YAMAHA

FWX120

ファイアウォール

Rev.11.03.27

コマンドリファレンス

ヤマハFWX120をお買い上げいただきありがとうございます。
お使いになる前に本書をよくお読みになり、正しく設置や設定を行ってください。
本書中の警告や注意を必ず守り、正しく安全にお使いください。
本書はなくさないように、大切に保管してください。

目次

序文 : はじめに 25
第 1 章 : コマンドリファレンスの見方 26
1.1 対応するプログラムのリビジョン 26
1.2 コマンドリファレンスの見方 26
1.3 インターフェース名について 26
1.4 no で始まるコマンドの入力形式について 27
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 27
1.6 相手先情報番号のモデルによる違いについて 27
1.7 工場出荷設定値について 27
第 2 章 : コマンドの使い方 28
2.1 コンソールについて 28
2.1.1 コンソールによる設定手順 28
2.1.2 CONSOLE または SERIAL ポートからの設定 29
2.1.3 TELNET による設定 32
2.2 SSH サーバーについて 33
2.2.1 SSH サーバー機能の使用に当たっての注意事項 33
2.2.2 SSH サーバーの設定 33
2.3 TFTP について 34
2.3.1 TFTP による設定手順 34
2.3.2 設定ファイルの読み出し 35
2.3.3 設定ファイルの書き込み 35
2.4 コンソール使用時のキーボード操作について 36
2.5 「show」で始まるコマンド 37
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 37
2.5.2 show コマンドの表示内容を見やすくする 38
2.5.3 外部メモリへのリダイレクト機能 39
第 3 章 : ヘルプ 41
3.1 コンソールに対する簡易説明の表示 41
3.2 コマンド一覧の表示 41
第 4 章 : 機器の設定 42
4.1 ログインパスワードの設定 42
4.2 ログインパスワードの暗号化保存 42
4.3 管理パスワードの設定 42
4.4 管理パスワードの暗号化保存 42
4.5 ログインユーザー名とログインパスワードの設定 42
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 43
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 43
4.8 ユーザーの属性を設定 44
4.9 他のユーザーの接続の強制切断 46
4.10 セキュリティークラスの設定 46
4.11 タイムゾーンの設定 47
4.12 現在の日付けの設定 48
4.13 現在の時刻の設定 48
4.14 リモートホストによる時計の設定 48
4.15 NTP による時計の設定 49

4.16 NTP パケットを送信するときの始点 IP アドレスの設定 49
4.17 Stratum 0 の NTP サーバーとの時刻同期を許可する設定 49
4.18 コンソールのプロンプト表示の設定 50
4.19 コンソールの言語とコードの設定 50
4.20 コンソールの表示文字数の設定 50
4.21 コンソールの表示行数の設定 51
4.22 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 51
4.23 SYSLOG を受けるホストの IP アドレスの設定 51
4.24 SYSLOG ファシリティの設定 52
4.25 NOTICE タイプの SYSLOG を出力するか否かの設定 52
4.26 INFO タイプの SYSLOG 出力の設定 52
4.27 DEBUG タイプの SYSLOG を出力するか否かの設定 53
4.28 SYSLOG を送信する時の始点 IP アドレスの設定 53
4.29 SYSLOG パケットの始点ポート番号の設定 53
4.30 SYSLOG に実行コマンドを出力するか否かの設定 53
4.31 TELNET サーバー機能の ON/OFF の設定 54
4.32 TELNET サーバー機能の listen ポートの設定 54
4.33 TELNET サーバーへアクセスできるホストの IP アドレスの設定 54
4.34 TELNET サーバーへ同時に接続できるユーザー数の設定 55
4.35 ファストパス機能の設定 55
4.36 LAN インターフェースの動作設定 56
4.37 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 56
4.38 LAN インターフェースのリンクアップ後の送信抑制時間の設定 56
4.39 ポートミラーリング機能の設定 57
4.40 LAN インターフェースの動作タイプの設定 57
4.41 ログインタイマの設定 61
4.42 TFTP によりアクセスできるホストの IP アドレスの設定 62
4.43 Magic Packet を LAN に中継するか否かの設定 62
4.44 インターフェースまたはシステムの説明の設定 63
4.45 TCP のコネクションレベルの syslog を出力するか否かの設定 63
4.46 HTTP リビジョンアップ実行を許可するか否かの設定 65
4.47 HTTP リビジョンアップ用 URL の設定 66
4.48 HTTP リビジョンアップ用 Proxy サーバーの設定 66
4.49 HTTP リビジョンアップ処理のタイムアウトの設定 66
4.50 リビジョンダウンを許可するか否かの設定 67
4.51 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 67
4.52 リビジョンアップ実行のスケジュール 67
4.53 SSH サーバー機能の ON/OFF の設定 68
4.54 SSH サーバー機能の listen ポートの設定 69
4.55 SSH サーバーへアクセスできるホストの IP アドレスの設定 69
4.56 SSH サーバーへ同時に接続できるユーザー数の設定 69
4.57 SSH サーバーホスト鍵の設定 70
4.58 SSH サーバーで利用可能な暗号アルゴリズムの設定 70
4.59 SSH クライアントの生存確認 71
4.60 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 71
4.61 SFTP サーバーへアクセスできるホストの IP アドレスの設定 72
4.62 SSH クライアント 72
4.63 SCP クライアント 73
4.64 SSH クライアントで利用可能な暗号アルゴリズムの設定 74

4.65 SSH サーバーの公開鍵情報を保存するファイルの設定 74
4.66 パケットバッファのパラメータを変更する 74
4.67 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 75
4.68 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 76
4.69 microSD 機能に関連するアラームを鳴らすか否かの設定 76
4.70 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 76
4.71 起動時のアラーム音を鳴らすか否かの設定 76
4.72 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 77
4.73 LED の輝度を調整する 77
4.74 環境変数の設定 77

第 5 章 : ヤマハルーター用ファイルシステム RTFS 79

5.1 RTFS のフォーマット 79
5.2 RTFS のガベージコレクト 79

第 6 章 : IP の設定 80

6.1 インターフェース共通の設定 80
6.1.1 IP パケットを扱うか否かの設定 80
6.1.2 IP アドレスの設定 80
6.1.3 セカンダリ IP アドレスの設定 81
6.1.4 インターフェースの MTU の設定 82
6.1.5 同一インターフェースに折り返すパケットを送信するか否かの設定 82
6.1.6 echo,discard,time サービスを動作させるか否かの設定 83
6.1.7 IP の静的経路情報の設定 83
6.1.8 IP パケットのフィルターの設定 85
6.1.9 フィルターセットの定義 88
6.1.10 Source-route オプション付き IP パケットをフィルターアウトするか否かの設定 88
6.1.11 ディレクテッドブロードキャストパケットをフィルターアウトするか否かの設定 89
6.1.12 動的フィルターの定義 89
6.1.13 動的フィルターのタイムアウトの設定 90
6.1.14 FQDN フィルターで使用するキャッシュのタイマーの設定 91
6.1.15 侵入検知機能の動作の設定 92
6.1.16 1 秒間に侵入検知情報を通知する頻度の設定 93
6.1.17 重複する侵入検知情報の通知抑制の設定 93
6.1.18 侵入検知情報の最大表示件数の設定 93
6.1.19 TCP セッションの MSS 制限の設定 94
6.1.20 TCP ウィンドウ・スケール・オプション を変更する 94
6.1.21 ルーターが端点となる TCP のセッション数の設定 95
6.1.22 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 95
6.1.23 フィルタリングによるセキュリティーの設定 96
6.1.24 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 97
6.1.25 IP パケットの TOS フィールドの書き換えの設定 97
6.1.26 代理 ARP の設定 98
6.1.27 ARP エントリーの寿命の設定 98
6.1.28 静的 ARP エントリーの設定 99
6.1.29 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 99
6.1.30 ARP エントリーの変化をログに残すか否かの設定 100
6.1.31 implicit 経路の優先度の設定 100
6.1.32 フローテーブルの各エントリーの寿命を設定する 100
6.2 PP 側の設定 101
6.2.1 PP 側 IP アドレスの設定 101

6.2.2 リモート IP アドレスプールの設定 102
6.2.3 PP 経由のキープアライブの時間間隔の設定 102
6.2.4 PP 経由のキープアライブを使用するか否かの設定 103
6.2.5 PP 経由のキープアライブのログをとるか否かの設定 104
6.2.6 常時接続の設定 104
6.3 RIP の設定 105
6.3.1 RIP を使用するか否かの設定 105
6.3.2 RIP に関して信用できるゲートウェイの設定 105
6.3.3 RIP による経路の優先度の設定 106
6.3.4 RIP パケットの送信に関する設定 106
6.3.5 RIP パケットの受信に関する設定 107
6.3.6 RIP のフィルタリングの設定 107
6.3.7 RIP で加算するホップ数の設定 108
6.3.8 RIP2 での認証の設定 108
6.3.9 RIP2 での認証キーの設定 109
6.3.10 回線切断時の経路保持の設定 109
6.3.11 回線接続時の PP 側の RIP の動作の設定 110
6.3.12 回線接続時の PP 側の RIP 送出の時間間隔の設定 110
6.3.13 回線切断時の PP 側の RIP の動作の設定 110
6.3.14 回線切断時の PP 側の RIP 送出の時間間隔の設定 111
6.3.15 バックアップ時の RIP の送信元インターフェース切り替えの設定 111
6.3.16 RIP で強制的に経路を広告する 112
6.3.17 RIP2 でのフィルターの比較方法 112
6.3.18 RIP のタイマーを調整する 113
6.4 VRRP の設定 113
6.4.1 インターフェース毎の VRRP の設定 113
6.4.2 シャットダウントリガの設定 114
6.5 バックアップの設定 115
6.5.1 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 115
6.5.2 バックアップからの復帰待ち時間の設定 116
6.5.3 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 116
6.5.4 バックアップからの復帰待ち時間の設定 117
6.5.5 LAN 経由のキープアライブを使用するか否かの設定 117
6.5.6 LAN 経由のキープアライブの時間間隔の設定 118
6.5.7 LAN 経由のキープアライブのログをとるか否かの設定 118
6.5.8 ネットワーク監視機能の設定 119
6.6 受信パケット統計情報の設定 120
6.6.1 受信パケットの統計情報を記録するか否かの設定 121
6.6.2 受信したパケットの統計情報のクリア 121
6.6.3 受信したパケットの統計情報の表示 122
6.6.4 統計情報を記録する受信パケットの分類数の設定 122
6.7 パケット転送フィルターの設定 123
6.7.1 パケット転送フィルターの定義 123
6.7.2 インターフェースへのパケット転送フィルターの適用 123
第 7 章 : イーサネットフィルターの設定 125
7.1 フィルター定義の設定 125
7.2 インターフェースへの適用の設定 127
7.3 イーサネットフィルターの状態の表示 127
第 8 章 : 入力遮断フィルターの設定 128

8.1 フィルター定義の設定 128
8.2 適用の設定 130
第 9 章 : ポリシーフィルターの設定 132
9.1 サービスの定義 132
9.2 インターフェースグループの定義 132
9.3 アドレスグループの定義 133
9.4 サービスグループの定義 134
9.5 ポリシーフィルターの定義 134
9.6 ポリシーセットの定義 136
9.7 ポリシーセットの有効化 137
9.8 ポリシーセットの自動切り替え 137
9.9 タイマーの設定 138
第 10 章 : URL フィルターの設定 140
10.1 フィルター定義の設定 140
10.2 URL フィルターのインターフェースへの適用 141
10.3 URL フィルターでチェックを行う HTTP のポート番号の設定 141
10.4 URL フィルターを使用するか否かの設定 142
10.5 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 142
10.6 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 143
10.7 プロキシ経由の HTTPS URL フィルターを使用するか否かの設定 143
10.8 プロキシ経由の HTTPS URL フィルターのインターフェースへの適用 143
10.9 HTTPS プロキシの待ち受けポート番号の設定 144
10.10 プロキシ自動設定ファイルの URL の設定 144
10.11 利用するデータベースの選択 145
10.12 データベースを持つサーバーアドレスの設定 145
10.13 Proxy サーバーの設定 146
10.14 チェックするカテゴリーの設定 146
10.15 Web レピュテーションによるフィルタの設定 147
10.16 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 148
10.17 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 148
10.18 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 149
10.19 指定した拡張子の URL を評価するか否かの設定 149
10.20 評価しない URL の拡張子の設定 149
10.21 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 150
10.22 シリアル ID を登録する URL の設定 150
10.23 データベースへアクセスするためのシリアル ID の設定 150
10.24 URL フィルタリングサービス事業者にシリアル ID の登録 151
10.25 URL フィルタリングサービス事業者との契約状況の確認 151
10.26 データベース情報の更新 152
10.27 ユーザー認証に失敗した場合の再送間隔と回数の設定 153
第 11 章 : PPP の設定 154
11.1 相手の名前とパスワードの設定 154
11.2 受け入れる認証タイプの設定 154
11.3 要求する認証タイプの設定 155
11.4 自分の名前とパスワードの設定 155
11.5 同一 username を持つ相手からの二重接続を禁止するか否かの設定 156
11.6 LCP 関連の設定 156
11.6.1 Address and Control Field Compression オプション使用の設定 156

11.6.2 Magic Number オプション使用の設定 156
11.6.3 Maximum Receive Unit オプション使用の設定 157
11.6.4 Protocol Field Compression オプション使用の設定 157
11.6.5 lcp-restart パラメータの設定 158
11.6.6 lcp-max-terminate パラメータの設定 158
11.6.7 lcp-max-configure パラメータの設定 158
11.6.8 lcp-max-failure パラメータの設定 158
11.6.9 Configure-Request をすぐに送信するか否かの設定 158
11.7 PAP 関連の設定 159
11.7.1 pap-restart パラメータの設定 159
11.7.2 pap-max-authreq パラメータの設定 159
11.8 CHAP 関連の設定 159
11.8.1 chap-restart パラメータの設定 159
11.8.2 chap-max-challenge パラメータの設定 159
11.9 IPCP 関連の設定 160
11.9.1 Van Jacobson Compressed TCP/IP 使用の設定 160
11.9.2 PP 側 IP アドレスのネゴシエーションの設定 160
11.9.3 ipcp-restart パラメータの設定 160
11.9.4 ipcp-max-terminate パラメータの設定 161
11.9.5 ipcp-max-configure パラメータの設定 161
11.9.6 ipcp-max-failure パラメータの設定 161
11.9.7 WINS サーバーの IP アドレスの設定 161
11.9.8 IPCP の MS 拡張オプションを使うか否かの設定 161
11.9.9 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 162
11.10 MSCBCP 関連の設定 162
11.10.1 mscbcp-restart パラメータの設定 162
11.10.2 mscbcp-maxretry パラメータの設定 162
11.11 CCP 関連の設定 163
11.11.1 全パケットの圧縮タイプの設定 163
11.11.2 ccp-restart パラメータの設定 163
11.11.3 ccp-max-terminate パラメータの設定 164
11.11.4 ccp-max-configure パラメータの設定 164
11.11.5 ccp-max-failure パラメータの設定 164
11.12 IPV6CP 関連の設定 164
11.12.1 IPV6CP を使用するか否かの設定 164
11.13 PPPoE 関連の設定 165
11.13.1 PPPoE で使用する LAN インターフェースの指定 165
11.13.2 アクセスコンセントレータ名の設定 165
11.13.3 セッションの自動接続の設定 165
11.13.4 セッションの自動切断の設定 165
11.13.5 PADI パケットの最大再送回数の設定 166
11.13.6 PADI パケットの再送時間の設定 166
11.13.7 PADR パケットの最大再送回数の設定 166
11.13.8 PADR パケットの再送時間の設定 166
11.13.9 PPPoE セッションの切断タイマの設定 167
11.13.10 サービス名の指定 167
11.13.11 TCP パケットの MSS の制限の有無とサイズの指定 167
11.13.12 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 168

11.13.13 PPPoE フレームを中継するインターフェースの指定 168
第 12 章 : DHCP の設定 169
12.1 DHCP サーバー・リレーエージェント機能 169
12.1.1 DHCP の動作の設定 169
12.1.2 RFC2131 対応動作の設定 170
12.1.3 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 171
12.1.4 DHCP スコープの定義 171
12.1.5 DHCP 予約アドレスの設定 172
12.1.6 DHCP アドレス割り当て動作の設定 174
12.1.7 DHCP 割り当て情報を元にした予約設定の生成 175
12.1.8 DHCP オプションの設定 176
12.1.9 DHCP リース情報の手動追加 177
12.1.10 DHCP リース情報の手動削除 177
12.1.11 DHCP サーバーの指定の設定 177
12.1.12 DHCP サーバーの選択方法の設定 178
12.1.13 DHCP BOOTREQUEST パケットの中継基準の設定 178
12.1.14 インターフェース毎の DHCP の動作の設定 178
12.2 DHCP クライアント機能 179
12.2.1 DHCP クライアントのホスト名の設定 179
12.2.2 要求する IP アドレスリース期間の設定 180
12.2.3 IP アドレス取得要求の再送回数と間隔の設定 180
12.2.4 DHCP クライアント ID オプションの設定 180
12.2.5 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 181
12.2.6 リンクダウンした時に情報を解放するか否かの設定 182
第 13 章 : ICMP の設定 183
13.1 IPv4 の設定 183
13.1.1 ICMP Echo Reply を送信するか否かの設定 183
13.1.2 ICMP Echo Reply をリンクダウン時に送信するか否かの設定 183
13.1.3 ICMP Mask Reply を送信するか否かの設定 183
13.1.4 ICMP Parameter Problem を送信するか否かの設定 184
13.1.5 ICMP Redirect を送信するか否かの設定 184
13.1.6 ICMP Redirect 受信時の処理の設定 184
13.1.7 ICMP Time Exceeded を送信するか否かの設定 185
13.1.8 ICMP Timestamp Reply を送信するか否かの設定 185
13.1.9 ICMP Destination Unreachable を送信するか否かの設定 185
13.1.10 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 186
13.1.11 受信した ICMP のログを記録するか否かの設定 186
13.1.12 ステルス機能の設定 187
13.2 IPv6 の設定 187
13.2.1 ICMP Echo Reply を送信するか否かの設定 187
13.2.2 ICMP Echo Reply をリンクダウン時に送信するか否かの設定 187
13.2.3 ICMP Parameter Problem を送信するか否かの設定 188
13.2.4 ICMP Redirect を送信するか否かの設定 188
13.2.5 ICMP Redirect 受信時の処理の設定 188
13.2.6 ICMP Time Exceeded を送信するか否かの設定 189
13.2.7 ICMP Destination Unreachable を送信するか否かの設定 189
13.2.8 受信した ICMP のログを記録するか否かの設定 190
13.2.9 ICMP Packet-Too-Big を送信するか否かの設定 190

13.2.10 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 190
13.2.11 ステルス機能の設定 191
第 14 章 : トンネリング 192
14.1 トンネルインターフェースの使用許可の設定 192
14.2 トンネルインターフェースの使用不許可の設定 192
14.3 トンネルインターフェースの種別の設定 192
14.4 トンネルインターフェースの IPv4 アドレスの設定 193
14.5 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 193
14.6 トンネルインターフェースの端点 IP アドレスの設定 193
14.7 トンネルの端点の名前の設定 194
第 15 章 : IPsec の設定 195
15.1 IPsec の動作の設定 195
15.2 IKE バージョンの設定 196
15.3 IKE の認証方式の設定 196
15.4 事前共有鍵の登録 197
15.5 IKEv2 の認証に使用する PKI ファイルの設定 197
15.6 EAP-MD5 認証で使用する自分の名前とパスワードの設定 198
15.7 EAP-MD5 によるユーザー認証の設定 198
15.8 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 199
15.9 IKE の鍵交換を始動するか否かの設定 199
15.10 設定が異なる場合に鍵交換を拒否するか否かの設定 200
15.11 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 201
15.12 鍵交換の再送回数と間隔の設定 201
15.13 相手側のセキュリティー・ゲートウェイの名前の設定 201
15.14 相手側セキュリティー・ゲートウェイの IP アドレスの設定 202
15.15 相手側の ID の設定 203
15.16 自分側のセキュリティー・ゲートウェイの名前の設定 203
15.17 自分側セキュリティー・ゲートウェイの IP アドレスの設定 204
15.18 自分側の ID の設定 205
15.19 IKE キープアライブ機能の設定 205
15.20 IKE キープアライブに関する SYSLOG を出力するか否かの設定 207
15.21 IKE が用いる暗号アルゴリズムの設定 207
15.22 受信した IKE パケットを蓄積するキューの長さの設定 208
15.23 IKE が用いるグループの設定 208
15.24 IKE が用いるハッシュアルゴリズムの設定 209
15.25 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 209
15.26 IKE ペイロードのタイプの設定 210
15.27 IKEv1 鍵交換タイプの設定 210
15.28 IKE の情報ペイロードを送信するか否かの設定 211
15.29 PFS を用いるか否かの設定 211
15.30 XAUTH の設定 212
15.31 XAUTH 認証、EAP-MD5 認証に使用するユーザー ID の設定 212
15.32 XAUTH 認証、EAP-MD5 認証に使用するユーザー ID の属性の設定 212
15.33 XAUTH 認証、EAP-MD5 認証に使用するユーザーグループの設定 213
15.34 XAUTH 認証、EAP-MD5 認証に使用するユーザーグループの属性の設定 214
15.35 XAUTH によるユーザー認証の設定 214
15.36 内部 IP アドレスプールの設定 215
15.37 IKE XAUTH Mode-Cfg メソッドの設定 215
15.38 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 216

15.39 IKE のログの種類の設定 216
15.40 ESP を UDP でカプセル化して送受信するか否かの設定 217
15.41 折衝パラメーターを制限するか否かの設定 217
15.42 IKE のメッセージ ID 管理の設定 218
15.43 CHILD SA 作成方法の設定 218
15.44 SA 関連の設定 219
15.44.1 SA の寿命の設定 219
15.44.2 SA のポリシーの定義 220
15.44.3 SA の手動更新 222
15.44.4 ダングリング SA の動作の設定 222
15.44.5 IPsec NAT トラバーサルを利用するための設定 223
15.44.6 SA の削除 224
15.45 トンネルインターフェース関連の設定 224
15.45.1 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 224
15.45.2 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 224
15.45.3 使用する SA のポリシーの設定 225
15.45.4 IPComp によるデータ圧縮の設定 225
15.45.5 トンネルバックアップの設定 226
15.45.6 トンネルテンプレートの設定 226
15.46 トランスポートモード関連の設定 228
15.46.1 トランスポートモードの定義 228
15.46.2 トランスポートモードのテンプレートの設定 229
15.47 PKI 関連の設定 229
15.47.1 証明書ファイルの設定 230
15.47.2 CRL ファイルの設定 230

第 16 章 : L2TP/IPsec 機能の設定 231

16.1 L2TP/IPsec を動作させるか否かの設定 231
16.2 L2TP トンネル認証に関する設定 231
16.3 L2TP トンネルの切断タイマの設定 232
16.4 L2TP キープアライブの設定 232
16.5 L2TP キープアライブのログ設定 232
16.6 L2TP のコネクション制御の syslog を出力するか否かの設定 233

第 17 章 : PPTP 機能の設定 234

17.1 共通の設定 234
17.1.1 PPTP サーバーを動作させるか否かの設定 234
17.1.2 相手先情報番号にバインドされるトンネルインターフェースの設定 234
17.1.3 PPTP の動作タイプの設定 235
17.1.4 PPTP ホスト名の設定 235
17.1.5 PPTP ホスト名の設定 235
17.1.6 PPTP パケットのウィンドウサイズの設定 236
17.1.7 PPTP 暗号鍵生成のための要求する認証方式の設定 236
17.1.8 PPTP 暗号鍵生成のための受け入れ可能な認証方式の設定 236
17.1.9 PPTP のコネクション制御の syslog を出力するか否かの設定 237
17.2 リモートアクセス VPN 機能 237
17.2.1 PPTP トンネルの出力切断タイマの設定 237
17.2.2 PPTP キープアライブの設定 237
17.2.3 PPTP キープアライブのログ設定 238
17.2.4 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 238
17.2.5 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 238

第 18 章 : SIP 機能の設定 240

18.1 共通の設定 240
18.1.1 SIP を使用するか否かの設定 240
18.1.2 SIP の session-timer 機能のタイマ値の設定 240
18.1.3 SIP による発信時に使用する IP プロトコルの選択 241
18.1.4 SIP による発信時に 100rel をサポートするか否かの設定 241
18.1.5 送信する SIP パケットに User-Agent ヘッダを付加する設定 241
18.1.6 SIP による着信時の INVITE に refresher 指定がない場合の設定 242
18.1.7 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 242
18.1.8 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 242
18.1.9 SIP 着信時にユーザー名を検証するか否かの設定 243
18.1.10 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 243
18.1.11 SIP で使用する IP アドレスの設定 243
18.1.12 SIP メッセージのログを記録するか否かの設定 244
18.2 NGN 機能の設定 244
18.2.1 NGN 網に接続するインターフェースの設定 244
18.2.2 NGN 網を介したトンネルインターフェースの切断タイマの設定 244
18.2.3 NGN 網を介したトンネルインターフェースの帯域幅の設定 245
18.2.4 NGN 網を介したトンネルインターフェースの着信許可の設定 245
18.2.5 NGN 網を介したトンネルインターフェースの発信許可の設定 246
18.2.6 NGN 網を介したトンネルインターフェースで使用する LAN インターフェースの設定 246
18.2.7 NGN 網を介したトンネルインター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 247
18.2.8 NGN 電話番号を RADIUS で認証するか否かの設定 247
18.2.9 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 247
18.2.10 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 248
18.2.11 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 248
18.2.12 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 248
18.2.13 NGN 網接続情報の表示 249

第 19 章 : SNMP の設定 250

19.1 SNMPv1 によるアクセスを許可するホストの設定 250
19.2 SNMPv1 の読み出し専用のコミュニティ名の設定 251
19.3 SNMPv1 の読み書き可能なコミュニティ名の設定 251
19.4 SNMPv1 トラップの送信先の設定 251
19.5 SNMPv1 トラップのコミュニティ名の設定 251
19.6 SNMPv2c によるアクセスを許可するホストの設定 252
19.7 SNMPv2c の読み出し専用のコミュニティ名の設定 252
19.8 SNMPv2c の読み書き可能なコミュニティ名の設定 253
19.9 SNMPv2c トラップの送信先の設定 253
19.10 SNMPv2c トラップのコミュニティ名の設定 253
19.11 SNMPv3 エンジン ID の設定 253
19.12 SNMPv3 コンテキスト名の設定 254
19.13 SNMPv3 USM で管理するユーザーの設定 254
19.14 SNMPv3 によるアクセスを許可するホストの設定 255
19.15 SNMPv3 VACM で管理する MIB ビューファミリの設定 255
19.16 SNMPv3 VACM で管理するアクセスポリシーの設定 256
19.17 SNMPv3 トラップの送信先の設定 257

19.18 SNMP 送信パケットの始点アドレスの設定 257
19.19 sysContact の設定 257
19.20 sysLocation の設定 258
19.21 sysName の設定 258
19.22 SNMP 標準トラップを送信するか否かの設定 258
19.23 SNMP の linkDown トラップの送信制御の設定 259
19.24 PP インターフェースの情報を MIB2 の範囲で表示するか否かの設定 259
19.25 トンネルインターフェースの情報を MIB2 の範囲で表示するか否かの設定 260
19.26 スイッチのインターフェースの情報を MIB2 の範囲で表示するか否かの設定 260
19.27 PP インターフェースのアドレスの強制表示の設定 260
19.28 LAN インター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 261
19.29 電波強度トラップを送信するか否かの設定 261
19.30 スイッチへ静的に付与するインターフェース番号の設定 262
19.31 スイッチへ静的に付与するスイッチ番号の設定 262
19.32 スイッチの状態による SNMP トラップの条件の設定 262
19.33 スイッチで共通の SNMP トラップの条件の設定 263

第 20 章 : RADIUS の設定 265

20.1 RADIUS による認証を使用するか否かの設定 265
20.2 RADIUS によるアカウントを使用するか否かの設定 265
20.3 RADIUS サーバーの指定 265
20.4 RADIUS 認証サーバーの指定 266
20.5 RADIUS アカウントサーバーの指定 266
20.6 RADIUS 認証サーバーの UDP ポートの設定 267
20.7 RADIUS アカウントサーバーの UDP ポートの設定 267
20.8 RADIUS シークレットの設定 267
20.9 RADIUS 再送信パラメータの設定 267

第 21 章 : NAT 機能 269

21.1 インターフェースへの NAT ディスクリプタ適用の設定 269
21.2 NAT ディスクリプタの動作タイプの設定 269
21.3 NAT 処理の外側 IP アドレスの設定 270
21.4 NAT 処理の内側 IP アドレスの設定 271
21.5 静的 NAT エントリの設定 271
21.6 IP マスカレード使用時に rlogin,rcp と ssh を使用するか否かの設定 272
21.7 静的 IP マスカレードエントリの設定 272
21.8 NAT の IP アドレスマップの消去タイマの設定 273
21.9 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 273
21.10 IP マスカレードで利用するポートの範囲の設定 274
21.11 FTP として認識するポート番号の設定 274
21.12 IP マスカレードで変換しないポート番号の範囲の設定 275
21.13 NAT のアドレス割当をログに記録するか否かの設定 275
21.14 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 275
21.15 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 276
21.16 IP マスカレードで変換するセッション数の設定 276

第 22 章 : DNS の設定 278

22.1 DNS を利用するか否かの設定 278
22.2 DNS サーバーの IP アドレスの設定 278
22.3 DNS ドメイン名の設定 279

22.4 DNS サーバーを通知してもらう相手先情報番号の設定 279
22.5 DNS サーバーアドレスを取得するインターフェースの設定 279
22.6 DHCP/IPCP MS 拡張で DNS サーバーを通知する順序の設定 280
22.7 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 280
22.8 SYSLOG 表示で DNS により名前解決するか否かの設定 281
22.9 DNS 問い合わせの内容に応じた DNS サーバーの選択 281
22.10 静的 DNS レコードの登録 282
22.11 DNS 問い合わせパケットの始点ポート番号の設定 284
22.12 DNS サーバーへアクセスできるホストの IP アドレス設定 284
22.13 DNS キャッシュを使用するか否かの設定 284
22.14 DNS キャッシュの最大エントリ数の設定 285
22.15 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 285

第 23 章 : 優先制御／帯域制御 287

23.1 インターフェース速度の設定 287
23.2 クラス分けのためのフィルター設定 287
23.3 キューイングアルゴリズムタイプの選択 289
23.4 クラス分けフィルターの適用 290
23.5 クラス毎のキュー長の設定 290
23.6 デフォルトクラスの設定 291
23.7 クラスの属性の設定 291
23.8 動的なクラス変更 (Dynamic Class Control) の設定 292

第 24 章 : 連携機能 294

24.1 連携動作を行うか否かの設定 294
24.2 連携動作で使用するポート番号の設定 294
24.3 帯域測定で連携動作を行う相手毎の動作の設定 294
24.4 負荷監視通知で連携動作を行う相手毎の動作の設定 296
24.5 負荷監視サーバーとしての動作トリガの設定 297
24.6 負荷監視クライアントとしての動作の設定 298
24.7 連携動作の手動実行 299

第 25 章 : OSPF 301

25.1 OSPF の有効設定 301
25.2 OSPF の使用設定 301
25.3 OSPF による経路の優先度設定 301
25.4 OSPF のルーター ID 設定 301
25.5 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 302
25.6 外部プロトコルによる経路導入 302
25.7 OSPF で受け取った経路をどう扱うかのフィルターの設定 303
25.8 外部経路導入に適用するフィルター定義 304
25.9 OSPF エリア設定 306
25.10 エリアへの経路広告 306
25.11 スタブ的接続の広告 307
25.12 仮想リンク設定 307
25.13 指定インターフェースの OSPF エリア設定 309
25.14 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 312
25.15 スタブが存在する時のネットワーク経路の扱いの設定 312
25.16 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 312
25.17 インター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 313

第 26 章 : BGP 314

26.1 BGP の起動の設定 314
26.2 経路の集約の設定 314
26.3 経路を集約するためのフィルターの設定 314
26.4 AS 番号の設定 315
26.5 ルーター ID の設定 315
26.6 BGP による経路の優先度の設定 316
26.7 BGP で受信した経路に対するフィルターの適用 316
26.8 BGP で受信する経路に適用するフィルターの設定 317
26.9 BGP に導入する経路に対するフィルターの適用 318
26.10 BGP の設定の有効化 319
26.11 BGP に導入する経路に適用するフィルターの設定 319
26.12 BGP による接続先の設定 320
26.13 BGP で使用する TCP MD5 認証の事前共有鍵の設定 321
26.14 BGP のログの設定 321
26.15 BGP で強制的に経路を広告する 321
26.16 インター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 322

第 27 章 : IPv6 323

27.1 共通の設定 323
27.1.1 IPv6 パケットを扱うか否かの設定 323
27.1.2 IPv6 インターフェースのリンク MTU の設定 323
27.1.3 TCP セッションの MSS 制限の設定 323
27.1.4 TCP ウィンドウ・スケール・オプション を変更する 324
27.1.5 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 324
27.1.6 IPv6 ファストパス機能の設定 325
27.2 IPv6 アドレスの管理 325
27.2.1 インターフェースの IPv6 アドレスの設定 325
27.2.2 インターフェースのプレフィックスに基づく IPv6 アドレスの設定 327
27.2.3 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 328
27.2.4 DHCPv6 の動作の設定 329
27.2.5 DAD(Duplicate Address Detection) の送信回数の設定 329
27.2.6 自動的に設定される IPv6 アドレスの最大数の設定 330
27.2.7 始点 IPv6 アドレスを選択する規則の設定 330
27.3 近隣探索 330
27.3.1 ルーター広告で配布するプレフィックスの定義 330
27.3.2 ルーター広告の送信の制御 332
27.4 経路制御 333
27.4.1 IPv6 の経路情報の追加 333
27.5 RIPng 334
27.5.1 RIPng の使用の設定 334
27.5.2 インターフェースにおける RIPng の送信ポリシーの設定 335
27.5.3 インターフェースにおける RIPng の受信ポリシーの設定 335
27.5.4 RIPng の加算ホップ数の設定 335
27.5.5 インターフェースにおける信頼できる RIPng ゲートウェイの設定 336
27.5.6 RIPng で送受信する経路に対するフィルタリングの設定 336
27.5.7 回線接続時の PP 側の RIPng の動作の設定 337
27.5.8 回線接続時の PP 側の RIPng 送出の時間間隔の設定 337
27.5.9 回線切断時の PP 側の RIPng の動作の設定 337
27.5.10 回線切断時の PP 側の RIPng 送出の時間間隔の設定 338
27.5.11 RIPng による経路を回線切断時に保持するか否かの設定 338

27.5.12 RIPng による経路の優先度の設定 338
27.6 VRRPv3 の設定 339
27.6.1 インターフェース毎の VRRPv3 の設定 339
27.6.2 シャットダウントリガの設定 340
27.7 フィルターの設定 341
27.7.1 IPv6 フィルターの定義 341
27.7.2 IPv6 フィルターの適用 342
27.7.3 IPv6 動的フィルターの定義 342
27.8 IPv6 マルチキャストパケットの転送の設定 343
27.8.1 MLD の動作の設定 344
27.8.2 MLD の静的な設定 345
27.9 近隣要請 346
27.9.1 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 346
第 28 章 : トリガによるメール通知機能 347
28.1 メール設定識別名の設定 347
28.2 SMTP メールサーバーの設定 347
28.3 POP メールサーバーの設定 348
28.4 メール処理のタイムアウト値の設定 348
28.5 メールの送信時に使用するテンプレートの設定 349
28.6 メール通知のトリガの設定 350
第 29 章 : メールセキュリティー 353
29.1 メールセキュリティーを使用するか否か 353
29.2 メールセキュリティーでチェックする受信ポート番号の設定 353
29.3 メールセキュリティーでチェックする送信ポート番号の設定 353
29.4 メールセキュリティーで件名に付与する文字列の設定 354
29.5 メールセキュリティーでチェックするメールサイズの上限 354
29.6 アンチスパム判定の判定基準 354
29.7 メールセキュリティーで機器が送信するメールの送信元アドレスの設定 355
29.8 メールセキュリティーで機器が送信するメールの宛先アドレスの設定 355
29.9 SMTP で送信するメールが不正なメールと判定されたときの動作の設定 356
29.10 SMTP で送信するメールのサイズが上限を超えたときの動作 356
29.11 メールセキュリティーを利用できない場合のメール送受信の動作 356
29.12 ホワイトリストの定義 357
29.13 ホワイトリストセットの定義 357
29.14 ホワイトリストセットの有効化 357
29.15 YSC への接続タイムアウトの設定 358
29.16 YSC へのメールスキャン要求に対するタイムアウトの設定 358
29.17 YSC への接続リトライ回数の設定 358
第 30 章 : HTTP サーバー機能 359
30.1 共通の設定 359
30.1.1 HTTP サーバー機能の有無の設定 359
30.1.2 HTTP サーバーへアクセスできるホストの IP アドレス設定 359
30.1.3 HTTP サーバーのセッションタイムアウト時間の設定 360
30.1.4 HTTP サーバー機能の listen ポートの設定 360
30.1.5 PP インターフェースとトンネルインターフェースの名前の設定 360
30.2 かんたん設定ページ用の設定 360
30.2.1 プロバイダ接続タイプの設定 361
30.2.2 プロバイダ情報の PP との関連付けと名前の設定 361

30.2.3 プロバイダ接続設定 361
30.2.4 プロバイダの DNS サーバーのアドレス設定 362
30.2.5 LAN インターフェースの DNS サーバーのアドレスの設定 362
30.2.6 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 363
30.2.7 フィルター型ルーティングの形式の設定 363
30.2.8 LAN 側のプロバイダ名称の設定 363
30.2.9 NTP サーバーの設定 364
30.2.10 プロバイダの NTP サーバーのアドレス設定 364
30.2.11 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 364
30.2.12 かんたん設定ページで IPv6 接続を行うか否かの設定 365
30.2.13 LAN インターフェースのプロバイダ情報とトンネルとの関連付け 365

第 31 章 : ネットボランチ DNS サービスの設定 366

31.1 ネットボランチ DNS サービスの使用の可否 366
31.2 ネットボランチ DNS サーバーへの手動更新 366
31.3 ネットボランチ DNS サーバーからの削除 367
31.4 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 367
31.5 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 367
31.6 ホスト名の登録 367
31.7 通信タイムアウトの設定 368
31.8 ホスト名を自動生成するか否かの設定 368
31.9 シリアル番号を使ったホスト名登録コマンドの設定 369
31.10 ネットボランチ DNS サーバーの設定 369
31.11 ネットボランチ DNS サーバーアドレス更新機能の ON/OFF の設定 369
31.12 ネットボランチ DNS サーバーアドレス更新機能のポート番号の設定 370
31.13 自動更新に失敗した場合のリトライ間隔と回数の設定 370
31.14 ネットボランチ DNS 登録の定期更新間隔の設定 371
31.15 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 371

第 32 章 : UPnP の設定 372

32.1 UPnP を使用するか否かの設定 372
32.2 UPnP に使用する IP アドレスを取得するインターフェースの設定 372
32.3 UPnP のポートマッピング用消去タイマのタイプの設定 372
32.4 UPnP のポートマッピングの消去タイマの設定 373
32.5 UPnP の syslog を出力するか否かの設定 373

第 33 章 : USB の設定 374

33.1 USB ホスト機能を使うか否かの設定 374
33.2 USB バスで過電流保護機能が働くまでの時間の設定 374

第 34 章 : スケジュール 375

34.1 スケジュールの設定 375

第 35 章 : VLAN の設定 378

35.1 VLAN ID の設定 378
35.2 スイッチングハブのポートが所属する VLAN の設定 378

第 36 章 : 生存通知機能 380

36.1 生存通知の共有鍵の設定 380
36.2 生存通知を受信するか否かの設定 380
36.3 生存通知の実行 381

第 37 章 : 生存通知機能　リリース 2 382

37.1 通知名称の設定 382

37.2 通知設定の定義 382
37.3 通知設定の有効化 383
37.4 通知間隔の設定 383
37.5 通知を送信した際にログを記録するか否かの設定 383
37.6 受信設定の定義 384
37.7 受信設定の有効化 384
37.8 受信間隔の監視設定 385
37.9 通知を受信した際にログを記録するか否かの設定 385
37.10 同時に保持できる生存情報の最大数の設定 385
37.11 生存通知の状態の表示 386
37.12 生存通知の状態のクリア 386

第 38 章 : SNTP サーバー機能 387

38.1 SNTP サーバー機能を有効にするか否かの設定 387
38.2 SNTP サーバーへのアクセスを許可するホストの設定 387

第 39 章 : 外部メモリ機能 389

39.1 microSD カードスロットを使うか否かの設定 389
39.2 外部メモリ用キャッシュメモリの動作モードの設定 389
39.3 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 390
39.4 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 391
39.5 外部メモリに保存する SYSLOG ファイル名の指定 392
39.6 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 394
39.7 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 394
39.8 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 395
39.9 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 395
39.10 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 396
39.11 ファイル検索時のタイムアウトを設定する 397
39.12 バッチファイルを実行する 397
39.13 バッチファイルと実行結果ファイルの設定 397
39.14 外部メモリ性能測定コマンド 398
39.15 DOWNLOAD ボタンを押した時に実行する機能の設定 399
39.16 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 399

第 40 章 : モバイルインターネット接続機能 400

40.1 携帯端末を使用するか否かの設定 400
40.2 携帯端末に入力する PIN コードの設定 401
40.3 携帯端末に直接コマンドを発行する 401
40.4 指定した相手に対して発信制限を解除する 402
40.5 PP で使用するインターフェースの設定 402
40.6 携帯端末からの自動発信設定 402
40.7 携帯端末を切断するタイマの設定 403
40.8 携帯端末を入力がないときに切断するタイマの設定 403
40.9 携帯端末を出力がないときに切断するタイマの設定 403
40.10 発信先アクセスポイントの設定 403
40.11 携帯端末に指示する発信先の設定 404
40.12 パケット通信量制限の設定 404
40.13 パケット通信時間制限の設定 405

40.14 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 406
40.15 LCP の Async Control Character Map オプション使用の設定 406
40.16 発信者番号通知 (186) を付加するかどうかの設定 407
40.17 詳細な SYSLOG を出力するか否かの設定 407
40.18 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 407
40.19 接続毎パケット通信量制限の設定 408
40.20 接続毎パケット通信時間制限の設定 408
40.21 通信制限の累積期間の設定 409
40.22 携帯端末でパケット着信機能を使用するか否かの設定 409
40.23 モバイルインターネット機能の着信許可の設定 410
40.24 電波の受信レベルの取得 410
40.25 電波の受信レベル取得機能の設定 410
40.26 定期実行で取得した電波の受信レベルの表示 411
40.27 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 411
40.28 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 412
40.29 携帯端末のファームウェア更新 412
40.30 携帯端末のネットワーク事業者モードの設定 413
40.31 自分の名前とパスワードの設定 413
40.32 WAN で使用するインターフェースの設定 414
40.33 携帯端末からの自動発信設定 414
40.34 携帯端末を切断するタイマの設定 414
40.35 携帯端末を入力がないときに切断するタイマの設定 415
40.36 携帯端末を出力がないときに切断するタイマの設定 415
40.37 常時接続の設定 416
40.38 発信先アクセスポイントの設定 416
40.39 パケット通信量制限の設定 417
40.40 パケット通信時間制限の設定 417
40.41 接続毎パケット通信量制限の設定 418
40.42 接続毎パケット通信時間制限の設定 419
40.43 通信制限の累積期間の設定 420

第 41 章 : ブリッジインターフェース (ブリッジ機能) 421

41.1 ブリッジインターフェースに収容する実インターフェースを設定する 421
41.2 自動的なラーニングを行うか否かの設定 421
41.3 ブリッジがラーニングした情報の消去タイマーの設定 422
41.4 静的なラーニング情報の設定 422

第 42 章 : Lua スクリプト機能 424

42.1 Lua スクリプト機能を有効にするか否かの設定 424
42.2 Lua スクリプトの実行 424
42.3 Lua コンパイラの実行 425
42.4 Lua スクリプトの走行状態の表示 425
42.5 Lua スクリプトの強制終了 426
42.6 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 426

第 43 章 : カスタム GUI 428

43.1 カスタム GUI を使用するか否かの設定 428
43.2 カスタム GUI を使用するユーザーの設定 428
43.3 カスタム GUI の API を使用するか否かの設定 429
43.4 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 429

第 44 章 : スイッチ制御機能 430

44.1 共通の設定 430
44.1.1 スイッチ制御機能を使用するか否かの設定 430
44.1.2 スイッチの監視時間間隔の設定 431
44.2 スイッチの制御 431
44.2.1 スイッチの選択 431
44.2.2 スイッチが持つ機能の設定 432
44.2.3 スイッチが持つ機能の設定内容や動作状態の取得 432
44.2.4 スイッチに対して特定の動作を実行 432
44.2.5 スイッチの設定の削除 433
44.2.6 スイッチのファームウェアの更新 433
44.2.7 LAN ケーブル二重化機能の設定 434
44.3 スイッチの機能 435
44.3.1 システム 435
44.3.1.1 BootROM バージョンの取得 435
44.3.1.2 ファームウェアリビジョンの取得 435
44.3.1.3 シリアル番号の取得 435
44.3.1.4 製品名称の取得 436
44.3.1.5 MAC アドレスの取得 436
44.3.1.6 機器の名前の設定 436
44.3.1.7 省電力機能を使用するか否かの設定 436
44.3.1.8 LED の輝度の調整 437
44.3.1.9 LED の表示モードの取得 437
44.3.1.10 ファンの状態の取得 438
44.3.1.11 ファンの回転数の取得 438
44.3.1.12 再起動 439
44.3.1.13 起動してからの時間の取得 439
44.3.2 ポート 439
44.3.2.1 リンクアグリゲーションのタイプの取得 439
44.3.2.2 ポートの通信速度および動作モードの設定 439
44.3.2.3 ポートを使用するか否かの設定 440
44.3.2.4 オートクロスオーバー機能を使用するか否かの設定 441
44.3.2.5 速度ダウンシフト機能を使用するか否かの設定 441
44.3.2.6 フロー制御を使用するか否かの設定 442
44.3.2.7 スイッチ制御パケットを遮断するか否かの設定 442
44.3.2.8 スイッチ制御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 443
44.3.2.9 コンボポートの使用状況の取得 443
44.3.2.10 ポートの受光レベルの取得 444
44.3.2.11 ポートのリンク状態の取得 444
44.3.3 MAC アドレステーブル 445
44.3.3.1 MAC アドレスエージング機能を使用するか否かの設定 445
44.3.3.2 MAC アドレスエージングの時間間隔の設定 445
44.3.3.3 MAC アドレスをキーにした MAC アドレステーブルの検索 446
44.3.3.4 ポート番号をキーにした MAC アドレステーブルの検索 446
44.3.3.5 MAC アドレステーブルのエントリの消去 446
44.3.4 VLAN 446
44.3.4.1 VLAN ID の設定 448
44.3.4.2 ポートの VLAN 動作モードの設定 448
44.3.4.3 アクセスポートの設定 448
44.3.4.4 トランクポートの設定 449

44.3.4.5 マルチプル VLAN を使用するか否かの設定 449
44.3.4.6 マルチプル VLAN のグループ設定 450
44.3.5 QoS 451
44.3.5.1 DSCP リマーキングの書き換え方式の設定 451
44.3.5.2 受信パケットのクラス分けの設定 451
44.3.5.3 帯域制限を行う際の速度単位の設定 452
44.3.5.4 受信トラフィックのポリシングを行うか否かの設定 452
44.3.5.5 受信トラフィックの帯域幅の設定 453
44.3.5.6 送信トラフィックのシェーピングを行うか否かの設定 453
44.3.5.7 送信トラフィックの帯域幅の設定 454
44.3.6 ミラーリング 454
44.3.6.1 ミラーリング機能を使用するか否かの設定 455
44.3.6.2 ミラーリングパケットを送出するポートの設定 456
44.3.6.3 受信したパケットをミラーリングするか否かの設定 456
44.3.6.4 送信するパケットをミラーリングするか否かの設定 457
44.3.7 カウンタ 457
44.3.7.1 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 457
44.3.7.2 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 459
44.3.7.3 受信フレームカウンタの値の取得 460
44.3.7.4 送信フレームカウンタの値の取得 461
44.3.7.5 受信オクテットカウンタの値の取得 461
44.3.7.6 送信オクテットカウンタの値の取得 462
44.3.7.7 カウンタのクリア 462
44.3.8 ループ検出 462
44.3.8.1 1 秒あたりのループが発生したと判断する閾値の設定 462
44.3.8.2 ループが発生したと判断するまでの時間の設定 463
44.3.8.3 ループ発生時の動作の設定 463
44.3.8.4 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 464
44.3.8.5 ループ検出機能を使用するか否かの設定 464
44.3.8.6 スイッチ制御パケットを用いたループ検出を行うか否かの設定 464
44.3.8.7 ループ検出機能に関するポートの状態の取得 465
44.3.8.8 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 465
44.3.8.9 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 466
44.3.9 PoE 給電 466
44.3.9.1 各ポートで給電可能なクラスの上限の設定 466
44.3.9.2 各ポートの給電状態の取得 467
44.3.9.3 各ポートに接続された機器のクラスの取得 467
44.3.9.4 スイッチの内部温度の取得 468
44.3.9.5 各ポートの消費電力の取得 468
44.3.9.6 各ポートの詳細な供給電力の取得 468
44.3.9.7 スイッチの総供給電力の取得 469
44.3.9.8 給電復帰 469
44.3.9.9 各ポートへの給電を開始 469
44.3.9.10 各ポートへの給電を停止 470
44.4 アクセスポイントの制御 470
44.4.1 アクセスポイントの選択 470
44.4.2 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 470
44.4.3 アクセスポイントの設定を保存するファイル名の指定 471
44.4.4 アクセスポイントの設定のバックアップ実行 471

44.4.5 アクセスポイントの設定の復元実行 471
44.4.6 アクセスポイントの設定の削除 472
44.4.7 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 472
44.4.8 アクセスポイントの HTTP リビジョンアップ機能の実行 473
44.4.9 アクセスポイント制御用の HTTP プロキシの使用 473
44.4.10 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 474

第 45 章 : YNO エージェント 475

45.1 YNO エージェント機能を使用するか否かの設定 475
45.2 YNO マネージャー接続用のアクセスコードの設定 475
45.3 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 476
45.4 YNO マネージャーに表示される自身の機器説明の設定 476
45.5 YNO エージェント機能の動作状態の表示 476

第 46 章 : 診断 478

46.1 ポートの開閉状態の診断 478
46.2 ポートへ到達可能なアクセス範囲の診断 479
46.3 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 479
46.4 ポートの開閉状態の診断結果の履歴数の設定 479
46.5 ポートの開閉状態の診断結果の表示 480
46.6 ポートへ到達可能なアクセス範囲の診断結果の表示 480
46.7 ポートの開閉状態の診断結果の消去 480

第 47 章 : 統計 481

47.1 統計機能を有効にするか否かの設定 481

第 48 章 : 操作 482

48.1 相手先情報番号の選択 482
48.2 トンネルインターフェース番号の選択 482
48.3 設定に関する操作 482
48.3.1 管理ユーザーへの移行 483
48.3.2 終了 483
48.3.3 設定内容の保存 483
48.3.4 設定ファイルの複製 483
48.3.5 ファームウェアファイルを内蔵フラッシュ ROM にコピー 485
48.3.6 設定ファイルの削除 485
48.3.7 デフォルト設定ファイルの設定 486
48.3.8 設定の初期化 486
48.3.9 遠隔地のルーターからの設定に対する制限 486
48.4 動的情報のクリア操作 487
48.4.1 アカウントのクリア 487
48.4.2 PP アカウントのクリア 487
48.4.3 携帯電話回線のアカウントのクリア 487
48.4.4 データコネクトのアカウントのクリア 487
48.4.5 ARP テーブルのクリア 487
48.4.6 IP の動的経路情報のクリア 487
48.4.7 ブリッジのラーニング情報のクリア 487
48.4.8 ログのクリア 488
48.4.9 DNS キャッシュのクリア 488
48.4.10 インターフェースのカウンター情報のクリア 488
48.4.11 NAT アドレステーブルのクリア 488
48.4.12 インターフェースの NAT アドレステーブルのクリア 489

48.4.13 PPPoE パススルー機能がラーニングした情報のクリア 489
48.4.14 IPv6 の動的経路情報の消去 489
48.4.15 近隣キャッシュの消去 489
48.4.16 起動情報の履歴を削除する 490
48.4.17 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 490
48.4.18 メールセキュリティーの検出履歴のクリア 490
48.4.19 メールセキュリティーのホワイトリスト情報のクリア 490
48.4.20 YSC との通信状態確認用カウンタ情報のクリア 490
48.5 ファイル、ディレクトリの操作 490
48.5.1 ディレクトリの作成 490
48.5.2 ファイルまたはディレクトリの削除 491
48.5.3 ファイルまたはディレクトリの複製 491
48.5.4 ファイル名またはディレクトリ名の変更 492
48.6 その他の操作 492
48.6.1 相手先の使用許可の設定 492
48.6.2 相手先の使用不許可の設定 492
48.6.3 再起動 493
48.6.4 インターフェースの再起動 493
48.6.5 発信 493
48.6.6 切断 494
48.6.7 ping 494
48.6.8 ping6 の実行 495
48.6.9 traceroute 496
48.6.10 traceroute6 の実行 496
48.6.11 nslookup 496
48.6.12 IPv4 動的フィルターのコネクション管理情報の削除 497
48.6.13 TELNET クライアント 497
48.6.14 IPv6 動的フィルターのコネクション管理情報の削除 498
48.6.15 スイッチングハブ MAC アドレステーブルの消去 498
48.6.16 Magic Packet の送信 499
48.6.17 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 499
48.6.18 入力遮断フィルターの状態のクリア 500
48.6.19 ポリシーフィルターの状態のクリア 500
48.6.20 URL フィルターの統計情報のクリア 500
48.6.21 外部データベース参照型 URL フィルターの統計情報のクリア 501
48.6.22 プロキシ経由の HTTPS URL フィルターの統計情報のクリア 501
48.6.23 メール通知の実行 501
48.6.24 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) 502
48.6.25 ライセンス認証の実行 502

第 49 章 : 設定の表示 503

49.1 機器設定の表示 503
49.2 すべての設定内容の表示 503
49.3 指定した AP の設定内容の表示 503
49.4 指定した PP の設定内容の表示 503
49.5 指定したスイッチの設定内容の表示 504
49.6 指定したトンネルの設定内容の表示 504
49.7 設定ファイルの一覧 504
49.8 ファイル情報の一覧の表示 504
49.9 インターフェースに付与されている IPv6 アドレスの表示 505

49.10 SSH サーバー公開鍵の表示 505
49.11 指定したインターフェースのフィルター内容の表示 506
49.12 ファームウェアファイルの一覧 506

第 50 章 : 状態の表示 507

50.1 ARP テーブルの表示 507
50.2 インターフェースの状態の表示 507
50.3 各相手先の状態の表示 507
50.4 IP の経路情報テーブルの表示 508
50.5 RIP で得られた経路情報の表示 508
50.6 IPv6 の経路情報の表示 508
50.7 IPv6 の RIP テーブルの表示 509
50.8 近隣キャッシュの表示 509
50.9 ブリッジのラーニング情報の表示 509
50.10 IPsec の SA の表示 509
50.11 証明書の情報の表示 510
50.12 CRL ファイルの情報の表示 510
50.13 VRRP の情報の表示 510
50.14 動的 NAT ディスクリプタのアドレスマップの表示 511
50.15 動作中の NAT ディスクリプタの適用リストの表示 511
50.16 LAN インターフェースの NAT ディスクリプタのアドレスマップの表示 511
50.17 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 512
50.18 L2TP の状態の表示 512
50.19 PPTP の状態の表示 512
50.20 OSPF 情報の表示 512
50.21 BGP の状態の表示 513
50.22 DHCP サーバーの状態の表示 513
50.23 DHCP クライアントの状態の表示 514
50.24 DHCPv6 の状態の表示 514
50.25 バックアップ状態の表示 514
50.26 動的フィルターによって管理されているコネクションの表示 514
50.27 IPv6 の動的フィルターによって管理されているコネクションの表示 515
50.28 ネットワーク監視機能の状態の表示 515
50.29 STATUS LED の情報の表示 515
50.30 侵入情報の履歴の表示 516
50.31 相手先ごとの接続時間情報の表示 516
50.32 PPPoE パススルー機能がラーニングした情報の表示 516
50.33 ネットボランチ DNS サービスに関する設定の表示 517
50.34 スイッチングハブ MAC アドレステーブルの表示 517
50.35 UPnP に関するステータス情報の表示 517
50.36 トンネルインターフェースの状態の表示 518
50.37 VLAN インターフェースの状態の表示 518
50.38 トリガによるメール通知機能の状態の表示 518
50.39 MLD のグループ管理情報の表示 519
50.40 IPv6 マルチキャストの経路情報の表示 519
50.41 ログインしているユーザー情報の表示 519
50.42 ログインしたユーザーのログイン履歴の表示 520
50.43 パケットバッファの状態の表示 520
50.44 QoS ステータスの表示 520
50.45 連携動作の状態の表示 521

50.46 入力遮断フィルターの状態表示 522
50.47 ポリシーフィルターの状態表示 522
50.48 ポリシーフィルターの制御対象サービスの表示 522
50.49 URL フィルターの情報の表示 523
50.50 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 523
50.51 データベースのライセンス情報の表示 524
50.52 プロキシ経由の HTTPS URL フィルターの情報の表示 524
50.53 生存通知の状態の表示 525
50.54 USB ホスト機能の動作状態を表示 525
50.55 リモートセットアップ機能に関する接続情報の表示 525
50.56 技術情報の表示 525
50.57 microSD スロットの動作状態を表示 526
50.58 外部メモリの動作状態を表示 526
50.59 RTFS の状態の表示 526
50.60 起動情報を表示する 526
50.61 起動情報の履歴の詳細を表示する 527
50.62 起動情報の履歴の一覧を表示する 527
50.63 ルーターが制御しているスイッチ一覧の表示 527
50.64 LAN ケーブル二重化機能の動作状態を表示 528
50.65 DNS キャッシュの表示 528
50.66 ライセンス情報の表示 528
50.67 ライセンス認証の状態の表示 529
50.68 メールセキュリティーの統計情報の表示 529
50.69 ホワイトリストの統計情報の表示 530
50.70 YSC との通信状態の表示 530
50.71 コピーライトの表示 530

第 51 章 : ロギング 531

51.1 ログの表示 531
51.2 アカウントの表示 531
51.3 PP アカウントの表示 532
51.4 携帯電話回線のアカウントの表示 532
51.5 データコネクトのアカウントの表示 532
51.6 通信履歴の表示 532

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

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.11.03.27 に対応しています。
このコマンドリファレンスの印刷より後にリリースされた最新のファームウェアや、マニュアル類および差分については以下に示す URL の WWW サーバーにある情報を参照してください。
http://www.rtpro.yamaha.co.jp

1.2 コマンドリファレンスの見方

このコマンドリファレンスは、ルーターのコンソールから入力するコマンドを説明しています。

1 つ 1 つのコマンドは次の項目の組合せで説明します。

[書式]	コマンドの入力形式を説明します。キー入力時には大文字と小文字のどちらを使用しても構いません。
	コマンドの名称部分は太字 (**Bold face**) で示します。
	パラメータ部分は斜体 (*Italic face*) で示します。
	キーワードは標準文字で示します。
	括弧 ([ ]) で囲まれたパラメータは省略可能であることを示します。
[設定値]	コマンドの設定値の種類とその意味を説明します。
[説明]	コマンドの解説部分です。
[ノート]	コマンドを使用する場合に特に注意すべき事柄を示します。
[設定例]	コマンドの具体例を示します。
[適用モデル]	コマンドが適用できるモデル名称を示します。

1.3 インター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ーフェースを指定するためにインターフェース名を利用します。
インターフェース名は、インターフェース種別とインターフェース番号を間に空白をおかずに続けて表記します。
インターフェース種別には、"lan" があります。インターフェース番号は、インター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。
lan インター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。
FWX120 では LAN 分割機能の拡張機能として VLAN インター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

インターフェースの種類	インターフェース名
メインモジュール上の LAN	lan1
タグ VLAN	lan1/1, lan1/2, ...
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, vlan3, vlan4

また、仮想的なインターフェースである loopback インターフェースと null インターフェース、ブリッジインターフェースを指定できます。

インターフェースの種類	インターフェース名
LOOPBACK	loopback1, loopback2, ...loopback9
NULL	null
BRIDGE	bridge1

1.4 no で始まるコマンドの入力形式について

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

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

1.5 コマンドの入力文字数とエスケープシーケンスについて

1 つのコマンドとして入力できる文字数は、コマンド本体とパラメータ部分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
FWX120	1-30

1.7 工場出荷設定値について

FWX120 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
```

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。

Rev.11.03.27 以降では **telnetd host lan** コマンドも設定されています。

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 インター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の 2 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

ヤマハルーター へは、それぞれに対して 1 ユーザー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ーになれるのは同時に 1 ユーザーだけです。例えば、シリアル端末でアクセスしているユーザーが管理ユーザーとして設定を行っている場合には、別のユーザーが一般ユーザーとしてアクセスすることはできても管理ユーザー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 ユーザーまで可能です。また複数のユーザーが同時に管理ユーザーになることができ、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、各ユーザーは現在アクセスしている全ユーザーのアクセス状況を確認することができ、管理ユーザーならば他のユーザーの接続を強制的に切断させることもできます。

2.1.1 コンソールによる設定手順

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

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

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

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

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

設定手順のおおまかな流れは次のようになります。

1. 一般ユーザ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 Crtl キーを押しながら Q キーを押します。

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

新たに管理ユーザ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。 セキュリティー上、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 FWX120 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。
- セキュリティーの設定や、詳細な各種パラメータなどの付加的な設定に関しては、個々のネットワークの運営方針などに基づいて行ってください。

2.1.2 CONSOLE または SERIAL ポートからの設定

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

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

2. [デバイスマネージャ]をクリックします。

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

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

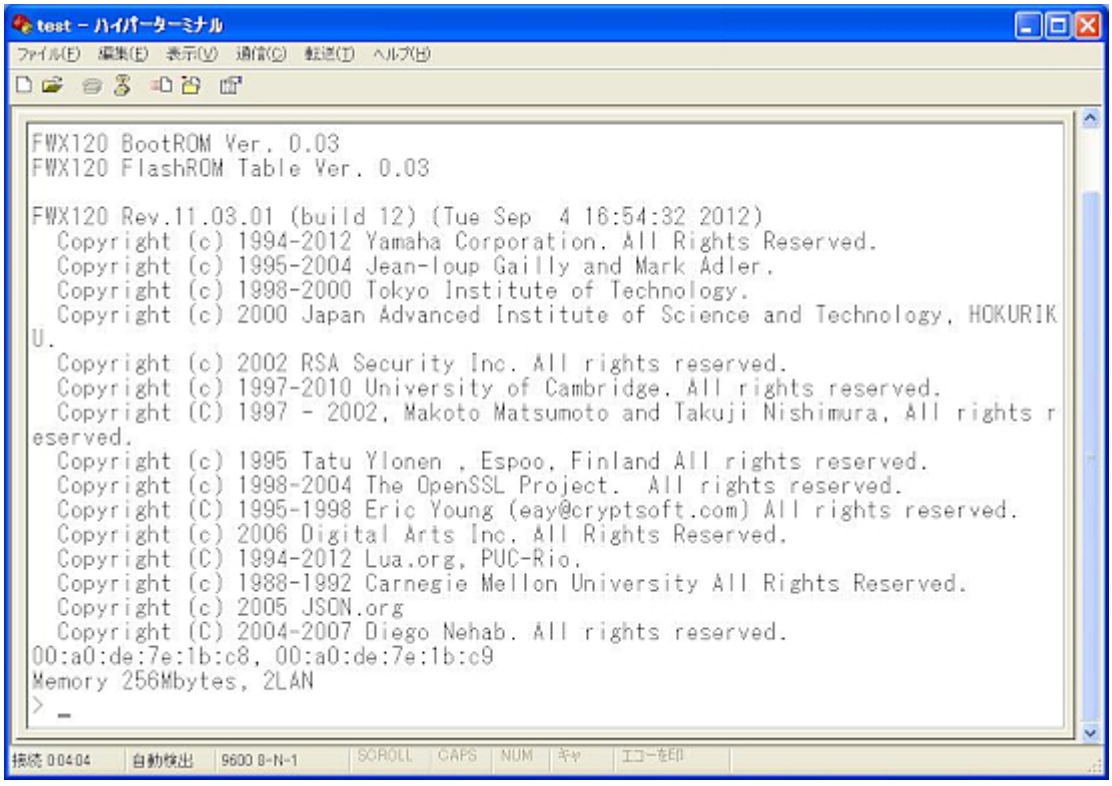
5. 「接続方法」欄から、手順 2 で調べた COM ポートを選択して[OK]をクリックします。

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

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

   ※TELNET 複数セッション機能対応機種で設定した名前ありユーザ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。
   以下の例はログインしたときの表示です。



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。

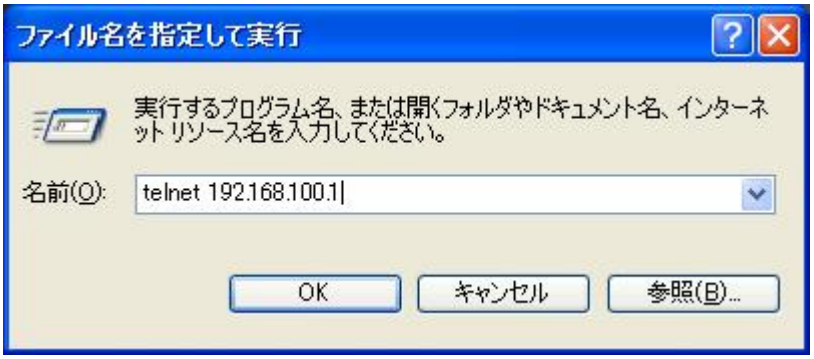
2.1.3 TELNET による設定

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

1. [スタート]メニューから[ファイル名を指定して実行]を選びます。

2. 「telnet 192.168.100.1」と入力してから、[OK]をクリックします。

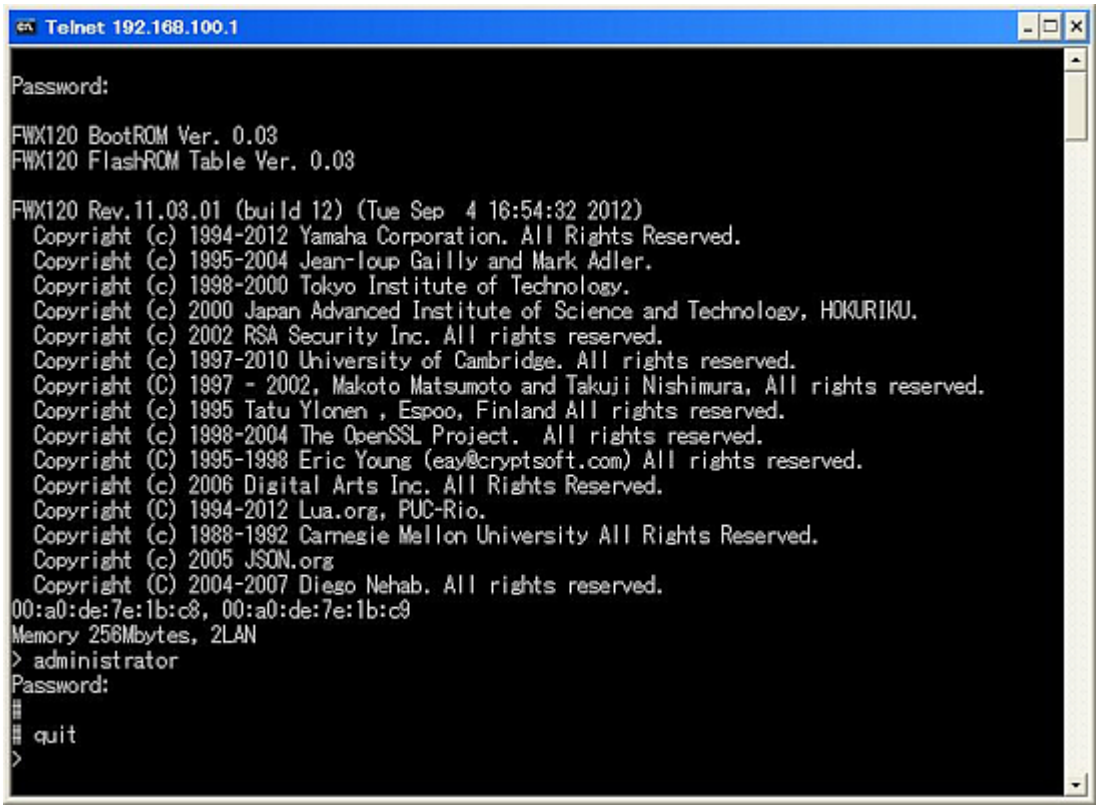
   本機の IP アドレスを変更している場合には、「192.168.100.1」のかわりにその IP アドレスを入力します。



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

   ※TELNET 複数セッション機能対応機種で設定した名前ありユーザ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。



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。

4. **administrator** と入力してから、Enter キーを押します。
5. 「Password:」と表示されたら、管理パスワードを入力します。

   「#」が表示されると、各種のコンソールコマンドを入力できます。
6. コンソールコマンドを入力して、設定を行います
7. 設定が終わったら、**save** と入力してから Enter キーを押します。

   コンソールコマンドで設定した内容が、本機の不揮発性メモリに保存されます。
8. 設定を終了するには、**quit** と入力してから Enter キーを押します。
9. コンソール画面を終了するには、もう 1 度 **quit** と入力してから Enter キーを押します。

2.2 SSH サーバーについて

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

2.2.1 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。

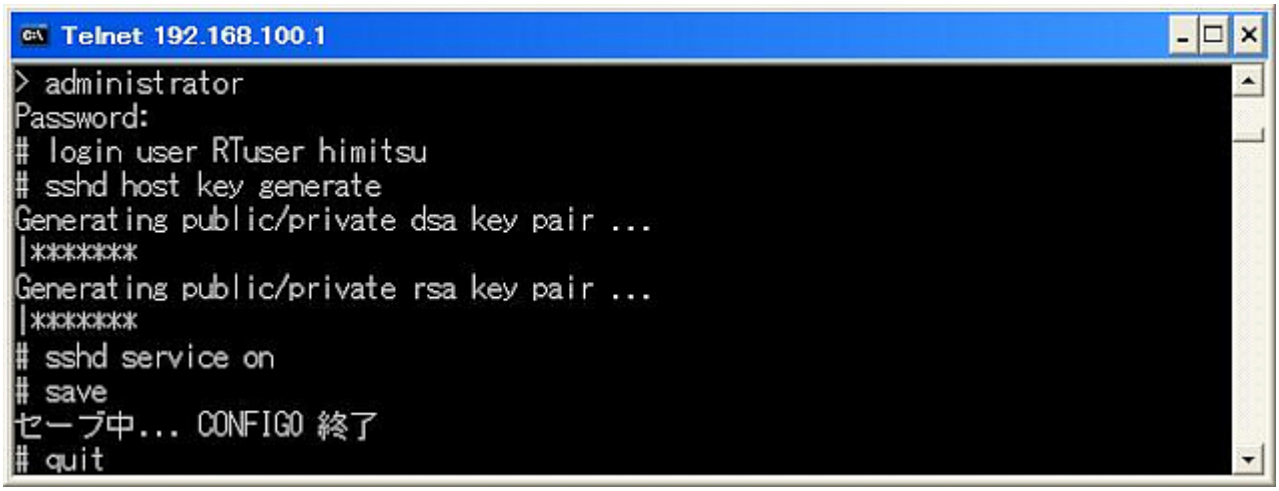
- SSH プロトコルバージョン 1
- パスワード認証以外のユーザー認証 (ホストベース認証、公開鍵認証、チャレンジ・レスポンス認証、GSSAPI 認証)
- ポートフォワーディング (X11/TCP 転送)
- Gateway Ports(ポート中継)
- 空パスワードの許可

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ーを登録します。SSH ではログイン時のユーザー名の入力が必須となるため、事前に必ず名前ありユーザーを登録しなければなりません。

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



2.3 TFTP について

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

TFTP は、Windows XP や MacOS X の『ターミナル』アプリケーション、UNIX 環境で標準的に搭載されており、実行することができます。TFTP が搭載されていない環境では、フリーソフトなどで TFTP クライアント機能のあるものを用意してください。この時、ヤマハルーター は TFTP サーバーとして動作します。
設定ファイルは全体の設定を記述したものであり、特定部分の設定だけを読み出したり差分点だけを書き込んだりすることはできません。設定ファイルは Windows のメモ帳等で直接編集できるテキストファイル (シフト JIS、CRLF 改行) です。
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。

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

2.3.1 TFTP による設定手順

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

次に、LAN 上のホストから TFTP コマンドを実行します。使用するコマンドの形式は、そのホストの OS に依存します。次の点に注意して実行してください。
- 本機の IP アドレス
- 転送モードは“アスキー”、"ascii" または“文字”にします。
  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

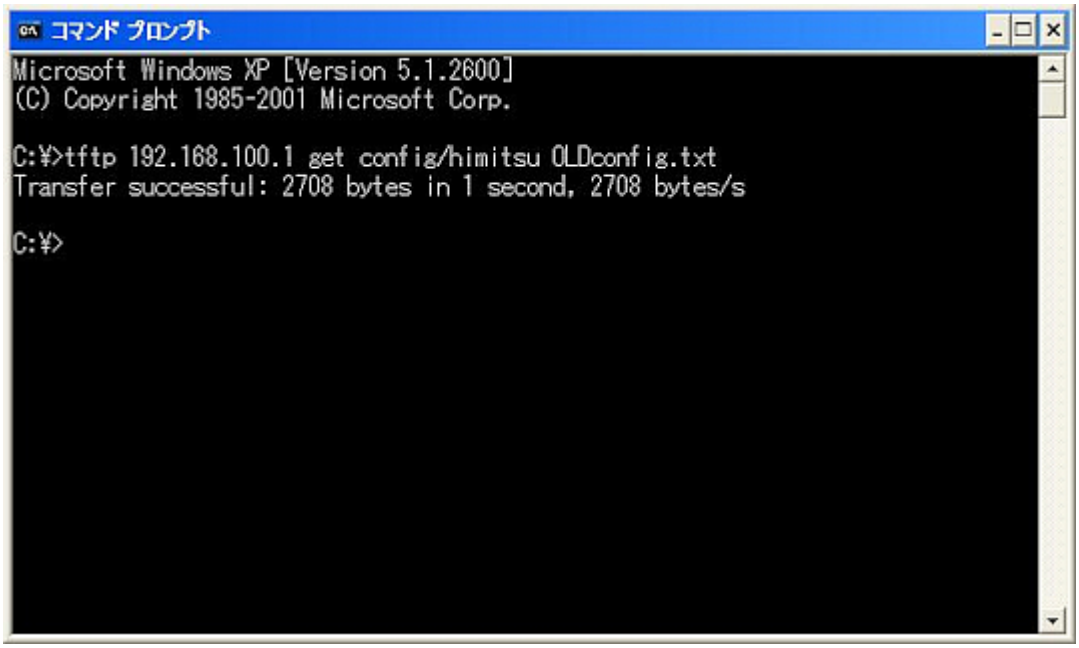
ここでは、Windows XP から設定ファイルを読み出す場合の例を示します。ヤマハルーターのコンソール操作ではないことに注意してください。この例では、ヤマハルーター の IP アドレスを 192.168.100.1、管理パスワードは“himitsu”、Windows に新しくできるファイルの名称を“OLDconfig.txt”とします。

1. [スタート]メニューから[すべてのプログラム]-[アクセサリ]-[コマンドプロンプト]を選びます。
2. 設定ファイルを保存するディレクトリに移動します。
3. **tftp 192.168.100.1 get config/himitsu OLDconfig.txt** と入力してから、Enter キーを押します。

   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 192.168.100.1 get config-encryption-aes128/himitsu OLDconfig.txt

   と入力してから、Enter キーを押します



2.3.3 設定ファイルの書き込み

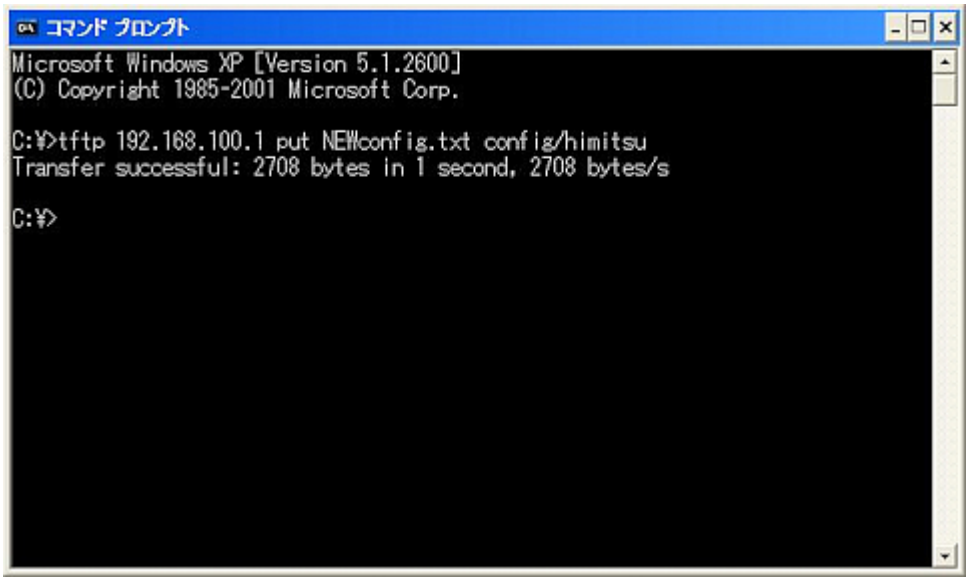
ここでは、Windows XP から設定ファイルを書き込む場合の例を示します。ヤマハルーター のコンソール操作ではないことに注意してください。この例では、ヤマハルーター の IP アドレスを 192.168.100.1、管理パスワードは“himitsu”、書き込むべき Windows 上のファイルの名称を“NEWconfig.txt”とします。

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

   暗号化された設定されたファイル"NEWconfig.rtfg"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 192.168.100.1 put NEWconfig.rtfg config/himitsu

   と入力してから、Enter キーを押します。



2.4 コンソール使用時のキーボード操作について

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

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

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

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

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

show config、**show config list**、**show config pp**、**show config tunnel**、**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 file list**、**less log** コマンドを使用します。

キーボード操作	説明・備考
{n} f	{n}画面先に進める
{n} Ctrl-F	
{n} SPACE	
{n} b	{n}画面後ろに戻す
{n} Ctrl-B	
{n} j	{n}行先に進める
{n} Ctrl-J	
{n} Ctrl-E	
{n} Ctrl-M	
{n} ENTER	
{n} RETURN	

キーボード操作	説明・備考
{n} k	{n}行後ろに戻す
{n} Ctrl-K	
{n} y	
{n} Ctrl-Y	
{n} Ctrl-P	
{n} d	{n}半画面先に進める
{n} Ctrl-D	
{n} u	{n}半画面後ろに戻す
{n} Ctrl-U	
{n} g	{n}行目へ移動
	{n]省略時は先頭行
{n} G	{n}行目へ移動
	{n]省略時は末尾行
{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' などに一致する。一方、-i オプションがなければ、'abc' は 'abc'

としか一致しない。
-v オプションを指定した時には、*pattern* に一致しない行を表示する。
-w オプションを指定した時には、*pattern* に一致するのは単語だけとなる。例えば、-w オプションがある時には 'IP' という *pattern* は 'IPv4' や 'IPv6' とは一致しないが、' IP '(前後に空白がある) や '[IP]' には一致する。一方、-w オプションが無ければ先に上げた例にはすべて一致する。
pattern は限定された正規表現である。一般的な正規表現では多くの特殊文字を使って多様な検索パターンを構成できるが、ここで実装されているのは以下の特殊文字のみである。

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

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

2.5.2 show コマンドの表示内容を見やすくする

[書式]

show [...] | **less**

[説明]

show コマンドの表示内容を 1 画面単位で表示し、最終行でコマンドを受け付ける。
表示内容が 1 画面に満たない場合には、すべての内容を表示して終了する。
コマンドは、数値プレフィクスとコマンド文字を入力することで実行される。数値プレフィクスはオプションで省

略できる。数値プレフィクスを省略した場合には 1 と見なされる。検索コマンドでは、コマンド文字の後に検索文字列を入力できる。

コマンドには以下の種類がある。

コマンド	内容 (数値プレフィックスを 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。

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
```

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。

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。

filename は半角 99 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
```

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。

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。

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]

一般ユーザー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)。

4.2 ログインパスワードの暗号化保存

[書式]

login password encrypted

[説明]

無名ユーザーのパスワードを 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。

4.3 管理パスワードの設定

[書式]

administrator password

[説明]

管理ユーザー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)。

4.4 管理パスワードの暗号化保存

[書式]

administrator password encrypted

[説明]

管理ユーザーのパスワードを 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。

4.5 ログインユーザー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] : ユーザー名 (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]

ログインユーザー名とパスワードを設定する。

登録できるユーザーは最大 32 人。

ユーザー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]

同一のユーザー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ー名で設定を行った場合は、元の設定が上書きされる。

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

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**

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**

4.8 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。

設定値	説明
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。

- 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。
インターフェース名	指定したインター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
120..21474836	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
  - 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。

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、タイマ値は 300 秒として扱う。

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

[ノート]

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。

4.9 他のユーザーの接続の強制切断

[書式]

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

[設定値及び初期値]

- *user*
  - [設定値] : ユーザー名
  - [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]

他ユーザーの接続を切断する。

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。

無名ユーザーを切断する場合は、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。

[設定例]

例 1) ユーザー名「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ーを切断する。

```
# disconnect user /telnet
```

4.10 セキュリティークラスの設定

[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" (ダブリュー、カンマ、エル、エックス、エル、エム、エー) でもログインでき、設定の変更も可能になる。ただしシリアルのみ
off	パスワードを入力しないとログインできない

  - [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]

セキュリティークラスを設定する。

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には FOMA 網を利用するため、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ーが接続している場合は、接続しているユーザーはそれを維持することができるが、接続しているユーザー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 キーワードは Rev.11.03.04 以降で使用可能。

4.11 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。

4.12 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。

4.13 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。

4.14 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。

4.15 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 10 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 16 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、**rdate** コマンドを使用した場合よりも精密な時計合わせが可能になる。
NTP サーバーはできるだけ近くのものを指定した方が良い。利用可能な NTP サーバーについてはプロバイダに問い合わせること。
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。

4.16 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、出力インターフェースの IP アドレスを利用する。

4.17 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。

4.18 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 (64 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。

4.19 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
ascii	英語で表示する、文字コードは ASCII
sjis	日本語で表示する、文字コードはシフト JIS
euc	日本語で表示する、文字コードは EUC

  - [初期値] : sjis

[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ーでも実行できる。

[ノート]

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。

4.20 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 (80..200)
  - [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ーでも実行できる。

[ノート]

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。

4.21 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ーでも実行できる。

[ノート]

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。

4.22 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。

4.23 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。

4.24 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。

4.25 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。

4.26 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。

4.27 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。

4.28 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、出力インターフェースの IP アドレスを利用する。

4.29 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。

4.30 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。

4.31 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。

4.32 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。

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

[書式]

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

[設定値及び初期値]

- *ip_range* : TELNET サーバーへアクセスを許可するホストの IP アドレス範囲のリストまたはニーモニック
  - [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	指定されたホストからのアクセスを許可する
any	すべてのホストからのアクセスを許可する
none	すべてのホストからのアクセスを禁止する
lan	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
LAN インターフェース名	指定したインターフェースへの接続のみ許可する
ブリッジインターフェース名	指定したインターフェースへの接続のみ許可する

- [初期値] : any

[説明]

TELNET サーバーへアクセスできるホストの IP アドレスを設定する。

[ノート]

ニーモニックをリストにすることはできない。
設定後の新しい TELNET 接続から適用される。

lan キーワードは Rev.11.03.27 以降で指定可能。

4.34 TELNET サーバーへ同時に接続できるユーザー数の設定

[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ー数を設定する。

[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ーが接続している場合は、接続しているユーザーはそれを維持することができるが、接続しているユーザー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。

4.35 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。

4.36 LAN インター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 インターフェース名
  - [初期値] : -
- *port*
  - [設定値] : ポート番号
  - [初期値] : -

[説明]

LAN インター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 インターフェース、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。

4.37 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。

4.38 LAN インター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 インターフェース名
  - [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。

4.39 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 インターフェース名
  - [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ーフェースにおいて、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 インターフェース名にはスイッチングハブを持つインターフェースだけが指定可能である。

[ノート]

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

[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
```

4.40 LAN インターフェースの動作タイプの設定

[書式]

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

no lan type *interface* [...]

[設定値及び初期値]

- *interface_with_swhub*
  - [設定値] : スイッチングハブを持つ LAN インターフェース名
  - [初期値] : -
- *interface_without_swhub*
  - [設定値] : スイッチングハブを持たない LAN インターフェース名
  - [初期値] : -
- *interface*
  - [設定値] : LAN インターフェース名
  - [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
      - インター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
divide-network	LAN 分割機能を有効にする

設定値	説明
split-into-split_pattern	ポート分離機能を有効にする(基本機能)
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)	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

- [初期値] :
  - mtu=1500
  - auto-crossover=on
  - macaddress-aging=300
  - port-based-ks8995m/port-based-option=off
  - speed-downshift=on

[説明]

指定した LAN インター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 インター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、"port-based-option" を入力する。Rev.11.03 系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*

インター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 インター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 インターフェースでは、64～1500 の範囲となる。

インターフェースの *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* としてはインターフェースの *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、インターフェースの *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。インターフェースの *mtu* も含めてすべて設定されていない時には、デフォルト値である 1500 が利用される。

○オートクロスオーバー機能

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

○MAC アドレスエージング機能

スイッチングハブを持つ LAN インター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。

機種	設定範囲
FWX120	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
FWX120	1024

○LAN 分割機能
スイッチングハブを持つ LAN インターフェースでのみ利用できる。

LAN 分割機能には基本機能と拡張機能があります。

基本機能では、スイッチングハブの各ポートが個別の LAN インターフェースとして動作する。各インターフェースにはそれぞれ個別の IP アドレスを付与でき、その間でのルーティグも可能になる。
例えば FWX120 は通常は LAN インターフェースを 2 つ持つルーターだが、LAN 分割機能を使えば LAN インターフェースを 5 個利用できることになる。

拡張機能では、スイッチングハブの各ポートを自由に組み合わせて 1 つの LAN インターフェース (VLAN インターフェース) とすることができる。
同一の VLAN インター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ー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 インターフェースのインターフェース名は元の LAN インター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、FWX120 は lan1 が 4 ポートのスイッチングハブを持つ LAN インターフェースなので、以下の LAN インターフェースが使用できるようになる。

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

拡張機能では、LAN インターフェースのインターフェース名として vlan1、vlan2、vlan3・・・(VLAN インターフェース) を使用する。基本機能とは異なり、VLAN インター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 インター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 インター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 インターフェース
FWX120	vlan1-vlan4

LAN 分割機能を有効にした場合、lan1 インター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 インターフェースの MAC アドレスは元の LAN インターフェースの 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
スイッチングハブを持つ LAN インター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。

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 インター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 インター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

同一 LAN インター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。

[ノート]

本コマンドの実行後、LAN インター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。

[設定例]

1. スイッチングハブを持つ LAN インターフェースで、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 インターフェースで、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。

   ```
   # lan type lan1 100-fdx 1 port-based-option=divide-network
   ```
3. スイッチングハブを持つ LAN インターフェースで、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。
   - 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-option=split-into-12:34
     ```

4.41 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	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。

4.42 TFTP によりアクセスできるホストの IP アドレスの設定

[書式]

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

[設定値及び初期値]

- *host*
  - [設定値] :

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

  - [初期値] : none

[説明]

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

[ノート]

セキュリティーの観点から、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。

4.43 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 インターフェース名
  - [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 インター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 インターフェースのディレクティッドブロードキャスト宛でなくてはいけない。

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

broadcast を指定した場合には、MagicPacket をブロードキャストパケットとして LAN インター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。

4.44 インター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 インターフェース名、WAN インターフェース名、'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、あるいはインター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。
インター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** で選択したインター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、インターフェースに対する設定内容はインターフェースに対する **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。

4.45 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 IP アドレス
  - [設定値] :
    - xxx.xxx.xxx.xxx は
      - 10 進数
      - *(ネットマスクの対応するビットが 8 ビットとも 0 と同じ)
    - 間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定
    - *(すべての IP アドレス)
  - [初期値] : -
- *dst_addr* : 終点 IP 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] :
    - "0xffffff00"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

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

Rev.11.03.04 以降で *src_port_list* または *dst_port_list* に submission を指定可能。

[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 )
```

4.46 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。

4.47 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/fwx120.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。

4.48 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。

4.49 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。

4.50 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
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。

4.51 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。

4.52 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*
no http revision-up schedule [*period time1 time2*]

[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、指定した日が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 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。

[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
```

4.53 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。

4.54 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。

4.55 SSH サーバーへアクセスできるホストの IP アドレスの設定

[書式]

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

[設定値及び初期値]

- *ip_range* : SSH サーバーへアクセスを許可するホストの IP アドレス範囲のリストまたはニーモニック
  - [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	指定されたホストからのアクセスを許可する
any	すべてのホストからのアクセスを許可する
none	すべてのホストからのアクセスを禁止する
LAN インターフェース名	SSH サーバーへアクセスを許可する LAN インターフェース名
ブリッジインターフェース名	SSH サーバーへアクセスを許可するブリッジインターフェース名

  - [初期値] : any

[説明]

SSH サーバーへアクセスできるホストの IP アドレスを設定する。

[ノート]

ニーモニックをリストにすることはできない。
設定後の新しい SSH 接続から適用される。

4.56 SSH サーバーへ同時に接続できるユーザー数の設定

[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ー数を設定する。

[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ーが接続している場合は、接続しているユーザーはそれを維持することができるが、接続しているユーザー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。

4.57 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

[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、Rev.11.03.22 以降で使用可能。

4.58 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
cast128-cbc	CAST-128-CBC
arcfour	Arcfour

  - [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。

4.59 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。

4.60 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ー目的として OpenSSH のバージョン情報を隠匿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。
Rev.11.03.13 以降で使用可能。

4.61 SFTP サーバーへアクセスできるホストの IP アドレスの設定

[書式]

sftpd host *ip_range* [*ip_range* ...]
no sftpd host [*ip_range*...]

[設定値及び初期値]

- *ip_range* : SFTP サーバーへアクセスを許可するホストの IP アドレス範囲のリストまたはニーモニック
  - [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	指定されたホストからのアクセスを許可する
any	すべてのホストからのアクセスを許可する
none	すべてのホストからのアクセスを禁止する
LAN インターフェース名	SFTP サーバーへアクセスを許可する LAN インターフェース名
ブリッジインターフェース名	SFTP サーバーへアクセスを許可するブリッジインターフェース名

  - [初期値] : none

[説明]

SFTP サーバーへアクセスできるホストの IP アドレスを設定する。

[ノート]

対象となるホストは **sshd 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。
ニーモニックをリストにすることはできない。
設定後の新しい SFTP 接続から適用される。

4.62 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ー名を使用して 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回だけサーバーに送られる。

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]

Rev.11.03.04 以降で使用可能。

4.63 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ー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* の両方にルーター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。

ルーターの設定ファイル (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、ルーターの exec0 にファイルをコピーする。

```
# scp user@192.168.1.1:fwx120.bin exec0
```

ルーター上のファイル 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]

Rev.11.03.04 以降で使用可能。

4.64 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
cast128-cbc	CAST-128-CBC
arcfour	Arcfour

  - [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。

Rev.11.03.04 以降で使用可能。

4.65 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]

Rev.11.03.04 以降で使用可能。

4.66 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, 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] :

    FWX120

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

[説明]

パケットバッファの管理パラメータを変更する。

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

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

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

[設定例]

```
# system packet-buffer small max-buffer=1000 max-free=500
# system packet-buffer large min-free=50
```

4.67 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 [*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]

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。

4.68 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 [*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]

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。

4.69 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。

4.70 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 [*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]

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。

4.71 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。

4.72 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。

4.73 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。

4.74 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 '_' が使用できるが、アンダースコアまたは数字を最初の文字にすることはできない。
変数名の長さに制限はないが、**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。
英字の大文字、小文字を区別する。例えば、abc と Abc は別の変数として扱われる。

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。

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。

第 6 章

IP の設定

6.1 インターフェース共通の設定

6.1.1 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。

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

インターフェースの 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 インターフェースに 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 インターフェースに IP アドレスを設定していない場合には、そのインターフェースは unnumbered として動作する。
DHCP クライアントとして動作させた場合に取得したクライアント ID は、**show status dhcpc** コマンドで確認することができる。

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。

6.1.3 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
ip *bridge_interface* **secondary address** *ip_address*/*mask*
ip *bridge_interface* **secondary address** dhcp
no ip *interface* **secondary address** [*ip_address*/*mask*]
no ip *bridge_interface* **secondary address** [*ip_address*/*mask*]

[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] : -
- *bridge_interface*
  - [設定値] : ブリッジインターフェース名
  - [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]

インターフェースのセカンダリ 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。

6.1.4 インターフェースの 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 インターフェース名、WAN インターフェース名
  - [初期値] : -
- *mtu0,mtu1,mtu2*
  - [設定値] : MTU の値 (64..1500)
  - [初期値] :
    - mtu0=1500
    - mtu1=1500
    - mtu2=1280

[説明]

各インターフェースの 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。

6.1.5 同一インター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 インターフェース名
  - [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

設定値	説明
off	折り返すパケットを送信しない

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

[説明]

同一インター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。

6.1.6 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。

6.1.7 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* : PP インターフェースへの経路
      - *peer_num*
        - 相手先情報番号
    - pp anonymous name=*name*

設定値	説明
name	PAP/CHAP による名前

    - dhcp *interface*

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(送り先が Default の時のみ有効)

    - tunnel *tunnel_num* : トンネルインターフェースへの経路
    - LOOPBACK インターフェース名、NULL インターフェース名
  - [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 *number* [*number*..]	フィルター型経路の指定 • *number* • フィルターの番号 (1..21474836) (空白で区切り複数設定可能)

metric *metric*	メトリックの指定
	• *metric*
	  • メトリック値 (1..15)
	  • 省略時は 1

hide	出力インターフェースが LAN インターフェース、または WAN インターフェース、PP インターフェース、TUNNEL インターフェースの場合のみ有効なオプションで、相手先が接続されている場合だけ経路が有効になることを意味する

weight *weight*	異なる経路間の比率を表す値
	• *weight*
	  • 経路への重み (0..2147483647)
	  • 省略時は 1

keepalive *keepalive_id*	*gateway1* に到達性のあるときにだけ有効となる • *keepalive_id* • キープアライブの識別子 (1..100)

  - [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ー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ーを適用していき、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、フィルター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、フィルター型経路が指定されていないゲートウェイが選択される。
フィルター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。
フィルター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 インターフェース、NULL インター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。

[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 、PP2 は PPPoE で接続しており、かつ各回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
```

6.1.8 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)
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 (ログに記録しない)
restrict-log	回線が接続されていれば通し、切断されていれば破棄する (ログに記録する)
restrict-nolog	回線が接続されていれば通し、切断されていれば破棄する (ログに記録しない)

  - [初期値] : -
- *src_addr* : IP パケットの始点 IP 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事が出来る。FQDN と混合する事も可能
  - 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為、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事が出来る。IP アドレスと混合する事も可能
  - * (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 IP 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] : -
- *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
udp	17	UDP パケット
ipv6	41	IPv6 パケット
gre	47	GRE パケット
esp	50	ESP パケット
ah	51	AH パケット
icmp6	58	ICMP6 パケット

    - 上項目のカンマで区切った並び (5 個以内)
    - 特殊指定

icmp-error	TYPE が 3、4、5、11、12、31、32 のいずれかである ICMP パケット
icmp-info	TYPE が 0、8〜10、13〜18、30、33〜36 のいずれかである ICMP パケット
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 *mask* の値の論理積 (AND) が、*value* に一致、または不一致である TCP パケット *value* と *mask* は 0x に続く十六進数で 0x0000～0xffff
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
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/tcprst/established/tcpflag)、UDP(udp) のいずれかが含まれる場合は、TCP/UDP のデスティネーションポート番号。*protocol* が ICMP(icmp) 単独の場合には、ICMP コード
  - [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** *interface* **secure filter**、**ip filter set**、**ip filter dynamic**、および **ip** *interface* **rip filter** コマンドで用いられる。

[ノート]

restrict-log 及び restrict-nolog を使ったフィルターは、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' 単独である場合にのみ、*src_port_list* は ICMP タイプ、*dest_port_list* は ICMP コードと見なされる。*protocol* に 'icmp' と他のプロトコルを列挙した場合には *src_port_list* と *dest_port_list* の指定は TCP/UDP のポート番号と見なされ、ICMP パケットとの比較は行われない。また、*protocol* に 'icmp-error' や '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.11.03.04 以降で *src_port_list* または *dest_port_list* に submission を指定可能。

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事が出来る。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。

src_addr および *dest_addr* への FQDN の指定は Rev.11.03.25 以降のファームウェアで指定可能。

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。

[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 * *
```

6.1.9 フィルターセットの定義

[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] : フィルター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ー
out	出力方向のフィルター

  - [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 (1000 個以内)
  - [初期値] : -

[説明]

フィルターセットを定義する。フィルターセットは、in/out のフィルターをそれぞれ定義し、RADIUS による指定や、**ip** *interface* **secure filter** コマンドによりインターフェースに適用される。

6.1.10 Source-route オプション付き IP パケットをフィルター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	フィルターアウトする
off	フィルターアウトしない

  - [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ーアウトするか否かを設定する。

6.1.11 ディレクテッドブロードキャストパケットをフィルター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	フィルターアウトする
off	フィルターアウトしない

  - [初期値] : on
- *filter_num*
  - [設定値] : 静的フィルター番号 (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ーでパケットを検査し、PASS フィルター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。

6.1.12 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*
  - [設定値] : 始点 IP アドレス
  - [初期値] : -
- *dstaddr*

  - [設定値] : 終点 IP アドレス
  - [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)
  - [初期値] : -
- *protocol* : プロトコルのニーモニック
  - [設定値] :
    - 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/submission

    以下のニーモニックは設定できますが、動的フィルターとして動作しません
    - dhcpc/dhcps/dhcpv6c/dhcpv6s
  - [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) 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。

[設定例]

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

6.1.13 動的フィルター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]

動的フィルター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。

6.1.14 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]

Rev.11.03.25 以降で使用可能。

6.1.15 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 インターフェース名、WAN インターフェース名
  - [初期値] : -
- *direction* : 観察するパケット・コネクションの方向
  - [設定値] :

設定値	説明
in	インターフェースの内向き
out	インターフェースの外向き

  - [初期値] : -
- *type* : 観察するパケット・コネクションの種類
  - [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]

指定したインターフェースで、指定された向きのパケットやコネクションについて異常を検知する。
type 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。

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。

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。

6.1.16 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 インターフェース名、WAN インターフェース名
  - [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。

6.1.17 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 インターフェース名、WAN インターフェース名
  - [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。

6.1.18 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 インターフェース名、WAN インターフェース名
  - [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。

6.1.19 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 インターフェース名、WAN インターフェース名
  - [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] :
    - off(Rev.11.03.22 以前)
    - auto(Rev.11.03.25 以降)

[説明]

インターフェースを通過する TCP セッションの MSS を制限する。インター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、インターフェースの MTU、もしくは PP インター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 インター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。

6.1.20 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 インターフェース名、WAN インターフェース名
  - [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]

Rev.11.03.22 以降で使用可能。

6.1.21 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] : 15000

[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。

6.1.22 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。

6.1.23 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 128 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て、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か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。
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。

6.1.24 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 *filter_num*	*filter_num* は **ip filter** コマンドで登録されたフィルター番号

  - [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、経路の途中に ICMP パケットをフィルターするファイアウォールなどがあるとアルゴリズムがうまく動作せず、特定の通信相手とだけは通信ができないなどの現象になることがある。この様な現象は、「経路 MTU 探索ブラックホール (Path MTU Discovery Blackhole)」と呼ばれている。この経路 MTU 探索ブラックホールがある場合には、このコマンドでそのような相手との通信に関して DF ビットを 0 に書き換えてしまえば、経路 MTU 探索は正しく動作しなくなるものの、通信できなくなるということはなくなる。

6.1.25 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
max-reliability	2

ニーモニック	TOS 値
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] : 静的フィルターの番号 (1..21474836)
  - [初期値] : -
- *filter_num_list*
  - [設定値] : 静的フィルターの番号 (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* リストのフィルターを順次適用していく。そして、最初にマッチした IP フィルターが 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。

6.1.26 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 インターフェース名
  - [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 インターフェースの実 MAC アドレスとなる。

第 2 書式を設定した時には、指定された VRID での VRRP の状態がマスターである場合のみ代理 ARP 動作を行う。利用する MAC アドレスは指定された VRID の仮想 MAC アドレスとなる。

6.1.27 ARP エントリーの寿命の設定

[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 エントリーの寿命秒数 (30..32767)
  - [初期値] : 1200
- *retry*
  - [設定値] : ARP の再送回数 (4..100)
  - [初期値] : 4

[説明]

ARP エントリーの寿命を設定する。ARP 手順で得られた IP アドレスと MAC アドレスの組は ARP エントリー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ーは消される。ただし、エントリー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ーは消される。
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。

6.1.28 静的 ARP エントリーの設定

[書式]

ip *interface* **arp static** *ip_address mac_address*
no ip *interface* **arp static** *ip_address*[...]

[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] : -
- *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] : -

[説明]

ARP エントリーを静的に設定する。このコマンドで設定された ARP エントリーは、**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ーは消えない。

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、インターフェースの MTU を固定で利用する。

6.1.29 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]

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。

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。

6.1.30 ARP エントリー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]

- *interface*
  - [設定値] : LAN インターフェース名
  - [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 エントリー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 エントリー履歴を確認することができる。

6.1.31 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ー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ー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 インター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 インターフェースを経由する implicit 経路として登録されている。

6.1.32 フローテーブルの各エントリーの寿命を設定する

[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
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
    - 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ー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ーには 'slow' が適用される。
NAT や動的フィルターを使用している場合には、それらのエントリーの寿命が適用される。

6.2 PP 側の設定

6.2.1 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 インターフェース名
    - 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。
dhcpc を設定した場合は、*interface* で指定した LAN インターフェースが 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。

6.2.2 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 インターフェース名
    - 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 インターフェースが 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 46。

6.2.3 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)..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 インター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。

6.2.4 PP 経由のキープアライブを使用するか否かの設定

[書式]

pp keepalive use lcp-echo
pp keepalive use icmp-echo *dest_ip* [*option=value...*] [*dest_ip* [*option=value...*]...]
pp keepalive use lcp-echo icmp-echo *dest_ip* [*option=value...*] [*dest_ip* [*option=value...*]...]
pp keepalive use off
no pp keepalive use

[設定値及び初期値]

- 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)
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 インターフェースが送出先となるよう設定される必要がある。

downwait パラメータで応答時間を制限する場合でも、**pp keepalive interval** コマンドの設定値の方が小さい場合には、**pp keepalive interval** コマンドの設定値が優先される。downwait、upwait パラメータのうち一方しか設定していない場合には、他方も同じ値が設定されたものとして動作する。

disconnect パラメータは、PPPoE で使用する場合に PPPoE レベルでの再接続が必要な場合に使用する。disconnect パラメータが設定されている場合に、設定時間内に icmp-echo の応答がない場合、PPPoE レベルで一度切断操作を行うため、**pp always-on** コマンドとの併用により再接続を行うことができる。

他のパラメータがデフォルト値の場合、disconnect パラメータは 70 秒程度に設定しておくと、ダウン検出後の切断動作が確実に行われる。

length パラメータで指定するのは ICMP データ部分の長さであり、IP パケット全体の長さではない。

6.2.5 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。

6.2.6 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、*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。

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**
- 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**

[ノート]

PP 毎のコマンドである。
PP として anonymous が選択された時には無効である。

6.3 RIP の設定

6.3.1 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、すべてのインターフェースに対して 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。

6.3.2 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 インターフェース名
  - [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]

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。

6.3.3 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] : 優先度 (1..2147483647)
  - [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 Rev.11.03.04 以降で指定可能。

6.3.4 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 インターフェース名
  - [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 (トンネルインターフェースの場合)
  - on (その他のインターフェースの場合)

- *version*
  - [設定値] : 送信する RIP のバージョン (1,2)
  - [初期値] : 1(トンネルインター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]

指定したインターフェースに対し、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。

6.3.5 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 インターフェース名
  - [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(トンネルインターフェースの場合)
    - on (その他のインターフェースの場合)
- *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]

指定したインターフェースに対し、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。

6.3.6 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 インターフェース名
  - [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ー番号の並び (100 個以内)
  - [初期値] : -

[説明]

インター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ーの始点 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、フィルターが 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。

6.3.7 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 インターフェース名
  - [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]

インター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。

6.3.8 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 インターフェース名
  - [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ー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。

6.3.9 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 インターフェース名
  - [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ーフェースの認証キーを設定する。

[設定例]

```
# ip lan1 rip auth key text testing123
# ip pp rip auth key text "hello world"
# ip lan2 rip auth key 01 02 ff 35 8e 49 a8 3a 5e 9d
```

6.3.10 回線切断時の経路保持の設定

[書式]

ip pp rip hold routing *rip_hold*
no ip pp rip hold routing [*rip_hold*]

[設定値及び初期値]

- *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 インターフェースから 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。

6.3.11 回線接続時の PP 側の RIP の動作の設定

[書式]

ip pp rip connect send *rip_action*
no ip pp rip connect send [*rip_action*]

[設定値及び初期値]

- *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
```

6.3.12 回線接続時の PP 側の RIP 送出の時間間隔の設定

[書式]

ip pp rip connect interval *time*
no ip pp rip connect interval [*time*]

[設定値及び初期値]

- *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
```

6.3.13 回線切断時の PP 側の RIP の動作の設定

[書式]

ip pp rip disconnect send *rip_action*
no ip pp rip disconnect send [*rip_action*]

[設定値及び初期値]

- *rip_action*
  - [設定値] :

設定値	説明
none	回線切断時に RIP を送出しない
interval	**ip pp rip disconnect interval** コマンドで設定された時間間隔で RIP を送出する
update	経路情報が変わった時にのみ RIP を送出する

- [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 を送出する条件を設定する。

[設定例]

```
# ip pp rip disconnect interval 1800
# ip pp rip disconnect send interval
```

6.3.14 回線切断時の PP 側の RIP 送出の時間間隔の設定

[書式]

ip pp rip disconnect interval *time*
no ip pp rip disconnect interval [*time*]

[設定値及び初期値]

- *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
```

6.3.15 バックアップ時の RIP の送信元インター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 の送信元インターフェースを切り替えるか否かを設定する。RIP の送信元インターフェースは、off のときには、バックアップ元のインターフェースであり、on のときには、バックアップ先のインターフェースとなる。

[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ー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ー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。

6.3.16 RIP で強制的に経路を広告する

[書式]

ip *interface* **rip force-to-advertise** *ip-address*/*netmask* [metric *metric*]
ip pp rip force-to-advertise *ip-address*/*netmask* [metric *metric*]
ip tunnel rip force-to-advertise *ip-address*/*netmask* [metric *metric*]
no ip *interface* **rip force-to-advertise** *ip-address*/*netmask* [metric *metric*]
no ip pp rip force-to-advertise *ip-address*/*netmask* [metric *metric*]
no ip tunnel rip force-to-advertise *ip-address*/*netmask* [metric *metric*]

[設定値及び初期値]

- *interface*
  - [設定値] : LAN インターフェース名
  - [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、指定されたインターフェースに対し、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。

[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
```

6.3.17 RIP2 でのフィルターの比較方法

[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 エントリーのアドレス部がその範囲に入っているかどうかを比較する。
	RIP2	
with-netmask	RIP1	
	RIP2	ネットマスク型のフィルターの、アドレスとネットマスク、RIP エントリーのアドレス、ネットマスクと一致するかどうかを比較する。

6.3.18 RIP のタイマーを調整する

[書式]

rip timer *update* [*invalid* [*holddown*]]
no rip timer [*update*]

[設定値及び初期値]

- *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。

update×3 ≦ *invalid* ≦ *update*×6
update×2 ≦ *holddown* ≦ *update*×4

[ノート]

PP インターフェースに対し、**ip pp rip connect/disconnect interval** コマンドが設定されているときは、そのコマンドの設定値が **rip timer** コマンドに優先する。ただし、**ip pp rip connect/disconnect interval** コマンドは *update* タイマーと *invalid* タイマーの値に影響するが、*holddown* タイマーの値には影響しない。**ip pp rip connect/disconnect interval** コマンドの設定値を T とした場合、各タイマーは以下のようになる。

update	T
invalid	T×6
holddown	**rip timer** コマンドの設定値 (デフォルト 120 秒)

PP インター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。

6.4 VRRP の設定

6.4.1 インターフェース毎の 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 インターフェース名
  - [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くてはいけない。これらが食い違った場合の動作は予測できない。
auth パラメータを指定しない場合には、認証なしとして動作する。

time1 および *time2* パラメータで、マスターが VRRP 広告を送信する間隔と、バックアップがそれを監視してダウンと判定するまでの時間を設定する。トラフィックが多いネットワークではこれらの値を初期値より長めに設定すると動作が安定することがある。これらの値はすべての VRRP ルーターで一致している必要がある。

[ノート]

priority および *preempt* パラメータの設定は、仮想ルーターの IP アドレスとして自分自身の LAN インター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。

6.4.2 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*
ip *interface* **vrrp shutdown trigger** *vrid* route *network* [*nexthop*]
no ip *interface* **vrrp shutdown trigger** *vrid interface*
no ip *interface* **vrrp shutdown trigger** *vrid* pp *peer_num* [...]
no ip *interface* **vrrp shutdown trigger** *vrid* route *network*

[設定値及び初期値]

- *interface*
  - [設定値] : LAN インターフェース名

  - [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] : -
- *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] :
    - インターフェース名
    - 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 インターフェース形式	指定した LAN インター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。 • **pp keepalive use** 設定によりダウンが検出された場合
route 形式	指定した経路が経路テーブルに存在しないか、*nexthop* で指定したインターフェースもしくは IP アドレスで指定するゲートウェイに向いていない場合に、シャットダウンする。*nexthop* を省略した場合には、経路がどのような先を向いていても存在する限りはシャットダウンしない。

6.5 バックアップの設定

6.5.1 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 インターフェース
  - [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] : トンネルインターフェース番号
  - [初期値] : -

[説明]

PP インターフェースが切断されたときにバックアップするインターフェースを指定する。
バックアップ先のインターフェースが PP インター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 インターフェースごとに設定できる。
PP インター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。

6.5.2 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。

6.5.3 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 インターフェース名
- [初期値] : -

- *peer_num*
  - [設定値] : バックアップとして pp を使用する場合の相手先情報番号
  - [初期値] : -
- *backup_interface*
  - [設定値] : バックアップとして使用する LAN インターフェース
  - [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] : トンネルインターフェース番号
  - [初期値] : -

[説明]

指定する LAN インターフェースに対して、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ー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。

6.5.4 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 インターフェース名
  - [初期値] : -
- *time*
  - [設定値] :
    - 秒数 (1..21474836)
    - off
  - [初期値] : off

[説明]

指定する LAN インターフェースに対して、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。

6.5.5 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 インターフェース名
  - [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 インターフェースに対して、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 インター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。

6.5.6 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 インターフェース名
  - [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 インターフェースに対して、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。

6.5.7 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 インターフェース名
  - [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。

6.5.8 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)
  - [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*
      - 以下が指定可

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 インターフェース名または WAN インターフェース名

  - [初期値] : -
- *option=value 列*
  - [設定値] :

option	***value***	説明
log	on	SYSLOG を出力する
	off	SYSLOG を出力しない
upwait	秒数	到達性があると判断するまでの待機時間 (1..1000000)
downwait	秒数	到達性がないと判断するまでの待機秒数 (1..1000000)
length	バイト	ICMP Echo パケットの長さ (64..1500)

option	*value*	説明
local-address	IP アドレス	始点 IP アドレス
ipsec-refresh	セキュリティー・ゲートウェイの識別子	DOWN→UP または UP→DOWN に状態が変化した場合に、指定のセキュリティー・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	セキュリティー・ゲートウェイの識別子	DOWN→UP に状態が変化した場合のみ、指定のセキュリティー・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	セキュリティー・ゲートウェイの識別子	UP→DOWN に状態が変化した場合のみ、指定のセキュリティー・ゲートウェイに属する SA を強制的に更新 (複数指定する場合はカンマで区切る)
gateway-selection-rule	head	ICMP Echo パケットを送信する際、該当する経路に複数のゲートウェイが指定されていても、必ず最初に指定されたゲートウェイへ送出する
	normal	ICMP Echo パケットを送信する際、該当する経路に複数のゲートウェイが指定されていたら、通常の規則に従い送出ゲートウェイを選択する

- [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。
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。

[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ー・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
```

6.6 受信パケット統計情報の設定

6.6.1 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 インターフェース名、WAN インターフェース名
  - [初期値] : -
- *switch*
  - [設定値] :

設定値	説明
on	指定したインターフェースで受信したパケットの統計情報を記録する
off	指定したインター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]

指定したインター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 つのインター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 設定があるインター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。
受信フィルターで破棄される通信については記録されない。

6.6.2 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 インターフェース名
  - [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、全インターフェースの統計情報をクリアする。

6.6.3 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 インターフェース名
  - [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、全インターフェースの統計情報を表示する。

[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
```

6.6.4 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 インターフェース名
  - [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]

指定したインターフェースにおいて、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。

6.7 パケット転送フィルターの設定

6.7.1 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 インターフェース
pp 番号	PP インターフェース
tunnel 番号	TUNNEL インターフェース

  - [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。
同じインター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。

6.7.2 インター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 インターフェース名、WAN インターフェース名
  - [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]

インターフェースにパケット転送フィルターを適用する。
指定したインター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。

第 7 章

イーサネットフィルターの設定

7.1 フィルター定義の設定

[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] : イーサネットフィルターの番号 (1..100)
  - [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

  - [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ーを設定する。本コマンドで設定されたフィルターは、**ethernet lan filter** コマンドで用いられる。

通常型のフィルターでは、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ーを適用する。

dhcp-bind 型のフィルターでは、以下のイーサネットフレームにフィルターを適用する。対象とならないイーサネットフレームはフィルター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ー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ーに合致するとみなす。

dhcp-not-bind 型のフィルターでは、以下のイーサネットフレームにフィルターを適用する。対象とならないイーサネットフレームはフィルター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 型のフィルターでは始点 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-leased 型のフィルターでは始点 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ーに合致するとみなす。

dhcp-bind、dhcp-not-bind、dhcp-leased、dhcp-not-leased 型のフィルターで対象とする 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、フィルターが適用されるインター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 型のフィルターが 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、フィルター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ので、それらのイーサネットフレームをフィルター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-leased、dhcp-not-leased 型のフィルターでは、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ーの判定をするため、**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-leased 型フィルターは、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-leased 型フィルター

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ことになる。

7.2 インター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 インターフェース名
  - [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 側に出ていくパケットのフィルタリング

  - [初期値] : -
- *list*
  - [設定値] : 空白で区切られたイーサネットフィルター番号の並び (100 個以内)
  - [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ーを組み合わせて、通過するパケットの種類を制限する。

[ノート]

LAN インターフェース名には、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。 LAN 分割機能で使用するインターフェースとして VLAN インターフェースを指定できる。

7.3 イーサネットフィルターの状態の表示

[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-leased	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ーの情報を表示する。

第 8 章

入力遮断フィルターの設定

8.1 フィルター定義の設定

[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*] [*protocol6* [*src_port* [*dst_port6*]]]]
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*] [*protocol6* [*src_port* [*dst_port6*]]]]]]

[設定値及び初期値]

- *id*
  - [設定値] : フィルターの識別子 (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
icmp-error	-	特定の TYPE コードの ICMP パケット

ニーモニック	10 進数	説明
icmp-info	-	特定の TYPE コードの ICMP パケット
icmp-nd	-	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
ipv6	41	IPv6 パケット
gre	47	GRE パケット
esp	50	ESP パケット
ah	51	AH パケット
icmp6	58	ICMP6 パケット

    - 上項目のカンマで区切った並び (5 個以内)
    - 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

ニーモニック	ポート番号
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)
    - 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]

インター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。

Rev.11.03.04 以降で *src_port* または *dst_port* に submission を指定可能。

8.2 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 インターフェース名、WAN インターフェース名
  - [初期値] : -
- *id*
  - [設定値] : **ip/ipv6 inbound filter** コマンドで定義したフィルターの識別子
  - [初期値] : -

[説明]

ip/ipv6 inbound filter コマンドによる設定を組み合わせて、インター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 インターフェースは指定可能。ただし **ipv6 inbound filter** コマンドでは、WAN インターフェースを指定できない。

第 9 章

ポリシーフィルターの設定

9.1 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。

9.2 インター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] : インター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* : インターフェース
  - [設定値] :

設定値	説明
*	すべて
lan*	すべての LAN インターフェース
pp*	すべての PP インターフェース
tunnel*	すべての TUNNEL インターフェース
lanN-lanM	LAN インターフェースの範囲 (例 :lan1-lan2)
ppN-ppM	PP インターフェースの範囲 (例 :pp1-pp30)
tunnelN-tunnelM	TUNNEL インターフェースの範囲 (例 :tunnel1-tunnel30)
lanN	LAN インターフェース
wan1	WAN インターフェース
ppN	PP インターフェース
ppanonymous	anonymous インターフェース
tunnelN	TUNNEL インターフェース
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ーフェースグループの識別子 (1..65535)
  - [初期値] : -

[説明]

インター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、他のインター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]

Rev.11.03.08 以降で *interface* に ppanonymous を指定可能となり、*や pp*を指定した場合は anonymous インターフェースも含まれる。

9.3 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

設定値	説明
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

  - [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。

9.4 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
ユーザー定義サービス	**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。

9.5 ポリシーフィルターの定義

[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] : ポリシーフィルターの識別子 (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* : 始点インターフェース
  - [設定値] :

設定値	説明
*	すべて
lan*	すべての LAN インターフェース
pp*	すべての PP インターフェース
tunnel*	すべての TUNNEL インターフェース
lanN-lanM	LAN インターフェースの範囲 (例 :lan1-lan2)
ppN-ppM	PP インターフェースの範囲 (例 :pp1-pp30)
tunnelN-tunnelM	TUNNEL インターフェースの範囲 (例 :tunnel1-tunnel30)
lanN	LAN インターフェース
wan1	WAN インターフェース
ppN	PP インターフェース
ppanonymous	anonymous インターフェース
tunnelN	TUNNEL インターフェース
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* : 終点インターフェース
  - [設定値] :
    - 書式は始点インターフェースと同じ
  - [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

設定値	説明
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
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
ユーザー定義サービス	**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]

ポリシーフィルターを定義する。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]

Rev.11.03.08 以降で *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 インター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
```

9.6 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 256 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ーから順に評価し、より深い階層のポリシーフィルターを採用する。
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。
ポリシーフィルターの番号の直後に「-」を付け加えることで、そのポリシーフィルターを無効にすることができる。
なお、同じポリシーフィルター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
```

9.7 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。

9.8 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ーで 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 triger winny
- **ip policy filter set switch** 1 3 triger ethernet-filter
- **ip policy filter set switch** 1 4 triger qos-class-control

事象が発生したときに切り替えるタイミングを、*count* と *interval* の組み合わせで指定できる。
interval で指定した時間内に *count* で指定した回数の事象が発生したら、ポリシーセットを切り替える。
count が 1 のときには、最初の事象が発生したときにすぐにポリシーセットを切り替えるので、*interval* の設定は意味を持たない。
事象が発生しなくなってから元のポリシーセットに戻すまでの時間を time で指定できる。
time として infinity を指定したときには、ポリシーセットを元に戻さない。
この場合には、**ip/ipv6 policy filter set enable** コマンドを実行することでポリシーセットを元に戻すことができる。
切り替えが動作しているときに **ip/ipv6 policy filter set** コマンドや **ip/ipv6 policy filter set enable** コマンドの設定を変更したときには、切り替えに関する動作は中断し、切り替え前の状態に戻る。
なお、*original* と *backup* に同じポリシーセットを指定することはできない。
また、*original*、*backup* パラメータで指定したポリシーセットが定義されていないときには、ポリシーセットは切り替わらない。

[設定例]

winny の検知とイーサネットフィルター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
```

9.9 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
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=15
- *timeout*
  - [設定値] : タイムアウト時間 (秒)
  - [初期値] : -

[説明]

ポリシーフィルター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。

第 10 章

URL フィルターの設定

10.1 フィルター定義の設定

[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] : フィルター番号 (1..21474836)
  - [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 によるフィルターを設定する。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。
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。

プロキシ経由の HTTPS コネクションに対するフィルタリングでは、*keyword* により検査する URL(文字列)が、“https://ホスト名:ポート番号“であることに注意する必要がある。

10.2 URL フィルターのインターフェースへの適用

[書式]

url *interface* **filter** *dir list* [**external-database** [**reputation** *reputation_list*] [**category** *category_list*]]
url pp filter *dir list* [**external-database** [**reputation** *reputation_list*] [**category** *category_list*]]
url tunnel filter *dir list* [**external-database** [**reputation** *reputation_list*] [**category** *category_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 インターフェース名、WAN インターフェース名
  - [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 フィルター番号の並び (128 個以内)
  - [初期値] : -
- *reputation_list*
  - [設定値] : 空白で区切られた Web レピュテーションフィルター番号の並び (128 個以内)
  - [初期値] : -
- *category_list*
  - [設定値] : 空白で区切られたカテゴリーリスト番号の並び (128 個以内)
  - [初期値] : -

[説明]

url filter コマンドで設定したフィルターを組み合わせて、インター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ーの数は、各フィルターで 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。

本コマンドにより、適用対象のインターフェースでは以下のように各フィルターが評価される。

- *list* が設定されている場合、内部データベース参照型 URL フィルターで評価し、その結果によってパケットが破棄されるか否かを決定する。 どのフィルターにもマッチしなかった、もしくは *list* が設定されていない場合は、*reputation_list* にて評価される。
- *reputation_list* が設定されている場合、外部データベース参照型 URL フィルターの Web レピュテーション機能で評価し、その結果によってパケットが破棄されるか否かを決定する。 どのフィルターにもマッチしなかった、もしくは *reputation_list* が設定されていない場合は、*category_list* にて評価される。
- *category_list* が設定されている場合、外部データベース参照型 URL フィルターのカテゴリチェック機能で評価し、その結果によってパケットが破棄されるか否かを決定する。 どのフィルターにもマッチしなかった、もしくは *category_list* が設定されていない場合は、パケットが破棄される。

[ノート]

Rev.11.03.04 以降で、Web レピュテーションフィルター番号のリストが指定可能となる。

10.3 URL フィルターでチェックを行う 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 フィルターでチェックを行う HTTP のポート番号を設定する。

10.4 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。

10.5 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 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
- 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] : -
- *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。
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ー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。

10.6 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 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。

10.7 プロキシ経由の HTTPS URL フィルターを使用するか否かの設定

[書式]

url filter https-proxy use *switch*
no url filter https-proxy use

[設定値及び初期値]

- *switch*
  - [設定値] :

設定値	説明
on	プロキシ経由の HTTPS URL フィルターを使用する
off	プロキシ経由の HTTPS URL フィルターを使用しない

  - [初期値] : off

[説明]

プロキシ経由の HTTPS 通信を対象に URL フィルタリングを実施するか否かを設定する。

本コマンドが'on'のとき、SSL トンネリングを処理する HTTPS プロキシを RT 自身で立ち上げ、Web クライアントからの代理接続要求、および以降のデータ中継を処理する。 ここで、**url** *interface* **proxy filter** コマンドによってプロキシ経由の HTTPS アクセスに対するフィルターが適用されていれば、当該インターフェースに対してフィルタリングが実施される。 なお、適用されていなければ無条件で通過する。

また、代理接続先が本機自身となるような要求は破棄する。

本コマンドを有効にするには **url filter use** コマンドが'on'である必要がある。

10.8 プロキシ経由の HTTPS URL フィルターのインターフェースへの適用

[書式]

url *interface* **proxy filter** *dir list*
url pp proxy filter *dir list*
url tunnel proxy filter *dir list*
no url *interface* **proxy filter** *dir*
no url pp proxy filter *dir*
no url tunnel proxy filter *dir*

[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] : -
- *dir*
  - [設定値] :

設定値	説明
in	入力方向の HTTPS コネクションをフィルタリングする
out	出力方向の HTTPS 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 フィルター番号の並び (128 個以内)
  - [初期値] : -

[説明]

url filter コマンドで設定したフィルターを組み合わせて、本機の HTTPS プロキシを経由する HTTPS アクセスに対して適用される。
設定できるフィルターの数は、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ーにマッチしないパケットは破棄される。

10.9 HTTPS プロキシの待ち受けポート番号の設定

[書式]

url filter https-proxy listen *port*
no url filter https-proxy listen

[設定値及び初期値]

- *port*
  - [設定値] : ポート番号(1..65535)
  - [初期値] : 8080

[説明]

HTTPS プロキシの待ち受けポート番号を設定する。

10.10 プロキシ自動設定ファイルの URL の設定

[書式]

url filter https-proxy_curl *url* [dhcp-scope=*scope_num*...]
no url filter https-proxy_curl

[設定値及び初期値]

- *url*
  - [設定値] :

設定値	説明
none	プロキシ自動設定ファイルの URL を通知しない
local	本機が提供する設定ファイルへの URL(http://本機の IP アドレス/wpad.dat)
プロキシ自動設定ファイルが存在する URL	http://で始まる文字列で、半角 255 文字以内

  - [初期値] : local
- *scope_num*
  - [設定値] : DHCP スコープ番号(カンマ「,」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] : -

[説明]

WPAD(Web Proxy Auto-Discovery)により通知するプロキシ自動設定ファイルの URL(CURL: Configuration URL)を設定する。 なお、WPAD で定義される CURL の通知方法のうち、本機では DHCP オプション(252)による通知のみ対応している。

本コマンドの設定に応じて、本機の DHCP サーバーが送信する DHCP パケットに WPAD オプション(252)を自動的に追加し、CURL を通知する。 なお、本コマンドが none の場合、もしくは **url filter https-proxy** コマンドが off の場合は WPAD オプションを追加しない。

dhcp-scope オプションを指定することにより、本コマンドを適用させる DHCP スコープを特定することができる。このオプションを指定しない場合は、すべてのスコープに対して適用される。 なお、適用対象のスコープに **dhcp option** コマンドで WPAD(252)オプションが設定されている場合は、そちらの設定値が優先される。

[ノート]

本機自身を CURL に設定する場合、**httpd service** *on* の設定が必要である。

10.11 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
ysl-mc	ヤマハ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
digitalarts2	デジタルアーツ株式会社のデータベースを使用する
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
ysl-mc	ヤマハ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]

Rev.11.03.04 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。
Rev.11.03.18 以降でヤマハ株式会社のデータベースが選択可能となる。

10.12 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

- [初期値] : -
- *port*
  - [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。

10.13 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
  - [初期値] : -
- *port*
  - [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。

10.14 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 .. 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
    - * ... すべてのカテゴリー番号
  - [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
    - * ... 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ーを設定する。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。
どのカテゴリーにも該当しない 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ー番号は、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。

10.15 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 .. 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ーレベルにマッチする
  - [初期値] : -
- *pharming_status*
  - [設定値] :

設定値	説明
pharmed	ファーミングを検出した場合にマッチする
unpharmed	ファーミ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 フィルターの 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ー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。

[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。

10.16 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。

10.17 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*
  - [設定値] :
    - 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] : -
- *off*
  - [設定値] :
    - 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
- *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。

10.18 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。

10.19 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

[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。

10.20 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*
  - [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。

10.21 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。

10.22 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*
  - [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。

10.23 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]

Rev.11.03.04 以降は *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。

10.24 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。

10.25 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。

10.26 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*
  - [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。

- カテゴリーデータベース×ネットスター株式会社

  カテゴリー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。
- カテゴリーデータベース×ヤマハ株式会社

  カテゴリー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。

[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。

10.27 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。

第 11 章

PPP の設定

11.1 相手の名前とパスワードの設定

[書式]

pp auth username *username password* [myname *myname mypass*] [*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] : 自分側のユーザー名
  - [初期値] : -
- *mypass*
  - [設定値] : 自分側のパスワード
  - [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] : ユーザー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。

双方向で認証を行う場合には、相手のユーザー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。

11.2 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設定する。発信時には常に適用される。anonymous でない着信の場合には発番号により PP が選択されてから適用される。anonymous での着信時には、発番号による PP の選択が失敗した場合に適用される。

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

11.3 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。

11.4 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。

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

[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。ユーザー管理を 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。

11.6 LCP 関連の設定

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

[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。

11.6.2 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

設定値	説明
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。

11.6.3 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*
  - [設定値] : MRU の値 (1280..1792)
  - [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。

11.6.4 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。

11.6.5 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。

11.6.6 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。

11.6.7 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。

11.6.8 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。

11.6.9 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。

11.7 PAP 関連の設定

11.7.1 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。

11.7.2 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。

11.8 CHAP 関連の設定

11.8.1 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。

11.8.2 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。

11.9 IPCP 関連の設定

11.9.1 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。

11.9.2 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。

11.9.3 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。

11.9.4 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。

11.9.5 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。

11.9.6 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。

11.9.7 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。

11.9.8 IPCP の MS 拡張オプションを使うか否かの設定

[書式]

ppp ipcp msext *msext*
no ppp ipcp msext [*msext*]

[設定値及び初期値]

- *msext*
  - [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。

11.9.9 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。

11.10 MSCBCP 関連の設定

11.10.1 mscbcp-restart パラメータの設定

[書式]

ppp mscbcp restart *time*
no ppp mscbcp restart [*time*]

[設定値及び初期値]

- *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。

11.10.2 mscbcp-maxretry パラメータの設定

[書式]

ppp mscbcp maxretry *count*
no ppp mscbcp maxretry [*count*]

[設定値及び初期値]

- *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。

11.11 CCP 関連の設定

11.11.1 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] :
    - stac

[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。

11.11.2 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。

11.11.3 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。

11.11.4 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。

11.11.5 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。

11.12 IPV6CP 関連の設定

11.12.1 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。

11.13 PPPoE 関連の設定

11.13.1 PPPoE で使用する LAN インターフェースの指定

[書式]

pppoe use *interface*
no pppoe use

[設定値及び初期値]

- *interface*
  - [設定値] : LAN インターフェース名、VLAN インターフェース名
  - [初期値] : -

[説明]

選択されている相手に対して、PPPoE で使用する LAN インターフェースまたは VLAN インターフェースを指定する。設定がない場合は、PPPoE は使われない。

11.13.2 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。

11.13.3 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。

11.13.4 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

設定値	説明
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。

11.13.5 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。

11.13.6 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。

11.13.7 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。

11.13.8 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。

11.13.9 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。

11.13.10 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。

11.13.11 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。

11.13.12 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。

11.13.13 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最大 5 つ指定できる。

[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。

第 12 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 **dhcpscope 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、インターフェースの IP アドレスやデフォルト経路情報などを外部の DHCP サーバーから受けることができます。ルーターを DHCP クライアントとして機能させるかどうかは、**ip** *interface* **address**、**ip** *interface* **secondary address**、**ip pp remote address**、**ip pp remote address pool** の各コマンドの設定値により決定されます。設定されている内容は、**show status dhcpc** コマンドにより知ることができます。

(*1)Dynamic Host Configuration Protocol; RFC1541 , RFC2131
URL 参照 : http://rfc.netvolante.jp/rfc/rfc1541.txt (rfc2131.txt)

12.1 DHCP サーバー・リレーエージェント機能

12.1.1 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。

12.1.2 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。

12.1.3 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。

12.1.4 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..2147483647	分
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]

ひとつのネットワークについて複数の DHCP スコープを設定することはできない。複数の DHCP スコープで同一の IP アドレスを含めることはできない。IP アドレス範囲にネットワークアドレス、ブロードキャストアドレスを含む場合、割り当て可能アドレスから除外される。
DHCP リレーエージェントを経由しない DHCP クライアントに対して gateway キーワードによる設定パラメータが省略されている場合にはルーター自身の IP アドレスを通知する。
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.11.03.22 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**

12.1.5 DHCP 予約アドレスの設定

[書式]

dhcp scope bind *scope_num ip_address* [*type*] *id*
dhcp scope bind *scope_num ip_address mac_address*
dhcp scope bind *scope_num ip_address* ipcp
no dhcp scope bind *scope_num ip_address*

[設定値及び初期値]

- *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
type が ethernet の場合	MAC アドレス
type が text の場合	文字列
type が省略された場合	2 桁十六進数の列で先頭は type フィールド

  - [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
  - [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。

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 機能が使用されないよう設定された時点で、コマンドの第 2 書式によるもの以外の予約は消去される。

コマンドの第 1 書式でのクライアント識別子は、クライアントがオプションで送ってくる値を設定する。*type* パラメータを省略した場合には、*type* フィールドの値も含めて入力する。*type* パラメータにキーワードを指定する場合には *type* フィールド値は一意に決定されるので Client-Identifier フィールドの値のみを入力する。

コマンドの第 2 書式による MAC アドレスでの予約は、クライアントの識別に DHCP パケットの chaddr フィールドを用いる。この形の予約機能は、RT の設定が **dhcp server rfc2131 compliant** off あるいは use-clientid 機能を使用しない設定になっているか、もしくは DHCP クライアントが DHCP パケット中に Client-Identifier オプションを付けてこない場合でないと動作しない。

クライアントが Client-Identifier オプションを使う場合、コマンドの第 2 書式での予約は、**dhcp server rfc2131 compliant** on あるいは use-clientid パラメータが指定された場合には無効になるため、新たに Client-Identifier オプションで送られる値で予約し直す必要がある。

Rev.11.03.22 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 scope_num ip_address ethernet 00:a0:de:01:23:45
B. # dhcp scope bind scope_num ip_address text client01
C. # dhcp scope bind scope_num ip_address 01 00 a0 de 01 23 45 01 01 01
D. # dhcp scope bind scope_num ip_address 00:a0:de:01:23:45
```

1. **dhcp server rfc2131 compliant** on あるいは use-clientid 機能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。

12.1.6 DHCP アドレス割り当て動作の設定

[書式]

dhcp scope lease type *scope_num type* [fallback=*fallback_scope_num*]
no dhcp scope lease type *scope_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

[説明]

scope_num で指定した DHCP スコープにおける、アドレスの割り当て方法を制御する。

type に bind-priority を指定した場合には、**dhcp scope bind** コマンドで予約されたクライアントには予約どおりの IP アドレスを、予約されていないクライアントには他のクライアントに予約されていない空きアドレスがスコープ内にある限りそれを割り当てる。

type に bind-priority を指定した場合には、fallback オプションは指定できない。

type に bind-only を指定した場合は、fallback オプションでフォールバックスコープを指定しているかどうかによって動作が変わる。

fallback オプションの指定が無い場合、**dhcp scope bind** コマンドで予約されているクライアントにのみ IP アドレスを割り当て、予約されていないクライアントにはたとえスコープに空きがあっても IP アドレスを割り当てない。

type に bind-only を指定し、同時に fallback オプションでフォールバックスコープを指定している場合には、以下のような動作になる。

1. クライアントが、スコープで IP アドレスを予約されている時には、予約どおりの IP アドレスを割り当てる。
2. クライアントが、スコープでは IP アドレスが予約されていないが、フォールバックスコープでは予約されている時には、フォールバックスコープでの予約どおりの IP アドレスを割り当てる。
3. クライアントが、スコープ、フォールバックスコープのいずれでも IP アドレスを予約されていない時には、フォールバックスコープに対する **dhcp scope lease type** コマンドの設定によって動作が変わる。
   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。

リース期間は DHCP スコープの定義に従う。

12.1.7 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	**show status dhcp summary** コマンドで表示されるインデックス番号、最大 100 個
all	割り当て中の情報全てを対象とする
省略	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** で確認するべきである

12.1.8 DHCP オプションの設定

[書式]

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

[設定値及び初期値]

- *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
    - 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.11.03.22 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**

12.1.9 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
type が text の場合	文字列
type が ethernet の場合	MAC アドレス
type が省略された場合	2 桁十六進数の列で先頭は *type* フィールド

  - [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。

12.1.10 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。

12.1.11 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。

12.1.12 DHCP サーバーの選択方法の設定

[書式]

dhcp relay select *type*
no dhcp relay select [*type*]

[設定値及び初期値]

- *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]

dhcprelay 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。

12.1.13 DHCP BOOTREQUEST パケットの中継基準の設定

[書式]

dhcp relay threshold *time*
no dhcp relay threshold [*time*]

[設定値及び初期値]

- *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。

12.1.14 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り、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]

Rev.11.03.13 以降で使用可能。

12.2 DHCP クライアント機能

12.2.1 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] : -
- *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]

WAN インターフェースを設定した時には、*secondary* は指定できない。

12.2.2 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] : -
- *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。

12.2.3 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] : -
- *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。

12.2.4 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] : -
- 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 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 ID オプションの type フィールドと ID を設定する。

[ノート]

WAN インターフェースを設定した時には、*secondary* は指定できない。

12.2.5 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] : -
- *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。
WAN インターフェースを設定した時には、*secondary* は指定できない。

[設定例]

1. LAN2 プライマリアドレスを DHCP サーバーから得る場合に特定アドレス (192.168.0.128) を要求する。

```
# dhcp client option lan2 primary 50=c0,a8,00,80
# ip lan2 address dhcp
( 注 : ただし、この場合でも要求アドレスがサーバーから与えられるか否かはサーバー次第である。)
```

12.2.6 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	インターフェースのリンクダウンが *time* 秒間継続すると、取得していた情報を解放する
off	インター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ー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**

第 13 章

ICMP の設定

13.1 IPv4 の設定

13.1.1 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。

13.1.2 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ー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。

13.1.3 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。

13.1.4 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。

13.1.5 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。

13.1.6 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。

13.1.7 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]

Rev.11.03.08 以降のファームウェアで rebound オプションを指定することができる。

13.1.8 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。

13.1.9 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]

Rev.11.03.08 以降のファームウェアで rebound オプションを指定することができる。

13.1.10 IPsec で復号したパケットに対して ICMP エラーを送るか否かの設定

[書式]

ip icmp error-decrypted-ipsec send *switch*
no ip icmp error-decrypted-ipsec send [*switch*]

[設定値及び初期値]

- *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、フィルター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。

13.1.11 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 を debug タイプのログに記録するか否かを設定する。

13.1.12 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ー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ー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、指定されたインター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ーフェースからパケットを受信した時に、通常であれば ICMP unreachable や TCP リセットを返送する。しかし、このコマンドを設定しておくとそれを禁止することができ、ポートスキャナーなどによる攻撃を受けた時にルーターの存在を隠すことができる。

[ノート]

指定されたインターフェースからの 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。

13.2 IPv6 の設定

13.2.1 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。

13.2.2 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ー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。

13.2.3 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。

13.2.4 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。

13.2.5 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。

13.2.6 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]

Rev.11.03.08 以降のファームウェアで rebound オプションを指定することができる。

13.2.7 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]

Rev.11.03.08 以降のファームウェアで rebound オプションを指定することができる。

13.2.8 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。

13.2.9 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。

13.2.10 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、フィルター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。

13.2.11 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ー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ー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、指定されたインター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ーフェースからパケットを受信した時に、通常であれば ICMP unreachable や TCP リセットを返送する。しかし、このコマンドを設定しておくとそれを禁止することができ、ポートスキャナーなどによる攻撃を受けた時にルーターの存在を隠すことができる。

[ノート]

指定されたインターフェースからの 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。

第 14 章

トンネリング

14.1 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*
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
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。

14.2 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
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。

14.3 トンネルインター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

設定値	説明
pptp	PPTP トンネル
l2tp	L2TP トンネル
ipudp	IPUDP トンネル

- [初期値] : ipsec

[説明]

トンネルインター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。
IPUDP トンネルは、データコネクト接続以外では使用できない。
データコネクト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。

14.4 トンネルインターフェースの 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]

トンネルインターフェースの 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。

14.5 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 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。

14.6 トンネルインターフェースの端点 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ーフェース端点の IP アドレス
  - [初期値] : -
- *remote*
  - [設定値] : 相手側のトンネルインターフェース端点の IP アドレス
  - [初期値] : -

[説明]

トンネルインターフェース端点の IP アドレスを設定する。IP アドレスは IPv4/IPv6 いずれのアドレスも設定できるが、*local* と *remote* では IPv4/IPv6 の種別が揃っていなくてはいけない。トンネルインター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、適当なインターフェースの 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、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。

14.7 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、ipudp の場合である。
pptp 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。

第 15 章

IPsec の設定

暗号化により IP 通信に対するセキュリティーを保証する 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ー・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ー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ー・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ー・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、トンネルインターフェースという仮想的なインターフェースを定義し、処理すべき IP パケットがトンネルインター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ーフェースはトンネルインター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。
トンネルインター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		トンネルインターフェース番号による設定
• **pp enable** • **pp disable** • **pp select**	<==>	• **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ーを保証するモードです。ルーターからリモートのルーターへ TELNET で入るなどの特殊な場合に利用できます。トランスポートモードを使用するには **ipsec transport** コマンドで定義を行い、使用をやめるには **no ipsec transport** コマンドで定義を削除します。

セキュリティー・ゲートウェイの識別子とトンネルインター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	セキュリティー・ゲートウェイの識別子	トンネルインターフェース番号
FWX120	1-30	1-30

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。

15.1 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。

15.2 IKE バージョンの設定

[書式]

ipsec ike version *gateway_id version*
no ipsec version *gateway_id* [*version*]

[設定値及び初期値]

- *gateway_id*
  - [設定値] : セキュリティー・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]

セキュリティー・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。

15.3 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] : セキュリティー・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

設定値	説明
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。

15.4 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] : セキュリティー・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 (128 バイト以内)
  - [初期値] : -
- *text*
  - [設定値] : ASCII 文字列で表した鍵 (128 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
```

15.5 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] : セキュリティー・ゲートウェイの識別子
  - [初期値] : -
- *cert_id*
  - [設定値] : 証明書ファイルの識別子 (1..8)
  - [初期値] : -
- *crl_id*
  - [設定値] : CRL ファイルの識別子 (1..8)
  - [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。

15.6 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] : セキュリティー・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。

15.7 EAP-MD5 によるユーザー認証の設定

[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] : セキュリティー・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ー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、該当のユーザーグループに含まれるユーザー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にのみ有効であり、始動側のセキュリティー・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 によるユーザー認証を行う。

[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。

15.8 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] : セキュリティー・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ー・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。

15.9 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] : セキュリティー・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ー・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 番のセキュリティー・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 番のセキュリティー・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
```

15.10 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] : セキュリティー・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、同様の状況で相手の提案を拒否する。このコマンドが適用されるパラメータと対応するコマンドは以下の通りである。

パラメータ	対応するコマンド
暗号アルゴリズム	**ipsec ike encryption**
グループ	**ipsec ike group**
ハッシュアルゴリズム	**ipsec ike hash**
PFS	**ipsec ike pfs**
フェーズ 1 のモード	**ipsec ike local name** など

[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。

15.11 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 *gateway_id*

[設定値及び初期値]

- *gateway_id*
  - [設定値] : セキュリティー・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。

15.12 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ー・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ー・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。

15.13 相手側のセキュリティー・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] : セキュリティー・ゲートウェイの識別子
  - [初期値] : -
- *name*
  - [設定値] : 名前 (256 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]

相手側のセキュリティー・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ー・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ー・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ー・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ー・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ー・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]

'tel'および'tel-key'は、データコネクト拠点間接続機能で使用する。

15.14 相手側セキュリティー・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] : セキュリティー・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ー・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ー・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ー・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ー・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ー・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。

15.15 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] : セキュリティー・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。

15.16 自分側のセキュリティー・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] : セキュリティー・ゲートウェイの識別子

  - [初期値] : -
- *name*
  - [設定値] : 名前 (256 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ー・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]

'tel'および'tel-key'は、データコネクト拠点間接続機能で使用する。

15.17 自分側セキュリティー・ゲートウェイの IP アドレスの設定

[書式]

ipsec ike local address *gateway_id ip_address*
ipsec ike local address *gateway_id* vrrp *interface vrid*
ipsec ike local address *gateway_id* ipv6 prefix *prefix* on *interface*
ipsec ike local address *gateway_id* ipcp pp *pp_num*
no ipsec ike local address *gateway_id* [*ip_address*]

[設定値及び初期値]

- *gateway_id*
  - [設定値] : セキュリティー・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ー･ゲートウェイの IP アドレス
  - [初期値] : -
- *interface*
  - [設定値] : LAN インターフェース名
  - [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] : -
- *pp_num*
  - [設定値] : PP インターフェース番号
  - [初期値] : -

[説明]

自分側セキュリティー・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 インターフェース/VRRP グループ ID の仮想 IP アドレスを自分側セキュリティー・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 インターフェースを指定する。

[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ー・ゲートウェイに近いインターフェースの IP アドレスを用いて IKE を起動する。

15.18 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] : セキュリティー・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。

15.19 IKE キープアライブ機能の設定

[書式]

ipsec ike keepalive use *gateway_id switch* [down=disconnect]
ipsec ike keepalive use *gateway_id switch* heartbeat [*interval count* [*upwait*]] [down=disconnect]
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] : セキュリティー・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

設定値	説明
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] : TYPE で icmp-echo を設定したときのデータ部の長さ (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ーフェースを有効にするまでの時間 (0..1000000)
  - [初期値] : 0

[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 インター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 インター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 インター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。

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。

15.20 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] : セキュリティー・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 キープアライブに関する SYSLOG を出力するか否かを設定する。この SYSLOG は DEBUG レベルの出力である。

15.21 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] : セキュリティー・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

[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]

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
```

15.22 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*
  - [設定値] : キュー長 (30 .. 60)
  - [初期値] : 60

[説明]

受信した IKE パケットを蓄積するキューの長さを設定する。 この設定は、短時間に集中して IKE パケットを受信した際のルーターの振る舞いを決定する。設定した値が大きいほど、IKE パケットが集中したときにより多くのパケットを取りこぼさないで処理することができるが、逆に IKE パケットがルーターに滞留する時間が長くなるためキープアライブの応答が遅れ、トンネルの障害を間違って検出する可能性が増える。 通常の運用では、この設定を変更する必要はないが、多数のトンネルを構成しており、多数の SA を同時に消す 状況があるならば値を大きめに設定するとよい。

[ノート]

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。

15.23 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* : セキュリティー・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] :
    - modp1024

[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ー・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。

15.24 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] : セキュリティー・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

[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]

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(Puseudo-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

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

15.25 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。

15.26 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] : セキュリティー・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

[ノート]

type2 パラメータは、Rev.11.03.04 以降で使用可能。

15.27 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]

Rev.11.03.08 以降で使用可能。

15.28 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] : セキュリティー・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。

15.29 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] : セキュリティー・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ー･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ー･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。

15.30 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] : セキュリティー・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。

15.31 XAUTH 認証、EAP-MD5 認証に使用するユーザー 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] : ユーザー識別番号 (1..1000)
  - [初期値] : -
- *username*
  - [設定値] : ユーザー名 (256 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]

IKEv1 の XAUTH 認証、または IKEv2 の EAP-MD5 認証に使用するユーザー ID を設定する。

15.32 XAUTH 認証、EAP-MD5 認証に使用するユーザー 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] : ユーザー識別番号 (1..1000)
  - [初期値] : -

- *attribute=value*
  - [設定値] : ユーザー属性
  - [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ー ID の属性を設定する。
設定できる属性は以下のとおり。

attribute	***value***	説明
xauth	on	IPsec の XAUTH 認証にこの ID を使用する
	off	IPsec の XAUTH 認証にこの ID を使用しない
xauth-address	IP address[/netmask](IPv6 アドレス可)	IPsec の接続時に、このアドレスを内部 IP アドレスとして通知する
xauth-dns	IP address(IPv6 アドレス可)	IPsec の接続時に、このアドレスを DNS サーバーアドレスとして通知する
xauth-wins	IP address(IPv6 アドレス可)	IPsec の接続時に、このアドレスを WINS サーバーアドレスとして通知する
xauth-filter	フィルターセットの名前を表す文字列	IPsec の接続時に、このフィルターを適用する
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、該当のユーザー ID が属しているユーザーグループに対して、**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。

15.33 XAUTH 認証、EAP-MD5 認証に使用するユーザーグループの設定

[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] : ユーザーグループ識別番号 (1..1000)
  - [初期値] : -
- *userid*
  - [設定値] : ユーザー識別番号もしくはユーザー識別番号の範囲 (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ー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
```

15.34 XAUTH 認証、EAP-MD5 認証に使用するユーザー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] : ユーザーグループ識別番号 (1..1000)
  - [初期値] : -
- *attribute=value*
  - [設定値] : ユーザーグループ属性
  - [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ー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ー 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ー 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	フィルターセットの名前を表す文字列	IPsec の接続時に、このフィルターを適用する
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、該当のユーザーグループに含まれるすべてのユーザーに対して有効となる。

15.35 XAUTH によるユーザー認証の設定

[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] : セキュリティー・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ー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 によるユーザー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、該当のユーザーグループに含まれるユーザーを認証の対象とする。
group_id の指定がない場合や、指定したユーザーグループに含まれるユーザー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にのみ有効であり、始動側のセキュリティー・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 によるユーザー認証を行う。

15.36 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。

15.37 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] : セキュリティー・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 を利用するときに、
option を指定していると XAUTH では接続できない。

15.38 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] : セキュリティー・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、認証ユーザー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。

15.39 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] : セキュリティー・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、セキュリティー・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。

15.40 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] : セキュリティー・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]

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。

15.41 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

設定値	説明
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。
Rev.11.03.13 以降で使用可能。

15.42 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。
Rev.11.03.13 以降で使用可能。

15.43 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 の従来の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。
Rev.11.03.22 以降で使用可能。

15.44 SA 関連の設定

再起動されるとすべての SA がクリアされることに注意しなくてはいけない。

15.44.1 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] : セキュリティー・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 (*sa* パラメータで isakmp-sa (ike-sa) 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、各セキュリティー・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ー・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。

15.44.2 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] : セキュリティー・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
- *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 つのセキュリティー・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、トンネルインターフェースでの優先/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
- 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。

[設定例]

```
# ipsec sa policy 101 1 esp aes-cbc sha-hmac
```

15.44.3 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。

15.44.4 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] : セキュリティー・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いけない。

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。

15.44.5 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] : セキュリティー・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 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。
IKEv1 メインモードでの NAT トラバーサルは、Rev.11.03.25 以降のファームウェアで利用できる。
type オプションは、Rev.11.03.25 以降のファームウェアで使用できる。

15.44.6 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。

15.45 トンネルインターフェース関連の設定

15.45.1 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、トンネルインター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。

15.45.2 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。
トンネルインターフェース毎のコマンドである。

[ノート]

トンネルインターフェースの MTU と実インターフェースの MTU の値の大小関係により、IPsec 化されたパケットをフラグメントしなくてはいけない時には、このコマンドの設定に関わらず DF ビットは 0 になる。

15.45.3 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ーフェースで使用する SA のポリシーを設定する。

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

15.45.5 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 インターフェース名
  - [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] : トンネルインターフェース番号
  - [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 インター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]

トンネルインター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ー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。

15.45.6 トンネルテンプレートの設定

[書式]

tunnel template *tunnel* [*tunnel ...*]

no tunnel template

[設定値及び初期値]

- *tunnel*
  - [設定値] : トンネルインターフェース番号、または間にハイフン (-) をはさんでトンネルインター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ーフェースを展開元として、当該インター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ーフェースを設定する。

展開元のトンネルインターフェースに設定することで、展開先のトンネルインター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(*)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ー・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ー・ゲートウェイの識別子を指定する場合)
- **tunnel encapsulation**
- **tunnel ngn arrive permit**
- **tunnel ngn bandwidth**
- **tunnel ngn disconnect time**
- **tunnel ngn radius auth**
- **l2tp** で始まるコマンド(*)
- **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ー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ー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	セキュリティー・ゲートウェイの識別子
ipsec auto refresh	セキュリティー・ゲートウェイの識別子
tunnel enable	トンネルインターフェース番号

ipsec sa policy コマンドでは、セキュリティー・ゲートウェイの識別子が展開先のトンネルインター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ー・ゲートウェイの名前の末尾に展開先のトンネルインターフェース番号が付加される。

展開元のトンネルインター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ー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ー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]

トンネルインターフェースが選択されている時にのみ使用できる。

展開対象となるコマンドのうち、末尾に(*)が付加されているコマンドについては、Rev.11.03.08 以降で使用可能。

[設定例]

展開先のトンネルインターフェースとして、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
```

15.46 トランスポートモード関連の設定

15.46.1 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
```

15.46.2 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 *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 は展開元のトランスポート 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]

Rev.11.03.08 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 *
```

15.47 PKI 関連の設定

15.47.1 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] : 証明書ファイルの識別子 (1..8)
  - [初期値] : -
- *file*
  - [設定値] : 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。)
  - [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。

15.47.2 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] : CRL ファイルの識別子 (1..8)
  - [初期値] : -
- *file*
  - [設定値] : 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)
  - [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。

第 16 章

L2TP/IPsec 機能の設定

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。

16.1 L2TP/IPsec を動作させるか否かの設定

[書式]

l2tp service *service*
no l2tp service [*service*]

[設定値及び初期値]

- *service*
  - [設定値] :

設定値	説明
on	L2TP/IPsec が動作する
off	L2TP/IPsec が動作しない

  - [初期値] : off

[説明]

L2TP/IPsec を動作させるか否かを設定する。
L2TP/IPsec 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/IPsec 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。

16.2 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 "FWX120" がパスワードとして使用される。
大文字小文字の区別に注意してください。

16.3 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。
トンネルインターフェースにのみ設定可能です。

16.4 L2TP キープアライブの設定

[書式]

l2tp keepalive use *switch* [*intarval* [*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。
トンネルインターフェースにのみ設定可能です。

16.5 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。
トンネルインターフェースにのみ設定可能です。

16.6 L2TP のコネクション制御の 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 のコネクション制御に関するログを SYSLOG に出力する
off	L2TP のコネクション制御に関するログを SYSLOG に出力しない

  - [初期値] : off

[説明]

L2TP のコネクション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。
トンネルインターフェースにのみ設定可能です。

第 17 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。

17.1 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。

17.1.1 PPTP サーバーを動作させるか否かの設定

[書式]

pptp service *service*
no pptp service [*service*]

[設定値及び初期値]

- *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。

17.1.2 相手先情報番号にバインドされるトンネルインターフェースの設定

[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
tunnelN-tunnelM	TUNNEL インターフェースの範囲

  - [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ーフェースを指定する。
第 2 書式は anonymous インターフェースを使って多数の接続先を登録するために複数連続したトンネルインターフェースをバインドする場合に用いる。
anonymous インターフェースに対しては第 1 書式・第 2 書式ともに指定可能であり、同時に続けて併記することも可能だが、anonymous インターフェース以外が選択されている場合は、複数のトンネルインターフェースを指定するとエラーとなる。

[ノート]

PPTP は PP 毎に設定する。
tunnel encapsulation コマンドで pptp を設定したトンネルインターフェースをバインドすることによって PPTP で通信することを可能にする。

17.1.3 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。

17.1.4 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(Rev.11.03.27 以降)
    - 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ー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。

17.1.5 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。

Rev.11.03.27 以降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。

17.1.6 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。

17.1.7 PPTP 暗号鍵生成のための要求する認証方式の設定

[書式]

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

[設定値及び初期値]

- *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。

17.1.8 PPTP 暗号鍵生成のための受け入れ可能な認証方式の設定

[書式]

pp auth accept *auth* [*auth*]
no pp auth accept [*auth auth*]

[設定値及び初期値]

- *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。

17.1.9 PPTP のコネクション制御の syslog を出力するか否かの設定

[書式]

pptp syslog *syslog*
no pptp syslog [*syslog*]

[設定値及び初期値]

- *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。

17.2 リモートアクセス VPN 機能

17.2.1 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。

17.2.2 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。

17.2.3 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。

17.2.4 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。

17.2.5 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。

第 18 章

SIP 機能の設定

18.1 共通の設定

18.1.1 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。

18.1.2 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。

18.1.3 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。

18.1.4 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
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。

18.1.5 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。

18.1.6 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。

18.1.7 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。

18.1.8 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 ともに使用でき、発信側またはサーバーで 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ーで 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、サーバー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。

18.1.9 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	ユーザー名を検証する
off	ユーザー名を検証しない

  - [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。

18.1.10 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。

18.1.11 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。

18.1.12 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。

18.2 NGN 機能の設定

データコネクトを利用して拠点間接続を行うにはトンネルインター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。

18.2.1 NGN 網に接続するインターフェースの設定

[書式]

ngn type *interface type*
no ngn type *interface* [*type*]

[設定値及び初期値]

- *interface*
  - [設定値] : LAN インターフェース
  - [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ーフェースを設定する。

18.2.2 NGN 網を介したトンネルインター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ー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。

18.2.3 NGN 網を介したトンネルインター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ー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。

bandwidth は、Rev.11.03.22 以降のファームウェアで任意の数値を設定可能。

18.2.4 NGN 網を介したトンネルインター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

設定値	説明
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。

18.2.5 NGN 網を介したトンネルインター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。

18.2.6 NGN 網を介したトンネルインターフェースで使用する LAN インターフェースの設定

[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 インターフェース名	LAN ポート

  - [初期値] : auto

[説明]

NGN 網を介したトンネルインターフェースで使用する LAN インターフェースを設定する。

auto に設定した時はトンネルインターフェースで設定した電話番号を利用して、使用する LAN インター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。

18.2.7 NGN 網を介したトンネルインター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ー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。

18.2.8 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]

データコネクト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]

トンネルインターフェースが選択されている時にのみ使用できる。
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**

18.2.9 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。

18.2.10 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**

18.2.11 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**

18.2.12 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]

Rev.11.03.22 以降で使用可能。

18.2.13 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。

第 19 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るようになります。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、セキュリティー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ーモデルを利用することで、より高度なセキュリティーを確保しています。

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ー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。

19.1 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
ip_address	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)
lanN	LAN インターフェース名
bridgeN	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、Rev.11.03.13 以降のファームウェアである。

19.2 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。

19.3 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。

19.4 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。

19.5 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。

19.6 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
ip_address	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)
lanN	LAN インターフェース名
bridgeN	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]

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、Rev.11.03.13 以降のファームウェアである。

19.7 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。

19.8 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。

19.9 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。

19.10 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。

19.11 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

19.12 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。

19.13 SNMPv3 USM で管理するユーザーの設定

[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] : ユーザー番号 (1..65535)
  - [初期値] : -
- *name*
  - [設定値] : ユーザー名 (32 文字以内)
  - [初期値] : -
- *group_id*
  - [設定値] : ユーザーグループ番号 (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ー情報を設定する。
ユーザー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、そのユーザーはすべての 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ー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ー設定と一致させておく必要がある。

19.14 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
ip_address	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)
lanN	LAN インターフェース名
bridgeN	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* : ユーザー番号
  - [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ー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、Rev.11.03.13 以降のファームウェアである。

19.15 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 オブジェクトの集合である。
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。

[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
```

19.16 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
view_id	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
view_id	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]

ユーザー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 オブジェクトへのアクセスは禁止される。

19.17 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] : ユーザー番号
  - [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ー設定は **snmpv3 usm user** コマンドで設定したユーザー設定が用いられる。

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。

19.18 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] : インター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。

19.19 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"
```

19.20 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"
```

19.21 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。

19.22 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	全設定初期化時
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ーフェース毎に制御できる。あるインターフェースについて、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。

19.23 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] : -
- *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]

指定したインターフェースの linkDown トラップを送信するか否かを設定する。

19.24 PP インターフェースの情報を 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 インターフェースを 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。

19.25 トンネルインターフェースの情報を 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、トンネルインターフェースを 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。

19.26 スイッチのインターフェースの情報を 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、スイッチのインターフェースを MIB2 の範囲で表示するかどうかを決定する。

19.27 PP インター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 インター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 インター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 インターフェースのアドレスとして使われる。この場合、SNMP では通常のインターフェースの IP アドレスを調べる手順で IPCP としてどのようなアドレスが得られたのか調べることができる。
しかし、NAT の外側アドレスとして 'ipcp' と指定している場合には、IPCP で得られた IP アドレスは NAT の外側アドレスとして使用され、インターフェースには付与されない。そのため、SNMP でインターフェースの IP アドレスを調べても、IPCP でどのようなアドレスが得られたのかを知ることができない。
本コマンドを on に設定しておくと、IPCP で得られた IP アドレスが NAT の外側アドレスとして使用される場合でも、SNMP ではそのアドレスをインター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ー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。

19.28 LAN インター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* : インターフェース (現状では 'lan1' のみ設定可能)
  - [設定値] :
    - lan1
  - [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。

19.29 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、ルーター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。

19.30 スイッチへ静的に付与するインター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]

スイッチのインター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、スイッチのインター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。

19.31 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。

19.32 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
poesuppply	給電開始
poeterminate	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 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 Rev.11.03.08 以降で設定可能。

19.33 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。

第 20 章

RADIUS の設定

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。

20.1 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ーネーム (PAP であれば UserID、CHAP であれば NAME) が、自分で持つユーザーネーム (**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。

20.2 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。

20.3 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。

20.4 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。

20.5 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。

20.6 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。

20.7 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。

20.8 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。

20.9 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。

第 21 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ーフェースに対して適用されます。インター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、インターフェースから本機を経由して他のインター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。

21.1 インターフェースへの 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 インターフェース名、WAN インターフェース名
  - [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]

適用されたインター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 インターフェースの場合、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。

21.2 NAT ディスクリプタの動作タイプの設定

[書式]

nat descriptor type *nat_descriptor type*
no nat descriptor type *nat_descriptor* [*type*]

[設定値及び初期値]

- *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

[説明]

NAT 変換の動作タイプを指定する。

[ノート]

nat-masquerade は、動的 NAT 変換できなかったパケットを IP マスカレード変換で救う。例えば、外側アドレスが 16 個利用可能の場合は先勝ちで 15 個 NAT 変換され、残りは IP マスカレード変換される。

21.3 NAT 処理の外側 IP アドレスの設定

[書式]

nat descriptor address outer *nat_descriptor outer_ipaddress_list*
no nat descriptor address outer *nat_descriptor* [*outer_ipaddress_list*]

[設定値及び初期値]

- *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

  - [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。
適用されるインターフェースにより使用できるパラメータが異なる。

適用インターフェース	LAN	PP	トンネル
ipcp	×	○	×
primary	○	×	×
secondary	○	×	×
IP アドレス	○	○	○

21.4 NAT 処理の内側 IP アドレスの設定

[書式]

nat descriptor address inner *nat_descriptor inner_ipaddress_list*
no nat descriptor address inner *nat_descriptor* [*inner_ipaddress_list*]

[設定値及び初期値]

- *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。

21.5 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。

21.6 IP マスカレード使用時に rlogin,rcp と ssh を使用するか否かの設定

[書式]

nat descriptor masquerade rlogin *nat_descriptor use*
no nat descriptor masquerade rlogin *nat_descriptor* [*use*]

[設定値及び初期値]

- *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。

21.7 静的 IP マスカレードエントリの設定

[書式]

nat descriptor masquerade static *nat_descriptor id inner_ip protocol* [*outer_port*=]*inner_port*
no nat descriptor masquerade static *nat_descriptor id* [*inner_ip protocol* [*outer_port*=]*inner_port*]

[設定値及び初期値]

- *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

設定値	説明
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ー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。

21.8 NAT の IP アドレスマップの消去タイマの設定

[書式]

nat descriptor timer *nat_descriptor time*
nat descriptor timer *nat_descriptor* protocol=*protocol* [port=*port_range*] *time*
nat descriptor timer *nat_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。

21.9 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。

21.10 IP マスカレードで利用するポートの範囲の設定

[書式]

nat descriptor masquerade port range *nat_descriptor port_range1* [*port_range2* [*port_range3*]]
no nat descriptor masquerade port range *nat_descriptor* [*port_range1* [*port_range2* [*port_range3*]]]

[設定値及び初期値]

- *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*
  - [設定値] : 間に - をはさんだポート番号の範囲
  - [初期値] : port_range1=60000-64095、port_range2=49152-59999、port_range3=32096-49151

[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。

21.11 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。

21.12 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。

21.13 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します。

21.14 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

[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。

21.15 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いけない。しかし、IP マスカレード処理では IP アドレスなどを書き換えてしまうため、ICMP エラーを正しく発信元に返せない場合がある。そうなると、パケットを永遠に届けることができなくなってしまう。このように、経路 MTU 探索のための ICMP エラーが正しく届かない状況を、経路 MTU ブラックホールと呼ぶ。

IP マスカレード変換時に同時に DF ビットを削除してしまうと、この経路 MTU ブラックホールを避けることができる。その代わりに、経路 MTU 探索が行われないことになるので、通信効率が下がる可能性がある。

[ノート]

ファストパス処理は、一度ノーマルパス処理で通過させたパケットの情報を保存しておき、同じ種類のパケットであれば高速に転送するという処理を行っている。そのため、例えば **ping** コマンドを実行した場合、最初の 1 回目はノーマルパス処理、2 回目以降はファストパス処理となる。そのため、最初の 1 回は DF ビットが削除されるが、2 回目以降は DF ビットが削除されないという状況だった。

21.16 IP マスカレードで変換するセッション数の設定

[書式]

nat descriptor masquerade session limit *nat_descriptor id limit*
no nat descriptor masquerade session limit *nat_descriptor id*

[設定値及び初期値]

- *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..32000)
  - [初期値] : 32000

[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。

第 22 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。

22.1 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。

22.2 DNS サーバーの IP アドレスの設定

[書式]

dns server *ip_address* [*ip_address...*]
no dns server [*ip_address...*]

[設定値及び初期値]

- *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] : -

[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。

22.3 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。

22.4 DNS サーバーを通知してもらう相手先情報番号の設定

[書式]

dns server pp *peer_num*
no dns server pp [*peer_num*]

[設定値及び初期値]

- *peer_num*
  - [設定値] : DNS サーバーを通知してもらう相手先情報番号
  - [初期値] : -

[説明]

DNS サーバーを通知してもらう相手先情報番号を設定する。このコマンドで相手先情報番号が設定されていると、DNS での名前解決を行う場合に、まずこの相手先に発信して、そこで PPP の 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ったり、接続できても DNS サーバーの通知がなかった場合には名前解決は行われない。
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。

[ノート]

この機能を使用する場合には、**dns server pp** コマンドで指定された相手先情報に、**ppp ipcp msext** on の設定が必要である。

[設定例]

```
# pp select 2
pp2# ppp ipcp msext on
pp2# dns server pp 2
```

22.5 DNS サーバーアドレスを取得するインターフェースの設定

[書式]

dns server dhcp *interface*
no dns server dhcp

[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] : -

[説明]

DNS サーバーアドレスを取得するインターフェースを設定する。このコマンドでインター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、指定したインターフェースで 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。

[ノート]

この機能は指定したインターフェースが DHCP クライアントとして動作していなければならない。
ブリッジインターフェースを指定できるのは Rev.10.00.38 以降のリビジョンである。
WAN インターフェースを指定できるのは Rev.10.01.32 以降の RTX1200、Rev.10.00.60 以降の SRT100、RTX810 である。

22.6 DHCP/IPCP MS 拡張で DNS サーバーを通知する順序の設定

[書式]

dns notice order *protocol server* [*server*]
no dns notice order *protocol* [*server* [*server*]]

[設定値及び初期値]

- *protocol*
  - [設定値] :

設定値	説明
dhcp	DHCP による通知
msext	IPCP MS 拡張による通知

  - [初期値] : dhcp および msext
- *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

  - [初期値] : me server

[説明]

DHCP や IPCPMS 拡張では DNS サーバーを複数通知できるが、それをどのような順序で通知するかを設定する。
none を設定すれば、他の設定に関わらず DNS サーバーの通知を行わなくなる。me は本機自身の DNS リカーシブサーバー機能を使うことを通知する。*server* では、**dns server** コマンドに設定したサーバー群を通知することになる。
IPCP MS 拡張では通知できるサーバーの数が最大 2 に限定されているので、後ろに me が続く場合は先頭の 1 つだけと本機自身を、*server* 単独で設定されている場合には先頭の 2 つだけを通知する。

22.7 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

設定値	説明
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。

22.8 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。

22.9 DNS 問い合わせの内容に応じた DNS サーバーの選択

[書式]

dns server select *id server* [*server2*] [*type*] *query* [*original-sender*] [restrict pp *connection-pp*]
dns server select *id* pp *peer_num* [*default-server*] [*type*] *query* [*original-sender*] [restrict pp *connection-pp*]
dns server select *id* dhcp *interface* [*default-server*] [*type*] *query* [*original-sender*] [restrict pp *connection-pp*]
dns server select *id* reject [*type*] *query* [*original-sender*]
no dns server select *id*

[設定値及び初期値]

- *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

設定値	説明
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
type が a、aaaa、mx、ns、cname の場合	*query* はドメイン名を表す文字列であり、後方一致とする。例えば、"yamaha.co.jp" であれば、rtpro.yamaha.co.jp などにマッチする。"." を指定するとすべてのドメイン名にマッチする。
type が ptr の場合	*query* は IP アドレス (*ip_address*[/*masklen*]) であり、*masklen* を省略したときは IP アドレスにのみマッチし、*masklen* を指定したときはネットワークアドレスに含まれるすべての IP アドレスにマッチする。DNS 問い合わせに含まれる.in-addr.arpa ドメインで記述された FQDN は、IP アドレスへ変換された後に比較される。すべての IP アドレスにマッチする設定はできない。
reject キーワードを指定した場合	*query* は完全一致とし、前方一致、及び後方一致には "*" を用いる。つまり、前方一致では、"NetVolante.*" であれば、NetVolante.jp、NetVolante.rtpro.yamaha.co.jp などにマッチする。また、後方一致では、"*yamaha.co.jp" と記述する。

  - [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
  - [初期値] : -
- *default-server*
  - [設定値] : *peer_num* パラメータで指定した接続相手から DNS サーバーを獲得できなかったときに使う DNS サーバーの IP アドレス
  - [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がサーバーの選択条件に追加される。相手先がアップしていないとサーバーは選択されない。相手先がアップしていて、かつ、他の条件もマッチしている場合に指定したサーバーが選択される。

22.10 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

***type* パラメータ**	***name***	***value***
a	FQDN	IPv4 アドレス
aaaa	FQDN	IPv6 アドレス
ptr	IPv4 アドレス	FQDN
mx	FQDN	FQDN
ns	FQDN	FQDN
cname	FQDN	FQDN

  - [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
```

22.11 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] :
    - 10000-10999

[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ーで扱うとき、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。

22.12 DNS サーバーへアクセスできるホストの IP アドレス設定

[書式]

dns host *ip_range* [*ip_range* [...]]
no dns host

[設定値及び初期値]

- *ip_range* : DNS サーバーへアクセスを許可するホストの IP アドレス範囲のリストまたはニーモニック
  - [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ハイフン (-) をはさんだ IP アドレス (範囲指定)、およびこれらを任意に並べたもの
any	すべてのホストからのアクセスを許可する
lan	すべての LAN ポート側ネットワーク内ならば許可する
lanN	ひとつの任意の LAN ポート側ネットワーク内ならば許可する (N はインターフェース番号)
none	すべてのホストからのアクセスを禁止する

  - [初期値] : any

[説明]

DNS サーバー機能へのアクセスを許可するホストを設定する。

[ノート]

このコマンドで LAN インタ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 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。

22.13 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。

22.14 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。

22.15 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

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。

第 23 章

優先制御／帯域制御

優先制御と帯域制御の機能は、インター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ー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。FWX120 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
FWX120	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。
これはインターフェースごとに選択することができます。

23.1 インターフェース速度の設定

[書式]

speed *interface speed*
no speed *interface* [*speed*]

[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] : -
- *speed*
  - [設定値] : インターフェース速度 (bit/s)
  - [初期値] : -

[説明]

指定したインターフェースに対して、インターフェースの速度を設定する。

[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。

23.2 クラス分けのためのフィルター設定

[書式]

queue class filter *num class1* [cos=*cos*] ip *src_addr* [*dest_addr* [*protocol* [*src_port* [*dest_port*]]]]
queue class filter *num class1* [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_dssr* [*dest_addr* [*protocol* [*src_port* [*dest_port*]]]]
queue class filter *num* **precedence** [mapping=*prec*:*class* [,*prec*:*class*...]] [**cos**=*cos*] ipv6 *src_dssr* [*dest_addr* [*protocol* [*src_port* [*dest_port*]]]]
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(1..100)
  - [初期値] : -
- *class1*
  - [設定値] : クラス(1..16)

- [初期値] : -
- *src_addr* : IP 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
    - IPv6 アドレス
    - * (すべての IP アドレスまたは IPv6 アドレスに対応)
    - 間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。
  - [初期値] : -
- *dest_addr* : IP パケットの終点 IP 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
ident	113
ntp	123
nntp	119
snmp	161
syslog	514
printer	515

ニーモニック	ポート番号
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] : -

[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

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。

パケットフィルター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ー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。

Rev.11.03.04 以降で *src_port* または *dest_port* に submission を指定可能。

[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
```

23.3 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 インターフェース名、WAN インターフェース名
  - [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
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]

指定したインターフェースに対して、キューイングアルゴリズムタイプを選択する。

fifo は最も基本的なキューである。fifo の場合、パケットは必ず先にルーターに到着したものから送信される。パケットの順番が入れ替わることは無い。fifo キューにたまったパケットの数が **queue** *interface* **length** コマンドで指定した値を越えた場合、キューの最後尾、つまり最後に到着したパケットが破棄される。

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。

shaping は LAN インターフェースに対する帯域制御を行う。LAN インター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、帯域速度の計算をプリアンブル、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]

shaping-level オプションは Rev.11.03.13 以降のファームウェアで指定可能。

23.4 クラス分けフィルターの適用

[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 インターフェース名、WAN インターフェース名
  - [初期値] : -
- *filter_list*
  - [設定値] : 空白で区切られたクラスフィルターの並び
  - [初期値] : -

[説明]

指定した LAN インターフェース、WAN インター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ーを適用する順番を設定する。フィルター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。

23.5 クラス毎のキュー長の設定

[書式]

queue *interface* **length** *len1* [*len2...lenN*]

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 インターフェース名、WAN インターフェース名
  - [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)
  - [初期値] : 200
- *len1..len16.*
  - [設定値] : クラス 1 からクラス 16 のキュー長 (1..10000)
  - [初期値] : 20

[説明]

インターフェースに対して、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。

23.6 デフォルトクラスの設定

[書式]

queue *interface* **default class** *class*
queue pp default class *class*
no queue *interface* **default class** [*class*]
no queue pp default class [*class*]

[設定値及び初期値]

- *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] : -
- *class*
  - [設定値] : クラス (1..16)
  - [初期値] : 2

[説明]

インターフェースに対して、フィルター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。

23.7 クラスの属性の設定

[書式]

queue *interface* **class property** *class* bandwidth=*bandwidth*
no queue *interface* **class property** *class* [...]

[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] : -
- *class*
  - [設定値] : クラス (1..16)
  - [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] : -

[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。 '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、トンネルインター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 インターフェースを設定する必要がある。 *bandtidth* パラメータに 'ngn' を指定可能なのは Rev.11.03.04 以降。

queue *interface* **type** コマンドで shaping が指定されている場合は、Dynamic Traffic Control による帯域制御を行うことが可能である。Dynamic Traffic Control を行うためには、 bandwidth パラメータに「,」(コンマ) でつないだ 2 つの速度を指定することで、保証帯域と上限帯域を設定する。記述順に関係なく、常に値の小さな方が保証帯域となる。なお、保証帯域の合計が回線全体の帯域を越えてはいけない。

このコマンドが設定されていないクラスには、常に 100% の帯域が割り振られている。そのため、帯域制御の設定をする場合には最低限でも対象としているクラスと、デフォルトクラスの 2 つに関してこのコマンドを設定しなくてはいけない。デフォルトクラスの設定を忘れると、デフォルトクラスに 100% の帯域が割り振られるため、対象とするクラスは常にデフォルトクラスより狭い帯域を割り当てられることになる。

23.8 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 インターフェース名、WAN インターフェース名
  - [初期値] : -
- *class*
  - [設定値] : DCC を有効にするクラス (1..16)
  - [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

option	*value*	説明
	adaptive	動作モードを適応制御モードにする
trigger	winny	Winny 検知をトリガとして制御を開始する
	share	Share 検知をトリガとして制御を開始する
	masquerade-session	IP マスカレード変換セッション数制限をトリガとして制御を開始する
notice	on	制御されていることを通知する
	off	制御されていることを通知しない

- [初期値] :
  - watch=source
  - threshold=70%,30
  - time=600
  - mode=forced
  - notice=on

[説明]

指定したインターフェースについて、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。監視対象のインター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、インターフェース帯域に対する占有率を監視する。監視時は 10 秒毎に占有率を求め、その占有率が指定秒数を超えたときに閾値超過と判定される。
例えば、threshold=70%,30 と設定した場合、帯域使用率 70% 以上である 10 秒間が連続して 3 回続いたときに閾値超過と判定される。

同一のホストから (watch=source)、あるいは、同一のホスト宛て (watch=destination) の過剰送信を検知した場合、そのトラフィックは *forwarding* パラメータに指定されたクラスへ転送され、転送先のクラス設定に従ってパケットの送出が行われる。なお、*forwarding* パラメータに reject を指定した場合、当該トラフィックは遮断される。また、*forwarding* パラメータは省略することも可能で、この場合転送制御は行われないが、threshold を超過しているホストを **show status qos** コマンドから確認することができる。

time パラメータは転送制御が行われる時間を示し、infinity を指定した場合は、無期限に対象のトラフィックの遮断、または、使用クラスの変更がなされる。

mode パラメータは動作モードを指定する。forced を指定した場合は、threshold パラメータで指定した占有時間が経過したら直ちに当該フローの制御を実行する。また、time パラメータで指定した制御時間が経過したら直ちに当該フローの制御を解除する。adaptive を指定した場合は、threshold パラメータで指定した占有時間が経過しても当該クラスの使用帯域が保証帯域の 90% 未満である間は制御を保留する。また、time パラメータで指定した制御時間が経過しても当該クラスの使用帯域が保証帯域の 90% 以上である間は制御解除を保留する。
制御が保留されているホストは **show status qos** コマンドで表示されず、制御が保留されている間に threshold の占有率を割ったらその時点で制御は解除される。

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。

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。

[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。

第 24 章

連携機能

24.1 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。

24.2 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。

24.3 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 インターフェースまたは WAN インター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 インターフェースまたは WAN インターフェース
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 インターフェースの **speed lan** コマンドの設定値、または WAN インターフェースの **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 インターフェースが設定されている場合には、その LAN インターフェースの **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 インター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、インターフェースに付与された IP アドレスを使用する

24.4 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にのみ可能
control	クライアント動作として、サーバーから通知を受けた時の制御動作定義番号 (1-65535)、相手側動作をサーバーに設定する時にのみ可能
port	相手側が使用する UDP のポート番号 (1-65535)
syslog	動作をログに残すか否か、'on'or'off'

設定値	説明
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、インター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、制御対象のインターフェースの速度はその時点の設定が保持される。

24.5 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
      - インターフェースでの単位時間当たりの受信量を監視する。値は 1 秒あたりのビット数で指定する

interface	インターフェース名 (LAN,TUNNEL)

    - *interface* overflow

- LAN インター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

interface	LAN インターフェース名

- *interface* [*class*] transmit
  - インターフェースでの単位時間当たりの送信量を監視する。値は 1 秒あたりのビット数で指定する

interface	インターフェース名 (LAN,TUNNEL)
class	クラス番号 (LAN インターフェースの場合)

  - [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。

24.6 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 インターフェース
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。

24.7 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。 インター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。

第 25 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。

25.1 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いけない。

25.2 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]

以下の機能はまだサポートされていない。

- NSSA (RFC1587)
- OSPF over demand circuit (RFC1793)
- OSPF MIB

25.3 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。

25.4 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、以下のインター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 インターフェース
- LOOPBACK インターフェース
- PP インターフェース

なお、プライマリ IPv4 アドレスが付与されたインター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。
Rev.11.03.22 以降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。

25.5 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ー番号
  - [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。指定したフィルター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]

フィルター番号は、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。

25.6 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

設定値	説明
rip	RIP
bgp	BGP

  - [初期値] : -
- *filter_num*
  - [設定値] : フィルター番号
  - [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ー番号を指定する。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ーにより検査され、フィルターに該当すればその経路は OSPF に導入される。該当するフィルター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、フィルターの検査で該当した **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

25.7 OSPF で受け取った経路をどう扱うかのフィルターの設定

[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] : フィルター番号
  - [初期値] : -
- *nr* : フィルターの解釈の方法
  - [設定値] :

設定値	説明
not	フィルターに該当しない経路を導入する
reject	フィルターに該当した経路を導入しない
省略時	フィルターに該当した経路を導入する

  - [初期値] : -
- *kind* : フィルター種別
  - [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ーを定義す

る。このコマンドで定義したフィルターは、**ospf export from** コマンドの filter 項で指定されてはじめて効果を持つ。*ip_address/mask* では、ネットワークアドレスを設定する。これは、複数設定でき、経路の検査時にはそれぞれのネットワークアドレスに対して検査を行う。

nr が省略されている場合には、一つでも該当するフィルター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ー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ー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]

not 指定のフィルターを **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 指定のフィルターに合致するネットワークアドレスは、そのフィルターでは導入するかどうかが決定しないため、次のフィルター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、フィルターの意味が無い。

```
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 番のフィルターでは、192.168.1.0/24 以外の経路を導入し、2 番のフィルターで 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 番のフィルターにより、経路 192.168.2.0/24 は 1 番のフィルター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
```

25.8 外部経路導入に適用するフィルター定義

[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] : フィルター番号
  - [初期値] : -
- *nr* : フィルターの解釈の方法
  - [設定値] :

設定値	説明
not	フィルターに該当しない経路を広告する
reject	フィルターに該当した経路を広告しない
省略時	フィルター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ーを定義する。このコマンドで定義したフィルターは、**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ー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ー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ー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]

not 指定のフィルターを **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 指定のフィルターに合致するネットワークアドレスは、そのフィルターでは導入するかどうかが決定しないため、次のフィルター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、フィルターの意味が無い。

```
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 番のフィルターでは、192.168.1.0/24 以外の経路を広告し、2 番のフィルターで 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 番のフィルターにより、経路 192.168.2.0/24 は 1 番のフィルター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
```

25.9 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、エリアボーダー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。

25.10 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。

25.11 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。

25.12 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

設定値	説明
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)
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、そのインターフェースから直接通信できるすべての近隣ルーターとの間で同じ値でなくてはいけない。これらのパラメータの値が設定値とは異なっている 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。

25.13 指定インターフェースの 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 インターフェース名、LOOPBACK インターフェース名
  - [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] : インターフェースは 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 インターフェース設定時)
    - type=point-to-point(PP または TUNNEL インターフェース設定時)
    - type=loopback(LOOPBACK インターフェース設定時)
    - passive=インターフェースは passive ではない
    - cost=1(LAN インターフェース、LOOPBACK インターフェース設定時)、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]

指定したインターフェースの属する OSPF エリアを設定する。
NAME パラメータの type はインター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

NAME	VALUE	説明
	point-to-multipoint	ポイント・マルチポイント
	non-broadcast	NBMA
passive		インターフェースに対して、OSPF パケットを送信しない。該当インターフェースに他の OSPF ルーターがいない場合に設定する。
cost	コスト	インターフェースのコストを設定する。初期値は、インターフェースの種類と回線速度によって決定される。LAN インターフェースの場合は 1、PP インターフェースの場合は、バインドされている回線の回線速度を S[kbit/s]とすると、以下の計算式で決定される。例えば、64kbit/s の場合は 1562、1.536Mbit/s の場合には 65 となる。(0..65535) • COST=100000/S TUNNEL インターフェースの場合は、1562 がデフォルト値となる。
priority	優先度	指定ルーターの選択の際の優先度を設定する。PRIORITY 値が大きいルーターが指定ルーターに選ばれる。0 を設定すると、指定ルーターに選ばれなくなる。(0..255)
retransmit-interval	秒数	LSA を連続して送る場合の再送間隔を秒単位で設定する。 (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	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

NAME	VALUE	説明
	"increment"	単調増加

LOOPBACK インターフェースに設定する場合は、*type* パラメータでインターフェースタイプを、*cost* パラメータでインターフェースのコストを指定できる。LOOPBACK インター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 的なインターフェースの扱い	
			タイプ	状態
type	loopback	LOOPBACK インターフェースの IP アドレスのみのホスト経路	point-to-point	Loopback
	loopback-network	LOOPBACK インターフェースの 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 インターフェースは broadcast のみが許される。PP インターフェースは、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** コマンドでインターフェースに適切な 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ーフェースでは、**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-tomultipoint 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、インターフェースが接続しているネットワークに他の OSPF ルーターが存在しない場合に指定する。
passive を指定しておくと、インターフェースから 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 インターフェース (type=broadcast であるインターフェース) の場合には、インター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 インター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 インターフェースに対して **ip** *interface* **ospf area** コマンドを設定していない場合は、インター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、そのインターフェースから直接通信できるすべての近隣ルーターとの間で同じ値でなくてはいけない。これらのパラメータの値が設定値とは異なっている OSPF HELLO パケットを受信した場合には、それは無視される。

・MD5 認証鍵について

MD5 認証鍵を複数設定できる機能は、MD5 認証鍵を円滑に変更するためである。
通常の運用では、MD5 認証鍵は 1 つだけ設定しておく。MD5 認証鍵を変更する場合は、まず 1 つのルーターで新旧の MD5 認証鍵を 2 つ設定し、その後、近隣ルーターで MD5 認証鍵を新しいものに変更していく。そして、最後に 2 つの鍵を設定したルーターで古い鍵を削除すれば良い。

25.14 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 インターフェース名
  - [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。

25.15 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。

25.16 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	インター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。

25.17 インター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]

ルーターのインター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 ではインター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、インター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。

Rev.11.03.22 以降で使用可能。

第 26 章

BGP

26.1 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]

いずれかのインター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。

26.2 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] : フィルター番号 (1..2147483647)
  - [初期値] : -

[説明]

BGP で広告する集約経路を設定する。フィルターの番号には、**bgp aggregate filter** コマンドで定義した番号を指定する。

26.3 経路を集約するためのフィルターの設定

[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] : フィルター番号 (1..2147483647)
  - [初期値] : -
- *protocol*
  - [設定値] :

設定値	説明
static	静的経路

設定値	説明
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ーを定義する。このコマンドで定義したフィルターは、**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。

26.4 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。

26.5 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] : インター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、以下のインター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 インターフェース
- LOOPBACK インターフェース
- PP インターフェース

なお、プライマリ IPv4 アドレスが付与されたインター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。
Rev.11.03.22 以降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。

26.6 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

26.7 BGP で受信した経路に対するフィルターの適用

[書式]

bgp export *remote_as* filter *filter_num ...*
bgp export aspath *seq "aspath_regexp"* filter *filter_num ...*
no bgp export *remote_as* [filter *filter_num ...*]
no bgp export aspath *seq* [*"aspath_regexp"* [filter *filter_num ...*]]

[設定値及び初期値]

- *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_regexp*
  - [設定値] : 正規表現
  - [初期値] : -
- *filter_num*
  - [設定値] : フィルター番号 (1..2147483647)
  - [初期値] : -

[説明]

BGP で受けた経路に対してフィルターを設定する。*remote_as* を指定してフィルターを設定した場合、接続先から受けた経路についてフィルター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。フィルター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。フィルターの番号には **bgp export filter** コマンドで定義した番号を指定する。
aspath_regexp を指定してフィルターを設定した場合、*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ーに該当した経路が導入される。*aspath_regexp* には **grep** コマンドで使用できる検索パターンを指定する。

aspath_regexp を指定したフィルターを複数設定した場合、*seq* の小さい順に評価される。また、*aspath_regexp* を指定したフィルターを設定した場合、 *remote_as* を指定したフィルター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
```

フィルター番号は、100 個まで設定できる。

26.8 BGP で受信する経路に適用するフィルターの設定

[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] : フィルター番号 (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ーを定義する。このコマンドで定義したフィルターは、**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
```

26.9 BGP に導入する経路に対するフィルターの適用

[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] : フィルター番号 (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ーを設定する。フィルターに該当しない経路は導入されない。フィルターの番号には、**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。

フィルター番号は、100 個まで設定できる。

26.10 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。

26.11 BGP に導入する経路に適用するフィルターの設定

[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] : フィルター番号 (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ーを定義する。このコマンドで定義したフィルターは、**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。

[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
```

26.12 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/インターフェース	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

  - [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

[説明]

BGP コネクションを接続する近隣ルーターを定義する。

[ノート]

metric パラメータはすべての MED の初期値として働くので、**bgp import** コマンドで MED を設定したときにはそれが優先される。

gateway オプションは、接続先が同一のセグメントにないときに、その接続先に対するゲートウェイ (ネクストホップ) を指定する。

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。

26.13 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]

Rev.11.03.22 以降で使用可能。

26.14 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。

26.15 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

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] : 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]

Rev.11.03.22 以降で使用可能。

26.16 インター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]

ルーターのインターフェースの状態が変化したとき、bgp に外部経路を反映させる時間の間隔を設定する。

BGP ではインター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、インター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。

Rev.11.03.22 以降で使用可能。

第 27 章

IPv6

27.1 共通の設定

27.1.1 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。

27.1.2 IPv6 インターフェースのリンク MTU の設定

[書式]

ipv6 *interface* **mtu** *mtu*
ipv6 pp mtu *mtu*
no ipv6 *interface* **mtu** [*mtu*]
no ipv6 pp mtu [*mtu*]

[設定値及び初期値]

- *interface*
  - [設定値] : LAN インターフェース名
  - [初期値] : -
- *mtu*
  - [設定値] : MTU の値 (1280..1500)
  - [初期値] : 1500

[説明]

IPv6 インターフェースの MTU の値を設定する

27.1.3 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 インターフェース名
  - [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] :
    - off(Rev.11.03.22 以前)
    - auto(Rev.11.03.25 以降)

[説明]

インターフェースを通過する TCP セッションの MSS を制限する。インター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、インターフェースの MTU、もしくは PP インター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 インター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。

27.1.4 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 インターフェース名
  - [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]

Rev.11.03.22 以降で使用可能。

27.1.5 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。

27.1.6 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。

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。

27.2 IPv6 アドレスの管理

27.2.1 インターフェースの 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 インターフェース名、LOOPBACK 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] : -
- *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ーフェースの 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ーフェースの 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
ra-prefix	RA プロキシ

      - *prefix_interface*

設定値	説明
prefix_interface	転送元のインターフェース名

      - *interface_id*

設定値	説明
interface_id	インターフェース ID

      - *prefix_len*

設定値	説明
prefix_len	IPv6 プレフィックス長

  - [初期値] : -

[説明]

インターフェースに 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 インター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ーフェース 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ーフェース 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ーフェースに向く。

LOOPBACK インター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 インターフェースは指定できない。

[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
```

27.2.2 インター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 インターフェース名、ブリッジインターフェース名
  - [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*]
      - *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
prefix_interface	転送元のインターフェース名

      - *interface_id*

設定値	説明
interface_id	インターフェース ID

- *prefix_len*

設定値	説明
prefix_len	IPv6 プレフィックス長

- [初期値] : -

[説明]

インターフェースに 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ー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 インターフェースやトンネルインターフェースでは LAN1 インターフェースの 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、インター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。
prefix_interface には LOOPBACK インターフェースは指定できない。

[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。 )
```

27.2.3 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 インターフェース名、ブリッジインターフェース名
  - [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

設定値	説明
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。

27.2.4 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 インターフェース名
  - [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]

各インターフェースにおける DHCPv6 の動作を設定する。

27.2.5 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 インターフェース名、ブリッジインターフェース名
  - [初期値] : -

- *count*
  - [設定値] : 選択したインターフェースでの DAD の再送回数 (0..10)
  - [初期値] : 1

[説明]

インターフェースに 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。

27.2.6 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 インターフェースあたりの最大数 (1〜256)
  - [初期値] : 16

[説明]

RA によりインターフェースに自動的に設定される IPv6 アドレスの 1 インターフェースあたりの最大数を設定する。

27.2.7 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。

27.3 近隣探索

27.3.1 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
prefix_interface	転送元のインターフェース名

      - *interface_id*

設定値	説明
interface_id	インターフェース ID

      - *prefix_len*

設定値	説明
prefix_len	IPv6 プレフィックス長

  - [初期値] : -
- *valid_lifetime*
  - [設定値] : プレフィックスの有効寿命 (0..4294967295)
  - [初期値] : 2592000
- *preferred_lifetime*
  - [設定値] : プレフィックスの推奨寿命 (0..4294967295)
  - [初期値] : 604800
- *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 (0 以上 4294967295 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 インターフェースは指定できない。

[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。 )
```

27.3.2 ルーター広告の送信の制御

[書式]

ipv6 *interface* **rtadv send** *prefix_id* [*prefix_id*...] [*option=value*...]
ipv6 pp rtadv send *prefix_id* [*prefix_id*...] [*option=value*...]
no ipv6 *interface* **rtadv send** [...]
no ipv6 pp rtadv send [...]

[設定値及び初期値]

- *interface*
  - [設定値] : LAN インターフェース名
  - [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。
o_flag	on、off	other stateful configuration フラグ。ルーター広告以外の手段により

NAME	VALUE	説明
		IPv6 アドレス以外のオプション情報をホストに自動的に取得させるか否かの設定。
max-rtr-adv-interval	秒数	ルーター広告を送信する最大間隔 (4-1,800 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 の場合はインターフェースの MTU を採用する。

- [初期値] :
  - m_flag = off
  - o_flag = off
  - max-rtr-adv-interval = 600
  - min-rtr-adv-interval = 200
  - adv-default-lifetime = 1800
  - adv-reachable-time = 0
  - adv-retrans-time = 0
  - adv-cur-hop-limit = 64
  - mtu=auto

[説明]

インター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。

27.4 経路制御

27.4.1 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* : PP インターフェースへの経路。
  - *peer_num*
    - 相手先情報番号
    - anonymous
- pp anonymous name=*name*

設定値	説明
name	PAP/CHAP による名前

- dhcp *interface*

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 インターフェース名、ブリッジ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
- tunnel *tunnel_num* : トンネルインターフェースへの経路

- [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

metric *metric*	メトリックの指定
	• *metric*
	  • メトリック値 (1..15)
	  • 省略時は 1

hide	出力インターフェースが PP インター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 インターフェースが複数ある機種ではスコープ識別子でインターフェースを指定する必要がある。インター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 インター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 インターフェース、NULL インター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。

27.5 RIPng

27.5.1 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
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。

27.5.2 インターフェースにおける 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 インターフェース名
  - [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。

27.5.3 インターフェースにおける 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 インターフェース名
  - [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。

27.5.4 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]

- *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 インター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。

27.5.5 インター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 インターフェース名
  - [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。

27.5.6 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 インターフェース名
  - [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] : フィルター番号
  - [初期値] : -

[説明]

インター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ーを設定する。

27.5.7 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
```

27.5.8 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
```

27.5.9 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
```

27.5.10 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
```

27.5.11 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 インターフェースから 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。

27.5.12 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。
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。

27.6 VRRPv3 の設定

27.6.1 インターフェース毎の 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 インターフェース名
  - [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いけない。これらが食い違った場合の動作は予測できない。
auth パラメータを指定しない場合には、認証なしとして動作する。

time1 および *time2* パラメータで、マスターが 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 インターフェー

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。

Rev.11.03.08 以降で使用可能。

27.6.2 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*
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* route *network*

[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] : -
- *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] : -
- *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] :
    - インターフェース名
    - 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 インターフェース形式	指定した LAN インター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。 • **pp keepalive use** 設定によりダウンが検出された場合
route 形式	指定した経路が経路テーブルに存在しないか、*nexthop* で指定したインターフェースもしくは 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]

Rev.11.03.08 以降で使用可能。

27.7 フィルターの設定

27.7.1 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*
  - [設定値] : IP パケットの始点 IP アドレス
  - [初期値] : -
- *prefix_len*
  - [設定値] : プレフィックス長
  - [初期値] : -
- *dest_addr*
  - [設定値] : IP パケットの終点 IP アドレス (*src_addr* と同じ形式)。省略時は 1 個の * と同じ。
  - [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。

[設定例]

```
PP 1 で送受信される IPv6 Packet Too Big を記録する
# pp select 1
# ip pp secure filter in 1 100
# ip pp secure filter out 1 100
```

```
# ipv6 filter 1 pass-log * * icmp6 2
# ipv6 filter 100 pass * *
```

27.7.2 IPv6 フィルターの適用

[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 128 個以内)
  - [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]

IPv6 フィルターをインターフェースに適用する。

[ノート]

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。
動的フィルターは **ip policy filter** コマンドを使用する。
NULL インターフェースで *direction* に 'in' は指定できない。

27.7.3 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*
  - [設定値] : 始点 IPv6 アドレス
  - [初期値] : -
- *prefix_len*
  - [設定値] : プレフィックス長
  - [初期値] : -
- *dstaddr*
  - [設定値] : 終点 IPv6 アドレス

  - [初期値] : -
- *protocol* : プロトコルのニーモニック
  - [設定値] :
    - 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	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
    - 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コネクション (トリガ) を検出したら、それ以降 in キーワードと out キーワードの後に記述されたフィルタ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。

27.8 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、インター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、下流のインターフェースに存在するリスナーの情報を、上流のインター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ーモード (FilterMode) とソースリスト (SourceList) を使用します。フィルターモードには 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。

- フィルターモード : 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。

27.8.1 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 インターフェース名
  - [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]

インターフェースの MLD の動作を設定する。

[ノート]

report-link-local-group オプションは、Rev.11.03.22 以降で指定可能。

27.8.2 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 pv6 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 インターフェース名
  - [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* : フィルターモード
  - [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

設定値	説明
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いときに設定する。*filter_mode* と *source* は、マルチキャストパケットの送信元を限定するものである。
filter_mode として include を指定したときには、*source* として受信したい送信元を列挙する。*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 を設定したインターフェースで通知される。もし、このインターフェースが MLDv1 を使う場合には、*filter_mode* や *source* の値は無視される。

27.9 近隣要請

27.9.1 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] :

option	*value*	説明
na-proxy	all	近隣要請を行った後で、アドレス重複チェックの送信元への近隣広告はすべてプロキシする
	discard-one-time	近隣要請を行った後で、アドレス重複チェックの送信元への近隣広告を一回のみ破棄し、その後はプロキシする

  - [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。

第 28 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。

28.1 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。

28.2 SMTP メールサーバーの設定

[書式]

mail server smtp *id address* [port=*port*] [smtp-auth *username password* [*auth_protocol*]] [pop-before-smtp]
no mail server smtp *id* [...]

[設定値及び初期値]

- *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 25)
  - [初期値] : -
- *username*
  - [設定値] : 認証用ユーザー名
  - [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] : -

[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 (ユーザー名、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。

28.3 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] : 認証用ユーザー名
  - [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。

28.4 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。

28.5 メールの送信時に使用するテンプレートの設定

[書式]

mail template *template_id mailserver_id* From:*from_address* To:*to_address* [Subject:*subject*] [Date:*date*] [MIME-Version:*mime_version*] [Content-Type:*content_type*] [notify-log=*switch*] [notify-wait-time=*sec*]
no mail template *template_id* [...]

[設定値及び初期値]

- *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
- *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。

[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:FWX120 test" "Date:Mon, 23 Feb 2004 09:54:20 +0900"
 MIME-Version:1.0 "Content-Type:text/plain; charset=iso-2022-jp"
```

28.6 メール通知のトリガの設定

[書式]

mail notify *id template_id* trigger backup *if_b* [[*range_b*] *if_b* ...]]
mail notify *id template_id* trigger route *route* [*route* ...]
mail notify *id template_id* trigger filter ethernet *if_f dir_f* [*if_f dir_f* [...]]
mail notify *id template_id* trigger status *type* [*type* [...]]
mail notify *id template_id* trigger intrusion *if_i* [*range_i*] *dir_i* [*if_i* [*range_i*] *dir_i* [...]]
no mail notify *id* [...]

[設定値及び初期値]

- *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ーフェース
  - [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] :
    - インター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
  - [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ーの設定された LAN インターフェース
  - [初期値] : -

- *dir_f* : フィルター設定の方向
  - [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	インターフェースの情報
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ーフェース
  - [設定値] :

設定値	説明
pp	PP インターフェース
lanN(N,M,N/M)	LAN インターフェース
wan1	WAN インターフェース
tunnel	TUNNEL インターフェース
*	全てのインターフェース

  - [初期値] : -
- *range_i*
  - [設定値] :
    - インターフェース番号および範囲指定
    - 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
  - [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] : -

[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ーのログ表示、**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	**ip route** コマンド

イーサネットフィルター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ー.....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*/**pp**/**tunnel intrusion detection** コマンドの設定により検出されたものが通知対象となる。

また、一つのテンプレート ID に所属するメール通知設定はまとめて処理される。

[設定例]

```
mail notify 1 1 trigger backup pp * lan2 tunnel 1-10,12
mail notify 2 1 trigger route 192.168.1.0/24 172.16.0.0/16
mail notify 3 1 trigger filter ethernet lan1 in
mail notify 4 1 trigger status all
mail notify 5 1 trigger intrusion lan1 in/out pp * in tunnel 1-3,5 out
```

第 29 章

メールセキュリティー

29.1 メールセキュリティーを使用するか否か

[書式]

mail security use *sw*
no mail security 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]

メールセキュリティーを使用するか否かを設定する。

off から on に変更したときは、「ライセンスキーの購入」と「購入時の規約の同意」が済んでいるか否かを問い合わせる。規約は以下の URL から参照できる。

- http://www.rtpro.yamaha.co.jp/RT/docs/mail_security/license.pdf

[ノート]

Rev.11.03.13 以降で使用可能。

29.2 メールセキュリティーでチェックする受信ポート番号の設定

[書式]

mail security port pop *list*
no mail security port pop [*list*]

[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] : 110

[説明]

メールセキュリティーでチェックする受信ポート番号を設定する。

[ノート]

Rev.11.03.13 以降で使用可能。

29.3 メールセキュリティーでチェックする送信ポート番号の設定

[書式]

mail security port smtp *list*
no mail security port smtp [*list*]

[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] : 25 587

[説明]

メールセキュリティーでチェックする送信ポート番号を設定する。

[ノート]

Rev.11.03.13 以降で使用可能。

29.4 メールセキュリティーで件名に付与する文字列の設定

[書式]

mail security prefix *type prefix*
no mail security prefix *type* [*prefix*]

[設定値及び初期値]

- *type*
  - [設定値] :

設定値	説明
spam	スパムメール
virus	ウイルスメール

  - [初期値] : -
- *prefix* : 件名に付与する文字列 (半角英数 32 文字)
  - [初期値] :
    - spam = [SPAM DETECTED]
    - virus = [VIRUS DETECTED]

[説明]

メールセキュリティーで不正なメールの件名に付与する文字列を設定する。

[ノート]

Rev.11.03.13 以降で使用可能。

29.5 メールセキュリティーでチェックするメールサイズの上限

[書式]

mail security max size *size*
no mail security max size [*size*]

[設定値及び初期値]

- *size*
  - [設定値] : 上限サイズ (1..10m)
  - [初期値] : 5m

[説明]

メールセキュリティーでチェックするメールサイズの上限を設定する。

[ノート]

Rev.11.03.13 以降で使用可能。

29.6 アンチスパム判定の判定基準

[書式]

mail security spam level *level*
no mail security spam level [*level*]

[設定値及び初期値]

- *level*
  - [設定値] :

設定値	説明
high	判定基準が厳しい
middle	標準
low	判定基準が緩い

  - [初期値] : middle

[説明]

アンチスパム判定の判定基準を設定する。

[ノート]

Rev.11.03.13 以降で使用可能。

29.7 メールセキュリティーで機器が送信するメールの送信元アドレスの設定

[書式]

mail security smtp from address *address*
mail security smtp from address *account*
mail security smtp from address auto
no mail security smtp from address [..]

[設定値及び初期値]

- *address*
  - [設定値] : メールアドレス (@ を含む、半角 254 文字以内)
  - [初期値] : -
- *account*
  - [設定値] : メールアカウント (@ より前のユーザーアカウント、半角 64 文字以内)
  - [初期値] : -
- auto : メールの送信元アドレスをそのまま使用することを示すキーワード
  - [初期値] : auto

[説明]

メールセキュリティーで送信するメールの送信元アドレスを設定する。

address には、@ を含むメールアドレス全体を指定する。
account には、@ より前のユーザー名を指定する。*account* 形式の場合、@ 以降のドメイン名には、受信したメールの FROM アドレスの @ 以降を使用する。
auto を指定すると、メールの送信元アドレスがそのまま使用される。

[ノート]

Rev.11.03.13 以降で使用可能。

29.8 メールセキュリティーで機器が送信するメールの宛先アドレスの設定

[書式]

mail security smtp to address *address*
mail security smtp to address *account*
mail security smtp to address auto
no mail security smtp to address [..]

[設定値及び初期値]

- *address*
  - [設定値] : メールアドレス (@ を含む、半角 254 文字以内)
  - [初期値] : -
- *account*
  - [設定値] : メールアカウント (@ より前のユーザーアカウント、半角 64 文字以内)
  - [初期値] : -
- auto : メールの送信元アドレスをそのまま使用することを示すキーワード
  - [初期値] : auto

[説明]

メールセキュリティーで送信するメールの宛先アドレスを設定する。

address には、@ を含むメールアドレス全体を指定する。
account には、@ より前のユーザー名を指定する。*account* 形式の場合、@ 以降のドメイン名には、受信したメールの FROM アドレスの @ 以降を使用する。
auto を指定すると、メールの送信元アドレスがそのまま使用される。

[ノート]

Rev.11.03.13 以降で使用可能。

29.9 SMTP で送信するメールが不正なメールと判定されたときの動作の設定

[書式]

mail security smtp detect illegal mail *action*
no mail security smtp detect illegal mail [*action*]

[設定値及び初期値]

- *action*
  - [設定値] :

設定値	説明
transfer	元メールを添付ファイルとして転送する
reject	メールの送信元に対してエラーを返し、転送を中止する

  - [初期値] : transfer

[説明]

SMTP で送信するメールが不正なメールと判定されたときの動作を設定する。

transfer を指定した場合、不正なメールであることを本文に記載し、送信する元のメールを添付ファイルとしたメールを、**mail security smtp to address** コマンドで指定した宛先に転送する。
reject を指定した場合、不正なメールの送信元に 554 エラーを返し、SMTP サーバーにはメールを送らない。

[ノート]

Rev.11.03.13 以降で使用可能。

29.10 SMTP で送信するメールのサイズが上限を超えたときの動作

[書式]

mail security smtp size overflow *type*
no mail security smtp size overflow [*type*]

[設定値及び初期値]

- *type*
  - [設定値] :

設定値	説明
pass	メールをチェックせずに通過させる
reject	メールの送信元に対してエラーを返し、転送を中止する

  - [初期値] : pass

[説明]

メールサイズの上限を超えたメールを通過させるか否かを設定する。

[ノート]

Rev.11.03.13 以降で使用可能。

29.11 メールセキュリティーを利用できない場合のメール送受信の動作

[書式]

mail security inactive transfer *action*
no mail security inactive transfer [*action*]

[設定値及び初期値]

- *action*
  - [設定値] :

設定値	説明
pass	メールの送受信を許可する
reject	メールの送受信を許可しない

  - [初期値] : reject

[説明]

メールセキュリティーを利用できない場合の動作を設定する。
メールセキュリティーを利用できない場合とは、ライセンス有効期間外、または、YSC へのアクセスに失敗した場合を指す。

[ノート]

Rev.11.03.18 以降で使用可能。

29.12 ホワイトリストの定義

[書式]

mail security white-list pattern *id* [from=*keyword*] [to=*keyword*]
no mail security white-list pattern *id* [..]

[設定値及び初期値]

- *id*
  - [設定値] : ホワイトリスト番号 (1..65535)
  - [初期値] : -
- *keyword* : 一致させるキーワード
  - [設定値] : 任意の文字列
  - [初期値] : -

[説明]

ホワイトリストを定義する。

keyword を省略すると全一致を示す '*' が設定される。

[ノート]

Rev.11.03.13 以降で使用可能。

29.13 ホワイトリストセットの定義

[書式]

mail security white-list set *id list_num ...*
no mail security white-list set *id* [*list_num ...*]

[設定値及び初期値]

- *id*
  - [設定値] : ホワイトリストセット番号 (1..65535)
  - [初期値] : -
- *list_num* : 空白で区切られたホワイトリスト番号の並び (最大 128 個まで)
  - [初期値] : -

[説明]

ホワイトリストセットを定義する。

[ノート]

Rev.11.03.13 以降で使用可能。

29.14 ホワイトリストセットの有効化

[書式]

mail security white-list set enable *id*
no mail security white-list set enable [*id*]

[設定値及び初期値]

- *id*
  - [設定値] : ホワイトリストセット番号 (1..65535)
  - [初期値] : -

[説明]

ホワイトリストセットを指定する。

このコマンドで指定したホワイトリストセットだけが実際に有効になる。同時に有効にできるホワイトリストセットは 1 つだけである。

[ノート]

Rev.11.03.13 以降で使用可能。

29.15 YSC への接続タイムアウトの設定

[書式]

ysc connection timeout *time*
no ysc connection timeout [*time*]

[設定値及び初期値]

- *time*
  - [設定値] : YSC への接続がタイムアウトするまでの秒数 (3..60)
  - [初期値] : 10

[説明]

YSC (Yamaha Security Cloud) への接続タイムアウトを設定する。

[ノート]

Rev.11.03.13 以降で使用可能。

29.16 YSC へのメールスキャン要求に対するタイムアウトの設定

[書式]

ysc request timeout *time*
no ysc request timeout [*time*]

[設定値及び初期値]

- *time*
  - [設定値] : YSC へのメールスキャン要求がタイムアウトするまでの秒数 (10..300)
  - [初期値] : 30

[説明]

YSC (Yamaha Security Cloud) へのメールスキャン要求に対するタイムアウトを設定する。

[ノート]

Rev.11.03.13 以降で使用可能。

29.17 YSC への接続リトライ回数の設定

[書式]

ysc retry *count*
no ysc retry [*count*]

[設定値及び初期値]

- *count*
  - [設定値] : YSC でのメールスキャンに失敗した場合に、接続をリトライする回数 (1..3)
  - [初期値] : 2

[説明]

YSC (Yamaha Security Cloud) への接続リトライ回数を設定する。

リトライ時には異なるサーバーへの接続を試みる。

[ノート]

Rev.11.03.13 以降で使用可能。

第 30 章

HTTP サーバー機能

30.1 共通の設定

30.1.1 HTTP サーバー機能の有無の設定

[書式]

httpd service *switch*
no httpd service [*switch*]

[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。

30.1.2 HTTP サーバーへアクセスできるホストの IP アドレス設定

[書式]

httpd host *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	指定されたホストからのアクセスを許可する
lanN	HTTP サーバーへアクセスを許可する LAN インターフェース名
wan1	WAN1 側ネットワーク内ならば許可する
bridge1	ブリッジ側ネットワーク内ならば許可する
vlanN	HTTP サーバーへアクセスを許可する VLAN インターフェース名

  - [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 側ネットワーク内ならば許可する
  - [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。

30.1.3 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。

30.1.4 HTTP サーバー機能の listen ポートの設定

[書式]

httpd listen *port*
no httpd listen [*port*]

[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。

30.1.5 PP インターフェースとトンネルインターフェースの名前の設定

[書式]

pp name *name*
tunnel name *name*
no pp name [*name*]
no tunnel name [*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 インターフェースやトンネルインター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でのみ用いられる。

30.2 かんたん設定ページ用の設定

本節のコマンドは、FWX120 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。

30.2.1 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。

30.2.2 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 *interface* [*name*]
provider set *peer_num* [*name*]
no provider set *interface* [*name*]
no provider set *peer_num* [*name*]

[設定値及び初期値]

- *interface*
  - [設定値] : WAN インターフェース
  - [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。

30.2.3 プロバイダ接続設定

[書式]

provider select *interface*
provider select *peer_num*
no provider select

[設定値及び初期値]

- *interface*
  - [設定値] : WAN インターフェース
  - [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。

30.2.4 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。

30.2.5 LAN インターフェースの 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 インターフェース名、WAN インターフェース名
  - [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 インターフェースや WAN インターフェース側 DNS サーバーの IP アドレスを設定する。

30.2.6 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。

30.2.7 フィルター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* : フィルター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ー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。

30.2.8 LAN 側のプロバイダ名称の設定

[書式]

provider *interface* **name** [*protocol*] *type*:*name*
no provider *interface* **name** [*protocol*] [*type*:*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
  - [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] : ユーザー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 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。

30.2.9 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。

30.2.10 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。

30.2.11 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
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。

30.2.12 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。

30.2.13 LAN インター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 インターフェース名、WAN インターフェース名
  - [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]

LAN インターフェースや WAN インター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。

第 31 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。

31.1 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 インターフェース名、WAN インターフェース名
  - [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。

31.2 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] : -

[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。

31.3 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] : -
- *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。
インター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。

31.4 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。

31.5 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] : -
- all : すべてのインターフェース
  - [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。

31.6 ホスト名の登録

[書式]

netvolante-dns hostname host *interface host* [duplicate]
netvolante-dns hostname host pp *host* [duplicate]
no netvolante-dns hostname host *interface* [*host* [duplicate]]

no netvolante-dns hostname host pp [*host* [duplicate]]

[設定値及び初期値]

- *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] : -
- *host*
  - [設定値] : ホスト名 (63 文字以内)
  - [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) をユーザー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ーフェースに同じ名前を登録できる。

31.7 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 インターフェース名、WAN インターフェース名
  - [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。

31.8 ホスト名を自動生成するか否かの設定

[書式]

netvolante-dns auto hostname *interface switch*
netvolante-dns auto hostname pp *switch*
no netvolante-dns auto hostname *interface* [*switch*]
no netvolante-dns auto hostname pp [*switch*]

[設定値及び初期値]

- *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] : -
- *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

[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"以外のときは、『'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"以外のときは Rev.11.03.18 以降でホスト名の自動生成機能を利用可能。

31.9 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 インターフェース名、WAN インター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ーが指定することはできない。

31.10 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。

31.11 ネットボランチ DNS サーバー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	サーバー番号
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	サーバーアドレスの更新機能を有効にする
off	サーバー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 サーバーからの 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。

31.12 ネットボランチ DNS サーバー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	サーバー番号
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 サーバーの IP アドレス更新通知の待ち受けポート番号を設定する。

31.13 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 インターフェース名、WAN インターフェース名
  - [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。

31.14 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	サーバー番号
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。

31.15 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	サーバー番号
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 サーバー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。

第 32 章

UPnP の設定

32.1 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。

32.2 UPnP に使用する IP アドレスを取得するインターフェースの設定

[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 インターフェース名	指定した LAN インターフェースの IP アドレスを取得する
WAN インターフェース名	指定した WAN インターフェースの IP アドレスを取得する
default	デフォルトルートのインターフェース

  - [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ーフェースを設定する。

32.3 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。

32.4 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。

32.5 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。

第 33 章

USB の設定

33.1 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。

33.2 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。

第 34 章

スケジュール

34.1 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...*
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

設定値	説明
sd-attached	microSD デバイス認識時

  - [初期値] : -
- *peer_num*
  - [設定値] :
    - 相手先情報番号
    - anonymous
  - [初期値] : -
- *tunnel_num*
  - [設定値] : トンネルインターフェースの番号
  - [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**、**auth user**、**auth user group**、**bgp configure refresh**、**cold start**、**console info** と **console prompt** を除く **console** で始まるコマンド、**copy**、**copy exec**、**date**、**delete**、**exit**、**external-memory performance-test go**、**help**、**http revision-up go**、**http revision-up schedule**、**interface reset**、**less** で始まるコマンド、**login password**、**login password encrypted**、**login timer**、**login user**、**luac**、**make directory**、**nslookup**、**ospf configure refresh**、**packetdump**、**ping**、**ping6**、**pp select**、**quit**、**remote setup**、**rename**、**rtfs format**、**rtfs garbage collect**、**save**、**schedule at**、**show** で始まるコマンド、**sshd host key generate**、**sshd session**、**switch control function get** *FUNCTION*、**system packet-buffer**、**telnet**、**telnetd session**、**time**、**timezone**、**traceroute**、**traceroute6**、**tunnel select**、**user attribute**

[ノート]

入力時、*command* パラメータに対して TAB キーによるコマンド補完は行うが、シンタックスエラーなどは実行時まで検出されない。**schedule at** コマンドにより指定されたコマンドを実行する場合には、何を実行しようとしたかを INFO タイプの SYSLOG に出力する。
date に数字と曜日を混在させて指定はできない。
startup を指定したスケジュールはルーター起動時に実行される。電源を入れたらすぐ発信したい場合などに便利。

[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 pppoe auto connect on
# schedule at 2 */mon-fri 17:00 pp 1 pppoe 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 pppoe auto connect on
# schedule at 2 *:15 pp 1 pppoe 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
```

第 35 章

VLAN の設定

35.1 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 インターフェース名
  - [初期値] : -
- *sub_interface*
  - [設定値] : 1-8
  - [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 インター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 インターフェースあたり最大 8VLAN の設定ができる。

[ノート]

タグ付きパケットを受信した場合､そのタグの VID が受信 LAN インターフェースに設定されていなければパケットを破棄する。同一 LAN インターフェースで LAN 分割機能 (**lan type** コマンドの port-based-option=divide-network) との併用はできない。両者のうち先に入力されたものが有効となり、後から入力されるものはコマンドエラーになる。

35.2 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)
  - [初期値] : -
- *vlan_interface*
  - [設定値] : VLAN インターフェース名 (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 インターフェースを指定する。
ポートの名称には lan1.N を使用する。
同一の VLAN インター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。

lan1.N が所属する VLAN インターフェースは vlanN となる。

[ノート]

lan type コマンドで "port-based-option=divide-network" を設定し、LAN 分割機能を有効にしなければ本コマンドは機

能しない。
"port-based-option=divide-network" の設定が無い場合でも **vlan port mapping** は設定できるが、スイッチングハブの動作は変化しない。

[設定例]

```
# vlan port mapping lan1.3 vlan4
# vlan port mapping lan1.4 vlan4
```

第 36 章

生存通知機能

36.1 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。

36.2 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] :

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

  - [初期値] : off
- *option=value*
  - [設定値] :

option	***value***	説明
log	on	受信した内容を syslog に出力する。
	off	受信した内容を syslog に出力しない。
monitor	監視時間[秒](30..21474836)	指定した秒数の間に通知がない場合にアラートを上げる。
	off	生存通知の受信がない場合でもアラートを上げない。

  - [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。

36.3 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。

第 37 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ー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、当該インターフェースに 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 インターフェースの中で、若番のインター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。

37.1 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称を設定する。

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。

37.2 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)。

37.3 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。

37.4 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。

37.5 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。

37.6 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。

37.7 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。

37.8 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。

37.9 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。

37.10 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 (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。

37.11 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場合が ある。

37.12 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場合が ある。

第 38 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。

38.1 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。

38.2 SNTP サーバーへのアクセスを許可するホストの設定

[書式]

sntpd host *host*
no sntpd host

[設定値及び初期値]

- *host* : SNTP サーバーへ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	指定されたホストからのアクセスを許可する
any	すべてのホストからのアクセスを許可する
lan	すべての LAN 側ネットワーク内ならば許可する
lanN	SNTP サーバーへのアクセスを許可する LAN インターフェース名
vlanN	SNTP サーバーへのアクセスを許可する VLAN インターフェース名
none	すべてのホストからのアクセスを禁止する

  - [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。

第 39 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 秒以上押下し続け、外部メモリから設定ファイルおよびファームウェアファイルをコピーする。

さらに FWX120 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

39.1 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。

39.2 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。

39.3 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
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ことがある。

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、すべてのインターフェースに対して *size* に最大値を設定した状態で、同時にすべてのインター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ー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)

39.4 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*]
no external-memory 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 (半角英数字のみ)
  - [設定値] :

設定値	説明
usb1:*filename*	ファイル名のプレフィックス
sd1:*filename*	ファイル名のプレフィックス

  - [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] : -

[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 インターフェースのトラフィック量を書き出すファイル名は、yamaha_traffic_lan2_20080708.csv のようになる。
暗号化をしないときには、*crypto*、*password* パラメータを指定してはならない。

[ノート]

term として daily を設定したときには 1 日ごとに新しいファイルが生成されるが、統計情報のファイル数は 100 個に制限されているため、統計情報の種類を絞るか、頻繁にファイルを削除しないと、すぐにファイルが最大数に達してしまうので注意が必要である。
実際のファイル名は、*prefix* の後に種別や日付を表す文字列が加わる。

ファイル名の書式は以下に従う。 *prefix_type[_id]_yyyymm[dd].ext*

- *prefix*
  - 本コマンドにより設定される任意の文字列
- *type*
  - 統計情報の種類

cpu	CPU 使用率
memory	メモリ使用率
flow	ファストパスのフロー数
route	経路数
nat	NAT テーブルのエントリー数
filter	動的フィルターのセッション数
traffic	インター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
    - インターフェース別のトラフィック量.....インターフェースを表す
    - QoS のクラス別のトラフィック量.....インター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。

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。

39.5 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 - 3000 単位:行)
  - [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。

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。

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。

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。

バックアップファイル名は半角 99 文字以内。

interval オプションと *line* オプションは、Rev.11.03.13 以降で使用可能。

39.6 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。

39.7 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。

39.8 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。

39.9 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
usb1:*filename*	USB メモリ内のファームウェアファイル名
sd1:*filename*	microSD カード内のファームウェアファイル名
*:*filename*	USB メモリおよび microSD カード内のファームウェアファイル名

  - [初期値] : *:(機種名).bin
- *to* : コピー先ファイル名
  - [設定値] :

設定値	説明
num	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 (0,1) (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。

filename は半角 99 文字以内。

[設定例]

- microSD カード内から "fwx120.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:fwx120.bin
```

- microSD カード内のディレクトリ "test" から "fwx120.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/fwx120.bin
```

39.10 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:*filename*	USB メモリ内の設定ファイル名
sd1:*filename*	microSD カード内の設定ファイル名
*:*filename*	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
- *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。

filename は半角 99 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
```

39.11 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。

39.12 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。

39.13 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:*filename*	USB メモリ内のバッチファイル名

設定値	説明
sd1:*filename*	microSD カード内のバッチファイル名
*:*filename*	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

- *logfile*
  - [設定値] :

設定値	説明
filename	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]

filename 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、半角 91 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
```

39.14 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 インターフェース
sd1	microSD インターフェース

  - [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。

39.15 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。

39.16 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。

第 40 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。これらの上限値は、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。

40.1 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、Rev.11.03.13 以降で指定可能。

40.2 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 インターフェース

  - [初期値] : -
- *pin*
  - [設定値] : PIN コード
  - [初期値] : -

[説明]

USB インター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。

40.3 携帯端末に直接コマンドを発行する

[書式]

execute at-command *interface command*

[設定値及び初期値]

- *interface*
  - [設定値] :
    - usb1
  - [初期値] : -
- *command*
  - [設定値] :
    - AT コマンド
  - [初期値] : -

[説明]

指定したインター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。

40.4 指定した相手に対して発信制限を解除する

[書式]

clear mobile access limitation [*interface*]
clear mobile access limitation pp [*peer_num*]

[設定値及び初期値]

- *interface*
  - [設定値] :

設定値	説明
usb1	USB インターフェース
wan1	WAN インターフェース

  - [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 コマンドや *wan* **access limit** コマンドによって発信制限がかかったインターフェースに対し、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。

40.5 PP で使用するインターフェースの設定

[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ーフェースを設定する。

40.6 携帯端末からの自動発信設定

[書式]

mobile auto connect *auto*
no mobile auto connect [*auto*]

[設定値及び初期値]

- *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。

40.7 携帯端末を切断するタイマの設定

[書式]

mobile disconnect time *time*
no mobile disconnect time [*time*]

[設定値及び初期値]

- *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。

40.8 携帯端末を入力がないときに切断するタイマの設定

[書式]

mobile disconnect input time *time*
no mobile disconnect input time [*time*]

[設定値及び初期値]

- *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。

40.9 携帯端末を出力がないときに切断するタイマの設定

[書式]

mobile disconnect output time *time*
no mobile disconnect output time [*time*]

[設定値及び初期値]

- *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。

40.10 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 )
```

40.11 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。

40.12 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
1-2147483647	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] : 200000
- *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。
携帯端末のパケット通信は 128 バイトごとに課金されるが、ルーターと携帯端末間で送受信されるデータが 128 バイト単位である保証はない。
例えばルーターが 512 バイト (128 バイト×4) のデータを送受信したとしても、4 パケット分の通信料金である保証はなく、携帯網ではそれより多くのパケットに分割されて送受信されている可能性がある。
また、ルーターと携帯端末の間を流れるデータは非同期データであり、データの内容によっては本来のデータよりも長くなることがある。
従って、本コマンドで設定するデータ長はあくまで目安にしかならないので注意が必要である。
off を設定したときは警告が表示される。

40.13 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* で 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。

40.14 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。

40.15 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。

40.16 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。

40.17 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だけが記録され、発信動作前のものは記録されない。FOMA リモートセットアップ時も記録されない。
併せて **syslog debug** on の設定が必要となる。

40.18 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。

40.19 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
1-2147483647	バイト数、送受信するパケットデータ長の上限値
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。
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がある。
従って、本コマンドで設定するデータ長はあくまで目安にしかならないので注意が必要である。

40.20 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。

40.21 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
1-604800	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。

40.22 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.rtpro.yamaha.co.jp/RT/docs/mobile-internet/

Rev.11.03.22 以降で使用可能。

40.23 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。

Rev.11.03.22 以降で使用可能。

40.24 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。

40.25 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ーフェース
    - 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
off	出力しない

    - 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に取得する。
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。

[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。

40.26 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。

40.27 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* : インターフェース名
  - [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。

40.28 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* : インターフェース名
  - [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] : off

[説明]

USB ポートに接続した機器のフロー制御を行うかどうかを設定する。
接続した機器を用いたリモートセットアップ通信時に通信が意図せず切断されてしまう場合に off に設定すると効果がある場合がある。

40.29 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/

Rev.11.03.22 以降で使用可能。

40.30 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/

Rev.11.03.25 以降で使用可能。

40.31 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 インターフェース名

  - [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。

40.32 WAN で使用するインターフェースの設定

[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 インターフェース名

  - [初期値] : -
- *interface*
  - [設定値] :

設定値	説明
usb1	USB インターフェース名

  - [初期値] : -

[説明]

指定した WAN インターフェースについて実際に使用するインターフェースを設定する。

40.33 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 インターフェース名

  - [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 インターフェースについて自動接続するか否かを設定する。

40.34 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 インターフェース名

- [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 インターフェースについて、送受信がない場合の切断までの時間を設定する。

40.35 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 インターフェース名

  - [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 インターフェースについて、データ受信がない場合の切断までの時間を設定する。

40.36 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 インターフェース名

  - [初期値] : -
- *time*
  - [設定値] :

設定値	説明
1-21474836	秒数

設定値	説明
off	タイマを設定しない

- [初期値] : 120

[説明]

指定した WAN インターフェースについて、データ送信がない場合の切断までの時間を設定する。

40.37 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 インターフェース名

  - [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 インターフェースについて、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。

40.38 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 インターフェース名

  - [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 インター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。

40.39 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 インターフェース名

  - [初期値] : -
- *length*
  - [設定値] :

設定値	説明
1-2147483647	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] : 200000
- *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 インターフェースについて、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がある。
従って、本コマンドで設定するデータ長はあくまで目安にしかならないので注意が必要である。
off を設定したときは警告が表示される。

40.40 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 インターフェース名

  - [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 インターフェースについて、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。

40.41 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 インターフェース名

- [初期値] : -

- *length*
  - [設定値] :

設定値	説明
1-2147483647	バイト数、送受信するパケットデータ長の上限値
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 インターフェースについて、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。
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がある。
従って、本コマンドで設定するデータ長はあくまで目安にしかならないので注意が必要である。

40.42 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 インターフェース名

  - [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 インターフェースについて、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。

40.43 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 インターフェース名

  - [初期値] : -
- *duration*
  - [設定値] :

設定値	説明
1-604800	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 インターフェースについて、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。

第 41 章

ブリッジインターフェース (ブリッジ機能)

ブリッジインターフェースは複数のインターフェースを 1 つの仮想インターフェースに収容し、収容したインターフェース間でブリッジングを行う機能です。
収容された各インター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。

41.1 ブリッジインターフェースに収容する実インター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] : ブリッジインターフェース名
  - [初期値] : -
- *interface*
  - [設定値] : LAN インターフェース名
  - [初期値] : -

[説明]

仮想インターフェースであるブリッジインターフェースに収容する実インターフェースを指定する。
収容したインターフェース間でブリッジ動作が行われる。

[ノート]

・収容する LAN インターフェースについて
収容した実インターフェースに IPv4,IPv6 アドレスを付与してはならない。
収容した実インターフェースの IPv6 リンクローカルアドレスは削除される。
収容する LAN インターフェースの 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ーフェースに収容した実インターフェースは、他のブリッジインターフェースに収容することはできない。
収容するインターフェースがスイッチングハブを持つインターフェースである場合、スイッチングハブのポート間で完結する通信は本機能によるブリッジ動作ではなく、スイッチングハブ LSI 内部で処理される。

・ブリッジインターフェースについて
ブリッジインターフェースのリンク状態は収容した LAN インター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ーフェースがアップ状態だった場合、ブリッジインターフェースはアップ状態になる。
すべてのインターフェースがダウン状態だった場合、ブリッジインターフェースもダウン状態になる。
ブリッジインターフェースの MAC アドレスは、収容した LAN インターフェースのうち、インターフェース番号がもっとも小さいインターフェースのアドレスを使用する。

41.2 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] : ブリッジインターフェース名
- [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ーフェース名を指定する。
ラーニングを行う場合、ブリッジインターフェースに収容したインター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ー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ー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、受信インターフェースを除くすべての収容インター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。

41.3 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] : ブリッジインターフェース名
  - [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ー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。

41.4 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] : ブリッジインターフェース名

  - [初期値] : -
- *mac_address*
  - [設定値] : MAC アドレス
  - [初期値] : -
- *interface*
  - [設定値] : LAN インターフェース名
  - [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ー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* で指定したインターフェースに出力されるようになる。
interface には *bridge_interface* に収容された LAN インター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 インターフェースが *bridge_interface* に収容されていない場合、登録した情報は無視される。

第 42 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。

42.1 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。

42.2 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。

42.3 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。

42.4 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

42.5 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	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。

42.6 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。

第 43 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ーインターフェース) をユーザー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ーフェースが用意されており、ユーザーは 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、ユーザー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ーによって画面を切り替えることが可能です。

43.1 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。

43.2 カスタム GUI を使用するユーザーの設定

[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 を使用するユーザーを設定する。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ー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ー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。

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ーは、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。

43.3 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。

43.4 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。

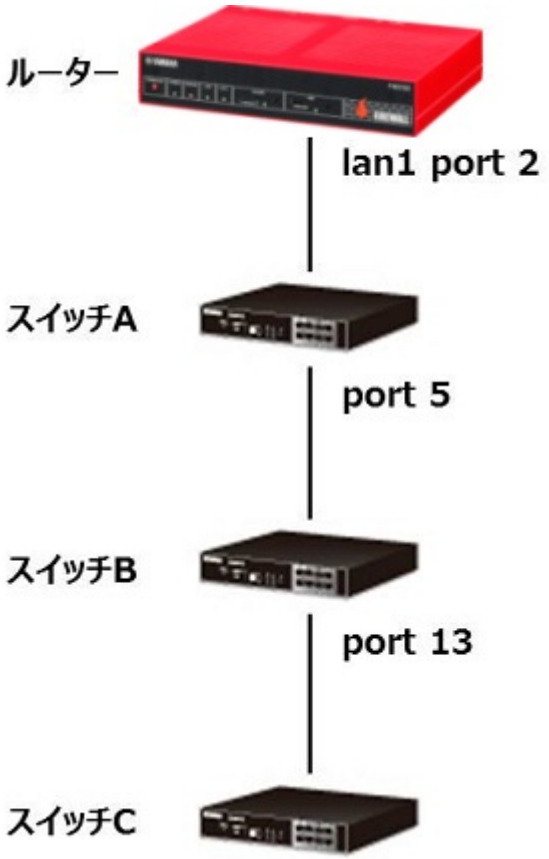
第 44 章

スイッチ制御機能

スイッチ制御機能とは、ヤマハのスイッチと無線 LAN アクセスポイントをルーターから制御するための機能です。スイッチやアクセスポイ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。

44.1 共通の設定

44.1.1 スイッチ制御機能を使用するか否かの設定

[書式]

switch control use *interface use*
no switch control use *interface*

[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] : -
- *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]

スイッチ制御機能を使用するか否かを LAN インターフェースごとに設定する。本コマンドが on に設定されたインターフェースでは、スイッチ制御機能に対応したスイッチを制御するための通信が行われる。スイッチ制御機能に対応したスイッチを配下に接続しないインターフェースにおいては本コマンドを off に設定することで、不要なパケットの送出を抑えることができる。

[ノート]

interface には物理的な LAN インターフェース (lanN) のみを指定することができる。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することができる。

44.1.2 スイッチ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]

スイッチを探索するパケットの送信時間間隔、およびスイッチ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、スイッチを接続してからルータ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、スイッチを接続してからルータ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スイッチから応答パケットを受信しない場合、当該スイッチはダウンしたと判断する。

[ノート]

スイッチ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スイッチがダウンしたと判断することがある。

44.2 スイッチの制御

44.2.1 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。

44.2.2 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。

44.2.3 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。

44.2.4 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。

44.2.5 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。

44.2.6 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。

44.2.7 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] : マスター経路
  - [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マスター経路とバックアップ経路を設定する。

route で指定した経路をマスター経路、*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* でマスター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 インターフェースで **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。

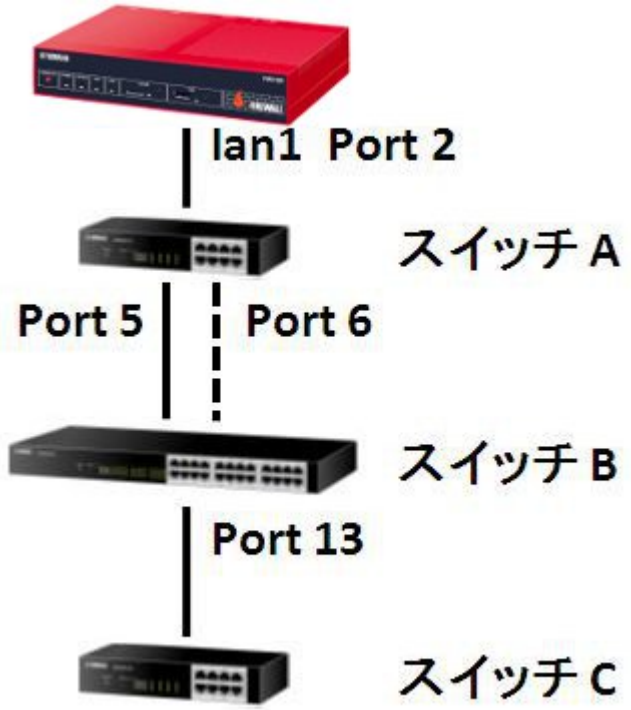
スイッチに本機能が実装されていない場合はコマンドエラーとなる。

Rev.11.03.04 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 をマスター経路、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
```



44.3 スイッチの機能

44.3.1 システム

44.3.1.1 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。

44.3.1.2 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。

44.3.1.3 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。

44.3.1.4 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。

44.3.1.5 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。

44.3.1.6 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 (_)。

44.3.1.7 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。

44.3.1.8 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。

44.3.1.9 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。 • 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。 • 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
duplex	各ポートの接続状態 (全二重/半二重) を表示する。 • 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。 • 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。

44.3.1.10 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。

44.3.1.11 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。

Rev.11.03.04 以降で使用可能。

44.3.1.12 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。

44.3.1.13 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。

44.3.2 ポート

44.3.2.1 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。

44.3.2.2 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。

44.3.2.3 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。

44.3.2.4 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無くなる。

[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。

44.3.2.5 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。

44.3.2.6 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。

44.3.2.7 スイッチ制御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]

スイッチ制御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。

Rev.11.03.04 以降で使用可能。

44.3.2.8 スイッチ制御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]

スイッチ制御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。

Rev.11.03.04 以降で使用可能。

44.3.2.9 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

状態	説明
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。

44.3.2.10 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。

44.3.2.11 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

状態	説明
10-hdx	10BASE-T 半二重
down	リンクダウン

44.3.3 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	

44.3.3.1 MAC アドレスエー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。

44.3.3.2 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。

44.3.3.3 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。

44.3.3.4 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。

44.3.3.5 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。

44.3.4 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
```

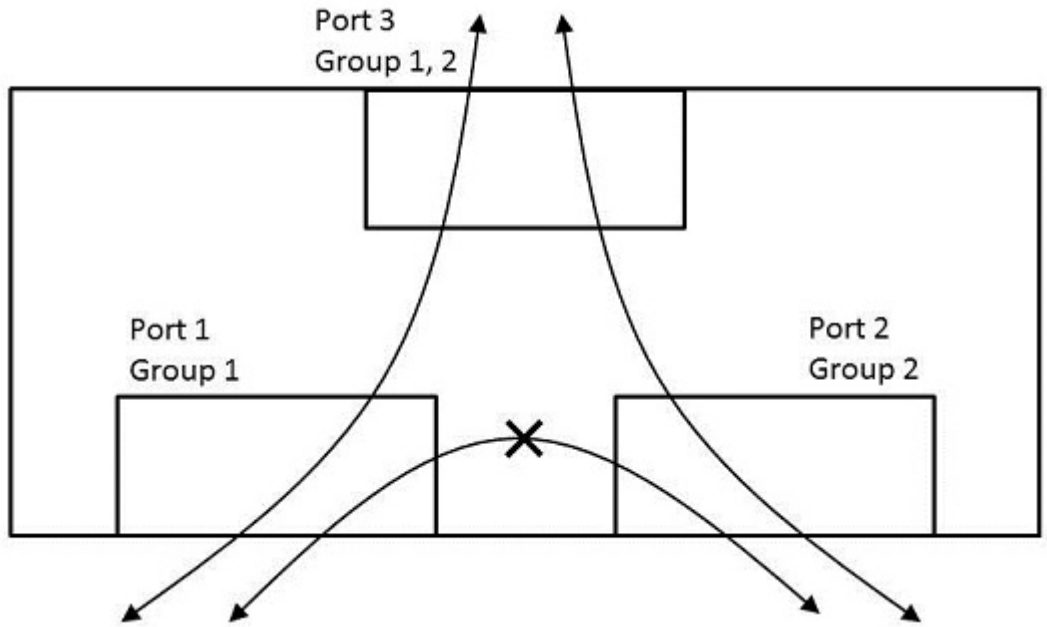
スイッチで受信したパケットは、VLAN タグの有無に関わらずいずれかの VLAN ID に分類され、その情報に基づいて転送処理が行われます。ポートの VLAN 動作モードは **vlan-port-mode** で設定します。

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。

44.3.4.1 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。

44.3.4.2 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。

44.3.4.3 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。

44.3.4.4 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。

44.3.4.5 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。

44.3.4.6 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。

44.3.5 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。具体的には以下のようになります。

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	

44.3.5.1 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。

44.3.5.2 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。

44.3.5.3 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。

44.3.5.4 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。

44.3.5.5 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。

44.3.5.6 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

設定値	説明
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。

44.3.5.7 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。

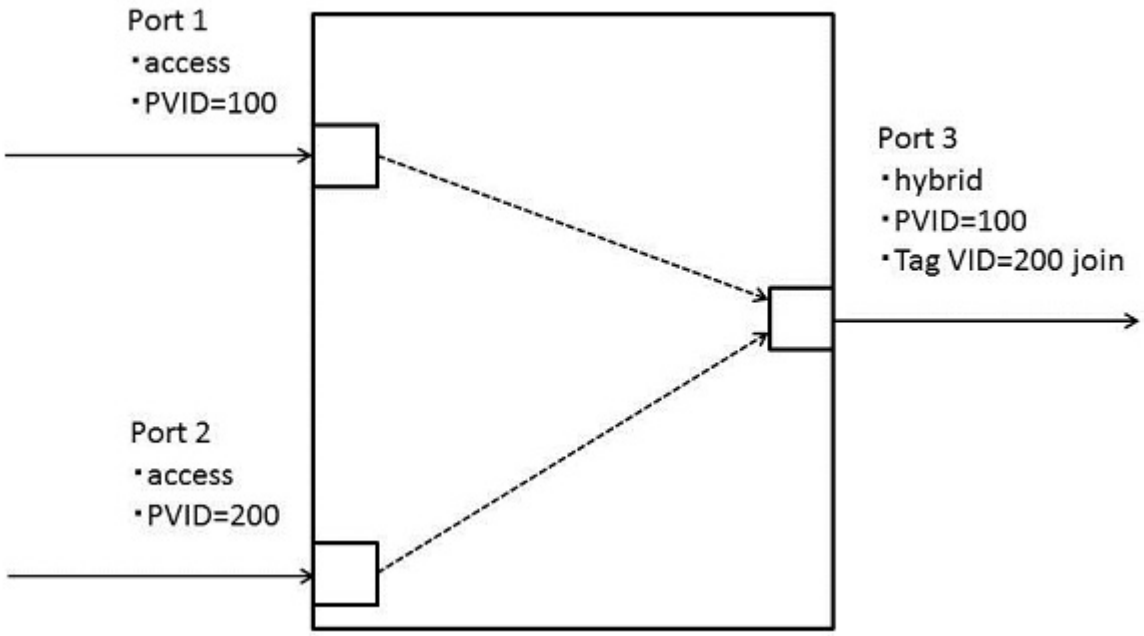
44.3.6 ミラーリング

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。

44.3.6.1 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。

44.3.6.2 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。

44.3.6.3 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。

44.3.6.4 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。

44.3.7 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。

44.3.7.1 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。

44.3.7.2 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
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

設定値	説明
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。

44.3.7.3 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。

44.3.7.4 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。

44.3.7.5 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。

44.3.7.6 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。

44.3.7.7 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。

44.3.8 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スイッチ制御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。

スイッチ制御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。

44.3.8.1 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。

44.3.8.2 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。

44.3.8.3 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。

44.3.8.4 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。

44.3.8.5 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。

44.3.8.6 スイッチ制御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]

スイッチ制御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。

Rev.11.03.04 以降で使用可能。

44.3.8.7 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

44.3.8.8 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。

44.3.8.9 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。

44.3.9 PoE 給電

44.3.9.1 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。

Rev.11.03.04 以降で使用可能。

44.3.9.2 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℃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 では Rev.11.03.04 以降で使用可能。

SWX2100-10PoE、SWX2100-5PoE では Rev.11.03.22 以降で使用可能。

44.3.9.3 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 では Rev.11.03.04 以降で使用可能。

SWX2100-10PoE、SWX2100-5PoE では Rev.11.03.22 以降で使用可能。

44.3.9.4 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。

Rev.11.03.04 以降で使用可能。

44.3.9.5 各ポートの消費電力の取得

[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]

各ポートの現在の消費電力を取得する。

[ノート]

SWX2200-8PoE では Rev.11.03.04 以降で使用可能。

SWX2100-10PoE、SWX2100-5PoE では Rev.11.03.22 以降で使用可能。

44.3.9.6 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。

44.3.9.7 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。

44.3.9.8 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。

Rev.11.03.04 以降で使用可能。

44.3.9.9 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。

44.3.9.10 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。

44.4 アクセスポイントの制御

44.4.1 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。

[ノート]

Rev.11.03.04 以降で使用可能。

44.4.2 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
  - [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。

[ノート]

Rev.11.03.04 以降で使用可能。

44.4.3 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
  - [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 が付いたものが使用される。

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。

[ノート]

Rev.11.03.04 以降で使用可能。

44.4.4 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 インターフェース名
  - [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 インターフェースを指定すると、LAN インター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。

Rev.11.03.04 以降で使用可能。

44.4.5 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 インターフェース名
  - [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 インターフェースを指定すると、LAN インター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。

Rev.11.03.04 以降で使用可能。

44.4.6 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。

Rev.11.03.04 以降で使用可能。

44.4.7 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

設定値	説明
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。

[ノート]

Rev.11.03.04 以降で使用可能。

44.4.8 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。

Rev.11.03.04 以降で使用可能。

44.4.9 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]

スイッチ制御機能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なくてもアクセスポイントの設定ができる。

Rev.11.03.04 以降で使用可能。

44.4.10 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。

[ノート]

Rev.11.03.04 以降で使用可能。

第 45 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

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/RT/docs/yno/agent/

45.1 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]

Rev.11.03.22 以降で使用可能。

45.2 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。

[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。

Rev.11.03.22 以降で使用可能。

45.3 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]

Rev.11.03.22 以降で使用可能。

45.4 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]

Rev.11.03.22 以降で使用可能。

45.5 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。

- 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	YNO 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	YNO 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	YNO エージェント機能が無効になり、YNO マネージャーと切断処理中
正常動作中	YNO マネージャーへの接続に成功した
異常発生	YNO 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

[ノート]

Rev.11.03.22 以降で使用可能。

[表示例]

```
> 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
```

第 46 章

診断

46.1 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 インターフェース名
  - [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ー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、フィルター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 フィルターは考慮されない。

46.2 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 インターフェース名
  - [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 フィルターは考慮されない。

46.3 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。

46.4 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。

46.5 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。

46.6 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。

46.7 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。

第 47 章

統計

47.1 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	通信量
flow	ファストパスフロー数
nat	NAT エントリ数
route	経路数
filter	フィルターにヒットした数
qos	各キューの処理量

  - [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。
当該ページにアクセスしても、統計情報を閲覧することはできない。

第 48 章

操作

48.1 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	接続相手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ーでも実行できる。
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 相手先情報番号のモデルによる違いについて」を参照。

48.2 トンネルインター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	トンネルインターフェース番号
none	トンネルインター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ーフェース番号を選択する。

[ノート]

本コマンドの操作は、一般ユーザーでも実行できる。
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ーフェース番号のモデルによる違いは 「IPsec の設定」を参照

48.3 設定に関する操作

48.3.1 管理ユーザーへの移行

[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。

48.3.2 終了

[書式]

quit
quit save
exit
exit save

[設定値及び初期値]

- save : 管理ユーザー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と、新しい設定内容を不揮発性メモリに保存するか否かを問い合わせる。不揮発性メモリに保存されれば、再起動を経ても同じ設定での起動が可能となる。

48.3.3 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
番号	内蔵フラッシュ ROM の設定ファイル番号 (0..4)
usb1:*filename*	USB メモリ内の設定ファイル名
sd1:*filename*	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]

filename は半角 99 文字以内。

48.3.4 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:*filename*	USB メモリ内の設定ファイル名
sd1:*filename*	microSD カード内の設定ファイル名
*:*filename*	USB メモリおよび microSD カード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
usb1:*filename*	USB メモリ内の設定ファイル名、*filename* は半角 64 文字以内
sd1:*filename*	microSD カード内の設定ファイル名、*filename* 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。

[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。
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。

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。

filename は半角 99 文字以内。

48.3.5 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
usb1:*filename*	USB メモリ内のファームウェアファイル名
sd1:*filename*	microSD カード内のファームウェアファイル名
*:*filename*	USB メモリおよび microSD カード内のファームウェアファイル名

  - [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。 (0 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。

filename は半角 99 文字以内。

48.3.6 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
番号	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]

保存されている設定ファイルを削除する。

48.3.7 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。

48.3.8 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。

48.3.9 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。

48.4 動的情報のクリア操作

48.4.1 アカウントのクリア

[書式]

clear account

[説明]

すべてのインターフェースに関するアカウントをクリアする。

48.4.2 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 インターフェースに関するアカウントをクリアする。

48.4.3 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。

48.4.4 データコネクト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。

48.4.5 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。

48.4.6 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。

48.4.7 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] : ブリッジインターフェース名
  - [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。

48.4.8 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 Rev.11.03.22 以降で指定可能。

48.4.9 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。

48.4.10 インター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 インターフェース名、WAN インターフェース名、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] : トンネルインターフェース番号
  - [初期値] : -

[説明]

指定したインター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ー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。 ブリッジインタフェースは Rev.11.03.08 以降で指定可能。

48.4.11 NAT アドレステーブルのクリア

[書式]

clear nat descriptor dynamic *nat_descriptor*

[設定値及び初期値]

- *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。

48.4.12 インターフェースの 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
    - 省略時は現在選択している相手先
  - [初期値] : -
- *tunnel_num*
  - [設定値] :
    - トンネルインターフェース番号
    - 省略時は現在選択されているトンネルインターフェース
  - [初期値] : -

[説明]

インター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。

48.4.13 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。

48.4.14 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。

48.4.15 近隣キャッシュの消去

[書式]

clear ipv6 neighbor cache

[説明]

近隣キャッシュを消去する。

48.4.16 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。

48.4.17 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ー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。

48.4.18 メールセキュリティーの検出履歴のクリア

[書式]

clear mail security history

[説明]

メールセキュリティーの検出履歴をクリアする。

[ノート]

Rev.11.03.13 以降で使用可能。

48.4.19 メールセキュリティーのホワイトリスト情報のクリア

[書式]

clear mail security white-list history

[説明]

メールセキュリティーのホワイトリスト情報をクリアする。

[ノート]

Rev.11.03.13 以降で使用可能。

48.4.20 YSC との通信状態確認用カウンタ情報のクリア

[書式]

clear status ysc

[説明]

YSC (Yamaha Security Cloud) との通信状態確認用カウンタ情報をクリアする。

[ノート]

Rev.11.03.13 以降で使用可能。

48.5 ファイル、ディレクトリの操作

48.5.1 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。

48.5.2 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。

48.5.3 ファイルまたはディレクトリの複製

[書式]

copy *path1 path2*

[設定値及び初期値]

- *path1*
  - [設定値] : コピー元となる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] : -
- *path2*
  - [設定値] : コピー先の相対パスまたは絶対パス
  - [初期値] : -

[説明]

ファイルまたはディレクトリを複製する。コピー元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。

path1 がファイルの場合の動作は以下の通りとなる。
path2 と同名のファイルが存在する場合は *path2* のデータが *path1* のデータで上書きされる。
path2 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 *path1* と同名のファイルが作成される。
path2 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 *path2* が作成される。

path1 がディレクトリの場合の動作は以下の通りとなる。
path2 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。
path2 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 *path1* と同名のディレクトリが作成される。
path2 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 *path2* が作成される。

path1、*path2* 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]

path1 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。

48.5.4 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。

48.6 その他の操作

48.6.1 相手先の使用許可の設定

[書式]

pp enable *peer_num*
no pp enable *peer_num*

[設定値及び初期値]

- *peer_num*
  - [設定値] :

設定値	説明
番号	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。

[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。

48.6.2 相手先の使用不許可の設定

[書式]

pp disable *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

設定値	説明
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。

48.6.3 再起動

[書式]

restart [*config*]

[設定値及び初期値]

- *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を指定できる。

48.6.4 インターフェースの再起動

[書式]

interface reset *interface* [*interface* ...]

[設定値及び初期値]

- *interface*
  - [設定値] :
    - LAN インターフェース名
    - WAN インターフェース名
    - USB インターフェース名
    - SD インターフェース名
  - [初期値] : -

[説明]

指定したインターフェースを再起動する。
LAN インターフェースでは、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。
USB と SD インターフェースでは、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]

FWX120 では、lan1 または lan2 に対してこのコマンドを実行すると、lan1 および lan2 インターフェースが同時にリセットされる。
USB と SD インターフェースは Rev.11.03.13 以降で指定可能。

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。対象とするインター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。

48.6.5 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 インターフェース名
  - [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
  - [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。

48.6.6 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 インターフェース名
  - [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
  - [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。

48.6.7 ping

[書式]

ping [-s *datalen*] [-c *count*] [-sa *ip_address*] [-w *wait*] *host*

[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
- *ip_address*
  - [設定値] : 始点 IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))
  - [初期値] : ルーターのインター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	Rev.11.03.13 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。

48.6.8 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] : ルーターのインター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	Rev.11.03.13 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]

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。
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。

48.6.9 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。

48.6.10 traceroute6 の実行

[書式]

traceroute6 *destination*

[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] : -

[説明]

指定した宛先までの経路を調べて表示する。

48.6.11 nslookup

[書式]

nslookup *host*

[設定値及び初期値]

- *host*

- [設定値] :
  - IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))
  - ホスト名
- [初期値] : -

[説明]

DNS による名前解決を行う。

[ノート]

IPv4 のみ対応。

48.6.12 IPv4 動的フィルター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。

48.6.13 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	*port* 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

設定値	説明
auto	*port* 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。

48.6.14 IPv6 動的フィルター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。

48.6.15 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 インターフェース名
  - [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。

48.6.16 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 インターフェース名
  - [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 インターフェースに 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ー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、Ctrl+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 インターフェース以外には Magic Packet を送信できない。

48.6.17 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る。

"no-confirm" オプションを指定すると、更新の確認をせずにファームウェアの書き換えを行う。さらに、"prompt" オプションを指定すると、コマンド実行直後にプロンプトが表示され、続けて他のコマンドを実行することができるようになる。ただし、ファームウェアを内蔵フラッシュ ROM に書き込んでいる間は他の操作ができなくなる。

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。

48.6.18 入力遮断フィルターの状態のクリア

[書式]

clear ip inbound filter [*interface* [*id*]]
clear ipv6 inbound filter [*interface* [*id*]]

[設定値及び初期値]

- *interface* : インターフェース
  - [設定値] :
    - LAN インターフェース (lan1、 lan2 など)
    - WAN インターフェース (wan1)
    - PP インターフェース (pp 1、 pp 2 など) ※'pp' と番号の間には空白が必要
    - TUNNEL インターフェース (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] : フィルターの識別子 (1 .. 65535)
  - [初期値] : -

[説明]

指定した入力遮断フィルターに関するログなどの情報をクリアする。インターフェースや ID を指定しないときには、すべてのインターフェースや ID が対象になる。

48.6.19 ポリシーフィルターの状態のクリア

[書式]

clear ip policy filter [*id*]
clear ipv6 policy filter [*id*]

[設定値及び初期値]

- *id*
  - [設定値] : フィルターの識別子 (1 .. 65535)
  - [初期値] : -

[説明]

指定したポリシーフィルター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ーが対象になる。

48.6.20 URL フィルター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]

URL フィルターの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。

48.6.21 外部データベース参照型 URL フィルター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。

48.6.22 プロキシ経由の HTTPS URL フィルターの統計情報のクリア

[書式]

clear url filter https-proxy
clear url filter https-proxy [*interface*]
clear url filter https-proxy pp [*peer_num*]
clear url filter https-proxy 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、ブリッジ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]

プロキシ経由の HTTPS URL フィルターの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。

48.6.23 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。

48.6.24 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ー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
```

48.6.25 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]

Rev.11.03.13 以降で使用可能。

第 49 章

設定の表示

49.1 機器設定の表示

[書式]

show environment

[説明]

以下の項目が表示される。

- システムのリビジョン
- CPU、メモリの使用量 (%)
- 動作しているファームウェアと設定ファイル
- 起動時に使用されるファームウェアと設定ファイル

49.2 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。

49.3 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]

Rev.11.03.13 以降で使用可能。

49.4 指定した PP の設定内容の表示

[書式]

show config pp [*peer_num*]
less config pp [*peer_num*]

[設定値及び初期値]

- *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。

49.5 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]

Rev.11.03.13 以降で使用可能。

49.6 指定したトンネルの設定内容の表示

[書式]

show config tunnel [*tunnel_num*] [expand]
less config tunnel [*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。

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。

49.7 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。

49.8 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]

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。

49.9 インター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、ブリッジ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
    - 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] : トンネルインターフェース番号
  - [初期値] : -

[説明]

各インターフェースに付与されている IPv6 アドレスを表示する。
インターフェースを指定しない場合は、すべてのインターフェースについて情報を表示する。

49.10 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、Rev.11.03.22 以降で使用可能。

[表示例]

```
> show sshd public key
ssh-dss XXXXXXXXXX1kc3MAAAEBAPTB9YYdgvE+4bbhF4mtoIJri+ujdAIfgr4hL/0w7Jlvc50eXg
sXJoCqlPlsLRGHOOzxVYbOouPCUV/jPFCatgOIii8eJNzUqSB1e6MOFtGjmESrdYiafyIUhps+YWqd
TlIo0AFnVUKMqAbYODA3Cy7kNVptYRK8rcKWk1ChbatWnT/Z7RcmEVEou0qlOyp79b3DcpFM7ofa4d
9ySb6mj06Y/Ok8lL5qFhCHmGOGtqJTKZsqb5VnPz8FYC8t1s6/tpyrUa5aG2af/yTEa5U5BDYAuc88
wNIUG9alGo/8WIHiBJAm432o7UPqTHWO/5nYEQu44gmEPQrPGJ65GT8AAAAVAOpjE0Jyei+4c5qWSF
PXUgrLf5HAAABAQCnnPO+ZjWZcZwGa6LxTGMczAjDy5uwD4DWBbRxsPKaXlsicJGC0aridnTthIGa8
ARypDjhpL1a37SDezx8yClQ5vh+4SPLdS1hdSSzXXE+MXIICXnOVPdiKC4ia10n81tMxW/EPw4SqFP
77r7VvCE/JpXv82AN2JTJ/HAn3X7lvMyCsKZLoWrEcEcBH5anvAQKByVt7RerToZ4vSgodskv7nyXX
XXXXXXX
ssh-rsa XXXXXXXXXX1yc2EAAAABIwAAAQEAwvAZK18jKTCHIHQfRV4r7UOYChX0oeKjBbuuLSDhSH
WmhpG3xxJO0pDIedSF3Knb7LX2SfymQYJ7XYIqMjmU0oziv/zi+De/z3M7wJHQUwfMZEDAdR6Mx39w
6Q04/ehQcaszjXi+0Al2wG/kk56lAU23CW/i21o//5GZTzkFKyEJUtWauHWEW9glF5Yy7F64PesqoH
6h5oDNK7LhlT7s4QXRnUJphIlINrW278Dnvyry3liR+tgTJAq3cGHfYsaQCdankDilIQhUazUY0vJO
/gjYCjMuWH6Ek/cst+PCtgnt0XV5Bl079uRUmcACs2pDX5EWrwbPXXXXXXXXXX==

> 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
```

49.11 指定したインターフェースのフィルター内容の表示

[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フィルター定義の内容を表示する。

49.12 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]

Rev.11.03.13 以降で使用可能。

第 50 章

状態の表示

50.1 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 インターフェース名
  - [初期値] : -
- *sub_interface*
  - [設定値] : 1-8
  - [初期値] : -

[説明]

ARP テーブルを表示する。インターフェース名を指定した場合、そのインター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。

50.2 インター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] : -

[説明]

インターフェースの状態を表示する。

50.3 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

50.4 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。

detail を指定した時には、現在有効な IPv4 経路に加えて、動的経路制御プロトコルによって得られた経路とのプリファレンス値の比較で隠されている静的経路も表示する。
summary を指定した時には、IPv4 の経路数をプロトコル毎に合計して表示する。

[ノート]

動的経路制御プロトコルで得られた経路については、プロトコルに応じて付加情報を表示する。表示する付加情報は以下のようになる。

プロトコル	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

50.5 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。

50.6 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。

50.7 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。

50.8 近隣キャッシュの表示

[書式]

show ipv6 neighbor cache

[説明]

近隣キャッシュの状態を表示する。

50.9 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] : ブリッジインターフェース名
  - [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。

50.10 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] :
    - セキュリティー・ゲートウェイの識別子
    - 省略時はすべてのセキュリティー・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ー名
- 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
- 適用したフィルターの情報

を同時に表示する。

50.11 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] : 証明書ファイルの識別子 (1..8)
  - [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。

50.12 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] : CRL ファイルの識別子 (1..8)
  - [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

50.13 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 インターフェース名

- [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。

50.14 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 マスカレードで大量にポートを使用している場合は、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** コマンドを使うことを推奨する。

50.15 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 インターフェース名、WAN インターフェース名
  - [初期値] : -

[説明]

NAT ディスクリプタと適用インターフェースのリストを表示する。

50.16 LAN インターフェースの 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]

インター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]

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。

50.17 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。

50.18 L2TP の状態の表示

[書式]

show status l2tp

[説明]

L2TP の状態を表示します。

50.19 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。

50.20 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

設定値	説明
interface	各インターフェースの状態
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。

50.21 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。

50.22 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)

50.23 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
  - インターフェース
  - 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

50.24 DHCPv6 の状態の表示

[書式]

show status ipv6 dhcp

[説明]

DHCPv6 に関係する状態を表示する。

50.25 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ーフェースについて、バックアップの状態を表示する。

50.26 動的フィルターによって管理されているコネクションの表示

[書式]

show ip connection
show ip connection [*interface* [*direction*]]
show ip connection pp [*peer_num* [*direction*]]
show ip connection tunnel [*tunnel_num* [*direction*]]
show ip connection summary

[設定値及び初期値]

- *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] : -
- *direction*
  - [設定値] :

設定値	説明
in	入力方向
out	出力方向

  - [初期値] : -
- summary : インターフェース/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] : -

[説明]

指定したインターフェースについて、動的なフィルターによって管理されているコネクションを表示する。インターフェースを指定しないときには、すべてのインターフェースの情報を表示する。

50.27 IPv6 の動的フィルターによって管理されているコネクションの表示

[書式]

show ipv6 connection
show ipv6 connection *interface* [*direction*]
show ipv6 connection pp [*peer_num* [*direction*]]
show ipv6 connection tunnel [*tunnel_num* [*direction*]]
show ipv6 connection summary

[設定値及び初期値]

- *interface*
  - [設定値] : LAN 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] : -
- *direction*
  - [設定値] :

設定値	説明
in	入力方向
out	出力方向

  - [初期値] : -
- summary : インターフェース/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] : -

[説明]

指定したインターフェースについて、動的なフィルターによって管理されているコネクションを表示する。インターフェースを指定しないときには、すべてのインターフェースの情報を表示する。

50.28 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。

50.29 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]

Rev.11.03.08 以降で使用可能。

50.30 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] : -
- *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ー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、以下のコマンドで設定した値となる。

- **ip** *interface* **intrusion detection report**
- **ip pp intrusion detection report**
- **ip tunnel intrusion detection report**

50.31 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。

50.32 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。

50.33 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
    - 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
インターフェース	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

50.34 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 インターフェース名
  - [初期値] : -
- *port*
  - [設定値] : ポート番号 (1..4)
  - [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 インターフェース名にはスイッチングハブを持つインターフェースだけが指定可能である。

50.35 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。

50.36 トンネルインターフェースの状態の表示

[書式]

show status tunnel [*tunnel_num*]
show status tunnel [*state*]

[設定値及び初期値]

- *tunnel_num*
  - [設定値] : トンネルインターフェース番号
  - [初期値] : -
- *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ー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ーフェース一覧を表示する

  - [初期値] : -

[説明]

トンネルインターフェースの状態を表示する。 state オプションは、PPTP トンネルには対応していない。PPTP トンネルは接続されていないトンネルインターフェースとして判定される。 また、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。

[ノート]

state オプションは、Rev.11.03.08 以降で使用可能。

50.37 VLAN インター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 インターフェース名
  - [初期値] : -
- *sub_interface*
  - [設定値] : 1-8
  - [初期値] : -

[説明]

VLAN インターフェースの情報を表示する。VLAN インターフェース名を指定した場合はそのインターフェースの情報だけを表示する。

50.38 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。

50.39 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。

50.40 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	入力インターフェース
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	出力インターフェース。複数のインターフェースに出力される場合は、"," 区切りで表示される。

50.41 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
```

50.42 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

[ノート]

Rev.11.03.08 以降で使用可能。

50.43 パケットバッファの状態の表示

[書式]

show status packet-buffer [*group*]

[設定値及び初期値]

- *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, 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

[表示例]

```
# show status packet-buffer large
large group: 2048 bytes length
 parameters: max-buffer=4992 max-free=1404 min-free=31
             buffer-in-chunk=312 init-chunk=4
 992 buffers in free list
 256 buffers are allocated, req/succ/fail/rel = 655/655/0/399
 4 chunks are allocated, req/succ/fail/rel = 4/4/0/0
```

50.44 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 インターフェース名 (省略時、全ての LAN インターフェースについて表示する)
  - [初期値] : -
- *class*
  - [設定値] : クラス (1..16)
  - [初期値] : -

[説明]

インターフェースに対して、QoS の設定情報や各クラスの使用状況を表示する。

- LAN インターフェース名
- キューイングアルゴリズム
- インターフェース速度
- 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

50.45 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

50.46 入力遮断フィルターの状態表示

[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]

入力遮断フィルターの状態を表示する。

50.47 ポリシーフィルターの状態表示

[書式]

show status ip policy filter [*id* [*type*]]
show status ip policy filter all *type*
show status ipv6 policy filter [*id* [*type*]]
show status ipv6 policy filter all *type*

[設定値及び初期値]

- *id*
  - [設定値] : 表示したいフィルターの識別子 (1..65535) ※省略時はすべてのフィルターについて表示する
  - [初期値] : -
- *type* : 表示の形式
  - [設定値] :

設定値	説明
connection	指定したフィルターに関係するコネクションの情報を表示する

  - [初期値] : -

[説明]

ポリシーフィルターの状態を表示する。
all キーワードを指定する書式では、ポリシーセットに設定されているすべてのフィルターが表示の対象となる。

[ノート]

all キーワードを指定する書式は、Rev.11.03.04 以降で使用可能。

50.48 ポリシーフィルター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]

ポリシーフィルターの制御対象とするサービスを表示する。

50.49 URL フィルターの情報の表示

[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]

インターフェースに適用されている URL フィルターの中で、どのフィルターに何回マッチしたかの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。

表示される内容は以下の通り。

- フィルター番号
- 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

[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ーがインター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ーとマッチした回数は表示されない。

50.50 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。

- セキュリティーレベル

- 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

50.51 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 Rev.11.03.04 以降で使用可能。

50.52 プロキシ経由の HTTPS URL フィルターの情報の表示

[書式]

show url filter https-proxy
show url filter https-proxy *interface*
show url filter https-proxy pp [*peer_num*]
show url filter https-proxy 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、ブリッジ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]

インターフェースに適用されているプロキシ経由の HTTPS コネクションの URL フィルターの中で、どのフィルターに何回マッチしたかの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。

表示される内容は以下の通り。
- フィルター番号
- 始点 IP アドレス
- HTTPS コネクションとフィルターが一致した回数

[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ーがインターフェースに適用されている場合、HTTPS コネクションがこのフィルターとマッチした回数は表示されない。

50.53 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)

50.54 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。

50.55 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。

50.56 技術情報の表示

[書式]

show techinfo

[説明]

技術サポートに必要な情報を一度に出力する。
他の **show** コマンドとは異なり、**show techinfo** コマンドの出力は **console columns/lines** コマンドの設定を無視して一度に出力される。一画面ごとに出力が停止するページ動作は行わない。そのため、ターミナルソフトのログ機能を用いて、出力を PC のファイルとして保存することが望ましい。
また、**console character** コマンドの設定も無視され、常に英語モードで出力される。
一画面ごとに内容を確認しながら出力したいときには、以下のように **less** コマンドを併用するとよい。ただし、**less** コマンドは画面制御シーケンスを多数出力するため、ログを記録しながら **less** コマンドを使用すると、ログファイルがわかりにくくなる。
show techinfo | less

[ノート]

ルーターに対して PC で動作する TFTP クライアントからアクセスし、ファイル名 'techinfo' を GET すると、**show techinfo** コマンドの出力と同じものが得られる。
Windows XP の TFTP.EXE を使用した例 :
C:\>tftp 192.168.0.1 get techinfo techinfo.txt

50.57 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。

50.58 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。

50.59 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
#
```

50.60 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

設定値	説明
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。

50.61 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。

50.62 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。

50.63 ルーターが制御しているスイッチ一覧の表示

[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
  - [初期値] : -

[説明]

ルーターが制御しているスイッチの一覧を表示する。インターフェースを指定しない場合は、すべてのインターフェースについて情報を表示する。

- MAC アドレス
- 機種名
- 機器名
- ルーターからの経路
- アップリンクポート
- スイッチ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

[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
```

```
> 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.
```

50.64 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]

マスター経路がリンクアップしている場合、マスター経路は 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。

マスター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、マスター経路は 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。

Rev.11.03.04 以降で使用可能。

50.65 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。

50.66 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)	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。
更新猶予期間 (Renew grace period)	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)	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。

Rev.11.03.13 以降で使用可能。

50.67 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]

Rev.11.03.13 以降で使用可能。

50.68 メールセキュリティーの統計情報の表示

[書式]

show status mail security [history]

[設定値及び初期値]

- history : 履歴を表示する
  - [初期値] : -

[説明]

メールセキュリティーの統計情報を表示する。

[ノート]

Rev.11.03.13 以降で使用可能。

50.69 ホワイトリストの統計情報の表示

[書式]

show status mail security white-list [history]

[設定値及び初期値]

- history : 履歴を表示する
  - [初期値] : -

[説明]

ホワイトリストにより許可されたメールの情報を表示する。

[ノート]

Rev.11.03.13 以降で使用可能。

50.70 YSC との通信状態の表示

[書式]

show status ysc

[説明]

YSC (Yamaha Security Cloud) との通信状態を表示する。

[ノート]

Rev.11.03.13 以降で使用可能。

50.71 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]

本コマンドは Rev.11.03.22 以降で使用可能。

第 51 章

ロギング

51.1 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] : リブ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。

ログを最大 3,000 件保持することができる。

最大数を越えた場合には、発生時刻の古いものから消去されていく。最大数以上のログを保存する場合には、**syslog host** コマンドでログを SYSLOG サーバーに転送して、そちらで保存する必要がある。

意図しないリブートが発生したときは、'saved' を指定することでリブ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。

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、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。

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。

51.2 アカウントの表示

[書式]

show account

[説明]

以下の項目を表示する。

- 発信回数
- 着信回数
- 課金情報の総計

[ノート]

電源 OFF や再起動により、それまでの課金情報はクリアされる。

51.3 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 インターフェースに関するアカウントを表示する。

51.4 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。

51.5 データコネクトのアカウントの表示

[書式]

show account ngn data

[説明]

データコネクト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る。

51.6 通信履歴の表示

[書式]

show history

[説明]

通信履歴を表示する。

索引

記号

> 39
>> 39

A

administrator 483
administrator password 42
administrator password encrypted 42
administrator radius auth 43
alarm batch 76
alarm entire 75
alarm http revision-up 77
alarm lua 426
alarm mobile 407
alarm sd 76
alarm startup 76
alarm usbhost 76
ap config directory 470
ap config filename 471
ap control config delete 472
ap control config get 471
ap control config set 471
ap control config-auto-set use 472
ap control firmware update go 473
ap control http proxy timeout 474
ap control http proxy use 473
ap select 470
auth user 212
auth user attribute 212
auth user group 213
auth user group attribute 214

B

bgp aggregate 314
bgp aggregate filter 314
bgp autonomous-system 315
bgp configure refresh 319
bgp export 316
bgp export aspath 316
bgp export filter 317
bgp force-to-advertise 321
bgp import 318
bgp import filter 319
bgp log 321
bgp neighbor 320
bgp neighbor pre-shared-key 321
bgp preference 316
bgp reric interval 322
bgp router id 315
bgp use 314
bridge learning 421
bridge learning bridge_interface static 422
bridge learning bridge_interface timer 422
bridge member 421

C

clear account 487
clear account mobile 487
clear account ngn data 487
clear account pp 487
clear arp 487
clear boot list 490
clear bridge learning 487
clear diagnosis config port 480
clear dns cache 488
clear external-memory syslog 490
clear heartbeat2 386
clear heartbeat2 id 386
clear heartbeat2 name 386
clear ip dynamic routing 487
clear ip inbound filter 500
clear ip policy filter 500
clear ip traffic list 121
clear ip traffic list pp 121
clear ip traffic list tunnel 121
clear ipv6 dynamic routing 489
clear ipv6 inbound filter 500
clear ipv6 neighbor cache 489
clear ipv6 policy filter 500
clear log 488
clear mail security history 490
clear mail security white-list history 490
clear mobile access limitation 402
clear mobile access limitation pp 402
clear nat descriptor dynamic 488
clear nat descriptor interface dynamic 489
clear nat descriptor interface dynamic pp 489
clear nat descriptor interface dynamic tunnel 489
clear pppoe pass-through learning 489
clear status 488
clear status ysc 490
clear switching-hub macaddress 498
clear url filter 500
clear url filter external-database 501
clear url filter external-database pp 501
clear url filter external-database tunnel 501
clear url filter https-proxy 501
clear url filter https-proxy pp 501
clear url filter https-proxy tunnel 501
clear url filter pp 500
clear url filter tunnel 500
cold start 486
connect 493
connect pp 493
connect tunnel 493
console character 50
console columns 50
console info 51
console lines 51
console prompt 50
cooperation 294
cooperation bandwidth-measuring remote 294
cooperation load-watch control 298
cooperation load-watch remote 296
cooperation load-watch trigger 297
cooperation port 294
cooperation type go 299
copy 491
copy config 483
copy exec 485

D

date 48
delete 491
delete config 485
description 63
description yno 476
dhcp client client-identifier 180
dhcp client client-identifier pool 180
dhcp client client-identifier pp 180
dhcp client hostname 179
dhcp client hostname pool 179
dhcp client hostname pp 179
dhcp client option 181
dhcp client option pool 181
dhcp client option pp 181
dhcp client release linkdown 182
dhcp convert lease to bind 175
dhcp duplicate check 171
dhcp manual lease 177
dhcp manual release 177
dhcp relay select 178
dhcp relay server 177
dhcp relay threshold 178
dhcp scope 171
dhcp scope bind 172
dhcp scope lease type 174
dhcp scope option 176
dhcp server rfc2131 compliant 170
dhcp service 169
diagnose config port access 479
diagnose config port map 478
diagnosis config port history-num 479
diagnosis config port max-detect 479
disconnect 494
disconnect ip connection 497
disconnect ipv6 connection 498
disconnect pp 494
disconnect tunnel 494
disconnect user 46
dns cache max entry 285
dns cache use 284
dns domain 279
dns host 284
dns notice order 280
dns private address spoof 280
dns server 278
dns server dhcp 279
dns server pp 279
dns server select 281
dns service 278
dns service fallback 285
dns srcport 284
dns static 282
dns syslog resolv 281

E

ethernet filter 125
ethernet interface filter 127
execute at-command 401
execute batch 397
exit 483
external-memory accelerator cache size 390
external-memory auto-search time 397
external-memory batch filename 397
external-memory boot permit 394
external-memory boot timeout 395
external-memory cache mode 389
external-memory config filename 396
external-memory exec filename 395
external-memory performance-test go 398
external-memory statistics filename prefix 391
external-memory syslog filename 392

G

grep 37

H

heartbeat pre-shared-key 380
heartbeat receive 380
heartbeat send 381
heartbeat2 myname 382
heartbeat2 receive 384
heartbeat2 receive enable 384
heartbeat2 receive log 385
heartbeat2 receive monitor 385
heartbeat2 receive record limit 385
heartbeat2 transmit 382
heartbeat2 transmit enable 383
heartbeat2 transmit interval 383
heartbeat2 transmit log 383
help 41
http revision-down permit 67
http revision-up go 499
http revision-up permit 65
http revision-up proxy 66
http revision-up schedule 67
http revision-up timeout 66
http revision-up url 66
httpd custom-gui api password 429
httpd custom-gui api use 429
httpd custom-gui use 428
httpd custom-gui user 428
httpd host 359
httpd listen 360
httpd service 359
httpd timeout 360

I

interface reset 493
ip arp timer 98
ip filter 85
ip filter directed-broadcast 89
ip filter dynamic 89
ip filter dynamic timer 90
ip filter set 88
ip filter source-route 88
ip flow timer 100
ip forward filter 123
ip fqdn filter timer 91
ip fragment remove df-bit 97
ip host 282
ip icmp echo-reply send 183
ip icmp echo-reply send-only-linkup 183
ip icmp error-decrypted-ipsec send 186
ip icmp log 186
ip icmp mask-reply send 183
ip icmp parameter-problem send 184

ip icmp redirect receive 184
ip icmp redirect send 184
ip icmp time-exceeded send 185
ip icmp timestamp-reply send 185
ip icmp unreachable send 185
ip implicit-route preference 100
ip inbound filter 128
ip interface address 80
ip interface arp log 100
ip interface arp queue length 99
ip interface arp static 99
ip interface dhcp lease time 180
ip interface dhcp retry 180
ip interface dhcp service 178
ip interface forward filter 123
ip interface inbound filter list 130
ip interface intrusion detection 92
ip interface intrusion detection notice-interval 93
ip interface intrusion detection repeat-control 93
ip interface intrusion detection report 93
ip interface mtu 82
ip interface nat descriptor 269
ip interface ospf area 309
ip interface ospf neighbor 312
ip interface proxyarp 98
ip interface proxyarp vrrp 98
ip interface rebound 82
ip interface rip auth key 109
ip interface rip auth key text 109
ip interface rip auth type 108
ip interface rip filter 107
ip interface rip force-to-advertise 112
ip interface rip hop 108
ip interface rip receive 107
ip interface rip send 106
ip interface rip trust gateway 105
ip interface secondary address 81
ip interface secure filter 96
ip interface secure filter name 96
ip interface tcp mss limit 94
ip interface tcp window-scale 94
ip interface traffic list 121
ip interface traffic list threshold 122
ip interface vrrp 113
ip interface vrrp shutdown trigger 114
ip interface wol relay 62
ip keepalive 119
ip local forward filter 123
ip policy address group 133
ip policy filter 134
ip policy filter set 136
ip policy filter set enable 137
ip policy filter set switch 137
ip policy filter timer 138
ip policy interface group 132
ip policy service 132
ip policy service group 134
ip pp address 80
ip pp forward filter 123
ip pp inbound filter list 130
ip pp intrusion detection 92
ip pp intrusion detection notice-interval 93
ip pp intrusion detection repeat-control 93
ip pp intrusion detection report 93
ip pp mtu 82
ip pp nat descriptor 269
ip pp ospf area 309
ip pp ospf neighbor 312
ip pp rebound 82
ip pp remote address 101
ip pp remote address pool 102
ip pp rip auth key 109
ip pp rip auth key text 109
ip pp rip auth type 108
ip pp rip backup interface 111
ip pp rip connect interval 110
ip pp rip connect send 110
ip pp rip disconnect interval 111
ip pp rip disconnect send 110
ip pp rip filter 107
ip pp rip force-to-advertise 112
ip pp rip hold routing 109
ip pp rip hop 108
ip pp rip receive 107
ip pp rip send 106
ip pp rip trust gateway 105
ip pp secure filter 96
ip pp secure filter name 96
ip pp tcp mss limit 94
ip pp tcp window-scale 94
ip pp traffic list 121
ip pp traffic list threshold 122
ip route 83
ip route change log 95
ip routing 80
ip routing process 55
ip simple-service 83
ip stealth 187
ip tos supersede 97
ip tunnel address 193
ip tunnel forward filter 123
ip tunnel inbound filter list 130
ip tunnel intrusion detection 92
ip tunnel intrusion detection notice-interval 93
ip tunnel intrusion detection repeat-control 93
ip tunnel intrusion detection report 93
ip tunnel mtu 82
ip tunnel nat descriptor 269
ip tunnel ospf area 309
ip tunnel ospf neighbor 312
ip tunnel rebound 82
ip tunnel remote address 193
ip tunnel rip auth key 109
ip tunnel rip auth key text 109
ip tunnel rip auth type 108
ip tunnel rip filter 107
ip tunnel rip force-to-advertise 112
ip tunnel rip hop 108
ip tunnel rip receive 107
ip tunnel rip send 106
ip tunnel rip trust gateway 105
ip tunnel secure filter 96
ip tunnel secure filter name 96
ip tunnel tcp mss limit 94
ip tunnel tcp window-scale 94
ip tunnel traffic list 121
ip tunnel traffic list threshold 122
ipsec auto refresh 199
ipsec ike always-on 201
ipsec ike auth method 196
ipsec ike backward-compatibility 210
ipsec ike child-exchange type 218

ipsec ike duration 219
ipsec ike eap myname 198
ipsec ike eap request 198
ipsec ike eap send certreq 199
ipsec ike encryption 207
ipsec ike esp-encapsulation 217
ipsec ike group 208
ipsec ike hash 209
ipsec ike keepalive log 207
ipsec ike keepalive use 205
ipsec ike local address 204
ipsec ike local id 205
ipsec ike local name 203
ipsec ike log 216
ipsec ike message-id-control 218
ipsec ike mode-cfg address 216
ipsec ike mode-cfg address pool 215
ipsec ike mode-cfg method 215
ipsec ike nat-traversal 223
ipsec ike negotiate-strictly 200
ipsec ike payload type 210
ipsec ike pfs 211
ipsec ike pki file 197
ipsec ike pre-shared-key 197
ipsec ike proposal-limitation 217
ipsec ike queue length 208
ipsec ike remote address 202
ipsec ike remote id 203
ipsec ike remote name 201
ipsec ike restrict-dangling-sa 222
ipsec ike retry 201
ipsec ike send info 211
ipsec ike version 196
ipsec ike xauth myname 212
ipsec ike xauth request 214
ipsec ipcomp type 225
ipsec log illegal-spi 209
ipsec refresh sa 222
ipsec sa delete 224
ipsec sa policy 220
ipsec transport 228
ipsec transport template 229
ipsec tunnel 225
ipsec tunnel fastpath-fragment-function follow df-bit 224
ipsec tunnel outer df-bit 224
ipsec use 195
ipv6 filter 341
ipv6 filter dynamic 342
ipv6 icmp echo-reply send 187
ipv6 icmp echo-reply send-only-linkup 187
ipv6 icmp error-decrypted-ipsec send 190
ipv6 icmp log 190
ipv6 icmp packet-too-big send 190
ipv6 icmp parameter-problem send 188
ipv6 icmp redirect receive 188
ipv6 icmp redirect send 188
ipv6 icmp time-exceeded send 189
ipv6 icmp unreachable send 189
ipv6 inbound filter 128
ipv6 interface address 325
ipv6 interface dad retry count 329
ipv6 interface dhcp service 329
ipv6 interface inbound filter list 130
ipv6 interface mld 344
ipv6 interface mld static 345
ipv6 interface mtu 323
ipv6 interface prefix 327
ipv6 interface prefix change log 328
ipv6 interface rip filter 336
ipv6 interface rip hop 335
ipv6 interface rip receive 335
ipv6 interface rip send 335
ipv6 interface rip trust gateway 336
ipv6 interface rtadv send 332
ipv6 interface secure filter 342
ipv6 interface tcp mss limit 323
ipv6 interface tcp window-scale 324
ipv6 interface vrrp 339
ipv6 interface vrrp shutdown trigger 340
ipv6 max auto address 330
ipv6 nd ns-trigger-dad 346
ipv6 policy address group 133
ipv6 policy filter 134
ipv6 policy filter set 136
ipv6 policy filter set enable 137
ipv6 policy filter set switch 137
ipv6 policy interface group 132
ipv6 policy service 132
ipv6 policy service group 134
ipv6 pp address 325
ipv6 pp dad retry count 329
ipv6 pp dhcp service 329
ipv6 pp inbound filter list 130
ipv6 pp mld 344
ipv6 pp mld static 345
ipv6 pp mtu 323
ipv6 pp prefix 327
ipv6 pp prefix change log 328
ipv6 pp rip connect interval 337
ipv6 pp rip connect send 337
ipv6 pp rip disconnect interval 338
ipv6 pp rip disconnect send 337
ipv6 pp rip filter 336
ipv6 pp rip hold routing 338
ipv6 pp rip hop 335
ipv6 pp rip receive 335
ipv6 pp rip send 335
ipv6 pp rip trust gateway 336
ipv6 pp rtadv send 332
ipv6 pp secure filter 342
ipv6 pp tcp mss limit 323
ipv6 pp tcp window-scale 324
ipv6 prefix 330
ipv6 rh0 discard 324
ipv6 rip preference 338
ipv6 rip use 334
ipv6 route 333
ipv6 routing 323
ipv6 routing process 325
ipv6 source address selection rule 330
ipv6 stealth 191
ipv6 tunnel address 325
ipv6 tunnel dhcp service 329
ipv6 tunnel inbound filter list 130
ipv6 tunnel mld 344
ipv6 tunnel mld static 345
ipv6 tunnel prefix 327
ipv6 tunnel prefix change log 328
ipv6 tunnel rip filter 336
ipv6 tunnel rip receive 335
ipv6 tunnel rip send 335
ipv6 tunnel secure filter 342

ipv6 tunnel tcp mss limit 323
ipv6 tunnel tcp window-scale 324

L

l2tp keepalive log 232
l2tp keepalive use 232
l2tp service 231
l2tp syslog 233
l2tp tunnel auth 231
l2tp tunnel disconnect time 232
lan backup 116
lan backup recovery time 117
lan count-hub-overflow 56
lan keepalive interval 118
lan keepalive log 118
lan keepalive use 117
lan linkup send-wait-time 56
lan port-mirroring 57
lan shutdown 56
lan type 57
less 38
less config 503
less config ap 503
less config list 504
less config pp 503
less config switch 504
less config tunnel 504
less exec list 506
less file list 504
less log 531
license authentication go 502
login password 42
login password encrypted 42
login radius use 43
login timer 61
login user 42
lua 424
lua use 424
luac 425

M

mail notify 350
mail notify status exec 501
mail security inactive transfer 356
mail security max size 354
mail security port pop 353
mail security port smtp 353
mail security prefix 354
mail security smtp detect illegal mail 356
mail security smtp from address 355
mail security smtp size overflow 356
mail security smtp to address 355
mail security spam level 354
mail security use 353
mail security white-list pattern 357
mail security white-list set 357
mail security white-list set enable 357
mail server name 347
mail server pop 348
mail server smtp 347
mail server timeout 348
mail template 349
make directory 490
mobile access limit connection length 408
mobile access limit connection time 408
mobile access limit duration 409
mobile access limit length 404
mobile access limit time 405
mobile access-point name 403
mobile arrive permit 410
mobile arrive use 409
mobile auto connect 402
mobile call prohibit auth-error count 406
mobile carrier mode 413
mobile dial number 404
mobile disconnect input time 403
mobile disconnect output time 403
mobile disconnect time 403
mobile display caller id 407
mobile firmware update go 412
mobile pin code 401
mobile signal-strength 410
mobile signal-strength go 410
mobile syslog 407
mobile use 400

N

nat descriptor address inner 271
nat descriptor address outer 270
nat descriptor ftp port 274
nat descriptor log 275
nat descriptor masquerade incoming 273
nat descriptor masquerade port range 274
nat descriptor masquerade remove df-bit 276
nat descriptor masquerade rlogin 272
nat descriptor masquerade session limit 276
nat descriptor masquerade static 272
nat descriptor masquerade unconvertible port 275
nat descriptor sip 275
nat descriptor static 271
nat descriptor timer 273
nat descriptor type 269
netvolante-dns auto hostname 368
netvolante-dns auto hostname pp 368
netvolante-dns auto save 371
netvolante-dns delete go 367
netvolante-dns delete go pp 367
netvolante-dns get hostname list 367
netvolante-dns get hostname list pp 367
netvolante-dns go 366
netvolante-dns go pp 366
netvolante-dns hostname host 367
netvolante-dns hostname host pp 367
netvolante-dns port 367
netvolante-dns register timer 371
netvolante-dns retry interval 370
netvolante-dns retry interval pp 370
netvolante-dns server 369
netvolante-dns server update address port 370
netvolante-dns server update address use 369
netvolante-dns set hostname 369
netvolante-dns timeout 368
netvolante-dns timeout pp 368
netvolante-dns use 366
netvolante-dns use pp 366
ngn radius account callee 248
ngn radius account caller 248
ngn radius auth password 247
ngn renumbering link-refresh 248

ngn type 244
nslookup 496
ntp backward-compatibility 49
ntp local address 49
ntpdate 49

O

operation button function download 399
operation execute batch permit 399
operation external-memory download permit 394
operation http revision-up permit 67
ospf area 306
ospf area network 306
ospf area stubhost 307
ospf configure refresh 301
ospf export filter 303
ospf export from ospf 302
ospf import filter 304
ospf import from 302
ospf log 312
ospf merge equal cost stub 312
ospf preference 301
ospf reric interval 313
ospf router id 301
ospf use 301
ospf virtual-link 307

P

ping 494
ping6 495
pki certificate file 230
pki crl file 230
pp always-on 104
pp auth accept 154, 236
pp auth multi connect prohibit 156
pp auth myname 155
pp auth request 155, 236
pp auth username 154
pp backup 115
pp backup pp 115
pp backup recovery time 116
pp backup tunnel 115
pp bind 234, 402
pp disable 492
pp enable 492
pp keepalive interval 102
pp keepalive log 104
pp keepalive use 103
pp name 360
pp select 482
ppp ccp maxconfigure 164
ppp ccp maxfailure 164
ppp ccp maxterminate 164
ppp ccp no-encryption 238
ppp ccp restart 163
ppp ccp type 163
ppp chap maxchallenge 159
ppp chap restart 159
ppp ipcp ipaddress 160
ppp ipcp maxconfigure 161
ppp ipcp maxfailure 161
ppp ipcp maxterminate 161
ppp ipcp msext 161
ppp ipcp remote address check 162
ppp ipcp restart 160
ppp ipcp vjc 160
ppp ipv6cp use 164
ppp lcp accm 406
ppp lcp acfc 156
ppp lcp magicnumber 156
ppp lcp maxconfigure 158
ppp lcp maxfailure 158
ppp lcp maxterminate 158
ppp lcp mru 157
ppp lcp pfc 157
ppp lcp restart 158
ppp lcp silent 158
ppp mscbcp maxretry 162
ppp mscbcp restart 162
ppp pap maxauthreq 159
ppp pap restart 159
pppoe access concentrator 165
pppoe auto connect 165
pppoe auto disconnect 165
pppoe disconnect time 167
pppoe invalid-session forced close 168
pppoe padi maxretry 166
pppoe padi restart 166
pppoe padr maxretry 166
pppoe padr restart 166
pppoe pass-through member 168
pppoe service-name 167
pppoe tcp mss limit 167
pppoe use 165
pptp hostname 235
pptp keepalive interval 238
pptp keepalive log 238
pptp keepalive use 237
pptp service 234
pptp service type 235
pptp syslog 237
pptp tunnel disconnect time 237
pptp vendorname 235
pptp window size 236
provider auto connect forced disable 364
provider dns server 362
provider dns server pp 363
provider filter routing 363
provider interface bind 365
provider interface dns server 362
provider interface name 363
provider ipv6 connect pp 365
provider ntp server 364
provider ntpdate 364
provider select 361
provider set 361
provider type 361

Q

queue class filter 287
queue interface class control 292
queue interface class filter list 290
queue interface class property 291
queue interface default class 291
queue interface length 290
queue interface type 289
queue pp class filter list 290
queue pp class property 291
queue pp default class 291

queue pp length 290
queue pp type 289
queue tunnel class filter list 290
quit 483

R

radius account 265
radius account port 267
radius account server 266
radius auth 265
radius auth port 267
radius auth server 266
radius retry 267
radius secret 267
radius server 265
rdate 48
remote setup accept 486
rename 492
restart 493
rip filter rule 112
rip preference 106
rip timer 113
rip use 105
rotate external-memory syslog 502
rtfs format 79
rtfs garbage-collect 79

S

save 483
schedule at 375
scp 73
sd use 389
security class 46
set 77
set-default-config 486
sftpd host 72
show account 531
show account mobile 532
show account ngn data 532
show account pp 532
show arp 507
show bridge learning 509
show command 41
show config 503
show config ap 503
show config list 504
show config pp 503
show config switch 504
show config tunnel 504
show copyright 530
show diagnosis config port access 480
show diagnosis config port map 480
show dns cache 528
show environment 503
show exec list 506
show file list 504
show history 532
show ip connection 514
show ip connection pp 514
show ip connection tunnel 514
show ip intrusion detection 516
show ip intrusion detection pp 516
show ip intrusion detection tunnel 516
show ip rip table 508
show ip route 508
show ip secure filter 506
show ip secure filter pp 506
show ip secure filter tunnel 506
show ip traffic list 122
show ip traffic list pp 122
show ip traffic list tunnel 122
show ipsec sa 509
show ipsec sa gateway 509
show ipv6 address 505
show ipv6 address pp 505
show ipv6 address tunnel 505
show ipv6 connection 515
show ipv6 connection pp 515
show ipv6 connection tunnel 515
show ipv6 mroute fib 519
show ipv6 neighbor cache 509
show ipv6 rip table 509
show ipv6 route 508
show log 531
show nat descriptor address 511
show nat descriptor interface address 511
show nat descriptor interface address pp 511
show nat descriptor interface address tunnel 511
show nat descriptor interface bind 511
show nat descriptor interface bind pp 511
show nat descriptor interface bind tunnel 511
show nat descriptor masquerade port summary 512
show pki certificate summary 510
show pki crl 510
show pp connect time 516
show pppoe pass-through learning 516
show sshd public key 505
show status 507
show status backup 514
show status bgp neighbor 513
show status boot 526
show status boot all 527
show status boot list 527
show status cooperation 521
show status dhcp 513
show status dhcpc 514
show status ethernet filter 127
show status external-memory 526
show status heartbeat 525
show status heartbeat2 386
show status heartbeat2 id 386
show status heartbeat2 name 386
show status ip inbound filter 522
show status ip keepalive 515
show status ip policy filter 522
show status ip policy service 522
show status ipv6 dhcp 514
show status ipv6 inbound filter 522
show status ipv6 mld 519
show status ipv6 policy filter 522
show status ipv6 policy service 522
show status l2tp 512
show status license 528
show status license authentication 529
show status lua 425
show status mail security 529
show status mail security white-list 530
show status mail service 518
show status mobile signal-strength 411
show status netvolante-dns 517

show status netvolante-dns pp 517
show status ngn 249
show status ospf 512
show status packet-buffer 520
show status pp 507
show status pptp 512
show status qos 520
show status remote setup 525
show status rtfs 526
show status sd 526
show status status-led 515
show status switch control 527
show status switch control route backup 528
show status switching-hub macaddress 517
show status tunnel 518
show status upnp 517
show status usbhost 525
show status user 519
show status user history 520
show status vlan 518
show status vrrp 510
show status yno 476
show status ysc 530
show techinfo 525
show url filter 523
show url filter external-database 523
show url filter external-database id 524
show url filter external-database pp 523
show url filter external-database tunnel 523
show url filter https-proxy 524
show url filter https-proxy pp 524
show url filter https-proxy tunnel 524
show url filter pp 523
show url filter tunnel 523
sip 100rel 241
sip arrive address check 243
sip arrive ringing p-n-uatype 242
sip arrive session timer method 242
sip arrive session timer refresher 242
sip ip protocol 241
sip log 244
sip outer address 243
sip response code busy 243
sip session timer 240
sip use 240
sip user agent 241
snmp community read-only 251
snmp community read-write 251
snmp display ipcp force 260
snmp host 250
snmp ifindex switch static index 262
snmp local address 257
snmp syscontact 257
snmp syslocation 258
snmp sysname 258
snmp trap community 251
snmp trap enable snmp 258
snmp trap enable switch 262
snmp trap enable switch common 263
snmp trap host 251
snmp trap link-updown separate-l2switch-port 261
snmp trap mobile signal-strength 261
snmp trap send linkdown 259
snmp trap send linkdown pp 259
snmp trap send linkdown tunnel 259
snmp yrifppdisplayatmib2 259
snmp yrifswitchdisplayatmib2 260
snmp yriftunneldisplayatmib2 260
snmp yrswindex switch static index 262
snmpv2c community read-only 252
snmpv2c community read-write 253
snmpv2c host 252
snmpv2c trap community 253
snmpv2c trap host 253
snmpv3 context name 254
snmpv3 engine id 253
snmpv3 host 255
snmpv3 trap host 257
snmpv3 usm user 254
snmpv3 vacm access 256
snmpv3 vacm view 255
sntpd host 387
sntpd service 387
speed 287
ssh 72
ssh encrypt algorithm 74
ssh known hosts 74
sshd client alive 71
sshd encrypt algorithm 70
sshd hide openssh version 71
sshd host 69
sshd host key generate 70
sshd listen 69
sshd service 68
sshd session 69
statistics 481
switch control firmware upload go 433
switch control function default 433
switch control function execute 432
switch control function execute clear-counter 462
switch control function execute clear-macaddress-table 446
switch control function execute reset-loopdetect 466
switch control function execute restart 439
switch control function execute restart-poe-supply 469
switch control function execute start-poe-supply 469
switch control function execute stop-poe-supply 470
switch control function get 432
switch control function get boot-rom-version 435
switch control function get counter-frame-rx-type 457
switch control function get counter-frame-tx-type 459
switch control function get energy-saving 436
switch control function get firmware-revision 435
switch control function get lag-type 439
switch control function get led-brightness 437
switch control function get loopdetect-count 462
switch control function get loopdetect-linkdown 463
switch control function get loopdetect-port-use 464
switch control function get loopdetect-recovery-timer 464
switch control function get loopdetect-time 463
switch control function get loopdetect-use-control-packet 464
switch control function get macaddress-aging 445
switch control function get macaddress-aging-timer 445
switch control function get mirroring-dest 456
switch control function get mirroring-src-rx 456
switch control function get mirroring-src-tx 457
switch control function get mirroring-use 455
switch control function get model-name 436
switch control function get poe-class 466
switch control function get port-auto-crossover 441
switch control function get port-blocking-control-packet 442
switch control function get port-blocking-data-packet 443
switch control function get port-flow-control 442

switch control function get port-speed 439
switch control function get port-speed-downshift 441
switch control function get port-use 440
switch control function get qos-dscp-remark-class 451
switch control function get qos-dscp-remark-type 451
switch control function get qos-policing-speed 453
switch control function get qos-policing-use 452
switch control function get qos-shaping-speed 454
switch control function get qos-shaping-use 453
switch control function get qos-speed-unit 452
switch control function get serial-number 435
switch control function get status-combo-port 443
switch control function get status-counter-frame-rx 460
switch control function get status-counter-frame-tx 461
switch control function get status-counter-octet-rx 461
switch control function get status-counter-octet-tx 462
switch control function get status-fan 438
switch control function get status-fan-rpm 438
switch control function get status-led-mode 437
switch control function get status-loopdetect-port 465
switch control function get status-loopdetect-recovery-timer 465
switch control function get status-macaddress-addr 446
switch control function get status-macaddress-port 446
switch control function get status-poe-detect-class 467
switch control function get status-poe-state 467
switch control function get status-poe-supply 468
switch control function get status-poe-supply-detail 468
switch control function get status-poe-supply-total 469
switch control function get status-poe-temperature 468
switch control function get status-port-sfp-rx-power 444
switch control function get status-port-speed 444
switch control function get system-macaddress 436
switch control function get system-name 436
switch control function get system-uptime 439
switch control function get vlan-access 448
switch control function get vlan-id 448
switch control function get vlan-multiple 450
switch control function get vlan-multiple-use 449
switch control function get vlan-port-mode 448
switch control function get vlan-trunk 449
switch control function set 432
switch control function set counter-frame-rx-type 457
switch control function set counter-frame-tx-type 459
switch control function set energy-saving 436
switch control function set led-brightness 437
switch control function set loopdetect-count 462
switch control function set loopdetect-linkdown 463
switch control function set loopdetect-port-use 464
switch control function set loopdetect-recovery-timer 464
switch control function set loopdetect-time 463
switch control function set loopdetect-use-control-packet 464
switch control function set macaddress-aging 445
switch control function set macaddress-aging-timer 445
switch control function set mirroring-dest 456
switch control function set mirroring-src-rx 456
switch control function set mirroring-src-tx 457
switch control function set mirroring-use 455
switch control function set poe-class 466
switch control function set port-auto-crossover 441
switch control function set port-blocking-control-packet 442
switch control function set port-blocking-data-packet 443
switch control function set port-flow-control 442
switch control function set port-speed 439
switch control function set port-speed-downshift 441
switch control function set port-use 440
switch control function set qos-dscp-remark-class 451
switch control function set qos-dscp-remark-type 451
switch control function set qos-policing-speed 453
switch control function set qos-policing-use 452
switch control function set qos-shaping-speed 454
switch control function set qos-shaping-use 453
switch control function set qos-speed-unit 452
switch control function set system-name 436
switch control function set vlan-access 448
switch control function set vlan-id 448
switch control function set vlan-multiple 450
switch control function set vlan-multiple-use 449
switch control function set vlan-port-mode 448
switch control function set vlan-trunk 449
switch control route backup 434
switch control use 430
switch control watch interval 431
switch select 431
syslog debug 53
syslog execute command 53
syslog facility 52
syslog host 51
syslog info 52
syslog local address 53
syslog notice 52
syslog srcport 53
system led brightness 77
system packet-buffer 74

T

tcp log 63
tcp session limit 95
telnet 497
telnetd host 54
telnetd listen 54
telnetd service 54
telnetd session 55
terminate lua 426
terminate lua file 426
tftp host 62
time 48
timezone 47
traceroute 496
traceroute6 496
tunnel backup 226
tunnel backup pp 226
tunnel backup tunnel 226
tunnel disable 192
tunnel enable 192
tunnel encapsulation 192
tunnel endpoint address 193
tunnel endpoint name 194
tunnel name 360
tunnel ngn arrive permit 245
tunnel ngn bandwidth 245
tunnel ngn call permit 246
tunnel ngn disconnect time 244
tunnel ngn fallback 247
tunnel ngn interface 246
tunnel ngn radius auth 247
tunnel select 482
tunnel template 226

U

upnp external address refer 372

upnp external address refer pp 372
upnp port mapping timer 373
upnp port mapping timer type 372
upnp syslog 373
upnp use 372
url filter 140
url filter external-database access failure 148
url filter external-database auth retry 153
url filter external-database category 146
url filter external-database id 150
url filter external-database id activate go 151
url filter external-database id check go 151
url filter external-database ipaddress access 149
url filter external-database log 150
url filter external-database lookup specified extension 149
url filter external-database lookup specified extension list 149
url filter external-database proxy server 146
url filter external-database register url 150
url filter external-database reject 148
url filter external-database reputation 147
url filter external-database server 145
url filter external-database update 152
url filter external-database use 145
url filter https-proxy curl 144
url filter https-proxy listen 144
url filter https-proxy use 143
url filter log 143
url filter port 141
url filter reject 142
url filter use 142
url interface filter 141
url interface proxy filter 143
url pp filter 141
url pp proxy filter 143
url tunnel filter 141
url tunnel proxy filter 143
usbhost modem flow control 412
usbhost modem initialize 411
usbhost overcurrent duration 374
usbhost use 374
user attribute 44

V

vlan interface 802.1q 378
vlan port mapping 378

W

wan access limit connection length 418
wan access limit connection time 419
wan access limit duration 420
wan access limit length 417
wan access limit time 417
wan access-point name 416
wan always-on 416
wan auth myname 413
wan auto connect 414
wan bind 414
wan disconnect input time 415
wan disconnect output time 415
wan disconnect time 414
wins server 161
wol send 499

Y

yno access code 475
yno log 476
yno use 475
ysc connection timeout 358
ysc request timeout 358
ysc retry 358

ヤマハルーターお客様ご相談センター
TEL : 03-5651-1330
FAX : 053-460-3489

ご相談受付時間
9:00 ～ 12:00　13:00 ～ 17:00
(土・日・祝日、弊社定休日、年末年始は休業とさせていただきます)

お問い合わせページ
http://jp.yamaha.com/products/network/

ヤマハ株式会社 (2018年6月 第10版)