーク機器の説明を設定する。

[ノート]

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。
 RTX1210 は Rev.14.01.14 以降で使用可能。
 RTX810 は Rev.11.01.28 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830, RTX810

54.5 YNO で使用する HTTPS プロキシサーバーの設定

[書式]

```
yno https-proxy proxy_server port
no yno https-proxy [proxy_server [port]]
```

[設定値及び初期値]

- *proxy_server*
 - [設定値]: HTTPS プロキシサーバーのホスト名、もしくは IP アドレス
 - [初期値]: -
- *port*
 - [設定値]: HTTPS プロキシサーバーのポート番号 (1..65535)
 - [初期値]: -

[説明]

YNO で使用する HTTPS プロキシサーバーを設定する。

proxy_server には、HTTPS プロキシサーバーの FQDN 形式のホスト名、または IP アドレスを 255 文字以内の半角英数字および半角記号で指定する。

port には、HTTPS プロキシサーバーのポート番号を指定する。

[ノート]

ユーザー認証が必要な HTTPS プロキシサーバーを使用することはできない。

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。
 RTX1210 は Rev.14.01.26 以降で使用可能。
 RTX830 は Rev.15.02.03 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

54.6 GUI Forwarder 接続のタイムアウト時間の設定

[書式]

```
yno gui-forwarder timeout time
no yno gui-forwarder timeout [time]
```

[設定値及び初期値]

- *time*
 - [設定値]: 秒数 (3..60)
 - [初期値]:
 - 30 (RTX1210 Rev.14.01.34 以降、RTX830 Rev.15.02.10 以降、RTX1220)
 - 5 (上記以外)

[説明]

GUI Forwarder 接続のタイムアウト時間を設定する。

本コマンドで設定した時間以内に GUI Forwarder サーバーからの応答がなかった場合、GUI Forwarder セッションを切断する。

[ノート]

RTX830 は Rev.15.02.03 以降で使用可能。
 RTX1210 は Rev.14.01.26 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX830

54.7 YNO のゼロコンフィグの設定

[書式]

```
yno zero-config id text operator_id place_id [password]
no yno zero-config id [text [operator_id [place_id [password]]]]
```

[設定値及び初期値]

- *operator_id*
 - [設定値]: オペレーター ID (半角 4 文字以上 かつ 半角 64 文字以内)
 - [初期値]: -
- *place_id*
 - [設定値]: プレース ID (半角 64 文字以内)
 - [初期値]: -
- *password*
 - [設定値]: パスワード (半角 64 文字以内 省略可)
 - [初期値]: -

[説明]

YNO エージェント機能のゼロコンフィグで使用するプレース ID やパスワードを設定する。本コマンドが設定されると自動で YNO マネージャーへの接続を試み、接続確立後にゼロコンフィグが作動する。

yno access code コマンドが設定されているときは、本コマンドは設定できない。

[ノート]

RTX5000 は Rev.14.00.32 以降で使用可能。
 RTX3500 は Rev.14.00.32 以降で使用可能。
 RTX1210 は Rev.14.01.32 以降で使用可能。
 RTX830 は Rev.15.02.08 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

54.8 YNO エージェント機能の動作状態の表示

[書式]

```
show status yno
```

[説明]

YNO エージェント機能の動作状態を表示する。ファームウェアのリビジョンにより表示内容が異なる。

- [新形式]
 - CWMP の動作状態

表示	説明
未接続(設定未完了)	YNO エージェント機能が無効、または設定が不足している
未接続(起動処理中)	YNO エージェント機能が有効になり、初期化および ACS への接続中
未接続(終了処理中)	YNO エージェント機能が無効になり、ACS と切断処理中

表示	説明
正常([セッション確立日時])	ACS との接続に成功した(括弧内にはセッションの確立日時を表示)
異常([理由])	ACS との接続に失敗した(括弧内には異常理由を表示)
ゼロコンフィグ処理中 ([異常理由])	ACS との接続に成功し、ゼロコンフィグが動作中(処理中に異常が発生した場合は括弧内に異常理由を表示)

• XMPP の動作状態

表示	説明
未接続	XMPP サーバーに接続していない
接続	XMPP を使用できる
異常	XMPP を使用できない

• GFW の動作状態

表示	説明
未接続	GFW サーバーに接続していない
接続	GFW を使用できる
異常	GFW を使用できない

• LAS の動作状態 (LAS 対応ファームウェアのみ)

表示	説明
未接続	LAS サーバーに接続していない
接続	LAS を使用できる
異常	LAS を使用できない

• ヤマハネットワーク機器を管理しているオペレーターの ID

• [旧型式]

• YNO エージェント機能の動作状態

現在の状態	説明
設定未完了	YN0 エージェント機能が無効、または設定が不足している
起動処理中	YN0 エージェント機能が有効になり、初期化および YNO マネージャーへの接続中
終了処理中	YN0 エージェント機能が無効になり、YN0 マネージャーと切断処理中
正常動作中	YN0 マネージャーへの接続に成功した
異常発生	YN0 マネージャーへの接続に失敗した

• ヤマハネットワーク機器を管理しているオペレーターの ID

• YNO マネージャーへのセッション確立日時

• XMPP プロトコルを使用できるか否か

• GUI Forwarder を使用できるか否か (GUI Forwarder 接続対応ファームウェアのみ)

[ノート]

以下の機種及びファームウェアでは新型式の内容が、その他では旧型式の内容が表示される。

機種	リビジョン
RTX5000	Rev.14.00.32 以降
RTX3500	Rev.14.00.32 以降

機種	リビジョン
RTX1210	Rev.14.01.28 以降
RTX830	Rev.15.02.03 以降
RTX1220	すべてのリビジョン

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。

RTX1210 は Rev.14.01.14 以降で使用可能。

RTX810 は Rev.11.01.28 以降で使用可能。

[表示例]

- [新形式]

```
> show status yno
CWMP:          正常 (2018/03/14 14:30:21)
XMPP:          正常
GFW:           正常
LAS:           正常
オペレーター ID:  dummy_id
```

```
> show status yno
CWMP:          異常 (ACS への接続に失敗しました)
XMPP:          未接続
GFW:           未接続
LAS:           未接続
オペレーター ID:  dummy_id
```

- [旧形式]

```
> show status yno
現在の状態:    正常動作中
オペレーター ID:  dummy_id
セッション確立日時: 2016/12/18 11:46:03
XMPP 接続:     有効
GFW 接続:      有効
```

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830, RTX810

54.9 LAS (Log Analysis Service)

54.9.1 SYSLOG 送信キューの長さの設定

[書式]

```
yno las syslog queue length length
```

```
no yno las syslog queue length
```

[設定値及び初期値]

- *length*

- [設定値]: 長さ
- [設定値]:
 - 1000..40000 (RTX5000/RTX3500)
 - 1000..10000 (上記以外)
- [初期値]:
 - 40000 (RTX5000/RTX3500)
 - 10000 (上記以外)

[説明]

SYSLOG 送信キュー長の最大値を設定する。現在の送信キュー長より小さい値を設定しても、すでに送信キューに蓄積されている SYSLOG は破棄されることなく、順次 LAS サーバーに送信される。

[ノート]

RTX5000 は Rev.14.00.32 以降で使用可能。
RTX3500 は Rev.14.00.32 以降で使用可能。
RTX1220 は Rev.15.04.03 以降で使用可能。
RTX1210 は Rev.14.01.40 以降で使用可能。
RTX830 は Rev.15.02.20 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

54.9.2 LAS クライアントが送信したリクエストに対する LAS サーバーからの応答待ちがタイムアウトするまでの時間の設定

[書式]

```
yno las request timeout seconds  
no yno las request timeout
```

[設定値及び初期値]

- *seconds*
 - [設定値]: 秒数 (10..60)
 - [初期値]: 30

[説明]

LAS クライアントが送信したリクエストに対する LAS サーバーからの応答待ちがタイムアウトするまでの時間を設定する。

[ノート]

RTX5000 は Rev.14.00.32 以降で使用可能。
RTX3500 は Rev.14.00.32 以降で使用可能。
RTX1220 は Rev.15.04.03 以降で使用可能。
RTX1210 は Rev.14.01.40 以降で使用可能。
RTX830 は Rev.15.02.20 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

54.9.3 LAS クライアントがリクエストの送信を再試行する回数の設定

[書式]

```
yno las request retry count  
no yno las request retry
```

[設定値及び初期値]

- *count*
 - [設定値]: 回数 (0..5)
 - [初期値]: 3

[説明]

LAS クライアントがリクエストの送信を再試行する回数を設定する。

[ノート]

RTX5000 は Rev.14.00.32 以降で使用可能。
RTX3500 は Rev.14.00.32 以降で使用可能。
RTX1220 は Rev.15.04.03 以降で使用可能。
RTX1210 は Rev.14.01.40 以降で使用可能。
RTX830 は Rev.15.02.20 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

54.9.4 LAS サーバーとの接続に対するキープアライブの設定

[書式]

```
yno las connection keepalive interval [timeout=sw]
```

```
no yno las connection keepalive
```

[設定値及び初期値]

- *interval*

- [設定値]:

設定値	説明
off	キープアライブをしない
30..300	キープアライブの時間間隔 (秒数)

- [初期値]: 60

- *sw*

- [設定値]:

設定値	説明
on	LAS サーバーから応答がない場合に接続を切断する
off	LAS サーバーから応答がなくても接続を切断しない

- [初期値]: off

[説明]

YNO マネージャーでリアルタイム表示をしている間、LAS クライアントは LAS サーバーとの間で接続を確立した状態となる。接続が確立されている間は、*interval* に設定された時間間隔で LAS クライアントからキープアライブパケットが送信される。*sw* が on に設定されている場合、キープアライブパケットが送信されてから *interval* で設定された時間までに LAS サーバーから応答がないと、LAS クライアントは接続を一旦切断し、再接続を試みる。

[ノート]

RTX5000 は Rev.14.00.32 以降で使用可能。

RTX3500 は Rev.14.00.32 以降で使用可能。

RTX1220 は Rev.15.04.03 以降で使用可能。

RTX1210 は Rev.14.01.40 以降で使用可能。

RTX830 は Rev.15.02.20 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

54.9.5 LAS の動作状態の表示

[書式]

```
show status yno las
```

[説明]

LAS の動作状態を表示する。

[ノート]

RTX5000 は Rev.14.00.32 以降で使用可能。

RTX3500 は Rev.14.00.32 以降で使用可能。

RTX1220 は Rev.15.04.03 以降で使用可能。

RTX1210 は Rev.14.01.40 以降で使用可能。

RTX830 は Rev.15.02.20 以降で使用可能。

[表示例]

```
> show status yno las
機能                : 有効
ログ送信結果        : 成功
SYSLOG 送信速度     : 100 行 / 60 秒
SYSLOG 送信キュー長 : 26
```

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

54.10 XMPP サーバーとのキープアライブの時間間隔の設定

[書式]

```
yno xmpp connection keepalive interval
no yno xmpp connection keepalive [interval]
```

[設定値及び初期値]

- *interval*
 - [設定値]: キープアライブパケットを送出する時間間隔 (30..300 秒)
 - [初期値]: 300

[説明]

XMPP サーバーとのキープアライブ通信を実施する時間間隔を設定する。

[ノート]

本コマンドを実行した場合、YNO マネージャーとの通信が一時的にできなくなる可能性があります。その場合、次の XMPP サーバーとのキープアライブ通信の実施時に XMPP 接続が再接続され、自動的に復旧されます。

RTX5000 は Rev.14.00.32 以降で使用可能。
RTX3500 は Rev.14.00.32 以降で使用可能。
RTX1210 は Rev.14.01.41 以降で使用可能。
RTX830 は Rev.15.02.22 以降で使用可能。
RTX1220 は Rev.15.04.04 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

第 55 章

診断

55.1 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
```

[設定値及び初期値]

- *interface*
 - [設定値]: 受信側の LAN、PP インタフェース名
 - [初期値]: -
- *protocol*
 - [設定値]: 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)
 - [設定値]:
 - 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

設定値	説明
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

- [初期値]: -
- *src_addr*
 - [設定値]: 入力パケットの送信元 IP アドレス
 - [初期値]: -
- *src_port*
 - [設定値]: 入力パケットの送信元ポート番号
 - [初期値]: -
- *dst_addr*
 - [設定値]: 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)
 - [初期値]: -

[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]

RTX1220, RTX1210, RTX1200, SRT100

55.2 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*

[設定値及び初期値]

- *interface*
 - [設定値]: 受信側の LAN、PP インタフェース名
 - [初期値]: -
- *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)
 - [設定値]:

設定値	説明
tcp	TCP パケット
udp	UDP パケット

- [初期値]: -
- *dst_addr*
 - [設定値]: 診断対象の宛先 IP アドレス
 - [初期値]: -
- *src_port*
 - [設定値]: 診断対象の宛先ポート番号
 - [初期値]: -

[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]

RTX1220, RTX1210, RTX1200, SRT100

55.3 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*

[設定値及び初期値]

- *num*
 - [設定値]: 検出可能な通過パケットの最大数 (100..1000000)
 - [初期値]: 2000

[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。

[適用モデル]

RTX1220, RTX1210, RTX1200, SRT100

55.4 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*

[設定値及び初期値]

- *num*
 - [設定値]: 診断結果として保存する履歴数 (1..10)
 - [初期値]: 3

[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。

[適用モデル]

RTX1220, RTX1210, RTX1200, SRT100

55.5 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]

RTX1220, RTX1210, RTX1200, SRT100

55.6 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]

RTX1220, RTX1210, RTX1200, SRT100

55.7 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]

RTX1220, RTX1210, RTX1200, SRT100

第 56 章

統計

56.1 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]
```

[設定値及び初期値]

- *type* : 内部リソースの種別
 - [設定値] :

設定値	説明
cpu	CPU 利用率
memory	メモリ使用率
traffic	インターフェース別のトラフィック量
flow	ファストパスフロー数
nat	NAT テーブルのエントリー数
route	経路数
filter	動的フィルターのセッション数
qos	各キューの処理量
application	アプリケーションのトラフィック情報

- [初期値] : -
- *sw*
 - [設定値] :

設定値	説明
on	統計機能を有効にする
off	統計機能を無効にする

- [初期値] : off

[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。

RTX1220、RTX1210、RTX830 では *type* パラメータの qos キーワードは使用できない。

type パラメータの application キーワードは RTX830 の Rev.15.02.13 以降で使用可能。

RTX1210 は Rev.14.01.34 以降で使用可能

RTX830 は Rev.15.02.10 以降で使用可能

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, SRT100

第 57 章

DPI

Deep Packet Inspection (以下 DPI) は、IP ネットワーク上を流れるトラフィックを高度に検査することにより、そのパケットがどのアプリケーションのものであるかを識別することができる技術です。

ヤマハルーターでは、DPI の識別結果を以下のように利用することができます。

- 経路の選択
- フィルタリング
- QoS
- トラフィックの可視化

DPI は有償サービスにより提供される機能です。ご利用いただくには、別途ライセンス製品を購入していただく必要があります。

本機能に関する技術情報は以下に示す URL で公開しています。

<http://www.rtpro.yamaha.co.jp/RT/docs/dpi/>

57.1 DPI を使用するか否かの設定

[書式]

```
dpi use switch [reject]
```

```
no dpi use [switch [reject]]
```

[設定値及び初期値]

- *switch*

- [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: off
- *reject*: 未識別のパケットを破棄するか否か

- [設定値]:

設定値	説明
on	破棄する
off	破棄しない

- [初期値]: off

[説明]

DPI を使用するか否かを設定する。

DPI のアクティベーション中でアプリケーションの識別ができない場合のパケットは、*reject* パラメーターの設定に従い通過、または破棄される。

[ノート]

アプリケーション識別のためには、すべてのパケットをノーマルパスで処理する必要がある。IPv4 の環境では、**ip routeing process** コマンドを、IPv6 の環境では **ipv6 routing process** コマンドを **normal** に設定する必要がある。

RTX830 は Rev.15.02.13 以降で使用可能。

[適用モデル]

RTX830

57.2 IPv4 の DPI フィルターの設定

[書式]

```
ip dpi filter filter_num pass_reject src_addr[/mask] [dest_addr[/mask] [application]]
ip dpi filter filter_num pass_reject src_addr[/mask] [dest_addr[/mask] [group_num]]
no ip dpi filter filter_num [pass_reject ...]
```

[設定値及び初期値]

- *filter_num*
 - [設定値]: DPI のフィルター番号 (1..2147483647)
 - [初期値]: -

- *pass_reject*
 - [設定値]:

設定値	説明
pass	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)
pass-nolog	一致すれば通す(ログに記録しない)
reject	一致すれば破棄する(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)

- [初期値]: -
- *src_addr*: IP パケットの始点アドレス
 - [設定値]:
 - IPv4 アドレス
 - A.B.C.D (A ~ D: 0 ~ 255 もしくは *)
 - 上記表記で A ~ D を * とすると、該当する 8 ビット分についてはすべての値に対応する
 - 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
 - カンマ区切りで複数設定することができる
 - FQDN
 - 任意の文字列 (半角 255 文字以内。/, : は使用できない。 , は区切り文字として使われるため、使用できない)
 - * から始まる FQDN は * より後ろの文字列を後方一致条件として判断する。たとえば *.example.co.jp は www.example.co.jp、mail.example.co.jp などと一致する
 - , を区切りとして複数設定することができる。IP アドレスと混在することも可能
 - * (すべてのアドレスに対応)
 - [初期値]: -
- *dest_addr*: IP パケットの終点アドレス
 - [設定値]:
 - *src_addr* と同じ形式
 - 省略した場合は 1 個の * と同じ
 - [初期値]: -
- *mask*: ネットワークアドレスのビットマスク
 - [設定値]:
 - A.B.C.D (A ~ D: 0 ~ 255)
 - 0x に続く十六進数
 - マスクビット数
 - 省略時は 0xffffffff と同じ
 - [初期値]: -
- *application*: フィルタリング対象とするアプリケーション、またはカテゴリー
 - [設定値]:

- アプリケーションを表すニーモニック
- "@" で始まるカテゴリをあらわすニーモニック
- 上記文字列をカンマで区切った並び (10 個以内、アプリケーションとカテゴリの混在が可能)
- 省略時は 1 つの * と同じ
- [初期値]:-
- `group_num`: グループ ID
 - [設定値]: **dpi group set** コマンドでグループ化したアプリケーションのグループ ID
 - [初期値]:-

[説明]

DPI で使用する IPv4 のフィルターを設定する。本コマンドで設定されたフィルターは **ip interface dpi filter** コマンドと組み合わせて利用することで、特定アプリケーションのパケットのフィルタリングをすることができる。また、フィルター型ルーティングと利用することで、特定アプリケーションのパケットの経路選択を行うことができる。アプリケーションを表すニーモニックには、**show dpi application** コマンドで表示されるものを使用する。またカテゴリを表すニーモニックには、**show dpi category** コマンドで表示されるものを使用する。

[ノート]

アプリケーションの識別が完了していないパケットは、フィルターの設定によらず必ず通過する。また、DPI のアクティベーション中でアプリケーションの識別結果が得られない場合には、すべてのパケットは **dpi use** コマンドの `reject` の設定に従う。

RTX830 は Rev.15.02.13 以降で使用可能。

[設定例]

- Web アクセスとメールの使用のみ許可する

```
# ip dpi filter 1 pass * * @web,@email,@webmail
# ip dpi filter 100 reject * *
# ip lan2 dpi filter out 1 100
```

- Office365 のパケットは PP1 インターフェース経由で、その他は TUNNEL1 経由で送信する

```
# dpi group set 100 name=o365 word_online sharepoint_online powerpoint_online
outlook office_docs office365 ms_sway ms_planner ms_onenote lync_online
excel_online
# ip dpi filter 1 pass * * 100
# ip route default gateway pp 1 dpi 1 gateway tunnel 1
```

[適用モデル]

RTX830

57.3 IPv6 の DPI フィルタの設定**[書式]**

```
ipv6 dpi filter filter_num pass_reject src_addr[/prefix_len] [dest_addr[/prefix_len][application]]
ipv6 dpi filter filter_num pass_reject src_addr[/prefix_len] [dest_addr[/prefix_len][group]]
no ipv6 dpi filter filter_num [pass_reject ...]
```

[設定値及び初期値]

- `filter_num`
 - [設定値]: DPI のフィルタ番号 (1..2147483647)
 - [初期値]:-
- `pass_reject`
 - [設定値]:

設定値	説明
pass	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)
pass-nolog	一致すれば通す(ログに記録しない)
reject	一致すれば破棄する(ログに記録しない)

設定値	説明
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)

- [初期値]:-
- *src_addr*: IPv6 パケットの始点アドレス
 - [設定値]:
 - IPv6 アドレス
 - 間に - を挟む、- を前につける、または - を後ろにつける範囲の指定ができる
 - カンマ区切りで複数設定することができる
 - *(すべてのアドレスに対応)
 - [初期値]:-
- *dest_addr*: IPv6 パケットの終点アドレス
 - [設定値]:
 - *src_addr* と同じ形式
 - 省略した場合は 1 個の * と同じ
 - [初期値]:-
- *prefix_len*
 - [設定値]: プレフィックス長
 - [初期値]:-
- *application*: フィルタリング対象とするアプリケーション、またはカテゴリー
 - [設定値]:
 - アプリケーションを表すニーモニック
 - "@" で始まるカテゴリーをあらわすニーモニック
 - 上記文字列をカンマで区切った並び (10 個以内、アプリケーションとカテゴリーの混在が可能)
 - 省略時は 1 つの * と同じ
 - [初期値]:-
- *group_num*: グループ ID
 - [設定値]: **dpi group set** コマンドでグループ化したアプリケーションのグループ ID
 - [初期値]:-

[説明]

DPI で使用する IPv6 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 **ipv6 interface dpi filter** コマンドと組み合わせて利用することで、特定アプリケーションのパケットのフィルタリングをすることができる。

アプリケーションを表すニーモニックには、**show dpi application** コマンドで表示されるものを使用する。またカテゴリーを表すニーモニックには、**show dpi category** コマンドで表示されるものを使用する。

[ノート]

アプリケーションの識別が完了していないパケットは、フィルタの設定によらず必ず通過する。また、DPI のアクティベーション中でアプリケーションの識別結果が得られない場合には、すべてのパケットは **dpi use** コマンドの *reject* の設定に従う。

RTX830 は Rev.15.02.13 以降で使用可能。

[設定例]

IPv6 による FTP サーバーへのアクセスは禁止する

```
# ipv6 dpi filter 1 reject * * ftp,ftp_data
# ipv6 dpi filter 100 pass * *
# ipv6 lan2 dpi filter out 1 100
```

[適用モデル]

RTX830

57.4 DPI のフィルターのインターフェースへの適用

[書式]

```

ip interface dpi filter direction filter_list...
ipv6 interface dpi filter direction filter_list...
ip pp dpi filter direction filter_list...
ipv6 pp dpi filter direction filter_list...
ip tunnel dpi filter direction filter_list...
ipv6 tunnel dpi filter direction filter_list...
no ip interface dpi filter direction [filter_list...]
no ipv6 interface dpi filter direction [filter_list...]
no ip pp dpi filter direction [filter_list...]
no ipv6 pp dpi filter direction [filter_list...]
no ip tunnel dpi filter direction [filter_list...]
no ipv6 tunnel dpi filter direction [filter_list...]

```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN 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
 - [初期値]: -
- *direction*

- [設定値]:

設定値	説明
in	受信したパケットに対するフィルタリング
out	送信したパケットに対するフィルタリング

- [初期値]: -
- *filter_list*
 - [設定値]: 空白で区切られた静的フィルタ番号の並び (最大 128 個以内)
 - [初期値]: -

[説明]

ip dpi filter コマンド、および **ipv6 dpi filter** コマンドによるフィルターを組み合わせ、インターフェースで送受信するパケットの種類を制限する。

送信/受信のそれぞれの方向に対して、適用するフィルター列をフィルター番号で指定する。指定された番号のフィルターが順番に適用され、パケットにマッチするフィルターが見つければそのフィルターにより通過/破棄が決定する。それ以降のフィルターは調べられない。すべてのフィルターにマッチしないパケットは破棄される。

[ノート]

RTX830 は Rev.15.02.13 以降で使用可能。

[設定例]

- 192.168.200.0/24 のネットワークに属する端末で、指定のファイル共有ソフトと、ゲームカテゴリーに属するアプリケーションを禁止する

```

# dpi group set 1000 name=file-sharing winmx winny share bittorrent
# ip dpi filter 1 reject 192.168.200.0/24 * 1000
# ip dpi filter 2 reject 192.168.200.0/24 * @game
# ip dpi filter 100 pass * *
# pp select 1
# ip pp dpi filter out 1 2 100

```

[適用モデル]

RTX830

57.5 DPI のアプリケーショングループの作成

[書式]

```
dpi group set group_num [name=name] application_list...
no dpi group set group_num [[name=name] application_list...]
```

[設定値及び初期値]

- *group_num*
 - [設定値]: グループ ID (1..2147483647)
 - [初期値]: -
- *name*
 - [設定値]: グループ名 (最大 32 文字以内)
 - [初期値]: -
- *application_list*
 - [設定値]: アプリケーション、およびカテゴリーの並び(空白区切り、最大 128 個以内)
 - [初期値]: -

[説明]

DPI のアプリケーションのグループを作成する。本コマンドで作成したグループは、以下の各コマンドで `group` キーワードに続いて指定することができる。

- **ip dpi filter**
- **ipv6 dpi filter**
- **queue class filter**

application_list には、アプリケーションやカテゴリーを表すニーモニックを並べて指定する。

name は、半角英数字、"-"(ハイフン)、および"_"(アンダースコア)で、最大 32 文字以内で指定する。グループはルーターの揮発性メモリが許す限り作成することができる。

[ノート]

RTX830 は Rev.15.02.13 以降で使用可能。

[設定例]

- 音楽ストリーミングアプリケーションを禁止する

```
# dpi group set 1000 name=music-streaming spotify google_play_music apple_music
amazon_music
# ip dpi filter 1 reject 1000
# ip dpi filter 100 pass * *
# ip lan2 dpi filter out 1 100
```

[適用モデル]

RTX830

57.6 シグネチャーのダウンロードの手動実行

[書式]

```
dpi signature download go [no-confirm [prompt]] [force]
```

[設定値及び初期値]

- `no-confirm`: 更新可能なシグネチャーが存在するときに、シグネチャーの更新を行うか否かを確認しない
 - [初期値]: -
- `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
 - [初期値]: -
- `force`: 新しいシグネチャーの有無のチェックを行わず、強制的にシグネチャーをダウンロードする
 - [初期値]: -

[説明]

DPI のシグネチャーのダウンロードや更新の手動実行をする。

シグネチャーのダウンロードに一度も成功していない状態で本コマンドを実行すると、配布サーバーからシグネチャーのダウンロードを試みる。ダウンロードに成功した場合、シグネチャーが DPI エンジンにロードされて DPI が使用可能な状態になる。

シグネチャーがダウンロードされている状態で本コマンドを実行した場合、配布サーバーに対して新しいシグネチャーの有無のチェックをして、更新可能なシグネチャーが存在すれば「更新しますか？(Y/N)」の確認を求める。「Y」を入力するとダウンロード、およびロードを行う。「N」を入力すると、更新を中止する。更新可能なシグネチャーがなければ、「新しいシグネチャーはありません。」と表示する。

`no-confirm` を指定すると、更新可能なシグネチャーが存在する場合に更新を行うか否かの確認を行わない。`prompt` 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。

`force` を指定した場合には、新しいシグネチャーの有無のチェックを行わず、強制的にシグネチャーをダウンロードする。外部メモリにシグネチャーを保存したい場合に有効である。

新しいシグネチャーの有無のチェックやダウンロードに失敗した場合でも、リトライはしない。

本コマンドは、`dpi use` コマンドが `off` に設定されている場合には実行できない。

[ノート]

シグネチャーのダウンロードや更新は自動で行われるため、通常は本コマンドを実行する必要はない。自動でのダウンロードに失敗したときなどに、直ちにリトライした場合に使用する。

RTX830 は Rev.15.02.13 以降で使用可能。

[適用モデル]
RTX830

57.7 シグネチャーのダウンロード先 URL の設定

[書式]

```
dpi signature download url url
no dpi signature download url [url]
```

[設定値及び初期値]

- *url*
 - [設定値]: シグネチャーを配布している URL を設定する
 - [初期値]: [http://www.rtpro.yamaha.co.jp/signature/rt_dpi_\(機種名\).ysig](http://www.rtpro.yamaha.co.jp/signature/rt_dpi_(機種名).ysig)

[説明]

個別に用意した Web サーバーを用いてシグネチャーを配布する場合に、シグネチャーが置かれている URL を 255 文字以内の半角英数字および半角記号で指定する。ヤマハの配信サーバーからシグネチャーをダウンロードして使用する場合には、本コマンドを設定する必要はない。

シグネチャーのダウンロードには、HTTP または HTTPS を使用できる。入力形式は以下の通りで、Web サーバーのアドレスは FQDN 形式のホスト名、もしくは IPv4 または IPv6 アドレスを指定する。

- `http[s]://(Web サーバーのアドレス):(ポート番号)/(パス名)`

ポート番号は HTTP の場合 80 番以外、HTTPS の場合 433 番以外を使用するときに指定する。

[ノート]

RTX830 は Rev.15.02.13 以降で使用可能。

[適用モデル]
RTX830

57.8 アプリケーションの識別に関するログを出力するか否かの設定

[書式]

```
dpi log switch
no dpi log [switch]
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	出力する
off	出力しない

- [初期値]: off

[説明]

DPI のアプリケーションの識別に関するログを出力するか否かの設定をする。

本コマンドを on に設定すると、アプリケーションの識別結果や識別処理に関するエラー情報を NOTICE レベルのログに出力する。

[ノート]

RTX830 は Rev.15.02.13 以降で使用可能。

[適用モデル]
RTX830

57.9 DPI の統計情報の表示

[書式]

```
show dpi statistics [all]
show dpi statistics application application [detail]
show dpi statistics category category
show dpi statistics address ip_address
```

[設定値及び初期値]

- *application*
 - [設定値]: アプリケーションを表すニーモニック
 - [初期値]: -
- *category*
 - [設定値]: "@"で始まるカテゴリーを表すニーモニック
 - [初期値]: -
- *ip_address*
 - [設定値]: 端末の IPv4 または IPv6 アドレス
 - [初期値]: -

[説明]

DPI の統計情報を表示する。

show dpi statistics コマンドをオプション無しで実行した場合、ルーターを通過するトラフィック全体に対して送信オクテット数と受信オクテット数の合計が上位 11 位以内のアプリケーションの送受信オクテット数と、全体に占める割合の高いものから表示する。all を指定した場合には、11 位以下の"other"にまとめられたアプリケーションの一覧を表示する

application に続いて *application* を指定した場合には、指定のアプリケーションに関する統計情報のみを表示する。*application* には **show dpi application** コマンドで表示されるアプリケーションのニーモニックを指定する。detail を指定した場合、端末ごとの情報も表示する。

category に続いて *category* を指定した場合には、指定のカテゴリーに属するアプリケーションに関する統計情報のみを表示する。*category* には "@" で始まる **show dpi category** コマンドで表示されるカテゴリーのニーモニックを指定する。カテゴリー内のアプリケーションは、アプリケーションのニーモニックを基準に、0-9、a-z の準に表示する。

address に続いて *ip_address* に端末の IPv4 アドレスまたは IPv6 アドレスを指定した場合には、指定した端末の統計情報を表示する。

[ノート]

統計情報を記録できる端末の台数には上限がある。機種別の上限の台数は以下の通り。

機種	上限の台数 (台)
RTX830	512

ルーターの揮発性メモリに記録されている統計情報は、以下の条件でクリアされる。

- ルーターの電源断
- ルーターの再起動
- **dpi use** コマンドを off に設定する、または削除する
- **clear dpi statistics** コマンドの実行

RTX830 は Rev.15.02.13 以降で使用可能。

[表示例]

```
# show dpi statistics
アプリケーション 送受信オクテット数 割合
-----+-----+-----
office365          18,754,987 25%
lync                15,854,347 21%
google_map         11,115,753 14%
facebook           9,835,354 11%
windows_update     6,354,682 8%
twitter            5,854,965 6%
dns                 5,032,886 5%
ftp                 4,258,369 4%
icmp                3,125,784 3%
imap                1,411,955 1%
other               1,923,854 2%
-----+-----+-----
合計                83,522,936 100%

# show dpi statistics application office365 detail
[office365]
                        オクテット数
端末                  送信          受信
-----+-----+-----
Total                  88,258        131,564
 192.168.0.15          11,254         10,223
 192.168.0.68          48,256         58,825
      :
      :

# show dpi statistics category @game
[@game]
                        オクテット数
アプリケーション    送信          受信
-----+-----+-----
akinator                456           1,675
all_slots_casino        11,254         10,223
      :
      :

# show dpi statistics address 192.168.0.15
[192.168.0.15]
                        オクテット数
アプリケーション    送信          受信
-----+-----+-----
lync                    32,645         1,556,998
office365                546           665,320
      :
      :
```

[適用モデル]
RTX830

57.10 DPI の統計情報のクリア

[書式]

clear dpi statistics

[説明]

ルーターの揮発性メモリに保存された DPI の統計情報をクリアする。
本コマンドを実行しても、外部メモリに記録された統計情報が削除されることはない。

[ノート]

RTX830 は Rev.15.02.13 以降で使用可能。

[適用モデル]

RTX830

57.11 識別結果のキャッシュの表示

[書式]

show dpi cache

[説明]

アプリケーションの識別結果のキャッシュを IPv4/IPv6 アドレスに分けて、0-9、a-z の順に表示する。TTL は分'秒" のフォーマットで表示する。

[ノート]

RTX830 は Rev.15.02.15 以降で使用可能。

[表示例]

```
# show dpi cache
エントリー数: 6
アプリケーション名      宛先 IP アドレス      ポート  TTL
-----+-----+-----+-----+
microsoft                203.0.113.254          443    58'41"
ntp                       203.0.113.110          123    51'38"
office365                 203.0.113.31           443     6'25"
microsoft                 2001:0db8:09ec:a541:20f7:3ba8:2808:bfd5 443    52'34"
ntp                       2001:0db8:e201:bc01:2951:c821:ba11:bbdd 123    12'56"
pokemon_go                2001:0db8:02c1:1bbb:5489:cde9:0001:ac19 443     2'12"
```

[適用モデル]

RTX830

57.12 識別結果のキャッシュのクリア

[書式]

clear dpi cache

[説明]

アプリケーションの識別結果のキャッシュをクリアする。

[ノート]

RTX830 は Rev.15.02.15 以降で使用可能。

[適用モデル]

RTX830

57.13 アプリケーションを表すニーモニック一覧の表示

[書式]

show dpi application [*category*]

show dpi application detail [*category*]

[設定値及び初期値]

- *category*

- [設定値]: "@で始まるカテゴリーを表すニーモニック
- [初期値]:-
- detail: ニーモニックに加えて、アプリケーションの詳細情報を表示する
- [初期値]:-

[説明]

ip dpi filter コマンド、**ipv6 dpi filter** コマンド、および、**queue class filter** コマンドで指定可能なアプリケーションを表すニーモニック一覧を 0-9、a-z の順に表示する。

category を指定した場合には、該当カテゴリーに属するアプリケーションを表すニーモニックのみを表示する。*category* には、**show dpi category** コマンドで表示される "@" で始まるニーモニックを指定する。*detail* キーワードを指定した場合には、アプリケーションの詳細情報を表示する。

[ノート]

RTX830 は Rev.15.02.13 以降で使用可能。

[表示例]

```
# show dpi application
01net          050plus          0zz0          10050net
10086cn       104com           1111tw        1141a
115com        118114cn         11st          123people
1337x         139mail          15min         163com
17173com      17u              20min         24h
24ora         24sata           24ur          2ch
2shared       3366_com         360buy        360cn
3gpp_li       3pc              4399com       4chan
4shared       4tube            51_com        51_com_bbs
51_com_music  51_com_posting   51job         51la
---つづく---
```

```
# show dpi application detail @game
ニーモニック      説明
```

```
-----+-----
akinator          Akinator the Genie
all_slots_casino  All Slots Casino
angry_birds       Angry Birds
aniping           Anipang
battlenet         battlenet
bf1               Battlefield 1
bf4               Battlefield 4
bitstrips         BitStrips
candy_crush_saga  Candy Crush Saga
champion_football Champion Football
---つづく---
```

[適用モデル]

RTX830

57.14 カテゴリーを表すニーモニック一覧の表示**[書式]**

```
show dpi category
show dpi category detail
```

[設定値及び初期値]

- detail: ニーモニックに加えて、カテゴリーの詳細情報を表示する
- [初期値]:-

[説明]

ip dpi filter コマンド、**ipv6 dpi filter** コマンド、および、**queue class filter** コマンドで指定可能なカテゴリーを表すニーモニック一覧を 0-9、a-z の順に、先頭に "@" を付加して表示する。

detail キーワードを指定した場合には、ニーモニックに加えてカテゴリーの詳細情報を表示する。

[ノート]

RTX830 は Rev.15.02.13 以降で使用可能。

[表示例]

```
# show dpi category
@antivirus          @app_service          @audio_video          @authentication
@behavioral         @compression          @database             @encrypted
@erp                @file_server          @file_transfer       @forum
@game              @instant_messaging    @mail                 @microsoft_office
@middleware         @network_management   @network_service     @peer_to_peer
@printer           @routing              @security_service    @standard
@telephony         @terminal             @thin_client         @tunneling
@wap               @web                  @webmail

# show dpi category detail
ニーモニック      詳細
-----+-----
@antivirus        Antivirus update
@app_service       Background service
@audio_video      Application/Protocol used to transport audio or video content
@authentication   Protocol used for authentication purposes
@behavioral       Protocol classified by non-deterministic criteria based on
statistical analysis of packet form and session behavior.
@compression      Compression layers
@database         Protocol used for database remote queries
@encrypted        Encryption protocol
@erp              Enterprise Resource Planning application
@file_server      File transfer protocol
---つづく---
```

[適用モデル]
RTX830

57.15 DPI の動作状態、およびシグネチャーの状態の表示

[書式]

show status dpi

[説明]

DPI の動作状態、およびシグネチャーの情報を表示する。

- DPI の状態

表示	説明
無効	DPI の設定は無効である
ライセンス認証中	ライセンス認証中である
シグネチャーのダウンロード中	シグネチャーをダウンロードしている
シグネチャーの読み込み中	シグネチャーを読み込んでいる
正常動作中	DPI は正常に動作している
停止処理中	DPI の停止処理をしている
ライセンス認証失敗	ライセンス認証に失敗して停止している、ライセンス認証の成功を待っている
シグネチャーのダウンロード失敗 (リトライ待ち)	シグネチャーのダウンロードに失敗し、リトライを待っている
異常停止中 (理由)	エラーが発生し、DPI は停止している(括弧内には異常理由を表示)

- シグネチャー情報
 - バージョン：シグネチャーのバージョン情報
 - ダウンロード日時：現在使用中のシグネチャーをダウンロードした日時

- 外部メモリのシグネチャーを使用している場合には"外部メモリのシグネチャーを使用中"と表示する
- 最終更新チェック日時：最後にシグネチャーの更新チェックを行った日時
- 保存先：ダウンロードしたシグネチャーの外部メモリ上の保存先
- 保存しない場合には "-" を表示する

[ノート]

RTX830 は Rev.15.02.13 以降で使用可能。

[表示例]

```
# show status dpi
現在の状態
  正常動作中
シグネチャーの情報
  バージョン           Ver. 1.0.6
  最終ダウンロード日時  外部メモリのシグネチャーを使用中
  最終更新チェック日時  2019/10/13 09:14:25
  保存先                usb1:/signature/rt_dpi_rtx830.ysig
```

[適用モデル]

RTX830

第 58 章

ダッシュボード

58.1 ダッシュボードのデータを蓄積するか否かの設定

[書式]

```
dashboard accumulate type sw  
no dashboard accumulate type [sw]
```

[設定値及び初期値]

- *type* : ガジェットの種類別
 - [設定値] :

設定値	説明
traffic	トラフィック情報
nat	NATセッション数

- [初期値] : -
- *sw*

- [設定値] :

設定値	説明
on	データを蓄積する
off	データを蓄積しない

- [初期値] : off

[説明]

Web GUI のダッシュボードのガジェットで使用するデータを蓄積するか否かを設定する。なお、ダッシュボードで *type* で示されるガジェットを追加すると自動的に本コマンドの設定が on となる。

[ノート]

RTX1210 は Rev.14.01.34 以降で使用不可。
RTX830 は Rev.15.02.10 以降で使用不可。
代わりに **statistics** コマンドを使用することができる。

[適用モデル]

RTX1210, RTX830

第 59 章

操作

59.1 相手先情報番号の選択

[書式]

```
pp select peer_num
```

```
no pp select
```

[設定値及び初期値]

- peer_num

- [設定値]:

設定値	説明
番号	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

- [初期値]: -

[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 を参照。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- peer_num

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.2 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
```

[設定値及び初期値]

- tunnel_num

- [設定値]:

設定値	説明
番号	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

- [初期値]:-

[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「[IPsec の設定](#)」を参照

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- `tunnel_num`

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

59.3 設定に関する操作

59.3.1 管理ユーザへの移行

[書式]

`administrator`

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.3.2 終了

[書式]

`quit`
`quit save`
`exit`
`exit save`

[設定値及び初期値]

- `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
- [初期値]:-

[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、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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.3.3 設定内容の保存

[書式]

save *[filename [comment]]*

[設定値及び初期値]

- *filename* : 設定を保存するファイル名
 - [設定値] :

設定値	説明
0~4	内蔵フラッシュ ROM の設定ファイル番号
usb1: <i>filename</i>	USB メモリ内の設定ファイル名
sd1: <i>filename</i>	microSD カード内の設定ファイル名

- [初期値] : -
- *comment*
 - [設定値] : 設定ファイルのコメント (半角 200 文字以内)
 - [初期値] : -

[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。

[ノート]

SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降、および、Rev.11.01 系以降では、*filename* は半角 99 文字以内。
上記以外の機種では、*filename* は半角 64 文字以内。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.3.4 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*]

[設定値及び初期値]

- *from* : コピー元ファイル名
 - [設定値] :

設定値	説明
0~4.2	内蔵フラッシュ ROM の設定ファイル番号
usb1: <i>filename</i>	USB メモリ内の設定ファイル名
sd1: <i>filename</i>	microSD カード内の設定ファイル名
*: <i>filename</i>	USB メモリおよび microSD カード内の設定ファイル名
emfs: <i>filename</i>	EMFS 内の設定ファイル名

- [初期値] : -
- *to* : コピー先ファイル名
 - [設定値] :

設定値	説明
0~4	内蔵フラッシュ ROM の設定ファイル番号

設定値	説明
usb1:filename	USB メモリ内の設定ファイル名、 <i>filename</i> は半角 64 文字以内
sd1:filename	microSD カード内の設定ファイル名、 <i>filename</i> は半角 64 文字以内

- [初期値]: -
- *crypto*: 暗号アルゴリズムの選択
- [設定値]:

設定値	説明
aes128	AES128 で暗号化する。
aes256	AES256 で暗号化する。

- [初期値]: -
- *password*
 - [設定値]: 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)
 - [初期値]: -

[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 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。

CRYPTO を指定した場合、設定ファイルを暗号化してから外部メモリにコピーする。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。復号するときの暗号アルゴリズムは自動的に判別するので、復号時には暗号アルゴリズムを指定する必要はない。

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。

外部メモリに暗号化して保存したファイルは、PC 上で RT-FileGuard を使用して復号することができる。

SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降、および、Rev.11.01 系以降では、*filename* は半角 99 文字以内。上記以外の機種では、*filename* は半角 64 文字以内。

EMFS 内のファイルは RTX5000、RTX3500 Rev.14.00.26 以降、RTX1210 Rev.14.01.28 以降、および RTX830 Rev.15.02.03 以降、RTX1220 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.3.5 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`

[設定値及び初期値]

- *from* : コピー元ファイル名
- [設定値]:

設定値	説明
番号	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 (RTX830、RTX810、SRT100 以外の機種で指定可能)、0 のみ指定可
<i>usb1:filename</i>	USB メモリ内のファームウェアファイル名 (USB インタフェースを持つ機種のみ)
<i>sd1:filename</i>	microSD カード内のファームウェアファイル名 (microSD インタフェースを持つ機種のみ)
<i>*:filename</i>	USB メモリおよび microSD カード内のファームウェアファイル名

- [初期値]: -
- *to* : コピー先ファイル名
- [設定値]:

設定値	説明
番号	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。(RTX5000、RTX3500、RTX1220、RTX1210、RTX1200 では 0、1 が指定可、RTX830、RTX810、SRT100 では 0 のみ指定可、左記以外の機種では 1 のみ指定可)

- [初期値]: -

[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 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。

SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアでは、*filename* は半角 99 文字以内。

上記以外の機種では、*filename* は半角 64 文字以内。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, SRT100

59.3.6 設定ファイルの削除

[書式]

delete config filename

[設定値及び初期値]

- *filename* : 削除するファイル名

- [設定値] :

設定値	説明
all	内蔵フラッシュ ROM の全ての設定ファイル
0~4.2	内蔵フラッシュ ROM の設定ファイル番号

- [初期値] :-

[説明]

保存されている設定ファイルを削除する。

[ノート]

all は Rev.11.01 系以降のファームウェアで指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.3.7 実行形式ファームウェアファイルの削除

[書式]

delete exec filename

[設定値及び初期値]

- *filename* : 削除するファイル名

- [設定値] :

設定値	説明
番号	実行形式ファームウェアファイル番号 (1 のみ指定可能)

- [初期値] :-

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RT250i

59.3.8 PKI ファイルの削除

[書式]

delete pki file type file

[設定値及び初期値]• *type*

- [設定値]:

設定値	説明
certificate	証明書ファイル
client	CRL ファイル

- [初期値]: -

• *file*

- [設定値]: 内蔵フラッシュ ROM の証明書ファイル番号(0..1)、または CRL ファイル番号(0..1)
- [初期値]: -

[説明]

指定した PKI ファイルを削除する。

証明書ファイル番号、および CRL ファイル番号は **show file list internal** コマンドで確認できる。

[ノート]

RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]

RTX3000

59.3.9 デフォルト設定ファイルの設定

[書式]

set-default-config *filename*

[設定値及び初期値]• *filename*

- [設定値]: 設定ファイル番号 (0..4.2)
- [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.3.10 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*

[設定値及び初期値]• *filename*

- [設定値]: 実行形式ファームウェアファイル番号 (0..1)
- [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RT250i

59.3.11 シリアルポートのボーレートの設定

[書式]

set-serial-baudrate *rate*

[設定値及び初期値]

- *rate*
 - [設定値]: ボーレート (9600 / 19200 / 38400 / 57600 / 115200)
 - [初期値]: 9600

[説明]

シリアルポートのボーレートを設定する。

[適用モデル]

RTX1220, RTX1210, RTX830

59.3.12 設定の初期化

[書式]

cold start

[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]

内蔵フラッシュ 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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.3.13 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*

[設定値及び初期値]

- *interface*: インタフェース名
 - [設定値]:
 - BRI インタフェース名
 - PRI インタフェース名
 - [初期値]: -
- *number*
 - [設定値]: ISDN 番号
 - [初期値]: -
- *sub_address*
 - [設定値]: ISDN サブアドレス (0x21 から 0x7e の ASCII 文字列)
 - [初期値]: -
- *dlci*
 - [設定値]: フレームリレーの DLCI 番号
 - [初期値]: -
- *type*: リモートセットアップの方式
 - [設定値]:

設定値	説明
retransmission	データの欠落に対応できる方式

- [初期値]: -

[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` は RT250i では指定できない。

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

59.3.14 遠隔地のルーターからの設定に対する制限

[書式]

```
remote setup accept tel_num [tel_num_list]
remote setup accept any
remote setup accept none
no remote setup accept
```

[設定値及び初期値]

- `tel_num`
 - [設定値]: 電話番号
 - [初期値]: -
- `tel_num_list`
 - [設定値]: 電話番号を空白で区切った並び
 - [初期値]: -
- `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
 - [初期値]: `any`
- `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
 - [初期値]: -

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, SRT100

59.4 動的情報のクリア操作

59.4.1 アカウントのクリア

[書式]

```
clear account
clear account interface
```

[設定値及び初期値]

- `interface`
 - [設定値]:
 - BRI インタフェース名
 - PRI インタフェース名
 - [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i

59.4.2 PP アカウントのクリア

[書式]

clear account pp [*peer_num*]

[設定値及び初期値]

- *peer_num*
 - [設定値]:
 - 相手先情報番号
 - 省略時は現在選択している相手先
 - [初期値]: -

[説明]

指定した PP インタフェースに関するアカウントをクリアする。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i

59.4.3 TUNNEL アカウントのクリア

[書式]

clear account tunnel [*tunnel_num*]

[設定値及び初期値]

- *tunnel_num*
 - [設定値]:
 - 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する
 - [初期値]: -

[説明]

指定したデータコネクタ接続設定がされているトンネルインタフェースに関するアカウントをクリアする。

[ノート]

RTX3000 は Rev.9.00.56 以降で使用可能。

RTX1200 は Rev.10.01.36 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200

59.4.4 携帯電話回線のアカウントのクリア

[書式]

clear account mobile

[説明]

携帯電話回線に関するアカウントをクリアする。

[適用モデル]

RTX830, RTX810

59.4.5 データコネクタのアカウントのクリア

[書式]

clear account ngn data

[説明]

データコネクトのアカウントをクリアする。

[ノート]

RTX3000 は Rev.9.00.56 以降で使用可能。

RTX1200 は Rev.10.01.36 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

59.4.6 ARP テーブルのクリア

[書式]

```
clear arp
```

[説明]

ARP テーブルをクリアする。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.4.7 IP の動的経路情報のクリア

[書式]

```
clear ip dynamic routing
```

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.4.8 ブリッジのラーニング情報のクリア

[書式]

```
clear bridge learning bridge_interface
```

[設定値及び初期値]

- *bridge_interface*
 - [設定値]: ブリッジインタフェース名
 - [初期値]: -

[説明]

動的に受け取ったブリッジのラーニング情報をすべて消去する。

[ノート]

静的に設定した登録情報は消去されない。

RTX5000 は Rev.14.00.12 以降で使用可能。

RTX3500 は Rev.14.00.12 以降で使用可能。

RTX810 は Rev.11.01.21 以降で使用可能。

RTX1200 は Rev.10.01.53 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

59.4.9 ログのクリア

[書式]

```
clear log [saved]
```

[設定値及び初期値]

- saved
 - [設定値]: リブート直前のログをクリアする
 - [初期値]: -

[説明]

ログをクリアする。

[ノート]

saved オプションは RTX1200 Rev.10.01.71 以降、RTX810 Rev.11.01.28 以降、RTX5000 / RTX3500 Rev.14.00.18 以降、RTX1210 Rev.14.01.11 以降のファームウェア、および、Rev.15.02 系以降のすべてのファームウェアで指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.4.10 InARP のクリア

[書式]

clear inarp

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

59.4.11 DNS キャッシュのクリア

[書式]

clear dns cache

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.4.12 インタフェースのカウンター情報のクリア

[書式]

clear status interface

clear status pp peer_num

clear status tunnel tunnel_num

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名、ブリッジインタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -

[説明]

指定したインタフェースのカウンター情報をクリアする。

[ノート]

モバイルインターネット機能で使用されるインタフェースの累積受信、累積送信、累計エラーは、発信制限に関する操作が行われないようにするためにクリアしない。これらの累積のカウンタ情報は、**clear mobile access limitation** コマンドを使用することでクリアできる。

RTX1200 は Rev.10.01.36 以降で使用可能。

RTX810 は Rev.11.01.06 以降で使用可能。

ブリッジインタフェースは RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

WAN インタフェースは RTX1200 Rev.10.01.42 以降のファームウェア、および、RTX1220、RTX1210、RTX830 で指定可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

59.4.13 PRI のステータス情報のクリア**[書式]**

clear pri status pri

[設定値及び初期値]

- *pri*
 - [設定値]: PRI 番号 (1..2)
 - [初期値]: -

[説明]

PRI のステータス情報をクリアする。

[適用モデル]

RTX5000, RTX3500, RTX3000, RT250i

59.4.14 NAT アドレステーブルのクリア**[書式]**

clear nat descriptor dynamic nat_descriptor

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]:

設定値	説明
1..2147483647	NAT ディスクリプタ番号
all	すべての NAT ディスクリプタ番号

- [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.4.15 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]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]:
 - 相手先情報番号
 - anonymous
 - 省略時は現在選択している相手先
 - [初期値]: -
- *tunnel_num*
 - [設定値]:
 - 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
 - [初期値]: -

[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。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.4.16 IP マスカレードで管理しているセッションの統計情報のクリア**[書式]**

```
clear nat descriptor masquerade session statistics [nat_descriptor]
```

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]:

- 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統計情報のクリアを行う。
- [初期値]:-

[説明]

IP マスカレードで管理しているセッションの統計情報をクリアする。

[ノート]

RTX5000 / RTX3500 Rev.14.00.32 以降、RTX1210 は Rev.14.01.33 以降、RTX830 は Rev.15.02.09 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

59.4.17 PPPoE パススルー機能がラーニングした情報のクリア

[書式]

```
clear pppoe pass-through learning
```

[説明]

PPPoE パススルー機能がラーニングした情報を消去する。

[ノート]

本コマンドを実行しても PPPoE のセッションが切れることはない。

RTX830 は Rev.15.02.03 以降で使用可能。

RTX1210 は Rev.14.01.26 以降で使用可能。

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

59.4.18 IPv6 の動的経路情報の消去

[書式]

```
clear ipv6 dynamic routing
```

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.4.19 近隣キャッシュの消去

[書式]

```
clear ipv6 neighbor cache [interface]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]:-

[説明]

近隣キャッシュを消去する。

interface を指定した場合、そのインタフェース経由で得られた近隣キャッシュのみ消去する。

[ノート]

interface は、RTX5000、RTX3500 は Rev.14.00.32 以降、RTX1210 は Rev.14.01.40 以降、RTX830 は Rev.15.02.20 以降、RTX1220 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.4.20 起動情報の履歴を削除する

[書式]

```
clear boot list
```

[説明]

起動情報の履歴を削除する。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

59.4.21 外部メモリに保存された SYSLOG のクリアとバックアップファイルの削除

[書式]

```
clear external-memory syslog
```

[説明]

外部メモリに保存された現在書き込み中の SYSLOG ファイル内のログのクリアとすべての SYSLOG のバックアップファイルの削除を行う。

削除の対象となる SYSLOG のバックアップファイルは、**external-memory syslog filename** コマンドで指定されたパス内に存在するファイルが対象となる。

なお、本コマンドは、**external-memory syslog filename** コマンドで SYSLOG ファイル名が設定されており、かつ、指定された外部ストレージインタフェースに外部メモリが接続されている場合にのみ動作する。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830, RTX810

59.5 ファイル、ディレクトリの操作

59.5.1 ディレクトリの作成

[書式]

```
make directory path
```

[設定値及び初期値]

- *path*
 - [設定値]: 相対パスまたは絶対パス
 - [初期値]: -

[説明]

指定した名前のディレクトリを作成する。

path に相対パスを指定した場合、環境変数 PWD を基点としたパスと解釈される。PWD は **set** コマンドで変更可能であり、初期値は "/" である。

[ノート]

SRT100 は Rev.10.00.52 以降で使用可能。 RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

59.5.2 ファイルまたはディレクトリの削除

[書式]

```
delete path
```

[設定値及び初期値]

- *path*
 - [設定値]: 相対パスまたは絶対パス
 - [初期値]: -

[説明]

指定したファイルまたはディレクトリを削除する。

ディレクトリが空でない場合は配下のファイルとディレクトリも同時に削除される。

path に相対パスを指定した場合、環境変数 `PWD` を基点としたパスと解釈される。`PWD` は `set` コマンドで変更可能であり、初期値は `"/"` である。

[ノート]

path に相対パスで `"config"` または `"exec"` を指定した場合、本コマンドではなく、`delete config` コマンドまたは `delete exec` コマンドが実行される。このような場合には相対パスを使用せず、絶対パスでファイルまたはディレクトリを指定する。

SRT100 は Rev.10.00.52 以降で使用可能。 RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

59.5.3 ファイルまたはディレクトリの複製

[書式]

`copy from to`

[設定値及び初期値]

- *from*
 - [設定値]: コピー元のファイル名またはディレクトリ名
 - [初期値]: -
- *to*
 - [設定値]: コピー先のファイル名またはディレクトリ名
 - [初期値]: -

[説明]

ファイルまたはディレクトリを複製する。*from* がディレクトリの場合は、配下のすべてのファイルとディレクトリが再帰的に複製される。

from と *to* は、それぞれ相対パスまたは絶対パスで指定する。

from がファイルの場合の動作は以下の通りとなる。

to と同名のファイルが存在する場合は *to* のデータが *from* のデータで上書きされる。

to と同名のディレクトリが存在する場合は、そのディレクトリの配下に *from* と同名のファイルが作成される。

to と同名のファイルやディレクトリが存在しない場合には *to* が作成される。

from がディレクトリの場合の動作は以下の通りとなる。

to と同名のファイルが存在する場合は複製を実行できない。

to と同名のディレクトリが存在する場合は、そのディレクトリの配下に *from* と同名のディレクトリが作成される。

to と同名のファイルやディレクトリが存在しない場合には *to* が作成される。

from、*to* に相対パスを指定した場合、環境変数 `PWD` を基点としたパスと解釈される。`PWD` は `set` コマンドで変更可能であり、初期値は `"/"` である。

[ノート]

from に相対パスで `"config"` または `"exec"` を指定した場合、本コマンドではなく、`copy config` コマンドまたは `copy exec` コマンドが実行される。このような場合には相対パスを使用せず、絶対パスでファイルまたはディレクトリを指定する。

本コマンドでは、必要に応じた親ディレクトリ作成が行われなため、*to* のパス中に存在しないディレクトリが含まれているとエラーになる。

SRT100 は Rev.10.00.52 以降で使用可能。 RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

59.5.4 ファイル名またはディレクトリ名の変更

[書式]

```
rename path name
```

[設定値及び初期値]

- *path*
 - [設定値]: 変更対象のファイルまたはディレクトリの相対パスまたは絶対パス
 - [初期値]: -
- *name*
 - [設定値]: 変更後の名前
 - [初期値]: -

[説明]

指定したファイルまたはディレクトリの名前を変更する。

path に相対パスを指定した場合、環境変数 PWD を基点としたパスと解釈される。PWD は **set** コマンドで変更可能であり、初期値は "/" である。

[ノート]

name パラメータに新しい名前を指定する場合、スラッシュ "/" を含む名前を指定することはできない。

SRT100 は Rev.10.00.52 以降で使用可能。 RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

59.6 その他の操作

59.6.1 相手先の使用許可の設定

[書式]

```
pp enable peer_num [peer_num ...]
```

```
no pp enable peer_num
```

[設定値及び初期値]

- *peer_num*
 - [設定値]:

設定値	説明
番号	相手先情報番号
番号 1-番号 2	番号 1 から番号 2 までの相手先情報番号
番号 1-	番号 1 以上のすべての相手先情報番号
-番号 1	番号 1 以下のすべての相手先情報番号
anonymous	anonymous インターフェース
all	すべての相手先情報番号

- [初期値]: -

[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。

複数指定した場合には、その全てで使用できる状態になる。複数指定は、RTX1200 Rev.10.01.75 以降、RTX810 Rev.11.01.31 以降、RTX5000 / RTX3500 Rev.14.00.26 以降、RTX1210 Rev.14.01.26 以降、RTX830 Rev.15.02.03 以降、RTX1220 で使用可能。

[ノート]

必ず、1. **pp disable**、2. **disconnect**、3. **pp** の設定変更、4. **pp enable**、5. **connect** の手順を踏んで設定を変更する。

pp enable コマンドを実行すると内部情報の初期化が行われる。pp の設定変更の有無に関わらず、pp が接続中に **pp enable** を実行すると、内部情報の初期化により、pp に紐付けられている tunnel 等が切断される場合がある。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.6.2 相手先の使用不許可の設定

[書式]

pp disable *peer_num* [*peer_num* ...]

[設定値及び初期値]

- *peer_num*
- [設定値]:

設定値	説明
番号	相手先情報番号
番号 1-番号 2	番号 1 から番号 2 までの相手先情報番号
番号 1-	番号 1 以上のすべての相手先情報番号
-番号 1	番号 1 以下のすべての相手先情報番号
anonymous	anonymous インターフェース
all	すべての相手先情報番号

- [初期値]:-

[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。

複数指定した場合には、その全てで使用できない状態になる。複数指定は、RTX1200 Rev.10.01.75 以降、RTX810 Rev.11.01.31 以降、RTX5000 / RTX3500 Rev.14.00.26 以降、RTX1210 Rev.14.01.26 以降、RTX830 Rev.15.02.03 以降、RTX1220 で使用可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.6.3 再起動

[書式]

restart [*binary* [*config*]]

restart [*config*]

[設定値及び初期値]

- *binary*

- [設定値]: 実行形式ファームウェアファイル番号 (0~1)
- [初期値]: -
- *config*
 - [設定値]: 内蔵フラッシュ ROM の設定ファイル番号 (0~4.2)
 - [初期値]: -

[説明]

ルーターを再起動する。
 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。
binary は、デフォルトファームウェアファイルに設定される。
config は、デフォルト設定ファイルに設定される。

[ノート]

RTX830、RTX810、RT107e、SRT100 では第 2 書式のみ使用可能。
 上記以外の機種では第 1 書式のみ使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.6.4 インタフェースの再起動

[書式]

```
interface reset interface [interface ...]
```

[設定値及び初期値]

- *interface*
 - [設定値]:
 - LAN インタフェース名
 - WAN 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
 - USB インタフェース名
 - SD インタフェース名
 - [初期値]: -

[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 インタフェースを使用中に回線種別を **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。
 BRI と PRI インタフェースで、MP を使用している場合には、**interface reset pp** コマンドを使用する。
 USB と SD インタフェースでは、ポートの給電が OFF,ON され、USB デバイスや microSD カードの再アタッチが行われる。

[ノート]

RTX5000、RTX3500、RTX1200 は、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。

RTX3000、RTX1220、RTX1210 は、このコマンドを実行すると、指定の lan インタフェースのみがリセットされる。
 RTX1500、RTX1100 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。lan3 に対してこのコマンドを実行すると、lan3 インタフェースのみがリセットされる。

RTX830、RTX810、RT107e、SRT100 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。

RT250i は、このコマンドを実行すると、lan1 インタフェースがリセットされる。

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。WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

USB インタフェースは RTX1200 Rev.10.01.65 以降、RTX810 Rev.11.01.25 以降、RTX1210 Rev.14.01.09 以降のファームウェア、および、Rev.15.02 系以降のすべてのファームウェアで指定可能。

SD インタフェースは RTX1200 Rev.10.01.65 以降、RTX810 Rev.11.01.25 以降、RTX5000 / RTX3500 Rev.14.00.18 以降、RTX1210 Rev.14.01.09 以降のファームウェア、および、Rev.15.02 系以降のすべてのファームウェアで指定可能。

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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.6.5 PP インタフェースの再起動

[書式]

```
interface reset pp [peer_num]
```

[設定値及び初期値]

- *peer_num*
 - [設定値]:
 - 相手先情報番号
 - anonymous
 - [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1210, RTX1200, RTX1100, RT250i

59.6.6 発信

[書式]

```
connect interface
```

```
connect peer_num
```

```
connect pp peer_num
```

```
connect tunnel tunnel_num
```

[設定値及び初期値]

- *interface*
 - [設定値]: WAN インタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]: 発信相手の相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: NGN 網を介したトンネル番号または L2TPv3 トンネル番号
 - [初期値]: -

[説明]

手動で発信する。

[ノート]

connect tunnel コマンドは、データコネクトを使用した拠点間接続以外のトンネルには使用できない。

データコネクタ接続機能を実装していないモデルでは、**connect pp** コマンドは使用できない。
 データコネクタ接続機能と L2TPv3 機能を実装していないモデルでは、**connect tunnel** コマンドは使用できない。
 WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、
 RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.6.7 切断

[書式]

```
disconnect interface
disconnect peer_num
disconnect pp peer_num
disconnect tunnel tunnel_num
```

[設定値及び初期値]

- *interface*
 - [設定値]: WAN インタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]:

設定値	説明
番号	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
anonymous1 ..	指定した anonymous

- [初期値]: -
- *tunnel_num*
 - [設定値]: NGN 網を介したトンネル番号または L2TPv3 トンネル番号
 - [初期値]: -

[説明]

手動で切断する。

[ノート]

disconnect tunnel コマンドは、データコネクタを使用した拠点間接続以外のトンネルには使用できない。
 データコネクタ接続機能を実装していないモデルでは、**disconnect pp** コマンドは使用できない。
 データコネクタ接続機能と L2TPv3 機能を実装していないモデルでは、**disconnect tunnel** コマンドは使用できない。
 WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、
 RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.6.8 ping

[書式]

ping [-s *datalen*] [-c *count*] [-sa *ip_address*] [-w *wait*] *host*

[設定値及び初期値]

- *datalen* : データ長

- [設定値] :

設定値	説明
1..65535 バイト	Rev.10.01.32 以降
64..65535 バイト	上記以外

- [初期値] : 64

- *count*

- [設定値] : 実行回数 (1..21474836)
- [初期値] : Ctrl+c キーが入力されるまで繰り返す

- *ip_address*

- [設定値] : 始点 IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))
- [初期値] : ルーターのインタフェースに付与されたアドレスの中から選択する

- *wait* : パケット送信間隔秒数

- [設定値] :

設定値	説明
0.1 .. 3600.0	RTX1200 Rev.10.01.59 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.18 以降、RTX1210 Rev.14.01.09 以降、Rev.15.02 系以降
0.1 .. 99.9	上記以外

- [初期値] : 1

- *host*

- [設定値] :
 - 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
- [初期値] : -

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.6.9 ping6 の実行

[書式]

```
ping6 [-s datalen] [-c count] [-sa ipv6_address] [-w wait] destination
ping6 [-s datalen] [-c count] [-sa ipv6_address] [-w wait] destination%scope_id
ping6 [-s datalen] [-c count] [-sa ipv6_address] [-w wait] destination interface
ping6 [-s datalen] [-c count] [-sa ipv6_address] [-w wait] destination pp peer_num
ping6 [-s datalen] [-c count] [-sa ipv6_address] [-w wait] destination tunnel tunnel_num
ping6 destination [count]
ping6 destination%scope_id [count]
ping6 destination interface [count]
ping6 destination pp peer_num [count]
ping6 destination tunnel tunnel_num [count]
```

[設定値及び初期値]

- *datalen*
 - [設定値]: データ長 (1..65535 バイト)
 - [初期値]: 64
- *count*
 - [設定値]: 実行回数 (1..21474836)
 - [初期値]: Ctrl+c キーが入力されるまで繰り返す
- *ipv6_address*
 - [設定値]: 始点 IPv6 アドレス
 - [初期値]: ルーターのインタフェースに付与されたアドレスの中から選択する
- *wait*: パケット送信間隔秒数
 - [設定値]:

設定値	説明
0.1 .. 3600.0	RTX1200 Rev.10.01.59 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.18 以降、RTX1210 Rev.14.01.09 以降、Rev.15.02 系以降
0.1 .. 99.9	上記以外

- [初期値]: 1
- *destination*
 - [設定値]: 送信する宛先の IPv6 アドレス、または名前
 - [初期値]: -
- *scope_id*
 - [設定値]: スコープ識別子
 - [初期値]: -
- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -

[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。

第 1～第 5 書式は、Rev.10.01.32 以降のリビジョンで指定できる。それ以外のリビジョンでは、第 6～第 10 書式で指定する。

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]

-s オプション、-c オプション、-sa オプション、-w オプションは Rev.10.01.32 以降で使用可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.6.10 traceroute**[書式]**

```
traceroute host [noresolv] [-sa source]
```

[設定値及び初期値]

- *host*
 - [設定値]:
 - traceroute をかけるホストの IP アドレス (xxx.xxx.xxx.xxx)
 - traceroute をかけるホストの名称
 - [初期値]: -
- *noresolv*: DNS による解決を行わないことを示すキーワード
 - [初期値]: -
- *source*
 - [設定値]: 始点 IP アドレス
 - [初期値]: -

[説明]

指定したホストまでの経路を調べて表示する。

source パラメータは

RTX1100, RTX1500, RT107e は Rev.8.03.87 以降、

RTX3000 は Rev.9.00.47 以降、

SRT100 は Rev.10.00.49 以降、

RTX1200 は Rev.10.01.16 以降、

RTX810, RTX5000, RTX3500, RTX1210, RTX830, RTX1220

で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.6.11 traceroute6 の実行

[書式]

traceroute6 *destination* [noresolv] [-sa *source*]

[設定値及び初期値]

- *destination*
 - [設定値]: 送信する宛先の IPv6 アドレス、または名前
 - [初期値]: -
- *noresolv*
 - [設定値]: DNS による解決を行わないことを示すキーワード
 - [初期値]: -
- *source*
 - [設定値]: 始点 IP アドレス
 - [初期値]: -

[説明]

指定した宛先までの経路を調べて表示する。

noresolv オプションおよび -sa オプションは RTX5000 / RTX3500 Rev.14.00.26 以降、RTX1210 Rev.14.01.33 以降、RTX830 Rev.15.02.09 以降、RTX1220 で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.6.12 nslookup

[書式]

nslookup *host*

[設定値及び初期値]

- *host*
 - [設定値]:
 - IP アドレス
 - IPv6 アドレス
 - ホスト名
 - [初期値]: -

[説明]

DNS による名前解決を行う。

[ノート]

AAAA レコードと IPv6 アドレスの PTR レコードは、以下の機種およびリビジョンで使用可能。

RTX830 Rev.15.02.09 以降

RTX1210 Rev.14.01.33 以降

RTX5000 / RTX3500 Rev.14.00.26 以降

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.6.13 SIP サーバーに対し手動で接続

[書式]

sip server connect *number*

[設定値及び初期値]

- *number*
 - [設定値]: 登録番号 (1..65535)

- [初期値]:-

[説明]

SIP サーバーに対し手動で接続(サインイン)する。

基本的には自動的に SIP サーバーに接続するので、本コマンドは手動で切断した時や接続されていない状態を確認した時に、接続する場合に使用する。

[ノート]

RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000

59.6.14 SIP サーバーに対し手動で切断

[書式]

sip server disconnect *number*

[設定値及び初期値]

- *number*
 - [設定値]: 登録番号(1..65535)
 - [初期値]:-

[説明]

SIP サーバーに対し手動で切断 (サインアウト) する。

切断後、ルーターを再起動するか手動で接続しない限り SIP サーバーに接続しない。

[ノート]

RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000

59.6.15 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*]

[設定値及び初期値]

- *session_id*
 - [設定値]: セッションの識別子
 - [初期値]:-
- *channel_id*
 - [設定値]: チャネルの識別子
 - [初期値]:-

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e

59.6.16 TELNET クライアント

[書式]

telnet *host* [*port* [*mode* [*negotiation* [*abort*]]]]

[設定値及び初期値]

- *host*
 - [設定値]: TELNET をかける相手の IP アドレス、ホスト名、または NGN 網電話番号
 - [初期値]: -
- *port*: 使用するポート番号
 - [設定値]:
 - 十進数
 - ポート番号のニーモニック
 - 省略時は 23 (TELNET)
 - [初期値]: 23
- *mode*: TELNET 通信 (送信) の動作モード
 - [設定値]:

設定値	説明
character	文字単位で通信する
line	行単位で通信する
auto	<i>port</i> パラメータの設定値により character/line を選択
省略	省略時は auto

- [初期値]: auto
- *negotiation*: TELNET オプションのネゴシエーションの選択
 - [設定値]:

設定値	説明
on	ネゴシエーションする
off	ネゴシエーションしない
auto	<i>port</i> パラメータの設定値により on/off を選択
省略	省略時は auto

- [初期値]: 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
 - [設定値]:
 - 十進数の ASCII コード
 - 省略時は 29(^)
 - [初期値]: 29

[説明]

TELNET クライアントを実行する。

[ノート]

ホスト名による接続は A レコード(IPv4)のみ対応している。

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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

59.6.17 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]
```

[設定値及び初期値]

- *session_id*
 - [設定値]: セッションの識別子
 - [初期値]: -
- *channel_id*
 - [設定値]: チャンネルの識別子
 - [初期値]: -

[説明]

指定したセッションに属する特定のチャンネルを削除する。チャン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ンネルを削除する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e

59.6.18 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]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -

[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。

[適用モデル]

RTX5000, RTX3500, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

59.6.19 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
```

[設定値及び初期値]

- *pri*
 - [設定値]: PRI 番号 (1..2)
 - [初期値]: -
- *a*: ループバック A を示すキーワード
 - [初期値]: -
- *timeslot*: タイムスロットループバックを示すキーワード
 - [初期値]: -
- *data*: 送信データパターン (1..4)
 - [設定値]:

<i>data</i>	擬似ランダムパターン
1	2^6-1

<i>data</i>	擬似ランダムパターン
2	2^7-1
3	2^9-1
4	$2^{11}-1$

- [初期値]: -
- *head*
 - [設定値]: 先頭タイムスロット番号 (1..24)
 - [初期値]: -
- *num*
 - [設定値]: タイムスロット数 (1..24)
 - [初期値]: -

[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ため、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]

RTX5000, RTX3500, RTX3000, RT250i

59.6.20 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
```

[設定値及び初期値]

- *pri*
 - [設定値]: PRI 番号 (1..2)
 - [初期値]: -
- *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
 - [初期値]: -
- *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
 - [初期値]: -
- *timeslot*: タイムスロットループバックを示すキーワード
 - [初期値]: -
- *head*
 - [設定値]: 先頭タイムスロット番号 (1..24)
 - [初期値]: -
- *number*
 - [設定値]: タイムスロット数 (1..24)
 - [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RT250i

59.6.21 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
```

[設定値及び初期値]

- *interval*
 - [設定値]: パケットの送信間隔 (秒)
 - [初期値]: 1
- *count*
 - [設定値]: パケットの送信回数
 - [初期値]: 4
- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *mac_address*
 - [設定値]: MAC アドレス
 - [初期値]: -
- *ip_address*
 - [設定値]: IPv4 アドレス
 - [初期値]: -
- *port*
 - [設定値]: UDP ポート番号
 - [初期値]: -
- *type*
 - [設定値]: イーサネットタイプフィールドの値 (1501..65535)
 - [初期値]: -

[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。SRT100 は、Rev.10.00.31 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, SRT100

59.6.22 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]]

[設定値及び初期値]

- **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
 - [初期値] :-
- **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
 - [初期値] :-

[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ります。

"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 RT107e では指定できない。

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。

[ノート]

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。

RTX1500、RTX1100、RT107e は Rev.8.03.37 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

59.6.23 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]]

[設定値及び初期値]

- **interface** : インタフェース
 - [設定値] :
 - LAN インタフェース (lan1、lan2 など)
 - WAN インタフェース (wan1)
 - 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
 - [初期値] :-
- **id**
 - [設定値] : フィルタの識別子 (1 .. 65535)
 - [初期値] :-

[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。

[ノート]

WAN インタフェースは Rev.10.00.60 以降で指定可能。

[適用モデル]

SRT100

59.6.24 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]
```

[設定値及び初期値]

- *id*
 - [設定値]: フィルタの識別子 (1 .. 65535)
 - [初期値]: -

[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]

SRT100

59.6.25 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 [peer_num]
```

```
clear url filter tunnel [tunnel_num]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -

[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]

RTX1100、RT107e は Rev.8.03.60 以降で使用可能。

RTX3000 は Rev.9.00.31 以降で使用可能。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

59.6.26 外部データベース参照型 URL フィルタの統計情報のクリア

[書式]

```
clear url filter external-database
```

```
clear url filter external-database [interface]
```

```
clear url filter external-database pp [peer_num]
clear url filter external-database tunnel [tunnel_num]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インターフェース名、WAN インターフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインターフェース番号
 - [初期値]: -

[説明]

外部データベース参照型 URL フィルターの Web レピュテーション統計情報、およびカテゴリーチェック統計情報を消去する。インターフェースが指定されない場合は、すべてのインターフェースの情報を消去する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1200, RTX1100, RT107e, SRT100

59.6.27 メール通知の実行**[書式]**

```
mail notify status exec id
```

[設定値及び初期値]

- *id*
 - [設定値]: 設定番号 (1..10)
 - [初期値]: -

[説明]

状態情報をメールで送信する。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

59.6.28 外部メモリに保存された SYSLOG ファイルのローテート (バックアップ)**[書式]**

```
rotate external-memory syslog
```

[説明]

外部メモリに保存された SYSLOG ファイルのローテート (バックアップ) を行う。
 現在書き込み中の SYSLOG ファイルをバックアップファイルに退避し、新たに書き込み用の SYSLOG ファイルを作成する。既に同名のバックアップファイルが存在する場合には実行されない。
 また、バックアップファイルを作成する際、バックアップファイル数が **external-memory syslog filename** コマンドで指定される上限数に達した場合、もしくは外部メモリに空き容量がなくなった場合は、最も古いバックアップファイルを削除してから新しいバックアップファイルが作成される。
 バックアップファイル名の書式については、**external-memory syslog filename** コマンドを参照のこと。
 なお、本コマンドは、**external-memory syslog filename** コマンドで SYSLOG ファイル名が設定されており、かつ、指定された外部ストレージインタフェースに外部メモリが接続されている場合にのみ動作する。

[ノート]

`schedule at` コマンドで定期的に本コマンドを実行するようにしておくと、日毎、週毎、あるいは月毎の SYSLOG のバックアップファイルを自動で作成することが可能になる。

[設定例]

```
schedule at 1 */* 00:00 * rotate external-memory syslog # 毎日バックアップを実行する
schedule at 1 */mon 00:00 * rotate external-memory syslog # 毎週月曜日にバックアップを実行する
```

```
schedule at 1 */1 00:00 * rotate external-memory syslog # 毎月 1 日にバックアップを実
行する
```

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830, RTX810

59.6.29 ライセンス認証の実行

[書式]

```
license authentication go
```

[説明]

LMS サーバーに対してライセンス認証を行う。実行中に Ctrl-C 押下で中断することができる。

[ノート]

RTX830 は Rev.15.02.13 以降で使用可能。

[適用モデル]

RTX830

59.6.30 ライセンス認証のリトライの間隔と回数の設定

[書式]

```
license authentication retry interval interval count
```

```
no license authentication retry interval [interval count]
```

[設定値及び初期値]

- *interval*
 - [設定値]: ライセンス認証をリトライするまでの間隔 (秒) (1 .. 3600)
 - [初期値]: 30
- *count*
 - [設定値]: ライセンス認証をリトライする回数 (1 - 10)
 - [初期値]: 5

[説明]

ライセンス認証に失敗したときのリトライ間隔と回数を設定する。

ライセンス認証に失敗したとき、*interval* に設定した間隔でライセンス認証のリトライを行う。*count* に設定した回数連続でライセンス認証に失敗した場合はリトライを停止する。

本コマンドの設定に関わらず、**license authentication go** コマンドによる手動認証に失敗した場合は、ライセンス認証のリトライは行わない。

[ノート]

ライセンス認証のリトライ待ちであるとき、**license authentication go** コマンドによる手動認証を行った場合は、ライセンス認証のリトライは停止する。

RTX830 は Rev.15.02.14 以降で使用可能。

[適用モデル]

RTX830

59.6.31 設定の一括更新

[書式]

```
load [config-type] config [difference] [silent | interactive] [no-configure-refresh] [no-key-generate] [rollback-timer=timer]
```

[設定値及び初期値]

- *config-type*: 引数 *config* の種類を表す
- [設定値]:

設定値	説明
config	config 番号
file	RTFS, EMFS, 外部メモリーに保存されているファイルのファイル名

- [初期値]: -
- *config*
 - [設定値]: config 番号、またはファイル名
 - [初期値]: -
- *timer*
 - [設定値]: 復元タイマーの値 (120 .. 21474836)
 - [初期値]: -

[説明]

指定された設定ファイルへ設定を復元・更新する。

config-type を省略した書き方をした場合、*config* は以下の順で解釈される。

- 保存されている config 番号に一致する場合はその設定
- 存在するファイル名と一致する場合はそのファイル

更新方法には、置換と差分の 2 種類がある。

- 置換: 現在の設定内容をいったんすべて消去し、設定ファイルの設定内容に置き換える。
- 差分: 現在の設定内容を設定ファイルの設定内容に変更する、最小限のコマンドを実行する。

デフォルト動作は置換更新であり、*difference* オプションを指定することで差分更新となる。

デフォルトでは、設定を置き換えるために実行するコマンドがコンソールに表示される。*silent* オプションを指定すると、コマンドの表示はせずに設定を書き換える。*interactive* オプションを指定すると、コマンドを一つずつ実行するかどうか確認しながら設定を更新できる。*interactive* オプションは、対話的ではないインターフェース (Web GUI 設定中のコマンド入力など) からは利用できない。*silent* オプションと *interactive* オプションを同時に指定することはできない。

load コマンドで設定を置き換えた場合、必要に応じて '**ospf configure refresh**'、'**bgp configure refresh**' あるいは '**ipv6 ospf configure refresh**' コマンドが追加で実行される。*no-configure-refresh* オプションを指定すると、この動作を抑止することができる。

更新前後の設定ファイルに **sshd host key generate** コマンドが設定されていた場合、*no-key-generate* オプションを指定するとホスト鍵の再生成は実行されず、更新前のホスト鍵の設定を引き継ぐことができる。

rollback-timer オプションで復元タイマーが設定できる。以下の場合に、自動的に設定が **load** コマンド実行前の内容に復元される。

- 復元タイマーがタイムアウトした。
- ログインタイマーがタイムアウトした。

復元タイマーを停止するには以下のいずれかの操作が必要である。

- **confirm** コマンドを実行する。
- **save** コマンドで設定を不揮発性メモリーに保存する。
- **quit**、または **exit** コマンドでログアウトする。
- **restart** コマンドで機器を再起動する。
- *rollback-timer* オプション無しの **load** コマンドを実行する。

一つのコンソールあたり、復元タイマーは一つしか動作しない。*rollback-timer* オプション付きの **load** コマンドあるいは **rollback timer** コマンドを複数回実行した場合には、最後のコマンドの復元タイマーのみが有効となる。

rollback-timer オプションを省略した場合には、復元タイマーは動作しない。

[ノート]

暗号化された設定ファイルには対応していない。

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。

RTX1210 は Rev.14.01.26 以降で指定可能。ただし、*no-key-generate* オプションは Rev.14.01.28 以降で使用可能。

RTX830 は Rev.15.02.03 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

59.6.32 ロールバックタイマーの起動

[書式]

rollback timer *timer*

[設定値及び初期値]

- *timer*
 - [設定値]: 復元タイマーの値 (秒、1.21474836)
 - [初期値]: -

[説明]

復元タイマーのみを設定する。以下の場合に、自動的に設定が **rollback timer** コマンド実行前の内容に復元される。

- 復元タイマーがタイムアウトした。
- ログインタイマーがタイムアウトした。

以下の場合に、復元タイマーは停止する。

- **confirm** コマンドを実行する。
- **save** コマンドで設定を不揮発性メモリーに保存する。
- **quit**、または **exit** コマンドでログアウトする。
- **restart** コマンドで機器を再起動する。
- **rollback-timer** オプション無しの **load** コマンドを実行する。

一つのコンソールあたり、復元タイマーは一つしか動作しない。**rollback-timer** オプション付きの **load** コマンドあるいは **rollback timer** コマンドを複数回実行した場合には、最後のコマンドの復元タイマーのみが有効となる。

[ノート]

このコマンドは、手動で設定を変更するときのセーフネットとして利用することができる。

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。

RTX1210 は Rev.14.01.26 以降で使用可能。

RTX830 は Rev.15.02.03 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

59.6.33 設定の確認

[書式]

confirm

[説明]

load コマンドあるいは **rollback timer** コマンドで起動した復元タイマーを停止し、設定変更の内容を確定させる。

[ノート]

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。

RTX1210 は Rev.14.01.26 以降で使用可能。

RTX830 は Rev.15.02.03 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

59.6.34 ファイルをマクロとして実行する

[書式]

call [-v] [-x] *filename* [*parameter..*]

[設定値及び初期値]

- *filename*
 - [設定値]: ファイル名
 - [初期値]: -
- *parameter*
 - [設定値]: マクロ引数
 - [初期値]: -

[説明]

filename で指定したファイルをマクロとして実行する。

マクロには引数を渡すことができる。引数が、NAME=VALUE の形をしている場合、マクロ内では変数 NAME として VALUE を参照できる。他の形の引数は位置引数として、指定された順番に、\$1、\$2 等でアクセスできる。\$0 はファイル名、\$* はすべての位置引数を空白で結合した文字列となる。引数はすべてマクロ内でのみ利用可能な変数である。

-v オプションを指定すると、マクロを実行するときに実行する各行について、変数とエイリアスの展開前の内容を表示しながら実行する。

-x オプションは、変数とエイリアスを展開した後の行を表示しながらマクロを実行する。

[ノート]

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。

RTX1210 は Rev.14.01.26 以降で使用可能。

RTX830 は Rev.15.02.03 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

59.6.35 echo

[書式]

echo [*string*]

[設定値及び初期値]

- *string*
 - [設定値]: 表示したい文字列
 - [初期値]: -

[説明]

指定された文字列を表示する。

[ノート]

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。

RTX1210 は Rev.14.01.26 以降で使用可能。

RTX830 は Rev.15.02.03 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

第 60 章

設定の表示

60.1 機器設定の表示

[書式]

```
show environment [detail]
```

[設定値及び初期値]

- detail
 - [設定値]: 全体の平均 CPU 使用率に加えて、各コア毎の CPU 使用率を表示する
 - [初期値]: -

[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 (%)
- パケットバッファの使用量 (%) (Rev.10.01 系以降のファームウェア)
- 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)
- ファンの状態 (RTX5000、RTX3500、RTX3000)
- 内部温度の状態 (RTX5000、RTX3500、RTX3000、RTX1500、RTX1220、RTX1210、RTX1200、RT250i)

detail オプションは RTX5000、RTX3500 で使用可能である。RTX5000、RTX3500 では detail オプションを省略した場合は全体の平均 CPU 使用率が表示され、detail オプションを指定した場合は全体の平均 CPU 使用率に加え、各コア毎の CPU 使用率が表示される。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

60.2 すべての設定内容の表示

[書式]

```
show config
show config filename
less config
less config filename
```

[設定値及び初期値]

- filename
 - [設定値]: 設定ファイル名または退避ファイル名 (0.4.2)
 - [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

60.3 指定した AP の設定内容の表示

[書式]

```
show config ap [ap]
```

```
less config ap [ap]
```

[設定値及び初期値]

- *ap*
 - [設定値]:
 - MAC アドレスもしくは経路
 - 省略時は、選択されている AP について表示する
 - [初期値]: -

[説明]

show config、**less config** コマンドの表示の中から、指定した AP に関するものだけを表示する。

[ノート]

RTX1210 は、Rev.14.01.09 以降で使用可能。

RTX810 は、Rev.11.01.25 以降で使用可能。

RTX1200 は、Rev.10.01.65 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

60.4 指定した PP の設定内容の表示

[書式]

```
show config pp [peer_num]
```

```
show config pp [peer_num-peer_num]
```

```
less config pp [peer_num]
```

```
less config pp [peer_num-peer_num]
```

[設定値及び初期値]

- *peer_num*
 - [設定値]:
 - 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
 - [初期値]: -

[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。

Rev.14.00 系以降のファームウェアで第 2 書式が利用できる。相手先情報番号の間にハイフン (-) を挟んで範囲指定すると、指定した範囲の相手先情報番号に関するものを表示する。

[拡張ライセンス対応]

[拡張ライセンス](#)をインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

60.5 指定したスイッチの設定内容の表示

[書式]

```
show config switch [switch]
```

```
less config switch [switch]
```

[設定値及び初期値]

- *switch*
 - [設定値]:
 - MAC アドレスもしくは経路
 - 省略時は、選択されているスイッチについて表示する
 - [初期値]:-

[説明]

show config、**less config** コマンドの表示の中から、指定したスイッチに関するものだけを表示する。

[ノート]

RTX1210 は、Rev.14.01.09 以降で使用可能。

RTX810 は、Rev.11.01.25 以降で使用可能。

RTX1200 は、Rev.10.01.65 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

60.6 指定したトンネルの設定内容の表示

[書式]

```
show config tunnel [tunnel_num] [expand]
```

```
show config tunnel [tunnel_num-tunnel_num] [expand]
```

```
less config tunnel [tunnel_num] [expand]
```

```
less config tunnel [tunnel_num-tunnel_num] [expand]
```

[設定値及び初期値]

- *tunnel_num*
 - [設定値]:
 - 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
 - [初期値]:-

[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。

Rev.14.00 系以降のファームウェアで第 2 書式が利用できる。トンネル番号の間にハイフン (-) を挟んで範囲指定すると、指定した範囲のトンネル番号に関するものを表示する。

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。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

60.7 設定の差分の表示

[書式]

```
show config difference [[config-type1] config1] [config-type2] config2
```

[設定値及び初期値]

- *config-type1/2* : 引数 *config1* , *config2* の種類を表す

- [設定値] :

設定値	説明
config	config 番号
file	RTFS, EMFS, 外部メモリーに保存されているファイルのファイル名

- [初期値] :-
- *config1/2*
 - [設定値] : '-' (現在動作中の設定)、config 番号、またはファイル名のいずれか
 - [初期値] :-

[説明]

config1 と *config2* の差分を、*config1* を *config2* へ変換するためのコマンド列という形で表示する。

config1 にあり、*config2* にないコマンドは no 形式で表示され、*config1* になく、*config2* にあるコマンドは通常形式で表示される。*config1*、*config2* ともに、**show config** コマンドでの表示に沿った形でインデント (段付け) されていなくてはならない。

config1 を省略した場合は、 '-' (現在動作中の設定) が指定されたものとする。

config-type1/2 を省略した場合、*config1/2* は以下の順で解釈される。

- 保存されている config 番号に一致する場合は、その設定
- 存在するファイル名と一致する場合は、そのファイル

[ノート]

config1/2 に config 番号を指定した場合で、保存されている設定に **login password**、**login password encrypted**、**administrator password**、**administrator password encrypted** コマンドが含まれている場合には、動作前にそれらのパスワードを入力する必要がある。

このコマンドは、管理者モードでのみ動作する。

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。

RTX1210 は Rev.14.01.26 以降で使用可能。

RTX830 は Rev.15.02.03 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

60.8 設定ファイルの一覧

[書式]

```
show config list
```

```
less config list
```

[説明]

内蔵フラッシュ 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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

60.9 ファイル情報の一覧の表示

[書式]

```
show file list location [all] [file-only]
```

less file list *location* [*all*] [*file-only*]

[設定値及び初期値]

- *location* : 表示するファイルのある位置
 - [設定値]:

設定値	説明
internal	内蔵フラッシュ ROM に格納されている config 一覧
絶対パスまたは相対パス	内蔵フラッシュ ROM の RTFS 領域および外部メモリ

- [初期値]:-
- *all* : 配下の全ディレクトリを対象にする
 - [初期値]:-
- *file-only* : ファイル名のみを表示する
 - [初期値]:-

[説明]

指定した場所に格納されているファイル情報の一覧を表示する。*location* に指定可能なパラメータは、リビジョンごとに以下の通りとなる。

リビジョン	パラメータ
Rev.10.00 系以降	internal、絶対パスまたは相対パス
上記以外	internal

all、*file-only* は Rev.10.00 系以降のファームウェアで使用可能。

location に相対パスを指定した場合、環境変数 PWD を基点としたパスと解釈される。PWD は **set** コマンドで変更可能であり、初期値は "/" である。

[ノート]

location に絶対パスまたは相対パスを指定した場合のみ、*all* と *file-only* を使用できる。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

60.10 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*]

[設定値及び初期値]

- *interface*
 - [設定値]: 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
 - [初期値]:-
- *peer_num*
 - [設定値]:
 - 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
 - [初期値]:-
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]:-

[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]

インタフェース名は Rev.8.03 系以降のすべてのファームウェアで指定可能。
 ブリッジインタフェースは SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、
 RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指
 定可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

60.11 マスタクロックを得ている回線の表示

[書式]

show line masterclock

[説明]

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

[適用モデル]

RTX5000, RTX3500, RTX3000, RT250i

60.12 SSH サーバー公開鍵の表示

[書式]

show sshd public key [fingerprint]

[設定値及び初期値]

- *fingerprint* : 鍵指紋を表示することを示すキーワード
 - [初期値] :-

[説明]

SSH サーバーの公開鍵を表示する。
fingerprint キーワードを指定した場合は、公開鍵の鍵長と鍵指紋を表示する。

[ノート]

fingerprint キーワードは、RTX1200 Rev.10.01.71 以降、RTX810 Rev.11.01.28 以降、RTX5000 / RTX3500 Rev.14.00.21 以降、RTX1210 Rev.14.01.11 以降のファームウェア、および、Rev.15.02 系以降のすべてのファームウェアで使用可能。

[表示例]

```
> show sshd public key
ssh-dss XXXXXXXXXXXX1kc3MAAAEBAPTb9YYdgvE+4bbhF4mtoIJri+ujdAI fgr4hL/0w7Jlvc50eXg
```

```
sXJocQlPlsLRGH0OzxVYbOouPCUV/jPFcatg0Iii8eJNzUqSBle6MOftGjmESrdYiafyIUhps+YWqd
T1Io0AFnVUKMqAbYODA3Cy7kNVptYRK8rcKwK1ChbatWnT/Z7RcmEVEou0q1Oyp79b3DcpFM7ofa4d
9ySb6mj06Y/Ok8lL5qFhChmGOGtqJTKZsqb5VnVz8FYC8t1s6/tpyrUa5aG2af/yTEa5U5BDYAuc88
wNIUG9a1Go/8WIHiBJAm432o7UPqTHWO/5nYEQu44gmEPQrPGJ65GT8AAAAVAOpjE0Jyei+4c5qWSF
PXUgrLf5HAAABAQCnnPO+ZjWZcZwGa6LxTGMczAjDy5uwD4DWBbRxsPKaXlsicJGC0aridnTthIGa8
ARypDjhpL1a37SDezx8yClQ5vh+4SPLds1hdSSzXXE+MXIICXnOVPdiKC4ia10n81tMxW/EPw4SqFP
77r7VvCE/JpXv82AN2JTJ/HAn3X7lvMyCsKZLoWrEcEcBH5anvAQKByVt7RerToZ4vSgods kv7nyXX
XXXXXX
```

```
ssh-rsa XXXXXXXXXXXX1yc2EAAAABIwAAAQEAwvAZK18jKTCHIHQfRV4r7UOYChX0oeKjBbuuLSDhSH
WmhpG3xxJO0pDIedSF3Kn7LX2SfymQYJ7XYIqMjmU0oziv/zi+De/z3M7wJHQUwfmZEDAdR6Mx39w
6Q04/ehQcaszjXi+0A12wG/kk561AU23CW/i21o//5GZTzkFKyEJUWauHWEW9glF5Yy7F64PesqoH
6h5oDNK7Lh1T7s4QXRnUJphI1INrW278Dnvyry3liR+tgTJAq3cGHfYsaQCdankDilIQhUazUY0vJO
/gjYCjMuWH6Ek/cst+Pctgnt0XV5B1079uRumcACs2pDX5EWrwPXXXXXXXXXX==
```

```
> show sshd public key fingerprint
```

```
ssh-dss 2048 XX:XX:77:c5:f9:48:fd:62:85:fb:27:a8:0a:c1:XX:XX
```

```
ssh-rsa 2048 XX:XX:58:89:e2:0b:ec:d9:6b:49:11:d2:a3:9d:XX:XX
```

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

60.13 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]
```

[設定値及び初期値]

- *interface*
 - [設定値]: フィルタの適用されたインタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -
- *dir*
 - [設定値]: フィルタの適用された方向、'in' または 'out'
 - [初期値]: -

[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。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

60.14 指定したインターフェースのIPv6 フィルター内容の表示

[書式]

```
show ipv6 secure filter interface [dir]
```



```
show ipv6 secure filter pp [peer_num] [dir]
show ipv6 secure filter tunnel [tunnel_num] [dir]
```

[設定値及び初期値]

- *interface*
 - [設定値]: フィルターの適用されたインターフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインターフェース番号
 - [初期値]: -
- *dir*
 - [設定値]: フィルターの適用された方向、'in' または 'out'
 - [初期値]: -

[説明]

指定したインターフェースに適用されている IPv6 フィルター定義の内容を表示する。

[ノート]

RTX5000、RTX3500 Rev.14.00.26 以降、RTX1210 Rev.14.01.33 以降、RTX830 Rev.15.02.09 以降、RTX1220 で使用可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

60.15 ファームウェアファイルの一覧

[書式]

```
show exec list
less exec list
```

[説明]

内蔵フラッシュ ROM に保存されている実行形式ファームウェアファイルの情報を表示する。起動中の実行形式ファームウェアファイルには '*' 印が表示される。実行形式ファームウェアファイルが保存されている外部メモリが接続されている場合には、そのファームウェアファイルの情報も表示される。

[ノート]

RTX1100, RTX1500 は、Rev.8.03.82 以降で使用可能。

RTX3000 は、Rev.9.00.43 以降で使用可能。

RTX810 は、Rev.11.01.21 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810

60.16 環境変数の表示

[書式]

show set [*name*]

[設定値及び初期値]

- name
 - [設定値]: 環境変数名
 - [初期値]: -

[説明]

指定した環境変数の値を表示する。

name を省略した場合には、設定されている環境変数をすべて表示する。

[ノート]

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。

RTX1210 は Rev.14.01.26 以降で使用可能。

RTX830 は Rev.15.02.03 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210

60.17 エイリアスの表示

[書式]

show alias [*name*]

[設定値及び初期値]

- name
 - [設定値]: エイリアス名
 - [初期値]: -

[説明]

指定したエイリアスの値を表示する。

name を省略した場合には、設定されているエイリアスをすべて表示する。

[ノート]

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。

RTX1210 は Rev.14.01.26 以降で使用可能。

RTX830 は Rev.15.02.03 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

60.18 マクロの表示

[書式]

show macro [*name*]

[設定値及び初期値]

- name
 - [設定値]: マクロ名
 - [初期値]: -

[説明]

指定したマクロの値を表示する。

name を省略した場合には、設定されているマクロをすべて表示する。

[ノート]

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。

RTX1210 は Rev.14.01.26 以降で使用可能。

RTX830 は Rev.15.02.03 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

第 61 章

状態の表示

61.1 ARP テーブルの表示

[書式]

```
show arp [interface[/sub_interface]]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *sub_interface*
 - [設定値]: 1-32 (RTX5000、RTX3500、RTX3000、RTX1220、RTX1210、RTX1200、RTX830)、1-8(左記以外の機種)
 - [初期値]: -

[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]

interface は、Rev.8.02 系以降のファームウェアで指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

61.2 インタフェースの状態の表示

[書式]

```
show status interface
```

[設定値及び初期値]

- *interface*
 - [設定値]:
 - LAN インタフェース名
 - WAN 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
 - [初期値]: -

[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は SRT100 Rev.10.00.38 以降、RTX1200 Rev.10.01.53 以降、RTX810 Rev.11.01.21 以降、RTX5000 / RTX3500 Rev.14.00.12 以降のファームウェア、および、Rev.14.01 系以降のすべてのファームウェアで指定可能。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

61.3 各相手先の状態の表示

[書式]

```
show status pp [peer_num]
```

[設定値及び初期値]

- *peer_num*
 - [設定値]:
 - 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
 - [初期値]:-

[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

[拡張ライセンス対応]

[拡張ライセンス](#)をインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

61.4 DLCI の表示

[書式]

```
show dlci [peer_num]
```

[設定値及び初期値]

- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]:-

[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, RTX1500, RTX1200, RTX1100, RT250i

61.5 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
```

[設定値及び初期値]

- *destination*
 - [設定値]:
 - 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
 - [初期値]: -
- *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
 - [初期値]: -
- *summary*: IPv4 の経路数をプロトコル毎に合計して表示する
 - [初期値]: -

[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ようになる。

プロトコル	メトリック値
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

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

61.6 RIP で得られた経路情報の表示

[書式]

```
show ip rip table
```

[説明]

RIP で得られた経路情報を表示する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

61.7 IPv6 の経路情報の表示

[書式]

```
show ipv6 route
show ipv6 route detail
show ipv6 route summary
```

[設定値及び初期値]

- detail : 現在有効な IPv6 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
 - [初期値] :-
- summary : IPv6 の経路数をプロトコル毎に合計して表示する
 - [初期値] :-

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

61.8 IPv6 の RIP テーブルの表示

[書式]

```
show ipv6 rip table
```

[説明]

IPv6 の RIP テーブルを表示する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

61.9 近隣キャッシュの表示

[書式]

```
show ipv6 neighbor cache [interface]
show ipv6 neighbor cache [interface] summary
```

[設定値及び初期値]

- interface
 - [設定値] : LAN インタフェース名
 - [初期値] :-

[説明]

近隣キャッシュの状態を表示する。

interface を指定した場合、そのインターフェース経由で得られた近隣キャッシュの状態のみ表示する。

summary を指定した場合、近隣キャッシュのエントリー数のみ表示する。

[ノート]

interface、summary は、RTX5000、RTX3500 は Rev.14.00.32 以降、RTX1210 は Rev.14.01.40 以降、RTX830 は Rev.15.02.20 以降、RTX1220 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

61.10 ブリッジのラーニング情報の表示

[書式]

```
show bridge learning bridge_interface
```

[設定値及び初期値]

- *bridge_interface*
 - [設定値]: ブリッジインタフェース名
 - [初期値]: -

[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。

[ノート]

RTX5000 は Rev.14.00.12 以降で使用可能。
 RTX3500 は Rev.14.00.12 以降で使用可能。
 RTX810 は Rev.11.01.21 以降で使用可能。
 RTX1200 は Rev.10.01.53 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

61.11 IPsec の SA の表示

[書式]

```
show ipsec sa [id]
show ipsec sa gateway [gateway_id] [detail]
```

[設定値及び初期値]

- *id*
 - [設定値]:
 - SA の識別子
 - 省略時はすべての SA について表示する
 - [初期値]: -
- *gateway_id*
 - [設定値]:
 - 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。
 - [初期値]: -
- *detail*: SA の詳細な情報を表示する。
 - [初期値]: -

[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 認証を行った場合、認証に使用したユーザ名

- RADIUS 認証を行ったか否か
- 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。

[拡張ライセンス対応]

[拡張ライセンス](#)をインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *gateway_id*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

61.12 証明書の情報の表示

[書式]

```
show pki certificate summary [cert_id]
```

[設定値及び初期値]

- *cert_id*

- [設定値]:

設定値	説明
1..2(RTX3000)	証明書ファイルの識別子
1..8(RTX3000 以外)	

- [初期値]: -

[説明]

証明書の情報を表示する。

表示される情報は以下の通り

- Subject
- SubjectAltName
- 使用可能期間 (Not Before, Not After)
- 証明書のタイプ (CA 証明書 / 機器証明書)

cert_id を指定した場合、指定したファイル識別子の証明書の情報だけを表示する。

[ノート]

RTX3000 は Rev.9.00.50 以降で使用可能。

RTX1200 は Rev.10.01.22 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

61.13 CRL ファイルの情報の表示

[書式]

```
show pki crl [crl_id]
```

[設定値及び初期値]

- *crl_id*

- [設定値]:

設定値	説明
1..2(RTX3000)	CRL ファイルの識別子
1..8(RTX3000 以外)	

- [初期値]: -

[説明]

CRL ファイルの情報を表示する。

表示される情報は以下の通り

- バージョン
- 発行者
- 更新日時

- 次回の更新日時

[ノート]

RTX3000 は Rev.9.00.50 以降で使用可能。
RTX1200 は Rev.10.01.22 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

61.14 VRRP の情報の表示

[書式]

```
show status vrrp [interface [vrid]]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *vrid*
 - [設定値]: VRRP グループ ID(1..255)
 - [初期値]: -

[説明]

VRRP の情報を表示する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

61.15 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] [detail]
```

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]:

設定値	説明
1..2147483647	NAT ディスクリプタ番号
all	すべての NAT ディスクリプタ番号

- [初期値]: -
- *detail*: 動的 IP マスカレードの全エントリを表示
 - [初期値]: -

[説明]

動的な NAT ディスクリプタのアドレスマップを表示する。

nat_descriptor を省略した場合はすべての NAT ディスクリプタ番号について表示する。

[ノート]

detail オプションは Rev.10.01 系以降で使用可能である。Rev.10.01 系以降では、*detail* オプションを省略した場合、動的 IP マスカレードエントリは内側 IP アドレスごとに集約して表示され、また、静的 IP マスカレードエントリから派生して生成された IP マスカレードエントリは表示されない。そのため、それ以前の全エントリ表示形式で表示させるためのオプションとして *detail* オプションが同系列から追加されている。

IP マスカレードのエントリが大量に存在する場合は、*detail* オプションを指定すると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またはセッション数を確認したい

ときは、detail オプションを指定しないようにするか、**show nat descriptor masquerade port summary** コマンド、または **show nat descriptor masquerade session 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 系以降で、**show nat descriptor masquerade session summary** コマンドは Rev.14.01 系以降で使用可能である。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

61.16 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
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -

[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。
 WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

61.17 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
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -

[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。
 RTX1200 Rev.10.01.09 以降、および、Rev.11.01 系以降のファームウェアでは、動的 IP マスカレードエントリは内側 IP アドレスごとに集約して表示され、また、静的 IP マスカレードエントリから派生して生成された IP マスカレードエントリは表示されない。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

61.18 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**

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]:
 - 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。
 - [初期値]:-

[説明]

動的 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。静的 IP マスカレードで確保されているポート番号の個数は含まれない。

[ノート]

Rev.14.01 系以降において、**nat descriptor backward-compatibility** コマンドで、*type* パラメータを 2 に設定した場合は本コマンドは使用できない。

代わりに、**show nat descriptor masquerade session summary** コマンドで、管理しているセッション数を表示することができる。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

61.19 IP マスカレードで使用しているセッション数の表示

[書式]

show nat descriptor masquerade session [*nat_descriptor*] **summary**

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]:
 - 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。
 - [初期値]:-

[説明]

IP マスカレードで管理しているセッション数およびセッション数のピーク値を表示する。セッション数のピーク値は NAT ディスクリプタの設定変更やルーターの再起動によってクリアされ、**clear nat descriptor dynamic** コマンドによるセッションの削除ではクリアされない。

[ノート]

本コマンドは、**nat descriptor backward-compatibility** コマンドで、*type* パラメータを 2 に設定した場合のみ使用可能である。

[適用モデル]

RTX1220, RTX1210, RTX830

61.20 IP マスカレードで管理しているセッションの統計情報の表示

[書式]

```
show nat descriptor masquerade session statistics [nat_descriptor]
```

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]:
 - NAT ディスクリプター番号 (1..2147483647)
 - *nat_descriptor* 省略時はすべての NAT ディスクリプターについて表示する。
 - [初期値]: -

[説明]

IP マスカレードで管理しているセッションの統計情報として始点 IP アドレスで識別されるホスト毎にセッション数、ピーク値、制限された回数と時刻を表示する。セッション数の制限値は、**nat descriptor masquerade session limit** コマンドの設定値に従う。

[ノート]

RTX5000 / RTX3500 Rev.14.00.32 以降、RTX1210 Rev.14.01.33 以降、RTX830 Rev.15.02.09 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

61.21 L2TP の状態の表示

[書式]

```
show status l2tp [tunnel tunnel_num]
```

[設定値及び初期値]

- *tunnel_num*
 - [設定値]: トンネル番号
 - [初期値]: -

[説明]

L2TP の状態を表示します。

[ノート]

RTX1500、RTX1100、RT107e は Rev.8.03.92 以降で使用可能。

RTX3000 は Rev.9.00.60 以降で使用可能。

SRT100 は Rev.10.00.60 以降で使用可能。

RTX1200 は Rev.10.01.32 以降で使用可能。

[拡張ライセンス対応]

[拡張ライセンス](#)をインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

61.22 PPTP の状態の表示

[書式]

```
show status pptp
```

[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]

RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810

61.23 IPIP トンネリングの状態の表示

[書式]

```
show status ipip [tunnel tunnel_num]
```

[設定値及び初期値]

- *tunnel_num*
 - [設定値]: トンネル番号
 - [初期値]: -

[説明]

IPIP トンネリングの状態を表示する。

[ノート]

RTX5000 / RTX3500 は Rev.14.00.22 以降で使用可能。

RTX1210 は Rev.14.01.20 以降で使用可能。

[拡張ライセンス対応]

[拡張ライセンス](#)をインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

61.24 OSPF 情報の表示

[書式]

```
show status ospf info
```

[設定値及び初期値]

- *info*: 表示する情報の種類
 - [設定値]:

設定値	説明
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

- [初期値]: -

[説明]

OSPF の各種情報を表示する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

61.25 BGP の状態の表示

[書式]

```
show status bgp neighbor [ip-address]
show status bgp neighbor ip-address route-type
```

[設定値及び初期値]

- *ip-address*
 - [設定値]: 隣接ルーターの IP アドレス
 - [初期値]: -
- *route-type*: 経路情報の表示
 - [設定値]:

設定値	説明
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

- [初期値]: -

[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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

61.26 DHCP サーバーの状態の表示

[書式]

```
show status dhcp [summary] [scope_n]
```

[設定値及び初期値]

- *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
 - [初期値]: -
- *scope_n*
 - [設定値]: スコープ番号 (1-65535)
 - [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

61.27 DHCP クライアントの状態の表示

[書式]

`show status dhcpc`

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

61.28 DHCPv6 の状態の表示

[書式]

`show status ipv6 dhcp`

[説明]

DHCPv6 に関する状態を表示する。

[ノート]

RTX3000 は、Rev.9.00.50 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

61.29 バックアップ状態の表示

[書式]

`show status backup`

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

61.30 動的フィルタによって管理されている接続の表示

[書式]

`show ip connection`

`show ip connection [interface [direction] [ip_address]]`


```
show ip connection pp [peer_num [direction] [ip_address]]
show ip connection tunnel [tunnel_num [direction] [ip_address]]
show ip connection summary
show ip connection detail [interface [direction]]
show ip connection detail pp [peer_num [direction]]
show ip connection detail tunnel [tunnel_num [direction]]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -
- *direction*
 - [設定値]:

設定値	説明
in	入力方向
out	出力方向

- [初期値]: -
- *ip_address*
 - [設定値]: IP アドレス xxx.xxx.xxx.xxx(xxx は十進数)
 - [初期値]: -
- *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
 - [初期値]: -
- *detail*: 動的フィルタによって管理されているすべてのコネクションを表示する
 - [初期値]: -

[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。

Rev.14.00 系以降では、*detail* を指定しない場合は管理されているコネクションを送信元 IP アドレスごとに集約して表示する。ただし、*ip_address* が指定された場合には *detail* を指定した場合の情報のうちソースアドレスが *ip_address* に一致するものを表示する。

[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、および、Rev.10.01 系以降のファームウェアで使用可能。

show ip connection detail コマンドは Rev.14.00 系以降のファームウェアで使用可能。

ip_address は Rev.14.00 系以降のファームウェアで指定可能。

WAN インタフェースは RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e

61.31 IPv6 の動的フィルタによって管理されている接続の表示

[書式]

```
show ipv6 connection
show ipv6 connection interface [direction] [ipv6_address]
show ipv6 connection pp [peer_num [direction] [ipv6_address]]
show ipv6 connection tunnel [tunnel_num [direction] [ipv6_address]]
show ipv6 connection summary
show ipv6 connection interface [direction]
show ipv6 connection pp [peer_num [direction]]
show ipv6 connection tunnel [tunnel_num [direction]]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -
- *direction*
 - [設定値]:

設定値	説明
in	入力方向
out	出力方向

- [初期値]: -
- *ipv6_address*
 - [設定値]: IPv6 アドレス部分
 - [初期値]: -
- *summary*: インタフェース/方向単位の管理接続数、および全体の合計を表示する
 - [初期値]: -
- *detail*: 動的フィルタによって管理されているすべての接続を表示する
 - [初期値]: -

[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接続を表示する。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。

Rev.14.00 系以降では、*detail* を指定しない場合は管理されている接続を送信元 IP アドレスごとに集約して表示する。ただし、*ipv6_address* が指定された場合には *detail* を指定した場合の情報のうちソースアドレスが *ipv6_address* に一致するものを表示する。

[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、および、Rev.10.01 系以降のファームウェアで使用可能。

show ipv6 connection detail コマンドは Rev.14.00 系以降のファームウェアで使用可能。

ipv6_address は Rev.14.00 系以降のファームウェアで指定可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

• *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

• *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e

61.32 ネットワーク監視機能の状態の表示

[書式]

show status ip keepalive

[説明]

ネットワーク監視機能の状態を表示する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

61.33 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*]]

[設定値及び初期値]• *interface*

• [設定値]: LAN インタフェース名、WAN インタフェース名

• [初期値]: -

• *peer_num*

• [設定値]: 相手先情報番号

• [初期値]: -

• *tunnel_num*

• [設定値]: トンネルインタフェース番号

• [初期値]: -

• *direction*

• [設定値]:

設定値	説明
in	入力方向
out	出力方向

• [初期値]: -

[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、Rev. 9.00 系以降のファームウェアでは **ip interface intrusion detection report** コマンドで設定した件数、それ以外のファームウェアでは 50 件となる。

[ノート]

RT250i では **show ip intrusion detection tunnel** コマンドは使用できない。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

61.34 相手先ごとの接続時間情報の表示

[書式]

```
show pp connect time [peer_num]
```

[設定値及び初期値]

- *peer_num*
 - [設定値]:
 - 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
 - [初期値]: -

[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]

RTX830, RTX810, RT107e, SRT100

61.35 PPPoE パススルー機能がラーニングした情報の表示

[書式]

```
show pppoe pass-through learning
```

[説明]

PPPoE パススルー機能がラーニングした情報を表示する。

[ノート]

RTX830 は Rev.15.02.03 以降で使用可能。

RTX1210 は Rev.14.01.26 以降で使用可能。

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

61.36 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]

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]:
 - 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
 - [初期値]: -

[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

[ノート]

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

61.37 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]] [mac_address]

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *port*
 - [設定値]: ポート番号 1..8 (RTX1220、RTX1210、RTX1200)、1..4 (左記以外の機種)
 - [初期値]: -
- *mac_address*
 - [設定値]: MAC アドレス
 - [初期値]: -

[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]

`mac_address` パラメータは Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

61.38 UPnP に関するステータス情報の表示

[書式]

```
show status upnp
```

[説明]

UPnP に関するステータス情報を表示する。

[適用モデル]

RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

61.39 トンネルインタフェースの状態の表示

[書式]

```
show status tunnel [tunnel_num]
```

```
show status tunnel [state]
```

```
show status tunnel [name=name]
```

[設定値及び初期値]

- `tunnel_num`
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -
- `state`: 接続状態
 - [設定値]:

設定値	説明
up	接続されているトンネルインタフェース一覧を表示する
down	接続されていないトンネルインタフェース一覧を表示する

- [初期値]: -
- `name`
 - [設定値]: 接続相手の名前
 - [初期値]: -

[説明]

トンネルインタフェースの状態を表示する。

第 2 書式は PPTP トンネルには対応していない。PPTP の対応機種では、PPTP トンネルは接続されていないトンネルインタフェースとして判定される。また、L2TP/IPsec 機能および L2TPv3/IPsec 機能の対応機種では、L2TP トンネルは IPsec トンネルの状態に応じて接続状態が判定される。

第 3 書式では、マルチポイントトンネルインタフェースで接続している相手の中から `name` に指定した文字列を含む名前が付与されている接続相手の情報を抽出して表示する。なお、接続相手の名前は相手側の **tunnel multipoint local name** コマンドで設定する。

[ノート]

第 2 書式は、SRT100 Rev.10.00.61 以降、RTX1200 Rev.10.01.53 以降のファームウェア、および、Rev.14.00 系以降のすべてのファームウェアで使用可能。

第3書式は、RTX5000 / RTX3500 Rev.14.00.26以降、RTX1210 Rev.14.01.20以降のファームウェア、および、Rev.15.02系以降のすべてのファームウェアで使用可能。

[拡張ライセンス対応]

拡張ライセンスをインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

61.40 VLAN インタフェースの状態の表示

[書式]

```
show status vlan [interface/sub_interface]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *sub_interface*
 - [設定値]: 1-32 (RTX5000、RTX3500、RTX3000、RTX1220、RTX1210、RTX1200、RTX830)、1-8 (左記以外の機種)
 - [初期値]: -

[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]

RTX1100、RT107e は Rev.8.02.28 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

61.41 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]
```

[設定値及び初期値]

- *template_id*
 - [設定値]: テンプレート ID (1..10)
 - [初期値]: -
- *debug*: デバッグ用の内部情報を表示させる
 - [初期値]: -

[説明]

トリガによるメール通知機能の内部状態を表示する。
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 についての状態を表示する。

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, SRT100

61.42 マルチキャストの経路情報の表示

[書式]

```
show ip mroute [option]
```

[設定値及び初期値]

- *option* : 出力する経路情報の粒度
- [設定値]:

設定値	説明
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。

- [初期値]: normal

[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。

出力される表中の各項目

項目名	説明
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)

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, RTX1500

61.43 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。

[適用モデル]

RTX3000, RTX1500

61.44 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。

[適用モデル]

RTX3000, RTX1500

61.45 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。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

61.46 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。

項目名	説明
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]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

61.47 ログインしているユーザー情報の表示

[書式]

```
show status user
```

[説明]

ルーターにログインしているユーザーの情報を表示する。以下の項目が表示される。

- ユーザー名
- 接続種別
- ログインした日時
- アイドル時間
- 接続相手の IP アドレス

また、ユーザーの状態に応じてユーザー名の前に以下の記号が表示される。

記号	状態
アスタリスク (*)	自分自身のユーザー情報
プラス (+)	管理者モードになっている
アットマーク (@)	RADIUS 認証でログインした

[表示例]

```
> show status user
(*: 自分自身のユーザー情報, +: 管理者モード, @: RADIUS での認証)
ユーザー名      接続種別      ログイン      アイドル      IP アドレス
-----
user-local      serial        09/16 10:21   0:00:17
@user-radius2   remote        09/16 10:22   0:00:36
*+@user-radius1 telnet1       09/16 10:22   0:00:00      192.168.0.100

> show status user
(*: current user, +: administrator mode, @: authenticated via RADIUS)
username        connection login time   idle      IP address
-----
user-local      serial        09/16 10:21   0:02:08
@user-radius2   remote        09/16 10:22   0:02:27
*+@user-radius1 telnet1       09/16 10:22   0:00:00      192.168.0.100
```

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

61.48 ログインしたユーザーのログイン履歴の表示

[書式]**show status user history****[説明]**

ルーターにログインしたユーザーのログイン履歴を最大で 50 件まで表示する。以下の項目が表示される。

- ユーザー名
- 接続種別
- ログインした日時
- アイドル時間
- 接続相手の IP アドレス

[適用モデル]

RTX1220, RTX1210, RTX830

61.49 パケットバッファの状態の表示

[書式]**show status packet-buffer [group]****[設定値及び初期値]**

- *group*: 表示するパケットバッファのグループを指定する
 - [設定値]:

設定値	説明
グループ名 (small, middle, large, jumbo, huge)	指定したグループの状態を表示する
省略	すべてのグループの状態を表示する

- [初期値]:-

[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。

[表示例]

```
# 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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

61.50 QoS ステータスの表示

[書式]

show status qos info [*interface* [*class*]]

[設定値及び初期値]

- *info* : 表示する情報の種類
 - [設定値] :

設定値	説明
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

- [初期値] :-
- *interface*
 - [設定値] : 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)
 - [初期値] :-
- *class*
 - [設定値] : クラス (RTX5000、RTX3500、RTX3000 : 1..100; 他の機種: 1..16)
 - [初期値] :-

[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 Rev.10.00 系以降である。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

61.51 連携動作の状態の表示

[書式]

```
show status cooperation type [id]
```

[設定値及び初期値]

- *type* : 連携動作タイプ
 - [設定値] :

設定値	説明
bandwidth-measuring	回線帯域検出
load-watch	負荷監視通知

- [初期値] : -
- *id*
 - [設定値] : 相手先 ID 番号 (1-100)
 - [初期値] : -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

61.52 OSPFv3 情報の表示

[書式]

```
show ipv6 ospf info
```

[設定値及び初期値]

- *info*
 - [設定値] :

設定値	説明
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

- [初期値] :-

[説明]

OSPFv3 の状態を表示する。

[ノート]

RTX1200 は Rev.10.01.53 以降で使用可能。

RTX810 は Rev.11.01.21 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

61.53 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]
```

[設定値及び初期値]

- *type* : 表示の種類

- [設定値] :

設定値	説明
summary	サマリーだけを表示する

- [初期値] :-

[説明]

入力遮断フィルタの状態を表示する。

[適用モデル]

SRT100

61.54 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]]
```

[設定値及び初期値]

- *id*

- [設定値] : 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

- [初期値] :-

- *type* : 表示の形式

- [設定値] :

設定値	説明
connection	指定したフィルタに関する接続の情報を表示する

- [初期値] :-

[説明]

ポリシーフィルタの状態を表示する。

[適用モデル]
SRT100

61.55 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]
SRT100

61.56 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]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、WAN インタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -

[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。

RTX1100、RT107e は Rev.8.03.60 以降で使用可能。

RTX3000 は Rev.9.00.31 以降で使用可能。

WAN インタフェースは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.32 以降のファームウェア、および、RTX1220、RTX1210、RTX830、RTX810 で指定可能。

[拡張ライセンス対応]

[拡張ライセンス](#)をインポートすると、以下のパラメーターに入力できる上限値が拡張される。

- *tunnel_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

- *peer_num*

ライセンス名	拡張後の上限値
YSL-VPN-EX1	100

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

61.57 外部データベース参照型 URL フィルターの統計情報の表示

[書式]

```
show url filter external-database
show url filter external-database [interface]
show url filter external-database pp [peer_num]
show url filter external-database tunnel [tunnel_num]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インターフェース名、WAN インターフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインターフェース番号
 - [初期値]: -

[説明]

外部データベース参照型 URL フィルターの Web レピュテーション統計情報、およびカテゴリーチェック統計情報を表示する。インターフェースが指定されない場合は、すべてのインターフェースの情報を表示する。

Web レピュテーション統計情報として表示される内容は以下の通り。

- セキュリティレベル
- 始点 IP アドレス
- HTTP コネクションとフィルターが一致した回数

カテゴリーチェック統計情報として表示される内容は以下の通り。

- データベースのカテゴリー番号
- 始点 IP アドレス
- HTTP コネクションとフィルターが一致した回数

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1200, RTX1100, RT107e, SRT100

61.58 データベースのライセンス情報の表示

[書式]

```
show url filter external-database id [database]
```

[設定値及び初期値]

- *database*
 - [設定値]:

設定値	説明
reputation	Web レピュテーションデータベースのみを対象とする
category	カテゴリーデータベースのみを対象とする

- [初期値]:-

[説明]

url filter external-database use コマンドの設定に従い、データベースのライセンス情報を表示する。

database パラメーターを指定することで、特定のデータベースのライセンス情報を表示する。また、*database* パラメーターを省略し、かつ複数のサービス事業者のデータベースを使用している場合は、それぞれのライセンス情報を表示する。

[ノート]

本コマンドを実行する前に、**url filter external-database use** コマンドで、使用するデータベースを設定する必要がある。

database パラメーターは SRT100 Rev.10.00.60 以降、RTX1200 Rev.10.01.36 以降のファームウェアで使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1200, RTX1100, RT107e, SRT100

61.59 生存通知の状態の表示

[書式]

show status heartbeat

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

61.60 USB ホスト機能の動作状態を表示

[書式]

show status usbhost [modem]

[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]

RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

61.61 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

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, SRT100

61.62 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 の TFTP.EXE を使用した例：

```
C:\>tftp 192.168.0.1 get techinfo techinfo.txt
```

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT107e, SRT100

61.63 microSD スロットの動作状態を表示

[書式]

show status sd

[説明]

microSD スロットの動作状態を表示する。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

61.64 外部メモリの動作状態を表示

[書式]

show status external-memory

[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 ポートに携帯端末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。

携帯端末の状態は **show status usbhost modem** で確認する。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

61.65 RTFS の状態の表示

[書式]

show status rtfs

[説明]

内蔵フラッシュ ROM の RTFS 領域の状態を表示する。表示する内容は次の通り。

- 容量
- 空き容量
- 作成可能エントリ数
- ファイル数
- ディレクトリ数

実行例は以下の通り。

```
# show status rtfs
容量                : 1572864 バイト
空き容量            : 1566025 バイト
作成可能エントリ数 : 995
ファイル数          : 2
ディレクトリ数      : 3
#
```

[ノート]

SRT100 は Rev.10.00.52 以降で使用可能。 RTX1200 は Rev.10.01.16 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

61.66 起動情報を表示する

[書式]

show status boot [*num*]

[設定値及び初期値]

- *num* : 履歴番号
- [設定値]:

設定値	説明
0..4	指定した番号の履歴を表示する
省略	省略時は 0

- [初期値]:-

[説明]

起動の情報を表示する。

show status boot list コマンドで表示される履歴番号を指定すると、その履歴の詳細が表示される。
num を省略した場合は、履歴番号=0 の履歴が表示される。

[ノート]

num パラメータは Rev.10.01 以降で指定可能である。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

61.67 起動情報の履歴の詳細を表示する

[書式]

show status boot all

[説明]

起動情報の履歴の詳細を最大で 5 件まで表示する。

cold start コマンド、**clear boot list** コマンドを実行すると、この履歴はクリアされる。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

61.68 起動情報の履歴の一覧を表示する**[書式]**

show status boot list

[説明]

起動情報の履歴を最大で 5 件まで表示する。

cold start コマンド、**clear boot list** コマンドを実行すると、この履歴はクリアされる。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810

61.69 エージェント一覧の表示**[書式]**

show status switch control [*interface*]

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インターフェース名、ブリッジインターフェース名
 - [初期値]: -

[説明]

エージェントの一覧を表示する。*interface* を省略した場合は、すべてのインターフェースについて情報を表示する。

L2MS の動作状態に応じて、以下の情報を表示する。

- L2MS のマネージャーとして動作している場合
 - MAC アドレス
 - 機種名
 - 機器名
 - マネージャーからの経路
 - アップリンクポート
 - エージェントを操作するときに指定する経路
 - 現在使用している設定内容
- L2MS のエージェントとして動作している場合
 - マネージャーの MAC アドレス

[ノート]

ブリッジインターフェースは RTX1210 Rev.14.01.20 以降のファームウェア、および、Rev.15.02 系以降のすべてのファームウェアで指定可能。

[表示例]

```
> show status switch control
LAN1
[00:a0:de:01:02:03]
機種名       : SWX2200-24G
機器名       : SWX2200-24G_0123456
経路         : lan1:1
アップリンク : 1
設定用経路   : lan1:1
設定         : switch select lan1:1
---
```

```

LAN2
スイッチ制御機能が有効になっていません
----
LAN3
スイッチ制御機能が有効になっていません
----
BRIDGE1
スイッチ制御機能が有効になっていません

```

```

> show status switch control
LAN1
[00:a0:de:01:02:03]
Model name       : SWX2200-24G
System name      : SWX2200-24G_0123456
Route            : lan1:1
Uplink           : 1
Route for Config: lan1:1
Config           : switch select lan1:1
----
LAN2
Switch control function is not available.
----
LAN3
Switch control function is not available.
----
BRIDGE1
Switch control function is not available.

```

```

> show status switch control
LAN1
マネージャー: 00:a0:de:01:02:03
----
LAN2
スイッチ制御機能が有効になっていません
----
LAN3
スイッチ制御機能が有効になっていません
----
BRIDGE1
スイッチ制御機能が有効になっていません

```

```

> show status switch control
LAN1
Manager: 00:a0:de:01:02:03
----
LAN2
Switch control function is not available.
----
LAN3
Switch control function is not available.
----
BRIDGE1
Switch control function is not available.

```

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

61.70 LAN ケーブル二重化機能の動作状態を表示**[書式]**

show status switch control route backup route

[設定値及び初期値]

- *route*
 - [設定値]: 経路
 - [初期値]: -

[説明]

LAN ケーブル二重化機能の動作状態を表示する。

状態	説明
none	LAN ケーブル二重化機能が動作していない
active	通信が可能な経路として動作している
force-linkdown	LAN ケーブル二重化機能によってリンクダウンしている
blocking	LAN ケーブル二重化機能によって通信が遮断されている

[ノート]

メイン経路がリンクアップしている場合、メイン経路は active で動作し、通信可能である。また、バックアップ経路は force-linkdown で動作し、ケーブルが接続されてもリンクアップしない。

メイン経路がリンクダウンしている場合、バックアップ経路は active で動作し、通信可能である。また、メイン経路は blocking で動作し、リンクアップした場合にループが発生しないよう、通信が遮断される。

スイッチに本機能が実装されていない場合はコマンドエラーとなる。

RTX1200 は Rev.10.01.45 以降で使用可能。 RTX810 は Rev.11.01.12 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

61.71 DNS キャッシュの表示

[書式]

show dns cache

[説明]

DNS キャッシュの内容を表示する。

[ノート]

SRT100 は Rev.10.00.61 以降で使用可能。

RTX1200 は Rev.10.01.36 以降で使用可能。

RTX810 は Rev.11.01.06 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX1200, RTX830, RTX810, SRT100

61.72 ライセンス情報の表示

[書式]

show status license

[説明]

LMS クライアントが取得したライセンス、および拡張ライセンスの情報を表示する。表示する項目は以下の通り。

品番	ライセンス製品の品番。
状態	ライセンスの状態。
有効期限	ライセンスの有効期限。"年/月/日"形式で示す。

ライセンスの状態には以下の種類がある。

有効 (Active)	<ul style="list-style-type: none"> LMS クライアントが取得したライセンス ライセンスが有効期限内であり、当該品番に対応するアプリケーションを使用できる状態。 拡張ライセンス ライセンスが有効であり、当該品番に対応する機能拡張が行われている状態。
---------------	---

更新猶予期間 (Renew grace period)	LMS クライアントが取得したライセンスでのみ表示される。有効期限を過ぎている状態。この状態より一定期間経過すると対応するアプリケーションを使用できなくなるため、ライセンスの購入手続きが必要となる。
認証猶予期間 (Authentication grace period)	LMS クライアントが取得したライセンスでのみ表示される。一時的にライセンス認証が猶予されている状態。ヤマハネットワーク機器が有効なライセンス情報を保持している状態で再起動し、その後 LMS サーバーと通信できない場合にこの状態となる。対応するアプリケーションを使用することはできるが、ディアクティベートまでの時間が経過するまでにライセンス認証を行う必要がある。ディアクティベートまでの時間は show status license authentication コマンドで確認することができる。

[ノート]

ライセンスを保持していない場合、あるいは LMS サーバーからライセンス情報を取得していない場合、当コマンドを実行しても情報は表示されない。

RTX830 は Rev.15.02.13 以降で使用可能。

拡張ライセンスの情報は RTX830 Rev.15.02.22 以降で表示される。

[適用モデル]

RTX830

61.73 ライセンス認証の状態の表示

[書式]

show status license authentication

[説明]

ライセンス認証の状態を表示する。表示する項目は以下の通り。

最終更新日時 (Last updated)	最後にライセンス認証に成功した日時。"年/月/日 時:分:秒" 形式で示す。
ディアクティベートまでの定期認証回数 (Counts to deactivation)	アプリケーションがディアクティベートされるまでの残り定期認証回数。
次の定期認証までの時間 (Time to periodic authentication)	次の定期認証までの時間。"時:分:秒" 形式で示す。
ディアクティベートまでの時間 (Time to deactivation)	ディアクティベートされるまでの時間。"時:分:秒" 形式で示す。この時間内はアプリケーションを使用できるが、経過するまでにライセンス認証を行う必要がある。

[ノート]

RTX830 は Rev.15.02.13 以降で使用可能。

[適用モデル]

RTX830

61.74 CPU スケジューリング(パケット転送)機能の状態の表示

[書式]

show status packet-scheduling

[説明]

現在の CPU スケジューリング(パケット転送)機能の状態を表示する。

- CPU スケジューリング方式
 - 動作中の CPU スケジューリング方式

設定値	説明
hash	ハッシュ方式

設定値	説明
load-balance	ロードバランス方式
lan-based	LAN インターフェース方式

- CPU 使用率
 - CPU コアごとの CPU コア全体の使用率
- フロー(IPv4/IPv6)
 - 全体の IPv4/IPv6 フロー数
 - CPU コアごとの IPv4/IPv6 フロー数
- 受信パケット
 - CPU コアごとの受信パケット数

CPU スケジューリング方式がロードバランス方式である場合、CPU コアごとの IPv4/IPv6 フロー数は表示されない。受信パケット数は、**system packet-scheduling** コマンドを実行するとクリアされる。

[ノート]

RTX5000、RTX3500 の Rev.14.00.13 以降で使用可能。

[表示例]

```
# show status packet-scheduling
CPU スケジューリング方式:      hash
CPU 使用率:
      CPU0:          57% (5sec)   56% (1min)   56% (5min)
      CPU1:          62% (5sec)   62% (1min)   62% (5min)
      CPU2:          88% (5sec)   89% (1min)   88% (5min)
      CPU3:          54% (5sec)   54% (1min)   54% (5min)
フロー (IPv4/IPv6):           2 エントリ / 2 エントリ
      CPU0:          0 エントリ / 1 エントリ
      CPU1:          1 エントリ / 0 エントリ
      CPU2:          1 エントリ / 0 エントリ
      CPU3:          0 エントリ / 1 エントリ
受信パケット:
      CPU0:          23155524 パケット
      CPU1:          14018842 パケット
      CPU2:          23624407 パケット
      CPU3:          22886347 パケット
```

[適用モデル]

RTX5000, RTX3500

61.75 STATUS LED の情報の表示

[書式]

```
show status status-led [history]
```

[設定値及び初期値]

- history : STATUS LED の状態変化の履歴を表示
 - [初期値] :-

[説明]

STATUS LED の情報を表示する。

点灯していた場合は、点灯の原因となったキープアライブが設定されているインターフェースの一覧が表示される。history オプションを指定した場合は状態変化の履歴も表示される。

[ノート]

RTX810 は、Rev.11.01.25 以降で使用可能。RTX1200 は、Rev.10.01.65 以降で使用可能。

[適用モデル]

RTX1220, RTX1210, RTX1200, RTX830, RTX810

61.76 LAN マップの状態を表示する

[書式]

```
show lan-map interface [detail]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インターフェース名、ブリッジインターフェース名
 - [初期値]: -
- *detail*: LAN マップで管理しているエージェントの情報に加えて、端末情報の詳細を表示する
 - [初期値]: -

[説明]

現在の LAN マップの状態を表示する。

- ファームウェアに取り込んでいる OUI の情報 (*detail* オプションを指定したときのみ)
- マネージャーの情報
 - リンクアップポート
 - マネージャー直下の端末情報
- エージェントの情報
 - 機種名
 - 機器名
 - 経路
 - リンクアップポート
 - アップリンクポート
 - ダウンリンクポート
 - エージェントの状態

状態	説明
Idle	通常状態
Search	検索要求を実行中

- 検出時刻
- 直近の検索要求が完了するまでに費やした時間
- エージェント配下の端末情報
- 消失したエージェントの情報
 - 機種名
 - 機器名
 - 検出時刻
 - 消失時刻
 - エージェント配下の端末情報
- 端末情報の詳細 (*detail* オプションを指定したときのみ)
 - IP アドレス
 - 検出時刻
 - 消失時刻
 - 種類
 - メーカー名
 - 機種名
 - 機器名
 - OS
 - コメント
 - スナップショット機能で警告の対象とするか否か

[ノート]

switch control mode コマンドで *mode* に *manager* が設定されている場合、本コマンドを使用できる。

ブリッジインターフェースは RTX1210 Rev.14.01.20 以降のファームウェア、および、Rev.15.02 系以降のすべてのファームウェアで指定可能。

[表示例]

```

# show lan-map lan1 detail
[OUI]
Generated           : Sat, 04 Mar 2017 04:31:14 -0400

[マネージャー]
リンクアップ       : lan1:1
端末数             : 0

[エージェント]
[00:a0:de:2a:dc:02]
機種名             : SWX2200-24G
機器名             : SWX1
経路               : lan1:1
リンクアップ       : 1 11
  アップリンク     : 1
  ダウンリンク     : なし
状態               : Idle
検出時刻           : 2017/05/24 11:28:59
検索時間           : 1 sec (867 msec)
端末数             : 1
  [ポート 1]
  [ポート 2]
  [ポート 3]
  [ポート 4]
  [ポート 5]
  [ポート 6]
  [ポート 7]
  [ポート 8]
  [ポート 9]
  [ポート 10]
  [ポート 11]
    [12:34:56:78:90:ab]
    IP アドレス     : 192.168.0.10
    検出時刻         : 2017/05/24 11:29:04
    種類             : Desktop PC
    メーカー         : Maker1
    機種名           : Modell1
    機器名           : Host1
    OS               : OS1
    コメント         : comment1
    スナップショット : on
  [ポート 12]
  [ポート 13]
  [ポート 14]
  [ポート 15]
  [ポート 16]
  [ポート 17]
  [ポート 18]
  [ポート 19]
  [ポート 20]
  [ポート 21]
  [ポート 22]
  [ポート 23]
  [ポート 24]

[消失エージェント]
[00:a0:de:7e:53:82]
機種名             : SWX2200-24G
機器名             : SWX2
検出時刻           : 2017/05/24 11:29:32
消失時刻           : 2017/05/24 12:18:50
端末数             : 0

```

[適用モデル]

RTX1220, RTX1210, RTX830

61.77 コピーライトの表示

[書式]

show copyright [detail]

[設定値及び初期値]

- detail
 - [設定値]: 条文を含めたソフトウェアの著作権情報を表示する
 - [初期値]: -

[説明]

ソフトウェアの著作権情報を表示する。

detail を指定することで、条文を含めたソフトウェアの著作権情報を表示することができる。

[ノート]

RTX810 は、Rev.11.01.28 以降で使用可能。

RTX5000、RTX3500 は、Rev.14.00.21 以降で使用可能。

RTX1210 は、Rev.14.01.11 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830, RTX810

第 62 章

ログイン

62.1 ログの表示

[書式]

```
show log [saved] [reverse]
show log external-memory [backup [fileid]]
less log [saved] [reverse]
```

[設定値及び初期値]

- saved
 - [設定値]: リポート直前のログを表示する
 - [初期値]: -
- reverse
 - [設定値]: ログを逆順に表示する
 - [初期値]: -
- external-memory
 - [設定値]: **external-memory syslog filename** コマンドで設定している SYSLOG ファイルの中身を表示する
 - [初期値]: -
- backup
 - [設定値]: SYSLOG バックアップファイルの中身を表示する、もしくは、SYSLOG バックアップファイルの一覧を表示する
 - [初期値]: -
- fileid: 指定した SYSLOG バックアップファイルの中身を表示する
 - [設定値]: `yyyymmdd_hhmmss`
 - [初期値]: -

[説明]

ルーターの動作状況を記録したログを表示する。

ログの最大保持件数を下表に示す。

機種	ファームウェア	件数
RTX5000	すべてのリビジョン	20000
RTX3500	すべてのリビジョン	20000
RTX3000	Rev.9.00.56 以降	3000
RTX1220	すべてのリビジョン	10000
RTX1210	すべてのリビジョン	10000
RTX1200	すべてのリビジョン	10000
RTX830	すべてのリビジョン	10000
RTX810	すべてのリビジョン	3000
上記以外の機種		500

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。

意図しないリポートが発生したときは、'saved' を指定することでリポート直前のログを表示することができる。

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。

パワーオフ・ログ保存機能に対応していない機種では、ルーターの電源を切るとログは消去される。

`external-memory` を指定した場合は、外部メモリ内の `SYSLOG` ファイルを表示する。

`external-memory backup` を指定した場合は、RTX1200 では、`SYSLOG` バックアップファイルの中身を表示する。Rev. 11.01 系以降のファームウェアでは、バックアップファイルの一覧を古いものから順に表示する。バックアップファイルの中身を表示するには、表示されたファイル名の日時データ (`yyyymmdd_hhmmss` 形式で表される文字列の 15 桁) を `fileid` に指定すると表示させることができる。

[ノート]

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、電源を切らない限りはログは保存される。

`saved` オプションは、RTX3000 Rev.9.00.56 以降、RTX1200 Rev.10.01.36 以降、SRT100 Rev.10.00.61 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで指定可能。RTX5000、RTX3500、RTX1210、RTX830、RTX1220 以外の機種では `saved` オプションを指定することで表示されるログは電源を切ると消去される。

`external-memory` を指定した場合は以下の制限がある。

- 外部メモリ内の暗号化したログファイルは表示できない
- リダイレクトを指定できない

`external-memory` を指定して、`external-memory syslog filename` コマンドが設定されていない場合は実行エラーとなる。

`external-memory`、`backup` パラメータは RTX1200 Rev.10.01.11 以降のファームウェア、および、Rev.11.01 系以降のすべてのファームウェアで指定可能。

`fileid` パラメータは Rev.11.01 系以降のすべてのファームウェアで指定可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i, RT107e, SRT100

62.2 アカウントの表示

[書式]

`show account`

`show account interface`

[設定値及び初期値]

- `interface`
 - [設定値]:
 - BRI インタフェース名
 - PRI インタフェース名
 - [初期値]: -

[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]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i

62.3 PP アカウントの表示

[書式]

```
show account pp [peer_num]
```

[設定値及び初期値]

- *peer_num*
 - [設定値]:
 - 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
 - [初期値]:-

[説明]

指定した PP インタフェースに関するアカウントを表示する。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1500, RTX1220, RTX1210, RTX1200, RTX1100, RTX830, RTX810, RT250i

62.4 TUNNEL アカウントの表示

[書式]

```
show account tunnel [tunnel_num]
```

[設定値及び初期値]

- *tunnel_num*
 - [設定値]:
 - 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する
 - [初期値]:-

[説明]

指定したデータコネクタ接続設定がされているトンネルインタフェースについて発着信回数や料金情報を表示する。発信回数、着信回数は切断時にカウントされる。料金情報は再起動によりクリアされる。**account threshold** コマンドで設定される閾値を超えたか否かの計算には、データコネクタ分の料金は含まれない。

[ノート]

RTX1200 は Rev.10.01.36 以降で使用可能。

RTX3000 は Rev.9.00.56 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200

62.5 携帯電話回線のアカウントの表示

[書式]

```
show account mobile
```

[説明]

携帯電話回線の発着信回数を表示する。

[適用モデル]

RTX830, RTX810

62.6 データコネクタのアカウントの表示

[書式]

```
show account ngn data
```

[説明]

データコネクタの発着信回数や課金情報を表示する。

[ノート]

課金情報は接続時間と設定した帯域幅から計算しているため、最終的に請求される料金とは異なる場合があります。

RTX1200 は Rev.10.01.36 以降で使用可能。

RTX3000 は Rev.9.00.56 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX3000, RTX1220, RTX1210, RTX1200, RTX830, RTX810

62.7 通信履歴の表示

[書式]

show history [reverse]

[設定値及び初期値]

- reverse
 - [設定値]: 履歴を逆順に表示する
 - [初期値]: -

[説明]

通信履歴を最大 100 件分表示する。履歴が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。

このコマンドでは、通常は時刻の古いものから順に表示するが、**reverse** オプション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。**reverse** オプションは Rev.15.02 系以降のファームウェアで指定可能。

[適用モデル]

RTX830, RTX810, RT107e

62.8 コマンド履歴の表示

[書式]

show command history [num]

[設定値及び初期値]

- num
 - [設定値]: ヒストリー番号 (1..21474836)
 - [初期値]: -

[説明]

コマンド履歴を表示する。

num を指定した場合は、指定した番号のコマンドから直前のコマンドまで表示する。num を省略した場合には、新しいものからさかのぼって最大 20 個のコマンドを表示する。

[ノート]

RTX5000、RTX3500 は Rev.14.00.26 以降で使用可能。

RTX1210 は Rev.14.01.26 以降で使用可能。

RTX830 は Rev.15.02.03 以降で使用可能。

[適用モデル]

RTX5000, RTX3500, RTX1220, RTX1210, RTX830

索引

記号

> 43
>> 43

A

account threshold 114
account threshold pp 114
administrator 741
administrator password 46
administrator password encrypted 46
administrator radius auth 48
alarm batch 101
alarm entire 100
alarm http revision-up 102
alarm http upload 610
alarm lua 652
alarm mobile 621
alarm sd 101
alarm startup 102
alarm usbhost 101
alias 103
ap config directory 708
ap config filename 708
ap control config delete 709
ap control config get 708
ap control config set 709
ap control config-auto-set use 710
ap control firmware update go 710
ap control http proxy timeout 711
ap control http proxy use 711
ap select 707
auth user 323
auth user attribute 324
auth user group 325
auth user group attribute 326

B

bgp aggregate 483
bgp aggregate filter 483
bgp autonomous-system 484
bgp configure refresh 488
bgp default med 493
bgp export 486
bgp export aspath 486
bgp export filter 487
bgp force-to-advertise 492
bgp import 488
bgp import filter 489
bgp log 491
bgp neighbor 490
bgp neighbor pre-shared-key 491
bgp preference 485
bgp reric interval 492
bgp router id 485
bgp use 483
bridge learning 639
bridge learning bridge_interface static 640
bridge learning bridge_interface timer 640
bridge member 638

C

call 776
clear account 748

clear account mobile 749
clear account ngn data 749
clear account pp 748
clear account tunnel 749
clear arp 750
clear boot list 755
clear bridge learning 750
clear diagnosis config port 724
clear dns cache 751
clear dpi cache 735
clear dpi statistics 734
clear ex-license 49
clear external-memory syslog 755
clear heartbeat2 589
clear heartbeat2 id 589
clear heartbeat2 name 589
clear inarp 751
clear ip dynamic routing 750
clear ip inbound filter 771
clear ip policy filter 772
clear ip traffic list 198
clear ip traffic list pp 198
clear ip traffic list tunnel 198
clear ipv6 dynamic routing 754
clear ipv6 inbound filter 771
clear ipv6 neighbor cache 754
clear ipv6 policy filter 772
clear log 750
clear mobile access limitation 613
clear mobile access limitation pp 613
clear nat descriptor dynamic 752
clear nat descriptor interface dynamic 753
clear nat descriptor interface dynamic pp 753
clear nat descriptor interface dynamic tunnel 753
clear nat descriptor masquerade session statistics 753
clear pppoe pass-through learning 754
clear pri status 752
clear status 751
clear switching-hub macaddress 768
clear url filter 772
clear url filter external-database 772
clear url filter external-database pp 772
clear url filter external-database tunnel 772
clear url filter pp 772
clear url filter tunnel 772
cloud vpn bind 369
cloud vpn name 369
cloud vpn option 370
cloud vpn parameter 368
cloud vpn service 368
cloud vpn set go 370
cloud vpn syslog 372
cold start 747
confirm 776
connect 760
connect pp 760
connect tunnel 760
console character 57
console columns 58
console info 59
console lines 58
console prompt 57
cooperation 460
cooperation bandwidth-measuring remote 461
cooperation load-watch control 465
cooperation load-watch remote 462
cooperation load-watch trigger 464
cooperation port 460

cooperation type go [466](#)
 copy [756](#)
 copy config [742](#)
 copy exec [744](#)

D

dashboard accumulate [739](#)
 date [54](#)
 delete [755](#)
 delete config [745](#)
 delete exec [745](#)
 delete pki file [745](#)
 description [79](#)
 description yno [714](#)
 dhcp client client-identifier [273](#)
 dhcp client client-identifier pool [273](#)
 dhcp client client-identifier pp [273](#)
 dhcp client hostname [271](#)
 dhcp client hostname pool [271](#)
 dhcp client hostname pp [271](#)
 dhcp client option [274](#)
 dhcp client option pool [274](#)
 dhcp client option pp [274](#)
 dhcp client release linkdown [275](#)
 dhcp convert lease to bind [265](#)
 dhcp duplicate check [260](#)
 dhcp manual lease [267](#)
 dhcp manual release [268](#)
 dhcp relay select [269](#)
 dhcp relay server [268](#)
 dhcp relay srcport [269](#)
 dhcp relay threshold [269](#)
 dhcp scope [261](#)
 dhcp scope bind [262](#)
 dhcp scope lease type [264](#)
 dhcp scope option [266](#)
 dhcp server rfc2131 compliant [259](#)
 dhcp service [258](#)
 diagnose config port access [723](#)
 diagnose config port map [722](#)
 diagnosis config port history-num [724](#)
 diagnosis config port max-detect [723](#)
 disconnect [761](#)
 disconnect ip connection [766](#)
 disconnect ipv6 connection [767](#)
 disconnect pp [761](#)
 disconnect tunnel [761](#)
 disconnect user [52](#)
 dns cache max entry [441](#)
 dns cache use [440](#)
 dns domain [430](#)
 dns host [439](#)
 dns notice order [433](#)
 dns private address spoof [434](#)
 dns server [429](#)
 dns server dhcp [432](#)
 dns server pp [431](#)
 dns server select [435](#)
 dns service [429](#)
 dns service aaaa filter [434](#)
 dns service fallback [441](#)
 dns srcport [439](#)
 dns static [438](#)
 dns syslog resolv [435](#)
 dpi group set [730](#)
 dpi log [732](#)
 dpi signature download go [731](#)
 dpi signature download url [732](#)
 dpi use [726](#)

E

echo [777](#)
 embedded file [105](#)
 ethernet filter [202](#)
 ethernet interface filter [204](#)
 ex-license password [48](#)
 execute at-command [613](#)
 execute batch [603](#)
 exit [741](#)
 external-memory accelerator cache size [594](#)
 external-memory auto-search time [603](#)
 external-memory batch filename [603](#)
 external-memory boot permit [599](#)
 external-memory boot timeout [600](#)
 external-memory cache mode [594](#)
 external-memory config filename [601](#)
 external-memory dpi signature directory [606](#)
 external-memory exec filename [600](#)
 external-memory performance-test go [604](#)
 external-memory statistics filename prefix [595](#)
 external-memory syslog filename [597](#)

F

fr backup [132](#)
 fr cir [130](#)
 fr compression use [132](#)
 fr congestion control [133](#)
 fr de [134](#)
 fr dlci [130](#)
 fr inarp [131](#)
 fr lmi [131](#)
 fr pp dequeue type [133](#)

G

grep [41](#)

H

heartbeat pre-shared-key [581](#)
 heartbeat receive [581](#)
 heartbeat send [582](#)
 heartbeat2 myname [583](#)
 heartbeat2 receive [586](#)
 heartbeat2 receive enable [586](#)
 heartbeat2 receive log [587](#)
 heartbeat2 receive monitor [587](#)
 heartbeat2 receive record limit [588](#)
 heartbeat2 transmit [583](#)
 heartbeat2 transmit enable [584](#)
 heartbeat2 transmit interval [585](#)
 heartbeat2 transmit log [585](#)
 help [45](#)
 http revision-down permit [84](#)
 http revision-up go [771](#)
 http revision-up permit [83](#)
 http revision-up proxy [83](#)
 http revision-up schedule [85](#)
 http revision-up timeout [84](#)
 http revision-up url [83](#)
 http upload [607](#)
 http upload go [610](#)
 http upload permit [608](#)
 http upload proxy [609](#)
 http upload retry interval [609](#)
 http upload timeout [609](#)
 http upload url [608](#)
 httpd custom-gui api password [655](#)
 httpd custom-gui api use [655](#)

[httpd custom-gui use 654](#)
[httpd custom-gui user 654](#)
[httpd host 550](#)
[httpd listen 551](#)
[httpd proxy-access l2ms permit 711](#)
[httpd service 550](#)
[httpd timeout 551](#)

I

[import ex-license key 49](#)
[import sshd authorized-keys 93](#)
[interface reset 759](#)
[interface reset pp 760](#)
[ip arp timer 163](#)
[ip dpi filter 726](#)
[ip filter 145](#)
[ip filter directed-broadcast 150](#)
[ip filter dynamic 150](#)
[ip filter dynamic timer 152](#)
[ip filter fqdn timer 153](#)
[ip filter set 149](#)
[ip filter source-route 149](#)
[ip flow limit 166](#)
[ip flow timer 166](#)
[ip forward filter 200](#)
[ip fragment remove df-bit 161](#)
[ip host 438](#)
[ip icmp echo-reply send 277](#)
[ip icmp echo-reply send-only-linkup 277](#)
[ip icmp error-decrypted-ipsec send 281](#)
[ip icmp log 281](#)
[ip icmp mask-reply send 277](#)
[ip icmp parameter-problem send 278](#)
[ip icmp redirect receive 279](#)
[ip icmp redirect send 278](#)
[ip icmp time-exceeded send 279](#)
[ip icmp timestamp-reply send 280](#)
[ip icmp unreachable send 280](#)
[ip icmp unreachable-for-truncated send 283](#)
[ip implicit-route preference 165](#)
[ip inbound filter 206](#)
[ip interface address 138](#)
[ip interface arp log 165](#)
[ip interface arp mtu discovery 282](#)
[ip interface arp queue length 164](#)
[ip interface arp static 163](#)
[ip interface dhcp auto default-route-add 144](#)
[ip interface dhcp auto interface-route-add 145](#)
[ip interface dhcp lease time 272](#)
[ip interface dhcp retry 272](#)
[ip interface dhcp service 270](#)
[ip interface dpi filter 729](#)
[ip interface forward filter 201](#)
[ip interface igmp 193](#)
[ip interface igmp static 194](#)
[ip interface inbound filter list 208](#)
[ip interface intrusion detection 153](#)
[ip interface intrusion detection notice-interval 155](#)
[ip interface intrusion detection repeat-control 155](#)
[ip interface intrusion detection report 156](#)
[ip interface intrusion detection threshold 156](#)
[ip interface mtu 140](#)
[ip interface nat descriptor 416](#)
[ip interface ospf area 477](#)
[ip interface ospf neighbor 480](#)
[ip interface pim sparse 194](#)
[ip interface proxyarp 162](#)
[ip interface proxyarp vrrp 162](#)
[ip interface rebound 141](#)
[ip interface rip auth key 177](#)
[ip interface rip auth key text 177](#)

[ip interface rip auth type 176](#)
[ip interface rip filter 175](#)
[ip interface rip force-to-advertise 181](#)
[ip interface rip hop 176](#)
[ip interface rip receive 174](#)
[ip interface rip send 174](#)
[ip interface rip trust gateway 172](#)
[ip interface secondary address 139](#)
[ip interface secure filter 159](#)
[ip interface secure filter name 159](#)
[ip interface tcp mss limit 157](#)
[ip interface tcp window-scale 158](#)
[ip interface traffic list 197](#)
[ip interface traffic list threshold 199](#)
[ip interface vrrp 183](#)
[ip interface vrrp shutdown trigger 184](#)
[ip interface wol relay 78](#)
[ip keepalive 190](#)
[ip local forward filter 201](#)
[ip pim sparse join-prune send 197](#)
[ip pim sparse log 196](#)
[ip pim sparse periodic-prune send 197](#)
[ip pim sparse register-checksum 196](#)
[ip pim sparse rendezvous-point static 195](#)
[ip policy address group 211](#)
[ip policy filter 213](#)
[ip policy filter set 215](#)
[ip policy filter set enable 215](#)
[ip policy filter set switch 216](#)
[ip policy filter timer 217](#)
[ip policy interface group 210](#)
[ip policy service 210](#)
[ip policy service group 212](#)
[ip pp address 138](#)
[ip pp dpi filter 729](#)
[ip pp forward filter 201](#)
[ip pp igmp 193](#)
[ip pp igmp static 194](#)
[ip pp inbound filter list 208](#)
[ip pp intrusion detection 153](#)
[ip pp intrusion detection notice-interval 155](#)
[ip pp intrusion detection repeat-control 155](#)
[ip pp intrusion detection report 156](#)
[ip pp intrusion detection threshold 156](#)
[ip pp mtu 140](#)
[ip pp nat descriptor 416](#)
[ip pp ospf area 477](#)
[ip pp ospf neighbor 480](#)
[ip pp pim sparse 194](#)
[ip pp rebound 141](#)
[ip pp remote address 167](#)
[ip pp remote address pool 168](#)
[ip pp rip auth key 177](#)
[ip pp rip auth key text 177](#)
[ip pp rip auth type 176](#)
[ip pp rip backup interface 180](#)
[ip pp rip connect interval 179](#)
[ip pp rip connect send 178](#)
[ip pp rip disconnect interval 180](#)
[ip pp rip disconnect send 179](#)
[ip pp rip filter 175](#)
[ip pp rip force-to-advertise 181](#)
[ip pp rip hold routing 178](#)
[ip pp rip hop 176](#)
[ip pp rip receive 174](#)
[ip pp rip send 174](#)
[ip pp rip trust gateway 172](#)
[ip pp secure filter 159](#)
[ip pp secure filter name 159](#)
[ip pp tcp mss limit 157](#)
[ip pp tcp window-scale 158](#)
[ip pp traffic list 197](#)

- ip pp traffic list threshold 199
- ip reassembly hold-time 167
- ip route 142
- ip route change log 159
- ip routing 138
- ip routing process 67
- ip simple-service 141
- ip stealth 282
- ip tos supersede 161
- ip tunnel address 292
- ip tunnel dpi filter 729
- ip tunnel forward filter 201
- ip tunnel igmp 193
- ip tunnel igmp static 194
- ip tunnel inbound filter list 208
- ip tunnel intrusion detection 153
- ip tunnel intrusion detection notice-interval 155
- ip tunnel intrusion detection repeat-control 155
- ip tunnel intrusion detection report 156
- ip tunnel intrusion detection threshold 156
- ip tunnel mtu 140
- ip tunnel nat descriptor 416
- ip tunnel ospf area 477
- ip tunnel ospf neighbor 480
- ip tunnel pim sparse 194
- ip tunnel rebound 141
- ip tunnel remote address 293
- ip tunnel rip auth key 177
- ip tunnel rip auth key text 177
- ip tunnel rip auth type 176
- ip tunnel rip filter 175
- ip tunnel rip force-to-advertise 181
- ip tunnel rip hop 176
- ip tunnel rip receive 174
- ip tunnel rip send 174
- ip tunnel rip trust gateway 172
- ip tunnel secure filter 159
- ip tunnel secure filter name 159
- ip tunnel tcp mss limit 157
- ip tunnel tcp window-scale 158
- ip tunnel traffic list 197
- ip tunnel traffic list threshold 199
- ipip keepalive log 366
- ipip keepalive use 366
- ipsec auto refresh 305
- ipsec ike always-on 307
- ipsec ike auth method 301
- ipsec ike backward-compatibility 321
- ipsec ike child-exchange type 335
- ipsec ike duration 336
- ipsec ike eap myname 303
- ipsec ike eap request 304
- ipsec ike eap send certreq 305
- ipsec ike encryption 316
- ipsec ike esp-encapsulation 332
- ipsec ike group 318
- ipsec ike hash 319
- ipsec ike keepalive log 315
- ipsec ike keepalive use 313
- ipsec ike license-key 330
- ipsec ike license-key use 331
- ipsec ike local address 312
- ipsec ike local id 313
- ipsec ike local name 311
- ipsec ike log 332
- ipsec ike message-id-control 334
- ipsec ike mode-cfg address 329
- ipsec ike mode-cfg address pool 328
- ipsec ike mode-cfg method 328
- ipsec ike nat-traversal 341
- ipsec ike negotiate-strictly 306
- ipsec ike negotiation receive 335
- ipsec ike payload type 320
- ipsec ike pfs 322
- ipsec ike pki file 303
- ipsec ike pre-shared-key 302
- ipsec ike proposal-limitation 333
- ipsec ike queue length 317
- ipsec ike remote address 309
- ipsec ike remote id 310
- ipsec ike remote name 308
- ipsec ike restrict-dangling-sa 340
- ipsec ike retry 307
- ipsec ike send info 322
- ipsec ike version 300
- ipsec ike xauth myname 323
- ipsec ike xauth request 327
- ipsec ipcomp type 344
- ipsec log illegal-spi 319
- ipsec refresh sa 339
- ipsec sa delete 342
- ipsec sa policy 337
- ipsec transport 348
- ipsec transport template 349
- ipsec tunnel 344
- ipsec tunnel fastpath-fragment-function follow df-bit 343
- ipsec tunnel outer df-bit 343
- ipsec use 300
- ipv6 dpi filter 728
- ipv6 filter 520
- ipv6 filter dynamic 523
- ipv6 icmp echo-reply send 283
- ipv6 icmp echo-reply send-only-linkup 284
- ipv6 icmp error-decrypted-ipsec send 287
- ipv6 icmp log 286
- ipv6 icmp packet-too-big send 287
- ipv6 icmp packet-too-big-for-truncated send 288
- ipv6 icmp parameter-problem send 284
- ipv6 icmp redirect receive 285
- ipv6 icmp redirect send 284
- ipv6 icmp time-exceeded send 285
- ipv6 icmp unreachable send 286
- ipv6 inbound filter 206
- ipv6 interface address 498
- ipv6 interface dad retry count 504
- ipv6 interface dhcp service 503
- ipv6 interface dpi filter 729
- ipv6 interface icmp-nd queue length 497
- ipv6 interface inbound filter list 208
- ipv6 interface mld 525
- ipv6 interface mld static 526
- ipv6 interface mtu 494
- ipv6 interface neighbor cache max entry 497
- ipv6 interface ospf area 531
- ipv6 interface prefix 500
- ipv6 interface prefix change log 502
- ipv6 interface rip filter 515
- ipv6 interface rip hop 514
- ipv6 interface rip receive 513
- ipv6 interface rip send 513
- ipv6 interface rip trust gateway 514
- ipv6 interface rtadv send 508
- ipv6 interface rtsol max-retransmit 510
- ipv6 interface secure filter 522
- ipv6 interface tcp mss limit 495
- ipv6 interface tcp window-scale 495
- ipv6 interface vrrp 518
- ipv6 interface vrrp shutdown trigger 519
- ipv6 max auto address 504
- ipv6 multicast routing process 527
- ipv6 nd ns-trigger-dad 528
- ipv6 nd ra-rdnss 507
- ipv6 ospf area 530
- ipv6 ospf area network 531

ipv6 ospf configure refresh 529
 ipv6 ospf export 535
 ipv6 ospf export from ospf 535
 ipv6 ospf import 537
 ipv6 ospf import from 537
 ipv6 ospf log 539
 ipv6 ospf preference 534
 ipv6 ospf router id 529
 ipv6 ospf use 529
 ipv6 ospf virtual-link 533
 ipv6 policy address group 211
 ipv6 policy filter 213
 ipv6 policy filter set 215
 ipv6 policy filter set enable 215
 ipv6 policy filter set switch 216
 ipv6 policy interface group 210
 ipv6 policy service 210
 ipv6 policy service group 212
 ipv6 pp address 498
 ipv6 pp dad retry count 504
 ipv6 pp dhcp service 503
 ipv6 pp dpi filter 729
 ipv6 pp inbound filter list 208
 ipv6 pp mld 525
 ipv6 pp mld static 526
 ipv6 pp mtu 494
 ipv6 pp ospf area 531
 ipv6 pp prefix 500
 ipv6 pp prefix change log 502
 ipv6 pp rip connect interval 516
 ipv6 pp rip connect send 515
 ipv6 pp rip disconnect interval 517
 ipv6 pp rip disconnect send 516
 ipv6 pp rip filter 515
 ipv6 pp rip hold routing 517
 ipv6 pp rip hop 514
 ipv6 pp rip receive 513
 ipv6 pp rip send 513
 ipv6 pp rip trust gateway 514
 ipv6 pp rtadv send 508
 ipv6 pp rtsol max-retransmit 510
 ipv6 pp secure filter 522
 ipv6 pp tcp mss limit 495
 ipv6 pp tcp window-scale 495
 ipv6 prefix 505
 ipv6 reassembly hold-time 498
 ipv6 rh0 discard 496
 ipv6 rip preference 517
 ipv6 rip use 512
 ipv6 route 510
 ipv6 route change log 512
 ipv6 routing 494
 ipv6 routing process 496
 ipv6 source address selection rule 505
 ipv6 stealth 288
 ipv6 tunnel address 498
 ipv6 tunnel dhcp service 503
 ipv6 tunnel dpi filter 729
 ipv6 tunnel inbound filter list 208
 ipv6 tunnel mld 525
 ipv6 tunnel mld static 526
 ipv6 tunnel mtu 494
 ipv6 tunnel ospf area 531
 ipv6 tunnel prefix 500
 ipv6 tunnel prefix change log 502
 ipv6 tunnel rip filter 515
 ipv6 tunnel rip receive 513
 ipv6 tunnel rip send 513
 ipv6 tunnel secure filter 522
 ipv6 tunnel tcp mss limit 495
 ipv6 tunnel tcp window-scale 495
 isdn arrive permit 119

isdn auto connect 119
 isdn call block time 120
 isdn call permit 120
 isdn call prohibit time 121
 isdn callback mscbcu user-specify 123
 isdn callback permit 122
 isdn callback permit type 122
 isdn callback request 121
 isdn callback request type 122
 isdn callback response time 123
 isdn callback wait time 124
 isdn disconnect input time 126
 isdn disconnect interval time 127
 isdn disconnect output time 126
 isdn disconnect policy 124
 isdn disconnect time 124
 isdn dsu 113
 isdn fast disconnect time 125
 isdn forced disconnect time 125
 isdn local address 112
 isdn piafs arrive 115
 isdn piafs call 116
 isdn piafs control 115
 isdn remote address 118
 isdn remote call order 119
 isdn terminator 113

J

jate number 611

L

l2tp always-on 356
 l2tp hostname 356
 l2tp keepalive log 355
 l2tp keepalive use 354
 l2tp local router-id 357
 l2tp remote end-id 358
 l2tp remote router-id 357
 l2tp service 352
 l2tp syslog 355
 l2tp tunnel auth 353
 l2tp tunnel disconnect time 353
 lan backup 187
 lan backup recovery time 188
 lan count-hub-overflow 68
 lan keepalive interval 189
 lan keepalive log 190
 lan keepalive use 189
 lan link-aggregation static 75
 lan linkup send-wait-time 68
 lan port-mirroring 69
 lan receive-buffer-size 76
 lan shutdown 67
 lan type 70
 lan-map log 661
 lan-map snapshot use 660
 lan-map sysname 662
 lan-map terminal watch interval 659
 leased backup 117
 leased keepalive down 172
 less 43
 less config 778
 less config ap 778
 less config list 781
 less config pp 779
 less config switch 779
 less config tunnel 780
 less exec list 785
 less file list 781
 less log 827

license authentication go [774](#)
 license authentication retry interval [774](#)
 line masterclock [65](#)
 line type [112](#), [136](#)
 load [774](#)
 login password [46](#)
 login password encrypted [46](#)
 login radius use [47](#)
 login timer [77](#)
 login user [47](#)
 lua [649](#)
 lua use [649](#)
 luac [650](#)

M

macro [104](#)
 mail notify [547](#)
 mail notify status exec [773](#)
 mail server name [543](#)
 mail server pop [544](#)
 mail server smtp [543](#)
 mail server timeout [545](#)
 mail template [545](#)
 mail-notify status exec [542](#)
 mail-notify status from [540](#)
 mail-notify status server [540](#)
 mail-notify status subject [541](#)
 mail-notify status timeout [541](#)
 mail-notify status to [541](#)
 mail-notify status type [542](#)
 mail-notify status use [540](#)
 make directory [755](#)
 mobile access limit connection length [621](#)
 mobile access limit connection time [622](#)
 mobile access limit duration [622](#)
 mobile access limit length [617](#)
 mobile access limit time [618](#)
 mobile access-point name [616](#)
 mobile arrive permit [623](#)
 mobile arrive use [623](#)
 mobile auto connect [615](#)
 mobile call prohibit auth-error count [619](#)
 mobile call type [612](#)
 mobile carrier mode [627](#)
 mobile dial number [616](#)
 mobile disconnect input time [615](#)
 mobile disconnect output time [616](#)
 mobile disconnect time [615](#)
 mobile display caller id [620](#)
 mobile firmware update go [627](#)
 mobile pin code [612](#)
 mobile signal-strength [624](#)
 mobile signal-strength go [624](#)
 mobile syslog [620](#)
 mobile use [611](#)

N

nat descriptor address inner [419](#)
 nat descriptor address outer [418](#)
 nat descriptor backward-compatibility [416](#)
 nat descriptor ftp port [424](#)
 nat descriptor log [425](#)
 nat descriptor masquerade incoming [423](#)
 nat descriptor masquerade port range [423](#)
 nat descriptor masquerade remove df-bit [426](#)
 nat descriptor masquerade rlogin [420](#)
 nat descriptor masquerade session limit [427](#)
 nat descriptor masquerade session limit total [427](#)
 nat descriptor masquerade static [420](#)
 nat descriptor masquerade ttl hold [422](#)

nat descriptor masquerade unconvertible port [425](#)
 nat descriptor sip [426](#)
 nat descriptor static [419](#)
 nat descriptor timer [421](#)
 nat descriptor type [417](#)
 nat46 ip address pool [443](#)
 nat46 ipv6 prefix [443](#)
 nat46 static [444](#)
 netvolante-dns auto hostname [563](#)
 netvolante-dns auto hostname pp [563](#)
 netvolante-dns auto save [567](#)
 netvolante-dns delete go [560](#)
 netvolante-dns delete go pp [560](#)
 netvolante-dns get hostname list [561](#)
 netvolante-dns get hostname list pp [561](#)
 netvolante-dns go [559](#)
 netvolante-dns go pp [559](#)
 netvolante-dns hostname host [561](#)
 netvolante-dns hostname host pp [561](#)
 netvolante-dns port [560](#)
 netvolante-dns register timer [566](#)
 netvolante-dns retry interval [565](#)
 netvolante-dns retry interval pp [565](#)
 netvolante-dns server [564](#)
 netvolante-dns server update address port [565](#)
 netvolante-dns server update address use [565](#)
 netvolante-dns set hostname [564](#)
 netvolante-dns timeout [562](#)
 netvolante-dns timeout pp [562](#)
 netvolante-dns use [559](#)
 netvolante-dns use pp [559](#)
 ngn radius account callee [390](#)
 ngn radius account caller [390](#)
 ngn radius auth password [390](#)
 ngn renumbering link-refresh [391](#)
 ngn type [385](#)
 nslookup [765](#)
 ntp backward-compatibility [56](#)
 ntp local address [56](#)
 ntpdate [55](#)

O

operation button function download [605](#)
 operation execute batch permit [605](#)
 operation external-memory download permit [599](#)
 operation http revision-up permit [85](#)
 operation usb-download permit [574](#)
 ospf area [474](#)
 ospf area network [474](#)
 ospf area stubhost [475](#)
 ospf configure refresh [468](#)
 ospf export filter [471](#)
 ospf export from ospf [470](#)
 ospf import filter [472](#)
 ospf import from [470](#)
 ospf log [481](#)
 ospf merge equal cost stub [481](#)
 ospf preference [468](#)
 ospf reric interval [482](#)
 ospf router id [469](#)
 ospf use [468](#)
 ospf virtual-link [476](#)

P

packetdump [62](#)
 packetdump pp [62](#)
 ping [762](#)
 ping6 [763](#)
 pki certificate file [350](#)
 pki crl file [351](#)

pp always-on 117
 pp auth accept 235, 362
 pp auth multi connect prohibit 237
 pp auth myname 236
 pp auth request 235, 362
 pp auth username 234
 pp backup 186
 pp backup pp 186
 pp backup recovery time 187
 pp backup tunnel 186
 pp bind 114, 137, 359, 614
 pp disable 758
 pp enable 757
 pp encapsulation 129
 pp keepalive interval 169
 pp keepalive log 171
 pp keepalive use 170
 pp name 552
 pp select 740
 ppp bacp maxconfigure 251
 ppp bacp maxfailure 251
 ppp bacp maxterminate 251
 ppp bacp restart 251
 ppp bap maxretry 252
 ppp bap restart 252
 ppp ccp maxconfigure 247
 ppp ccp maxfailure 247
 ppp ccp maxterminate 247
 ppp ccp no-encryption 365
 ppp ccp restart 246
 ppp ccp type 246
 ppp chap maxchallenge 241
 ppp chap restart 241
 ppp ipcp ipaddress 242
 ppp ipcp maxconfigure 243
 ppp ipcp maxfailure 243
 ppp ipcp maxterminate 243
 ppp ipcp msex 244
 ppp ipcp remote address check 245
 ppp ipcp restart 243
 ppp ipcp vjc 242
 ppp ipv6cp use 248
 ppp lcp accm 619
 ppp lcp acfc 237
 ppp lcp magicnumber 238
 ppp lcp maxconfigure 240
 ppp lcp maxfailure 240
 ppp lcp maxterminate 239
 ppp lcp mru 238
 ppp lcp pfc 239
 ppp lcp restart 239
 ppp lcp silent 240
 ppp mp control 248
 ppp mp divide 250
 ppp mp interleave 451
 ppp mp load threshold 249
 ppp mp maxlink 249
 ppp mp minlink 250
 ppp mp timer 250
 ppp mp use 248
 ppp msccp maxretry 245
 ppp msccp restart 245
 ppp pap maxauthreq 241
 ppp pap restart 241
 pppoe access concentrator 253
 pppoe auto connect 253
 pppoe auto disconnect 253
 pppoe disconnect time 255
 pppoe invalid-session forced close 256
 pppoe padi maxretry 254
 pppoe padi restart 254
 pppoe padr maxretry 254

pppoe padr restart 254
 pppoe pass-through member 256
 pppoe service-name 255
 pppoe tcp mss limit 255
 pppoe use 252
 pptp call-id mode 361
 pptp hostname 360
 pptp keepalive interval 364
 pptp keepalive log 364
 pptp keepalive use 363
 pptp service 359
 pptp service type 360
 pptp syslog 363
 pptp tunnel disconnect time 363
 pptp vendorname 361
 pptp window size 361
 pri leased channel 136
 pri loopback active 768
 pri loopback passive 769
 provider auto connect forced disable 556
 provider dns server 553
 provider dns server pp 554
 provider filter routing 554
 provider interface bind 557
 provider interface dns server 554
 provider interface name 555
 provider ipv6 connect pp 557
 provider ntp server 556
 provider ntpdate 556
 provider select 553
 provider set 552
 provider type 552

Q

qac-tm client permit 646
 qac-tm client port 644
 qac-tm client refresh go 647
 qac-tm client update 644
 qac-tm port 645
 qac-tm redirect 644
 qac-tm server 642
 qac-tm server refresh go 647
 qac-tm unqualified client access control 645
 qac-tm use 642
 qac-tm version margin 643
 qac-tm warning url 646
 queue class filter 447
 queue interface class control 457
 queue interface class filter list 452
 queue interface class property 455
 queue interface default class 454
 queue interface default class secondary 455
 queue interface length 453
 queue interface length secondary 454
 queue interface type 450
 queue pp class filter list 452
 queue pp class property 455
 queue pp default class 454
 queue pp length 453
 queue pp type 450
 queue tunnel class filter list 452
 queue tunnel default class 454
 quit 741

R

radius account 412
 radius account port 414
 radius account server 413
 radius auth 412
 radius auth port 414

radius auth server 413
radius retry 415
radius secret 415
radius server 413
rdate 55
remote setup 747
remote setup accept 748
rename 756
restart 758
rip advertise mode 177
rip filter rule 182
rip preference 173
rip timer 182
rip use 172
rollback timer 775
rotate external-memory syslog 773
rtfs format 111
rtfs garbage-collect 111

S

save 741
schedule at 576
scp 97
sd use 593
security class 53
set 103
set-default-config 746
set-default-exec 746
set-serial-baudrate 746
sftpd host 95
show account 828
show account mobile 829
show account ngn data 829
show account pp 828
show account tunnel 829
show alias 786
show arp 788
show bridge learning 792
show command 45
show command history 830
show config 778
show config ap 778
show config difference 780
show config list 781
show config pp 779
show config switch 779
show config tunnel 780
show copyright 826
show diagnosis config port access 724
show diagnosis config port map 724
show dlci 789
show dns cache 821
show dpi application 735
show dpi cache 735
show dpi category 736
show dpi statistics 733
show environment 778
show exec list 785
show file list 781
show history 830
show ip connection 800
show ip connection pp 800
show ip connection tunnel 800
show ip intrusion detection 803
show ip intrusion detection pp 803
show ip intrusion detection tunnel 803
show ip mroute 807
show ip rip table 790
show ip route 789
show ip secure filter 784
show ip secure filter pp 784
show ip secure filter tunnel 784
show ip traffic list 199
show ip traffic list pp 199
show ip traffic list tunnel 199
show ipsec sa 792
show ipsec sa gateway 792
show ipv6 address 782
show ipv6 address pp 782
show ipv6 address tunnel 782
show ipv6 connection 802
show ipv6 connection pp 802
show ipv6 connection tunnel 802
show ipv6 mroute fib 809
show ipv6 neighbor cache 791
show ipv6 ospf 812
show ipv6 rip table 791
show ipv6 route 791
show ipv6 secure filter 784
show ipv6 secure filter pp 784
show ipv6 secure filter tunnel 784
show lan-map 823
show line masterclock 783
show log 827
show macro 786
show nat descriptor address 794
show nat descriptor interface address 795
show nat descriptor interface address pp 795
show nat descriptor interface address tunnel 795
show nat descriptor interface bind 795
show nat descriptor interface bind pp 795
show nat descriptor interface bind tunnel 795
show nat descriptor masquerade port summary 796
show nat descriptor masquerade session statistics 797
show nat descriptor masquerade session summary 796
show pki certificate summary 793
show pki crl 793
show pp connect time 804
show pppoe pass-through learning 804
show set 785
show sshd authorized-keys 94
show sshd host key 89
show sshd public key 783
show status 788
show status backup 800
show status bgp neighbor 799
show status boot 818
show status boot all 818
show status boot list 819
show status cloud vpn 371
show status cooperation 812
show status dhcp 799
show status dhcpc 800
show status dpi 737
show status ethernet filter 205
show status external-memory 817
show status heartbeat 816
show status heartbeat2 588
show status heartbeat2 id 588
show status heartbeat2 name 588
show status ip igmp 808
show status ip inbound filter 813
show status ip keepalive 803
show status ip pim sparse 808
show status ip policy filter 813
show status ip policy service 814
show status ipip 798
show status ipv6 dhcp 800
show status ipv6 inbound filter 813
show status ipv6 mld 809
show status ipv6 policy filter 813
show status ipv6 policy service 814
show status l2tp 797

show status license 821
 show status license authentication 822
 show status lua 650
 show status mail service 807
 show status mobile signal-strength 625
 show status nat46 table 444
 show status netvolante-dns 804
 show status netvolante-dns pp 804
 show status ngn 392
 show status ospf 798
 show status packet-buffer 810
 show status packet-scheduling 822
 show status pp 788
 show status pptp 798
 show status qac-tm 647
 show status qac-tm client 647
 show status qac-tm qualified 647
 show status qac-tm server 647
 show status qac-tm unqualified 647
 show status qos 811
 show status remote setup 816
 show status rdfs 818
 show status sd 817
 show status status-led 823
 show status switch control 819
 show status switch control route backup 820
 show status switching-hub macaddress 805
 show status tunnel 806
 show status upnp 806
 show status usbhost 816
 show status user 809
 show status user history 810
 show status vlan 807
 show status vrrp 794
 show status yno 716
 show status yno las 720
 show techinfo 817
 show url filter 814
 show url filter external-database 815
 show url filter external-database id 815
 show url filter external-database pp 815
 show url filter external-database tunnel 815
 show url filter pp 814
 show url filter tunnel 814
 sip 100rel 374
 sip arrive address check 377
 sip arrive ringing p-n-uatype 376
 sip arrive session timer method 376
 sip arrive session timer refresher 375
 sip ip protocol 374
 sip log 378
 sip outer address 378
 sip response code busy 377
 sip server 378
 sip server 100rel 382
 sip server call own permit 385
 sip server call remote domain 382
 sip server connect 765
 sip server dial number-only 384
 sip server disconnect 766
 sip server display name 381
 sip server pilot address 380
 sip server privacy 380
 sip server qvalue 384
 sip server register request-uri 383
 sip server register timer 383
 sip server session timer 379
 sip session timer 373
 sip use 373
 sip user agent 375
 snmp community read-only 394
 snmp community read-write 394
 snmp display ipcp force 407
 snmp host 393
 snmp ifindex switch static index 408
 snmp local address 401
 snmp syscontact 402
 snmp syslocation 402
 snmp sysname 402
 snmp trap community 395
 snmp trap cpu threshold 403
 snmp trap delay-timer 404
 snmp trap enable snmp 403
 snmp trap enable switch 409
 snmp trap enable switch common 410
 snmp trap host 394
 snmp trap link-updown separate-l2switch-port 407
 snmp trap memory threshold 404
 snmp trap mobile signal-strength 408
 snmp trap send linkdown 405
 snmp trap send linkdown pp 405
 snmp trap send linkdown tunnel 405
 snmp yrifppdisplayatmib2 406
 snmp yrifswitchdisplayatmib2 407
 snmp yriftunneldisplayatmib2 406
 snmp yrswindex switch static index 409
 snmpv2c community read-only 396
 snmpv2c community read-write 396
 snmpv2c host 395
 snmpv2c trap community 397
 snmpv2c trap host 396
 snmpv3 context name 398
 snmpv3 engine id 397
 snmpv3 host 399
 snmpv3 trap host 401
 snmpv3 usm user 398
 snmpv3 vacm access 400
 snmpv3 vacm view 399
 snrpd host 591
 snrpd service 591
 speed 446
 speed pp 446
 ssh 96
 ssh encrypt algorithm 97
 ssh known hosts 98
 sshd auth method 91
 sshd authorized-keys filename 92
 sshd client alive 90
 sshd encrypt algorithm 90
 sshd hide openssh version 91
 sshd host 87
 sshd host key generate 88
 sshd listen 87
 sshd service 86
 sshd session 88
 statistics 725
 switch config directory 666
 switch config filename 666
 switch control config get 667
 switch control config set 668
 switch control firmware upload go 665
 switch control function default 664
 switch control function execute 664
 switch control function execute clear-counter 698
 switch control function execute clear-macaddress-table 681
 switch control function execute reset-loopdetect 703
 switch control function execute restart 673
 switch control function execute restart-poe-supply 706
 switch control function execute start-poe-supply 706
 switch control function execute stop-poe-supply 707
 switch control function get 663
 switch control function get boot-rom-version 668
 switch control function get counter-frame-rx-type 693
 switch control function get counter-frame-tx-type 695

switch control function get energy-saving 670
 switch control function get firmware-revision 669
 switch control function get lag-type 673
 switch control function get led-brightness 671
 switch control function get loopdetect-count 699
 switch control function get loopdetect-linkdown 700
 switch control function get loopdetect-port-use 701
 switch control function get loopdetect-recovery-timer 700
 switch control function get loopdetect-time 699
 switch control function get loopdetect-use-control-packet 701
 switch control function get macaddress-aging 679
 switch control function get macaddress-aging-timer 680
 switch control function get mirroring-dest 691
 switch control function get mirroring-src-rx 692
 switch control function get mirroring-src-tx 692
 switch control function get mirroring-use 691
 switch control function get model-name 669
 switch control function get poe-class 703
 switch control function get port-auto-crossover 675
 switch control function get port-blocking-control-packet 677
 switch control function get port-blocking-data-packet 677
 switch control function get port-flow-control 676
 switch control function get port-speed 674
 switch control function get port-speed-downshift 675
 switch control function get port-use 674
 switch control function get qos-dscp-remark-class 687
 switch control function get qos-dscp-remark-type 686
 switch control function get qos-policing-speed 688
 switch control function get qos-policing-use 688
 switch control function get qos-shaping-speed 689
 switch control function get qos-shaping-use 689
 switch control function get qos-speed-unit 687
 switch control function get serial-number 669
 switch control function get status-combo-port 678
 switch control function get status-counter-frame-rx 697
 switch control function get status-counter-frame-tx 697
 switch control function get status-counter-octet-rx 697
 switch control function get status-counter-octet-tx 698
 switch control function get status-fan 672
 switch control function get status-fan-rpm 672
 switch control function get status-led-mode 671
 switch control function get status-loopdetect-port 702
 switch control function get status-loopdetect-recovery-timer 702
 switch control function get status-macaddress-addr 680
 switch control function get status-macaddress-port 681
 switch control function get status-poe-detect-class 704
 switch control function get status-poe-state 704
 switch control function get status-poe-supply 705
 switch control function get status-poe-supply-detail 705
 switch control function get status-poe-supply-total 706
 switch control function get status-poe-temperature 705
 switch control function get status-port-sfp-rx-power 678
 switch control function get status-port-speed 679
 switch control function get system-macaddress 669
 switch control function get system-name 670
 switch control function get system-uptime 673
 switch control function get vlan-access 683
 switch control function get vlan-id 683
 switch control function get vlan-multiple 685
 switch control function get vlan-multiple-use 685
 switch control function get vlan-port-mode 683
 switch control function get vlan-trunk 684
 switch control function set 663
 switch control function set counter-frame-rx-type 693
 switch control function set counter-frame-tx-type 695
 switch control function set energy-saving 670
 switch control function set led-brightness 671
 switch control function set loopdetect-count 699
 switch control function set loopdetect-linkdown 700
 switch control function set loopdetect-port-use 701
 switch control function set loopdetect-recovery-timer 700
 switch control function set loopdetect-time 699

switch control function set loopdetect-use-control-packet 701
 switch control function set macaddress-aging 679
 switch control function set macaddress-aging-timer 680
 switch control function set mirroring-dest 691
 switch control function set mirroring-src-rx 692
 switch control function set mirroring-src-tx 692
 switch control function set mirroring-use 691
 switch control function set poe-class 703
 switch control function set port-auto-crossover 675
 switch control function set port-blocking-control-packet 677
 switch control function set port-blocking-data-packet 677
 switch control function set port-flow-control 676
 switch control function set port-speed 674
 switch control function set port-speed-downshift 675
 switch control function set port-use 674
 switch control function set qos-dscp-remark-class 687
 switch control function set qos-dscp-remark-type 686
 switch control function set qos-policing-speed 688
 switch control function set qos-policing-use 688
 switch control function set qos-shaping-speed 689
 switch control function set qos-shaping-use 689
 switch control function set qos-speed-unit 687
 switch control function set system-name 670
 switch control function set vlan-access 683
 switch control function set vlan-id 683
 switch control function set vlan-multiple 685
 switch control function set vlan-multiple-use 685
 switch control function set vlan-port-mode 683
 switch control function set vlan-trunk 684
 switch control mode 657
 switch control route backup 665
 switch control use 658
 switch control watch interval 659
 switch select 662
 syslog debug 61
 syslog execute command 62
 syslog facility 59
 syslog host 59
 syslog info 60
 syslog local address 61
 syslog notice 60
 syslog srport 61
 system cpu threshold 66
 system led brightness 102
 system memory threshold 66
 system packet-buffer 98
 system packet-scheduling 106
 system packet-scheduling filter 107
 system packet-scheduling filter list 109
 system temperature threshold 66

T

take lan-map snapshot 661
 tcp log 80
 tcp session limit 158
 telnet 766
 telnetd host 64
 telnetd listen 63
 telnetd service 63
 telnetd session 65
 terminate lua 652
 terminate lua file 652
 tftp host 78
 time 54
 timezone 54
 traceroute 764
 traceroute6 764
 tunnel backup 345
 tunnel backup pp 345
 tunnel backup tunnel 345
 tunnel disable 290

tunnel enable 290
 tunnel encapsulation 292
 tunnel endpoint address 294
 tunnel endpoint local address 294
 tunnel endpoint name 295
 tunnel endpoint remote address 293
 tunnel map-e type 297
 tunnel multipoint limit 296
 tunnel multipoint local name 296
 tunnel multipoint server 295
 tunnel name 552
 tunnel ngn arrive permit 387
 tunnel ngn bandwidth 386
 tunnel ngn call permit 388
 tunnel ngn disconnect time 386
 tunnel ngn fallback 389
 tunnel ngn interface 388
 tunnel ngn radius auth 389
 tunnel select 740
 tunnel template 346
 tunnel translation 297
 tunnel type 291

U

upnp external address refer 568
 upnp external address refer pp 568
 upnp port mapping timer 569
 upnp port mapping timer type 569
 upnp syslog 570
 upnp use 568
 url filter 219
 url filter external-database access failure 226
 url filter external-database auth retry 232
 url filter external-database category 224
 url filter external-database id 230
 url filter external-database id activate go 230
 url filter external-database id check go 231
 url filter external-database ipaddress access 227
 url filter external-database log 229
 url filter external-database lookup specified extension 228
 url filter external-database lookup specified extension list 228
 url filter external-database proxy server 224
 url filter external-database register url 230
 url filter external-database reject 227
 url filter external-database reputation 225
 url filter external-database server 223
 url filter external-database update 232
 url filter external-database use 222
 url filter log 222
 url filter port 220
 url filter reject 221
 url filter use 221
 url interface filter 220
 url pp filter 220
 url tunnel filter 220
 usbhost config filename 574
 usbhost exec filename 575
 usbhost modem flow control 626
 usbhost modem initialize 626
 usbhost overcurrent duration 575
 usbhost statistics filename prefix 572
 usbhost syslog filename 571
 usbhost use 571
 user attribute 49

V

vlan interface 802.1q 579
 vlan port mapping 579

W

wan access limit connection length 635
 wan access limit connection time 636
 wan access limit duration 636
 wan access limit length 633
 wan access limit time 634
 wan access-point name 632
 wan always-on 631
 wan auth myname 628
 wan auto connect 629
 wan bind 629
 wan disconnect input time 630
 wan disconnect output time 631
 wan disconnect time 630
 wins server 244
 wol send 770

Y

yno access code 713
 yno gui-forwarder timeout 715
 yno https-proxy 715
 yno las connection keepalive 719
 yno las request retry 719
 yno las request timeout 719
 yno las syslog queue length 718
 yno log 714
 yno use 713
 yno xmpp connection keepalive 721
 yno zero-config id 716