

コマンドリファレンス

Rev.19.00.08, Rev.19.01.06

目次

序文：はじめに	19
第1章：コマンドリファレンスの見方	20
1.1 対応するプログラムのリビジョン	20
1.2 コマンドリファレンスの見方	20
1.3 インタフェース名について	20
1.4 no で始まるコマンドの入力形式について	21
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	21
1.6 デプロイ時の設定値について	21
第2章：コマンドの使い方	22
2.1 コンソールについて	22
2.1.1 コンソールによる設定手順	22
2.1.2 仮想マシンコンソールによる設定	23
2.1.3 TELNET による設定	25
2.1.4 SSH による設定	26
2.2 SSH サーバーについて	27
2.2.1 SSH サーバー機能の使用に当たっての注意事項	28
2.2.2 SSH サーバーの設定	28
2.3 TFTP について	28
2.3.1 TFTP による設定手順	29
2.3.2 設定ファイルの読み出し	29
2.3.3 設定ファイルの書き込み	30
2.4 コンソール使用時のキーボード操作について	30
2.5 「show」で始まるコマンド	32
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	32
2.5.2 show コマンドの表示内容を見やすくする	33
2.5.3 外部ストレージへのリダイレクト機能	34
第3章：ヘルプ	35
3.1 コンソールに対する簡易説明の表示	35
3.2 コマンド一覧の表示	35
第4章：機器の設定	36
4.1 ログインパスワードの設定	36
4.2 ログインパスワードの暗号化保存	36
4.3 管理パスワードの設定	36
4.4 管理パスワードの暗号化保存	36
4.5 一般ユーザ名とログインパスワードの設定	37
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	37
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	38
4.8 ソフトウェアライセンスの操作	38
4.8.1 ユーザー ID とパスワードの設定	38
4.8.2 ライセンスファイルの保存ディレクトリの設定	38
4.8.3 ライセンスが有効であるか否かの判定スケジュールの設定	39
4.8.4 ライセンスのインポート	39
4.8.5 ライセンスのエクスポート	40
4.8.6 ライセンスの削除	40
4.9 ユーザーの属性を設定	40

4.10 他のユーザの接続の強制切断	42
4.11 セキュリティクラスの設定	43
4.12 タイムゾーンの設定	44
4.13 現在の日付けの設定	44
4.14 現在の時刻の設定	44
4.15 リモートホストによる時計の設定	45
4.16 NTP による時計の設定	45
4.17 NTP パケットを送信するときの始点 IP アドレスの設定	46
4.18 Stratum 0 の NTP サーバーとの時刻同期を許可する設定	46
4.19 コンソールのプロンプト表示の設定	46
4.20 コンソールの言語とコードの設定	47
4.21 コンソールの表示文字数の設定	47
4.22 コンソールの表示行数の設定	47
4.23 コンソールにシステムメッセージを表示するか否かの設定	48
4.24 SYSLOG を受けるホストの IP アドレスの設定	48
4.25 SYSLOG ファシリティの設定	48
4.26 NOTICE タイプの SYSLOG を出力するか否かの設定	49
4.27 INFO タイプの SYSLOG 出力の設定	49
4.28 DEBUG タイプの SYSLOG を出力するか否かの設定	50
4.29 SYSLOG ファイルの設定	50
4.30 SYSLOG ファイルのファイルサーバーへの保存設定	51
4.31 SYSLOG を送信する時の始点 IP アドレスの設定	52
4.32 SYSLOG パケットの始点ポート番号の設定	52
4.33 SYSLOG に実行コマンドを出力するか否かの設定	52
4.34 インタフェースパケットのダンプを SYSLOG へ出力するか否かの設定	53
4.35 TELNET サーバー機能の ON/OFF の設定	53
4.36 TELNET サーバー機能の listen ポートの設定	54
4.37 TELNET サーバーへアクセスできるホストの設定	54
4.38 TELNET サーバーへ同時に接続できるユーザ数の設定	55
4.39 CPU 使用率の閾値の設定	55
4.40 メモリ使用率の閾値の設定	56
4.41 ファストパス機能の設定	56
4.42 LAN インタフェースの動作設定	57
4.43 LAN インタフェースのリンクアップ後の送信抑制時間の設定	57
4.44 LAN インタフェースの動作タイプの設定	57
4.45 LAN インタフェースの受信パケットバッファサイズの設定	58
4.46 ログインタイマの設定	59
4.47 TFTP によりアクセスできるホストの設定	59
4.48 Magic Packet を LAN に中継するか否かの設定	60
4.49 インタフェースまたはシステムの説明の設定	60
4.50 SSH サーバー機能の ON/OFF の設定	61
4.51 SSH サーバー機能の listen ポートの設定	61
4.52 SSH サーバーへアクセスできるホストの設定	62
4.53 SSH サーバーへ同時に接続できるユーザ数の設定	62
4.54 SSH サーバーホスト鍵の設定	63
4.55 SSH サーバーホスト鍵の表示	63
4.56 SSH サーバーで利用可能な暗号アルゴリズムの設定	64
4.57 SSH クライアントの生存確認	64
4.58 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	65

4.59 SSH サーバーで利用可能な認証方式の設定	65
4.60 SSH サーバーの公開鍵認証に用いる公開鍵情報を保存するファイルの設定	66
4.61 SSH サーバーの公開鍵認証に用いる公開鍵の設定	67
4.62 SSH サーバーの公開鍵認証に用いる公開鍵の表示	67
4.63 SFTP サーバーへアクセスできるホストの設定	68
4.64 SSH クライアント	69
4.65 SCP クライアント	69
4.66 SSH クライアントで利用可能な暗号アルゴリズムの設定	70
4.67 SSH サーバーの公開鍵情報を保存するファイルの設定	71
4.68 パケットバッファのパラメータを変更する	71
4.69 環境変数の設定	72
4.70 エイリアスの設定	73
4.71 マクロの設定	73
4.72 EMFS ファイルの作成、削除	74
4.73 CPU スケジューリング方式の設定	75
第 5 章 : IP の設定	77
5.1 インタフェース共通の設定	77
5.1.1 IP パケットを扱うか否かの設定	77
5.1.2 IP アドレスの設定	77
5.1.3 セカンダリ IP アドレスの設定	78
5.1.4 インタフェースの MTU の設定	79
5.1.5 同一インタフェースに折り返すパケットを送信するか否かの設定	79
5.1.6 IP の静的経路情報の設定	80
5.1.7 DHCP で IP アドレスを取得したときにデフォルト経路を自動的に追加するか否かを設定	82
5.1.8 DHCP で IP アドレスを取得したときに implicit 経路を自動的に追加するか否かを設定	82
5.1.9 IP パケットのフィルターの設定	83
5.1.10 フィルタセットの定義	86
5.1.11 Source-route オプション付き IP パケットをフィルタアウトするか否かの設定	86
5.1.12 ディレクテッドブロードキャストパケットをフィルタアウトするか否かの設定	87
5.1.13 動的フィルターの定義	87
5.1.14 動的フィルタのタイムアウトの設定	88
5.1.15 FQDN フィルターで使用するキャッシュのタイマーの設定	89
5.1.16 侵入検知機能の動作の設定	90
5.1.17 1 秒間に侵入検知情報を通知する頻度の設定	91
5.1.18 重複する侵入検知情報の通知抑制の設定	91
5.1.19 侵入検知情報の最大表示件数の設定	92
5.1.20 TCP セッションの MSS 制限の設定	92
5.1.21 TCP ウィンドウ・スケール・オプションを変更する	93
5.1.22 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	93
5.1.23 フィルタリングによるセキュリティの設定	93
5.1.24 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	95
5.1.25 IP パケットの TOS フィールドの書き換えの設定	95
5.1.26 代理 ARP の設定	96
5.1.27 ARP エントリの寿命の設定	96
5.1.28 静的 ARP エントリの設定	97
5.1.29 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	97
5.1.30 ARP エントリの変化をログに残すか否かの設定	98

5.1.31 implicit 経路の優先度の設定	98
5.1.32 フローテーブルの各エントリの寿命を設定する	98
5.1.33 フローテーブルのエントリー数の設定	99
5.1.34 フラグメントパケットを再構成するために保持しておく時間を設定	99
5.2 PP 側の設定	100
5.2.1 PP 側 IP アドレスの設定	100
5.2.2 リモート IP アドレスプールの設定	100
5.2.3 PP 経由のキープアライブの時間間隔の設定	101
5.2.4 PP 経由のキープアライブを使用するか否かの設定	102
5.2.5 PP 経由のキープアライブのログをとるか否かの設定	103
5.3 RIP の設定	103
5.3.1 RIP を使用するかどうかの設定	103
5.3.2 RIP に関して信用できるゲートウェイの設定	104
5.3.3 RIP による経路の優先度の設定	104
5.3.4 RIP パケットの送信に関する設定	105
5.3.5 RIP パケットの受信に関する設定	105
5.3.6 RIP のフィルタリングの設定	106
5.3.7 RIP で加算するホップ数の設定	106
5.3.8 RIP2 での認証の設定	107
5.3.9 RIP2 での認証キーの設定	107
5.3.10 RIP2 での広告動作モードの設定	108
5.3.11 回線切断時の経路保持の設定	108
5.3.12 回線接続時の PP 側の RIP の動作の設定	109
5.3.13 回線接続時の PP 側の RIP 送出の時間間隔の設定	109
5.3.14 回線切断時の PP 側の RIP の動作の設定	110
5.3.15 回線切断時の PP 側の RIP 送出の時間間隔の設定	110
5.3.16 バックアップ時の RIP の送信元インタフェース切り替えの設定	110
5.3.17 RIP で強制的に経路を広告する	111
5.3.18 RIP2 でのフィルタの比較方法	112
5.3.19 RIP のタイマーを調整する	112
5.4 VRRP の設定	113
5.4.1 インタフェース毎の VRRP の設定	113
5.4.2 シャットダウントリガの設定	114
5.5 バックアップの設定	115
5.5.1 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
5.5.2 バックアップからの復帰待ち時間の設定	116
5.5.3 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
5.5.4 バックアップからの復帰待ち時間の設定	117
5.5.5 LAN 経由のキープアライブを使用するか否かの設定	117
5.5.6 LAN 経由のキープアライブの時間間隔の設定	118
5.5.7 LAN 経由のキープアライブのログをとるか否かの設定	118
5.5.8 ネットワーク監視機能の設定	119
5.6 受信パケット統計情報の設定	121
5.6.1 受信パケットの統計情報を記録するか否かの設定	121
5.6.2 受信したパケットの統計情報のクリア	121
5.6.3 受信したパケットの統計情報の表示	122
5.6.4 統計情報を記録する受信パケットの分類数の設定	122
5.7 パケット転送フィルターの設定	123
5.7.1 パケット転送フィルターの定義	123

5.7.2 インタフェースへのパケット転送フィルターの適用	124
第6章：イーサネットフィルタの設定	125
6.1 フィルタ定義の設定	125
6.2 インタフェースへの適用の設定	126
6.3 イーサネットフィルタの状態の表示	127
第7章：PPPの設定	128
7.1 相手の名前とパスワードの設定	128
7.2 受け入れる認証タイプの設定	128
7.3 要求する認証タイプの設定	129
7.4 自分の名前とパスワードの設定	129
7.5 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	130
7.6 常時接続の設定	130
7.7 LCP 関連の設定	131
7.7.1 Address and Control Field Compression オプション使用の設定	131
7.7.2 Magic Number オプション使用の設定	131
7.7.3 Maximum Receive Unit オプション使用の設定	132
7.7.4 Protocol Field Compression オプション使用の設定	132
7.7.5 lcp-restart パラメータの設定	132
7.7.6 lcp-max-terminate パラメータの設定	133
7.7.7 lcp-max-configure パラメータの設定	133
7.7.8 lcp-max-failure パラメータの設定	133
7.7.9 Configure-Request をすぐに送信するか否かの設定	133
7.8 PAP 関連の設定	134
7.8.1 pap-restart パラメータの設定	134
7.8.2 pap-max-authreq パラメータの設定	134
7.9 CHAP 関連の設定	134
7.9.1 chap-restart パラメータの設定	134
7.9.2 chap-max-challenge パラメータの設定	135
7.10 IPCP 関連の設定	135
7.10.1 Van Jacobson Compressed TCP/IP 使用の設定	135
7.10.2 PP 側 IP アドレスのネゴシエーションの設定	135
7.10.3 ipcp-restart パラメータの設定	136
7.10.4 ipcp-max-terminate パラメータの設定	136
7.10.5 ipcp-max-configure パラメータの設定	136
7.10.6 ipcp-max-failure パラメータの設定	136
7.10.7 WINS サーバーの IP アドレスの設定	137
7.10.8 IPCP の MS 拡張オプションを使うか否かの設定	137
7.10.9 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	137
7.11 MSCBCP 関連の設定	138
7.11.1 mscbcpc-restart パラメータの設定	138
7.11.2 mscbcpc-maxretry パラメータの設定	138
7.12 CCP 関連の設定	138
7.12.1 全パケットの圧縮タイプの設定	138
7.12.2 ccp-restart パラメータの設定	139
7.12.3 ccp-max-terminate パラメータの設定	139
7.12.4 ccp-max-configure パラメータの設定	139
7.12.5 ccp-max-failure パラメータの設定	140
7.13 IPV6CP 関連の設定	140
7.13.1 IPV6CP を使用するか否かの設定	140

7.14 BACP 関連の設定	140
7.14.1 bacp-restart パラメータの設定	140
7.14.2 bacp-max-terminate パラメータの設定	141
7.14.3 bacp-max-configure パラメータの設定	141
7.14.4 bacp-max-failure パラメータの設定	141
7.15 BAP 関連の設定	141
7.15.1 bap-restart パラメータの設定	141
7.15.2 bap-max-retry パラメータの設定	142
7.16 PPPoE 関連の設定	142
7.16.1 PPPoE で使用する LAN インタフェースの指定	142
7.16.2 アクセスコンセントレータ名の設定	142
7.16.3 セッションの自動接続の設定	142
7.16.4 セッションの自動切断の設定	143
7.16.5 PADI パケットの最大再送回数の設定	143
7.16.6 PADI パケットの再送時間の設定	143
7.16.7 PADR パケットの最大再送回数の設定	144
7.16.8 PADR パケットの再送時間の設定	144
7.16.9 PPPoE セッションの切断タイマの設定	144
7.16.10 サービス名の指定	145
7.16.11 TCP パケットの MSS の制限の有無とサイズの指定	145
7.16.12 ルーター側には存在しない PPPoE セッションを強制的に切断するか否かの設定	145

第 8 章 : DHCP の設定147

8.1 DHCP サーバー・リレーエージェント機能	147
8.1.1 DHCP の動作の設定	147
8.1.2 RFC2131 対応動作の設定	148
8.1.3 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	149
8.1.4 DHCP スコープの定義	149
8.1.5 DHCP 予約アドレスの設定	150
8.1.6 DHCP アドレス割り当て動作の設定	152
8.1.7 DHCP 割り当て情報を元にした予約設定の生成	153
8.1.8 DHCP オプションの設定	154
8.1.9 DHCP リース情報の手動追加	155
8.1.10 DHCP リース情報の手動削除	155
8.1.11 DHCP サーバーの指定の設定	156
8.1.12 DHCP リレーエージェント機能で使用する始点ポート番号の設定	156
8.1.13 DHCP サーバーの選択方法の設定	156
8.1.14 DHCP BOOTREQUEST パケットの中継基準の設定	157
8.1.15 インターフェース毎の DHCP の動作の設定	157
8.2 DHCP クライアント機能	158
8.2.1 DHCP クライアントのホスト名の設定	158
8.2.2 要求する IP アドレスリース期間の設定	158
8.2.3 IP アドレス取得要求の再送回数と間隔の設定	159
8.2.4 DHCP クライアント ID オプションの設定	159
8.2.5 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	160
8.2.6 リンクダウンした時に情報を解放するか否かの設定	161

第 9 章 : ICMP の設定162

9.1 IPv4 の設定	162
9.1.1 ICMP Echo Reply を送信するか否かの設定	162

9.1.2 ICMP Echo Reply をリンクダウン時に送信するか否かの設定	162
9.1.3 ICMP Mask Reply を送信するか否かの設定	162
9.1.4 ICMP Parameter Problem を送信するか否かの設定	163
9.1.5 ICMP Redirect を送信するか否かの設定	163
9.1.6 ICMP Redirect 受信時の処理の設定	163
9.1.7 ICMP Time Exceeded を送信するか否かの設定	164
9.1.8 ICMP Timestamp Reply を送信するか否かの設定	164
9.1.9 ICMP Destination Unreachable を送信するか否かの設定	165
9.1.10 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	165
9.1.11 受信した ICMP のログを記録するか否かの設定	166
9.2 IPv6 の設定	166
9.2.1 ICMP Echo Reply を送信するか否かの設定	166
9.2.2 ICMP Echo Reply をリンクダウン時に送信するか否かの設定	166
9.2.3 ICMP Parameter Problem を送信するか否かの設定	167
9.2.4 ICMP Redirect を送信するか否かの設定	167
9.2.5 ICMP Redirect 受信時の処理の設定	167
9.2.6 ICMP Time Exceeded を送信するか否かの設定	168
9.2.7 ICMP Destination Unreachable を送信するか否かの設定	168
9.2.8 受信した ICMP のログを記録するか否かの設定	169
9.2.9 ICMP Packet-Too-Big を送信するか否かの設定	169
9.2.10 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	169

第 10 章：トンネリング171

10.1 トンネルインターフェースの使用許可の設定	171
10.2 トンネルインターフェースの使用不許可の設定	171
10.3 トンネルインタフェースの接続種別の設定	172
10.4 トンネルインタフェースの種別の設定	172
10.5 トンネルインタフェースの IPv4 アドレスの設定	173
10.6 トンネルインタフェースの相手側の IPv4 アドレスの設定	173
10.7 相手側トンネルインタフェースの端点 IP アドレスの設定	173
10.8 自分側トンネルインタフェースの端点 IP アドレスの設定	174
10.9 トンネルインタフェースの端点 IP アドレスの設定	174
10.10 トンネルの端点の名前の設定	175
10.11 マルチポイントトンネルのサーバーの設定	175
10.12 マルチポイントトンネルで使用する自分の名前の設定	176
10.13 マルチポイントトンネルで接続する相手の最大数の設定	176

第 11 章：IPsec の設定177

11.1 IPsec の動作の設定	177
11.2 IKE バージョンの設定	178
11.3 IKE の認証方式の設定	178
11.4 事前共有鍵の登録	179
11.5 IKEv2 の認証に使用する PKI ファイルの設定	180
11.6 EAP-MD5 認証で使用する自分の名前とパスワードの設定	180
11.7 EAP-MD5 によるユーザ認証の設定	181
11.8 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	181
11.9 IKE の鍵交換を始動するか否かの設定	182
11.10 設定が異なる場合に鍵交換を拒否するか否かの設定	182
11.11 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	183
11.12 鍵交換の再送回数と間隔の設定	183
11.13 相手側のセキュリティ・ゲートウェイの名前の設定	184

11.14	相手側セキュリティ・ゲートウェイの IP アドレスの設定	185
11.15	相手側の ID の設定	185
11.16	自分側のセキュリティ・ゲートウェイの名前の設定	186
11.17	自分側セキュリティ・ゲートウェイの IP アドレスの設定	187
11.18	自分側の ID の設定	187
11.19	IKE キープアライブ機能の設定	188
11.20	IKE キープアライブに関する SYSLOG を出力するか否かの設定	189
11.21	IKE が用いる暗号アルゴリズムの設定	190
11.22	受信した IKE パケットを蓄積するキューの長さの設定	191
11.23	IKE が用いるグループの設定	191
11.24	IKE が用いるハッシュアルゴリズムの設定	192
11.25	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	192
11.26	IKE ペイロードのタイプの設定	193
11.27	IKEv1 鍵交換タイプの設定	194
11.28	IKE の情報ペイロードを送信するか否かの設定	194
11.29	PFS を用いるか否かの設定	194
11.30	XAUTH の設定	195
11.31	XAUTH 認証、EAP-MD5 認証に使用するユーザ ID の設定	195
11.32	XAUTH 認証、EAP-MD5 認証に使用するユーザ ID の属性の設定	196
11.33	XAUTH 認証、EAP-MD5 認証に使用するユーザグループの設定	197
11.34	XAUTH 認証、EAP-MD5 認証に使用するユーザグループの属性の設定	197
11.35	XAUTH によるユーザ認証の設定	198
11.36	内部 IP アドレスプールの設定	199
11.37	IKE XAUTH Mode-Cfg メソッドの設定	199
11.38	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	200
11.39	VPN クライアントの同時接続制限ライセンスの登録	200
11.40	VPN クライアントの同時接続制限ライセンスの適用	201
11.41	IKE のログの種類の設定	202
11.42	ESP を UDP でカプセル化して送受信するか否かの設定	202
11.43	折衝パラメーターを制限するか否かの設定	203
11.44	IKE のメッセージ ID 管理の設定	203
11.45	CHILD SA 作成方法の設定	204
11.46	鍵交換の始動パケットを受信するか否かの設定	204
11.47	SA 関連の設定	205
11.47.1	SA の寿命の設定	205
11.47.2	SA のポリシーの定義	206
11.47.3	SA の手動更新	208
11.47.4	ダンダリング SA の動作の設定	208
11.47.5	IPsec NAT トランパースルを利用するための設定	209
11.47.6	SA の削除	210
11.48	トンネルインタフェース関連の設定	210
11.48.1	IPsec トンネルの外側の IPv4 パケットに対するフラグメントの設定	210
11.48.2	IPsec トンネルの外側の IPv4 パケットに対する DF ビットの制御の設定	211
11.48.3	使用する SA のポリシーの設定	211
11.48.4	IPComp によるデータ圧縮の設定	212
11.48.5	トンネルバックアップの設定	212
11.48.6	トンネルテンプレートの設定	213
11.49	トランスポートモード関連の設定	215
11.49.1	トランスポートモードの定義	215

11.49.2	トランスポートモードのテンプレートの設定	215
11.50	PKI 関連の設定	216
11.50.1	証明書ファイルの設定	216
11.50.2	CRL ファイルの設定	217
第 12 章	L2TP 機能の設定	218
12.1	L2TP を動作させるか否かの設定	218
12.2	L2TP トンネル認証に関する設定	218
12.3	L2TP トンネルの切断タイマの設定	219
12.4	L2TP キープアライブの設定	219
12.5	L2TP キープアライブのログ設定	220
12.6	L2TP のコネクション制御の syslog を出力するか否かの設定	220
12.7	L2TPv3 の常時接続の設定	221
12.8	L2TP トンネルのホスト名の設定	221
12.9	L2TPv3 の Local Router ID の設定	221
12.10	L2TPv3 の Remote Router ID の設定	222
12.11	L2TPv3 の Remote End ID の設定	222
12.12	相手先情報番号にバインドされるトンネルインタフェースの設定	222
第 13 章	IPIP トンネリング機能の設定	224
13.1	IPIP キープアライブの設定	224
13.2	IPIP キープアライブのログ設定	224
第 14 章	SIP 機能の設定	226
14.1	共通の設定	226
14.1.1	SIP を使用するか否かの設定	226
14.1.2	SIP の session-timer 機能のタイマ値の設定	226
14.1.3	SIP による発信時に使用する IP プロトコルの選択	227
14.1.4	SIP による発信時に 100rel をサポートするか否かの設定	227
14.1.5	送信する SIP パケットに User-Agent ヘッダを付加する設定	228
14.1.6	SIP による着信時の INVITE に refresher 指定がない場合の設定	228
14.1.7	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	228
14.1.8	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	229
14.1.9	SIP 着信時にユーザー名を検証するか否かの設定	229
14.1.10	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	230
14.1.11	SIP で使用する IP アドレスの設定	230
14.1.12	SIP メッセージのログを記録するか否かの設定	230
14.2	NGN 機能の設定	231
14.2.1	NGN 網に接続するインタフェースの設定	231
14.2.2	NGN 網を介したトンネルインタフェースの切断タイマの設定	231
14.2.3	NGN 網を介したトンネルインタフェースの帯域幅の設定	231
14.2.4	NGN 網を介したトンネルインタフェースの着信許可の設定	232
14.2.5	NGN 網を介したトンネルインタフェースの発信許可の設定	232
14.2.6	NGN 網を介したトンネルインタフェースで使用する LAN インタフェースの設定	233
14.2.7	NGN 網を介したトンネルインタフェースで接続に失敗した場合に接続を試みる相手番号の設定	233
14.2.8	NGN 電話番号を RADIUS で認証するか否かの設定	234
14.2.9	NGN 電話番号を RADIUS で認証するとき使用するパスワードの設定	234
14.2.10	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	234
14.2.11	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	235

14.2.12 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	235
14.2.13 NGN 網接続情報の表示	236
第 15 章 : SNMP の設定	237
15.1 SNMPv1 によるアクセスを許可するホストの設定	237
15.2 SNMPv1 の読み出し専用のコミュニティ名の設定	238
15.3 SNMPv1 の読み書き可能なコミュニティ名の設定	238
15.4 SNMPv1 トラップの送信先の設定	238
15.5 SNMPv1 トラップのコミュニティ名の設定	238
15.6 SNMPv2c によるアクセスを許可するホストの設定	239
15.7 SNMPv2c の読み出し専用のコミュニティ名の設定	239
15.8 SNMPv2c の読み書き可能なコミュニティ名の設定	240
15.9 SNMPv2c トラップの送信先の設定	240
15.10 SNMPv2c トラップのコミュニティ名の設定	240
15.11 SNMPv3 エンジン ID の設定	241
15.12 SNMPv3 コンテキスト名の設定	241
15.13 SNMPv3 USM で管理するユーザの設定	241
15.14 SNMPv3 によるアクセスを許可するホストの設定	242
15.15 SNMPv3 VACM で管理する MIB ビューファミリの設定	243
15.16 SNMPv3 VACM で管理するアクセスポリシーの設定	243
15.17 SNMPv3 トラップの送信先の設定	244
15.18 SNMP 送信パケットの始点アドレスの設定	244
15.19 sysContact の設定	244
15.20 sysLocation の設定	245
15.21 sysName の設定	245
15.22 SNMP 標準トラップを送信するか否かの設定	246
15.23 CPU 使用率監視機能による SNMP トラップを送信するか否かの設定	246
15.24 メモリ使用率監視機能による SNMP トラップを送信するか否かの設定	247
15.25 SNMP トラップの送信の遅延時間の設定	247
15.26 SNMP の linkDown トラップの送信制御の設定	247
15.27 PP インタフェースの情報を MIB2 の範囲で表示するか否かの設定	248
15.28 トンネルインタフェースの情報を MIB2 の範囲で表示するか否かの設定	248
15.29 PP インタフェースのアドレスの強制表示の設定	249
第 16 章 : RADIUS の設定	250
16.1 RADIUS による認証を使用するか否かの設定	250
16.2 RADIUS によるアカウントを使用するか否かの設定	250
16.3 RADIUS サーバーの指定	251
16.4 RADIUS 認証サーバーの指定	251
16.5 RADIUS アカウントサーバーの指定	251
16.6 RADIUS 認証サーバーの UDP ポートの設定	252
16.7 RADIUS アカウントサーバーの UDP ポートの設定	252
16.8 RADIUS シークレットの設定	252
16.9 RADIUS 再送信パラメータの設定	253
第 17 章 : NAT 機能	254
17.1 NAT 機能の動作タイプの設定	254
17.2 インタフェースへの NAT ディスクリプタ適用の設定	254
17.3 NAT ディスクリプタの動作タイプの設定	255
17.4 NAT 処理の外側 IP アドレスの設定	255

17.5 NAT 処理の内側 IP アドレスの設定	256
17.6 静的 NAT エントリの設定	257
17.7 IP マスカレード使用時に rlogin,rcp と ssh を使用するか否かの設定	257
17.8 静的 IP マスカレードエントリの設定	258
17.9 NAT の IP アドレスマップの消去タイマの設定	259
17.10 外側から受信したパケットに該当する変換テーブルが存在しないときの動作の設定	259
17.11 IP マスカレードで利用するポートの範囲の設定	260
17.12 FTP として認識するポート番号の設定	260
17.13 IP マスカレードで変換しないポート番号の範囲の設定	261
17.14 NAT のアドレス割当をログに記録するか否かの設定	261
17.15 SIP メッセージに含まれる IP アドレスを書き換えるか否かの設定	261
17.16 IP マスカレード変換時に DF ビットを削除するか否かの設定	262
17.17 IP マスカレードで変換するホスト毎のセッション数の設定	262
17.18 IP マスカレードで変換する合計セッション数の設定	263
第 18 章 : DNS の設定	264
18.1 DNS を利用するか否かの設定	264
18.2 DNS サーバーの IP アドレスの設定	264
18.3 DNS ドメイン名の設定	265
18.4 DNS サーバーを通知してもらう相手先情報番号の設定	265
18.5 DNS サーバーアドレスを取得するインタフェースの設定	266
18.6 DHCP/PCP MS 拡張で DNS サーバーを通知する順序の設定	267
18.7 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	267
18.8 DNS サーバーへの AAAA レコードの問い合わせを制限するか否かの設定	268
18.9 SYSLOG 表示で DNS により名前解決するか否かの設定	268
18.10 DNS 問い合わせの内容に応じた DNS サーバーの選択	268
18.11 静的 DNS レコードの登録	270
18.12 DNS 問い合わせパケットの始点ポート番号の設定	271
18.13 DNS サーバーへアクセスできるホストの設定	272
18.14 DNS キャッシュを使用するか否かの設定	272
18.15 DNS キャッシュの最大エントリ数の設定	273
18.16 DNS フォールバック動作をルーター全体で統一するか否かの設定	273
第 19 章 : 優先制御 / 帯域制御	275
19.1 インタフェース速度の設定	275
19.2 クラス分けのためのフィルター設定	275
19.3 キューイングアルゴリズムタイプの選択	278
19.4 クラス分けフィルタの適用	278
19.5 クラス毎のキュー長の設定	279
19.6 デフォルトクラスの設定	279
19.7 クラスの属性の設定	280
19.8 動的なクラス変更 (Dynamic Class Control) の設定	281
第 20 章 : OSPF	283
20.1 OSPF の有効設定	283
20.2 OSPF の使用設定	283
20.3 OSPF による経路の優先度設定	283
20.4 OSPF のルーター ID 設定	284
20.5 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	284
20.6 外部プロトコルによる経路導入	284
20.7 OSPF で受け取った経路をどう扱うかのフィルタの設定	285

20.8 外部経路導入に適用するフィルタ定義	286
20.9 OSPF エリア設定	288
20.10 エリアへの経路広告	289
20.11 スタブ的接続の広告	289
20.12 仮想リンク設定	290
20.13 指定インタフェースの OSPF エリア設定	291
20.14 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	294
20.15 スタブが存在する時のネットワーク経路の扱いの設定	294
20.16 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	295
20.17 インタフェースの状態変化時、OSPF に外部経路を反映させる時間間隔の設定	295
第 21 章 : BGP	297
21.1 BGP の起動の設定	297
21.2 経路の集約の設定	297
21.3 経路を集約するためのフィルタの設定	297
21.4 AS 番号の設定	298
21.5 ルーター ID の設定	298
21.6 BGP による経路の優先度の設定	299
21.7 BGP で受信した経路に対するフィルタの適用	299
21.8 BGP で受信する経路に適用するフィルタの設定	300
21.9 BGP に導入する経路に対するフィルタの適用	301
21.10 BGP の設定の有効化	302
21.11 BGP に導入する経路に適用するフィルタの設定	302
21.12 BGP による接続先の設定	303
21.13 BGP のログの設定	304
21.14 BGP で強制的に経路を広告する	304
21.15 インタフェースの状態変化時、BGP に外部経路を反映させる時間間隔の設定	305
21.16 BGP の最適経路選択における MED 属性が付加されていない経路のデフォルトの MED 値 の設定	305
第 22 章 : IPv6	307
22.1 共通の設定	307
22.1.1 IPv6 パケットを扱うか否かの設定	307
22.1.2 IPv6 インタフェースのリンク MTU の設定	307
22.1.3 TCP セッションの MSS 制限の設定	307
22.1.4 TCP ウィンドウ・スケール・オプションを変更する	308
22.1.5 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	309
22.1.6 IPv6 ファストパス機能の設定	309
22.1.7 ICMPv6 でアドレス解決が完了するまでに送信を保留しておくことのできるパケッ ト数の設定	309
22.1.8 近隣キャッシュの最大エントリ数の設定	310
22.1.9 IPv6 のフラグメントパケットを再構成するために保持しておく時間を設定	310
22.2 IPv6 アドレスの管理	310
22.2.1 インタフェースの IPv6 アドレスの設定	310
22.2.2 インタフェースのプレフィックスに基づく IPv6 アドレスの設定	312
22.2.3 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	314
22.2.4 DHCPv6 の動作の設定	314
22.2.5 DAD(Duplicate Address Detection) の送信回数数の設定	315
22.2.6 自動的に設定される IPv6 アドレスの最大数の設定	315
22.2.7 始点 IPv6 アドレスを選択する規則の設定	316
22.3 近隣探索	316

22.3.1 ルーター広告で配布するプレフィックスの定義	316
22.3.2 ルーター広告の送信の制御	318
22.3.3 ルーター要請の再送機能の設定	319
22.4 経路制御	320
22.4.1 IPv6 の経路情報の追加	320
22.5 RIPng	321
22.5.1 RIPng の使用の設定	321
22.5.2 インタフェースにおける RIPng の送信ポリシーの設定	321
22.5.3 インタフェースにおける RIPng の受信ポリシーの設定	321
22.5.4 RIPng の加算ホップ数の設定	322
22.5.5 インタフェースにおける信頼できる RIPng ゲートウェイの設定	322
22.5.6 RIPng で送受信する経路に対するフィルタリングの設定	323
22.5.7 回線接続時の PP 側の RIPng の動作の設定	323
22.5.8 回線接続時の PP 側の RIPng 送出の時間間隔の設定	324
22.5.9 回線切断時の PP 側の RIPng の動作の設定	324
22.5.10 回線切断時の PP 側の RIPng 送出の時間間隔の設定	325
22.5.11 RIPng による経路を回線切断時に保持するか否かの設定	325
22.5.12 RIPng による経路の優先度の設定	325
22.6 VRRPv3 の設定	326
22.6.1 インタフェース毎の VRRPv3 の設定	326
22.6.2 シャットダウントリガの設定	327
22.7 フィルタの設定	328
22.7.1 IPv6 フィルタの定義	328
22.7.2 IPv6 フィルタの適用	329
22.7.3 IPv6 動的フィルタの定義	330
22.8 近隣要請	331
22.8.1 アドレス重複チェックをトリガに近隣要請を行うか否かの設定	331
第 23 章：トリガによるメール通知機能	332
23.1 メール設定識別名の設定	332
23.2 SMTP メールサーバーの設定	332
23.3 POP メールサーバーの設定	333
23.4 メール処理のタイムアウト値の設定	334
23.5 メールの送信時に使用するテンプレートの設定	334
23.6 メール通知のトリガの設定	335
第 24 章：スケジュール	338
24.1 スケジュールの設定	338
第 25 章：生存通知機能	340
25.1 生存通知の共有鍵の設定	340
25.2 生存通知を受信するか否かの設定	340
25.3 生存通知の実行	341
第 26 章：生存通知機能 リリース 2	342
26.1 通知名称の設定	342
26.2 通知設定の定義	342
26.3 通知設定の有効化	343
26.4 通知間隔の設定	343
26.5 通知を送信した際にログを記録するか否かの設定	344
26.6 受信設定の定義	344
26.7 受信設定の有効化	345

26.8 受信間隔の監視設定	345
26.9 通知を受信した際にログを記録するか否かの設定	345
26.10 同時に保持できる生存情報の最大数の設定	346
26.11 生存通知の状態の表示	346
26.12 生存通知の状態のクリア	347
第 27 章 : SNTP サーバー機能	348
27.1 SNTP サーバー機能を有効にするか否かの設定	348
27.2 SNTP サーバーへのアクセスを許可するホストの設定	348
第 28 章 : ブリッジインタフェース (ブリッジ機能)	350
28.1 ブリッジインタフェースに収容するインタフェースを設定する	350
28.2 自動的なラーニングを行うか否かの設定	351
28.3 ブリッジがラーニングした情報の消去タイマーの設定	351
28.4 静的なラーニング情報の設定	352
第 29 章 : Lua スクリプト機能	353
29.1 Lua スクリプト機能を有効にするか否かの設定	353
29.2 Lua スクリプトの実行	353
29.3 Lua コンパイラの実行	354
29.4 Lua スクリプトの走行状態の表示	354
29.5 Lua スクリプトの強制終了	355
第 30 章 : 操作	356
30.1 相手先情報番号の選択	356
30.2 トンネルインタフェース番号の選択	356
30.3 設定に関する操作	357
30.3.1 管理ユーザへの移行	357
30.3.2 終了	357
30.3.3 設定内容の保存	357
30.3.4 設定ファイルの複製	357
30.3.5 設定ファイルの削除	358
30.3.6 デフォルト設定ファイルの設定	359
30.3.7 設定の初期化	359
30.3.8 遠隔地のルーターからの設定に対する制限	359
30.4 動的情報のクリア操作	360
30.4.1 アカウントのクリア	360
30.4.2 PP アカウントのクリア	360
30.4.3 TUNNEL アカウントのクリア	360
30.4.4 データコネクタのアカウントのクリア	360
30.4.5 ARP テーブルのクリア	360
30.4.6 IP の動的経路情報のクリア	361
30.4.7 ブリッジのラーニング情報のクリア	361
30.4.8 ログのクリア	361
30.4.9 DNS キャッシュのクリア	361
30.4.10 インタフェースのカウンター情報のクリア	361
30.4.11 NAT アドレステーブルのクリア	362
30.4.12 インタフェースの NAT アドレステーブルのクリア	362
30.4.13 IP マスカレードで管理しているセッションの統計情報のクリア	363
30.4.14 IPv6 の動的経路情報の消去	363
30.4.15 近隣キャッシュの消去	363
30.4.16 起動情報の履歴を削除する	363

30.5	ファイル、ディレクトリの操作	363
30.5.1	ディレクトリの作成	363
30.5.2	ファイルまたはディレクトリの削除	364
30.5.3	ファイルまたはディレクトリの複製	364
30.5.4	ファイル名またはディレクトリ名の変更	365
30.6	外部ストレージの操作	365
30.6.1	外部ストレージをマウントする	365
30.6.2	外部ストレージをアンマウントする	366
30.7	その他の操作	367
30.7.1	相手先の使用許可の設定	367
30.7.2	相手先の使用不許可の設定	367
30.7.3	再起動	368
30.7.4	電源オフ	368
30.7.5	インタフェースの再起動	368
30.7.6	発信	368
30.7.7	切断	369
30.7.8	ping	369
30.7.9	ping6 の実行	370
30.7.10	traceroute	371
30.7.11	traceroute6 の実行	371
30.7.12	nslookup	372
30.7.13	IPv4 動的フィルタのコネクション管理情報の削除	372
30.7.14	TELNET クライアント	372
30.7.15	IPv6 動的フィルタのコネクション管理情報の削除	373
30.7.16	Magic Packet の送信	373
30.7.17	メール通知の実行	374
30.7.18	設定の一括更新	375
30.7.19	ロールバックタイマーの起動	376
30.7.20	設定の確認	376
30.7.21	ファイルをマクロとして実行する	376
30.7.22	echo	377
第 31 章	設定の表示	378
31.1	機器設定の表示	378
31.2	すべての設定内容の表示	378
31.3	指定した PP の設定内容の表示	378
31.4	指定したトンネルの設定内容の表示	379
31.5	設定の差分の表示	379
31.6	設定ファイルの一覧	380
31.7	ファイル情報の一覧の表示	380
31.8	インタフェースに付与されている IPv6 アドレスの表示	381
31.9	指定したインタフェースのフィルタ内容の表示	381
31.10	指定したインターフェースの IPv6 フィルター内容の表示	381
31.11	環境変数の表示	382
31.12	エイリアスの表示	382
31.13	マクロの表示	382
第 32 章	状態の表示	384
32.1	ARP テーブルの表示	384
32.2	インタフェースの状態の表示	384
32.3	各相手先の状態の表示	384

32.4 IP の経路情報テーブルの表示	385
32.5 RIP で得られた経路情報の表示	386
32.6 IPv6 の経路情報の表示	386
32.7 IPv6 の RIP テーブルの表示	386
32.8 近隣キャッシュの表示	386
32.9 ブリッジのラーニング情報の表示	386
32.10 IPsec の SA の表示	387
32.11 証明書の情報の表示	387
32.12 CRL ファイルの情報の表示	388
32.13 VRRP の情報の表示	388
32.14 動的 NAT ディスクリプタのアドレスマップの表示	388
32.15 動作中の NAT ディスクリプタの適用リストの表示	389
32.16 LAN インタフェースの NAT ディスクリプタのアドレスマップの表示	389
32.17 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	390
32.18 IP マスカレードで使用しているセッション数の表示	390
32.19 IP マスカレードで管理しているセッションの統計情報の表示	390
32.20 L2TP の状態の表示	391
32.21 IPIP トンネリングの状態の表示	391
32.22 OSPF 情報の表示	391
32.23 BGP の状態の表示	391
32.24 DHCP サーバーの状態の表示	392
32.25 DHCP クライアントの状態の表示	392
32.26 DHCPv6 の状態の表示	393
32.27 バックアップ状態の表示	393
32.28 動的フィルタによって管理されているコネクションの表示	393
32.29 IPv6 の動的フィルタによって管理されているコネクションの表示	394
32.30 ネットワーク監視機能の状態の表示	395
32.31 侵入情報の履歴の表示	395
32.32 トンネルインタフェースの状態の表示	395
32.33 トリガによるメール通知機能の状態の表示	396
32.34 ルーターにマウントされている外部ストレージの一覧を表示する	396
32.35 ログインしているユーザー情報の表示	397
32.36 ログインしたユーザーのログイン履歴の表示	397
32.37 パケットバッファの状態の表示	398
32.38 QoS ステータスの表示	398
32.39 生存通知の状態の表示	399
32.40 技術情報の表示	399
32.41 起動情報を表示する	400
32.42 起動情報の履歴の詳細を表示する	400
32.43 起動情報の履歴の一覧を表示する	400
32.44 DNS キャッシュの表示	400
32.45 ライセンス情報の表示	401
32.46 CPU スケジューリング (パケット転送) 機能の状態の表示	402
32.47 サードパーティー製ソフトウェアの著作権情報を表示	402
32.48 サードパーティー製ソフトウェアに適用される一般的なライセンスの条文を表示	403
第 33 章 : ログイン	405
33.1 ログの表示	405
33.2 アカウントの表示	405
33.3 PP アカウントの表示	406

33.4 TUNNEL アカウントの表示	406
33.5 データコネクトのアカウントの表示	406
33.6 コマンド履歴の表示	406

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

第 1 章

コマンドリファレンスの見方

1.1 対応するプログラムのリビジョン

このコマンドリファレンスは、ヤマハルーターのリビジョン、Rev.19.00.08, Rev.19.01.06 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リビジョンや、マニュアル類および差分については以下に示す URL の WWW サーバーにある情報を参照してください。

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

1.2 コマンドリファレンスの見方

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

1 つ 1 つのコマンドは次の項目の組合せで説明します。

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

1.3 インタフェース名について

コマンドの入力形式において、ルーターの各インタフェースを指定するためにインタフェース名を利用します。インタフェース名は、インタフェース種別とインタフェース番号を間に空白をおかずに続けて表記します。インタフェース種別には、"lan" があります。インタフェース番号は、インタフェースの種別ごとに起動時に検出された順番で振られていきます。

例

インタフェースの種類	インタフェース名
LAN	lan1

また、仮想的なインタフェースである loopback インタフェースと null インタフェースを指定できます。

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

vRX VMware ESXi 版では仮想的なインタフェースであるブリッジインタフェースを指定できます。

インタフェースの種類	インタフェース名
BRIDGE	bridge1

1.4 no で始まるコマンドの入力形式について

コマンドの入力形式に **no** で始まる形のものがあり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 デプロイ時の設定値について

vRX Amazon EC2 版では、デプロイ時の状態および **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、以下に示すデプロイ時の設定になっています。

```
ip route default gateway dhcp lan2
ip lan1 address dhcp
ip lan2 address dhcp
telnetd service off
dns server dhcp lan2
sshd service on
sshd host key generate *
```

vRX VMware ESXi 版では、デプロイ時に「テンプレートのカスタマイズ」によりデプロイ直後の設定を変更できますが、この変更を行わなかった場合のデプロイ時の状態および **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。

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

各種設定を行うには、ハイパーバイザーの管理ソフトウェアが提供しているコンソール機能(仮想マシンコンソール)からログインする方法と、ヤマハルーターのネットワーク上のホストから TELNET、または SSH でログインする方法があります。

ヤマハルーターへのアクセス方法
仮想マシンコンソールでログイン (vRX VMware ESXi 版で使用可能)
ネットワーク上のホストから TELNET または SSH でログイン

TELNET または SSH による同時アクセスは最大 8 ユーザまで可能です。また複数のユーザが同時に管理ユーザになることができ、異なるホストから同時に設定を行うこともできます。そのほか、各ユーザは現在アクセスしている全ユーザのアクセス状況を確認することができ、管理ユーザならば他のユーザの接続を強制的に切断させることもできます。

2.1.1 コンソールによる設定手順

仮想マシンコンソールで設定を行う場合は、vRX を実行しているハイパーバイザーの管理ソフトウェアが提供しているコンソール機能を使用します。

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

SSH で設定を行う場合は、パソコンでは SSH 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『SSH』ソフトウェアまたは SSH クライアント機能のあるフリーソフトなどを使用します。macOS をお使いの場合は、OS に付属の『ターミナル』アプリケーションで `ssh` 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 UTF-8 です。これは、`console character` コマンドを使用して端末の文字表示の能力に応じて選択できます。いずれの場合でもコマンドの入力文字は ASCII で共通であることに注意してください。

設定手順のおおまかな流れは次のようになります。

1. 一般ユーザとしてログインした後、`administrator` コマンドで管理ユーザとしてアクセスします。この時管理パスワードが設定してあれば、管理パスワードの入力が必要です。
2. 各種機能のコマンドを使用して、設定内容を変更します。
3. `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。

セキュリティの観点から、コンソールにキー入力がない時には、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。

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

-  **注意:** ご購入直後の起動や `cold start` 後にはログインパスワードも管理パスワードも設定されていません。セキュリティ上、ログインパスワードと管理パスワードの設定をお勧めします。
- ヤマハルーターのご購入直後の起動でコンソールから各種の設定が行える状態になりますが、実際にパケットを配送する動作は行いません。

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

2.1.2 仮想マシンコンソールによる設定

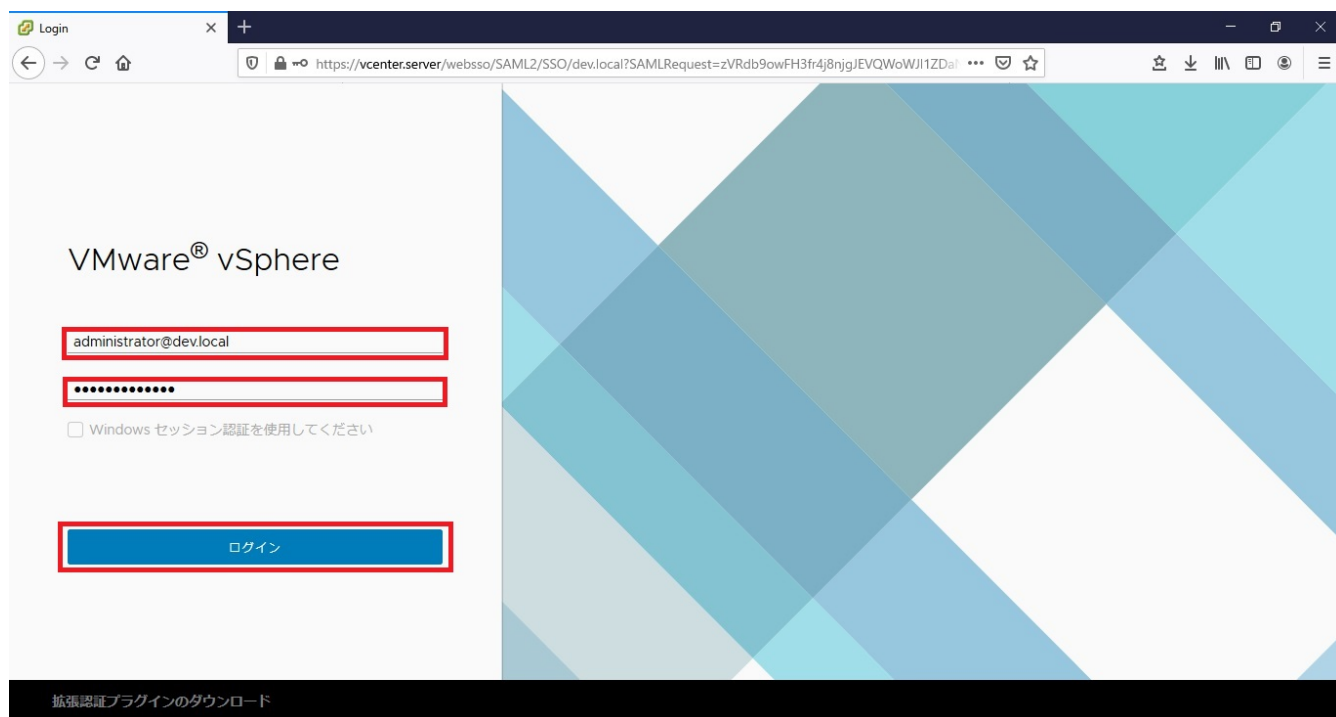
仮想マシンコンソールによる設定手順の一例を説明します。仮想マシンコンソールは vRX VMware ESXi 版で使用可能です。ここでは、仮想マシンコンソールとして vSphere Client の Web コンソールを使用します。

以下の条件を例に説明します。

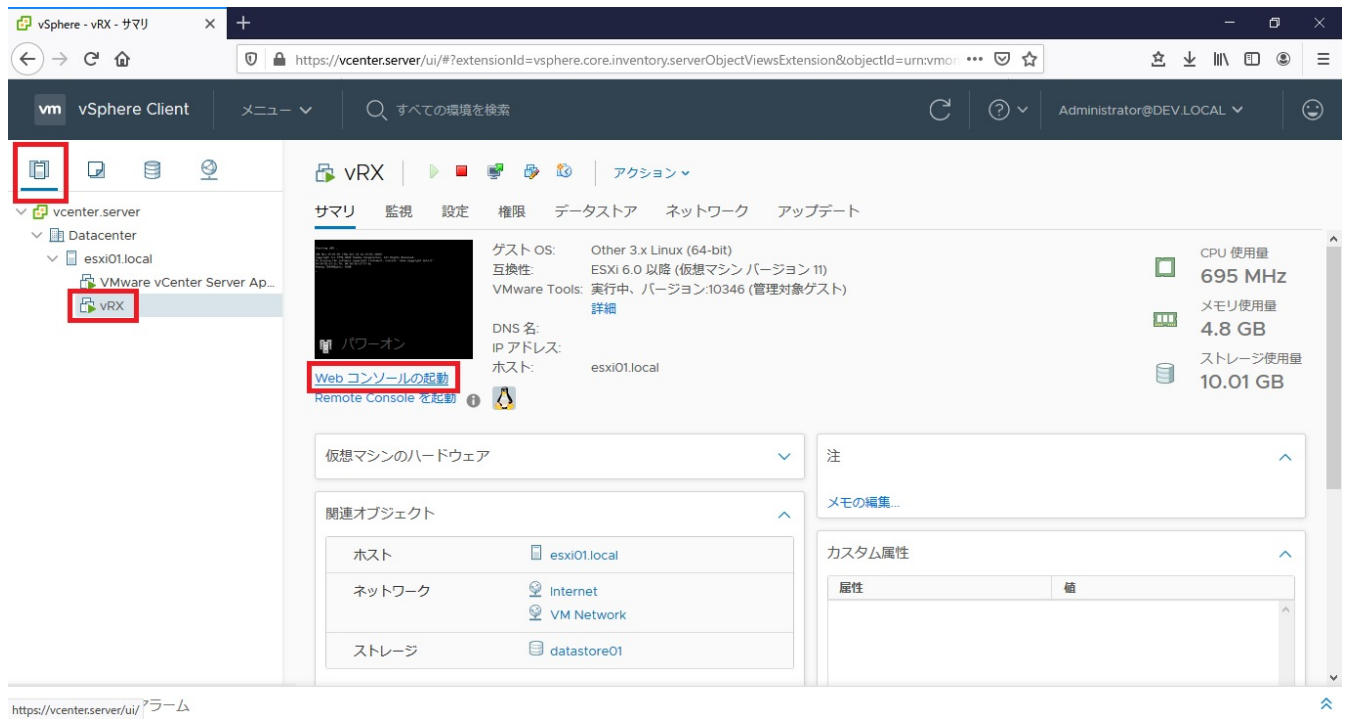
- vRX は、VMware ESXi へデプロイし、起動まで済んでいる。
 - vCenter Server はインストール済みで、デプロイした vRX は管理対象となっている。
1. Web ブラウザを開き、VMware Vsphere を起動します。
 2. ログイン画面が表示されたら、ID@ドメインとパスワードを入力してからログインを押します。

画像の ID、ドメイン、パスワードは入力例です。

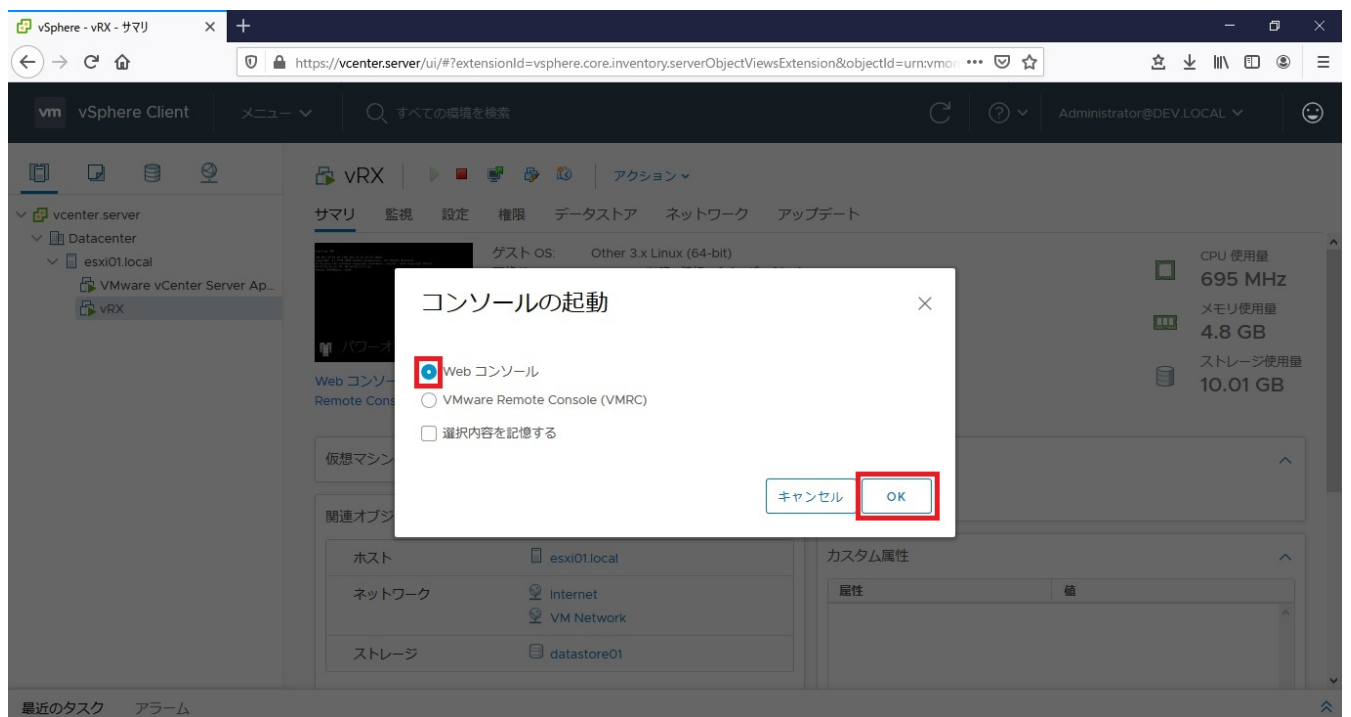
実際は接続先の vCenter Server に対して権限があるユーザーの認証情報をご使用ください。



3. 「ホストおよびクラスタ」画面からデプロイ済みの vRX を選択し、「Web コンソールの起動」を選択します。



4. 「コンソールの起動」ポップアップが表示されるため、「Web コンソール」にチェック後、OK を押します。



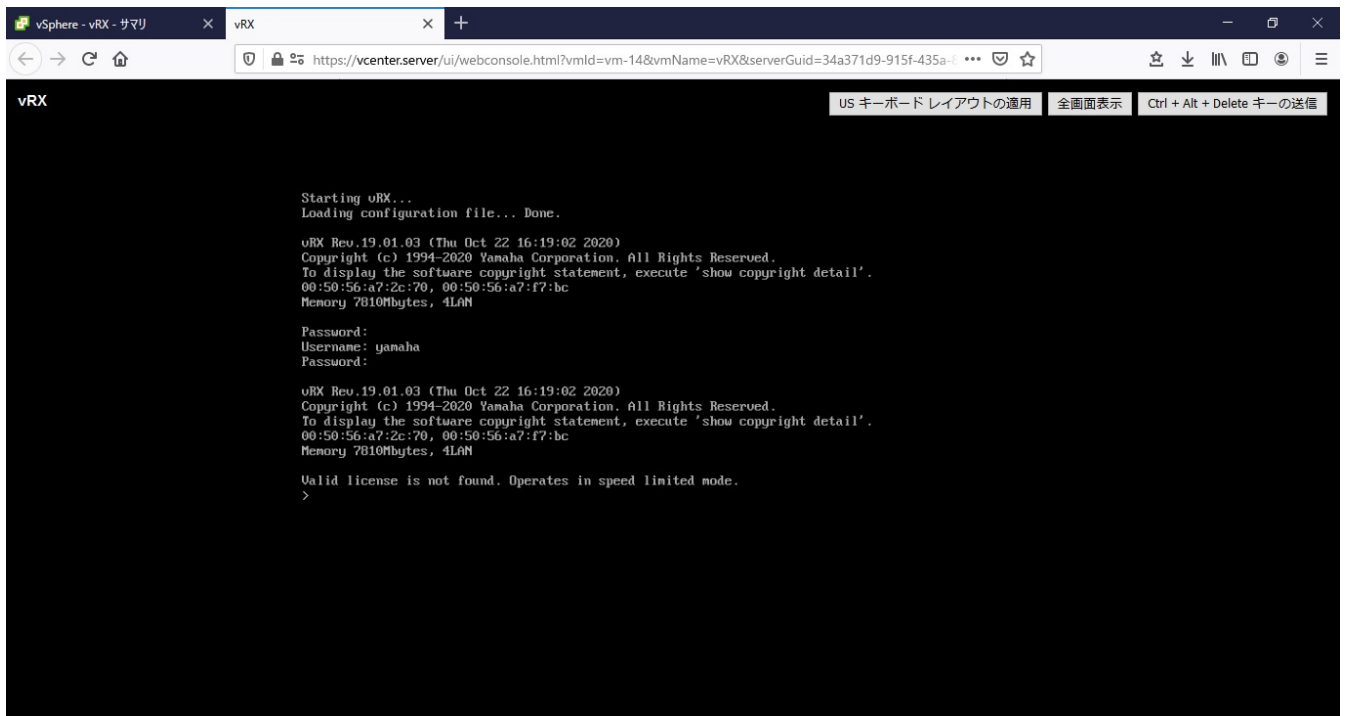
注:

- VMware Remote Console を利用するには別途インストールが必要です。

5. 「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。

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

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



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。

6. **administrator** と入力してから、Enter キーを押します。
7. 「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。
8. コンソールコマンドを入力して、設定を行います
9. 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。
10. 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。
11. 仮想マシンコンソールでの操作を終了するには、もう 1 度 **quit** と入力してから Enter キーを押します。

2.1.3 TELNET による設定

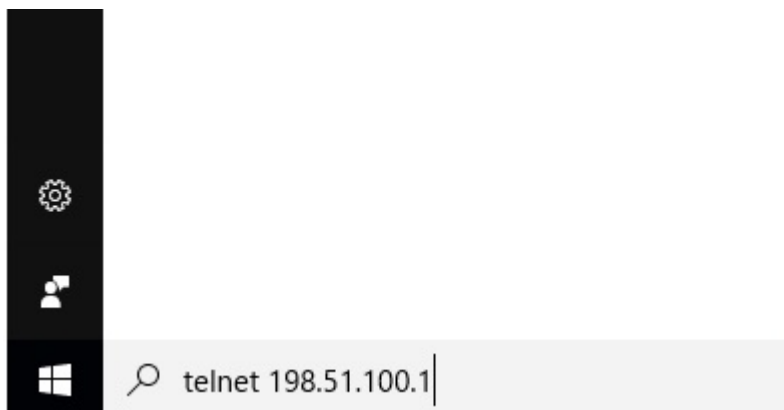
ここでは、Windows の TELNET を使用する場合を例に説明します。ヤマハルーターの IP アドレスは 198.51.100.1 とした場合の例です。

TELNET には暗号化機能がないためセキュリティの観点から VPN 上で使用することを推奨します。VPN 構築以前は SSH による設定をご利用ください。

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

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

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



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

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

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

```

Telnet 198.51.100.1
Password:
Username: yamaha
Password:

vRX Rev.19.00.01 (Fri Sep 13 12:13:56 2019) ** Compact Mode **
Copyright (c) 1994-2019 Yamaha Corporation. All Rights Reserved.
To display the software copyright statement, execute 'show copyright detail'.
00:50:56:92:6b:a7, 00:50:56:92:01:f1
Memory 3787Mbytes, 4LAN
> administrator
Password:
The administrator password is factory default setting. Please change the password by the
'administrator password' command.
#
# quit
>

```

注:

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

3. **administrator** と入力してから、Enter キーを押します。
4. 「Password:」と表示されたら、管理パスワードを入力します。
「#」が表示されると、各種のコンソールコマンドを入力できます。
5. コンソールコマンドを入力して、設定を行います
6. 設定が終わったら、**save** と入力してから Enter キーを押します。
コンソールコマンドで設定した内容が、本機の不揮発性メモリに保存されます。
7. 設定を終了するには、**quit** と入力してから Enter キーを押します。
8. コンソール画面を終了するには、もう1度 **quit** と入力してから Enter キーを押します。

2.1.4 SSH による設定

ここでは、Windows の SSH を使用する場合を例に説明します。ヤマハルーターに設定されているユーザ名は yamaha、IP アドレスは 198.51.100.1 とした場合の例です。

1. [スタート]メニューから「ssh yamaha@198.51.100.1」と入力します。
実際には「yamaha@198.51.100.1」のかわりに本機に設定されているユーザ名@IP アドレスと入力します。



- 「Are you sure you want to continue connecting (yes/no)?」と表示されたら、「yes」と入力してから Enter キーを押します。
「yamaha@198.51.100.1's 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。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。

```

OpenSSH SSH client
The authenticity of host '198.51.100.1 (198.51.100.1)' can't be established.
RSA key fingerprint is SHA256:eVvHM2yrjKxEFIPgn9Iplqq99nfZBxMMWotCjpoKdBEY.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '198.51.100.1' (RSA) to the list of known hosts.
yamaha@198.51.100.1's password:

vRX Rev.19.00.01 (Fri Sep 13 12:13:56 2019) ** Compact Mode **
Copyright (c) 1994-2019 Yamaha Corporation. All Rights Reserved.
To display the software copyright statement, execute 'show copyright detail'.
00:50:56:92:6b:a7, 00:50:56:92:01:f1
Memory 3787Mbytes, 4LAN
> administrator
Password:
The administrator password is factory default setting. Please change the password by
the 'administrator password' command.
#
# quit
>

```

👉 注:

- **help** と入力してから Enter キーを押すと、キー操作の説明が表示されます。
 - **show command** と入力してから Enter キーを押すと、コマンド一覧が表示されます。
- administrator** と入力してから、Enter キーを押します。
 - 「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。
 - コンソールコマンドを入力して、設定を行います
 - 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。
 - 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。
 - 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

ネットワーク上のホストから SSH でログインして設定することができます。このときホスト側で使用する SSH クライアントは、macOS の『ターミナル』アプリケーションや UNIX 環境では標準的に搭載されており、実行するこ

とができますが、Windows 系 OS では Windows 10 の version 1803 以前では標準で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、および、公開鍵認証以外のユーザ認証 (ホストベース認証、チャレンジ・レスポンス認証、GSSAPI 認証)
- 二段階認証 (たとえば、パスワード認証と公開鍵認証を併用して公開鍵認証後にパスワード認証を実施)
- ポートフォワーディング (X11/TCP 転送)
- Gateway Ports (ポート中継)
- 空パスワードの許可
- scp

2.2.2 SSH サーバーの設定

SSH サーバー機能は、デプロイ時の設定では公開鍵認証によるユーザー認証方式で使用できるよう設定されています。

1. SSH クライアントの秘密鍵として、EC の設定時に選択したキーペアまたは作成したキーペアのプライベートキーファイルを指定してください。

また、名前ありユーザで 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要となるため、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。
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。

```

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

```

2.3 TFTP について

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

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

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

TFTP では、平文の設定ファイルと暗号化された設定ファイルを扱うことができます。対応している暗号化形式は、

AES128 及び、AES256 です。パスワードを指定して暗号化されたファイルは利用できません。RT-Tftp Client では暗号化に対応していません。



注意:

- 設定ファイルの内容はコマンドの書式やパラメータの指定などの内容が正しく記述されている必要があります。間違った書式や内容があった場合には、その内容は動作に反映されず無視されます。
- TFTP により設定ファイルを読み込む場合において **system packet-scheduling** コマンドのように再起動が必要な設定変更を行う場合は、設定の最後に **restart** コマンドが必要なことに注意してください。

2.3.1 TFTP による設定手順

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

```

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

```

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

- 本機の IP アドレス
- 転送モードは“アスキー”、“ascii”または“文字”にします。
暗号化された設定ファイルを扱う場合は“バイナリ”、“binary”にします。
- 本機に管理パスワードが設定されている場合には、ファイル名称の後ろに管理パスワードを指定する必要があります。
- 起動中の設定ファイルを読み出したり書き込んだりする場合は、設定ファイル名は、“config”と指定します。

2.3.2 設定ファイルの読み出し

ここでは、Windows から設定ファイルを読み出す場合の例を示します。ヤマハルーターのコンソール操作ではないことに注意してください。この例では、ヤマハルーターの IP アドレスを 198.51.100.1、管理パスワードは“himitsu”、Windows に新しくできるファイルの名称を“OLDconfig.txt”とします。

1. [スタート]メニューから[Windows システム ツール]-[コマンドプロンプト]を選びます。
2. 設定ファイルを保存するディレクトリに移動します。
3. **tftp 198.51.100.1 get config/himitsu OLDconfig.txt** と入力してから、Enter キーを押します。

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

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

と入力してから、Enter キーを押します


```

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

```

2.3.3 設定ファイルの書き込み

ここでは、Windows から設定ファイルを書き込む場合の例を示します。ヤマハルーターのコンソール操作ではないことに注意してください。この例では、ヤマハルーターの IP アドレスを 198.51.100.1、管理パスワードは“himitsu”、書き込むべき Windows 上のファイルの名称を“NEWconfig.txt”とします。

1. [スタート]メニューから[Windows システム ツール]-[コマンドプロンプト]を選びます。
2. 設定ファイルを保存するディレクトリに移動します。
3. **tftp 198.51.100.1 put NEWconfig.txt config/himitsu** と入力してから、Enter キーを押します。

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

tftp -i 198.51.100.1 put NEWconfig.rtf config/himitsu

と入力してから、Enter キーを押します。

```

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

```

2.4 コンソール使用時のキーボード操作について

restart コマンドで本製品を再起動する他に、Ctrl+Alt+Del の入力によって再起動することが出来ます。

キーボード操作	説明・備考
Ctrl-Alt-Del	再起動

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

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

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

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

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

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

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

説明：

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

2.5 「show」で始まるコマンド

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

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

[書式]

```
show [...] | grep [-i] [-v] [-w] pattern
```

[設定値及び初期値]

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

[説明]

show コマンドの表示内容から検索パターンである *pattern* に一致する行だけを抜き出して表示する。

-i オプションを指定した時には、*pattern* 中の英大文字 / 小文字を区別せずに検索する。例えば -i オプションがある時には 'abc' という *pattern* は 'abc' や 'ABC'、'aBc'、'ABc' などと一致する。一方、-i オプションがなければ、'abc' は 'abc' としか一致しない。

-v オプションを指定した時には、*pattern* に一致しない行を表示する。

-w オプションを指定した時には、*pattern* に一致するのは単語だけとなる。例えば、-w オプションがある時には 'IP' という *pattern* は 'IPv4' や 'IPv6' とは一致しないが、'IP' (前後に空白がある) や '[IP]' には一致する。一方、-w オプションが無ければ先に上げた例にはすべて一致する。

pattern は限定された正規表現である。一般的な正規表現では多くの特殊文字を使って多様な検索パターンを構成できるが、ここで実装されているのは以下の特殊文字のみである。

文字	意味	使用例	一致する文字列の例
.	任意の 1 文字に一致する	a.b	aab、aXb、a-b
?	直前の文字が 0 回または 1 回出現するパターンに一致する	b?c	ac、abc
*	直前の文字が 0 回以上繰り返し返すパターンに一致する	ab*c	ac、abc、abbc、abbbbbbbbc
+	直前の文字が 1 回以上繰り返し返すパターンに一致する	ab+c	abc、abbc、abbbbbbbbc
	前後の文字のいずれかに一致する	ab cd	abd、acd
[]	[] 内の文字のいずれかに一致する	a[bc]d	abd、acd
[^]	[] 内の文字以外のものに一致する	a[^bc]d	aad、axd
^	行の先頭に一致する	^abc	abc で始まる行
\$	行の末尾に一致する	abc\$	abc で終わる行

文字	意味	使用例	一致する文字列の例
()	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
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

2.5.2 show コマンドの表示内容を見やすくする

[書式]

```
show [...] | less
```

[説明]

show コマンドの表示内容を 1 画面単位で表示し、最終行でコマンドを受け付ける。

表示内容が 1 画面に満たない場合には、すべての内容を表示して終了する。

コマンドは、数値プレフィックスとコマンド文字を入力することで実行される。数値プレフィックスはオプションで省略できる。数値プレフィックスを省略した場合には 1 と見なされる。検索コマンドでは、コマンド文字の後に検索文字列を入力できる。

コマンドには以下の種類がある。

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

コマンド	内容 (数値プレフィックスを N とする)
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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

2.5.3 外部ストレージ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
<code>prefix:path</code>	外部ストレージ内のファイル

- [初期値]: -

[説明]

show コマンドの実行結果を外部ストレージに保存させることができる。

`name` の `prefix` には **mount** コマンドでマウントした外部ストレージを指定できる。マウントされている外部ストレージは **show status storage interface** コマンドで確認できる。

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、既存ファイルを指定した場合はファイルを上書きしてよいか確認メッセージが表示される。ただし、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。

外部ストレージの既存ファイルに対してリダイレクト (>>) 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。

パイプ (|) と併用することで必要な行のみをファイルとして保存させることができる。

保存ファイルの暗号化には対応していない。

[ノート]

リダイレクトの後にパイプ (|) は指定できない。

リダイレクトを複数回指定できない。

show 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。

ストレージ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。

`path` に含まれるディレクトリ名およびファイル名は半角 255 文字以内。

[設定例]

パイプ (|) と併用し、必要な行のみを保存する。

```
# show log | grep IKE > smb001:/log.txt
```

リダイレクト (>) を使用して、コマンドの実行結果を既存ファイルを上書きして保存する。

```
# show log > smb001:(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)
```

リダイレクト (>>) を使用して、コマンドの実行結果を既存ファイルに追加する。

```
# show log > smb001:/log.txt ... 新規ファイル
```

```
# show log >> smb001:/log.txt ... 既存ファイルの末尾に追加
```

[適用モデル]

vRX VMware ESXi 版

第 3 章

ヘルプ

3.1 コンソールに対する簡易説明の表示

[書式]

help

[説明]

コンソールの使用方法の簡単な説明を表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

3.2 コマンド一覧の表示

[書式]

show command

[説明]

コマンドの名称とその簡単な説明を一覧表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

第 4 章

機器の設定

4.1 ログインパスワードの設定

[書式]

login password

[説明]

一般ユーザとしてログインするためのパスワードを 32 文字以内で設定する。パラメータはなく、コマンド入力後にプロンプトに応じて改めてパスワードを入力する形になる。

パスワードに使用できる文字は、半角英数字および記号 (7bit ASCII Code で表示可能なもの)。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.2 ログインパスワードの暗号化保存

[書式]

login password encrypted

[説明]

無名ユーザのパスワードを 32 文字以内で設定し、暗号化して保存する。パラメータはなく、コマンド入力後にプロンプトに応じて改めてパスワードを入力する形になる。

パスワードに使用できる文字は、半角英数字および記号 (7bit ASCII Code で表示可能なもの)。

[ノート]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.3 管理パスワードの設定

[書式]

administrator password

[説明]

管理ユーザとしてルーターの設定を変更するための管理パスワードを 32 文字以内で設定する。パラメータはなく、コマンド入力後にプロンプトに応じて改めてパスワードを入力する形になる。

パスワードに使用できる文字は、半角英数字および記号 (7bit ASCII Code で表示可能なもの)。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.4 管理パスワードの暗号化保存

[書式]

administrator password encrypted

[説明]

管理ユーザのパスワードを 32 文字以内で設定し、暗号化して保存する。パラメータはなく、コマンド入力後にプロンプトに応じて改めてパスワードを入力する形になる。

パスワードに使用できる文字は、半角英数字および記号 (7bit ASCII Code で表示可能なもの)。

[ノート]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.5 一般ユーザ名とログインパスワードの設定

[書式]

```
login user user [password]
login user user encrypted password
no login user user [password]
```

[設定値及び初期値]

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

[説明]

一般ユーザ名とパスワードを設定する。

登録できるユーザは最大 32 人。

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

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

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

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

[ノート]

同一のユーザ名を複数登録することはできない。

既に登録されているユーザ名で設定を行った場合は、元の設定が上書きされる。

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

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**

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

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**

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.8 ソフトウェアライセンスの操作

4.8.1 ユーザー ID とパスワードの設定

[書式]

vrX user user_id password

no vrX user [*user_id password*]

[設定値及び初期値]

- *user_id*
 - [設定値]: ユーザー ID (半角 4 文字以上、64 文字以下)
 - [初期値]: -
- *password*
 - [設定値]: パスワード (半角 8 文字以上、64 文字以下)
 - [初期値]: -

[説明]

ルーターを使用するユーザー ID とパスワードを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.8.2 ライセンスファイルの保存ディレクトリの設定

[書式]

vrX license file directory path

no vrx license file directory [*path*]

[設定値及び初期値]

- *path*
 - [設定値]: ライセンスファイルを保存するディレクトリの絶対パス、または相対パス
 - [初期値]: /

[説明]

インポートするライセンスファイル、およびエクスポートしたライセンスファイルを保存するディレクトリを設定する。

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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.8.3 ライセンスが有効であるか否かの判定スケジュールの設定

[書式]

vrX license update schedule *time1 time2*
no vrx license update schedule [*time1 time2*]

[設定値及び初期値]

- *time1,time2*
 - [設定値]: ライセンスの有効であるか否かの判定を行う時間帯 (24 時間制 HH:MM 形式)
 - [初期値]:
 - *time1* ... 01:00
 - *time2* ... 03:00

[説明]

ルーターにインポートされているライセンスが有効であるか否かの判定を行うスケジュールを設定する。

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ライセンスの判定を行う。

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。この場合、タイミングによってはライセンスが有効となるのが約 1 日遅れとなる可能性がある。

例えば、*time1* を 23:00、*time2* を 01:00 と設定した状態で、開始日が 2020/04/10 であるライセンスがインポートされているとする。このとき、2020/04/09 の 23:00 ~ 23:59 の間にライセンスの判定が行われると、ライセンスが有効となるのは 2020/04/10 の 23:00 ~ 2020/04/11 の 01:00 の間となる。

確実にライセンスを開始日に有効としたい場合は、*time2* を *time1* で指定した時刻よりも遅い時刻となるように設定する。

有効な基本ライセンスが見つかった場合は、ルーターは当該ライセンスの機能制限に従って動作する。オプションライセンスがインポートされている場合はあわせて有効となる。

有効な基本ライセンスが見つからなかった場合は、ルーターはライセンス無効時の機能制限に従って動作する。

有効期限が被っている基本ライセンスが複数見つかった場合は、有効期限の開始日が現在の日付に一番近い基本ライセンスが有効となる。

有効期限の開始日が同じである場合は、有効期限の満了日が一番最後の基本ライセンスが有効となる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.8.4 ライセンスのインポート

[書式]

import vrx license file
import vrx license key [*key*]

[設定値及び初期値]

- *key*: インポートするライセンスキー
 - [初期値]: -

[説明]

基本ライセンス、およびオプションライセンスをインポートする。

基本ライセンスをインポートする前に **ntpdate** コマンドまたは **date** コマンドで日時設定を完了しておく必要がある。

オプションライセンスは、ルーターにインポートされている基本ライセンスと紐づくライセンスのみインポートで

きる。

第1書式を入力した場合は、ライセンスファイルでライセンスをインポートする。

`vrX license file directory` コマンドで指定したディレクトリに保存されているライセンスファイルを一括でインポートする。

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

第2書式を入力した場合は、ライセンスキーでライセンスをインポートする。

`key` を省略した場合は、インポートするライセンスキーの入力を求められる。

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

`key` にインポートするライセンスキーを入力した場合は、インポートを続行するか否かは問われず、正常なライセンスであれば自動的にインポートされる。

[ノート]

`key` パラメータは vRX VMware ESXi 版で使用可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.8.5 ライセンスのエクスポート

[書式]

`export vrX license file`

[説明]

ルーターにインポートされているライセンスをライセンスファイルとしてエクスポートする。

エクスポートしたライセンスファイルは `vrX license file directory` コマンドで指定したディレクトリ内の `vrX_license` ディレクトリに保存される。 `vrX_license` ディレクトリがない場合は自動的に作成される。エクスポートしたライセンスファイルには、以下の名前が付けられる。

ライセンス	ファイル名
基本ライセンス	<code>vrX_basic_yyyymmdd_hhmmss.lic</code>
VPN ライセンス	<code>vrX_vpn_yyyymmdd_hhmmss.lic</code>

`yyymmdd_hhmmss` はエクスポートを行った日時。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.8.6 ライセンスの削除

[書式]

`clear vrX license [history]`

[設定値及び初期値]

- `history`
 - [設定値]: 有効期限切れとなったライセンスのみ削除
 - [初期値]: -

[説明]

ルーターにインポートされている基本ライセンス、およびオプションライセンスを削除する。

`history` オプションを付与すると、有効期限切れとなったライセンスのみ削除する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.9 ユーザーの属性を設定

[書式]

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

`no user attribute [user...]`

[設定値及び初期値]

• *user*

- [設定値]:

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

- [初期値]: -

• *attribute=value* : ユーザー属性

- [設定値]:

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

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

- *connection* : ルーターへのアクセス方法を示す属性

設定値	説明
off	すべての接続を禁止する。
all	すべての接続を許可する。
serial	シリアルコンソールからの接続を許可する。
telnet	TELNET による接続を許可する。
ssh	SSH による接続を許可する。
sftp	SFTP による接続を許可する。

- *host* : ルーターへのアクセスホストを指定する属性

設定値	説明
IP アドレス	指定したホストからの接続を許可する。
any	すべてのホストからの接続を許可する。
インタフェース名	指定したインタフェースからの接続を許可する。

- *multi-session* : 複数接続を許可するかどうかを示す属性

設定値	説明
on	同一ユーザー名による TELNET、SSH での複数接続を許可する。
off	同一ユーザー名による TELNET、SSH 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,ssh,sftp*
- *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 及び SFTP 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 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、SSH と TELNET 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パスワード認証による SSH、SFTP による接続を許可することができない。公開鍵認証を使用する場合は SSH、SFTP による接続を許可することができる。

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 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.10 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

- [初期値]: -
- *no*
 - [設定値]: 接続番号

- [初期値]: -

[説明]

他ユーザの接続を切断する。

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

無名ユーザを切断する場合は、第 2 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) ユーザ名「test」でログインしているすべての接続を切断する。

```
# disconnect user test
```

例 2) TELNET で接続しているすべてのユーザを切断する。

```
# disconnect user /telnet
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.11 セキュリティクラスの設定

[書式]

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

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

[設定値及び初期値]

- *level*

- [設定値]:

設定値	説明
1	シリアル、TELNET、SSH でログインできる
2	シリアル、TELNET、SSH でログインできる
3	シリアルからのみログインできる

- [初期値]: 1

- *forget*

- [設定値]:

設定値	説明
on	設定したパスワードの代わりに "w,lXlma" (ダブルユー、カンマ、エル、エックス、エル、エム、エー) でもログインでき、設定の変更も可能になる。ただしシリアルのみ
off	パスワードを入力しないとログインできない

- [初期値]: on

- *telnet*

- [設定値]:

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

- [初期値]: off

- *ssh*

- [設定値]:

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

- [初期値]: off

[説明]

セキュリティクラスを設定する。

[ノート]

vRX Amazon EC2 版で本コマンドの *level* を 3 に設定した場合、vRX へアクセスできなくなります。意図せずこの設定を行い、アクセス可能な状態へ復旧させる場合はユーザーガイドの 4 章 8 節「本製品の起動時 CONFIG の設定」に習い、**no security class** をユーザーデータへ設定してください。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.12 タイムゾーンの設定

[書式]

`timezone timezone`

`no timezone [timezone]`

[設定値及び初期値]

- *timezone*: その地域と世界標準時との差
- [設定値]:

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

- [初期値]: jst

[説明]

タイムゾーンを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.13 現在の日付けの設定

[書式]

`date date`

[設定値及び初期値]

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

[説明]

現在の日付けを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.14 現在の時刻の設定

[書式]

`time time`

[設定値及び初期値]

- *time*
 - [設定値]: hh:mm:ss

- [初期値]:-

[説明]

現在の時刻を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.15 リモートホストによる時計の設定

[書式]

```
rdate host [syslog]
```

[設定値及び初期値]

- *host*
 - [設定値]:

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

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

[説明]

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

[ノート]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.16 NTP による時計の設定

[書式]

```
ntpdate ntp_server [syslog]
```

[設定値及び初期値]

- *ntp_server*
 - [設定値]:

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

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

[説明]

NTP を利用してルーターの時計を設定する。このコマンドが実行されるとホストの UDP の 123 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を指定した方がよい。利用可能な NTP サーバーについてはプロバイダに問

い合わせる。

syslog キーワードを指定した場合には、コマンドの出力結果を INFO レベルの SYSLOG へ出力する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.17 NTP パケットを送信するときの始点 IP アドレスの設定

[書式]

ntp local address *ip_address*

no ntp local address

[設定値及び初期値]

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

[説明]

NTP パケットを送信するときの始点 IP アドレスを設定する。

始点 IP アドレスが設定されていないときは、通常の UDP パケットの送信ルールに従い、出力インタフェースの IP アドレスを利用する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

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

[書式]

ntp backward-compatibility *comp*

no ntp backward-compatibility [*comp*]

[設定値及び初期値]

- *comp*
 - [設定値]:

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

- [初期値]: -

[説明]

Stratum 0 の NTP サーバーとの時刻同期を許可する。

[ノート]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.19 コンソールのプロンプト表示の設定

[書式]

console prompt *prompt*

no console prompt [*prompt*]

[設定値及び初期値]

- *prompt*
 - [設定値]: コンソールのプロンプトの先頭文字列 (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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.20 コンソールの言語とコードの設定

[書式]

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

[設定値及び初期値]

- *code*
 - [設定値]:

設定値	説明
en.ascii	英語で表示する、文字コードは ASCII
ja.sjis	日本語で表示する、文字コードはシフト JIS
ja.euc	日本語で表示する、文字コードは EUC
ja.utf8	日本語で表示する、文字コードは UTF-8

- [初期値]: ja.utf8

[説明]

コンソールに表示する言語とコードを設定する。

本コマンドは一般ユーザでも実行できる。

vRX VMware ESXi 版では、VMware ESXi の Web コンソールを使用しているときには、本コマンドの設定に関わらず英語で表示され、文字コードは ASCII となる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.21 コンソールの表示文字数の設定

[書式]

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

[設定値及び初期値]

- *col*
 - [設定値]: コンソールの表示文字数 (80..200; vRX Amazon EC2 版、80..4096; vRX VMware ESXi 版)
 - [初期値]: 80

[説明]

コンソールの 1 行あたりの表示文字数を設定する。

本コマンドは一般ユーザでも実行できる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.22 コンソールの表示行数の設定

[書式]

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

[設定値及び初期値]

- *lines*
 - [設定値]:

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

- [初期値]: 24

[説明]

コンソールの表示行数を設定する。
このコマンドは一般ユーザでも実行できる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.23 コンソールにシステムメッセージを表示するか否かの設定

[書式]

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

[設定値及び初期値]

- *info*
 - [設定値]:

設定値	説明
on	表示する
off	表示しない

- [初期値]: off

[説明]

コンソールにシステムメッセージを表示するか否かを設定する。

[ノート]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.24 SYSLOG を受けるホストの IP アドレスの設定

[書式]

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

[設定値及び初期値]

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

[説明]

SYSLOG を受けるホストの IP アドレスを設定する。

IP アドレスは IPv4/IPv6 いずれのアドレスも設定できる。

syslog debug コマンドが on に設定されている場合、大量のデバッグメッセージが送信されるので、このコマンドで設定するホストには十分なディスク領域を確保しておくことが望ましい。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.25 SYSLOG ファシリティの設定

[書式]

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

[設定値及び初期値]

- *facility*
 - [設定値]:

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

- [初期値]: user

[説明]

SYSLOG のファシリティを設定する。

[ノート]

ファシリティ番号の意味づけは、各 SYSLOG サーバーで独自に行う。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.26 NOTICE タイプの SYSLOG を出力するか否かの設定

[書式]

syslog notice notice

no syslog notice [*notice*]

[設定値及び初期値]

- *notice*
- [設定値]:

設定値	説明
on	出力する
off	出力しない

- [初期値]: off

[説明]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.27 INFO タイプの SYSLOG 出力の設定

[書式]

syslog info info

no syslog info [*info*]

[設定値及び初期値]

- *info*
- [設定値]:

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

- [初期値]: on

[説明]

ルーターの動作状況に関する SYSLOG 出力の設定をする。

[ノート]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.28 DEBUG タイプの SYSLOG を出力するか否かの設定

[書式]

```
syslog debug debug
no syslog debug [debug]
```

[設定値及び初期値]

- *debug*
 - [設定値]:

設定値	説明
on	出力する
off	出力しない

- [初期値]: off

[説明]

ルーターのデバッグ情報を SYSLOG で出力するか否かを設定する。

[ノート]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.29 SYSLOG ファイルの設定

[書式]

```
syslog file [crypto password] [name=name] [limit=size] [backup=num] [interval=interval] [line=line]
no syslog file [[crypto password] [name=name] [limit=size] [backup=num] [interval=interval] [line=line]]
```

[設定値及び初期値]

- *crypto*: SYSLOG を暗号化して保存する場合の暗号化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]: -
- *name*
 - [設定値]: SYSLOG ファイルの名前
 - [初期値]: syslog.txt
- *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 をファイルに書き出す間隔 (2..86400 単位: 秒)
 - [初期値]: 3600
- *line*
 - [設定値]: SYSLOG をファイルに書き出す行数 (1000..10000 単位: 行)
 - [初期値]: 1000

[説明]

SYSLOG ファイルの保存について設定する。

SYSLOG ファイルは /yamaha_sys に保存される。

crypto および *password* を指定した場合、SYSLOG は暗号化して保存される。暗号化する場合は *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。拡張子を省略した場合は自動的にファイル名に *.rtfg* 拡張子が追加される。暗号化しない場合は *name* に *.rtfg* 拡張子を含むファイル名は指定できない。

SYSLOG ファイルが *size* で指定したサイズに達すると、バックアップファイルを作成する。バックアップファイル名は *name* で指定したファイル名にバックアップ日時 (*_yyymmdd_hhmmss*) を付加したものとなる。

- *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の数が *num* で指定した数に達した場合、もしくは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を作成する。

[ノート]

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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.30 SYSLOG ファイルのファイルサーバーへの保存設定

[書式]

syslog mount-server filename name [*crypto password*] [*limit=size*] [*backup=num*]

no syslog mount-server filename [*name* [*crypto password*] [*limit=size*] [*backup=num*]]

[設定値及び初期値]

- *name*
 - [設定値]: ファイルサーバーのパスを含めた SYSLOG ファイルの名前
 - [初期値]: -
- *crypto*: SYSLOG を暗号化して保存する場合の暗号化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

[説明]

SYSLOG ファイルのファイルサーバー (NFS、または SMB) への保存について設定する。

ファイルサーバーは **mount** コマンドでマウントされている必要がある。本コマンドが設定されている場合であっても、ファイルサーバーがマウントされていない状態では SYSLOG は保存されない。

name には **mount** コマンドで指定したプレフィックスからはじまるパスを含めた SYSLOG ファイルの名前を指定する。

- (例) server:/syslog/log.txt

crypto および *password* を指定した場合、SYSLOG は暗号化して保存される。暗号化する場合は *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。拡張子を省略した場合は自動的にファイル名に *.rtfg* 拡張子が追加される。暗号化しない場合は *name* に *.rtfg* 拡張子を含むファイル名は指定できない。

SYSLOG ファイルが *size* で指定したサイズに達すると、バックアップファイルを作成する。バックアップファイル名は *name* で指定したファイル名にバックアップ日時 (*_yyyymmdd_hhmmss*) を付加したものとなる。

- *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の数が *num* で指定した数に達した場合、もしくは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を作成する。

以下の設定については、**syslog file** コマンドの設定に従う。

- SYSLOG をファイルに書き出す間隔
- SYSLOG をファイルに書き出す行数

syslog file コマンドの *interval* オプションで指定した時間が経過、または *line* オプションで指定した行数だけ SYSLOG が出力されたとき、ファイルサーバーの SYSLOG ファイルに SYSLOG を書き出す。

[ノート]

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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.31 SYSLOG を送信する時の始点 IP アドレスの設定

[書式]

```
syslog local address address
no syslog local address [address]
```

[設定値及び初期値]

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

[説明]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.32 SYSLOG パケットの始点ポート番号の設定

[書式]

```
syslog srcport port
no syslog srcport [port]
```

[設定値及び初期値]

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

[説明]

本機が送信する SYSLOG パケットの始点ポート番号を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.33 SYSLOG に実行コマンドを出力するか否かの設定

[書式]

```
syslog execute command switch
```

no syslog execute command [*switch*]

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	実行されたコマンドをログに残す
off	実行されたコマンドをログに残さない

- [初期値]: off

[説明]

実行されたコマンドを SYSLOG で出力するか否かを設定する。

[ノート]

コマンド実行に成功した場合、そのコマンド入力をログに出力する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

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

[書式]

packetdump *interface count*

packetdump pp *peer_num count*

[設定値及び初期値]

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

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

- [初期値]: off

[説明]

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

[ノート]

本コマンドの設定は、**show config** コマンドで表示されない。

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

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

すべてのパケットがダンプされるわけではない。パケットロスすることもある。

ファストパスで処理されたパケットは出力されない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.35 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。

デプロイ時の状態および **cold start** コマンド実行後の本コマンドの設定値については「1.6 デプロイ時の設定値について」を参照してください。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.36 TELNET サーバー機能の listen ポートの設定

[書式]

```
telnetd listen port
no telnetd listen
```

[設定値及び初期値]

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

[説明]

TELNET サーバー機能の listen ポートを選択する。

[ノート]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.37 TELNET サーバーへアクセスできるホストの設定

[書式]

```
telnetd host ip_range [ip_range...]
telnetd host any
telnetd host none
telnetd host lan
no telnetd host
```

[設定値及び初期値]

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

設定値	説明
1 個の IP アドレスまたは間にハイフン (-) をはさんだ IP アドレス (範囲指定)、およびこれらを任意に並べたもの	指定したホストからのアクセスを許可する

- [初期値]: -

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

[初期設定]

telnetd host any

[説明]

TELNET サーバーへのアクセスを許可するホストを設定する。

[ノート]

設定後の新しい TELNET 接続から適用される。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.38 TELNET サーバーへ同時に接続できるユーザ数の設定

[書式]

```
telnetd session num
```

```
no telnetd session
```

[設定値及び初期値]

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

[説明]

TELNET に同時に接続できるユーザ数を設定する。

[ノート]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.39 CPU 使用率の閾値の設定

[書式]

```
system cpu threshold off
```

```
system cpu threshold cpu1 cpu2 [duration=duration]
```

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

[設定値及び初期値]

- off
 - [設定値]: 警告を発しない
 - [初期値]: -
- *cpu1*
 - [設定値]: 警告を発する CPU 使用率の閾値の上限 (0..100 %)
 - [初期値]: -
- *cpu2*
 - [設定値]: 警告を発する CPU 使用率の閾値の下限 (0..100 %)
 - [初期値]: -
- *duration*
 - [設定値]: 判定時間 (1..300 秒)
 - [初期値]: 1

[初期設定]

```
system cpu threshold off
```

[説明]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.40 メモリ使用率の閾値の設定

[書式]

```
system memory threshold off
system memory threshold memory1 memory2 [duration=duration]
no system memory threshold [memory1 [memory2 [duration=duration]]]
```

[設定値及び初期値]

- off
 - [設定値]: 警告を発しない
 - [初期値]: -
- *memory1*
 - [設定値]: 警告を発するメモリ使用率の閾値の上限 (0..100 %)
 - [初期値]: -
- *memory2*
 - [設定値]: 警告を発するメモリ使用率の閾値の下限 (0..100 %)
 - [初期値]: -
- *duration*
 - [設定値]: 判定時間 (1..300 秒)
 - [初期値]: 1

[初期設定]

```
system memory threshold off
```

[説明]

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

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.41 ファストパス機能の設定

[書式]

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

[設定値及び初期値]

- *process*
 - [設定値]:

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

- [初期値]: fast

[説明]

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

[ノート]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.42 LAN インタフェースの動作設定

[書式]

```
lan shutdown interface
no lan shutdown interface
```

[設定値及び初期値]

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

[説明]

LAN インタフェースを利用できないようにする。このコマンドを設定した LAN インタフェースは、LAN ケーブルを接続してもリンクアップしなくなる。

[ノート]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.43 LAN インタフェースのリンクアップ後の送信抑制時間の設定

[書式]

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

[設定値及び初期値]

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

[説明]

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

[ノート]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.44 LAN インタフェースの動作タイプの設定

[書式]

```
lan type interface speed [option=value...]
no lan type interface [...]
```

[設定値及び初期値]

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

- [初期値]: auto
- *option=value*: オプション機能

- [設定値]:

- mtu
 - インタフェースで送受信できる最大データ長
- auto-crossover
 - オートクロスオーバー機能

設定値	説明
on	オートクロスオーバー機能を有効にする
off	オートクロスオーバー機能を無効にする

- [初期値]:
 - mtu=1500
 - auto-crossover=on

[説明]

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

○mtu

インタフェースで送受信できる最大データ長を指定する。データ長には MAC ヘッダと FCS は含まれない。指定できるデータ長の範囲は 64~1500 の範囲となる。

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

○オートクロスオーバー機能

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

[ノート]

LAN インターフェースが使用できる場合、本コマンドの実行後、LAN インタフェースのリセットが自動で行われ、その後に設定が有効となる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.45 LAN インタフェースの受信パケットバッファサイズの設定

[書式]

lan receive-buffer-size *size*

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

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *size*
 - [設定値]: 受信パケットバッファサイズ
 - [設定値]:
 - 1..16384
 - [初期値]:
 - 1024
 - 8 (vRX Amazon EC2 版で QoS 設定時)

[説明]

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

本コマンドで設定したサイズが全 CPU コアの受信処理に適用される。

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.46 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 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.47 TFTP によりアクセスできるホストの設定

[書式]

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

tftp host any

tftp host none

tftp host lan

no tftp host

[設定値及び初期値]

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

- [設定値]:

設定値	説明
1 個の IP アドレスまたは間にハイフン (-) をはさんだ IP アドレス (範囲指定)、およびこれらを任意に並べたもの	指定したホストからのアクセスを許可する
lanN	LAN インターフェースからのアクセスを許可する

- [初期値]: -

- any

- [設定値]: すべてのホストからのアクセスを許可する

- [初期値]: -

- none

- [設定値]: すべてのホストからのアクセスを禁止する

- [初期値]: -

- lan

- [設定値]: すべての LAN 側ネットワーク内からのアクセスを許可する

- [初期値]: -

[初期設定]

tftp host none

[説明]

TFTP サーバーへのアクセスを許可するホストを設定する。

[ノート]

セキュリティの観点から、設定ファイルの読み書きが終了したらすぐに **none** にする。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.48 Magic Packet を LAN に中継するか否かの設定

[書式]

ip interface wol relay relay

no ip interface wol relay

[設定値及び初期値]

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

設定値	説明
broadcast	Magic Packet をブロードキャストパケットとして中継する
unicast	Magic Packet をユニキャストパケットとして中継する
off	Magic Packet かどうか検査しない

- [初期値]: off

[説明]

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

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

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

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

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

[ノート]

いずれの場合も、Magic Packet として中継されなかった場合のパケットは、**ip filter directed-broadcast** コマンドの設定に基づき処理される。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.49 インタフェースまたはシステムの説明の設定

[書式]

description id description

no description id [description]

description interface description

no description interface [description]

[設定値及び初期値]

- *id*
 - [設定値]: システム全体の説明を記述する場合の ID (1..21474836)
 - [初期値]: -

- *interface*
 - [設定値]: LAN インタフェース名、'pp'、'tunnel' のいずれか
 - [初期値]: -
- *description*
 - [設定値]: 説明の文字列 (最大 64 文字/ASCII、32 文字/シフト JIS)
 - [初期値]: -

[説明]

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

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

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

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

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

説明には、ASCII 文字だけではなく、シフト JIS で表現できる範囲の日本語文字 (半角カタカナを除く) も使用できる。ただし、**console character** コマンドの設定が *ja.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。

また、vRX VMware ESXi 版では、VMware ESXi の Web コンソールを使用しているときには、**console character** コマンドの設定が *ja.sjis* の場合でも、文字化けすることがある。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.50 SSH サーバー機能の ON/OFF の設定

[書式]

```
ssh service service
no ssh 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。

デプロイ時の状態および **cold start** コマンド実行後の本コマンドの設定値については「1.6 デプロイ時の設定値について」を参照してください。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.51 SSH サーバー機能の listen ポートの設定

[書式]

```
ssh listen port
no ssh listen [port]
```

[設定値及び初期値]

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

[説明]

SSH サーバーの listen ポートを選択する。

[ノート]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.52 SSH サーバーへアクセスできるホストの設定

[書式]

```
sshhd host ip_range [ip_range...]
sshhd host any
sshhd host none
sshhd host lan
no sshhd host
```

[設定値及び初期値]

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

設定値	説明
1 個の IP アドレスまたは間にハイフン (-) をはさんだ IP アドレス (範囲指定)、およびこれらを任意に並べたもの	指定したホストからのアクセスを許可する
lanN	LAN インターフェースからのアクセスを許可する

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

[初期設定]

```
sshhd host any
```

[説明]

SSH サーバーへのアクセスを許可するホストを設定する。

[ノート]

設定後の新しい SSH 接続から適用される。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.53 SSH サーバーへ同時に接続できるユーザ数の設定

[書式]

```
sshhd session num
no sshhd session [num]
```

[設定値及び初期値]

- *num*

- [設定値]: 同時接続数 (1..8)
- [初期値]: 8

[説明]

SSH に同時に接続できるユーザ数を設定する。

[ノート]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.54 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]:
 - 2048

[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、インスタンスによって異なるが、1024 ビット鍵では数秒程度、2048 ビット鍵では十数秒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。

デプロイ時の状態および **cold start** コマンド実行後の本コマンドの設定値については「1.6 デプロイ時の設定値について」を参照してください。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.55 SSH サーバーホスト鍵の表示

[書式]

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

[設定値及び初期値]

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

設定値	説明
md5	MD5
sha256	SHA-256

- [初期値]: sha256

[説明]

SSH サーバーのホスト鍵を表示する。

fingerprint キーワードを指定した場合は、公開鍵の鍵長と鍵指紋を表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.56 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

- [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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.57 SSH クライアントの生存確認

[書式]

sshd client alive switch [*interval* [*count*]]

no sshd client alive [*switch* ...]

[設定値及び初期値]

- *switch*

- [設定値] :

設定値	説明
on	クライアントの生存確認を行う
off	クライアントの生存確認を行わない

- [初期値] : off

- *interval*

- [設定値] : 送信間隔の秒数 (1..2147483647)

- [初期値] : 100

- *count*

- [設定値] : 試行回数 (1..2147483647)

- [初期値] : 3

[説明]

クライアントの生存確認を行うか否かを設定する。

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

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

[書式]

```
sshd hide openssh version use
```

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

[設定値及び初期値]

- *use*
- [設定値]:

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

- [初期値]: off

[説明]

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

[ノート]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.59 SSH サーバーで利用可能な認証方式の設定

[書式]

```
sshd auth method all
```

```
sshd auth method method [method]
```

```
no sshd auth method [...]
```

[設定値及び初期値]

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

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

- [初期値]: -

[説明]

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

[ノート]

本コマンドが使用できないファームでは、**sshd auth method password** 相当の動作となります。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

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

[書式]

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

[設定値及び初期値]

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

[説明]

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

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

user を省略した場合は、無名ユーザに対する設定となる。

path には `mount` コマンドでマウントした外部ストレージを指定できる。外部ストレージのパスは、マウント時に設定したプレフィックスを先頭に付与して指定する。

例えば、プレフィックスが "storage:" である外部ストレージの "/dir/sample" を指定する場合は、"storage:/dir/sample" と指定する。

マウントされている外部ストレージは `show status storage interface` コマンドで確認できる。

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

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

[サンプル]

例:RSA 2048bit の公開鍵の場合

```
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAp3eK3sk60fhHP9zsRgI39tqAoNfljbnCNiJ7horhwu6
lZyaKDKf8BiiCsKnvFsLifSgcOejllfBtrFX3bN8iu+me2Ggh52vuIWDS/SUEQNwCYCaY0Ign8u8O
zVxldx1QABzuAKEKA654gkhQA40iaCKbKD5RGp4zujqDA6p8Y9o06pC/Ns7GzkgegrMxg40feB+0hjS
+K2eY49uqqwqYUYCdNw6bTIJiH6nAgsXSUDjbo3N+b9CY/9/7txKBykt1zt04WCXepngxVRw2ss+JOV
kPisDmtl0//Q7Xdi+MxiLKhjeZk3jppqrSHiLon6D30xU/5/FY0cwcRBwrj4Uuw== user1
```

例:ECDSA 256bit の公開鍵の場合

```
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBP211Vy
IP8Bg+r8rZhNmRq+ber0+sOaYCsVm5TN1CGt5WpCNkpwkV3c3rxwA6GAgGxuJsSn4J6Bo1mABhHg+YH
M= user2
```

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

[ノート]

path への外部ストレージ指定は vRX VMware ESXi 版で可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.61 SSH サーバーの公開鍵認証に用いる公開鍵の設定

[書式]

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

[設定値及び初期値]

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

[説明]

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

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

user を省略した場合は、無名ユーザに対する設定となる。

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

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

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

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

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.62 SSH サーバーの公開鍵認証に用いる公開鍵の表示

[書式]

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

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

[設定値及び初期値]

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

設定値	説明
md5	MD5
sha256	SHA-256

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

[説明]

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

fingerprint を指定した場合は、公開鍵の鍵長と鍵指紋を表示する。

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

第 2 書式では、全ユーザの `authorized_keys` ファイルを表示する。

[設定例]

例: RSA 2048bit の公開鍵を表示する場合

```
# show sshd authorized-keys user1
```

```
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAp3eK3sk60fhHP9zsRgI39tqAoNfljbnCNiJ7horhwu6
lZyaKDKf8BiiCsKnvFsLifSgcOejllfBtrFX3bN8iu+me2Ggh52vuIWDS/SUEQNwCYCaY0Ign8u80
```

```
zVxldx1QABzuAKEKA654gkhQA40iaCKbKD5RGp4zujqDA6p8Y9o06pC/Ns7GzkgegrMxg40feB+0hjS
+K2eY49uqqwqYUYCdNw6bTIJiH6nAgsXSUDjbo3N+b9CY/9/7txKBykt1zt04WCXepngxVRw2ss+JOV
kPisDmtl0//Q7Xdi+MxiLKhjeZk3jppqrSHiLon6D30xU/5/FY0cwcRBwrj4Uuw== user1
```

```
例:RSA 2048bit の公開鍵の鍵指紋を SHA-256 で表示した場合
# show sshd authorized-keys user1 type=fingerprint sha256
2048 SHA256:uk2janKfeZXBsUniTMdNwL2fhdcAdfy0MsGSsCtpg8E user1 (RSA)
```

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

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

```
# show sshd authorized-keys * type=fingerprint sha256
(noname) /ssh/authorized_keys/no.name
2048 SHA256:fMIGwY5YlQvz9xEObkDXaO7TuvIlgFIakmV0K2MGbyU (RSA)
```

```
user1 /ssh/authorized_keys/user1
2048 SHA256:uk2janKfeZXBsUniTMdNwL2fhdcAdfy0MsGSsCtpg8E user1 (RSA)
```

```
user2 /pub-key
2048 SHA256:UI7sScopCUNPA5IndPWzHhkANqr3PkD2k3GMv0qS5NA user2 (RSA)
```

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.63 SFTP サーバーへアクセスできるホストの設定

[書式]

```
sftpd host ip_range [ip_range...]
sftpd host any
sftpd host none
sftpd host lan
no sftpd host
```

[設定値及び初期値]

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

設定値	説明
1 個の IP アドレスまたは間にハイフン (-) をはさんだ IP アドレス (範囲指定)、およびこれらを任意に並べたもの	指定したホストからのアクセスを許可する
lanN	LAN インターフェースからのアクセスを許可する

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

[初期設定]

```
sftpd host none
```

[説明]

SFTP サーバーへのアクセスを許可するホストを設定する。

[ノート]

対象となるホストは **ssh host** コマンドでもアクセスが許可されていなければならない。
設定後の新しい SFTP 接続から適用される。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.64 SSH クライアント

[書式]

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

[設定値及び初期値]

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

[説明]

SSH を実行し、指定したホストにリモートログインする。

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

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

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

[設定例]

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]
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.65 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。

ルーターの設定ファイル (config、config0～config4) を指定する場合には、*file* に "config" のようにファイル名のみを指定する。

外部ストレージを指定する場合には、マウント時に設定したプレフィックスを先頭に付与して指定する。例えば、プレフィックスが "storage:" である外部ストレージの "/dir/sample.txt" を指定する場合は、"storage:/dir/sample.txt" と指定する。マウントされている外部ストレージは show status storage interface コマンドで確認できる。

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。

[ノート]

転送元・転送先ファイルへの外部ストレージ指定は vRX VMware ESXi 版で可能。

[設定例]

リモートホスト (192.168.1.1) から、ルーターのルートディレクトリにファイルをコピーする。

```
# scp user@192.168.1.1:example.txt /example.txt
```

ルーター上のファイル /yamaha_sys/syslog.txt を、リモートホスト (2001:1::1) へコピーする。

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.66 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

- [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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.67 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.68 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

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

vRX Amazon EC2 版

group	max-buffer
small	10000
middle	26664
large	40000
huge	532

vRX VMware ESXi 版

group	max-buffer
small	45000

group	max-buffer
middle	120000
large	180000
huge	532

[説明]

パケットバッファの管理パラメータを変更する。

各モデルの *value* パラメータには以下の範囲の値を指定できる。

vRX Amazon EC2 版

group	max-buffer
small	1..40000
middle	1..106656
large	1..160000
huge	1..2128

vRX VMware ESXi 版

group	max-buffer
small	45000..75000
middle	120000..200000
large	180000..300000
huge	532

[ノート]

本コマンドによる設定の変更を反映するには、ルーターの再起動が必要となる。

[設定例]

```
# system packet-buffer large max-buffer=60000
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.69 環境変数の設定

[書式]

```
set name=value
```

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

[設定値及び初期値]

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

[説明]

ルーターの環境変数を設定する。

環境変数名の命名規則は次の通りである。

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

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

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

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.70 エイリアスの設定

[書式]**alias** *name*=*value***no alias** *name*[=*value*]**[設定値及び初期値]**

- *name*
 - [設定値]: エイリアス名
 - [初期値]: -
- *value*
 - [設定値]: 設定値
 - [初期値]: -

[説明]

エイリアスを設定する。

エイリアスの命名規則は次の通りである。

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.71 マクロの設定

[書式]**macro** [-v] [-x] *name* <<*eom***no macro** [-v] [-x] *name* [<<*eom*]**[設定値及び初期値]**

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

[説明]

マクロを設定する。

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

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

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

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

実行例は以下の通り。

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

[ノート]

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

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

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.72 EMFS ファイルの作成、削除

[書式]

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

[設定値及び初期値]

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

[説明]

EMFS 上のファイルを作成、削除する。

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

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

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

実行例は以下の通り。

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

[ノート]

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

Lua スクリプトの `rt.command()` で複数行からなるコマンドを実行する場合には、各行を改行文字（'\n'）で連結した

文字列をコマンドとして渡す。改行文字は '\n' でなくてはならず、'\r' や '\r\n' ではエラーとなる。
実行例は以下の通り。

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

4.73 CPU スケジューリング方式の設定

[書式]

system packet-scheduling *mode*

no system packet-scheduling [*mode*]

[設定値及び初期値]

- *mode*: CPU スケジューリング方式
 - [設定値]:

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

- [初期値]: hash

[説明]

CPU スケジューリング方式を設定する。

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

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

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

CPU コア数が 4、NIC のバインド数が 4 のとき

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

CPU コア数が 2、NIC のバインド数が 3 のとき

受信 LAN インターフェース	CPU コア
LAN1	CPU1
LAN2	CPU1
LAN3	CPU1

fixed を選択した場合、パケットを受信した LAN インターフェースによらず、転送処理は常に CPU1 で実行される。

[ノート]

vRX Amazon EC2 版で本コマンドによる設定の変更を反映するには、ルーターの再起動が必要となる。

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

ノーマルパスの処理対象となるパケットは、本コマンドの設定に従って決定された CPU コアでは受信処理のみが実行され、転送処理は常に CPU0 で実行される。これは、**ip routing process** コマンドで **normal** が設定されている場合はすべてのパケットが対象となる。

CPU スケジューリング方式に **hash** を選択した場合、IPv4/IPv6 ヘッダを持たない受信パケットの転送処理は CPU1 で実行される。

CPU スケジューリング方式に **load-balance** を選択した場合、パケットの順番が入れ替わる可能性がある。パケットの順番が入れ替わると UDP を用いるアプリケーションで問題が発生する可能性がある。なお、TCP ではパケットの順番が入れ替わっても通常は問題は発生しない。

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

第 5 章

IP の設定

5.1 インタフェース共通の設定

5.1.1 IP パケットを扱うか否かの設定

[書式]

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

[設定値及び初期値]

- *routing*
- [設定値]:

設定値	説明
on	IP パケットを処理対象として扱う
off	IP パケットを処理対象として扱わない

- [初期値]: on

[説明]

IP パケットをルーティングするかどうかを設定する。

[ノート]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.2 IP アドレスの設定

[書式]

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

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *loopback*
 - [設定値]: LOOPBACK インタフェース名
 - [初期値]: -
- *bridge_interface*
 - [設定値]: ブリッジインタフェース名
 - [初期値]: -
- *ip_address*
 - [設定値]: IP アドレス xxx.xxx.xxx.xxx(xxx は十進数)
 - [初期値]: -

- `dhcp`: DHCP クライアントとして IP アドレスを取得することを示すキーワード
 - [初期値]: -
- `mask`
 - [設定値]:
 - xxx.xxx.xxx.xxx(xxx は十進数)
 - 0x に続く十六進数
 - マスクビット数
 - [初期値]: -
- `broadcast_ip`
 - [設定値]: ブロードキャスト IP アドレス
 - [初期値]: -
- `switch`
 - [設定値]:

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

- [初期値]: off

[説明]

インタフェースの IP アドレスとネットマスクを設定する。“`broadcast broadcast_ip`” を指定すると、ブロードキャストアドレスを指定できる。省略した場合には、ディレクティッドブロードキャストアドレスが使われる。

`dhcp` を指定すると、設定直後に DHCP クライアントとして IP アドレスを取得する。また `dhcp` を指定している場合に **no ip interface address** を入力すると、取得していた IP アドレスの開放メッセージを DHCP サーバーに送る。

AutoIP 機能を使うに設定し、`ip bridge_interface dhcp retry` 設定で `dhcp` の `retry` 回数が有限に設定してあると、`dhcp` でのアドレスの割り当てが失敗した場合に自動的に 169.254.0.0/16 のアドレスが決定される。

[ノート]

LAN インタフェースに IP アドレスを設定していない場合には、RARP により IP アドレスを得ようとする。PP インタフェースに IP アドレスを設定していない場合には、そのインタフェースは `unnumbered` として動作する。DHCP クライアントとして動作させた場合に取得したクライアント ID は、`show status dhcp` コマンドで確認することができる。

デプロイ時および `cold start` コマンド実行後の本コマンドの設定値については「1.6 デプロイ時の設定値について」を参照してください。

ブリッジインタフェースは vRX VMware ESXi 版で指定可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.3 セカンダリ IP アドレスの設定

[書式]

```
ip interface secondary address ip_address[/mask]
ip interface secondary address dhcp
no ip interface secondary address [ip_address/mask]
```

[設定値及び初期値]

- `interface`
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- `ip_address`
 - [設定値]: セカンダリ IP アドレス xxx.xxx.xxx.xxx(xxx は十進数)
 - [初期値]: -
- `dhcp`: DHCP クライアントとして IP アドレスを取得することを示すキーワード
 - [初期値]: -
- `mask`
 - [設定値]:
 - xxx.xxx.xxx.xxx(xxx は十進数)

- 0x に続く十六進数
- マスクビット数
- [初期値]:-

[説明]

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

[ノート]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.4 インタフェースの MTU の設定

[書式]

```
ip interface mtu mtu0
ip pp mtu mtu1
ip tunnel mtu mtu2
no ip interface mtu [mtu0]
no ip pp mtu [mtu1]
no ip tunnel mtu [mtu2]
```

[設定値及び初期値]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.5 同一インタフェースに折り返すパケットを送信するか否かの設定

[書式]

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

[設定値及び初期値]

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

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

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

[説明]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.6 IP の静的経路情報の設定**[書式]**

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

[設定値及び初期値]

- *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
<i>name</i>	PAP/CHAP による名前

- *dhcp interface*

設定値	説明
<i>interface</i>	DHCP にて与えられるデフォルトゲートウェイを使う場合の、DHCP クライアントとして動作する LAN インタフェース名

- *tunnel tunnel_num* : トンネルインタフェースへの経路
- LOOPBACK インタフェース名、NULL インタフェース名
- [初期値]: -
- *parameter* : 以下のパラメータを空白で区切り複数設定可能
 - [設定値]:

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

設定値	説明
metric <i>metric</i>	メトリックの指定 <ul style="list-style-type: none"> • <i>metric</i> <ul style="list-style-type: none"> • メトリック値 (1..15) • 省略時は 1
hide	出力インターフェースが LAN インターフェース、または 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 <i>weight</i>	異なる経路間の比率を表す値 <ul style="list-style-type: none"> • <i>weight</i> <ul style="list-style-type: none"> • 経路への重み (0..2147483647) • 省略時は 1
keepalive <i>keepalive_id</i>	<i>gateway1</i> に到達性のあるときにだけ有効となる <ul style="list-style-type: none"> • <i>keepalive_id</i> <ul style="list-style-type: none"> • キープアライブの識別子 (通常モードは 1..6000; コンパクトモードは 1..1000)

- [初期値]: -

[説明]

IP の静的経路を設定する。

gateway のパラメータとしてフィルタ型経路を指定した場合には、記述されている順にフィルタを適用していき、適合したゲートウェイが選択される。

適合するゲートウェイが存在しない場合や、フィルタ型経路が指定されているゲートウェイが一つも記述されていない場合には、フィルタ型経路が指定されていないゲートウェイが選択される。

フィルタ型経路が指定されていないゲートウェイも存在しない場合には、その経路は存在しないものとして処理が継続される。

フィルタ型経路が指定されていないゲートウェイが複数記述された場合の経路の選択は、それらの経路を使用する時点でラウンドロビンにより決定される。

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

いずれの場合でも、*hide* キーワードが指定されているゲートウェイは、回線が接続している場合のみ有効で、回線が接続していない場合には評価されない。なお LOOPBACK インターフェース、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。

デプロイ時の状態および **cold start** コマンド実行後の本コマンドの設定値については「1.6 デプロイ時の設定値について」を参照してください。

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

[設定例]

- デフォルトゲートウェイを 192.168.0.1 とする。

```
# ip route default gateway 192.168.0.1
```

- PP1 で接続している相手のネットワークは 192.168.1.0/24 である。

```
# ip route 192.168.1.0/24 gateway pp 1
```

- マルチホーミングによる負荷分散を行う。デフォルトゲートウェイとして 2 経路持ち、PP1 には専用線 128k で、PP2 には専用線 64k で接続しており、かつ各専用線ダウン時の経路を無効としてパケットロスを防ぐ。

※ NAT 機能と専用線キープアライブの併用が必要となる。

```
# ip route default gateway pp 1 weight 2 hide gateway pp 2 weight 1 hide
```

- PP1 が有効な時には PP1 のみが使われる。PP1 がダウンすると PP2 が使われる。

```
# ip route 192.168.0.1/24 gateway pp 1 hide gateway pp 2 weight 0
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

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

[書式]

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

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

[設定値及び初期値]

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

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

- [初期値]: on

[説明]

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

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

[ノート]

ブリッジインタフェースは vRX VMware ESXi 版で指定可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

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

[書式]

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

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

[設定値及び初期値]

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

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

- [初期値]: on

[説明]

指定したインターフェースを使用中、DHCP で IP アドレスを取得したときにアドレスを取得したインターフェースの implicit なネットワーク経路を自動的に追加するか否かを設定する。
すでに DHCP で IP アドレスを取得しているインターフェースに対してこのコマンドの設定が変更された場合、次に DHCP で IP アドレスを取得した時点から新しい設定が反映される。

[ノート]

ブリッジインタフェースは vRX VMware ESXi 版で指定可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.9 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 パケットの始点アドレス
 - [設定値]:
 - IP アドレス
 - A.B.C.D (A~D: 0~255 もしくは*)
 - 上記表記で A~D を*とすると、該当する 8 ビット分についてはすべての値に対応する
 - 間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。
 - , を区切りとして複数設定することができる。FQDN と混合することも可能
 - 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ため、使用できない)
 - * から始まる FQDN は * より後ろの文字列を後方一致条件として判断する 例えば *.example.co.jp は www.example.co.jp、mail.example.co.jp などと一致する
 - , を区切りとして複数設定することができる。IP アドレスと混合することも可能
 - * (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
- 特殊指定

icmp-error	TYPE が 3、4、5、11、12、31、32 のいずれかである ICMP パケット
icmp-info	TYPE が 0、8~10、13~18、30、33~36 のいずれかである ICMP パケット
tcpsyn	SYN フラグの立っている tcp パケット
tcpfin	FIN フラグの立っている tcp パケット
tcprst	RST フラグの立っている tcp パケット
established	ACK フラグの立っている tcp パケット内から外への接続は許可するが、外から内への接続は拒否する機能
tcpflag=value/mask	TCP フラグの値と <i>mask</i> の値の論理積 (AND) が、 <i>value</i> に一致、または不一致である TCP パケット <i>value</i> と <i>mask</i> は 0x に続く十六進数で 0x0000~0xffff
tcpflag!=value/mask	
*	すべてのプロトコル

- 省略時は * と同じ。
- [初期値]: -
- *src_port_list*: *protocol* に、TCP(tcp/tcpsyn/tcpfin/tcprst/established/tcpflag)、UDP(udp) のいずれかが含まれる場合は、TCP/UDP のソースポート番号。*protocol* が ICMP(icmp) 単独の場合には、ICMP タイプ。
- [設定値]:
 - ポート番号、タイプを表す十進数
 - ポート番号を表すニーモニック (一部)

ニーモニック	ポート番号
ftp	20,21
ftpdata	20
telnet	23
smtp	25
domain	53
gopher	70
finger	79
www	80
pop3	110
sunrpc	111
ident	113
ntp	123
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 filter directed-broadcast**、**ip filter dynamic**、**ip filter set**、**ip forward filter**、**ip fragment remove df-bit**、**ip interface rip filter**、**ip interface secure filter**、および **ip route** コマンドで用いられる。

[ノート]

restrict-log 及び restrict-nolog を使ったフィルターは、回線が接続されている時だけ通せば十分で、そのために回線に発信するまでもないようなパケットに有効である。例えば、時計を合わせるための NTP パケットがこれに該当する。ICMP パケットに対して、ICMP タイプと ICMP コードをフィルターでチェックしたい場合には、*protocol* には 'icmp' だけを単独で指定する。*protocol* が 'icmp' 単独である場合のみ、*src_port_list* は ICMP タイプ、*dest_port_list* は ICMP コードと見なされる。*protocol* に 'icmp' と他のプロトコルを列挙した場合には *src_port_list* と *dest_port_list* の指定は TCP/UDP のポート番号と見なされ、ICMP パケットとの比較は行われぬ。また、*protocol* に 'icmp-error' や 'icmpinfo' を指定した場合には、*src_port_list* と *dst_port_list* の指定は無視される。*protocol* に '*' を指定するか、TCP/UDP を含む複数のプロトコルを列挙している場合には、*src_port_list* と *dest_port_list* の指定は TCP/UDP のポート番号と見なされ、パケットが TCP または UDP である場合のみポート番号がフィルターが比較される。パケットがその他のプロトコル (ICMP を含む) の場合には、*src_port_list* と *dest_port_list* の指定は存在しないものとしてフィルターと比較される。

src_addr および *dest_addr* に FQDN を指定することによって、固定 IP アドレスではないサーバーや 1 つの FQDN に対して複数の固定 IP アドレスを持つサーバーを対象にしたフィルタリングを行うことができる。FQDN を使用す

る場合、ルーター自身が DNS リカーシブサーバーとして動作し、ルーター配下の端末は、DNS サーバーとして本機を指定する必要がある。

指定した FQDN に一致する通信が発生した場合、設定した FQDN に該当する IP アドレスの情報が保持される。保持される期間は、**ip filter fqdn timer** コマンドで指定できる。

[設定例]

LAN1 で送受信される IPv4 ICMP ECHO/REPLY を pass-log で記録する

```
# ip lan1 secure filter in 1 2 100
# ip lan1 secure filter out 1 2 100
# ip filter 1 pass-log * * icmp 8
# ip filter 2 pass-log * * icmp 0
# ip filter 100 pass * *
```

LAN2 から送信される IPv4 Redirect のうち、"for the Host" だけを通さない

```
# ip lan2 secure filter out 1 100
# ip filter 1 reject * * icmp 5 1
# ip filter 100 pass * *
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.10 フィルタセットの定義

[書式]

```
ip filter set name direction filter_list [filter_list ...]
no ip filter set name [direction ...]
```

[設定値及び初期値]

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

設定値	説明
in	入力方向のフィルタ
out	出力方向のフィルタ

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

[説明]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.11 Source-route オプション付き IP パケットをフィルタアウトするか否かの設定

[書式]

```
ip filter source-route filter_out
no ip filter source-route [filter_out]
```

[設定値及び初期値]

- *filter_out*
 - [設定値]:

設定値	説明
on	フィルタアウトする
off	フィルタアウトしない

- [初期値]: on

[説明]

Source-route オプション付き IP パケットをフィルタアウトするか否かを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.12 ディレクテッドブロードキャストパケットをフィルタアウトするか否かの設定**[書式]**

```
ip filter directed-broadcast filter_out
ip filter directed-broadcast filter filter_num [filter_num ...]
no ip filter directed-broadcast
```

[設定値及び初期値]

- *filter_out*
 - [設定値]:

設定値	説明
on	フィルタアウトする
off	フィルタアウトしない

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

[説明]

終点 IP アドレスがディレクテッドブロードキャストアドレス宛になっている IP パケットをルーターが接続されているネットワークにブロードキャストするか否かを設定する。

on を指定した場合には、ディレクティッドブロードキャストパケットはすべて破棄する。

off を指定した場合には、ディレクティッドブロードキャストパケットはすべて通過させる。

filter を指定した場合には、**ip filter** コマンドで設定したフィルタでパケットを検査し、PASS フィルタにマッチした場合のみパケットを通過させる。

[ノート]

このコマンドでのチェックよりも、**ip interface wol relay** コマンドのチェックの方が優先される。**ip interface wol relay** コマンドでのチェックにより通過させることができなかったパケットのみが、このコマンドでのチェックを受ける。いわゆる smurf 攻撃を防止するためには on にしておく。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.13 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]: 始点アドレス
 - [初期値]: -
- *dstaddr*
 - [設定値]: 終点アドレス
 - [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/netmeeting
 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 (トリガー) を検出したら、それ以降 *in* キーワードと *out* キーワードの後に記述されたフィルターに該当するコネクションを通過させる。*in* キーワードはトリガーの方向に対して逆方向のアクセスを制御し、*out* キーワードは動的フィルターと同じ方向のアクセスを制御する。なお、**ip filter** コマンドの IP アドレスは無視される。*pass/reject* の引数も同様に無視される。プロトコルとして *tcp* や *udp* を指定した場合には、アプリケーションに固有な処理は実施されない。特定のアプリケーションを扱う必要がある場合には、アプリケーション名を指定する。

[設定例]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.14 動的フィルタのタイムアウトの設定

[書式]

```
ip filter dynamic timer option=timeout [option=timeout...]
no ip filter dynamic timer
```

[設定値及び初期値]

- *option* : オプション名
 - [設定値] :

設定値	説明
tcp-syn-timeout	SYN を受けてから設定された時間内に接続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接続を強制的に解放する
tcp-idle-time	設定された時間内に TCP 接続のデータが流れなければ接続を切断する
udp-idle-time	設定された時間内に UDP 接続のデータが流れなければ接続を切断する
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接続を切断する

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

[説明]

動的フィルタのタイムアウトを設定する。

[ノート]

本設定はすべての検査において共通に使用される。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.15 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.16 侵入検知機能の動作の設定

[書式]

```
ip interface intrusion detection direction [type] switch [option]
ip pp intrusion detection direction [type] switch [option]
ip tunnel intrusion detection direction [type] switch [option]
no ip interface intrusion detection direction [type] switch [option]
no ip pp intrusion detection direction [type] switch [option]
no ip tunnel intrusion detection direction [type] switch [option]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *direction*: 観察するパケット・接続の方向
 - [設定値]:

設定値	説明
in	インタフェースの内向き
out	インタフェースの外向き

- [初期値]: -
- *type*: 観察するパケット・接続の種類
 - [設定値]:

設定値	説明
ip	IP ヘッダ
ip-option	IP オプションヘッダ
fragment	フラグメント
icmp	ICMP
udp	UDP
tcp	TCP
ftp	FTP
winny	Winny
share	Share
default	設定していないものすべて

- [初期値]: -
- *switch*
 - [設定値]:

設定値	説明
on	実行する
off	実行しない

- [初期値]:
 - *type* を指定しないとき=off
 - *type* を指定したとき=on
- *option*
 - [設定値]:

設定値	説明
reject=on	不正なパケットを破棄する
reject=off	不正なパケットを破棄しない

- [初期値]: off

[説明]

指定したインタフェースで、指定された向きのパケットや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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.17 1 秒間に侵入検知情報を通知する頻度の設定

[書式]

```
ip interface intrusion detection notice-interval frequency
ip pp intrusion detection notice-interval frequency
ip tunnel intrusion detection notice-interval frequency
no ip interface intrusion detection notice-interval
no ip pp intrusion detection notice-interval
no ip tunnel intrusion detection notice-interval
```

[設定値及び初期値]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.18 重複する侵入検知情報の通知抑制の設定

[書式]

```
ip interface intrusion detection repeat-control time
ip pp intrusion detection repeat-control time
ip tunnel intrusion detection repeat-control time
no ip interface intrusion detection repeat-control
no ip pp intrusion detection repeat-control
no ip tunnel intrusion detection repeat-control
```

[設定値及び初期値]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.19 侵入検知情報の最大表示件数の設定**[書式]**

ip interface intrusion detection report num

ip pp intrusion detection report num

ip tunnel intrusion detection report num

no ip interface intrusion detection report

no ip pp intrusion detection report

no ip tunnel intrusion detection report

[設定値及び初期値]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.20 TCP セッションの MSS 制限の設定**[書式]**

ip interface tcp mss limit mss

ip pp tcp mss limit mss

ip tunnel tcp mss limit mss

no ip interface tcp mss limit [mss]

no ip pp tcp mss limit [mss]

no ip tunnel tcp mss limit [mss]

[設定値及び初期値]

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

設定値	説明
536..1460	MSS の最大長
auto	自動設定
off	設定しない

- [初期値]: auto

[説明]

インタフェースを通過する TCP セッションの MSS を制限する。インタフェースを通過する TCP パケットを監視し、*mss* オプションの値が設定値を越えている場合には、設定値に書き換える。キーワード *auto* を指定した場合には、インタフェースの MTU、もしくは PP インタフェースの場合で相手の MRU 値が分かる場合にはその MRU 値から計算した値に書き換える。

[ノート]

PPPoE 用の PP インタフェースに対しては、**pppoe tcp mss limit** コマンドでも TCP セッションの MSS を制限することができる。このコマンドと **pppoe tcp mss limit** コマンドの両方が有効な場合は、MSS はどちらかより小さな方の値に制限される。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.21 TCP ウィンドウ・スケール・オプションを変更する

[書式]

```
ip interface tcp window-scale sw
ip pp tcp window-scale sw
ip tunnel tcp window-scale sw
no ip interface tcp window-scale [...]
no ip pp tcp window-scale [...]
no ip tunnel tcp window-scale [...]
```

[設定値及び初期値]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.22 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.23 フィルタリングによるセキュリティの設定

[書式]

```
ip interface secure filter direction [filter_list...] [dynamic_filter_list...]
ip pp secure filter direction [filter_list...] [dynamic_filter_list...]
ip tunnel secure filter direction [filter_list...] [dynamic_filter_list...]
ip interface secure filter name set_name
```

```

ip pp secure filter name set_name
ip tunnel secure filter name set_name
no ip interface secure filter direction [filter_list]
no ip pp secure filter direction [filter_list]
no ip tunnel secure filter direction [filter_list]
no ip interface secure filter name [set_name]
no ip pp secure filter name [set_name]
no ip tunnel secure filter name [set_name]

```

[設定値及び初期値]

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

設定値	説明
in	受信したパケットのフィルタリング
out	送信するパケットのフィルタリング

- [初期値]: -
- *filter_list*
 - [設定値]: 空白で区切られたフィルタ番号の並び (静的フィルタと動的フィルタの数の合計として 300 個以内)
 - [初期値]: -
- *set_name*
 - [設定値]: フィルタ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を組み合わせ、インタフェースで送受信するパケットの種類を制限する

方向を指定する書式では、それぞれの方向に対して適用するフィルタ列をフィルタ番号で指定する。指定された番号のフィルタが順番に適用され、パケットにマッチするフィルタが見つければそのフィルタにより通過/破棄が決定する。それ以降のフィルタは調べられない。すべてのフィルタにマッチしないパケットは破棄される。

フィルタセットの名前を指定する書式では、指定されたフィルタセットが適用される。フィルタを調べる順序などは方向を指定する書式の方法に準ずる。定義されていないフィルタセットの名前が指定された場合には、フィルタは設定されていないものとして動作する。

[ノート]

フィルタリストを走査して、一致すると通過、破棄が決定する。

```

# ip filter 1 pass 192.168.0.0/24 *
# ip filter 2 reject 192.168.0.1
# ip lan1 secure filter in 1 2

```

この設定では、始点 IP アドレスが 192.168.0.1 であるパケットは、最初のフィルタ 1 で通過が決定してしまうため、フィルタ 2 での検査は行われず。そのため、フィルタ 2 は何も意味を持たない。フィルタリストを操作した結果、どのフィルタにも一致しないパケットは破棄される。

PP Anonymous で認証に RADIUS を利用する場合で、RADIUS サーバーから送られた Access-Response にアトリビュート 'Filter-Id' が付いていた場合には、その値に指定されたフィルタセットを適用し、**ip pp secure filter** コマンドの設定は無視される。

ただしアトリビュート "Filter-Id" が存在しない場合には、**ip pp secure filter** コマンドの設定がフィルタとして利用される。

LOOPBACK インタフェースと NULL インタフェースでは動的フィルタは使用できない。

NULL インタフェースで *direction* に 'in' は指定できない。
ブリッジインタフェースは vRX VMware ESXi 版で指定可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.24 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 <i>filter_num</i>	<i>filter_num</i> は ip filter コマンドで登録されたフィルタ番号

- [初期値]: -

[説明]

フォワーディングする IP パケットの内、*rule* に一致するものは DF ビットを 0 に書き換える。

[ノート]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.25 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
max-throughput	4
min-delay	8

- [初期値]: -
- *precedence*
- [設定値]:
 - *precedence* 値 (0..7)
 - *precedence* を省略した場合、PRECEDENCE 値は変更しない
- [初期値]: -

- *filter_num*
 - [設定値]: 静的フィルタの番号 (1..21474836)
 - [初期値]: -
- *filter_num_list*
 - [設定値]: 静的フィルタの番号 (1..21474836) の並び
 - [初期値]: -

[説明]

IP パケットを中継する場合に TOS フィールドを指定した値に書き換える。識別番号順にリストをチェックし、*filter_num* リストのフィルタを順次適用していく。そして、最初にマッチした IP フィルタが `pass`、`pass-log`、`pass-nolog`、`restrict`、`restrict-log`、`restrict-nolog` のいずれかであれば TOS フィールドが書き換えられる。

`reject`、`reject-log` または `reject-nolog` である場合は書き換えずに処理を終わる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.26 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 インタフェース名、ブリッジインタフェース名
 - [初期値]: -
- *proxyarp*
 - [設定値]:

設定値	説明
on	代理 ARP 動作をする
off	代理 ARP 動作をしない

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

[説明]

代理 ARP 動作をするか否か設定する。on を設定した時には、代理 ARP 動作を行う。この時利用する MAC アドレスは、LAN インタフェースの実 MAC アドレスとなる。ブリッジインタフェースを指定した時には、ブリッジインタフェースに收容された実 LAN インタフェースにおいて、代理 ARP 動作をするか否か設定する。この時利用する MAC アドレスは ARP を受信した実 LAN インタフェースの MAC アドレスとなる。

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

[ノート]

ブリッジインタフェースおよび *vrid* は vRX VMware ESXi 版で指定可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.27 ARP エントリの寿命の設定**[書式]**

```
ip arp timer timer [retry]
no ip arp timer [timer [retry]]
```

[設定値及び初期値]

- *timer*

- [設定値]: ARP エントリの寿命秒数 (30..32767)
- [初期値]: 1200
- *retry*
 - [設定値]: ARP リクエスト再送回数 (4..100)
 - [初期値]: 4

[説明]

ARP エントリの寿命を設定する。ARP 手順で得られた IP アドレスと MAC アドレスの組は ARP エントリとして記憶されるが、このコマンドで設定した時間だけ経過するとエントリは消される。ただし、エントリが消される前に再度 ARP 手順が実行され、その ARP に応答が無い場合にエントリは消される。

retry パラメーターで ARP リクエストの再送回数を設定できる。ARP リクエストの再送間隔は初回は 2 秒、その後は 1 秒である。

retry パラメーターについては、通常は初期値から変更する必要はない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.28 静的 ARP エントリの設定**[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 エントリを静的に設定する。このコマンドで設定された ARP エントリは、**show arp** コマンドで TTL が 'permanent' と表示され、常に有効となる。また、**clear arp** コマンドを実行してもエントリは消えない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.29 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 インタフェース名
 - [初期値]: -
- *len*
 - [設定値]: キュー長 (0..10000)
 - [初期値]:
 - 40

[説明]

ARP が解決していないホストに対してパケットを送信しようとした時に、ARP が解決するか、タイムアウトにより ARP が解決できないことが確定するまで、インタフェース毎に送信を保留しておくことのできるパケットの最大数を設定する。

0 を設定するとパケットを保留しなくなるため、例えば ARP が解決していない相手に ping を実行すると必ず最初の 1 パケットは失敗するようになる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.30 ARP エントリの変化をログに残すか否かの設定

[書式]

ip interface arp log switch**no ip interface arp log [switch]**

[設定値及び初期値]

- *switch*

- [設定値]:

設定値	説明
on	記録する
off	記録しない

- [初期値]: off

[説明]

ARP エントリの変更をログに記録するか否かを設定する

[ノート]

show log | grep ARP: を実行することによって、過去の ARP エントリ履歴を確認することができる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.31 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、数字が大きいくほど優先度が高い。

implicit 経路が動的経路制御プロトコルで得られた経路または **ip route** コマンドで設定された静的な経路と食い違う場合には、優先度が高い方が採用される。静的な経路と優先度が同じ場合には、静的な経路が優先される。

動的経路制御プロトコルで得られた経路と優先度が同じ場合には、時間的に先に採用された経路が有効となる。

なお、本コマンドで implicit 経路の優先度を変更しても、その時点で既にルーティングテーブルに登録されている implicit 経路の優先度は変更されない。

[ノート]

implicit 経路とは、IP アドレスを設定したインタフェースが有効な状態になったときに暗黙のうちに登録されるそのインタフェースを経由する経路のことである。例えば、IP アドレスを設定した LAN インタフェースがリンクアップ状態のときには、設定した IP アドレスとネットマスクの組み合わせから決定されるネットワークアドレスが、その LAN インタフェースを経由する implicit 経路として登録されている。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.32 フローテーブルの各エントリの寿命を設定する

[書式]

ip flow timer protocol time**no ip flow timer protocol [time]**

[設定値及び初期値]

- *protocol*: 寿命を指定するプロトコル

- [設定値]:

設定値	説明
tcp	TCP パケット
udp	UDP パケット
icmp	ICMP パケット
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の寿命をプロトコル毎に設定する。
 FIN/RST の通過したエントリには 'slow' が適用される。
 NAT や動的フィルタを使用している場合には、それらのエントリの寿命が適用される。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.33 フローテーブルのエントリー数の設定

[書式]

```
ip flow limit limit
no ip flow limit [limit]
```

[設定値及び初期値]

- *limit*
 - [設定値]:
 - 制限値 (10..1000000) (通常モード)
 - 制限値 (10..131072) (コンパクトモード)
 - [初期値]:
 - 1000000 (通常モード)
 - 131072 (コンパクトモード)

[説明]

IPv4 ファストパスまたは IPv6 ファストパスのそれぞれで使用可能なフローテーブルのエントリー数を設定する。
 ファストパス機能使用時でも本制限値を超える分のフローはノーマルパスで処理される。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.1.34 フラグメントパケットを再構成するために保持しておく時間を設定

[書式]

```
ip reassembly hold-time sec
no ip reassembly hold-time [sec]
```

[設定値及び初期値]

- *sec*
 - [設定値]:

設定値	説明
秒数 (1..255)	フラグメントパケットを再構成するために保持しておく時間

- [初期値]: 15 秒

[説明]

IPv4 のフラグメントパケットを再構成するために保持しておく時間。
設定した時間が経過しても再構成ができなかった場合、保持していたパケットは破棄される。
コマンド実行時にすでに保持していたパケットについては変更しない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.2 PP 側の設定

5.2.1 PP 側 IP アドレスの設定

[書式]

```
ip pp remote address ip_address
ip pp remote address dhcp [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]:-
- 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]:-
- *interface*
 - [設定値]:
 - DHCP クライアントとして動作する LAN インタフェース名
 - 省略時は lan1
 - [初期値]:-

[説明]

選択されている相手の PP 側の IP アドレスを設定する。
dhcp を設定した場合は、自分自身が DHCP サーバーとして動作している必要がある。自分で管理している DHCP スコープの中から、IP アドレスを割り当てる。
dhcp を設定した場合は、*interface* で指定した LAN インタフェースが DHCP クライアントとして IP アドレスを取得し、そのアドレスを PP 側に割り当てる。取得できなかった場合は、0.0.0.0 を割り当てる。

[設定例]

ルーター A 側が

```
no ip pp remote address
ppp ipcp ipaddress on
```

と設定し、接続するルーター B 側が

```
ip pp remote address yyy.yyy.yyy.yyy
```

と設定している場合には、実際のルーター A の PP 側の IP アドレスは "yyy.yyy.yyy.yyy" になる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.2.2 リモート IP アドレスプールの設定

[書式]

```
ip pp remote address pool ip_address [ip_address...]
ip pp remote address pool ip_address-ip_address
ip pp remote address pool dhcp
```

```
ip pp remote address pool dhcpc [interface]
no ip pp remote address pool
```

[設定値及び初期値]

- *ip_address*
 - [設定値]: anonymous のためにプールする IP アドレス
 - [初期値]: -
- *ip_address-ip_address*
 - [設定値]: IP アドレスの範囲
 - [初期値]: -
- *dhcp*: 自分自身の DHCP サーバー機能を利用することを示すキーワード
 - [初期値]: -
- *dhcpc*: DHCP クライアントを利用することを示すキーワード
 - [初期値]: -
- *interface*
 - [設定値]:
 - DHCP クライアントとして動作する LAN インタフェース名
 - 省略時は lan1
 - [初期値]: -

[説明]

anonymous で相手に割り当てるための IP アドレスプールを設定する。PP として *anonymous* が選択された場合のみ有効である。

dhcp を設定した場合は、自分自身が DHCP サーバーとして動作している必要がある。自分で管理している DHCP スコープの中から、IP アドレスを割り当てる。

dhcpc を設定した場合は、*interface* で指定した LAN インタフェースが DHCP クライアントとして IP アドレス情報のみを取得し、そのアドレスを割り当てる。取得できなかった場合は、0.0.0.0 を割り当てる。

[ノート]

ip_address として設定できる数は 1040 である。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.2.3 PP 経由のキープアライブの時間間隔の設定

[書式]

```
pp keepalive interval interval [retry-interval=retry-interval] [count=count] [time=time]
no pp keepalive interval [interval [count]]
```

[設定値及び初期値]

- *interval*
 - [設定値]: キープアライブパケットを送出する時間間隔[秒] (1..65535)
 - [初期値]: 30
- *retry-interval*
 - [設定値]:
 - キープアライブパケットの確認に一度失敗した後の送信間隔[秒] (1..65535)
 - キープアライブパケットが確認できれば、送信間隔はまた *interval* に戻る
 - [初期値]: 1
- *count*
 - [設定値]: この回数連続して応答がなければ相手側のルーターをダウンしたと判定する (3..100)
 - [初期値]: 6
- *time*
 - [設定値]:
 - キープアライブパケットの確認に失敗するようになってから回線断と判断するまでの時間[秒] ($(interval + 1) \cdot 65535$)
 - *count* パラメータとは同時には指定できない
 - [初期値]: -

[説明]

PP インタフェースでのキープアライブパケットの送信間隔と、回線断と判定するまでの再送回数および時間を設定する。

送信したキープアライブパケットに対して返事が返って来ている間は *interval* で指定した間隔でキープアライブパケットを送信する。一度、返事が確認できなかった時には送信間隔が *retry-interval* パラメータの値に変更される。*count* パラメータに示された回数だけ連続して返事が確認できなかった時には回線断と判定する。

回線断判定までの時間を *time* パラメータで指定した場合には、少なくとも指定した時間の間、キープアライブパケットの返事が連続して確認できない時に回線断と判定する。

[ノート]

time パラメータを指定した場合には、その値はキープアライブの間隔と再送回数によって再計算されるため、設定値とは異なる値が **show config** で表示されることがある。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.2.4 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 インタフェースが送出先となるよう設定される必要がある。

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

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

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

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.2.5 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 インタフェースで共通に用いられる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.3 RIP の設定

5.3.1 RIP を使用するか否かの設定

[書式]

```
rip use use
no rip use [use]
```

[設定値及び初期値]

- *use*
 - [設定値]:

設定値	説明
on	RIP を使用する
off	RIP を使用しない

- [初期値]: off

[説明]

RIP を使用するか否かを設定する。この機能を off にすると、すべてのインタフェースに対して RIP パケットを送信することはなくなり、受信した RIP パケットは無視される。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.3.2 RIP に関して信用できるゲートウェイの設定

[書式]

```
ip interface rip trust gateway [except] gateway [gateway...]
ip pp rip trust gateway [except] gateway [gateway...]
ip tunnel rip trust gateway [except] gateway [gateway...]
no ip interface rip trust gateway [[except] gateway [gateway...]]
no ip pp rip trust gateway [[except] gateway [gateway...]]
no ip tunnel rip trust gateway [[except] gateway [gateway...]]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *gateway*
 - [設定値]: IP アドレス
 - [初期値]: -

[説明]

RIP に関して信用できる、あるいは信用できないゲートウェイを設定する。

`except` キーワードを指定していない場合には、列挙したゲートウェイを信用できるゲートウェイとし、それらからの RIP だけを受信する。

`except` キーワードを指定した場合は、列挙したゲートウェイを信用できないゲートウェイとし、それらを除いた他のゲートウェイからの RIP だけを受信する。

`gateway` は 10 個まで指定可能。

[ノート]

信用できる、あるいは信用できないゲートウェイは設定されておらず、すべてのホストからの RIP を信用できるものとして扱う。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.3.3 RIP による経路の優先度の設定

[書式]

```
rip preference preference [invalid-route-reactivate=switch]
no rip preference [preference [invalid-route-reactivate=switch]]
```

[設定値及び初期値]

- *preference*
 - [設定値]: 1 以上の数値
 - [初期値]: 1000
- *switch*
 - [設定値]:

設定値	説明
on	無効となった RIP 由来の経路を削除しない
off	無効となった RIP 由来の経路を削除する

- [初期値]: off

[説明]

RIP により得られた経路の優先度を設定する。経路の優先度は 1 以上の数値で表され、数字が大きい程優先度が高い。スタティックと RIP など複数のプロトコルで得られた経路が食い違う場合には、優先度が高い方が採用される。優先度が同じ場合には時間的に先に採用された経路が有効となる。

RIP で他のルーターから経路を受信しているとき、スタティックや OSPF など RIP より優先度が高く設定されたルーティングプロトコルで同じ経路を受信した場合、通常 RIP により受信した経路は無効となって削除されるが、`invalid-route-reactivate` オプションを `on` で指定している場合、優先度が高い経路が消滅したときに無効になっていた RIP 由来の経路を再有効化する。

[ノート]

スタティック経路の優先度は 10000 で固定である。

`invalid-route-reactivate` オプションを *on* で指定しているとき、再有効化した経路を RIP の発信元が広告しなくなっても当該経路がルーティングテーブル上に残り続けることがあるため、`invalid-route-reactivate` オプションは *off* にすることが望ましい。

なお、上記のルーティングテーブルに残った経路は、RIP の使用を停止することで削除できる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.3.4 RIP パケットの送信に関する設定

[書式]

```
ip interface rip send send [version version [broadcast]]
```

```
ip pp rip send send [version version [broadcast]]
```

```
ip tunnel rip send send [version version [broadcast]]
```

```
no ip interface rip send [send...]
```

```
no ip pp rip send [send...]
```

```
no ip tunnel rip send [send...]
```

[設定値及び初期値]

• *interface*

- [設定値]: LAN インタフェース名
- [初期値]: -

• *send*

- [設定値]:

設定値	説明
on	RIP パケットを送信する
off	RIP パケットを送信しない

- [初期値]:

- off (トンネルインタフェースの場合)
- on (その他のインタフェースの場合)

• *version*

- [設定値]: 送信する RIP のバージョン (1,2)
- [初期値]: 1 (トンネルインタフェース以外の場合)

• *broadcast*

- [設定値]: `ip interface address` コマンドで指定したブロードキャスト IP アドレス
- [初期値]: -

[説明]

指定したインタフェースに対し、RIP パケットを送信するか否かを設定する。

"`version version`" で送信する RIP のバージョンを指定できる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.3.5 RIP パケットの受信に関する設定

[書式]

```
ip interface rip receive receive [version version [version]]
```

```
ip pp rip receive receive [version version [version]]
```

```
ip tunnel rip receive receive [version version [version]]
```

```
no ip interface rip receive [receive...]
```

```
no ip pp rip receive [receive...]
```

```
no ip tunnel rip receive [receive...]
```

[設定値及び初期値]

• *interface*

- [設定値]: LAN インタフェース名

- [初期値]: -
- *receive*
- [設定値]:

設定値	説明
on	RIP パケットを受信する
off	RIP パケットを受信しない

- [初期値]:
 - off (トンネルインタフェースの場合)
 - on (その他のインタフェースの場合)
- *version*
 - [設定値]: 受信する RIP のバージョン (1,2)
 - [初期値]: 12 (トンネルインターフェース以外の場合)

[説明]

指定したインタフェースに対し、RIP パケットを受信するか否かを設定する。
 "version *version*" で受信する RIP のバージョンを指定できる。指定しない場合は、RIP1/2 とともに受信する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.3.6 RIP のフィルタリングの設定

[書式]

```
ip interface rip filter direction filter_list
ip pp rip filter direction filter_list
ip tunnel rip filter direction filter_list
no ip interface rip filter direction [filter_list]
no ip pp rip filter direction filter_list
no ip tunnel rip filter direction filter_list
```

[設定値及び初期値]

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

設定値	説明
in	受信した RIP のフィルタリング
out	送信する RIP のフィルタリング

- [初期値]: -
- *filter_list*
 - [設定値]: 空白で区切られた静的フィルタ番号の並び (100 個以内)
 - [初期値]: -

[説明]

インタフェースで送受信する RIP のフィルタリングを設定する。
ip filter コマンドで設定されたフィルタの始点 IP アドレスが、送受信する RIP の経路情報にマッチする場合は、フィルタが **pass** であればそれを処理し、**reject** であればその経路情報だけを破棄する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.3.7 RIP で加算するホップ数の設定

[書式]

```
ip interface rip hop direction hop
ip pp rip hop direction hop
```

```
ip tunnel rip hop direction hop
no ip interface rip hop direction hop
no ip pp rip hop direction hop
no ip tunnel rip hop direction hop
```

[設定値及び初期値]

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

設定値	説明
in	受信した RIP に加算する
out	送信する RIP に加算する

- [初期値]: -
- *hop*
 - [設定値]: 加算する値 (0..15)
 - [初期値]: 0

[説明]

インタフェースで送受信する RIP に加算するホップ数を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.3.8 RIP2 での認証の設定

[書式]

```
ip interface rip auth type type
ip pp rip auth type type
ip tunnel rip auth type type
no ip interface rip auth type [type]
no ip pp rip auth type [type]
no ip tunnel rip auth type [type]
```

[設定値及び初期値]

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

設定値	説明
text	テキスト型の認証を行う

- [初期値]: -

[説明]

RIP2 を使用する場合のインタフェースでの認証の設定をする。text の場合はテキスト型の認証を行う。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.3.9 RIP2 での認証キーの設定

[書式]

```
ip interface rip auth key hex_key
ip pp rip auth key hex_key
ip tunnel rip auth key hex_key
ip interface rip auth key text text_key
ip pp rip auth key text text_key
ip tunnel rip auth key text text_key
```

```
no ip interface rip auth key
no ip pp rip auth key
no ip tunnel rip auth key
no ip interface rip auth key text
no ip pp rip auth key text
no ip tunnel rip auth key text
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *hex_key*
 - [設定値]: 十六進数の列で表現された認証キー
 - [初期値]: -
- *text_key*
 - [設定値]: 文字列で表現された認証キー
 - [初期値]: -

[説明]

RIP2 を使用する場合のインタフェースの認証キーを設定する。

[設定例]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.3.10 RIP2 での広告動作モードの設定

[書式]

```
rip advertise mode mode
no rip advertise mode [mode]
```

[設定値及び初期値]

- *mode*
 - [設定値]:

設定値	説明
1	RIP の送信インタフェースが属するネットワークアドレスと広告する経路の宛先ネットワークアドレスが一致し、サブネットマスクが異なる場合は、その経路を広告しない。
2	RIP の送信インタフェースが属するネットワークアドレスと広告する経路の宛先ネットワークアドレスが一致し、サブネットマスクが異なる場合は、その経路を広告する。

- [初期値]: 1

[説明]

RIP2 で RIP 送信インタフェースが属するネットワークアドレスと広告する経路の宛先ネットワークアドレスが一致し、サブネットマスクが異なる場合、当該経路の広告動作を *mode* の設定値によって変更する。

本コマンドに対応していないリビジョンでは、*mode* の設定値が 1 のときの動作をする。

RIP1 の動作には影響はない。

[適用モデル]

vRX VMware ESXi 版

5.3.11 回線切断時の経路保持の設定

[書式]

```
ip pp rip hold routing rip_hold
```

no ip pp rip hold routing [*rip_hold*]

[設定値及び初期値]

- *rip_hold*
 - [設定値]:

設定値	説明
on	回線が切断されても RIP による経路を保持し続ける
off	回線が切断されたら RIP による経路を破棄する

- [初期値]: off

[説明]

PP インタフェースから RIP で得られた経路を、回線が切断された場合に保持し続けるかどうかを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.3.12 回線接続時の PP 側の RIP の動作の設定

[書式]

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

[設定値及び初期値]

- *rip_action*
 - [設定値]:

設定値	説明
interval	ip pp rip connect interval コマンドで設定された時間間隔で RIP を送出する
update	経路情報が変わった場合にのみ RIP を送出する
none	RIP を送出しない

- [初期値]: update

[説明]

選択されている相手について回線接続時に RIP を送出する条件を設定する。

[設定例]

```
# ip pp rip connect interval 60
# ip pp rip connect send interval
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.3.13 回線接続時の PP 側の RIP 送出の時間間隔の設定

[書式]

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

[設定値及び初期値]

- *time*
 - [設定値]: 秒数 (30..21474836)
 - [初期値]: 30

[説明]

選択されている相手について回線接続時に RIP を送出する時間間隔を設定する。

ip pp rip send と **ip pp rip receive** コマンドが on、**ip pp rip connect send** コマンドが interval の時に有効である。

[設定例]

```
# ip pp rip connect interval 60
# ip pp rip connect send interval
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.3.14 回線切断時の PP 側の RIP の動作の設定

[書式]

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

[設定値及び初期値]

- *rip_action*
 - [設定値]:

設定値	説明
none	回線切断時に RIP を送出しない
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
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.3.15 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
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.3.16 バックアップ時の RIP の送信元インタフェース切り替えの設定

[書式]

```
ip pp rip backup interface switch
no ip pp rip backup interface
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	切り替える
off	切り替えない

- [初期値]: off

[説明]

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

[ノート]

両者の違いは、送信元の IP アドレスの違いとなって現れる。off のときには、バックアップ元のインタフェースのアドレスが選ばれ、on のときには、バックアップ先のインタフェースのアドレスが選ばれる。なお、どちらの場合にも、バックアップ回線を通じて RIP が送信される。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.3.17 RIP で強制的に経路を広告する**[書式]**

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

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *ip-address/netmask*
 - [設定値]: 強制的に広告したい経路のネットワークアドレスとネットマスク長、または 'default'
 - [初期値]: -
- *metric*
 - [設定値]: 広告する際のメトリック値 (1..15)
 - [初期値]: 1

[説明]

設定した経路が経路テーブルに存在しない場合でも、指定されたインタフェースに対し、RIP で経路を強制的に広告する。経路として 'default' を指定した場合にはデフォルト経路が広告される。

[設定例]

LAN1 側に、LAN2 の一部のホストだけを広告する。

```
ip lan1 address 192.168.0.1/24
ip lan2 address 192.168.1.1/24
```

```
rip use on
rip filter rule with-netmask
ip lan1 rip send on version 2
ip lan1 rip receive on version 2
```

```
ip filter 1 reject 192.168.1.0/24
ip filter 100 pass *
ip lan1 rip filter out 1 100
```

```
ip lan1 rip force-to-advertise 192.168.1.28/30
ip lan1 rip force-to-advertise 192.168.1.100/32
ip lan1 rip force-to-advertise 192.168.1.101/32
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.3.18 RIP2 でのフィルタの比較方法

[書式]

```
rip filter rule rule
no rip filter rule [rule]
```

[設定値及び初期値]

- *rule*
 - [設定値]:

設定値	説明
address-only	ネットワークアドレスだけを比較対象とする
with-netmask	RIP2 の場合、ネットワークアドレスとネットマスクを比較対象とする

- [初期値]: address-only

[説明]

RIP フィルターで、設定されたフィルターと RIP エントリの内容の比較方法を設定する。

rip filter rule コマンド	プロトコル	比較方法
address-only	RIP1	ネットマスク型のフィルターは範囲指定と解釈され、RIP エントリのアドレス部がその範囲に入っているかどうかを比較する。
	RIP2	
with-netmask	RIP1	ネットマスク型のフィルターの、アドレスとネットマスク、RIP エントリのアドレス、ネットマスクと一致するかどうかを比較する。
	RIP2	

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.3.19 RIP のタイマーを調整する

[書式]

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

[設定値及び初期値]

- *update*
 - [設定値]: 定期的な広告の送信間隔 (10..60 (秒))
 - [初期値]: 30 秒
- *invalid*
 - [設定値]: 広告を受け取れなくなってから経路を削除するまでの時間 (30..360 (秒))
 - [初期値]: update×6 (180 秒)
- *holddown*
 - [設定値]: 経路が削除されたときにメトリック 16 で経路を広告する時間 (20..240 (秒))
 - [初期値]: update×4 (120 秒)

[説明]

RIP のタイマー値を設定する。

update、*invalid*、*holddown* の各値の間には以下の不等式が成立している必要がある。

$update \times 3 \leq invalid \leq update \times 6$
 $update \times 2 \leq holddown \leq update \times 4$

[ノート]

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

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

PP インタフェース以外は該当するコマンドがないため、常に **rip timer** コマンドの設定値が有効である。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.4 VRRP の設定

5.4.1 インタフェース毎の VRRP の設定

[書式]

```
ip interface vrrp vrid ip_address [priority=priority] [preempt=preempt] [auth=auth] [advertise-interval=time1] [down-interval=time2]
no ip interface vrrp vrid [vrid...]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *vrid*
 - [設定値]: VRRP グループ ID (1..255)
 - [初期値]: -
- *ip_address*
 - [設定値]: 仮想ルーターの IP アドレス
 - [初期値]: -
- *priority*
 - [設定値]: 優先度 (1..254)
 - [初期値]: 100
- *preempt*: プリエンプトモード
 - [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: on
- *auth*
 - [設定値]: テキスト認証文字列 (8 文字以内)
 - [初期値]: -
- *time1*
 - [設定値]: VRRP 広告の送信間隔 (1..60 秒)
 - [初期値]: 1
- *time2*
 - [設定値]: マスターがダウンしたと判定するまでの時間 (3..180 秒)
 - [初期値]: 3

[説明]

指定した VRRP グループを利用することを設定する。

同じ VRRP グループに所属するルーターの間では、VRID および仮想ルーターの IP アドレスを一致させておかななくてはならない。これらが食い違った場合の動作は予測できない。

auth パラメータを指定しない場合には、認証なしとして動作する。

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

[ノート]

priority および *preempt* パラメータの設定は、仮想ルーターの IP アドレスとして自分自身の LAN インタフェースに付与されているアドレスを指定している場合には無視される。この場合、優先度は最高の 255 となり、常にプリエンプトモードで動作する。

[適用モデル]

vRX VMware ESXi 版

5.4.2 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 tunnel tunnel_num
ip interface vrrp shutdown trigger vrid route network [nexthop]
no ip interface vrrp shutdown trigger vrid interface
no ip interface vrrp shutdown trigger vrid pp peer_num
no ip interface vrrp shutdown trigger vrid tunnel tunnel_num
no ip interface vrrp shutdown trigger vrid route network
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *vrid*
 - [設定値]: VRRP グループ ID (1..255)
 - [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: tunnel インターフェース番号
 - [初期値]: -
- *network*
 - [設定値]:
 - ネットワークアドレス
 - IP アドレス/マスク長
 - default
 - [初期値]: -
- *nexthop*
 - [設定値]:
 - インタフェース名
 - IP アドレス
 - [初期値]: -

[説明]

設定した VRRP グループでマスタールーターとして動作している場合に、指定した条件によってシャットダウンすることを設定する。

形式	説明
LAN インタフェース形式	指定した LAN インタフェースがリンクダウンするか、あるいは lan keepalive でダウンが検知されると、シャットダウンする。
pp 形式	指定した相手先情報番号に該当する回線で通信できなくなった場合にシャットダウンする。通信できなくなるとは、ケーブルが抜けるなどレイヤ 1 が落ちた場合と、以下の場合である。 <ul style="list-style-type: none"> 回線が専用線である時には、LCP キープアライブによって通信相手が落ちたと判断した場合 pp keepalive use 設定によりダウンが検出された場合
tunnel 形式	指定した tunnel インターフェースが以下の条件によりダウンした場合にシャットダウンする。 <ul style="list-style-type: none"> IPsec トンネルで、ipsec ike keepalive use 設定によりダウンが検出された場合 L2TP/IPsec、L2TPv3、L2TPv3/IPsec のいずれかのトンネルで、l2tp keepalive use 設定によりダウンが検出された場合 IPIP トンネルで、ipip keepalive use 設定によりダウンが検出された場合
route 形式	指定した経路が経路テーブルに存在しないか、 <i>nexthop</i> で指定したインタフェースもしくは IP アドレスで指定するゲートウェイに向いていない場合に、シャットダウンする。 <i>nexthop</i> を省略した場合には、経路がどのような先に向いていても存在する限りはシャットダウンしない。

[適用モデル]

vRX VMware ESXi 版

5.5 バックアップの設定

5.5.1 プロバイダ接続がダウンした時に PP バックアップする接続先の指定

[書式]

```
pp backup none
pp backup pp peer_num [ipsec-fast-recovery=action]
pp backup interface ip_address
pp backup tunnel tunnel_num
no pp backup
```

[設定値及び初期値]

- none : バックアップ動作しない
 - [初期値] : none
- peer_num
 - [設定値] : バックアップ先として PP を使用する場合の相手先情報番号
 - [初期値] : -
- action : バックアップから復帰した直後に SA の再構築を実施するか否か
 - [設定値] :

設定値	説明
on	再構築する
off	再構築しない

- [初期値] : off
- interface
 - [設定値] : バックアップ先として使用する LAN インタフェース
 - [初期値] : -
- ip_address

- [設定値]: ゲートウェイの IP アドレス
- [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -

[説明]

PP インタフェースが切断されたときにバックアップするインタフェースを指定する。バックアップ先のインタフェースが PP インタフェースの場合には、`ipsec-fast-recovery` オプションを設定できる。このオプションで `on` を設定したときには、バックアップから復帰した直後に IPsec の SA をすぐに再構築するため、IPsec の通信が可能になるまでの時間を短縮できる。

[ノート]

このコマンドは PP インタフェースごとに設定できる。PP インタフェースの切断を検知するために `pp always-on` コマンドで `on` を設定する必要がある。専用線の場合には `pp always-on` コマンドの代わりに、`pp keepalive use lcp-echo` コマンドを使用する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.5.2 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.5.3 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]: -
- *interface*
 - [設定値]: バックアップ対象の LAN インタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]: バックアップとして pp を使用する場合の相手先情報番号

- [初期値]: -
- *backup_interface*
 - [設定値]: バックアップとして使用する LAN インタフェース
 - [初期値]: -
- *ip_address*
 - [設定値]: ゲートウェイの IP アドレス
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -

[初期設定]

```
lan backup interface none
```

[説明]

指定する LAN インタフェースに対して、LAN 経由でのプロバイダ接続がダウンした場合にバックアップするインタフェース情報を設定する。

[ノート]

バックアップ動作のためには、LAN 経由での接続のダウンを検知するために **lan keepalive use** コマンドでの設定が併せて必要である。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.5.4 バックアップからの復帰待ち時間の設定

[書式]

```
lan backup recovery time interface time
no lan backup recovery time interface [time]
```

[設定値及び初期値]

- *interface*
 - [設定値]: バックアップ対象の LAN インタフェース名
 - [初期値]: -
- *time*
 - [設定値]:
 - 秒数 (1..21474836)
 - off
 - [初期値]: off

[説明]

指定する LAN インタフェースに対して、バックアップから復帰する場合に、すぐに復帰させるか、設定された時間だけ待ってから復帰するかを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.5.5 LAN 経由のキープアライブを使用するか否かの設定

[書式]

```
lan keepalive use interface icmp-echo dest_ip [option=value...] [dest_ip [option=value...]...]
lan keepalive use interface arp dest_ip [dest_ip...]
lan keepalive use interface icmp-echo dest_ip [option=value...] [dest_ip [option=value...]...] arp dest_ip [dest_ip...]
lan keepalive use interface off
no lan keepalive use interface [...]
```

[設定値及び初期値]

- *interface*
 - [設定値]: バックアップ対象の LAN インタフェース名
 - [初期値]: -
- *dest_ip*
 - [設定値]: キープアライブ確認先の IP アドレス

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

<i>option</i>	<i>value</i>	説明
upwait	ミリ秒	アップ検知のための許容応答時間 (1..10000)
downwait	ミリ秒	ダウン検知のための許容応答時間 (1..10000)
length	バイト	ICMP Echo パケットの長さ (64-1500)

- [初期値]: -

[説明]

指定する LAN インタフェースに対して、キープアライブ動作を行うか否かを設定する。icmp-echo を指定すれば ICMP Echo/Reply を用い、arp を指定すれば ARP Request/Reply を用いる。併記することで併用も可能である。

[ノート]

icmp-echo で確認する IP アドレスに対する経路は、バックアップをする LAN インタフェースに向くことが必要である。

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

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.5.6 LAN 経由のキープアライブの時間間隔の設定

[書式]

```
lan keepalive interval interface interval [count]
no lan keepalive interval interface
```

[設定値及び初期値]

- *interface*
 - [設定値]: バックアップ対象の LAN インタフェース名
 - [初期値]: -
- *interval*
 - [設定値]: キープアライブパケットを送出する時間間隔 (1..65535)
 - [初期値]: 30
- *count*
 - [設定値]: ダウン検出を判定する回数 (3..100)
 - [初期値]: 6

[説明]

指定する LAN インタフェースに対して、キープアライブパケットの送出間隔とダウン検出を判定する回数を設定する。count に設定した回数だけ連続して応答パケットを検出できない場合に、ダウンと判定する。

一度応答が返ってこないのを検出したら、その後のキープアライブパケットの送出間隔は 1 秒に短縮される。そのため、デフォルトの設定値の場合でもダウン検出に要する時間は 35 秒程度である。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.5.7 LAN 経由のキープアライブのログをとるか否かの設定

[書式]

```
lan keepalive log interface log
no lan keepalive log interface
```

[設定値及び初期値]

- *interface*

- [設定値]: バックアップ対象の LAN インタフェース名
- [初期値]: -
- *log*
 - [設定値]:

設定値	説明
on	ログをとる
off	ログをとらない

- [初期値]: off

[説明]

キープアライブパケットのログをとるか否かを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.5.8 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 (通常モードは 1..6000; コンパクトモードは 1..1000)
 - [初期値]: -
- *kind*: 監視方式
 - [設定値]:

設定値	説明
icmp-echo	ICMP Echo を使用する

- [初期値]: -
- *interval*
 - [設定値]: キープアライブの送信間隔秒数 (1..65535)
 - [初期値]: -
- *count*
 - [設定値]: 到達性がないと判断するまでに送信する回数 (3..100)
 - [初期値]: -
- *gateway*: 複数指定可 (10 個以内)
 - [設定値]:
 - IP アドレス
 - xxx.xxx.xxx.xxx (xxx は十進数)
 - *dhcp interface*

設定値	説明
interface	DHCP にて与えられるデフォルトゲートウェイを使う場合の、DHCP クライアントとして動作する LAN インタフェース名

- [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)

option	value	説明
downwait	秒数	到達性がないと判断するまでの待機秒数 (1..1000000)
length	バイト	ICMP Echo パケットの長さ (64-1500)
local-address	IP アドレス	始点 IP アドレス
ipsec-refresh	セキュリティ・ゲートウェイの識別子	DOWN→UP または UP→DOWN に状態が変化した場合に、指定のセキュリティ・ゲートウェイに属する SA を強制的に更新 (複数指定する場合はカンマで区切る)
ipsec-refresh-up	セキュリティ・ゲートウェイの識別子	DOWN→UP に状態が変化した場合のみ、指定のセキュリティ・ゲートウェイに属する SA を強制的に更新 (複数指定する場合はカンマで区切る)
ipsec-refresh-down	セキュリティ・ゲートウェイの識別子	UP→DOWN に状態が変化した場合のみ、指定のセキュリティ・ゲートウェイに属する SA を強制的に更新 (複数指定する場合はカンマで区切る)
gateway-selection-rule	head	ICMP Echo パケットを送信する際、該当する経路に複数のゲートウェイが指定されていても、必ず最初に指定されたゲートウェイへ送出する
	normal	ICMP Echo パケットを送信する際、該当する経路に複数のゲートウェイが指定されていたら、通常の規則に従い送出ゲートウェイを選択する

- [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・ゲートウェイの識別子 3 に属する SA を強制的に更新させる。

```
# ip route 172.16.0.0/24 gateway pp 10 keepalive 1 gateway pp 11 weight 0
# ip keepalive 1 icmp-echo 5 5 172.16.0.1 ipsec-refresh-up=3
```

ネットワークバックアップ機能を利用して、IP キープアライブ 1 がダウンしたのをトリガにして経路 172.16.224.0/24 を活性化させる。

```
# ip route 172.16.112.0/24 gateway null keepalive 1 gateway 172.16.0.1 weight 0
# ip route 172.16.224.0/24 gateway 172.16.112.1 keepalive 2
```



```
# ip keepalive 1 icmp-echo 5 5 192.168.100.101
# ip keepalive 2 icmp-echo 5 5 172.16.112.1 gateway-selection-rule=normal
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.6 受信パケット統計情報の設定

5.6.1 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 インタフェース名
 - [初期値]: -
- *sw*
 - [設定値]:

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

- [初期値]: off

[説明]

指定したインタフェースで受信したパケットの統計情報を記録するか否かを設定する。送信元 IP アドレスと送信先 IP アドレスの組み合わせが同じパケットについて、それぞれのパケット数とオクテット数を統計情報として記録する。最大で 3 つのインタフェースについての統計情報を同時に記録することができる。

[ノート]

ファストパスで処理されたパケットは統計情報には記録されない。
off に設定すると統計情報がクリアされ、記録が停止する。
on に設定したときにもそれまでの統計情報はいったんクリアされ、新たに記録が開始する。
NAT 設定があるインタフェースで動作させる場合に表示される IP アドレスは、NAT 変換可能な状態であれば NAT 変換後の IP アドレスが表示され、NAT 変換ができない状態であれば NAT 変換前の IP アドレスが表示される。
受信フィルタで破棄される通信については記録されない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.6.2 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 インタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号、省略時は選択されている相手先情報番号

- [初期値]: -
- *tunnel_num*
 - [設定値]: トンネル番号、省略時は選択されているトンネル番号
 - [初期値]: -

[説明]

受信したパケットの統計情報をクリアする。
interface を省略したときは、全インタフェースの統計情報をクリアする。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.6.3 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 インタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号、省略時は選択されている相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネル番号、省略時は選択されているトンネル番号
 - [初期値]: -

[説明]

受信したパケットの統計情報を表示する。
interface を省略したときは、全インタフェースの統計情報を表示する。

[表示例]

```
# show ip traffic list lan1
Source IP      Destination IP  Packets  Octets
-----
192.168.200.2  133.176.200.1  1411449  1326237183
133.176.200.3  133.176.200.226  12080    2115561
192.168.200.1  192.168.100.1   802      97211
192.168.200.2  133.176.200.3   17       17348
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.6.4 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 インタフェース名
 - [初期値]: -
- *value*
 - [設定値]: 統計情報に記録するパケットの最大分類数 (64..5000)

- [初期値]: 64

[説明]

指定したインタフェースにおいて、統計情報として記録する受信パケットの分類数を指定する。

[ノート]

送信元 IP アドレスと送信先 IP アドレスの組み合わせによってパケットを分類する。

記録されている受信パケット情報の分類数が最大値に達した場合、それ以降で新規に分類された受信パケット情報は記録されない。

このコマンドで設定を行なうとそれまでの統計情報はクリアされる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.7 パケット転送フィルターの設定

5.7.1 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
pp 番号	PP インタフェース
tunnel 番号	TUNNEL インタフェース

- [初期値]: -
- *filter_id*
 - [設定値]: **ip filter** コマンドの識別子
 - [初期値]: -
- *keepalive_id*
 - [設定値]: **ip keepalive** コマンドの識別子
 - [初期値]: -

[説明]

パケット転送フィルターを定義する。

id パラメータは、複数のパケット転送フィルターをグループ化するための識別子である。

同じインタフェースに対して複数のパケット転送フィルターを設定するときには、それらのすべてに対して、同じ番号を指定しなければならない。

order パラメータは、評価の順番を示すもので、若い番号を持つものほど優先的に採用される。

filter_id パラメータとしては、**ip filter** コマンドの識別子を最大 16 個まで指定できる。

複数の識別子を指定したときには、前にあるものが優先的に評価される。

前から順に対応する **ip filter** コマンドを調べ、パケットの内容と合致すれば、その **ip filter** コマンドの設定を採用する。

ip filter コマンドの動作が **reject** であれば、パケットを転送せずに破棄し、そうでなければ、*gateway* パラメータで指定したゲートウェイにパケットを転送する。

keepalive_id には、**ip keepalive** コマンドの識別子を指定する。

ここで指定した IP キープアライブの結果が **down** であれば、このゲートウェイを使用しない。

つまり、該当する **ip filter** コマンドがあったとしても、該当しなかったものとして扱う。
なお、実際に動作させるためには、**ip interface forward filter** コマンドも設定する必要がある。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

5.7.2 インタフェースへのパケット転送フィルターの適用

[書式]

```
ip interface forward filter id
ip pp forward filter id
ip tunnel forward filter id
ip local forward filter id
no ip interface forward filter [id]
no ip pp forward filter [id]
no ip tunnel forward filter [id]
no ip local forward filter [id]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *id*
 - [設定値]: **ip forward filter** コマンドで指定したパケット転送フィルターの識別子 (1..255)
 - [初期値]: -

[説明]

インタフェースにパケット転送フィルターを適用する。
指定したインタフェースで受信したパケットを、指定したパケット転送フィルターの設定と比較し、転送先のゲートウェイを決定する。

ip local forward filter コマンドは自分自身が送信するパケットを対象にするときに指定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

第 6 章

イーサネットフィルタの設定

6.1 フィルタ定義の設定

[書式]

```
ethernet filter num kind src_mac [dst_mac [offset byte_list]]
```

```
ethernet filter num kind type [scope] [offset byte_list]
```

```
no ethernet filter num [kind ...]
```

[設定値及び初期値]

- *num*
 - [設定値]: 静的フィルタの番号 (1..512)
 - [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を設定する。本コマンドで設定されたフィルタは、**ethernet lan filter** コマンドで用いられる。

通常型のフィルタでは、始点 MAC アドレス、終点 MAC アドレスなどで送受信するイーサネットフレームにフィルタを適用する。

dhcp-bind 型のフィルタでは、以下のイーサネットフレームにフィルタを適用する。対象とならないイーサネットフレームはフィルタに合致しないものとして扱う。

- 以下のいずれかに該当する、IPv4 パケットの場合
- イーサネットタイプが IPv4(0x0800)
- PPPoE 環境で、イーサネットタイプが PPPoE データフレーム (0x8864)、プロトコル ID が IPv4(0x0800)

イーサネットフレームの始点 MAC アドレスと始点 IP アドレスの組が、対象となる DHCP スコープで予約されているならフィルタに合致するとみなす。

- イーサネットタイプが、以下のいずれかの場合
- ARP(0x0806)
- RARP(0x8035)
- PPPoE 制御パケット (0x8863)
- MAC レイヤ制御パケット (0x8808)

イーサネットフレームの始点 MAC アドレスが、対象となる DHCP スコープで予約されているならフィルタに合致するとみなす。

dhcp-not-bind 型のフィルタでは、以下のイーサネットフレームにフィルタを適用する。対象とならないイーサネットフレームはフィルタに合致しないものとして扱う。

- イーサネットタイプが IPv4(0x0800) である場合

イーサネットフレームの始点 IP アドレスが、対象となる DHCP スコープのリース範囲に含まれていて、かつ、dhcp-not-bind 型のフィルタでは始点 MAC アドレスが DHCP スコープで予約されていないときにフィルタに合致するとみなす。

dhcp-bind、dhcp-not-bind 型のフィルタで対象とする DHCP スコープは、*scope* パラメータで指定する。

scope パラメータとしては DHCP スコープ番号を指定することもできるし、DHCP スコープが定義されているサブネットに含まれる IP アドレスで指定することもできる。IP アドレスで DHCP スコープを指定する場合には、複数の DHCP スコープが該当する時には、その中で最も長いネットマスク長を持つ DHCP スコープを選択する。

scope パラメータを省略した場合には、フィルタが適用されるインタフェースで使用される DHCP スコープがすべて対象となる。

dhcp-bind、dhcp-not-bind 型のフィルタが DHCP リレーエージェントとして動作しているルーターに設定された場合、DHCP サーバーから DHCP スコープとその DHCP スコープにおけるクライアントの予約情報を取得し、フィルタの適用時に参照する。DHCP サーバーからの DHCP スコープおよび予約情報の取得は、DHCP メッセージをリレーする際、DHCP メッセージのオプション部に予約情報を書き込んで通知することにより行なわれる。

[ノート]

dhcp-bind、dhcp-not-bind 型のフィルタでは、イーサネットフレームの始点 MAC アドレスや始点 IP アドレスを用いてフィルタの判定をするため、**ethernet lan filter** コマンドでは通常 in 方向にのみ使用することになる。

out 方向の場合、始点 MAC アドレスはルーター自身の MAC アドレスになるため、DHCP の予約情報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 型フィルタは、予約もしくはアドレスがリースされているクライアントだけを通過させる、という形になるため、通常は *pass* 等と組み合わせて使用する。一方、dhcp-not-bind 型フィルタは、予約もしくはアドレスがリースされていないクライアントを破棄する、という形になるため、通常は *reject* 等と組み合わせて使用することになる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

6.2 インタフェースへの適用の設定

[書式]

```
ethernet interface filter dir list
no ethernet interface filter dir [list]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、トンネルインタフェース名
 - [初期値]: -
- *dir*
 - [設定値]:

設定値	説明
in	LAN 側から入ってくるパケットのフィルタリング
out	LAN 側に出ていくパケットのフィルタリング

- [初期値]: -
- *list*
 - [設定値]: 空白で区切られた静的フィルタ番号の並び (512 個以内)
 - [初期値]: -

[説明]

LAN、および、トンネルインタフェースを通るパケットについて、**ethernet filter** コマンドによるパケットのフィルタを組み合わせ、通過するパケットの種類を制限する。

[ノート]

LAN インタフェース名には、物理 LAN インタフェースで使用するインタフェースを指定できる。

interface にトンネルインタフェースを指定した場合、指定したインタフェースがブリッジインタフェースに収容されているときだけ、フィルターが適用される。

トンネルインタフェースは vRX VMware ESXi 版で指定可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

6.3 イーサネットフィルタの状態の表示

[書式]

```
show status ethernet filter type [scope]
```

[設定値及び初期値]

- *type*
 - [設定値]:

設定値	説明
dhcp-bind	指定された DHCP スコープで予約設定されているホスト

- [初期値]: -
- *scope*
 - [設定値]: スコープ番号 (1..65535)
 - [初期値]: -

[説明]

イーサネットフィルタの情報を表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

第 7 章

PPP の設定

7.1 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.2 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

設定値	説明
mschap-v2	MSCHAP Version2 による認証を受け入れる

- [初期値]: 認証を受け入れない

[説明]

相手からの PPP 認証要求を受け入れるかどうかを設定する。発信時には常に適用される。anonymous でない着信の場合には発番号により PP が選択されてから適用される。anonymous での着信時には、発番号による PP の選択が失敗した場合に適用される。

このコマンドで認証を受け入れる設定になっていても、**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 インタフェース毎のコマンドである。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.3 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.4 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 インタフェース毎のコマンドである。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

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

[書式]

```
pp auth multi connect prohibit prohibit
no pp auth multi connect prohibit [prohibit]
```

[設定値及び初期値]

- *prohibit*
 - [設定値]:

設定値	説明
on	禁止する
off	禁止しない

- [初期値]: off

[説明]

pp auth username コマンドで登録した同一 *username* を持つ相手からの二重接続を禁止するか否かを設定する。

[ノート]

定額制プロバイダを営む場合に便利である。ユーザ管理を RADIUS で行う場合には、二重接続の禁止は RADIUS サーバーの方で対処する必要がある。
anonymous が選択された場合のみ有効である。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.6 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には *time* に設定された時間間隔を待

った後に再接続の要求を行い、正常な通信終了時には直ちに再接続の要求を行う。*switch* が on に設定されている場合には、*time* の設定が有効となる。*time* が設定されていない場合、*time* は 60 になる。

switch を off に設定した時点で切断処理が行われる。

[ノート]

PP インタフェース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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.7 LCP 関連の設定

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

[書式]

```
ppp lcp acfc acfc
```

```
no ppp lcp acfc [acfc]
```

[設定値及び初期値]

- *acfc*

- [設定値]:

設定値	説明
on	用いる
off	用いない

- [初期値]: off

[説明]

選択されている相手について[PPP,LCP]の Address and Control Field Compression オプションを用いるか否かを設定する。

[ノート]

on を設定していても相手に拒否された場合は用いない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.7.2 Magic Number オプション使用の設定

[書式]

```
ppp lcp magicnumber magicnumber
```

```
no ppp lcp magicnumber [magicnumber]
```

[設定値及び初期値]

- *magicnumber*

- [設定値]:

設定値	説明
on	用いる
off	用いない

- [初期値]: on

[説明]

選択されている相手について[PPP,LCP]の Magic Number オプションを用いるか否かを設定する。

[ノート]

on を設定していても相手に拒否された場合は用いない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.7.3 Maximum Receive Unit オプション使用の設定

[書式]

```
ppp lcp mru mru [length]
no ppp lcp mru [mru [length]]
```

[設定値及び初期値]

- *mru*
 - [設定値]:

設定値	説明
on	用いる
off	用いない

- [初期値]: on
- *length*: MRU の値
 - [設定値]:
 - 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.7.4 Protocol Field Compression オプション使用の設定

[書式]

```
ppp lcp pfc pfc
no ppp lcp pfc [pfc]
```

[設定値及び初期値]

- *pfc*
 - [設定値]:

設定値	説明
on	用いる
off	用いない

- [初期値]: off

[説明]

選択されている相手について[PPP,LCP]の Protocol Field Compression オプションを用いるか否かを設定する。

[ノート]

on を設定していても相手に拒否された場合は用いない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.7.5 lcp-restart パラメータの設定

[書式]

```
ppp lcp restart time
no ppp lcp restart [time]
```

[設定値及び初期値]

- *time*

- [設定値]: ミリ秒 (20..10000)
- [初期値]: 3000

[説明]

選択されている相手について[PPP,LCP]の `configure-request`、`terminate-request` の再送時間を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.7.6 lcp-max-terminate パラメータの設定

[書式]

```
ppp lcp maxterminate count
no ppp lcp maxterminate [count]
```

[設定値及び初期値]

- `count`
 - [設定値]: 回数 (1..10)
 - [初期値]: 2

[説明]

選択されている相手について[PPP,LCP]の `terminate-request` の送信回数を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.7.7 lcp-max-configure パラメータの設定

[書式]

```
ppp lcp maxconfigure count
no ppp lcp maxconfigure [count]
```

[設定値及び初期値]

- `count`
 - [設定値]: 回数 (1..10)
 - [初期値]: 10

[説明]

選択されている相手について[PPP,LCP]の `configure-request` の送信回数を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.7.8 lcp-max-failure パラメータの設定

[書式]

```
ppp lcp maxfailure count
no ppp lcp maxfailure [count]
```

[設定値及び初期値]

- `count`
 - [設定値]: 回数 (1..10)
 - [初期値]: 10

[説明]

選択されている相手について[PPP,LCP]の `configure-nak` の送信回数を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.7.9 Configure-Request をすぐに送信するか否かの設定

[書式]

```
ppp lcp silent switch
no ppp lcp silent [switch]
```

[設定値及び初期値]

- `switch`
 - [設定値]:

設定値	説明
on	PPP/LCP で、回線接続直後の Configure-Request の送信を、相手から Configure-Request を受信するまで遅らせる
off	PPP/LCP で、回線接続直後に Configure-Request を送信する

- [初期値]: off

[説明]

PPP/LCP で、回線接続後 Configure-Request をすぐに送信するか、あるいは相手から Configure-Request を受信するまで遅らせるかを設定する。通常は回線接続直後に Configure-Request を送信して構わないが、接続相手によってはこれを遅らせた方がよいものがある。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.8 PAP 関連の設定

7.8.1 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]の authenticate-request の再送時間を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.8.2 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]の authenticate-request の送信回数を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.9 CHAP 関連の設定

7.9.1 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]の challenge の再送時間を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.9.2 chap-max-challenge パラメータの設定

[書式]

```
ppp chap maxchallenge count
no ppp chap maxchallenge [count]
```

[設定値及び初期値]

- *count*
 - [設定値]: 回数 (1..10)
 - [初期値]: 10

[説明]

選択されている相手について[PPP,CHAP]challenge の送信回数を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.10 IPCP 関連の設定

7.10.1 Van Jacobson Compressed TCP/IP 使用の設定

[書式]

```
ppp ipcp vjc compression
no ppp ipcp vjc [compression]
```

[設定値及び初期値]

- *compression*
 - [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: off

[説明]

選択されている相手について[PPP,IPCP] Van Jacobson Compressed TCP/IP を使用するか否かを設定する。

[ノート]

on を設定していても相手に拒否された場合は用いない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.10.2 PP 側 IP アドレスのネゴシエーションの設定

[書式]

```
ppp ipcp ipaddress negotiation
no ppp ipcp ipaddress [negotiation]
```

[設定値及び初期値]

- *negotiation*
 - [設定値]:

設定値	説明
on	ネゴシエーションする
off	ネゴシエーションしない

- [初期値]: off

[説明]

選択されている相手について PP 側 IP アドレスのネゴシエーションをするか否かを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.10.3 ipcp-restart パラメータの設定

[書式]

```
ppp ipcp restart time
no ppp ipcp restart [time]
```

[設定値及び初期値]

- *time*
 - [設定値]: ミリ秒 (20..10000)
 - [初期値]: 3000

[説明]

選択されている相手について[PPP,IPCP]の configure-request、 terminate-request の再送時間を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.10.4 ipcp-max-terminate パラメータの設定

[書式]

```
ppp ipcp maxterminate count
no ppp ipcp maxterminate [count]
```

[設定値及び初期値]

- *count*
 - [設定値]: 回数 (1..10)
 - [初期値]: 2

[説明]

選択されている相手について[PPP,IPCP]の terminate-request の送信回数を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.10.5 ipcp-max-configure パラメータの設定

[書式]

```
ppp ipcp maxconfigure count
no ppp ipcp maxconfigure [count]
```

[設定値及び初期値]

- *count*
 - [設定値]: 回数 (1..10)
 - [初期値]: 10

[説明]

選択されている相手について[PPP,IPCP]の configure-request の送信回数を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.10.6 ipcp-max-failure パラメータの設定

[書式]

```
ppp ipcp maxfailure count
no ppp ipcp maxfailure [count]
```

[設定値及び初期値]

- *count*
 - [設定値]: 回数 (1..10)
 - [初期値]: 10

[説明]

選択されている相手について[PPP,IPCP]の configure-nak の送信回数を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.10.7 WINS サーバーの IP アドレスの設定

[書式]

wins server *server1* [*server2*]**no wins server** [*server1* [*server2*]]

[設定値及び初期値]

- *server1*、*server2*
 - [設定値]: IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))
 - [初期値]: -

[説明]

WINS (Windows Internet Name Service) サーバーの IP アドレスを設定する。

[ノート]

IPCP の MS 拡張オプションおよび DHCP でクライアントに渡すための WINS サーバーの IP アドレスを設定する。ルーターはこのサーバーに対し WINS クライアントとしての動作は一切行わない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.10.8 IPCP の MS 拡張オプションを使うか否かの設定

[書式]

ppp ipcp msex *msex***no ppp ipcp msex** [*msex*]

[設定値及び初期値]

- *msex*
 - [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: off

[説明]

選択されている相手について、[PPP,IPCP]の MS 拡張オプションを使うか否かを設定する。

IPCP の Microsoft 拡張オプションを使うように設定すると、DNS サーバーの IP アドレスと WINS(Windows Internet Name Service) サーバーの IP アドレスを、接続した相手である Windows マシンに渡すことができる。渡すための DNS サーバーや WINS サーバーの IP アドレスはそれぞれ、**dns server** コマンドおよび **wins server** コマンドで設定する。

off の場合は、DNS サーバーや WINS サーバーのアドレスを渡されても受け取らない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.10.9 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

設定値	説明
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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.11 MSCBCP 関連の設定

7.11.1 mscbcpr-restart パラメータの設定

[書式]

```
ppp mscbcpr restart time
no ppp mscbcpr restart [time]
```

[設定値及び初期値]

- *time*
 - [設定値] : ミリ秒 (20..10000)
 - [初期値] : 1000

[説明]

選択されている相手について[PPP, MSCBCP]の request/Response の再送時間を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.11.2 mscbcpr-maxretry パラメータの設定

[書式]

```
ppp mscbcpr maxretry count
no ppp mscbcpr maxretry [count]
```

[設定値及び初期値]

- *count*
 - [設定値] : 回数 (1..30)
 - [初期値] : 30

[説明]

選択されている相手について[PPP, MSCBCP]の request/Response の再送回数を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.12 CCP 関連の設定

7.12.1 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

設定値	説明
cstac	Stac LZS で圧縮する (接続相手が Cisco ルーターの場合)
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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.12.2 ccp-restart パラメータの設定**[書式]**

```
ppp ccp restart time
no ppp ccp restart [time]
```

[設定値及び初期値]

- *time*
 - [設定値]: ミリ秒 (20..10000)
 - [初期値]: 3000

[説明]

選択されている相手について[PPP,CCP]の *configure-request*、*terminate-request* の再送時間を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.12.3 ccp-max-terminate パラメータの設定**[書式]**

```
ppp ccp maxterminate count
no ppp ccp maxterminate [count]
```

[設定値及び初期値]

- *count*
 - [設定値]: 回数 (1..10)
 - [初期値]: 2

[説明]

選択されている相手について[PPP,CCP]の *terminate-request* の送信回数を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.12.4 ccp-max-configure パラメータの設定**[書式]**

```
ppp ccp maxconfigure count
no ppp ccp maxconfigure [count]
```

[設定値及び初期値]

- *count*

- [設定値]: 回数 (1..10)
- [初期値]: 10

[説明]

選択されている相手について[PPP,CCP]の `configure-request` の送信回数を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.12.5 ccp-max-failure パラメータの設定

[書式]

```
ppp ccp maxfailure count
no ppp ccp maxfailure [count]
```

[設定値及び初期値]

- `count`
 - [設定値]: 回数 (1..10)
 - [初期値]: 10

[説明]

選択されている相手について[PPP,CCP]の `configure-nak` の送信回数を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.13 IPV6CP 関連の設定

7.13.1 IPV6CP を使用するか否かの設定

[書式]

```
ppp ipv6cp use use
no ppp ipv6cp use [use]
```

[設定値及び初期値]

- `use`
 - [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: on

[説明]

選択されている相手について IPV6CP を使用するか否かを選択する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.14 BACP 関連の設定

7.14.1 bacp-restart パラメータの設定

[書式]

```
ppp bacp restart time
no ppp bacp restart [time]
```

[設定値及び初期値]

- `time`
 - [設定値]: ミリ秒 (20..10000)
 - [初期値]: 3000

[説明]

選択されている相手について[PPP,BACP]の `configure-request`、`terminate-request` の再送時間を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.14.2 bacp-max-terminate パラメータの設定

[書式]

```
ppp bacp maxterminate count
no ppp bacp maxterminate [count]
```

[設定値及び初期値]

- *count*
 - [設定値]: 回数 (1..10)
 - [初期値]: 2

[説明]

選択されている相手について[PPP,BACP]の terminate-request の送信回数を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.14.3 bacp-max-configure パラメータの設定

[書式]

```
ppp bacp maxconfigure count
no ppp bacp maxconfigure [count]
```

[設定値及び初期値]

- *count*
 - [設定値]: 回数 (1..10)
 - [初期値]: 10

[説明]

選択されている相手について[PPP, BACP]の configure-request の送信回数を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.14.4 bacp-max-failure パラメータの設定

[書式]

```
ppp bacp maxfailure count
no ppp bacp maxfailure [count]
```

[設定値及び初期値]

- *count*
 - [設定値]: 回数 (1..10)
 - [初期値]: 10

[説明]

選択されている相手について[PPP,BACP]の configure-nak の送信回数を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.15 BAP 関連の設定

7.15.1 bap-restart パラメータの設定

[書式]

```
ppp bap restart time
no ppp bap restart [time]
```

[設定値及び初期値]

- *time*
 - [設定値]: ミリ秒 (20..10000)
 - [初期値]: 1000

[説明]

選択されている相手について[PPP,BAP]の `configure-request`、`terminate-request` の再送時間を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.15.2 bap-max-retry パラメータの設定

[書式]

`ppp bap maxretry count`

`no ppp bap maxretry [count]`

[設定値及び初期値]

- `count`
 - [設定値]: 再送回数 (1..30)
 - [初期値]: 30

[説明]

選択されている相手について[PPP,BAP]の最大再送回数を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

7.16 PPPoE 関連の設定

7.16.1 PPPoE で使用する LAN インタフェースの指定

[書式]

`pppoe use interface`

`no pppoe use`

[設定値及び初期値]

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

[説明]

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

[適用モデル]

vRX VMware ESXi 版

7.16.2 アクセスコンセントレータ名の設定

[書式]

`pppoe access concentrator name`

`no pppoe access concentrator`

[設定値及び初期値]

- `name`
 - [設定値]: アクセスコンセントレータの名前を表す文字列 (7bit US-ASCII)
 - [初期値]: -

[説明]

選択されている相手について PPPoE で接続するアクセスコンセントレータの名前を設定する。接続できるアクセスコンセントレータが複数ある場合に、どのアクセスコンセントレータに接続するのかを指定するために使用する。

[適用モデル]

vRX VMware ESXi 版

7.16.3 セッションの自動接続の設定

[書式]

`pppoe auto connect switch`

`no pppoe auto connect`

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	自動接続する
off	自動接続しない

- [初期値]: on

[説明]

選択されている相手に対して、PPPoE のセッションを自動で接続するか否かを設定する。

[適用モデル]

vRX VMware ESXi 版

7.16.4 セッションの自動切断の設定**[書式]**

```
pppoe auto disconnect switch
no pppoe auto disconnect
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	自動切断する
off	自動切断しない

- [初期値]: on

[説明]

選択されている相手に対して、PPPoE のセッションを自動で切断するか否かを設定する。

[適用モデル]

vRX VMware ESXi 版

7.16.5 PADI パケットの最大再送回数の設定**[書式]**

```
pppoe padi maxretry times
no pppoe padi maxretry
```

[設定値及び初期値]

- *times*
 - [設定値]: 回数 (1..10)
 - [初期値]: 5

[説明]

PPPoE プロトコルにおける PADI パケットの最大再送回数を設定する。

[適用モデル]

vRX VMware ESXi 版

7.16.6 PADI パケットの再送時間の設定**[書式]**

```
pppoe padi restart time
no pppoe padi restart
```

[設定値及び初期値]

- *time*
 - [設定値]: ミリ秒 (20..10000)
 - [初期値]: 3000

[説明]

PPPoE プロトコルにおける PADI パケットの再送時間を設定する。

[適用モデル]

vRX VMware ESXi 版

7.16.7 PADR パケットの最大再送回数の設定

[書式]

pppoe padr maxretry *times*

no pppoe padr maxretry

[設定値及び初期値]

- *times*
 - [設定値]: 回数 (1..10)
 - [初期値]: 5

[説明]

PPPoE プロトコルにおける PADR パケットの最大再送回数を設定する。

[適用モデル]

vRX VMware ESXi 版

7.16.8 PADR パケットの再送時間の設定

[書式]

pppoe padr restart *time*

no pppoe padr restart

[設定値及び初期値]

- *time*
 - [設定値]: ミリ秒 (20..10000)
 - [初期値]: 3000

[説明]

PPPoE プロトコルにおける PADR パケットの再送時間を設定する。

[適用モデル]

vRX VMware ESXi 版

7.16.9 PPPoE セッションの切断タイマの設定

[書式]

pppoe disconnect time *time*

no pppoe disconnect time

[設定値及び初期値]

- *time*
 - [設定値]:

設定値	説明
1..21474836	秒数
off	タイマを設定しない

- [初期値]: off

[説明]

選択されている相手に対して、タイムアウトにより PPPoE セッションを自動切断する時間を設定する。

[ノート]

LCP と NCP パケットは監視対象外。

[適用モデル]

vRX VMware ESXi 版

7.16.10 サービス名の指定

[書式]

pppoe service-name *name*
no pppoe service-name

[設定値及び初期値]

- *name*
 - [設定値]: サービス名を表す文字列 (7bit US-ASCII、255 文字以内)
 - [初期値]: -

[説明]

選択されている相手について PPPoE で要求するサービス名を設定する。
 接続できるアクセスコンセントレータが複数ある場合に、要求するサービスを提供することが可能なアクセスコンセントレータを選択して接続するために使用する。

[適用モデル]

vRX VMware ESXi 版

7.16.11 TCP パケットの MSS の制限の有無とサイズの指定

[書式]

pppoe tcp mss limit *length*
no pppoe tcp mss limit

[設定値及び初期値]

- *length*
 - [設定値]:

設定値	説明
1240..1452	データ長
auto	MSS を MTU の値に応じて制限する
off	MSS を制限しない

- [初期値]: auto

[説明]

PPPoE セッション上で TCP パケットの MSS(Maximum Segment Size) を制限するか否かを設定する。

[ノート]

このコマンドと **ip interface tcp mss limit** コマンドの両方が有効な場合は、MSS はどちらかより小さな方の値に制限される。

[適用モデル]

vRX VMware ESXi 版

7.16.12 ルーター側には存在しない PPPoE セッションを強制的に切断するか否かの設定

[書式]

pppoe invalid-session forced close *sw*
no pppoe invalid-session forced close

[設定値及び初期値]

- *sw*
 - [設定値]:

設定値	説明
on	ルーター側には存在しない PPPoE セッションを強制的に切断する
off	ルーター側には存在しない PPPoE セッションを強制的に切断しない

- [初期値]: on

[説明]

ルーター側には存在しない PPPoE セッションを強制的に切断するか否かを設定します。

[適用モデル]

vRX VMware ESXi 版

第 8 章

DHCP の設定

本機は DHCP(*1) 機能として、DHCP サーバー機能、DHCP リレーエージェント機能、DHCP クライアント機能を実装しています。

DHCP 機能の利用により、基本的なネットワーク環境の自動設定を実現します。

DHCP クライアント機能は Windows 等の OS に実装されており、これらと本機の DHCP サーバー機能、DHCP リレーエージェント機能を組み合わせることにより DHCP クライアントの基本的なネットワーク環境の自動設定を実現します。

ルーターが DHCP サーバーとして機能するか DHCP リレーエージェントとして機能するか、どちらとしても機能させないかは **dhcp service** コマンドにより設定します。現在の設定は、**show status dhcp** コマンドにより知ることができます。

DHCP サーバー機能は、DHCP クライアントからのコンフィギュレーション要求を受けて IP アドレスの割り当て (リース) や、ネットマスク、DNS サーバーの情報等を提供します。

割り当てる IP アドレスの範囲とリース期間は **dhcp scope** コマンドにより設定されたものが使用されます。

IP アドレスの範囲は複数の設定が可能であり、それぞれの範囲を DHCP スコープ番号で管理します。DHCP クライアントからの設定要求があると DHCP サーバーは DHCP スコープの中で未割り当ての IP アドレスを自動的に通知します。なお、特定の DHCP クライアントに特定の IP アドレスを固定的にリースする場合には、**dhcp scope** コマンドで定義したスコープ番号を用いて **dhcp scope bind** コマンドで予約します。予約の解除は **no dhcp scope bind** コマンドで行います。IP アドレスのリース期間には時間指定と無期限の両方が可能であり、これは **dhcp scope** コマンドの **expire** および **maxexpire** キーワードのパラメータで指定します。

リース状況は **show status dhcp** コマンドにより知ることができます。DHCP クライアントに通知する DNS サーバーの IP アドレス情報は、**dns server** コマンドで設定されたものを使用します。

DHCP リレーエージェント機能は、ローカルセグメントの DHCP クライアントからの要求を、予め設定されたリモートのネットワークセグメントにある DHCP サーバーへ転送します。リモートセグメントの DHCP サーバーは **dhcp relay server** コマンドで設定します。DHCP サーバーが複数ある場合には、**dhcp relay select** コマンドにより選択方式を指定することができます。

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

(*1)Dynamic Host Configuration Protocol; RFC1541 , RFC2131

8.1 DHCP サーバー・リレーエージェント機能

8.1.1 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

8.1.2 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

8.1.3 リースする IP アドレスの重複をチェックするか否かの設定

[書式]

```
dhcp duplicate check check1 check2
no dhcp duplicate check
```

[設定値及び初期値]

- *check1* : LAN 内を対象とするチェックの確認用待ち時間
 - [設定値] :

設定値	説明
1..1000	ミリ秒
off	LAN 内を対象とするチェックを行わない

- [初期値] : 100
- *check2* : LAN 外 (DHCP リレーエージェント経由) を対象とするチェックの確認用待ち時間
 - [設定値] :

設定値	説明
1..3000	ミリ秒
off	LAN 外 (DHCP リレーエージェント経由) を対象とするチェックを行わない

- [初期値] : 500

[説明]

DHCP サーバーとして機能する場合、IP アドレスを DHCP クライアントにリースする直前に、その IP アドレスを使っているホストが他にいないことをチェックするか否かを設定する。

[ノート]

LAN 内のスコープに対しては ARP を、DHCP リレーエージェント経由のスコープに対しては PING を使ってチェックする。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

8.1.4 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。

netmask は/16 から/32 まで設定できる

[ノート]

同一ネットワークの DHCP スコープを複数設定できる。

複数の DHCP スコープで同一の IP アドレスを含めることはできない。IP アドレス範囲にネットワークアドレス、ブロードキャストアドレスを含む場合、割り当て可能アドレスから除外される。

DHCP リレーエージェントを経由しない DHCP クライアントに対して *gateway* キーワードによる設定パラメータが省略されている場合にはルーター自身の IP アドレスを通知する。

expire の設定値は *maxexpire* の設定値以下でなければならない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

8.1.5 DHCP 予約アドレスの設定

[書式]

```

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

```

[設定値及び初期値]

- *scope_num*
 - [設定値]: スコープ番号 (1..65535)
 - [初期値]:-
- *ip_address*
 - [設定値]:

設定値	説明
XXX.XXX.XXX.XXX	(xxx は十進数) 予約する IP アドレス
*	割り当てる IP アドレスを指定しない

- [初期値]: -
- *type*: Client-Identifier オプションの *type* フィールドを決定する
- [設定値]:

設定値	説明
text	0x00
ethernet	0x01

- [初期値]: -
- *id*
- [設定値]:

設定値	説明
<i>type</i> が ethernet の場合	MAC アドレス
<i>type</i> が text の場合	文字列
<i>type</i> が省略された場合	2 桁十六進数の列で先頭は <i>type</i> フィールド

- [初期値]: -
- *mac_address*
- [設定値]:
 - xx:xx:xx:xx:xx:xx (xx は十六進数) 予約 DHCP クライアントの MAC アドレス
 - xx:xx:xx:* のように下位 3 オクテットをアスタリスク (*) にすることで、OUI(ベンダー ID) のみの指定となる
- [初期値]: -
- *ipcp*: IPCP でリモート側に与えることを示すキーワード
- [初期値]: -

[説明]

IP アドレスを割り当てる DHCP クライアントを固定的に設定する。

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 チャン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。

コマンドの第 2 書式で 1 つの OUI(ベンダー ID)を複数設定することができる。OUI(ベンダー ID)設定と MAC アドレス設定の両方がある場合、MAC アドレス設定を優先する。

[設定例]

```
A. # dhcp scope bind 1 192.168.100.2 ethernet 00:a0:de:01:23:45
B. # dhcp scope bind 1 192.168.100.2 text client01
C. # dhcp scope bind 1 192.168.100.2 01 00 a0 de 01 23 45 01 01 01
D. # dhcp scope bind 1 192.168.100.2 00:a0:de:01:23:45
E. # dhcp scope bind 1 192.168.100.2-192.168.100.19 00:a0:de:*
```

1. **dhcp server rfc2131 compliant on** あるいは **use-clientid** 機能を使用する設定の場合

- A. B. C. の書式では、クライアントの識別に **Client-Identifier** オプションを使用する。
- D. の書式では DHCP パケットの **chaddr** フィールドを使用する。ただし、**Client-Identifier** オプションが存在する場合、この設定は無視される。

DHCP サーバーは **chaddr** フィールドの値より **Client-Identifier** オプションの値の方が優先して使用される。

show status dhcp コマンドを実行してクライアントの識別子を確認することで、クライアントが **Client-Identifier** オプションを使っているか否かを判別することも可能である。

- リースしているクライアントとして MAC アドレスが表示されていれば **Client-Identifier** オプションは使用していない
- リースしているクライアントとして十六進数の文字列、あるいは文字列が表示されていれば、**Client-Identifier** オプションが使われている **Client-Identifier** オプションを使うクライアントへの予約は、ここに表示される十六進数の文字列あるいは文字列を使用する

2. **dhcp server rfc2131 compliant off** あるいは **use-clientid** 機能を使用しない場合

- A. B. C. の書式では指定できない。**Client-Identifier** オプションは無視される。
- D. の書式では DHCP パケットの **chaddr** フィールドを使用する。

なお、クライアントとの相互動作に関して以下の留意点がある。

- 個々の機能を単独で用いるとクライアント側で思わぬ動作を招く可能性があるため、**dhcp server rfc2131 compliant on** あるいは **dhcp server rfc2131 compliant off** で使用することを推奨する。
- ルーターの再起動やスコープの再設定によりリース情報が消去されている場合、アドレスの延長要求をした時やリース期間内のクライアントを再起動した時にクライアントが使用する IP アドレスは変わることがある。

これを防ぐためには **dhcp server rfc2131 compliant on** (あるいは **remain-silent** 機能を有効にする) 設定がある。この設定にすると、ヤマハルーターがリース情報を持たないクライアントからの DHCPREQUEST に対して DHCPNAK を返さず無視するようになる。

この結果、リース期限満了時にクライアントが出す DHCPDISCOVER に Requested IP Address オプションが含まれていれば、そのクライアントには引き続き同じ IP アドレスをリースすることができる。

E. の書式では、OUI (ベンダー ID) のみ指定し、その OUI (ベンダー ID) を持つ機器にのみ IP アドレスを割り当てることができる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

8.1.6 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

8.1.7 DHCP 割り当て情報を元にした予約設定の生成

[書式]

`dhcp convert lease to bind scope_n [except] [idx [...]]`

[設定値及び初期値]

- `scope_n`
 - [設定値]: スコープ番号 (1..65535)
 - [初期値]: -
- `idx`
 - [設定値]:

設定値	説明
番号	<code>show status dhcp summary</code> コマンドで表示されるインデックス番号、最大 100 個
all	割り当て中の情報全てを対象とする
省略	省略時は all

- [初期値]: -

[説明]

現在の割り当て情報を元に予約設定を作成する。`except` キーワードを指示すると、指定した番号以外の情報が予約設定に反映される。

[ノート]

以下の変換規則で IP アドレス割り当て情報が予約設定に変換される。

IP アドレス割り当て情報のクライアント識別種別 (<code>show status dhcp</code> 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

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
	(01) 31 32 33	00 31 32 33

※1 : rfc2131 compliant on あるいは use-clientid ありの場合、このような IP アドレス割り当て情報の表示は ARP チェックの結果である可能性が高く、通常の割り当て時にはクライアント ID オプションが使われるため、この形式で予約設定をする。ただし、MAC アドレスと異なるクライアント ID を使うホストが存在する場合はこの自動変換による予約は有効に機能しないため、そのようなホストに対する予約設定は別途、手動で行う必要がある

※2 : rfc2131 compliant off あるいは use-clientid なしの場合、chaddr フィールドを使用する

コマンド実行時点での割り当て情報を元に予約設定を作成する。サマリ表示からこの変換コマンドの実行までに時間が経過した場合には、本コマンド実行後に意図したペアの予約が作成されていることを **show config** で確認すべきである

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

8.1.8 DHCP オプションの設定

[書式]

dhcp scope option *scope_num option=value [option=value...]*

no dhcp scope option *scope_num [...]*

[設定値及び初期値]

- *scope_num*
 - [設定値]: スコープ番号 (1..65535)
 - [初期値]: -
- *option*
 - [設定値]:
 - オプション番号
 - 1..49,62..254
 - 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

8.1.9 DHCP リース情報の手動追加

[書式]

```
dhcp manual lease ip_address [type] id
dhcp manual lease ip_address mac_address
dhcp manual lease ip_address ipcp
```

[設定値及び初期値]

- *ip_address*
 - [設定値]: リースする IP アドレス
 - [初期値]: -
- *type*: Client-Identifier オプションの *type* フィールドを決定する
 - [設定値]:

設定値	説明
text	0x00
ethernet	0x01

- [初期値]: -

- *id*

- [設定値]:

設定値	説明
<i>type</i> が text の場合	文字列
<i>type</i> が ethernet の場合	MAC アドレス
<i>type</i> が省略された場合	2 桁十六進数の列で先頭は <i>type</i> フィールド

- [初期値]: -
- *mac_address*
 - [設定値]: XX:XX:XX:XX:XX:XX (XX は十六進数) DHCP クライアントの MAC アドレス
 - [初期値]: -
- *ipcp*: IPCP でリモート側に与えたものとするキーワード
 - [初期値]: -

[説明]

手動で、特定 IP アドレスのリース情報を追加する。

[ノート]

本コマンドは自動で行われる DHCP のアドレス配布に影響を与えるため、意図して特定の IP アドレスのリース情報を追加したい場合を除いて、使用するべきではない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

8.1.10 DHCP リース情報の手動削除

[書式]

```
dhcp manual release ip_address
```

[設定値及び初期値]

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

[説明]

手動で、特定 IP アドレスのリース情報を削除する。

[ノート]

本コマンドは自動で行われる DHCP のアドレス配布に影響を与えるため、意図して特定の IP アドレスのリース情報を削除したい場合を除いて、使用するべきではない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

8.1.11 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 パケットを複製してすべてのサーバーに中継するか、あるいは 1 つだけサーバーを選択して中継するかは **dhcp relay select** コマンドの設定で決定される。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

8.1.12 DHCP リレーエージェント機能で使用する始点ポート番号の設定

[書式]

```
dhcp relay srcport port
no dhcp relay srcport [port]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号 (1..65535)
 - [初期値]: 68

[説明]

DHCP リレーエージェント機能で使用する始点ポート番号を設定する。

[適用モデル]

vRX VMware ESXi 版

8.1.13 DHCP サーバーの選択方法の設定

[書式]

```
dhcp relay select type
no dhcp relay select [type]
```

[設定値及び初期値]

- *type*
 - [設定値]:

設定値	説明
hash	Hash 関数を利用して一つだけサーバーを選択する
all	すべてのサーバーを選択する

- [初期値]: hash

[説明]

dhcp relay server コマンドで設定された複数のサーバーの取り扱いを設定する。hash が指定された場合は、Hash 関数を利用して一つだけサーバーが選択されてパケットが中継される。この Hash 関数は、DHCP メッセージの **chaddr** フィールドを引数とするので、同一の DHCP クライアントに対しては常に同じサーバーが選択されるはずである。all が指定された場合は、パケットはすべてのサーバーに対し複製中継される。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

8.1.14 DHCP BOOTREQUEST パケットの中継基準の設定

[書式]

```
dhcp relay threshold time
no dhcp relay threshold [time]
```

[設定値及び初期値]

- *time*
 - [設定値]: 秒数 (0..65535)
 - [初期値]: 0

[説明]

DHCP BOOTREQUEST パケットの *secs* フィールドとこのコマンドによる秒数を比較し、設定値より小さな *secs* フィールドを持つ DHCP BOOTREQUEST パケットはサーバーに中継しないようにする。

これにより、同一 LAN 上に別の DHCP サーバーがあるにも関わらず遠隔地の DHCP サーバーにパケットを中継してしまうのを避けることができる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

8.1.15 インターフェース毎の DHCP の動作の設定

[書式]

```
ip interface dhcp service type [host1 [host2 [host3 [host4]]]]
no ip interface dhcp service
```

[設定値及び初期値]

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

設定値	説明
off	DHCP サーバーとしても DHCP リレーエージェントとしても機能しない
server	DHCP サーバーとして機能させる
relay	DHCP リレーエージェントとして機能させる

- [初期値]: -
- *host1..host4*
 - [設定値]: DHCP サーバーの IP アドレス
 - [初期値]: -

[説明]

インターフェース毎に DHCP の動作を設定する。

DHCP サーバーを設定した場合には、ネットワークアドレスが合致する DHCP スコープから IP アドレスを 1 つ割り当てる。

DHCP リレーエージェントを設定した場合には、*host* を設定する必要があり、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]

ブリッジインタフェースは vRX VMware ESXi 版で指定可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

8.2 DHCP クライアント機能

8.2.1 DHCP クライアントのホスト名の設定

[書式]

```

dhcp client hostname interface primary host
dhcp client hostname interface secondary host
dhcp client hostname pp peer_num host
dhcp client hostname pool pool_num host
no dhcp client hostname interface primary [host]
no dhcp client hostname interface secondary [host]
no dhcp client hostname pp peer_num [host]
no dhcp client hostname pool pool_num [host]

```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]:
 - 相手先情報番号
 - anonymous
 - [初期値]: -
- *pool_num*
 - [設定値]: **ip pp remote address pool dhcp** コマンドで取得する IP アドレスの番号。例えば、**ip pp remote address pool dhcp** コマンドで IP アドレスを 2 個取得する場合、*pool_num* に "1" または "2" を設定することで、それぞれのクライアント ID オプションに任意の ID を付けることができる。(1..**ip pp remote address pool dhcp** コマンドで取得できる IP アドレスの最大数)
 - [初期値]: -
- *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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

8.2.2 要求する IP アドレスリース期間の設定

[書式]

```

ip interface dhcp lease time time
no ip interface dhcp lease time [time]

```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、ブリッジインタフェース名
 - [初期値]: -
- *time*
 - [設定値]: 分数 (1..21474836)
 - [初期値]: -

[説明]

DHCP クライアントが要求する IP アドレスのリース期間を設定する。

[ノート]

リース期間の要求が受け入れられなかった場合、要求しなかった場合は、DHCP サーバーからのリース期間を利用

する。
ブリッジインタフェースは vRX VMware ESXi 版で指定可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

8.2.3 IP アドレス取得要求の再送回数と間隔の設定

[書式]

```
ip interface dhcp retry retry interval
no ip interface dhcp retry [retry interval]
```

[設定値及び初期値]

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

設定値	説明
1..100	回数
infinity	無制限

- [初期値]: infinity
- *interval*
 - [設定値]: 秒数 (1..100)
 - [初期値]: 5

[説明]

IP アドレスの取得に失敗したときにリトライする回数とその間隔を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

8.2.4 DHCP クライアント ID オプションの設定

[書式]

```
dhcp client client-identifier interface primary [type type] id
dhcp client client-identifier interface secondary [type type] id
dhcp client client-identifier pp peer_num [type type] id
dhcp client client-identifier pool pool_num [type type] id
no dhcp client client-identifier interface primary
no dhcp client client-identifier interface secondary
no dhcp client client-identifier pp peer_num
no dhcp client client-identifier pool pool_num
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [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 個取得する場合、*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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

8.2.5 DHCP クライアントが DHCP サーバーへ送るメッセージ中に格納するオプションの設定

[書式]

```

dhcp client option interface primary option=value
dhcp client option interface secondary option=value
dhcp client option pp peer_num option=value
dhcp client option pool pool_num option=value
no dhcp client option interface primary [option=value]
no dhcp client option interface secondary [option=value]
no dhcp client option pp peer_num [option=value]
no dhcp client option pool pool_num [option=value]

```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [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 個取得する場合、*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。

[設定例]

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

```
# dhcp client option lan2 primary 50=c0,a8,00,80
```



```
# ip lan2 address dhcp
```

(注：ただし、この場合でも要求アドレスがサーバーから与えられるか否かはサーバー次第である。)

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

8.2.6 リンクダウンした時に情報を解放するか否かの設定

[書式]

```
dhcp client release linkdown switch [time]
```

```
no dhcp client release linkdown [switch [time]]
```

[設定値及び初期値]

- *switch*

- [設定値]:

設定値	説明
on	インタフェースのリンクダウンが <i>time</i> 秒間継続すると、取得していた情報を解放する
off	インタフェースがリンクダウンしても情報は保持する

- [初期値]: off

- *time*

- [設定値]: 秒数 (0..259200)
- [初期値]: 3

[説明]

DHCP クライアントとして DHCP サーバーから IP アドレスを得ているインタフェースがリンクダウンした時に、DHCP サーバーから得ていた情報を解放するか否かを設定する。

リンクダウンするとタイマーが働き、*time* の秒数だけリンクダウン状態が継続すると情報を解放する。*time* が設定されていない場合には *time* は 3 秒となる。

情報が解放されると、次にリンクアップした時に情報の取得を試みる。

[ノート]

タイマーの値を長く設定すると、不安定なリンク状態の影響を避けることができる。

本コマンドの設定は、コマンド実行後に発生したリンクダウン以降で有効になる。

タイマーの満了前にリンクアップした場合にはタイマーはクリアされ、情報を解放しない。

タイマーの満了前に情報のリース期間が満了した場合には、タイマーはクリアされ、情報は解放される。

以下のコマンド実行時には、動作中のタイマーはクリアされる。

ip interface address, ip pp remote address, ip pp remote address pool, dhcp client release linkdown

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

第 9 章

ICMP の設定

9.1 IPv4 の設定

9.1.1 ICMP Echo Reply を送信するか否かの設定

[書式]

```
ip icmp echo-reply send send
no ip icmp echo-reply send [send]
```

[設定値及び初期値]

- *send*
- [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: on

[説明]

ICMP Echo を受信した場合に、ICMP Echo Reply を返すか否かを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

9.1.2 ICMP Echo Reply をリンクダウン時に送信するか否かの設定

[書式]

```
ip icmp echo-reply send-only-linkup send
no ip icmp echo-reply send-only-linkup [send]
```

[設定値及び初期値]

- *send*
- [設定値]:

設定値	説明
on	リンクアップしている時だけ ICMP Echo Reply を返す
off	リンクの状態に関わらず ICMP Echo Reply を返す

- [初期値]: off

[説明]

リンクダウンしているインタフェースに付与された IP アドレスを終点 IP アドレスとする ICMP Echo を受信した時に、それに対して ICMP Echo Reply を返すかどうかを設定する。on に設定した時には、リンクアップしている時だけ ICMP Echo を返すので、リンクの状態を ping で調べることができるようになる。off に設定した場合には、リンクの状態に関わらず ICMP Echo を返す。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

9.1.3 ICMP Mask Reply を送信するか否かの設定

[書式]

```
ip icmp mask-reply send send
no ip icmp mask-reply send [send]
```

[設定値及び初期値]

- *send*
- [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値] : on

[説明]

ICMP Mask Request を受信した場合に、ICMP Mask Reply を返すか否かを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

9.1.4 ICMP Parameter Problem を送信するか否かの設定

[書式]

```
ip icmp parameter-problem send send
no ip icmp parameter-problem send [send]
```

[設定値及び初期値]

- *send*
 - [設定値] :

設定値	説明
on	送信する
off	送信しない

- [初期値] : off

[説明]

受信した IP パケットの IP オプションにエラーを検出した場合に、ICMP Parameter Problem を送信するか否かを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

9.1.5 ICMP Redirect を送信するか否かの設定

[書式]

```
ip icmp redirect send send
no ip icmp redirect send [send]
```

[設定値及び初期値]

- *send*
 - [設定値] :

設定値	説明
on	送信する
off	送信しない

- [初期値] : on

[説明]

他のゲートウェイ宛の IP パケットを受信して、そのパケットを適切なゲートウェイに回送した場合に、同時にパケットの送信元に対して ICMP Redirect を送信するか否かを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

9.1.6 ICMP Redirect 受信時の処理の設定

[書式]

```
ip icmp redirect receive action
no ip icmp redirect receive [action]
```

[設定値及び初期値]

- *action*
 - [設定値] :

設定値	説明
on	処理する
off	無視する

- [初期値] : off

[説明]

ICMP Redirect を受信した場合に、それを処理して自分の経路テーブルに反映させるか、あるいは無視するかを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

9.1.7 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

9.1.8 ICMP Timestamp Reply を送信するか否かの設定

[書式]

```
ip icmp timestamp-reply send send
no ip icmp timestamp-reply send [send]
```

[設定値及び初期値]

- *send*
 - [設定値] :

設定値	説明
on	送信する
off	送信しない

- [初期値] : on

[説明]

ICMP Timestamp を受信した場合に、ICMP Timestamp Reply を返すか否かを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

9.1.9 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

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

[書式]

```
ip icmp error-decryptd-ipsec send switch
no ip icmp error-decryptd-ipsec send [switch]
```

[設定値及び初期値]

• *switch*

- [設定値]:

設定値	説明
on	IPsec で復号したパケットに対して ICMP エラーを送る
off	IPsec で復号したパケットに対して ICMP エラーを送らない

- [初期値]: on

[説明]

IPsec で復号したパケットに対して ICMP エラーを送るか否か設定する。

[ノート]

ICMP エラーには復号したパケットの先頭部分が含まれるため、ICMP エラーが送信元に返送される時にも IPsec で処理されないようになっており、本来 IPsec で保護したい通信が保護されずにネットワークに流れてしまう可能性がある。特に、フィルタ型ルーティングでプロトコルによって IPsec で処理するかどうか切替えている場合には注意が必要となる。

ICMP エラーを送らないように設定すると、traceroute に対して反応がなくなるなどの現象になる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

9.1.11 受信した ICMP のログを記録するか否かの設定

[書式]

```
ip icmp log log
no ip icmp log [log]
```

[設定値及び初期値]

- *log*
- [設定値]:

設定値	説明
on	記録する
off	記録しない

- [初期値]: off

[説明]

受信した ICMP エラーを DEBUG レベルのログに記録するか否かを設定する。Echo Request や Echo Reply のログは記録しない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

9.2 IPv6 の設定

9.2.1 ICMP Echo Reply を送信するか否かの設定

[書式]

```
ipv6 icmp echo-reply send send
no ipv6 icmp echo-reply send [send]
```

[設定値及び初期値]

- *send*
- [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: on

[説明]

ICMP Echo Reply を送信するか否かを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

9.2.2 ICMP Echo Reply をリンクダウン時に送信するか否かの設定

[書式]

```
ipv6 icmp echo-reply send-only-linkup send
no ipv6 icmp echo-reply send-only-linkup [send]
```

[設定値及び初期値]

- *send*
- [設定値]:

設定値	説明
on	リンクアップしている時だけ ICMP Echo Reply を返す
off	リンクの状態に関わらず ICMP Echo Reply を返す

- [初期値]: off

[説明]

リンクダウンしているインタフェースに付与された IP アドレスを終点 IP アドレスとする ICMP Echo を受信した時に、それに対して ICMP Echo Reply を返すかどうかを設定する。on に設定した時には、リンクアップしている時だ

け ICMP Echo を返すので、リンクの状態を ping で調べることができるようになる。off に設定した場合には、リンクの状態に関わらず ICMP Echo を返す。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

9.2.3 ICMP Parameter Problem を送信するか否かの設定

[書式]

```
ipv6 icmp parameter-problem send send
no ipv6 icmp parameter-problem send [send]
```

[設定値及び初期値]

- *send*
- [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: off

[説明]

ICMP Parameter Problem を送信するか否かを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

9.2.4 ICMP Redirect を送信するか否かの設定

[書式]

```
ipv6 icmp redirect send send
no ipv6 icmp redirect send [send]
```

[設定値及び初期値]

- *send*
- [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: on

[説明]

ICMP Redirect を出すか否かを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

9.2.5 ICMP Redirect 受信時の処理の設定

[書式]

```
ipv6 icmp redirect receive action
no ipv6 icmp redirect receive [action]
```

[設定値及び初期値]

- *action*
- [設定値]:

設定値	説明
on	処理する
off	無視する

- [初期値]: off

[説明]

ICMP Redirect を受けた場合に処理するか無視するかを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

9.2.6 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

9.2.7 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

9.2.8 受信した ICMP のログを記録するか否かの設定

[書式]

```
ipv6 icmp log log
no ipv6 icmp log [log]
```

[設定値及び初期値]

- *log*
- [設定値]:

設定値	説明
on	記録する
off	記録しない

- [初期値]: off

[説明]

受信した ICMP を DEBUG タイプのログに記録するか否かを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

9.2.9 ICMP Packet-Too-Big を送信するか否かの設定

[書式]

```
ipv6 icmp packet-too-big send send
no ipv6 icmp packet-too-big send [send]
```

[設定値及び初期値]

- *send*
- [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: on

[説明]

ICMP Packet-Too-Big を出すか否かを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

9.2.10 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、tracertoute に対して反応がなくなるなどの現象になる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

第 10 章

トンネリング

10.1 トンネルインターフェースの使用許可の設定

[書式]

```
tunnel enable tunnel_num [tunnel_num ...]
```

```
no tunnel enable tunnel_num
```

[設定値及び初期値]

- *tunnel_num*
- [設定値]:

設定値	説明
番号	トンネルインターフェース番号
番号 1-番号 2	番号 1 から番号 2 までのトンネルインターフェース番号
番号 1-	番号 1 以上のすべてのトンネルインターフェース番号
-番号 1	番号 1 以下のすべてのトンネルインターフェース番号
all	すべてのトンネルインターフェース

- [初期値]:-

[説明]

トンネルインターフェースを使用できる状態にする。

工場出荷時は、すべてのトンネルインターフェースは `disable` 状態であり、使用する場合は本コマンドにより、インターフェースを有効にしなければならない。

複数指定した場合には、その全てで使用できる状態になる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

10.2 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
番号 1-番号 2	番号 1 から番号 2 までのトンネルインターフェース番号
番号 1-	番号 1 以上のすべてのトンネルインターフェース番号
-番号 1	番号 1 以下のすべてのトンネルインターフェース番号
all	すべてのトンネルインターフェース

- [初期値]:-

[説明]

トンネルインターフェースを使用できない状態にする。

トンネル先の設定を行う場合は、`disable` 状態で行うのが望ましい。

複数指定した場合には、その全てで使用できない状態になる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

10.3 トンネルインタフェースの接続種別の設定

[書式]

```
tunnel type type [role]
no tunnel type [type [role]]
```

[設定値及び初期値]

- *type*
 - [設定値]:

設定値	説明
point-to-point	point-to-point トンネル
multipoint	point-to-multipoint トンネル

- [初期値]: point-to-point
- *role*

- [設定値]:

設定値	説明
server	サーバーの役割を割り当てる
client	クライアントの役割を割り当てる

- [初期値]: client

[説明]

トンネルインタフェースの接続種別を、接続先を 1 箇所だけ持つ **point-to-point** トンネル、もしくは、複数の接続先を持つ **point-to-multipoint** トンネル (マルチポイントトンネル) に設定する。

role オプションは *type* に **multipoint** を設定した場合のみ設定可能なオプションで、マルチポイントトンネルでは同一のトンネルに接続する複数のルーターの中から **server** と **client** をそれぞれ 1 台以上指定する必要がある。

[ノート]

マルチポイントトンネルはハブ・アンド・スポーク型の構成を基本構成とし、通常はハブ・ルーターの *role* オプションのみに **server** を指定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

10.4 トンネルインタフェースの種別の設定

[書式]

```
tunnel encapsulation type
no tunnel encapsulation
```

[設定値及び初期値]

- *type*
 - [設定値]:

設定値	説明
ipsec	IPsec トンネル
ipip	IPv6 over IPv4 トンネル、IPv4 over IPv6 トンネル、IPv4 over IPv4 トンネルまたは IPv6 over IPv6 トンネル
l2tp	L2TP/IPsec トンネル
l2tpv3-raw	L2TPv3 トンネル
l2tpv3	L2TPv3/IPsec トンネル
ipudp	IPUDP トンネル

- [初期値]: ipsec

[説明]

トンネルインタフェースの種別を設定する。

[ノート]

トンネリングと NAT を併用する場合には **tunnel endpoint address** コマンドにより始点 IP アドレスを設定することが望ましい。

L2TP/IPsec 機能を実装していないモデルでは、**l2tp** キーワードは使用できない。

L2TPv3 機能を実装していないモデルでは、**l2tpv3-raw** キーワードおよび **l2tpv3** キーワードは使用できない。

IPUDP トンネルは、データコネクタ接続以外では使用できない。

データコネクタ接続機能を実装していないモデルでは、**ipudp** キーワードは使用できない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

10.5 トンネルインタフェースの IPv4 アドレスの設定

[書式]

```
ip tunnel address ip_address[/mask]
```

```
no ip tunnel address [ip_address[/mask]]
```

[設定値及び初期値]

- *ip_address*
 - [設定値]: IPv4 アドレス
 - [初期値]: -
- *mask*
 - [設定値]:
 - xxx.xxx.xxx.xxx (xxx は十進数)
 - 0x に続く十六進数
 - マスクビット数
 - [初期値]: -

[説明]

トンネルインタフェースの IPv4 アドレスとネットマスクを設定する。

このコマンドの設定によりトンネルインタフェースを経由して BGP のコネクションを確立できるようになる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

10.6 トンネルインタフェースの相手側の IPv4 アドレスの設定

[書式]

```
ip tunnel remote address ip_address
```

```
no ip tunnel remote address [ip_address]
```

[設定値及び初期値]

- *ip_address*
 - [設定値]: IPv4 アドレス
 - [初期値]: -

[説明]

トンネルインタフェースの IPv4 アドレスとネットマスクを設定する。

このコマンドの設定によりトンネルインタフェースを経由して BGP のコネクションを確立できるようになる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

10.7 相手側トンネルインタフェースの端点 IP アドレスの設定

[書式]

```
tunnel endpoint remote address remote
```

```
no tunnel endpoint remote address [remote]
```

[設定値及び初期値]

- *remote*
 - [設定値]: 相手側のトンネルインタフェース端点の IP アドレス、またはホスト名 (半角 64 文字以内)

- [初期値]:-

[説明]

相手側のトンネルインタフェース端点の IP アドレス、またはホスト名を設定する。IP アドレスは IPv4/IPv6 いずれのアドレスも設定できる。トンネルインタフェース端点として IPv4 アドレスを設定した場合には、IPv4 over IPv4 トンネルと IPv6 over IPv4 トンネルが、IPv6 アドレスを設定した場合には IPv4 over IPv6 トンネルと IPv6 over IPv6 トンネルが利用できる。

tunnel endpoint local address コマンドの設定がない場合、もしくは *local* と *remote* で IPv4/IPv6 の種別が異なる場合は、ローカルエンドポイントアドレスに適切なインタフェースの IP アドレスが利用される。また、本コマンドでホスト名を設定し、**tunnel endpoint local address** コマンドで IP アドレスを設定した場合、**tunnel endpoint local address** コマンドの IPv4/IPv6 種別に従ってホスト名の名前解決が行われる。

[ノート]

本コマンドにより設定した IP アドレスおよびホスト名が利用されるのは、**tunnel encapsulation** コマンドの設定値が *ipip* の場合である。本コマンドが設定されている場合、**tunnel endpoint address** コマンドおよび **tunnel endpoint name** コマンドの設定は利用されない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

10.8 自分側トンネルインタフェースの端点 IP アドレスの設定

[書式]

```
tunnel endpoint local address local
no tunnel endpoint local address [local]
```

[設定値及び初期値]

- *local*
 - [設定値]: 自分側のトンネルインタフェース端点の IP アドレス、またはホスト名 (半角 64 文字以内)
 - [初期値]:-

[説明]

自分側のトンネルインタフェース端点の IP アドレス、またはホスト名を設定する。IP アドレスは IPv4/IPv6 いずれのアドレスも設定できる。トンネルインタフェース端点として IPv4 アドレスを設定した場合には、IPv4 over IPv4 トンネルと IPv6 over IPv4 トンネルが、IPv6 アドレスを設定した場合には IPv4 over IPv6 トンネルと IPv6 over IPv6 トンネルが利用できる。

tunnel endpoint remote address コマンドの設定がない場合、もしくは *local* と *remote* で IPv4/IPv6 の種別が異なる場合は、本コマンドの設定は反映されない。また、本コマンドでホスト名を設定し、**tunnel endpoint remote address** コマンドで IP アドレスを設定した場合、**tunnel endpoint remote address** コマンドの IPv4/IPv6 種別に従ってホスト名の名前解決が行われる。

[ノート]

本コマンドにより設定した IP アドレスおよびホスト名が利用されるのは、**tunnel encapsulation** コマンドの設定値が *ipip* の場合である。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

10.9 トンネルインタフェースの端点 IP アドレスの設定

[書式]

```
tunnel endpoint address [local] remote
no tunnel endpoint address [[local] remote]
```

[設定値及び初期値]

- *local*
 - [設定値]: 自分側のトンネルインタフェース端点の IP アドレス
 - [初期値]:-
- *remote*
 - [設定値]: 相手側のトンネルインタフェース端点の IP アドレス
 - [初期値]:-

[説明]

トンネルインタフェース端点の IP アドレスを設定する。IP アドレスは IPv4/IPv6 いずれのアドレスも設定できるが、*local* と *remote* では IPv4/IPv6 の種別が揃っていないといけない。トンネルインタフェース端点として IPv4 ア

ドレスを設定した場合には、IPv4 over IPv4 トンネルと IPv6 over IPv4 トンネルが、IPv6 アドレスを設定した場合には IPv4 over IPv6 トンネルと IPv6 over IPv6 トンネルが利用できる。

local を省略した場合は、適当なインタフェースの IP アドレスが利用される。

[ノート]

このコマンドにより設定した IP アドレスが利用されるのは、**tunnel encapsulation** コマンドの設定値が *l2tp*、*l2tpv3-raw*、*l2tpv3*、*ipip* の場合である。IPsec トンネルでは、トンネル端点は **ipsec ike local address** および **ipsec ike remote address** コマンドにより設定される。

L2TP/IPsec サーバーの Anonymous で受ける場合には設定する必要はない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

10.10 トンネルの端点の名前の設定

[書式]

```
tunnel endpoint name [local_name] remote_name [type]
```

```
no tunnel endpoint name [local_name remote_name type]
```

[設定値及び初期値]

- *local_name*
 - [設定値]: 自分側端点
 - [初期値]: -
- *remote_name*
 - [設定値]: 相手側端点
 - [初期値]: -
- *type*: 名前の種類
 - [設定値]:

設定値	説明
fqdn	FQDN
tel	NGN 網電話番号

- [初期値]: fqdn

[説明]

トンネル端点の名前を指定する。

[ノート]

tunnel endpoint address コマンドが設定されている場合には、そちらが優先される。

このコマンドが利用されるのは、**tunnel encapsulation** コマンドの設定値が *l2tpv3-raw*、*l2tpv3*、*ipip*、*ipudp* の場合である。

l2tpv3-raw、*l2tpv3*、*ipip* トンネルの場合、名前にはドメイン名 (FQDN) を指定する。

ipudp トンネルの場合、名前には NGN 網電話番号を指定する。ハイフン無しで記述する。

データコネクタ接続機能を実装していないモデルでは、*type* パラメータは使用できない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

10.11 マルチポイントトンネルのサーバーの設定

[書式]

```
tunnel multipoint server id ip_address
```

```
no tunnel multipoint server id [ip_address]
```

[設定値及び初期値]

- *id*
 - [設定値]: サーバー識別子 (1..3)
 - [初期値]: -
- *ip_address*
 - [設定値]: IPv4/IPv6 アドレスまたはホスト名
 - [初期値]: -

[説明]

マルチポイントトンネルにおいて、サーバーの役割が割り当てられているルーターのアドレスを設定する。本コマンドは **tunnel type** コマンドで接続種別に **multipoint**、**role** オプションに **client** が設定されているトンネルインタフェース（マルチポイントトンネルのクライアント側のトンネルインタフェース）で有効になる。

本コマンドを複数設定し、複数のサーバーを指定している場合は、接続可能なサーバーすべてに対してトンネルが接続される。最大で3台のサーバーを指定できる。

[ノート]

マルチポイントトンネルはハブ・アンド・スポーク型の構成を基本構成とし、通常はハブ・ルーターがサーバーとなる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

10.12 マルチポイントトンネルで使用する自分の名前の設定

[書式]

```
tunnel multipoint local name name
no tunnel multipoint local name [name]
```

[設定値及び初期値]

- *name*
 - [設定値]: 名前（半角で 64 文字以内、全角で 32 文字以内）
 - [初期値]: -

[説明]

マルチポイントトンネルで使用する自分の名前を設定する。

本コマンドで設定した名前はトンネル接続後に接続相手にも通知され、接続相手側でもトンネルの識別情報として SYSLOG 等で利用される。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

10.13 マルチポイントトンネルで接続する相手の最大数の設定

[書式]

```
tunnel multipoint limit limit
no tunnel multipoint limit [limit]
```

[設定値及び初期値]

- *limit*
 - [設定値]: 最大数 (1..100)
 - [初期値]: 100

[説明]

選択されているトンネルインタフェースで接続できる相手の最大数を設定する。本コマンドは **tunnel type** コマンドの接続種別に **multipoint**、**role** オプションに **server** が設定されているトンネルインタフェース（マルチポイントトンネルのサーバー側のトンネルインタフェース）で有効になる。

すべてのトンネルインタフェースの接続相手の合計数の上限は定められているトンネル最大対地数となる。そのため、複数のトンネルインタフェースを使用する場合は、本コマンドで設定した最大数の制限だけでなく、トンネル最大対地数の制限も受ける。接続相手の数が本コマンドで設定した最大数を下回っている場合でも、すべてのトンネルインタフェースの合計数がトンネル最大対地数に達している場合は新たに接続することはできない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

第 11 章

IPsec の設定

vRX では、暗号化により IP 通信に対するセキュリティを保証する IPsec 機能を実装しています。IPsec では、鍵交換プロトコル IKE(Internet Key Exchange) を使用します。必要な鍵は IKE により自動的に生成されますが、鍵の種となる事前共有鍵は **ipsec ike pre-shared-key** コマンドで事前に登録しておく必要があります。この鍵はセキュリティ・ゲートウェイごとに設定できます。また、鍵交換の要求に応じるかどうかは、**ipsec ike remote address** コマンドで設定します。

鍵や鍵の寿命、暗号や認証のアルゴリズムなどを登録した管理情報は、SA(Security Association) で管理します。SA を区別する ID は自動的に付与されます。SA の ID や状態は **show ipsec sa** コマンドで確認することができます。SA には、鍵の寿命に合わせた寿命があります。SA の属性のうちユーザが指定可能なパラメータをポリシーと呼びます。またその番号はポリシー ID と呼び、**ipsec sa policy** コマンドで定義し、**ipsec ike duration ipsec-sa**、**ipsec ike duration isakmp-sa** コマンドで寿命を設定します。

SA の削除は **ipsec sa delete** コマンドで、SA の初期化は **ipsec refresh sa** コマンドで行います。**ipsec auto refresh** コマンドにより、SA を自動更新させることも可能です。

IPsec による通信には、大きく分けてトンネルモードとトランスポートモードの 2 種類があります。

トンネルモードは IPsec による VPN(Virtual Private Network) を利用するためのモードです。ルーターがセキュリティ・ゲートウェイとなり、LAN 上に流れる IP パケットデータを暗号化して対向のセキュリティ・ゲートウェイとの間でやりとりします。ルーターが IPsec に必要な処理をすべて行うので、LAN 上の始点や終点となるホストには特別な設定を必要としません。

トンネルモードを用いる場合は、トンネルインタフェースという仮想的なインタフェースを定義し、処理すべき IP パケットがトンネルインタフェースに流れるように経路を設定します。個々のトンネルインタフェースはトンネルインタフェース番号で管理されます。設定のためにトンネル番号を切替えるには **tunnel select** コマンドを使用します。トンネルインタフェースを使用するか使用しないかは、それぞれ **tunnel enable**、**tunnel disable** コマンドを使用します。

相手先情報番号による設定		トンネルインタフェース番号による設定
<ul style="list-style-type: none"> • pp enable • pp disable • pp select 	<=>	<ul style="list-style-type: none"> • tunnel enable • tunnel disable • tunnel select

トランスポートモードは特殊なモードであり、ルーター自身が始点または終点になる通信に対してセキュリティを保証するモードです。トランスポートモードを使用するには **ipsec transport** コマンドで定義を行い、使用をやめるには **no ipsec transport** コマンドで定義を削除します。

セキュリティ・ゲートウェイの識別子とトンネルインタフェース番号はモデルにより異なり、以下の表のようになります。

モデル	セキュリティ・ゲートウェイの識別子	トンネルインタフェース番号
• vRX Amazon EC2 版	• 1-6000 (通常モード)	• 1-6000 (通常モード)
• vRX VMware ESXi 版	• 1-1000 (コンパクトモード)	• 1-1000 (コンパクトモード)

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。

11.1 IPsec の動作の設定

[書式]

ipsec use use

no ipsec use [*use*]

[設定値及び初期値]

- *use*
 - [設定値]:

設定値	説明
on	動作させる
off	動作させない

- [初期値]: on

[説明]

IPsec を動作させるか否かを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.2 IKE バージョンの設定

[書式]

ipsec ike version *gateway_id* *version*

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

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *version*
 - [設定値]: 使用する IKE のバージョン
 - [設定値]:

設定値	説明
1	IKE バージョン 1
2	IKE バージョン 2

- [初期値]: 1

[説明]

セキュリティ・ゲートウェイで使用する IKE のバージョンを設定する。

[ノート]

version で指定したバージョン以外での接続以外は受け付けない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.3 IKE の認証方式の設定

[書式]

ipsec ike auth method *gateway_id* *method*

no ipsec ike auth method *gateway_id* [*method*]

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *method*
 - [設定値]:

設定値	説明
auto	認証方式を自動的に選択する
pre-shared-key	事前共有鍵

設定値	説明
certificate	デジタル署名
eap-md5	EAP-MD5

- [初期値]:
 - auto

[説明]

IKE の認証方式を設定する。

METHOD に auto を設定した場合、以下の条件にしたがって認証方式が決定される。

- 事前共有鍵方式
 - **ipsec ike pre-shared-key** コマンドが設定されている場合。
- デジタル署名方式

次の条件をすべて満たしている場合

- **ipsec ike pki file** コマンドで指定した場所に証明書が保存されている。
- **ipsec ike eap request** コマンドおよび **ipsec ike eap myname** コマンドが設定されていない。

- EAP-MD5 方式

次の条件をすべて満たしている場合

- **ipsec ike pki file** コマンドで指定した場所に証明書が保存されている。
- **ipsec ike eap request** コマンド、または **ipsec ike eap myname** コマンドが設定されていない。

上記、認証方式を決定する条件のうち、複数の条件に合致する場合、次の順番で認証方式が優先される。

1. 事前共有鍵方式
2. デジタル署名方式
3. EAP-MD5 方式

method に auto 以外を指定した場合、上記の認証方式を決定する条件にかかわらず、*method* に指定した方式で認証を行う。

[ノート]

本コマンドは IKEv2 でのみ有効であり、IKEv1 の動作に影響を与えない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.4 事前共有鍵の登録

[書式]

```
ipsec ike pre-shared-key gateway_id key
ipsec ike pre-shared-key gateway_id text text
no ipsec ike pre-shared-key gateway_id [...]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *key*
 - [設定値]: 鍵となる 0x ではじまる十六進数列 (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 0xCDEEEDC0CDED
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.5 IKEv2 の認証に使用する PKI ファイルの設定

[書式]

```
ipsec ike pki file gateway_id certificate=cert_id [crl=crl_id]
no ipsec ike pki file gateway_id [...]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *cert_id*
 - [設定値]:

設定値	説明
1..8	証明書ファイルの識別子

- [初期値]: -
- *crl_id*
 - [設定値]:

設定値	説明
1..8	CRL ファイルの識別子

- [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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.6 EAP-MD5 認証で使用する自分の名前とパスワードの設定

[書式]

```
ipsec ike eap myname gateway_id name password
no ipsec ike eap myname gateway_id [...]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *name*
 - [設定値]: 名前 (半角 256 文字以内)
 - [初期値]: -
- *password*
 - [設定値]: パスワード (半角 64 文字以内)
 - [初期値]: -

[説明]

EAP-MD5 認証を要求されたときに使用する名前とパスワードを設定する。

[ノート]

本コマンドは IKEv2 でのみ有効であり、IKEv1 の動作に影響を与えない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.7 EAP-MD5 によるユーザ認証の設定

[書式]

```
ipsec ike eap request gateway_id sw group_id
no ipsec ike eap request gateway_id [...]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *sw*
 - [設定値]:

設定値	説明
on	要求する
off	要求しない

- [初期値]: off
- *group_id*
 - [設定値]: 認証に使用するユーザグループの識別番号
 - [初期値]: -

[説明]

IKEv2 で、EAP-MD5 認証をクライアントに要求するか否かを設定する。 *group_id* を指定した場合には、該当のユーザグループに含まれるユーザを認証の対象とする。

本コマンドによる設定はルーターが応答側として動作するときのみ有効であり、始動側のセキュリティゲートウェイから送信された IKE AUTH 交換に AUTH ペイロードが含まれない場合に EAP-MD5 によるユーザ認証を行う。

[ノート]

本コマンドは IKEv2 でのみ有効であり、IKEv1 の動作に影響を与えない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.8 EAP-MD5 認証で証明書要求ペイロードを送信するか否かの設定

[書式]

```
ipsec ike eap send certreq gateway_id switch
no ipsec ike eap send certreq gateway_id [switch]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *switch*
 - [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: off

[説明]

EAP-MD5 認証方式の場合、始動側のセキュリティ・ゲートウェイから送信する IKE_AUTH 交換に、証明書要求 (CERTREQ) ペイロードを含めるか否かを設定する。

[ノート]

本コマンドは IKEv2 でのみ有効であり、IKEv1 の動作に影響を与えない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.9 IKE の鍵交換を始動するか否かの設定

[書式]

```
ipsec auto refresh [gateway_id] switch
```

```
no ipsec auto refresh [gateway_id]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *switch*
 - [設定値]:

設定値	説明
on	鍵交換を始動する
off	鍵交換を始動しない

- [初期値]:
 - off (全体的な動作)
 - on (*gateway_id* 毎)

[説明]

IKE の鍵交換を始動するかどうかを設定する。他のルーターが始動する鍵交換については、このコマンドに関係なく常に受け付ける。

gateway_id パラメータを指定しない書式は、ルーターの全体的な動作を決める。この設定が off のときにはルーターは鍵交換を始動しない。

gateway_id パラメータを指定する書式は、指定したセキュリティゲートウェイに対する鍵交換の始動を抑制するために用意されている。

例えば、次の設定では、1 番のセキュリティゲートウェイのみが鍵交換を始動しない。

```
ipsec auto refresh on
ipsec auto refresh 1 off
```

[ノート]

ipsec auto refresh off の設定では、*gateway_id* パラメータを指定する書式は効力を持たない。例えば、次の設定では、1 番のセキュリティゲートウェイでは鍵交換を始動しない。

```
ipsec auto refresh off (デフォルトの設定)
ipsec auto refresh 1 on
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.10 設定が異なる場合に鍵交換を拒否するか否かの設定

[書式]

```
ipsec ike negotiate-strictly gateway_id switch
```

```
no ipsec ike negotiate-strictly gateway_id
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *switch*
 - [設定値]:

設定値	説明
on	鍵交換を拒否する
off	鍵交換を受理する

- [初期値]: off

[説明]

IKEv1 として動作する際、設定が異なる場合に鍵交換を拒否するか否かを設定する。このコマンドの設定が `off` のときには、従来のファームウェアと同様に動作する。すなわち、相手の提案するパラメータが自分の設定と異なる場合でも、そのパラメータをサポートしていれば、それを受理する。このコマンドの設定が `on` のときには、同様の状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	<code>ipsec ike encryption</code>
グループ	<code>ipsec ike group</code>
ハッシュアルゴリズム	<code>ipsec ike hash</code>
PFS	<code>ipsec ike pfs</code>
フェーズ 1 のモード	<code>ipsec ike local name</code> 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.11 IKE の鍵交換に失敗したときに鍵交換を休止せずに継続するか否かの設定

[書式]

```
ipsec ike always-on gateway_id switch
no ipsec ike always-on
```

[設定値及び初期値]

- `gateway_id`
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- `switch`
 - [設定値]:

設定値	説明
<code>on</code>	鍵交換を継続する
<code>off</code>	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 キーペ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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.12 鍵交換の再送回数と間隔の設定

[書式]

```
ipsec ike retry count interval [max_session]
no ipsec ike retry [count interval [max_session]]
```

[設定値及び初期値]

- `count`
 - [設定値]: 再送回数 (1..50)
 - [初期値]: 10
- `interval`
 - [設定値]: 再送間隔の秒数 (1..100)
 - [初期値]: 5
- `max_session`
 - [設定値]: 同時に動作するフェーズ 1 の最大数 (1..5)
 - [初期値]: 3

[説明]

鍵交換のパケットが相手に届かないときに実施する再送の回数と間隔を設定する。

また、`max_session` パラメータは、IKEv1 において同時に動作するフェーズ 1 の最大数を指定する。ルーターは、フェーズ 1 が確立せずに再送を継続する状態にあるとき、鍵の生成を急ぐ目的で、新しいフェーズ 1 を始動することがある。このパラメータは、このような状況で、同時に動作するフェーズ 1 の数を制限するものである。なお、このパラメータは、始動側のフェーズ 1 のみを制限するものであり、応答側のフェーズ 1 に対しては効力を持たない。

[ノート]

IKEv2 として動作する場合、`max_session` パラメータは効力を持たない。同じ相手側セキュリティ・ゲートウェイに対して始動する鍵交換セッションは、常に最大 1 セッションとなる。

相手側セキュリティ・ゲートウェイに掛かっている負荷が非常に高い場合、本コマンドの設定値を調整することで鍵交換が成功しやすくなる可能性がある。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.13 相手側のセキュリティ・ゲートウェイの名前の設定

[書式]

```
ipsec ike remote name gateway name [type]
```

```
no ipsec ike remote name gateway [name]
```

[設定値及び初期値]

- `gateway`
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- `name`
 - [設定値]: 名前 (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・ゲートウェイの名前と ID の種類を設定する。

その他、動作する IKE のバージョンによって異なる、本コマンドの影響、注意点については以下の通り。

- IKEv1

このコマンドの設定は、フェーズ 1 のアグレッシブモードで使用され、メインモードでは使用されない。また、`type` パラメータは相手側セキュリティ・ゲートウェイの判別時に考慮されない。
- IKEv2

相手側セキュリティ・ゲートウェイの判別時には `name`、`type` パラメータの設定が共に一致している必要がある。`type` パラメータが 'tel' の場合、相手側 IPv6 アドレス(ID_IPV6_ADDR)を相手側セキュリティ・ゲートウェイの判別に使用する。`type` パラメータが 'tel-key' の場合、設定値を ID_KEY_ID として相手側セキュリティ・ゲートウェイの判別に使用する。`type` パラメータが 'key-id' 以外の場合、`name` から相手側セキュリティ・ゲートウェイの IP アドレスの特定を試

み、特定できれば、そのホストに対して鍵交換を始動する。この場合、**ipsec ike remote address** コマンドの設定は不要である。

ただし、**ipsec ike remote address** コマンドが設定されている場合は、そちらの設定にしたがって始動時の接続先ホストが決定される。

[ノート]

type パラメータの 'tel' および 'tel-key' は vRX VMware ESXi 版で指定可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.14 相手側セキュリティ・ゲートウェイの IP アドレスの設定

[書式]

```
ipsec ike remote address gateway_id ip_address
no ipsec ike remote address gateway_id [ip_address]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *ip_address*
 - [設定値]:

設定値	説明
IP アドレス、またはホスト名	相手側セキュリティ・ゲートウェイの IP アドレス、またはホスト名(半角 255 文字以内)
any	自動選択

- [初期値]: -

[説明]

相手側セキュリティ・ゲートウェイの IP アドレスまたはホスト名を設定する。ホスト名で設定した場合には、鍵交換の始動時にホスト名から IP アドレスを DNS により検索する。

その他、動作する IKE バージョンによって異なる、本コマンドの影響、注意点については以下の通り。

• IKEv1

応答側になる場合、本コマンドで指定したホストは相手側セキュリティ・ゲートウェイの判別に使用される。'any' が設定された場合は、相手側セキュリティ・ゲートウェイとして任意のホストから鍵交換を受け付ける。その代わりに、自分から鍵交換を始動することはできない。例えば、アグレッシブモードで固定のグローバルアドレスを持つ場合などに利用する。

• IKEv2

このコマンドで設定したホストは、鍵交換を始動する際の接続先としてのみ使用される。'any' は自分側から鍵交換を始動しないことを明示的に示す。

応答側となる場合、本コマンドの設定による相手側セキュリティ・ゲートウェイの判別は **ipsec ike remote name** コマンド等の設定によって行われる。

[ノート]

ホスト名を指定する場合には、**dns server** コマンドなどで必ず DNS サーバーを設定しておくこと。IPsec メインモード接続では、相手側セキュリティ・ゲートウェイの IP アドレスおよびホスト名を重複して設定しない。相手側セキュリティ・ゲートウェイの IP アドレスおよびホスト名を重複して設定した場合の動作は保証されない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.15 相手側の ID の設定

[書式]

```
ipsec ike remote id gateway_id ip_address[/mask]
no ipsec ike remote id gateway_id [ip_address[/mask]]
```

[設定値及び初期値]

- *gateway_id*

- [設定値]: セキュリティ・ゲートウェイの識別子
- [初期値]: -
- *ip_address*
 - [設定値]: IP アドレス
 - [初期値]: -
- *mask*
 - [設定値]: ネットマスク
 - [初期値]: -

[説明]

IKEv1 のフェーズ 2 で用いる相手側の ID を設定する。

このコマンドが設定されていない場合は、フェーズ 2 で ID を送信しない。

mask パラメータを省略した場合は、タイプ 1 の ID が送信される。また、*mask* パラメータを指定した場合は、タイプ 4 の ID が送信される。

[ノート]

本コマンドは IKEv2 の動作には影響を与えない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.16 自分側のセキュリティ・ゲートウェイの名前の設定

[書式]

```
ipsec ike local name gateway_id name [type]
no ipsec ike local name gateway_id [name]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *name*
 - [設定値]: 名前 (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・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]

type パラメータの 'tel' および 'tel-key' は vRX VMware ESXi 版で指定可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.17 自分側セキュリティ・ゲートウェイの IP アドレスの設定

[書式]

```

ipsec ike local address gateway_id ip_address
ipsec ike local address gateway_id vrrp interface vrid
ipsec ike local address gateway_id ipv6 prefix prefix on interface
ipsec ike local address gateway_id ipcp pp 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・ゲートウェイの識別子
 - [初期値]: -
- *ip_address*
 - [設定値]: 自分側セキュリティ・ゲートウェイの IP アドレス
 - [初期値]: -
- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *vrid*
 - [設定値]: VRRP グループ ID(1..255)
 - [初期値]: -
- *prefix*
 - [設定値]: プレフィックス
 - [初期値]: -
- *pp_num*
 - [設定値]: PP インタフェース番号
 - [初期値]: -

[説明]

自分側セキュリティ・ゲートウェイの IP アドレスを設定する。

vrrp キーワードを指定する第 2 書式では、VRRP マスターとして動作している場合のみ、指定した LAN インタフェース/VRRP グループ ID の仮想 IP アドレスを自分側セキュリティ・ゲートウェイアドレスとして利用する。VRRP マスターでない場合には鍵交換は行わない。

ipv6 キーワードを指定する第 3 書式では、IPv6 のダイナミックアドレスを指定する。

ipcp キーワードを指定する第 4 書式では、IPCP アドレスを取得する PP インタフェースを指定する。

[ノート]

本コマンドが設定されていない場合には、相手側のセキュリティ・ゲートウェイに近いインタフェースの IP アドレスを用いて IKE を起動する。

vrrp キーワードは vRX VMware ESXi 版で指定可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.18 自分側の ID の設定

[書式]

```

ipsec ike local id gateway_id ip_address[/mask]
no ipsec ike local id gateway_id [ip_address[/mask]]

```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *ip_address*

- [設定値]: IP アドレス
- [初期値]: -
- *mask*
 - [設定値]: ネットマスク
 - [初期値]: -

[説明]

IKEv1 のフェーズ 2 で用いる自分側の ID を設定する。

このコマンドが設定されていない場合には、フェーズ 2 で ID を送信しない。
mask パラメータを省略した場合は、タイプ 1 の ID が送信される。
 また、*mask* パラメータを指定した場合は、タイプ 4 の ID が送信される。

[ノート]

本コマンドは IKEv2 としての動作には影響を与えない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.19 IKE キープアライブ機能の設定

[書式]

```
ipsec ike keepalive use gateway_id switch [down=disconnect] [send-only-new-sa=send]
```

```
ipsec ike keepalive use gateway_id switch heartbeat [interval count [upwait]] [down=disconnect] [send-only-new-sa=send]
```

```
ipsec ike keepalive use gateway_id switch icmp-echo ip_address [length=length] [interval count [upwait]]  
[down=disconnect]
```

```
ipsec ike keepalive use gateway_id switch dpd [interval count [upwait]]
```

```
ipsec ike keepalive use gateway_id switch rfc4306 [interval count [upwait]]
```

```
no ipsec ike keepalive use gateway_id [switch ....]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *switch*: キープアライブの動作
 - [設定値]:

設定値	説明
on	キープアライブを使用する
off	キープアライブを使用しない
auto	対向のルーターがキープアライブを送信するときに限って送信する (heartbeat、rfc4306 でのみ有効)

- [初期値]: auto
- *ip_address*
 - [設定値]: ping を送信する宛先の IP アドレス (IPv4/IPv6)
 - [初期値]: -
- *length*
 - [設定値]: ICMP Echo のデータ部の長さ (64..1500)
 - [初期値]: 64
- *interval*
 - [設定値]: キープアライブパケットの送信間隔秒数 (1..600)
 - [初期値]: 10
- *count*
 - [設定値]: キープアライブパケットが届かないときに障害とみなすまでの試行回数 (1..50)
 - [初期値]: 6
- *upwait*
 - [設定値]: IPsec SA が生成されてから実際にトンネルインタフェースを有効にするまでの時間 (0..1000000)
 - [初期値]: 0
- *send*

- [設定値]:

設定値	説明
on	新旧の SA が混在する場合、新しい SA のみに対してキープアライブパケットを送信する
off	新旧の SA が混在する場合、新旧 SA の両方に対してキープアライブパケットを送信する

- [初期値]: off

[説明]

IKE キープアライブの動作を設定する。
本コマンドは、動作する IKE のバージョンによって以下のように動作が異なる。

- IKEv1

キープアライブの方式としては、heartbeat、ICMP Echo、DPD(RFC3706) の 3 種類から選ぶことができる。第 1 書式は自動的に heartbeat 書式となる。

heartbeat 書式を利用するには第 1、第 2 書式を使用する。 heartbeat 方式において switch パラメータが auto に設定されている場合は、相手から heartbeat パケットを受信したときだけ heartbeat パケットを送信する。従って、双方の設定が auto になっているときには、IKE キープアライブは動作しない。

ICMP Echo を利用するときには第 3 書式を使用し、送信先の IP アドレスを設定する。オプションとして、ICMP Echo のデータ部の長さを指定することができる。この方式では、switch パラメータが auto でも on の場合と同様に動作する。

DPD を利用するときには第 4 書式を使用する。この方式では switch パラメータが auto でも on の場合と同様に動作する。

その他、IKEv1 で対応していない方式(書式)が設定されている場合は、代替方式として heartbeat で動作する。このとき、switch、count、interval、upwait パラメータは設定内容が反映される。

- IKEv2

キープアライブの方式として、RFC4306(IKEv2 標準)、ICMP Echo の 2 種類から選ぶことができる。第 1 書式は自動的に RFC4306 方式となる。

switch パラメータが auto の場合には、RFC4306 方式のキープアライブパケットを受信したときだけ応答パケットを送信する。なお、IKEv2 ではこの方式のキープアライブパケットには必ず応答しなければならないため、switch パラメータが auto でも off の場合でも同様に動作する。

ICMP Echo を利用するときには第 3 書式を使用し、送信先の IP アドレスを設定する。オプションとして、ICMP Echo のデータ部の長さを指定することができる。この方式では、switch パラメータが auto でも on の場合と同様に動作する。

その他、IKEv2 で対応していない方式(書式)が設定されている場合は、代替方式として RFC4306 で動作する。このとき、switch、count、interval、upwait パラメータは設定内容が反映される。

[ノート]

相手先が PP インタフェースの先にある場合、down オプションを指定することができる。down オプションを指定すると、キープアライブダウン検出時と IKE の再送回数満了時に PP インタフェースの切断を行うことができる。網側の状態などで PP インタフェースの再接続によりトンネル確立状態の改善を望める場合に利用することができる。

キープアライブの方式として heartbeat を使用する場合、send-only-new-sa オプションを指定することができる。send-only-new-sa オプションに on を設定すると、鍵交換後の新旧の SA が混在するときに新しい SA のみに対してキープアライブパケットを送信するようになり、鍵交換時の負荷を軽減することができる。ただし、send-only-new-sa オプションに対応していないファームウェアとトンネルを構築する場合は、send-only-new-sa オプションを off に設定しておかなければトンネルがダウンする。

length パラメータで指定するのは ICMP データ部分の長さであり、IP パケット全体の長さではない。同じ相手に対して、複数の方法を併用することはできない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.20 IKE キープアライブに関する SYSLOG を出力するか否かの設定

[書式]

```
ipsec ike keepalive log gateway_id log
no ipsec ike keepalive log gateway_id [log]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *log*
 - [設定値]:

設定値	説明
on	出力する
off	出力しない

- [初期値]: on

[説明]

IKE キー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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.21 IKE が用いる暗号アルゴリズムの設定

[書式]

```
ipsec ike encryption gateway_id algorithm
no ipsec ike encryption gateway_id [algorithm]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *algorithm*
 - [設定値]:

設定値	説明
3des-cbc	3DES-CBC
des-cbc	DES-CBC
aes-cbc	AES-CBC
aes256-cbc	AES256-CBC

- [初期値]:
 - 3des-cbc

[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
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.22 受信した IKE パケットを蓄積するキューの長さの設定

[書式]

```
ipsec ike queue length length
no ipsec ike queue length [length]
```

[設定値及び初期値]

- *length* : キュー長
 - [設定値] :

設定値	モード
6000...24000	通常モード
1000...4000	コンパクトモード

- [初期値] :
 - 12000 (通常モード)
 - 2000 (コンパクトモード)

[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くほど、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えて検出する可能性が増える。通常の運用では、この設定を変更する必要はないが、多数のトンネルを構成しており、多数の SA を同時に消す状況があるならば値を大きめに設定するとよい。

[ノート]

キューの長さを長くすると、一度に受信して処理できる IKE パケットの数を増やすことができる。しかし、あまり大きくすると、ルーター内部にたまった IKE パケットの処理が遅れ、対向のルーターでタイムアウトと検知されてしまう可能性が増える。そのため、このコマンドの設定を変更する際には、慎重に行う必要がある。

通常の運用では、この設定を変更する必要はない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.23 IKE が用いるグループの設定

[書式]

```
ipsec ike group gateway_id group [group]
no ipsec ike group gateway_id [group [group]]
```

[設定値及び初期値]

- *gateway_id* : セキュリティ・ゲートウェイの識別子
 - [初期値] : -
- *group* : グループ識別子
 - [設定値] :
 - modp768
 - modp1024
 - modp1536
 - modp2048
 - [初期値] :
 - 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・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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.24 IKE が用いるハッシュアルゴリズムの設定

[書式]

```
ipsec ike hash gateway_id algorithm
no ipsec ike hash gateway_id [algorithm]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *algorithm*
 - [設定値]:

設定値	説明
md5	MD5
sha	SHA-1
sha256	SHA-256

- [初期値]:
 - sha

[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(Pseudo-Random Function)がある。IKEv2 で **ipsec ike proposal-limitation** コマンドが on に設定されているとき、本コマンドで設定されたアルゴリズムを提案する。**ipsec ike proposal-limitation** コマンドが off に設定されているときは、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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.25 受信したパケットの SPI 値が無効な値の場合にログに出力するか否かの設定

[書式]

```
ipsec log illegal-spi switch
no ipsec log illegal-spi
```

[設定値及び初期値]

- switch
 - [設定値]:

設定値	説明
on	ログに出力する
off	ログに出力しない

- [初期値]: off

[説明]

IPsec で、受信したパケットの SPI 値が無効な値の場合に、その旨をログに出力するか否かを設定する。SPI 値と相手の IP アドレスがログに出力される。
無効な SPI 値を含むパケットを大量に送り付けられることによる DoS の可能性を減らすため、ログは 1 秒あたり最大 10 種類のパケットだけを記録する。実際に受信したパケットの数を知ることはできない。

[ノート]

鍵交換時には、鍵の生成速度の差により一方が新しい鍵を使い始めても他方ではまだその鍵が使用できない状態になっているためにこのログが一時的に出力されてしまうことがある。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.26 IKE ペイロードのタイプの設定

[書式]

```
ipsec ike payload type gateway_id type1 [type2]
no ipsec ike payload type gateway_id [type1 ...]
```

[設定値及び初期値]

- gateway_id
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- type1: IKEv1 のメッセージのフォーマット
 - [設定値]:

設定値	説明
1	ヤマハルーターのリリース 2 との互換性を保持する
2	ヤマハルーターのリリース 3 に合わせる
3	初期ベクトル (IV) の生成方法を一部の実装に合わせる

- [初期値]: 2
- type2: IKEv2 のメッセージのフォーマット
 - [設定値]:

設定値	説明
1	ヤマハルーターの IKEv2 のリリース 1 との互換性を保持する
2	鍵交換や鍵の使用方法を一部の実装に合わせる

- [初期値]: 2

[説明]

IKEv1 および IKEv2 のペイロードのタイプを設定する。
IKEv1 でヤマハルーターの古いリビジョンと接続する場合には、type1 パラメータを 1 に設定する必要がある。
IKEv2 でヤマハルーターの以下のリビジョンと接続する場合には、type2 パラメータを 1 に設定する必要がある。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.27 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リース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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.28 IKE の情報ペイロードを送信するか否かの設定

[書式]

```
ipsec ike send info gateway_id info
no ipsec ike send info gateway_id [info]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *info*
 - [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: on

[説明]

IKEv1 動作時に、情報ペイロードを送信するか否かを設定する。受信に関しては、この設定に関わらず、すべての情報ペイロードを解釈する。

[ノート]

このコマンドは、接続性の検証などの特別な目的で使用される。定常の運用時は on に設定する必要がある。

本コマンドは IKEv2 としての動作には影響を与えない。IKEv2 では常に、必要に応じて情報ペイロードの送受信を行う。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.29 PFS を用いるか否かの設定

[書式]

```
ipsec ike pfs gateway_id pfs
```

no ipsec ike pfs gateway_id [pfs]

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *pfs*
 - [設定値]:

設定値	説明
on	用いる
off	用いない

- [初期値]: off

[説明]

IKE の始動側として働く場合に、PFS (Perfect Forward Secrecy) を用いるか否かを設定する。応答側として働く場合は、このコマンドの設定に関係なく、相手側セキュリティ・ゲートウェイの PFS の使用有無に合わせて動作する。ただし、IKEv1 として動作し、且つ **ipsec ike negotiate-strictly** コマンドが on の場合は、本コマンドの設定と相手側セキュリティ・ゲートウェイの PFS の使用有無が一致していなければならない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.30 XAUTH の設定

[書式]

ipsec ike xauth myname gateway_id name password
no ipsec ike xauth myname gateway_id

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *name*
 - [設定値]: XAUTH で通知する名前 (32 文字以内)
 - [初期値]: -
- *password*
 - [設定値]: XAUTH で通知するパスワード (32 文字以内)
 - [初期値]: -

[説明]

XAUTH の認証を要求されたときに通知する名前とパスワードを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.31 XAUTH 認証、EAP-MD5 認証に使用するユーザ ID の設定

[書式]

auth user userid username password
no auth user userid [username ...]

[設定値及び初期値]

- *userid*: ユーザ識別番号
 - [設定値]:

設定値	説明
1..6000	通常モード
1..1000	コンパクトモード

- [初期値]: -
- *username*
 - [設定値]: ユーザー名 (256 文字以内) (* 3 文字以上に設定してください。)

- [初期値]: -
- *password*
 - [設定値]: パスワード (64 文字以内)(* 同上)
 - [初期値]: -

[説明]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.32 XAUTH 認証、EAP-MD5 認証に使用するユーザ ID の属性の設定

[書式]

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

```
no auth user attribute userid [attribute=value ...]
```

[設定値及び初期値]

- *userid*: ユーザ識別番号
 - [設定値]:

設定値	説明
1..6000	通常モード
1..1000	コンパクトモード

- [初期値]: -
- *attribute=value*
 - [設定値]: ユーザ属性
 - [初期値]: xauth=off

[説明]

IKEv1 の XAUTH 認証、または IKEv2 の EAP-MD5 認証に使用するユーザ ID の属性を設定する。
設定できる属性は以下のとおり。

<i>attribute</i>	<i>value</i>	説明
xauth	on	IPsec の XAUTH 認証にこの ID を使用する
	off	IPsec の XAUTH 認証にこの ID を使用しない
xauth-address	IP address[/netmask](IPv6 アドレス可)	IPsec の接続時に、このアドレスを内部 IP アドレスとして通知する
xauth-dns	IP address(IPv6 アドレス可)	IPsec の接続時に、このアドレスを DNS サーバーアドレスとして通知する
xauth-wins	IP address(IPv6 アドレス可)	IPsec の接続時に、このアドレスを WINS サーバーアドレスとして通知する
xauth-filter	フィルタセットの名前を表す文字列	IPsec の接続時に、このフィルタを適用する
eap-md5	on	IKEv2 の EAP-MD5 認証にこの ID を使用する
	off	IKEv2 の EAP-MD5 認証にこの ID を使用しない

同じ属性が重複して指定されている場合はコマンドエラーとなる。

[ノート]

本コマンドにて明示的に設定した属性値は、該当のユーザ ID が属しているユーザグループに対して、**auth user group attribute** コマンドによって設定された属性値に優先して適用される。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

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

[書式]

auth user group *groupid* *userid* [*userid* ...]**no auth user group** *groupid*

[設定値及び初期値]

- *groupid*: ユーザグループ識別番号
 - [設定値]:

設定値	説明
1..6000	通常モード
1..1000	コンパクトモード

- [初期値]: -
- *userid*
 - [設定値]: ユーザ識別番号もしくはユーザ識別番号の範囲 (複数指定することが可能)
 - [初期値]: -

[説明]

IKEv1 の XAUTH 認証、または IKEv2 の EAP-MD5 認証に使用するユーザグループを設定する。

[設定例]

```
# auth user group 1 100 101 102
# auth user group 1 200-300
# auth user group 1 100 103 105 107-110 113
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.34 XAUTH 認証、EAP-MD5 認証に使用するユーザグループの属性の設定

[書式]

auth user group attribute *groupid* *attribute=value* [*attribute=value* ...]**no auth user group attribute** *groupid* [*attribute=value* ...]

[設定値及び初期値]

- *groupid*: ユーザグループ識別番号
 - [設定値]:

設定値	説明
1..6000	通常モード
1..1000	コンパクトモード

- [初期値]: -
- *attribute=value*
 - [設定値]: ユーザグループ属性
 - [初期値]: xauth=off

[説明]

IKEv1 の XAUTH 認証、または IKEv2 の EAP-MD5 認証に使用するユーザグループの属性を設定する。
設定できる属性は以下のとおり。

<i>attribute</i>	<i>value</i>	説明
xauth	on	IPsec の XAUTH 認証にこのグループに含まれるユーザ ID を使用する

attribute	value	説明
	off	IPsec の XAUTH 認証にこのグループに含まれるユーザ ID を使用しない
xauth-address-pool	IP アドレスの範囲 (IPv6 アドレス可)	IPsec の接続時に、このアドレスプールからアドレスを選択し、内部 IP アドレスとして通知する
xauth-dns	IP address(IPv6 アドレス可)	IPsec の接続時に、このアドレスを DNS サーバーアドレスとして通知する
xauth-wins	IP address(IPv6 アドレス可)	IPsec の接続時に、このアドレスを WINS サーバーアドレスとして通知する
xauth-filter	フィルタセットの名前を表す文字列	IPsec の接続時に、このフィルタを適用する
eap-md5	on	IKEv2 の EAP-MD5 認証にこの ID を使用する
	off	IKEv2 の EAP-MD5 認証にこの ID を使用しない

xauth-address-pool の属性値である IP アドレスの範囲は、以下のいずれかの書式にて記述する。

- IP address[/netmask]
- IP address-IP address[/netmask]

同じ属性が重複して指定されている場合はコマンドエラーとなる。

[ノート]

本コマンドで設定した属性値は、該当のユーザグループに含まれるすべてのユーザに対して有効となる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.35 XAUTH によるユーザ認証の設定

[書式]

```
ipsec ike xauth request gateway_id auth [group_id]
no ipsec ike xauth request gateway_id [auth ...]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティゲートウェイの識別子
 - [初期値]: -
- *group_id*
 - [設定値]: 認証に使用するユーザグループの識別番号
 - [初期値]: -
- *auth*
 - [設定値]:

設定値	説明
on	要求する
off	要求しない

- [初期値]: off

[説明]

IPsec の認証を行う際、Phase1 終了後に XAUTH によるユーザ認証をクライアントに要求するか否かを設定する。

group_id を指定した場合には、該当のユーザグループに含まれるユーザを認証の対象とする。

group_id の指定がない場合や、指定したユーザグループに含まれるユーザ情報では認証できなかった場合、RADIUS サーバーの設定があれば RADIUS サーバーを用いた認証を追加で試みる。

[ノート]

本コマンドによる設定はルーターが受動側として動作する時にのみ有効であり、始動側のセキュリティゲートウェイから送信された isakmp SA パラメータの提案に、認証方式として XAUTHInitPreShared(65001) が含まれていた場合に、この提案を受け入れ、XAUTH によるユーザ認証を行う。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.36 内部 IP アドレスプールの設定

[書式]

```
ipsec ike mode-cfg address pool pool_id ip_address[/mask]
ipsec ike mode-cfg address pool pool_id ip_address-ip_address[/mask]
no ipsec ike mode-cfg address pool pool_id [ip_address ...]
```

[設定値及び初期値]

- *pool_id*
 - [設定値]: アドレスプール ID(1..65535)
 - [初期値]: -
- *ip_address*
 - [設定値]: IP アドレス (IPv6 アドレス可)
 - [初期値]: -
- *ip_address-ip_address*
 - [設定値]: IP アドレスの範囲 (IPv6 アドレス可)
 - [初期値]: -
- *mask*
 - [設定値]: ネットマスク (IPv6 アドレスの時はプレフィックス長)
 - [初期値]: -

[説明]

IPsec クライアントに割り当てる内部 IP アドレスのアドレスプールを設定する。

本コマンドにて設定したアドレスプールは、**ipsec ike mode-cfg address gateway_id ...** コマンドにて用いられる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.37 IKE XAUTH Mode-Cfg メソッドの設定

[書式]

```
ipsec ike mode-cfg method gateway_id method [option]
no ipsec ike mode-cfg method gateway_id [method...]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティゲートウェイの識別子
 - [初期値]: -
- *method*
 - [設定値]:

設定値	説明
set	SET メソッド

- [初期値]: set

• *option*

- [設定値]:

設定値	説明
openswan	Openswan 互換モード

- [初期値]: -

[説明]

IKE XAUTH の Mode-Cfg でのアドレス割り当てメソッドを設定する。指定できるのは SET メソッドのみである。

option に 'openswan' を指定した場合には Openswan 互換モードとなり、Openswan と接続できるようになる。

[ノート]

ダイヤルアップ VPN の発呼側にヤマハルーターおよび YMS-VPN1 を利用するときに、*option* を指定していると XAUTH では接続できない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.38 IPsec クライアントに割り当てる内部 IP アドレスプールの設定

[書式]

```
ipsec ike mode-cfg address gateway_id pool_id
no ipsec ike mode-cfg address gateway_id [pool_id]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティゲートウェイの識別子
 - [初期値]: -
- *pool_id*
 - [設定値]: アドレスプール ID
 - [初期値]: -

[説明]

IPsec クライアントに内部 IP アドレスを割り当てる際に参照する、内部 IP アドレスプールを設定する。

内部 IP アドレスの IPsec クライアントへの通知は、XAUTH 認証に使用する Config-Mode にて行われるため、XAUTH 認証を行わない場合には通知は行われない。

以下のいずれかの方法にて、認証ユーザ毎に割り当てる内部 IP アドレスが設定されている場合には、アドレスプールからではなく、個別に設定されているアドレスを通知する。

- RADIUS サーバーに登録されている場合
- 以下のコマンドを用いて設定されている場合
 - **auth user attribute** *userid* xauth-address=*address[/mask]*
 - **auth user group attribute** *groupid* xauth-address-pool=*address-address[/mask]*

アドレスプールに登録されているアドレスが枯渇した場合には、アドレスの割当を行わない。

[ノート]

VPN クライアントとして YMS-VPN1 を用いる場合、XAUTH 認証を行うためには必ず内部 IP アドレスの通知を行う設定にしなければならない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.39 VPN クライアントの同時接続制限ライセンスの登録

[書式]

```
ipsec ike license-key license_id key
no ipsec ike license-key license_id [...]
```

[設定値及び初期値]

- *license_id*
 - [設定値]: ルーターキーの識別番号 (1..500)
 - [初期値]: -
- *key*
 - [設定値]: ルーターキー (64 文字以内)
 - [初期値]: -

[説明]

VPN クライアントソフト (同時接続版) からの VPN 接続を受け入れるためのルーターキー (ライセンスキー) を設定する。

各ルーターキーには固有の同時接続数が付与されており、異なる複数のルーターキーを登録することで、各ルーターキーの合計分の最大同時接続数を確保することができる。このとき、VPN クライアントソフトは本コマンドで登録したルーターキーに対応するクライアントキーならばどれを使用してもよい。VPN クライアントソフトが使用するクライアントキーに関わらず、登録された各ルーターキーの合計の最大同時接続数を基に接続制限が施される。

[設定例]

[YMS-VPN1-CP/YMS-VPN7-CP の場合]

```
# tunnel select 1
# tunnel template 2-20
# ipsec tunnel 1
# ipsec sa policy 1 1 esp aes-cbc sha-hmac
# ipsec ike log 1 payload-info
# ipsec ike remote address 1 any
# ipsec ike xauth request 1 on 11
# ipsec ike mode-cfg address 1 1
# ipsec ike license-key use 1 on
# tunnel enable 1
# ipsec ike license-key 1 abcdefg-10-hijklmno
# ipsec ike license-key 2 pqrstuvwxyz-10-wxyz0123
# ipsec ike mode-cfg address pool 1 172.16.0.1-172.16.0.20/32
# auth user 1 user1 pass1
# auth user 2 user2 pass2
:
# auth user 20 user20 pass20
# auth user group 11 1-20
# auth user group attribute 11 xauth=on xauth-dns=10.10.10.1
```

[YMS-VPN8-CP の場合]

```
# pp select anonymous
# pp bind tunnel1-tunnel20
# pp auth request mschap-v2
# pp auth username user1 pass1
# pp auth username user2 pass2
:
# pp auth username user20 pass20
# ppp ipcp ipaddress on
# ppp ipcp msexp on
# ip pp remote address pool 172.16.0.1-172.16.0.20
# ip pp mtu 1258
# pp enable anonymous
# tunnel select 1
# tunnel encapsulation l2tp
# ipsec tunnel 1
# ipsec sa policy 1 1 esp 3des-cbc sha-hmac
# ipsec ike keepalive use 1 off
# ipsec ike local address 1 172.16.0.254
# ipsec ike remote address 1 any
# ipsec ike license-key use 1 on
# l2tp tunnel disconnect time off
# ip tunnel tcp mss limit auto
# tunnel enable 1
:
# ipsec ike license-key 1 abcdefg-10-hijklmno
# ipsec ike license-key 2 pqrstuvwxyz-10-wxyz0123
# ipsec transport 1 1 udp 1701
# ipsec auto refresh on
# l2tp service on
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.40 VPN クライアントの同時接続制限ライセンスの適用

[書式]

```
ipsec ike license-key use gateway_id sw
no ipsec ike license-key use gateway_id [...]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *sw*
 - [設定値]:

設定値	説明
on	ルーターキーの適用を許可する
off	ルーターキーの適用を許可しない

- [初期値]: off

[説明]

VPN クライアントソフト (同時接続版) からの VPN 接続を受け入れるためのルーターキー (ライセンスキー) の適用を許可するか否かを設定する。

ルーターキーの適用を許可されたゲートウェイが、対応するクライアントキーを持つ VPN クライアントソフトと接続可能になる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.41 IKE のログの種類の設定

[書式]

```
ipsec ike log [gateway_id] type [type]
```

```
no ipsec ike log [gateway_id] [type]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *type*
 - [設定値]:

設定値	説明
message-info	IKE メッセージの内容
payload-info	ペイロードの処理内容
key-info	鍵計算の処理内容

- [初期値]: -

[説明]

出力するログの種類を設定する。ログはすべて、debug レベルの SYSLOG で出力される。

gateway_id パラメータを省略した設定は、応答側として働く際、セキュリティ・ゲートウェイが特定できない時点での通信に対して適用される。

[ノート]

このコマンドが設定されていない場合には、最小限のログしか出力しない。複数の *type* パラメータを設定することもできる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.42 ESP を UDP でカプセル化して送受信するか否かの設定

[書式]

```
ipsec ike esp-encapsulation gateway_id encap
```

```
no ipsec ike esp-encapsulation gateway_id
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *encap*
 - [設定値]:

設定値	説明
on	ESP を UDP でカプセル化して送信する

設定値	説明
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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.43 折衝パラメーターを制限するか否かの設定

[書式]

```
ipsec ike proposal-limitation gateway_id switch
no ipsec ike proposal-limitation gateway_id [switch]
```

[設定値及び初期値]

- gateway_id
 - [設定値] : セキュリティ・ゲートウェイの識別子
 - [初期値] : -
- switch
 - [設定値] :

設定値	説明
on	折衝パラメーターを制限する
off	折衝パラメーターを制限しない

- [初期値] : off

[説明]

IKEv2 で鍵交換を開始するとき、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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.44 IKE のメッセージ ID 管理の設定

[書式]

```
ipsec ike message-id-control gateway_id switch
no ipsec ike message-id-control gateway_id [switch]
```

[設定値及び初期値]

- gateway_id
 - [設定値] : セキュリティ・ゲートウェイの識別子
 - [初期値] : -

- *switch*
- [設定値]:

設定値	説明
on	リクエストメッセージの送信をメッセージ ID で管理する
off	リクエストメッセージの送信をメッセージ ID で管理しない

- [初期値]: off

[説明]

自機から IKEv2 のリクエストメッセージを送信するときのメッセージ ID 管理方法を設定する。
on に設定しているとき、同じ IKE SA を使用して送信済みの IKE メッセージに対する全てのレスポンスメッセージを受信していない場合、新しい IKE メッセージは送信しない。

[ノート]

本コマンドは IKEv2 でのみ有効であり、IKEv1 の動作に影響を与えない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.45 CHILD SA 作成方法の設定

[書式]

```
ipsec ike child-exchange type gateway_id type
no ipsec ike child-exchange type gateway_id [type]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *type*: IKEv2 の CHILD SA 作成方法のタイプ
 - [設定値]:

設定値	説明
1	ヤマハルーターの IKEv2 の従来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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.46 鍵交換の始動パケットを受信するか否かの設定

[書式]

```
ipsec ike negotiation receive gateway_id switch
no ipsec ike negotiation receive gateway_id [switch]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *switch*
 - [設定値]:

設定値	説明
on	鍵交換の始動パケットを受信する
off	鍵交換の始動パケットを受信しない

- [初期値] : on

[説明]

IKEv2 で、鍵交換の始動パケットを受信するか否かを設定する。
 受信しないに設定した場合は、結果として受動側としては動作せず、必ず始動側として動作するようになる。

[ノート]

本コマンドは IKEv2 でのみ有効であり、IKEv1 の動作に影響を与えない。
 off にする場合には、**ipsec ike remote address** コマンドまたは **ipsec ike remote name** コマンドを IP アドレスで設定しておく必要がある。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.47 SA 関連の設定

再起動されるとすべての SA がクリアされることに注意しなくてはならない。

11.47.1 SA の寿命の設定

[書式]

```
ipsec ike duration sa gateway_id second [kbytes] [rekey rekey]
no ipsec ike duration sa gateway_id [second [kbytes] [rekey rekey]]
```

[設定値及び初期値]

- *sa*
- [設定値] :

設定値	説明
ipsec-sa (もしくは child-sa)	IPsec SA (CHILD SA)
isakmp-sa (もしくは ike-sa)	ISAKMP SA (IKE SA)

- [初期値] : -
- *gateway_id*
 - [設定値] : セキュリティ・ゲートウェイの識別子
 - [初期値] : -
- *second*
 - [設定値] : 秒数 (300..691200)
 - [初期値] : 28800 秒
- *kbytes*
 - [設定値] : キロ単位のバイト数 (100..2147483647 or off)
 - [初期値] : 2000000
- *rekey* : SA を更新するタイミング
 - [設定値] :

設定値	説明
70%-90%	パーセント
off	更新しない (<i>sa</i> パラメータで 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。

vRX が始動側になる場合は、最大で 2147483647 KB のバイト寿命値を相手側へ提案可能であるが、相手側機器が vRX 以外の場合は 2 GB を超えるバイト寿命値を正しく認識できないため、vRX 以外の機種と接続する場合は必ず 2 GB 以下に設定する必要がある。

- IKEv2

IKEv2 では SA 寿命値は折衝されず、各セキュリティ・ゲートウェイが独立して管理するものとなっている。従って、確立された SA には、常にこのコマンドで設定した寿命値がセットされる。ただし、相手側セキュリティ・ゲートウェイの方が SA 更新のタイミングが早ければ、SA はその分早く更新されることになる。

ISAKMP SA (IKE SA) の寿命が IPsec SA (CHILD SA) の寿命より先に尽きた場合は、ISAKMP SA (IKE SA) の寿命値を IPsec SA (CHILD SA) の寿命値に合わせる。

なお、このコマンドを設定しても、すでに存在する SA の寿命値は変化せず、新しく作られる SA にのみ、新しい寿命値が適用される。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.47.2 SA のポリシーの定義

[書式]

```
ipsec sa policy policy_id gateway_id ah [ah_algorithm] [local-id=local-id] [remote-id=remote-id] [anti-replay-check=check]
```

```
ipsec sa policy policy_id gateway_id esp [esp_algorithm] [ah_algorithm] [anti-replay-check=check]
```

```
no ipsec sa policy policy_id [gateway_id]
```

[設定値及び初期値]

- *policy_id*
 - [設定値]: ポリシー ID(1..2147483647)
 - [初期値]: -
- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- ah: 認証ヘッダ (Authentication Header) プロトコルを示すキーワード
 - [初期値]: -
- esp: 暗号ペイロード (Encapsulating Security Payload) プロトコルを示すキーワード
 - [初期値]: -
- *ah_algorithm*: 認証アルゴリズム
 - [設定値]:

設定値	説明
md5-hmac	HMAC-MD5
sha-hmac	HMAC-SHA-1

設定値	説明
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・ゲートウェイに対して、複数の IPsec SA を生成し、IP パケットの内容に応じて SA を使い分けることができるようになる。

check=on の場合、受信パケット毎にシーケンス番号の重複や番号順のチェックを行い、エラーとなるパケットは破棄する。破棄する際には *debug* レベルで

[IPSEC] sequence difference
 [IPSEC] sequence number is wrong

といったログが記録される。

相手側が、トンネルインタフェースでの優先/帯域制御を行っている場合、シーケンス番号の順序が入れ替わってパケットを受信することがある。その場合、実際にはエラーではないのに上のログが表示され、パケットが破棄されることがあるので、そのような場合には設定を *off* にするとよい。

IKEv2 では、**ipsec ike proposal-limitation** コマンドが *on* に設定されているとき、本コマンドの *ah_algorithm*、および *esp_algorithm* パラメーターで設定されたアルゴリズムを提案する。**ipsec ike proposal-limitation** コマンドが *off* に設定されているときは、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
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.47.3 SA の手動更新

[書式]

```
ipsec refresh sa
```

[説明]

SA を手動で更新する。

[ノート]

管理されている SA をすべて削除して、IKE の状態を初期化する。

このコマンドでは、SA の削除を相手に通知しないので、通常の運用では **ipsec sa delete all** コマンドの方が望ましい。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.47.4 ダングリング SA の動作の設定

[書式]

```
ipsec ike restrict-dangling-sa gateway_id action
no ipsec ike restrict-dangling-sa gateway_id [action]
```

[設定値及び初期値]

- *gateway_id*
 - [設定値]: セキュリティ・ゲートウェイの識別子
 - [初期値]: -
- *action*
 - [設定値]:

設定値	説明
auto	アグレッシブモードの始動側でのみ IKE SA と IPsec SA を同期させる
off	IKE SA と IPsec SA を同期させない。

- [初期値]: auto

[説明]

このコマンドは IKEv1 のダングリング SA の動作に制限を設ける。

ダングリング SA とは、IKE SA を削除するときに対応する IPsec SA を削除せずに残したときの状態を指す。

RT シリーズでは基本的にはダングリング SA を許す方針で実装しており、IKE SA と IPsec SA を独立のタイミングで削除する。

auto を設定したときには、アグレッシブモードの始動側でダングリング SA を排除し、IKE SA と IPsec SA を同期して削除する。この動作は IKE keepalive が正常に動作するために必要な処置である。

off を設定したときには、常にダングリング SA を許す動作となり、IKE SA と IPsec SA を独立なタイミングで削除する。

ダイヤルアップ VPN のクライアント側ではない場合には、このコマンドの設定に関わらず常に IKE SA と IPsec SA は独立に管理され、削除のタイミングは必ずしも同期しない。

[ノート]

ダングリング SA の強制削除が行われても、通常は新しい IKE SA に基づいた新しい IPsec SA が存在するので通信に支障が出ることはない。

ダイヤルアップ VPN のクライアント側では、このコマンドにより動作を変更でき、それ以外では、ダングリング SA が発生しても何もせず通信を続ける。

ダイヤルアップ VPN のクライアント側でダングリング SA を許さないのは、IKE キープアライブを正しく機能させるために必要なことである。

IKE キープアライブでは、IKE SA に基づいてキープアライブを行う。ダングリング SA が発生した場合には、その SA についてはキープアライブを行う IKE SA が存在せず、キープアライブ動作が行えない。そのため、IKE キープアライブを有効に動作させるにはダングリング SA が発生したら強制的に削除して、通信は対応する IKESA が存在する IPsec SA で行われるようにしなくてはならない。

本コマンドは IKEv2 の動作には影響を与えない。IKEv2 では仕様として、ダングリング SA の存在を禁止している。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.47.5 IPsec NAT トラバーサルを利用するための設定

[書式]

```
ipsec ike nat-traversal gateway switch [keepalive=interval] [force=force_switch] [type=type]
no ipsec ike nat-traversal gateway [switch ...]
```

[設定値及び初期値]

- gateway
 - [設定値]: セキュリティゲートウェイの識別子
 - [初期値]: -
- switch : 動作の有無
 - [設定値]:

設定値	説明
on	NAT トラバーサルの動作を有効にする
off	NAT トラバーサルの動作を無効にする

- [初期値]: off
- interval : NAT キープアライブの送信間隔
 - [設定値]:

設定値	説明
off	送信しない
30-100000	時間[秒]

- [初期値]: 300
- force_switch
 - [設定値]:

設定値	説明
on	通信経路上に NAT がなくても NAT トラバーサルを使用する
off	通信経路上に NAT がなければ NAT トラバーサルを使用しない

- [初期値]: off
- type
 - [設定値]:

設定値	説明
1	ヤマハルーターの従来動作との互換性を保持する
2	NAT トラバーサル使用時に交換するペイロードを一部の実装に合わせる

- [初期値]: 1

[説明]

NAT トラバーサルの動作を設定する。この設定があるときには、IKE で NAT トラバーサルの交渉を行う。相手が NAT トラバーサルに対応していないときや、通信経路上に NAT の処理がないときには、NAT トラバーサル

を使用せず、ESP パケットを使って通信する。

対向のルーターや端末でも NAT トラバーサルの設定が必要である。いずれか一方にしか設定がないときには、NAT トラバーサルを使用せず、ESP パケットを使って通信する

type に対応した機種同士で接続する場合、*type* を同じ設定にして接続する必要がある。また、*type* に 2 を指定した場合、*type* に対応していない機種との接続はできない。

IKEv2 では、イニシエータとして動作する場合のみ *switch* パラメータが影響する。このオプションは、通信経路上に NAT 処理がなくても NAT トラバーサル動作が必要な対向機器と接続する場合に使用する。なお、通常は 'off' にしておくことが望ましい。

[ノート]

ipsec ike esp-encapsulation コマンドとの併用はできない。

また、IPComp が設定されているトンネルインタフェースでは利用できない。

IKEv1 では、メインモードおよび、アグレッシブモードの ESP トンネルでのみ利用できる。AH では利用できず、トランスポートモードでも利用できない。

ただし、L2TP/IPsec と L2TPv3 を用いた L2VPN で使用される IKEv1 では、メインモードかつトランスポートモードの ESP トンネルでも利用できる。

IKEv2 では、ESP トンネルを確立する場合のみ利用できる。AH では利用できず、トランスポートモードでも利用できない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.47.6 SA の削除

[書式]

ipsec sa delete *id*

[設定値及び初期値]

- *id*
 - [設定値]:

設定値	説明
番号	SA の ID
all	すべての SA

- [初期値]: -

[説明]

指定した SA を削除する。

SA の ID は自動的に付与され、**show ipsec sa** コマンドで確認することができる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.48 トンネルインタフェース関連の設定

11.48.1 IPsec トンネルの外側の IPv4 パケットに対するフラグメントの設定

[書式]

ipsec tunnel fastpath-fragment-function follow df-bit *switch*

no ipsec tunnel fastpath-fragment-function follow df-bit [*switch*]

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	ESP パケットをフラグメントする必要がある場合に ESP パケットの DF ビットに従ってフラグメントするかを決定する

設定値	説明
off	ESP パケットをフラグメントする必要がある場合に ESP パケットの DF ビットに関係なくフラグメントする

- [初期値] : off

[説明]

ESP パケットをフラグメントする必要がある場合に、DF ビットに従ってフラグメントするか否かを設定する。**ipsec tunnel outer df-bit** コマンドによって DF ビットがセットされた ESP パケットであっても本コマンドで off が設定されている場合はフラグメントされる。本コマンドは、トンネルインタフェースに対して設定し、ファストパスで処理される ESP パケットのみを対象とする。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.48.2 IPsec トンネルの外側の IPv4 パケットに対する DF ビットの制御の設定

[書式]

```
ipsec tunnel outer df-bit mode
no ipsec tunnel outer df-bit [mode]
```

[設定値及び初期値]

- mode
- [設定値] :

設定値	説明
copy	内側の IPv4 パケットの DF ビットを外側にもコピーする
set	常に 1
clear	常に 0

- [初期値] : copy

[説明]

IPsec トンネルの外側の IPv4 パケットで、DF ビットをどのように設定するかを制御する。
 copy の場合には、内側の IPv4 パケットの DF ビットをそのまま外側にもコピーする。
 set または clear の場合には、内側の IPv4 パケットの DF ビットに関わらず、外側の IPv4 パケットの DF ビットはそれぞれ 1、または 0 に設定される。
 トンネルインタフェース毎のコマンドである。

[ノート]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.48.3 使用する SA のポリシーの設定

[書式]

```
ipsec tunnel policy_id
no ipsec tunnel [policy_id]
```

[設定値及び初期値]

- policy_id
- [設定値] : 整数 (1..2147483647)
- [初期値] :-

[説明]

選択されているトンネルインタフェースで使用する SA のポリシーを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.48.4 IPComp によるデータ圧縮の設定

[書式]

```
ipsec ipcomp type type
no ipsec ipcomp type [type]
```

[設定値及び初期値]

- *type*
 - [設定値]:

設定値	説明
deflate	deflate 圧縮でデータを圧縮する
none	データ圧縮を行わない

- [初期値]: none

[説明]

IPComp でデータ圧縮を行うかどうかを設定する。サポートしているアルゴリズムは deflate のみである。受信した IPComp パケットを展開するためには、特別な設定を必要としない。すなわち、サポートしているアルゴリズムで圧縮された IPComp パケットを受信した場合には、設定に関係なく展開する。必ずしもセキュリティ・ゲートウェイの両方にこのコマンドを設定する必要はない。片側にのみ設定した場合には、そのセキュリティ・ゲートウェイから送信される IP パケットのみが圧縮される。トランスポートモードのみを使用する場合には、IPComp を使用することはできない。

[ノート]

データ圧縮には、PPP で使われる CCP もある。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、一定の効果を得られる。また、CCP とは異なり、対向のセキュリティ・ゲートウェイまでの全経路で圧縮されたままのデータが流れるため、例えば本機の実出力インタフェースが LAN であってもデータ圧縮効果を期待できる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.48.5 トンネルバックアップの設定

[書式]

```
tunnel backup none
tunnel backup interface ip_address
tunnel backup pp peer_num [switch-router=switch1]
tunnel backup tunnel tunnel_num [switch-interface=switch2]
no tunnel backup
```

[設定値及び初期値]

- none: トンネルバックアップを使用しない
 - [初期値]: -
- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *ip_address*
 - [設定値]: バックアップ先のゲートウェイの IP アドレス
 - [初期値]: -
- *peer_num*
 - [設定値]: バックアップ先の相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -
- *switch1*: バックアップの受け側のルーターを 2 台に分けるか否か
 - [設定値]:

設定値	説明
on	分ける
off	分けない

- [初期値]: off
- *switch2*: LAN/PP インタフェースのバックアップにしたがってトンネルを作り直すか否か
- [設定値]:

設定値	説明
on	作り直す
off	作り直さない

- [初期値]: on

[初期設定]

tunnel backup none

[説明]

トンネルインタフェースに障害が発生したときにバックアップとして利用するインタフェースを指定する。

switch-router オプションについては、以下の2つの条件を満たすときに **on** を設定する。

- バックアップの受け側に2台のルーターがあり、一方がバックアップ元の回線に接続し、もう一方がバックアップ先の回線に接続している。
- バックアップ先の回線に接続しているルーターのファームウェアがこのリビジョンよりも古い。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.48.6 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]: トンネルインタフェース番号、または間にハイフン (-) をはさんでトンネルインタフェース番号を範囲指定したもの
 - [初期値]: -

[説明]

tunnel select コマンドにて選択されたトンネルインタフェースを展開元として、当該インタフェースに設定されているコマンドの展開先となるトンネルインタフェースを設定する。

展開元のトンネルインタフェースに設定することで、展開先のトンネルインタフェースにも適用されるコマンドは以下のとおりである。

- **ipsec tunnel**
- **ipsec sa policy**
- **ipsec ike** で始まるコマンドのうち、パラメータにセキュリティ・ゲートウェイの識別子をとるもの
- **ipsec auto refresh** (引数にセキュリティ・ゲートウェイの識別子を指定する場合)
- **tunnel encapsulation**
- **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フェース番号に一致する場合のみ、コマンドが展開される。その場合、当該パラメータの値は展開先のトンネルインタフェース番号に置換される。

コマンド	パラメータ
ipsec tunnel	ポリシー ID
ipsec sa policy	ポリシー ID
ipsec ike で始まるコマンド	セキュリティ・ゲートウェイの識別子
ipsec auto refresh	セキュリティ・ゲートウェイの識別子
tunnel enable	トンネルインタフェース番号

ipsec sa policy コマンドでは、セキュリティ・ゲートウェイの識別子が展開先のトンネルインタフェース番号に置換される。

ipsec ike remote name コマンドでは、相手側セキュリティ・ゲートウェイの名前の末尾に展開先のトンネルインタフェース番号が付加される。

展開元のトンネルインタフェースに設定されているコマンドと同じコマンドが、展開先のトンネルインタフェースに既に設定されている場合、展開先のトンネルインタフェースに設定されているコマンドが優先される。

コマンド展開後の、ルーターの動作時に参照される設定は **show config tunnel** コマンドに **expand** キーワードを指定することで確認できる。

[ノート]

トンネルインタフェースが選択されている時のみ使用できる。

[設定例]

展開先のトンネルインタフェースとして、番号の指定と範囲の指定を同時に記述することができる。

```
tunnel select 1
tunnel template 8 10-20
tunnel select 2
tunnel template 100 200-300 400
```

以下の 2 つの設定は同じ内容を示している。

```
tunnel select 1
tunnel template 2
ipsec tunnel 1
ipsec sa policy 1 1 esp aes-cbc sha-hmac
ipsec ike encryption 1 aes-cbc
ipsec ike group 1 modp1024
ipsec ike local address 1 192.168.0.1
ipsec ike pre-shared-key 1 text himitsu1
ipsec ike remote address 1 any
ipsec ike remote name 1 pc
tunnel enable 1
tunnel select 2
ipsec ike pre-shared-key 2 text himitsu2
```

```
tunnel select 1
ipsec tunnel 1
ipsec sa policy 1 1 esp aes-cbc sha-hmac
ipsec ike encryption 1 aes-cbc
ipsec ike group 1 modp1024
ipsec ike local address 1 192.168.0.1
ipsec ike pre-shared-key 1 text himitsu1
ipsec ike remote address 1 any
ipsec ike remote name 1 pc
tunnel enable 1
tunnel select 2
ipsec tunnel 2
ipsec sa policy 2 2 esp aes-cbc sha-hmac
ipsec ike encryption 2 aes-cbc
ipsec ike group 2 modp1024
ipsec ike local address 2 192.168.0.1
ipsec ike pre-shared-key 2 text himitsu2
ipsec ike remote address 2 any
ipsec ike remote name 2 pc2
tunnel enable 2
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.49 トランスポートモード関連の設定

11.49.1 トランスポートモードの定義

[書式]

```
ipsec transport id policy_id [proto [src_port_list [dst_port_list]]]
no ipsec transport id [policy_id [proto [src_port_list [dst_port_list]]]]
```

[設定値及び初期値]

- *id*
 - [設定値]: トランスポート ID(1..2147483647)
 - [初期値]: -
- *policy_id*
 - [設定値]: ポリシー ID(1..2147483647)
 - [初期値]: -
- *proto*
 - [設定値]: プロトコル
 - [初期値]: -
- *src_port_list*: UDP 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ク
 - *(すべてのポート)
 - [初期値]: -
- *dst_port_list*: UDP 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。

[ノート]

proto パラメータに *tcp* は指定できない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.49.2 トランスポートモードのテンプレートの設定

[書式]

```
ipsec transport template id1 id2 [id2 ...]
no ipsec transport template id1 [id2 ...]
```

[設定値及び初期値]

- *id1*
 - [設定値]: 展開元のトランスポート ID
 - [初期値]: -
- *id2*
 - [設定値]: 展開先のトランスポート ID、または間にハイフン(-)をはさんでトランスポート ID を範囲指定したもの
 - [初期値]: -

[説明]

指定した **ipsec transport** コマンドの設定の展開先となるトランスポート ID を設定する。展開先のポリシー ID は展開先のトランスポート ID と同じ値が設定される。

展開先のトランスポート ID に対して既に設定が存在する場合、展開先の設定が優先される。

本コマンドによって VPN 対地数まで **ipsec transport** コマンドの設定を展開することができる。VPN 対地数を超える範囲に展開することはできない。

[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 *
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.50 PKI 関連の設定

11.50.1 証明書ファイルの設定

[書式]

```
pki certificate file cert_id file type [password]
no pki certificate file cert_id [file ...]
```

[設定値及び初期値]

- *cert_id*
 - [設定値]:

設定値	説明
1..8	証明書ファイルの識別子

- [初期値]: -

- *file*
 - [設定値]:

設定値	説明
証明書ファイルを絶対パスまたは相対パスで指定する。	証明書ファイルのファイル名

- [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。

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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

11.50.2 CRL ファイルの設定

[書式]

```
pki crl file crl_id file
no pki crl file crl_id [file]
```

[設定値及び初期値]

- *crl_id*
 - [設定値]:

設定値	説明
1..8	CRL ファイルの識別子

- [初期値]: -
- *file*

- [設定値]:

設定値	説明
CRL ファイルを絶対パスまたは相対パスで指定する	CRL ファイルのファイル名

- [初期値]: -

[説明]

CRL ファイルを設定する。

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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

第 12 章

L2TP 機能の設定

L2TP/IPsec 機能

L2TP (Layer Two Tunneling Protocol) は、ネットワーク間での VPN (Virtual Private Network) 接続を実現するトンネリングプロトコルです。L2TP 自体は暗号化の仕組みを持ちませんが、IPsec を併用することでデータの機密性や完全性を確保した VPN 接続を実現する L2TP/IPsec があります。ヤマハルーターは、L2TP/IPsec を用いたリモートアクセス VPN のサーバーとして動作します。スマートフォンなどに搭載されている L2TP クライアントからインターネット越しにヤマハルーター配下のプライベートネットワーク内の端末とのセキュアな通信を可能にします。

ヤマハルーターでサポートする L2TP/IPsec には以下の制限があります。

- L2TP 単体での機能は提供しません。L2TP/IPsec のみサポートします。
- リモートアクセス VPN のサーバーとして動作します。クライアントとしては動作しません。
- LAN 間接続 VPN には対応していません。
- L2TP パケットの最初の待ち受けは UDP のポート番号 1701 が使用されます。変更することはできません。
- IKEv1 にのみ対応しており、IKEv2 は使用できません。

12.1 L2TP を動作させるか否かの設定

[書式]

```
l2tp service service [version [version]]
no l2tp service [service [version [version]]]
```

[設定値及び初期値]

- *service*
 - [設定値]:

設定値	説明
on	L2TP を有効にする
off	L2TP を無効にする

- [初期値]: off
- *version*

- [設定値]:

設定値	説明
l2tp	L2TP/IPsec を有効にする
l2tpv3	L2TPv3, L2TPv3/IPsec を有効にする

- [初期値]: -

[説明]

L2TP を動作させるか否かを設定する。

version によって動作する L2TP のバージョンを指定できる。*version* を指定しない場合には L2TPv2 と L2TPv3 の両方が動作する。

L2TP が有効になると UDP のポート番号 1701 を開き、L2TP コネクションの接続を待つ。

L2TP が無効になると UDP のポート番号 1701 を閉じ、接続中の L2TP コネクションはすべて切断される。

[ノート]

version は L2TPv3 機能が実装されたモデルでのみ指定可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

12.2 L2TP トンネル認証に関する設定

[書式]

```
l2tp tunnel auth switch [password]
no l2tp tunnel auth [switch ...]
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	L2TP トンネル認証を行う
off	L2TP トンネル認証を行わない

- [初期値]: off
- *password*
 - [設定値]: L2TP トンネル認証に用いるパスワード(32 文字以内)
 - [初期値]: -

[説明]

L2TP トンネル認証を行うか否かを設定する。
password を省略した場合には機種名がパスワードとして使用される。
 vRX の場合には "vRX" がパスワードとなる。大文字小文字の区別に注意してください。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

12.3 L2TP トンネルの切断タイマの設定

[書式]

```
l2tp tunnel disconnect time time
no l2tp tunnel disconnect time [time]
```

[設定値及び初期値]

- *time*
 - [設定値]:

設定値	説明
1..21474836	秒数
off	タイマを設定しない

- [初期値]: 60

[説明]

L2TP トンネルの切断タイマを設定する。
 選択されている L2TP トンネルに対して、データパケット無入力・無送信時に、タイムアウトにより L2TP トンネルを切断する時間を設定する。
 L2TP 制御メッセージ以外はすべてデータパケットとなるため、PPP キープアライブを使用する場合などは切断タイマによる L2TP トンネルの切断は行われない場合がある。
 トンネルインタフェースにのみ設定可能です。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

12.4 L2TP キープアライブの設定

[書式]

```
l2tp keepalive use switch [interval [count]]
no l2tp keepalive use [switch ...]
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	L2TP キープアライブを使用する

設定値	説明
off	L2TP キープアライブを使用しない

- [初期値]: on
- *interval*
 - [設定値]: キープアライブパケットを送出する時間間隔[秒] (1..600)
 - [初期値]: 10
- *count*
 - [設定値]: ダウン検出を判定する回数 (1..50)
 - [初期値]: 6

[説明]

L2TP キープアライブを使用するか否かを選択する。

キープアライブを行う場合は *interval* と *count* の設定値の応じて L2TP の Hello メッセージによるキープアライブが動作する。

トンネルインタフェースにのみ設定可能です。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

12.5 L2TP キープアライブのログ設定

[書式]

l2tp keepalive log *log*

no l2tp keepalive log [*log*]

[設定値及び初期値]

- *log*
 - [設定値]:

設定値	説明
on	L2TP キープアライブをログに出力する
off	L2TP キープアライブをログに出力しない

- [初期値]: off

[説明]

L2TP キープアライブのログを出力するか否かを設定する。

ログはすべて、debug レベルの SYSLOG に出力される。

トンネルインタフェースにのみ設定可能です。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

12.6 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 の接続制御に関するログを SYSLOG に出力するか否かを設定する。
 L2TP のキープアライブに関するログは出力されない。
 ログはすべて、debug レベルの SYSLOG に出力される。
 トンネルインタフェースにのみ設定可能です。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

12.7 L2TPv3 の常時接続の設定**[書式]**

```
l2tp always-on sw
no l2tp always-on [sw]
```

[設定値及び初期値]

- *sw*
- [設定値]:

設定値	説明
on	常時接続する
off	常時接続しない

- [初期値]: on

[説明]

L2TPv3 の接続を常時接続するか否かを設定する。
 トンネルインタフェースにのみ設定可能です。

[適用モデル]

vRX VMware ESXi 版

12.8 L2TP トンネルのホスト名の設定**[書式]**

```
l2tp hostname hostname
no l2tp hostname [name]
```

[設定値及び初期値]

- *name*
- [設定値]: ホスト名 (32 文字以内)
- [初期値]: 機種名

[説明]

接続相手に通知するホスト名を設定する。
 show status l2tp コマンドで出力される L2TP トンネル情報に表示される。
 本コマンドを設定しない場合には機種名がホスト名として使用される。
 トンネルインタフェースのみ設定可能です。

[適用モデル]

vRX VMware ESXi 版

12.9 L2TPv3 の Local Router ID の設定**[書式]**

```
l2tp local router-id ipv4_address
no l2tp local router-id [ipv4_address]
```

[設定値及び初期値]

- *ipv4_address*
- [設定値]: IPv4 アドレス
- [初期値]: 0.0.0.0

[説明]

L2TPv3 の接続相手に通知する Router ID を設定する。
 接続相手の Remote Router ID と同じ IPv4 アドレスを設定します。
 ルーターに設定されている IPv4 アドレスを使用する必要はない。
 トンネルインターフェースにのみ設定可能です。

[適用モデル]

vRX VMware ESXi 版

12.10 L2TPv3 の Remote Router ID の設定**[書式]**

```
l2tp remote router-id ipv4_address  
no l2tp remote router-id [ipv4_address]
```

[設定値及び初期値]

- *ipv4_address*
 - [設定値]: IPv4 アドレス
 - [初期値]: 0.0.0.0

[説明]

L2TPv3 の接続相手の Router ID を設定する。
 接続相手の Local Router ID と同じ IPv4 アドレスを設定する。
 ルーターに設定されている IPv4 アドレスを使用する必要はない。
 トンネルインターフェースにのみ設定可能です。

[適用モデル]

vRX VMware ESXi 版

12.11 L2TPv3 の Remote End ID の設定**[書式]**

```
l2tp remote end-id end-id  
no l2tp remote end-id [end-id]
```

[設定値及び初期値]

- *end-id*
 - [設定値]: 任意文字列(32 文字以内)
 - [初期値]: なし

[説明]

L2TPv3 の Remote End ID を設定する。
 接続相手の Remote End ID と同じ文字列を設定する。
 トンネルインターフェースにのみ設定可能です。

[適用モデル]

vRX VMware ESXi 版

12.12 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 インタフェース名
tunnelN-tunnelM	TUNNEL インタフェースの範囲

- [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フェースを指定する。
anonymous インタフェースに対してのみ、複数のトンネルインタフェースが指定できる。
また、連続している複数のトンネルインタフェースの場合は、インタフェース範囲指定が可能である。

[ノート]

L2TP/IPsec の PP 毎に設定する。

tunnel encapsulation コマンドで `l2tp` を設定したトンネルインタフェースをバインドすることによって L2TP/IPsec で通信することを可能にする。

[適用モデル]

vRX VMware ESXi 版

第 13 章

IPIP トンネリング機能の設定

IPIP トンネリング機能

IPIP トンネリング (IP over IP) は、IP パケットにさらに IP ヘッダを付加してカプセル化することでネットワーク間での VPN (Virtual Private Network) 接続を実現するトンネリングプロトコルです。IPIP トンネリングには認証や暗号化の仕組みは無いため、閉域網サービスなど安全な通信が提供されている環境で利用します。

ヤマハルーターでは独自仕様の IPIP キープアライブを使用することができます。IPIP キープアライブを使用すると、以下のようなメリットがあります。

- 対向ルーターの応答を確認してからトンネルを確立することで、確実に対向ルーターにパケットを送信することができます。
- トンネル端点をホスト名で指定している場合に、ホスト名に対応する IP アドレスが変わっても、切断検知後に再度名前解決を行うことで自動的に復旧することができます。

13.1 IPIP キープアライブの設定

[書式]

```
ipip keepalive use switch [interval [count]]
no ipip keepalive use [switch ...]
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	IPIP キープアライブを使用する
off	IPIP キープアライブを使用しない

- [初期値]: off
- *interval*
 - [設定値]: キープアライブパケットを送出する時間間隔[秒] (1..600)
 - [初期値]: 10
- *count*
 - [設定値]: ダウンと見なすまでのキープアライブパケット送信回数 (1..50)
 - [初期値]: 6

[説明]

IPIP キープアライブを使用するか否かを選択する。

キープアライブを行う場合は *interval* と *count* の設定値に応じて独自仕様の IPIP キープアライブが動作する。

トンネルインタフェースにのみ設定可能。

キープアライブ有効時に、*count* 回連続してキープアライブの応答が確認できなければ接続性がないと見なしてトンネルをダウンする。

また、トンネル端点を名前指定している場合は、*count* 回キープアライブを送信しても応答がない場合、再度名前解決を実行する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

13.2 IPIP キープアライブのログ設定

[書式]

```
ipip keepalive log log
no ipip keepalive log [log]
```

[設定値及び初期値]

- *log*
 - [設定値]:

設定値	説明
on	IPIP キープアライブをログに出力する
off	IPIP キープアライブをログに出力しない

- [初期値]: off

[説明]

IPIP キープアライブのログを出力するか否かを設定する。
ログはすべて、`debug` レベルの `SYSLOG` に出力される。
トンネルインタフェースにのみ設定可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

第 14 章

SIP 機能の設定

14.1 共通の設定

14.1.1 SIP を使用するか否かの設定

[書式]

`sip use use`

`no sip use`

[設定値及び初期値]

- `use`

- [設定値]:

設定値	説明
off	使用しない
on	使用する

- [初期値]: off

[説明]

SIP プロトコルを使用するか否かを設定する。

[ノート]

on から off への変更は再起動後有効となる。

[適用モデル]

vRX VMware ESXi 版

14.1.2 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

設定値	説明
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。

[適用モデル]

vRX VMware ESXi 版

14.1.3 SIP による発信時に使用する IP プロトコルの選択

[書式]

sip ip protocol *protocol*

no sip ip protocol

[設定値及び初期値]

- *protocol*
- [設定値] :

設定値	説明
udp	UDP を使用
tcp	TCP を使用

- [初期値] : udp

[説明]

SIP による発信時の呼制御に使用する IP プロトコルを選択する。

[ノート]

着信した場合は、この設定に関わらず、受信したプロトコルで送信を行なう。

[適用モデル]

vRX VMware ESXi 版

14.1.4 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。

[適用モデル]

vRX VMware ESXi 版

14.1.5 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。

[適用モデル]

vRX VMware ESXi 版

14.1.6 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。

[適用モデル]

vRX VMware ESXi 版

14.1.7 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。

[適用モデル]

vRX VMware ESXi 版

14.1.8 SIP による着信時のセッションタイマーのリクエストを設定

[書式]

```

sip arrive session timer method method
no sip arrive session timer method [method]

```

[設定値及び初期値]

- *method*
 - [設定値]:

設定値	説明
auto	自動的に判断する
invite	INVITE のみを使用する

- [初期値]: auto

[説明]

SIP による着信時にセッションタイマー機能で使用するリクエストを設定する。

auto に設定した場合には UPDATE, INVITE とともに使用でき、発信側またはサーバで UPDATE に対応していれば UPDATE を使用する。

invite に設定した場合には、発信側またはサーバで UPDATE に対応していてもこれを使用せずに動作する。

UPDATE のみを使用する設定はできない。

また、サーバ毎に設定することできないため、全ての着信でこの設定が有効となる。

発信の場合は、**sip session timer** の *update* オプションで設定できる。

[適用モデル]

vRX VMware ESXi 版

14.1.9 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。

また、SIP サーバーに RTV01 を利用する場合にも off にする。

[ノート]

この検証は **sip server** 設定がある場合に有効となる。

[適用モデル]

vRX VMware ESXi 版

14.1.10 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。

[適用モデル]

vRX VMware ESXi 版

14.1.11 SIP で使用する IP アドレスの設定

[書式]

sip outer address ipaddress

no sip outer address

[設定値及び初期値]

- *ipaddress*
- [設定値]:

設定値	説明
auto	自動設定
IP アドレス	IP アドレス

- [初期値]: auto

[説明]

SIP で使用する IP アドレスを設定する。RTP/RTCP もこの値が使用される。

[ノート]

初期設定のまま使用する事を推奨する。

[適用モデル]

vRX VMware ESXi 版

14.1.12 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。

[適用モデル]
vRX VMware ESXi 版

14.2 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。

14.2.1 NGN 網に接続するインタフェースの設定

[書式]

```
ngn type interface type
no ngn type interface [type]
```

[設定値及び初期値]

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

設定値	説明
off	NGN 網のサービスを使用しない
ntt	NTT 東日本または NTT 西日本が提供する NGN 網を使用する

- [初期値]: off

[説明]

NGN 網に接続するインタフェースを設定する。

[適用モデル]
vRX VMware ESXi 版

14.2.2 NGN 網を介したトンネルインタフェースの切断タイマの設定

[書式]

```
tunnel ngn disconnect time time
no tunnel ngn disconnect time [time]
```

[設定値及び初期値]

- *time*
 - [設定値]:

設定値	説明
1..21474836	秒数
off	タイマを設定しない

- [初期値]: 60

[説明]

NGN 網を介したトンネルインタフェースのデータ送受信がない場合の切断までの時間を設定する。off に設定した場合は切断しない。

[ノート]

通信中の変更は無効。

[適用モデル]
vRX VMware ESXi 版

14.2.3 NGN 網を介したトンネルインタフェースの帯域幅の設定

[書式]

```
tunnel ngn bandwidth bandwidth [arrivepermit=switch]
no tunnel ngn bandwidth [bandwidth arrivepermit=switch]
```

[設定値及び初期値]

- *bandwidth*
- [設定値]:

設定値	説明
64k	64kbps
512k	512kbps
1m	1Mbps
1k..1000m	帯域

- [初期値]: 1m
- *switch*
- [設定値]:

設定値	説明
on	帯域の設定と一致しない着信も許可する
off	帯域の設定と一致した着信のみ許可する

- [初期値]: on

[説明]

NGN 網を介したトンネルインタフェースの帯域幅を設定した値にする。

帯域の設定が一致しない着信について、`arrivepermit` オプションが `off` の場合は着信せず、`on` の場合は着信する。

[ノート]

通信中の変更は無効。

[適用モデル]

vRX VMware ESXi 版

14.2.4 NGN 網を介したトンネルインタフェースの着信許可の設定

[書式]

```
tunnel ngn arrive permit permit
no tunnel ngn arrive permit [permit]
```

[設定値及び初期値]

- *permit*
- [設定値]:

設定値	説明
on	許可する
off	許可しない

- [初期値]: on

[説明]

選択されている相手からの着信を許可するか否かを設定する。

[ノート]

`tunnel ngn arrive permit`、`tunnel ngn call permit` コマンドとも `off` を設定した場合は通信できない。

[適用モデル]

vRX VMware ESXi 版

14.2.5 NGN 網を介したトンネルインタフェースの発信許可の設定

[書式]

```
tunnel ngn call permit permit
no tunnel ngn call permit [permit]
```


[設定値及び初期値]

- *permit*
 - [設定値]:

設定値	説明
on	許可する
off	許可しない

- [初期値]: on

[説明]

選択されている相手への発信を許可するか否かを設定する。

[ノート]

tunnel ngn arrive permit、**tunnel ngn call permit** コマンドとも off を設定した場合は通信できない。

[適用モデル]

vRX VMware ESXi 版

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

[書式]

tunnel ngn interface *lan*
no tunnel ngn interface [*lan*]

[設定値及び初期値]

- *lan*
 - [設定値]:

設定値	説明
auto	自動設定
LAN インタフェース名	LAN ポート

- [初期値]: auto

[説明]

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

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

追加番号を使用する場合や HGW 配下で使用する場合に設定する。

[適用モデル]

vRX VMware ESXi 版

14.2.7 NGN 網を介したトンネルインタフェースで接続に失敗した場合に接続を試みる相手番号の設定

[書式]

tunnel ngn fallback *remote_tel ...*
no tunnel ngn fallback [*remote_tel ...*]

[設定値及び初期値]

- *remote_tel*
 - [設定値]: 相手電話番号
 - [初期値]: -

[説明]

NGN 網を介したトンネルインタフェースで使用する相手番号は、**ipsec ike remote name** コマンドや **tunnel endpoint name** コマンドで設定した番号に対して発信するが、これが何らかの原因で接続できなかった場合に、設定された番号に対して発信する。

設定は最大 7 個まで可能で、接続に失敗すると設定された順番に次の番号を用いて接続を試みる。

[適用モデル]

vRX VMware ESXi 版

14.2.8 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]

データコネクタを利用した拠点間接続において、着信を受けたときに発信元の NGN 電話番号を RADIUS で認証するか否かを設定する。

[ノート]

トンネルインタフェースが選択されている時にのみ使用できる。

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**

[適用モデル]

vRX VMware ESXi 版

14.2.9 NGN 電話番号を RADIUS で認証するとき使用するパスワードの設定

[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 で認証するとき使用するパスワードを設定する。NGN 電話番号をユーザー名、当コマンドで設定した文字列をパスワードとして RADIUS サーバーに問い合わせを行う。

PASSWORD に使用できる文字は半角英数字および記号 (7bit ASCII Code で表示可能なもの) で、文字列の長さは 0 文字以上 64 文字以下となる。

[ノート]

当コマンドが設定されていない場合は、NGN 電話番号を RADIUS で認証することができない。

[適用モデル]

vRX VMware ESXi 版

14.2.10 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**

[適用モデル]

vRX VMware ESXi 版

14.2.11 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**

[適用モデル]

vRX VMware ESXi 版

14.2.12 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

設定値	説明
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。

[適用モデル]

vRX VMware ESXi 版

14.2.13 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。

[適用モデル]

vRX VMware ESXi 版

第 15 章

SNMP の設定

SNMP (Simple Network Management Protocol) の設定を行うことにより、SNMP 管理ソフトウェアに対してネットワーク管理情報のモニタと変更を行うことができます。このときヤマハルーターは SNMP エージェントとなります。

ヤマハルーターは SNMPv1、SNMPv2c、SNMPv3 による通信に対応しています。また MIB (Management information Base) として RFC1213 (MIB-II) とプライベート MIB に対応しています。プライベート MIB については以下の URL から参照することができます。

- YAMAHA private MIB: <http://www.rtpro.yamaha.co.jp/RT/docs/mib/>

SNMPv1 および SNMPv2c では、コミュニティと呼ばれるグループの名前を相手に通知し、同じコミュニティに属するホスト間でのみ通信します。このとき、読み出し専用 (read-only) と読み書き可能 (read-write) の 2 つのアクセスモードに対して別々にコミュニティ名を設定することができます。

このようにコミュニティ名はある種のパスワードとして機能しますが、その反面、コミュニティ名は必ず平文でネットワーク上を流れるという特性があり、セキュリティ面では脆弱と言えます。よりセキュアな通信が必要な場合は SNMPv3 の利用を推奨します。

SNMPv3 では通信内容の認証、および暗号化に対応しています。SNMPv3 はコミュニティの概念を廃し、新たに USM (User-based Security Model) と呼ばれるセキュリティモデルを利用することで、より高度なセキュリティを確保しています。

ヤマハルーターの状態を通知する SNMP メッセージをトラップと呼びます。ヤマハルーターでは SNMP 標準トラップの他にも、一部機能で特定のイベントを通知するため独自のトラップを送信することがあります。なお、これらの独自トラップはプライベート MIB として定義されています。

トラップの送信先ホストについては、各 SNMP バージョン毎に複数のホストを設定することができます。

SNMPv1 および SNMPv2c で利用する読み出し専用と送信トラップ用のコミュニティ名は、共に初期値が "public" となっています。SNMP 管理ソフトウェア側も "public" がコミュニティ名である場合が多いため、当該バージョンの通信でセキュリティを考慮する場合は適切なコミュニティ名に変更してください。ただし、上述の通りコミュニティ名はネットワーク上を平文で流れますので、コミュニティ名にログインパスワードや管理パスワードを決して使用しないよう注意してください。

工場出荷状態では、各 SNMP バージョンにおいてアクセスが一切できない状態となっています。また、トラップの送信先ホストは設定されておらず、どこにもトラップを送信しません。

15.1 SNMPv1 によるアクセスを許可するホストの設定

[書式]

```
snmp host host [ro_community [rw_community]]
no snmp host [host]
```

[設定値及び初期値]

- *host*: SNMPv1 によるアクセスを許可するホスト
 - [設定値]:

設定値	説明
<i>ip_address</i>	1 個の IP アドレスまたは間にハイフン(-)をはさんだ IP アドレス (範囲指定)
<i>lanN</i>	LAN インターフェース名
<i>any</i>	すべてのホストからのアクセスを許可する
<i>none</i>	すべてのホストからのアクセスを禁止する

- [初期値]: none
- *ro_community*
 - [設定値]: 読み出し専用のコミュニティ名 (16 文字以内)
 - [初期値]: -
- *rw_community*
 - [設定値]: 読み書き可能なコミュニティ名 (16 文字以内)
 - [初期値]: -

[説明]

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` 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.2 SNMPv1 の読み出し専用のコミュニティ名の設定

[書式]

snmp community read-only name

no snmp community read-only

[設定値及び初期値]

- *name*
 - [設定値]: コミュニティ名 (16 文字以内)
 - [初期値]: public

[説明]

SNMPv1 によるアクセスモードが読み出し専用であるコミュニティ名を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.3 SNMPv1 の読み書き可能なコミュニティ名の設定

[書式]

snmp community read-write name

no snmp community read-write

[設定値及び初期値]

- *name*
 - [設定値]: コミュニティ名 (16 文字以内)
 - [初期値]: -

[説明]

SNMPv1 によるアクセスモードが読み書き可能であるコミュニティ名を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.4 SNMPv1 トラップの送信先の設定

[書式]

snmp trap host host [community]

no snmp trap host host

[設定値及び初期値]

- *host*
 - [設定値]: SNMPv1 トラップの送信先ホストの IP アドレス (IPv4/IPv6)
 - [初期値]: -
- *community*
 - [設定値]: コミュニティ名 (16 文字以内)
 - [初期値]: -

[説明]

SNMPv1 トラップを送信するホストを指定する。コマンドを複数設定することで、複数のホストを同時に指定できる。トラップ送信時のコミュニティ名にはこのコマンドの *community* パラメータが用いられるが、省略されている場合には **snmp trap community** コマンドの設定値が用いられる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.5 SNMPv1 トラップのコミュニティ名の設定

[書式]

```
snmp trap community name
no snmp trap community
```

[設定値及び初期値]

- *name*
 - [設定値]: コミュニティ名 (16 文字以内)
 - [初期値]: public

[説明]

SNMPv1 トラップを送信する際のコミュニティ名を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.6 SNMPv2c によるアクセスを許可するホストの設定

[書式]

```
snmpv2c host host [ro_community [rw_community]]
no snmpv2c host [host]
```

[設定値及び初期値]

- *host*: SNMPv2c によるアクセスを許可するホスト
 - [設定値]:

設定値	説明
<i>ip_address</i>	1 個の IP アドレスまたは間にハイフン(-)をはさんだ IP アドレス (範囲指定)
<i>lanN</i>	LAN インターフェース名
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* 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.7 SNMPv2c の読み出し専用のコミュニティ名の設定

[書式]

```
snmpv2c community read-only name
no snmpv2c community read-only
```

[設定値及び初期値]

- *name*
 - [設定値]: コミュニティ名 (16 文字以内)
 - [初期値]: public

[説明]

SNMPv2c によるアクセスモードが読み出し専用であるコミュニティ名を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.8 SNMPv2c の読み書き可能なコミュニティ名の設定

[書式]

```
snmpv2c community read-write name
no snmpv2c community read-write
```

[設定値及び初期値]

- *name*
 - [設定値]: コミュニティ名 (16 文字以内)
 - [初期値]: -

[説明]

SNMPv2c によるアクセスモードが読み書き可能であるコミュニティ名を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.9 SNMPv2c トラップの送信先の設定

[書式]

```
snmpv2c trap host host [type [community]]
no snmpv2c trap host host
```

[設定値及び初期値]

- *host*
 - [設定値]: SNMPv2c トラップの送信先ホストの IP アドレス (IPv4/IPv6)
 - [初期値]: -
- *type*: メッセージタイプ
 - [設定値]:

設定値	説明
trap	トラップを送信する
inform	Inform リクエストを送信する

- [初期値]: trap
- *community*
 - [設定値]: コミュニティ名 (16 文字以内)
 - [初期値]: -

[説明]

SNMPv2c トラップを送信するホストを指定する。コマンドを複数設定することで、複数のホストを同時に指定できる。トラップ送信時のコミュニティ名にはこのコマンドの *community* パラメータが用いられるが、省略されている場合には **snmpv2c trap community** コマンドの設定値が用いられる。

type パラメータで 'inform' を指定した場合は、送信先からの応答があるまで、5 秒間隔で最大 3 回再送する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.10 SNMPv2c トラップのコミュニティ名の設定

[書式]

```
snmpv2c trap community name
no snmpv2c trap community
```

[設定値及び初期値]

- *name*
 - [設定値]: コミュニティ名 (16 文字以内)
 - [初期値]: public

[説明]

SNMPv2c トラップを送信する際のコミュニティ名を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.11 SNMPv3 エンジン ID の設定

[書式]

```
snmpv3 engine id engine_id
no snmpv3 engine id
```

[設定値及び初期値]

- *engine_id*
 - [設定値]: SNMP エンジン ID (27 文字以内)
 - [初期値]: LAN1 の MAC アドレス

[説明]

SNMP エンジンを識別するためのユニークな ID を設定する。SNMP エンジン ID は SNMPv3 通信で相手先に通知される。

相手先に通知されるフォーマットは以下。

- *engine_id* が初期値の場合
「8000049e03」 + (LAN1 の MAC アドレス)
- *engine_id* に任意の値を設定した場合
「8000049e04」 + 設定値の ASCII 文字列

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.12 SNMPv3 コンテキスト名の設定

[書式]

```
snmpv3 context name name
no snmpv3 context name
```

[設定値及び初期値]

- *name*
 - [設定値]: SNMP コンテキスト名 (16 文字以内)
 - [初期値]: -

[説明]

SNMP コンテキストを識別するための名前を設定する。SNMP コンテキスト名は SNMPv3 通信で相手先に通知される。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.13 SNMPv3 USM で管理するユーザの設定

[書式]

```
snmpv3 usm user user_id name [group group_id] [auth auth_pass [priv priv_pass]]
no snmpv3 usm user user_id
```

[設定値及び初期値]

- *user_id*
 - [設定値]: ユーザ番号 (1..65535)
 - [初期値]: -
- *name*
 - [設定値]: ユーザ名 (32 文字以内)
 - [初期値]: -
- *group_id*
 - [設定値]: ユーザグループ番号 (1..65535)
 - [初期値]: -
- *auth*: 認証アルゴリズム

- [設定値]:

設定値	説明
md5	HMAC-MD5-96
sha	HMAC-SHA1-96

- [初期値]: -

- *auth_pass*

- [設定値]: 認証パスワード (8 文字以上、32 文字以内)
- [初期値]: -

- *priv*: 暗号アルゴリズム

- [設定値]:

設定値	説明
des-cbc	DES-CBC
aes128-cfb	AES128-CFB

- [初期値]: -

- *priv_pass*

- [設定値]: 暗号パスワード (8 文字以上、32 文字以内)
- [初期値]: -

[説明]

SNMPv3 によるアクセスが可能なユーザ情報を設定する。

ユーザグループ番号を指定した場合は VACM によるアクセス制御の対象となる。指定しない場合、そのユーザはすべての MIB オブジェクトにアクセスできる。

SNMPv3 では通信内容の認証および暗号化が可能であり、本コマンドでユーザ名と共にアルゴリズムおよびパスワードを設定して使用する。なお、認証を行わず暗号化のみを行うことはできない。

認証や暗号化の有無、アルゴリズムおよびパスワードは、対向となる SNMP マネージャ側のユーザ設定と一致させておく必要がある。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.14 SNMPv3 によるアクセスを許可するホストの設定

[書式]

```
snmpv3 host host user user_id ...
```

```
snmpv3 host none
```

```
no snmpv3 host [host]
```

[設定値及び初期値]

- *host*: SNMPv3 によるアクセスを許可するホスト

- [設定値]:

設定値	説明
<i>ip_address</i>	1 個の IP アドレスまたは間にハイフン(-)をはさんだ IP アドレス (範囲指定)
<i>lanN</i>	LAN インターフェース名
any	すべてのホストからのアクセスを許可する

- [初期値]: -

- none: すべてのホストからのアクセスを禁止する

- [初期値]: none

- *user_id*: ユーザ番号

- [設定値]:

- 1 個の数字、または間に - をはさんだ数字 (範囲指定)、およびこれらを任意に並べたもの (128 個以内)

- [初期値]: -

[説明]

SNMPv3 によるアクセスを許可するホストを設定する。

host パラメータに 'any' を設定した場合は任意のホストからの SNMPv3 によるアクセスを許可する。なお、アクセス

のあったホストが *host* パラメータに合致していても、*user_id* パラメータで指定したユーザに合致しなければアクセスはできない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.15 SNMPv3 VACM で管理する MIB ビューファミリの設定

[書式]

```
snmpv3 vacm view view_id type oid [type oid ...]
```

```
no snmpv3 vacm view view_id
```

[設定値及び初期値]

- *view_id*
 - [設定値]: ビュー番号 (1..65535)
 - [初期値]: -
- *type*
 - [設定値]:

設定値	説明
include	指定したオブジェクト ID を管理対象にする
exclude	指定したオブジェクト ID を管理対象から除外する

- [初期値]: -
- *oid*
 - [設定値]: MIB オブジェクト ID (サブ ID の数は 2 個以上、128 個以下)
 - [初期値]: -

[説明]

VACM による管理で使用する MIB ビューファミリを設定する。MIB ビューファミリとは、アクセス権を許可する際に指定する MIB 変数の集合である。

type パラメータと *oid* パラメータの組は、指定のオブジェクト ID 以降の MIB サブツリーを管理対象とする／しないことを意味する。また複数の組を指定した際に、それぞれ指定したオブジェクト ID の中で包含関係にあるものは、より下位の階層まで指定したオブジェクト ID に対応する *type* パラメータが優先される。128 組まで指定可能。

[設定例]

- inetnet サブツリー (1.3.6.1) 以降を管理対象とする。ただし enterprises サブツリー (1.3.6.1.4.1) 以降は管理対象から除外する

```
# snmpv3 vacm view 1 include 1.3.6.1 exclude 1.3.6.1.4.1
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.16 SNMPv3 VACM で管理するアクセスポリシーの設定

[書式]

```
snmpv3 vacm access group_id read read_view write write_view
```

```
no snmpv3 vacm access group_id
```

[設定値及び初期値]

- *group_id*
 - [設定値]: グループ番号 (1..65535)
 - [初期値]: -
- *read_view*
 - [設定値]:

設定値	説明
<i>view_id</i>	読み出し可能なアクセス権を設定するビュー番号
none	読み出し可能なビューを設定しない

- [初期値]: -
- *write_view*

- [設定値]:

設定値	説明
<i>view_id</i>	書き込み可能なアクセス権を設定するビュー番号
none	書き込み可能なビューを設定しない

- [初期値]: -

[説明]

ユーザグループに対してアクセスできる MIB ビューファミリを設定する。このコマンドで設定された MIB ビューファミリに含まれない MIB 変数へのアクセスは禁止される。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.17 SNMPv3 トラップの送信先の設定

[書式]

```
snmpv3 trap host host [type] user user_id
no snmpv3 trap host host
```

[設定値及び初期値]

- *host*
 - [設定値]: SNMPv3 トラップの送信先ホストの IP アドレス (IPv4/IPv6)
 - [初期値]: -
- *type*: メッセージタイプ
 - [設定値]:

設定値	説明
trap	トラップを送信する
inform	Inform リクエストを送信する

- [初期値]: trap
- *user_id*
 - [設定値]: ユーザ番号
 - [初期値]: -

[説明]

SNMPv3 トラップを送信するホストを指定する。コマンドを複数設定することで、複数のホストを同時に指定できる。トラップ送信時のユーザ設定は **snmpv3 usm user** コマンドで設定したユーザ設定が用いられる。

type パラメータで 'inform' を指定した場合は、送信先からの応答があるまで、5 秒間隔で最大 3 回再送する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.18 SNMP 送信パケットの始点アドレスの設定

[書式]

```
snmp local address ip_address
no snmp local address
```

[設定値及び初期値]

- *ip_address*
 - [設定値]: IP アドレス (IPv4/IPv6)
 - [初期値]: インタフェースに設定されているアドレスから自動選択

[説明]

SNMP 送信パケットの始点 IP アドレスを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.19 sysContact の設定

[書式]

```
snmp syscontact name
no snmp syscontact
```

[設定値及び初期値]

- *name*
 - [設定値]: sysContact として登録する名称 (255 文字以内)
 - [初期値]: -

[説明]

MIB 変数 sysContact を設定する。空白を含ませるためには、パラメータ全体をダブルクォート (")、もしくはシングルクォート (') で囲む。

sysContact は一般的に、管理者の名前や連絡先を記入しておく変数である。

[設定例]

```
# snmp syscontact "RT administrator"
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.20 sysLocation の設定

[書式]

```
snmp syslocation name
no snmp syslocation
```

[設定値及び初期値]

- *name*
 - [設定値]: sysLocation として登録する名称 (255 文字以内)
 - [初期値]: -

[説明]

MIB 変数 sysLocation を設定する。空白を含ませるためには、パラメータ全体をダブルクォート (")、もしくはシングルクォート (') で囲む。

sysLocation は一般的に、機器の設置場所を記入しておく変数である。

[設定例]

```
# snmp syslocation "RT room"
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.21 sysName の設定

[書式]

```
snmp sysname name
no snmp sysname
```

[設定値及び初期値]

- *name*
 - [設定値]: sysName として登録する名称 (255 文字以内)
 - [初期値]: -

[説明]

MIB 変数 sysName を設定する。空白を含ませるためには、パラメータ全体をダブルクォート (")、もしくはシングルクォート (') で囲む。

sysName は一般的に、機器の名称を記入しておく変数である。

[設定例]

```
# snmp sysname "vRX"
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.22 SNMP 標準トラップを送信するか否かの設定

[書式]

snmp trap enable snmp trap [*trap...*]**snmp trap enable snmp all****no snmp trap enable snmp**

[設定値及び初期値]

- *trap* : 標準トラップの種類

- [設定値] :

設定値	説明
coldstart	電源投入時
warmstart	再起動時
linkdown	リンクダウン時
linkup	リンクアップ時
authenticationfailure	認証失敗時

- [初期値] : -

- all : 全ての標準トラップを送信する

- [初期値] : -

[初期設定]

snmp trap enable snmp all

[説明]

SNMP 標準トラップを送信するか否かを設定する。

all を設定した場合には、すべての標準トラップを送信する。個別にトラップを設定した場合には、設定されたトラップだけが送信される。

[ノート]

authenticationFailure トラップを送信するか否かはこのコマンドによって制御される。

coldStart トラップは、電源投入、再投入による起動後に coldStart トラップを送信する。

linkDown トラップは、**snmp trap send linkdown** コマンドによってインタフェース毎に制御できる。あるインタフェースについて、linkDown トラップが送信されるか否かは、**snmp trap send linkdown** コマンドで送信が許可されており、かつ、このコマンドでも許可されている場合に限られる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.23 CPU 使用率監視機能による SNMP トラップを送信するか否かの設定

[書式]

snmp trap cpu threshold switch**no snmp trap cpu threshold**

[設定値及び初期値]

- *switch*

- [設定値] :

設定値	説明
on	送信する
off	送信しない

- [初期値] : off

[説明]

system cpu threshold コマンドにより設定した警告を発する CPU 使用率の閾値の上限を超える、または、閾値の下限を下回った際に SNMP トラップを送信するか否かの設定

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.24 メモリ使用率監視機能による SNMP トラップを送信するか否かの設定

[書式]

```
snmp trap memory threshold switch
no snmp trap memory threshold
```

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: off

[説明]

system memory threshold コマンドにより設定した警告を発するメモリ使用率の閾値の上限を超える、または、閾値の下限を下回った際に SNMP トラップを送信するか否かの設定

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.25 SNMP トラップの送信の遅延時間の設定

[書式]

```
snmp trap delay-timer [wait]
snmp trap delay-timer off
no snmp trap delay-timer [wait]
```

[設定値及び初期値]

- *wait*
- [設定値]: SNMP トラップを送信するまでの遅延時間の秒数 (1..21474836)
- [初期値]: -

[説明]

SNMP トラップを送信するイベントが発生してからトラップを送信するまでの間隔を指定する。off を設定した場合、即座に SNMP トラップを送信する。設定する遅延時間は最低限保証する値であり、設定値以上遅延する場合もある。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.26 SNMP の linkDown トラップの送信制御の設定

[書式]

```
snmp trap send linkdown interface switch
snmp trap send linkdown pp peer_num switch
snmp trap send linkdown tunnel tunnel_num switch
no snmp trap send linkdown interface
no snmp trap send linkdown pp peer_num
no snmp trap send linkdown tunnel tunnel_num
```

[設定値及び初期値]

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

- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -
- *switch*
 - [設定値]:

設定値	説明
on	送信する
off	送信しない

- [初期値]: on

[説明]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.27 PP インタフェースの情報を MIB2 の範囲で表示するか否かの設定

[書式]

```
snmp yrifppdisplayatmib2 switch
no snmp yrifppdisplayatmib2
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	MIB 変数 yrIfPpDisplayAtMib2 を "enabled(1)" とする
off	MIB 変数 yrIfPpDisplayAtMib2 を "disabled(2)" とする

- [初期値]: off

[説明]

MIB 変数 yrIfPpDisplayAtMib2 の値をセットする。この MIB 変数は、PP インタフェースを MIB2 の範囲で表示するかどうかを決定する。Rev.4 以前と同じ表示にする場合には、MIB 変数を "enabled(1)" に、つまり、このコマンドで on を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.28 トンネルインタフェースの情報を MIB2 の範囲で表示するか否かの設定

[書式]

```
snmp yriftunneldisplayatmib2 switch
no snmp yriftunneldisplayatmib2
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	MIB 変数 yrIfTunnelDisplayAtMib2 を "enabled(1)" とする
off	MIB 変数 yrIfTunnelDisplayAtMib2 を "disabled(2)" とする

- [初期値]: off

[説明]

MIB 変数 `yrIfTunnelDisplayAtMib2` の値をセットする。この MIB 変数は、トンネルインタフェースを MIB2 の範囲で表示するかどうかを決定する。Rev.4 以前と同じ表示にする場合には、MIB 変数を "enabled(1)" に、つまり、このコマンドで `on` を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

15.29 PP インタフェースのアドレスの強制表示の設定

[書式]

```
snmp display ipcp force switch
```

```
no snmp display ipcp force
```

[設定値及び初期値]

- `switch`

- [設定値]:

設定値	説明
on	IPCP により付与された IP アドレスを PP インタフェースのアドレスとして必ず表示する
off	IPCP により付与された IP アドレスは PP インタフェースのアドレスとして必ずしも表示されない

- [初期値]: off

[説明]

NAT を使用しない場合や、NAT の外側アドレスとして固定の IP アドレスが指定されている場合には、IPCP で得られた IP アドレスはそのまま PP インタフェースのアドレスとして使われる。この場合、SNMP では通常のインタフェースの IP アドレスを調べる手順で IPCP としてどのようなアドレスが得られたのか調べることができる。

しかし、NAT の外側アドレスとして 'ipcp' と指定している場合には、IPCP で得られた IP アドレスは NAT の外側アドレスとして使用され、インタフェースには付与されない。そのため、SNMP でインタフェースの IP アドレスを調べても、IPCP でどのようなアドレスが得られたのかを知ることができない。

本コマンドを `on` に設定しておく、IPCP で得られた IP アドレスが NAT の外側アドレスとして使用される場合でも、SNMP ではそのアドレスをインタフェースのアドレスとして表示する。アドレスが実際にインタフェースに付与されるわけではないので、始点 IP アドレスとして、その IP アドレスが利用されることはない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

第 16 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。

16.1 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名 (PAP であれば UserID、CHAP であれば NAME) が、自分で持つユーザー名 (**pp auth username** コマンドで指定) の中に含まれていない場合には RADIUS サーバーに問い合わせるか否かを設定する。

[ノート]

RADIUS による認証と RADIUS によるアカウントは独立して使用できる。
サポートしているアトリビュートについては、WWW サイトのドキュメント<<http://www.rtpro.yamaha.co.jp>> を参照すること。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

16.2 RADIUS によるアカウントを使用するか否かの設定

[書式]

```
radius account account
no radius account [account]
```

[設定値及び初期値]

- *account*
 - [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: off

[説明]

RADIUS によるアカウントを使用するか否かを設定する。

[ノート]

RADIUS による認証と RADIUS によるアカウントは独立して使用できる。
サポートしているアトリビュートについては、WWW サイトのドキュメント<<http://www.rtpro.yamaha.co.jp>> を参照すること。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

16.3 RADIUS サーバーの指定

[書式]

```
radius server ip1 [ip2]
no radius server [ip1 [ip2]]
```

[設定値及び初期値]

- *ip1*
 - [設定値]: RADIUS サーバー(正)の IP アドレス (IPv6 アドレス可)
 - [初期値]: -
- *ip2*
 - [設定値]: RADIUS サーバー(副)の IP アドレス (IPv6 アドレス可)
 - [初期値]: -

[説明]

RADIUS サーバーを設定する。2 つまで指定でき、最初のサーバーから返事をもらえない場合は、2 番目のサーバーに問い合わせを行う。

[ノート]

RADIUS には認証とアカウントの 2 つの機能があり、それぞれのサーバーは **radius auth server/radius account server** コマンドで個別に設定できる。**radius server** コマンドでの設定は、これら個別の設定が行われていない場合に有効となり、認証、アカウントいずれでも用いられる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

16.4 RADIUS 認証サーバーの指定

[書式]

```
radius auth server ip1 [ip2]
no radius auth server [ip1 [ip2]]
```

[設定値及び初期値]

- *ip1*
 - [設定値]: RADIUS 認証サーバー(正)の IP アドレス (IPv6 アドレス可)
 - [初期値]: -
- *ip2*
 - [設定値]: RADIUS 認証サーバー(副)の IP アドレス (IPv6 アドレス可)
 - [初期値]: -

[説明]

RADIUS 認証サーバーを設定する。2 つまで指定でき、最初のサーバーから返事をもらえない場合は、2 番目のサーバーに問い合わせを行う。

[ノート]

このコマンドで RADIUS 認証サーバーの IP アドレスが指定されていない場合は、**radius server** コマンドで指定した IP アドレスを認証サーバーとして用いる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

16.5 RADIUS アカウントサーバーの指定

[書式]

```
radius account server ip1 [ip2]
no radius account server [ip1 [ip2]]
```

[設定値及び初期値]

- *ip1*
 - [設定値]: RADIUS アカウントサーバー(正)の IP アドレス (IPv6 アドレス可)
 - [初期値]: -
- *ip2*
 - [設定値]: RADIUS アカウントサーバー(副)の IP アドレス (IPv6 アドレス可)
 - [初期値]: -

[説明]

RADIUS アカウントサーバーを設定する。2 つまで指定でき、最初のサーバーから返事をもらえない場合は、2 番目のサーバーに問い合わせを行う。

[ノート]

このコマンドで RADIUS アカウントサーバーの IP アドレスが指定されていない場合は、**radius server** コマンドで指定した IP アドレスをアカウントサーバーとして用いる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

16.6 RADIUS 認証サーバーの UDP ポートの設定

[書式]

```
radius auth port port_num  
no radius auth port [port_num]
```

[設定値及び初期値]

- *port_num*
 - [設定値]: UDP ポート番号
 - [初期値]: 1645

[説明]

RADIUS 認証サーバーの UDP ポート番号を設定する

[ノート]

RFC2138 ではポート番号として 1812 を使うことになっている。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

16.7 RADIUS アカウントサーバーの UDP ポートの設定

[書式]

```
radius account port port_num  
no radius account port [port_num]
```

[設定値及び初期値]

- *port_num*
 - [設定値]: UDP ポート番号
 - [初期値]: 1646

[説明]

RADIUS アカウントサーバーの UDP ポート番号を設定する。

[ノート]

RFC2138 ではポート番号として 1813 を使うことになっている。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

16.8 RADIUS シークレットの設定

[書式]

```
radius secret secret  
no radius secret [secret]
```

[設定値及び初期値]

- *secret*
 - [設定値]: シークレット文字列 (16 文字以内)
 - [初期値]: -

[説明]

RADIUS シークレットを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

16.9 RADIUS 再送信パラメータの設定

[書式]

radius retry count time

no radius retry [*count time*]

[設定値及び初期値]

- *count*
 - [設定値]: 再送回数 (1..10)
 - [初期値]: 4
- *time*
 - [設定値]: ミリ秒 (20..10000)
 - [初期値]: 3000

[説明]

RADIUS パケットの再送回数とその時間間隔を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

第 17 章

NAT 機能

NAT 機能は、ルーターが転送する IP パケットの始点/終点 IP アドレスや、TCP/UDP のポート番号を変換することにより、アドレス体系の異なる IP ネットワークを接続することができる機能です。

NAT 機能を用いると、プライベートアドレス空間とグローバルアドレス空間との間でデータを転送したり、1 つのグローバル IP アドレスに複数のホストを対応させたりすることができます。

ヤマハルーターでは、始点/終点 IP アドレスの変換だけを行うことを NAT と呼び、TCP/UDP のポート番号の変換を伴うものを IP マスカレードと呼んでいます。

アドレス変換規則を表す記述を NAT ディスクリプタと呼び、それぞれの NAT ディスクリプタには、アドレス変換の対象とすべきアドレス空間が定義されます。アドレス空間の記述には、**nat descriptor address inner**、**nat descriptor address outer** コマンドを用います。前者は NAT 処理の内側 (INNER) のアドレス空間を、後者は NAT 処理の外側 (OUTER) のアドレス空間を定義するコマンドです。原則的に、これら 2 つのコマンドを対で設定することにより、変換前のアドレスと変換後のアドレスとの対応づけが定義されます。

NAT ディスクリプタはインタフェースに対して適用されます。インタフェースに接続された先のネットワークが NAT 処理の外側であり、インタフェースから本機を経由して他のインタフェースから繋がるネットワークが NAT 処理の内側になります。

NAT ディスクリプタは動作タイプ属性を持ちます。IP マスカレードやアドレスの静的割当てなどの機能を利用する場合には、該当する動作タイプを選択する必要があります。

17.1 NAT 機能の動作タイプの設定

[書式]

```
nat descriptor backward-compatibility type
no nat descriptor backward-compatibility [type]
```

[設定値及び初期値]

- *type*
 - [設定値]:

設定値	説明
1	Rev.14 系以前の動作タイプ (ポートセービング IP マスカレード機能を無効にする)
2	Rev.14.01 系以降の動作タイプ (ポートセービング IP マスカレード機能を有効にする)

- [初期値]: 2

[説明]

NAT 機能全体の動作タイプを設定する。

ポートセービング IP マスカレード機能に対応しており、IP マスカレードにおいて同一のポート番号を使用して複数の接続先とのセッションを確立できる。本コマンドは、ポートセービング IP マスカレード機能をサポートしていない Rev.14 系以前の機種との互換性維持のために用意されており、*type* パラメータを 1 に設定した場合の NAT 機能の動作は、Rev.14 系以前の NAT 機能の動作と同等となる。*type* パラメータを 2 に設定して動作させた場合に問題が生じる場合は、*type* パラメータを 1 にして NAT 機能を使用する必要がある。

[ノート]

本コマンドによる設定の変更を反映するには、ルーターの再起動が必要となる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

17.2 インタフェースへの NAT ディスクリプタ適用の設定

[書式]

```
ip interface nat descriptor nat_descriptor_list [reverse nat_descriptor_list]
ip pp nat descriptor nat_descriptor_list [reverse nat_descriptor_list]
ip tunnel nat descriptor nat_descriptor_list [reverse nat_descriptor_list]
```

```
no ip interface nat descriptor [nat_descriptor_list [reverse nat_descriptor_list]]
no ip pp nat descriptor [nat_descriptor_list [reverse nat_descriptor_list]]
no ip tunnel nat descriptor [nat_descriptor_list [reverse nat_descriptor_list]]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *nat_descriptor_list*
 - [設定値]: 空白で区切られた NAT ディスクリプタ番号 (1..2147483647) の並び (16 個以内)
 - [初期値]: -

[説明]

適用されたインタフェースを通過するパケットに対して、リストに定義された順番で NAT ディスクリプタによって定義された NAT 変換を順番に処理する。

reverse の後ろに記述した NAT ディスクリプタでは、通常処理される IP アドレス、ポート番号とは逆向きの IP アドレス、ポート番号に対して NAT 変換を施す。

[ノート]

LAN インタフェースの場合、NAT ディスクリプタの外側アドレスに対しては、同一 LAN の ARP 要求に対して応答する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

17.3 NAT ディスクリプタの動作タイプの設定

[書式]

```
nat descriptor type nat_descriptor type
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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

17.4 NAT 処理の外側 IP アドレスの設定

[書式]

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

[設定値及び初期値]

- *nat_descriptor*

- [設定値]: NAT ディスクリプタ番号 (1..2147483647)
- [初期値]: -
- *outer_ipaddress_list*: NAT 対象の外側 IP アドレス範囲のリストまたはニーモニック
- [設定値]:

設定値	説明
IP アドレス	1 個の IP アドレスまたは間に - をはさんだ IP アドレス (範囲指定)、およびこれらを任意に並べたもの
ipcp	PPP の IPCP の IP-Address オプションにより接続先から通知される IP アドレス
primary	ip interface address コマンドで設定されている IP アドレス
secondary	ip interface secondary address コマンドで設定されている IP アドレス

- [初期値]: ipcp

[説明]

動的 NAT 処理の対象である外側の IP アドレスの範囲を指定する。IP マスカレードでは、先頭の 1 個の外側の IP アドレスが使用される。

[ノート]

ニーモニックをリストにすることはできない。
適用されるインタフェースにより使用できるパラメータが異なる。

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

17.5 NAT 処理の内側 IP アドレスの設定

[書式]

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

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]: NAT ディスクリプタ番号 (1..2147483647)
 - [初期値]: -
- *inner_ipaddress_list*: NAT 対象の内側 IP アドレス範囲のリストまたはニーモニック
- [設定値]:

設定値	説明
IP アドレス	1 個の IP アドレスまたは間に - をはさんだ IP アドレス (範囲指定)、およびこれらを任意に並べたもの
auto	すべて

- [初期値]: auto

[説明]

NAT/IP マスカレード処理の対象である内側の IP アドレスの範囲を指定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

17.6 静的 NAT エントリの設定

[書式]

```

nat descriptor static nat_descriptor id outer_ip=inner_ip [count]
nat descriptor static nat_descriptor id outer_ip=inner_ip/netmask
no nat descriptor static nat_descriptor id [outer_ip=inner_ip [count]]

```

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]: NAT ディスクリプタ番号 (1..2147483647)
 - [初期値]: -
- *id*
 - [設定値]: 静的 NAT エントリの識別情報 (1..2147483647)
 - [初期値]: -
- *outer_ip*
 - [設定値]: 外側 IP アドレス (1 個)
 - [初期値]: -
- *inner_ip*
 - [設定値]: 内側 IP アドレス (1 個)
 - [初期値]: -
- *count*
 - [設定値]:
 - 連続設定する個数
 - 省略時は 1
 - [初期値]: -
- *netmask*
 - [設定値]:
 - xxx.xxx.xxx.xxx (xxx は十進数)
 - 0x に続く十六進数
 - マスクビット数 (16..32)
 - [初期値]: -

[説明]

NAT 変換で固定割り付けする IP アドレスの組み合わせを指定する。個数を同時に指定すると指定されたアドレスを始点とした範囲指定とする。

[ノート]

外側アドレスが NAT 処理対象として設定されているアドレスである必要は無い。

静的 NAT のみを使用する場合には、**nat descriptor address outer** コマンドと **nat descriptor address inner** コマンドの設定に注意する必要がある。初期値がそれぞれ `ipcp` と `auto` であるので、例えば何らかの IP アドレスをダミーで設定しておくことで動的動作しないようにする。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

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

[書式]

```

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

```

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]: NAT ディスクリプタ番号 (1..2147483647)
 - [初期値]: -
- *use*
 - [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: off

[説明]

IP マスカレード使用時に rlogin、rcp、ssh の使用を許可するか否かを設定する。

[ノート]

on にすると、rlogin、rcp と ssh のトラフィックに対してはポート番号を変換しなくなる。
また on の場合に rsh は使用できない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

17.8 静的 IP マスカレードエントリの設定

[書式]

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

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]: NAT ディスクリプタ番号 (1..2147483647)
 - [初期値]: -
- *id*
 - [設定値]: 静的 IP マスカレードエントリの識別情報 (1 以上の数値)
 - [初期値]: -
- *inner_ip*
 - [設定値]: 内側 IP アドレス (1 個)
 - [初期値]: -
- *protocol*
 - [設定値]:

設定値	説明
esp	ESP
tcp	TCP プロトコル
udp	UDP プロトコル
icmp	ICMP プロトコル
プロトコル番号	IANA で割り当てられている protocol numbers

- [初期値]: -
- *outer_port*
 - [設定値]: 固定する外側ポート番号 (ニーモニック)
 - [初期値]: -
- *inner_port*
 - [設定値]: 固定する内側ポート番号 (ニーモニック)
 - [初期値]: -

[説明]

IP マスカレードによる通信でポート番号変換を行わないようにポートを固定する。

[ノート]

outer_port と *inner_port* を指定した場合には IP マスカレード適用時にインタフェースの外側から内側へのパケットは *outer_port* から *inner_port* に、内側から外側へのパケットは *inner_port* から *outer_port* へとポート番号が変換される。

outer_port を指定せず、*inner_port* のみの場合はポート番号の変換はされない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

17.9 NAT の IP アドレスマップの消去タイマの設定

[書式]

```

nat descriptor timer nat_descriptor time
nat descriptor timer nat_descriptor protocol=protocol [port=port_range] time
nat descriptor timer nat_descriptor tcpfin time2
no nat descriptor timer nat_descriptor [time]
no nat descriptor timer nat_descriptor protocol=protocol [port=port_range] [time]
no nat descriptor timer nat_descriptor tcpfin [time2]
    
```

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]: NAT ディスクリプタ番号 (1..2147483647)
 - [初期値]: -
- *time*
 - [設定値]: 消去タイマの秒数 (30..21474836)
 - [初期値]: 900
- *time2*
 - [設定値]: TCP/FIN 通過後の消去タイマの秒数 (1..21474836)
 - [初期値]: 60
- *protocol*
 - [設定値]: プロトコル
 - [初期値]: -
- *port_range*
 - [設定値]: ポート番号の範囲、プロトコルが TCP または UDP の場合にのみ有効
 - [初期値]: -

[説明]

NAT や IP マスカレードのセッション情報を保持する期間を表す NAT タイマを設定する。IP マスカレードの場合には、プロトコルやポート番号別の NAT タイマを設定することもできる。指定されていないプロトコルの場合は、第一の形式で設定した NAT タイマの値が使われる。

IP マスカレードの場合には、TCP/FIN 通過後の NAT タイマを設定することができる。TCP/FIN が通過したセッションは終了するセッションなので、このタイマを短くすることで NAT テーブルの使用量を抑えることができる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

17.10 外側から受信したパケットに該当する変換テーブルが存在しないときの動作の設定

[書式]

```

nat descriptor masquerade incoming nat_descriptor action [ip_address]
no nat descriptor masquerade incoming nat_descriptor
    
```

[設定値及び初期値]

- *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	

設定値	説明	
	TCP/0~1023 宛ての packets	左記以外
forward	指定されたホストに転送する	

- [初期値]: reject
- *ip_address*
 - [設定値]: 転送先の IP アドレス
 - [初期値]: -

[説明]

IP マスカレードで外側から受信したパケットに該当する変換テーブルが存在しないときの動作を設定する。
action が forward のときには *ip_address* を設定する必要がある。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

17.11 IP マスカレードで利用するポートの範囲の設定

[書式]

```
nat descriptor masquerade port range nat_descriptor port_range1 [port_range2 [port_range3 [port_range4]]]
no nat descriptor masquerade port range nat_descriptor [port_range1 [port_range2 [port_range3 [port_range4]]]]
```

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]: NAT ディスクリプタ番号 (1..2147483647)
 - [初期値]: -
- *port_range1*, *port_range2*, *port_range3*, *port_range4*
 - [設定値]: 間に - をはさんだポート番号の範囲 (1..65534)
 - [初期値]: port_range1=60000-64095, port_range2=49152-59999, port_range3=44096-49151

[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。

同一のポート番号を使用して複数の接続先とのセッションを確立できるため、本コマンドで設定したポート数を超えるセッションの確立が可能である。最大セッション数は **nat descriptor masquerade session limit total** コマンドで設定する。ただし、**nat descriptor backward-compatibility** コマンドで *type* パラメーターを 1 に変更した場合は、最大セッション数は本コマンドで設定したポート数と同等となるため、最大セッション数を変更する場合は本コマンドの設定を変更する必要がある。

[ノート]

ポート範囲を 16 個まで設定できる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

17.12 FTP として認識するポート番号の設定

[書式]

```
nat descriptor ftp port nat_descriptor port [port...]
no nat descriptor ftp port nat_descriptor [port...]
```

[設定値及び初期値]

- *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 の制御チャンネルの通信だとみなして処理をする。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

17.13 IP マスカレードで変換しないポート番号の範囲の設定**[書式]**

```
nat descriptor masquerade unconvertible port nat_descriptor if-possible
nat descriptor masquerade unconvertible port nat_descriptor protocol port
no nat descriptor masquerade unconvertible port nat_descriptor protocol [port]
```

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]: NAT ディスクリプタ番号 (1..2147483647)
 - [初期値]: -
- *protocol*
 - [設定値]:

設定値	説明
tcp	TCP
udp	UDP

- [初期値]: -
- *port*
 - [設定値]: ポート番号の範囲
 - [初期値]: -

[説明]

IP マスカレードで変換しないポート番号の範囲を設定する。

if-possible が指定されている時には、処理しようとするポート番号が他の通信で使われていない場合には値を変換せずそのまま利用する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

17.14 NAT のアドレス割当をログに記録するか否かの設定**[書式]**

```
nat descriptor log switch
no nat descriptor log
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	記録する
off	記録しない

- [初期値]: off

[説明]

NAT のアドレス割当をログに記録するか否かを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

17.15 SIP メッセージに含まれる IP アドレスを書き換えるか否かの設定**[書式]**

```
nat descriptor sip nat_descriptor sip
no nat descriptor sip nat_descriptor
```

[設定値及び初期値]

- *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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

17.16 IP マスカレード変換時に DF ビットを削除するか否かの設定

[書式]

```
nat descriptor masquerade remove df-bit remove
no nat descriptor masquerade remove df-bit [remove]
```

[設定値及び初期値]

- *remove*
 - [設定値]:

設定値	説明
on	IP マスカレード変換時に DF ビットを削除する
off	IP マスカレード変換時に DF ビットを削除しない

- [初期値]: on

[説明]

IP マスカレード変換時に DF ビットを削除するか否かを設定する。

DF ビットは経路 MTU 探索のために用いるが、そのためには長すぎるパケットに対する ICMP エラーを正しく発信元まで返さなくてはならない。しかし、IP マスカレード処理では IP アドレスなどを書き換えてしまうため、ICMP エラーを正しく発信元に返せない場合がある。そうすると、パケットを永遠に届けることができなくなってしまう。このように、経路 MTU 探索のための ICMP エラーが正しく届かない状況を、経路 MTU ブラックホールと呼ぶ。

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

17.17 IP マスカレードで変換するホスト毎のセッション数の設定

[書式]

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

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]: NAT ディスクリプタ番号 (1..2147483647)
 - [初期値]: -
- *id*
 - [設定値]: セッション数設定の識別番号 (1)
 - [初期値]: -

- *limit*
 - [設定値]:
 - 制限値 (1..65534)
 - [初期値]:
 - 65534

[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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

17.18 IP マスカレードで変換する合計セッション数の設定

[書式]

```
nat descriptor masquerade session limit total nat_descriptor limit
no nat descriptor masquerade session limit total nat_descriptor
```

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]: NAT ディスクリプタ番号 (1..2147483647)
 - [初期値]: -
- *limit*
 - [設定値]:
 - 制限値 (1..2147483647)
 - [初期値]:
 - 500000 (通常モード)
 - 65534 (コンパクトモード)

[説明]

ひとつの NAT ディスクリプターにおいて、IP マスカレードで変換するセッション数の最大数を設定する。**nat descriptor masquerade session limit** コマンドとは異なり、すべてのホストのセッション数の合計が対象となる。

[ノート]

本コマンドの設定は、**nat descriptor backward-compatibility** コマンドで、*type* パラメータを 2 に設定した場合のみ有効となる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

第 18 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 **tracert**、**rdns**、**ntpdns**、**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。

18.1 DNS を利用するか否かの設定

[書式]

```
dns service service
no dns service [service]
```

[設定値及び初期値]

- *service*
- [設定値]:

設定値	説明
recursive	DNS リカーシブサーバーとして動作する
off	サービスを停止させる

- [初期値]: recursive

[説明]

DNS リカーシブサーバーとして動作するかどうかを設定する。off を設定すると、DNS 的機能は一切動作しない。また、ポート 53/udp も閉じられる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

18.2 DNS サーバーの IP アドレスの設定

[書式]

```
dns server [edns=sw] ip_address [ip_address [edns=sw]...]
no dns server [ip_address [edns=sw]...]
```

[設定値及び初期値]

- *ip_address*
 - [設定値]: DNS サーバーの IP アドレス (空白で区切って最大 4 ヶ所まで設定可能)
 - [初期値]: -
- *sw*
 - [設定値]:

設定値	説明
on	対象の DNS サーバーへの通信は EDNS で行う
off	対象の DNS サーバーへの通信は DNS で行う

- [初期値]: off

[説明]

DNS サーバーの IP アドレスを指定する。

この IP アドレスはルーターが DHCP サーバーとして機能する場合に DHCP クライアントに通知するためや、IPCP の MS 拡張オプションで相手に通知するためにも使用される。

他のコマンドでも DNS サーバーが設定されている場合は、最も優先順位の高いコマンドの設定が使用される。DNS サーバーを設定する各種コマンドの優先順位は、本章冒頭の説明を参照。

edns オプションを省略、または edns=off を指定すると、対象の DNS サーバーへの名前解決は DNS で通信を行う。

edns=on を指定すると、対象の DNS サーバーへの名前解決は EDNS で通信を行う。

edns=on で名前解決ができない場合、edns=off に変更すると名前解決できる場合がある。

EDNS はバージョン 0 に対応。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

18.3 DNS ドメイン名の設定

[書式]

dns domain *domain_name*

no dns domain [*domain_name*]

[設定値及び初期値]

- *domain_name*
 - [設定値]: DNS ドメインを表す文字列
 - [初期値]: -

[説明]

ルーターが所属する DNS ドメインを設定する。

ルーターのホストとしての機能 (ping, traceroute) を使うときに名前解決に失敗した場合、このドメイン名を補完して再度解決を試みる。ルーターが DHCP サーバーとして機能する場合、設定したドメイン名は DHCP クライアントに通知するためにも使用される。ルーターのあるネットワークおよびそれが含むサブネットワークの DHCP クライアントに対して通知する。

空文字列を設定する場合には、**dns domain .** と入力する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

18.4 DNS サーバーを通知してもらおう相手先情報番号の設定

[書式]

dns server pp *peer_num* [edns=sw]

no dns server pp [*peer_num* [edns=sw]]

[設定値及び初期値]

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

設定値	説明
on	対象の DNS サーバーへの通信は EDNS で行う
off	対象の DNS サーバーへの通信は DNS で行う

- [初期値]: off

[説明]

DNS サーバーを通知してもらい相手先情報番号を設定する。このコマンドで相手先情報番号が設定されていると、DNS での名前解決を行う場合に、まずこの相手先に発信して、そこで PPP の IPCPMS 拡張機能で通知された DNS サーバーに対して問い合わせを行う。

相手先に接続できなかつたり、接続できても DNS サーバーの通知がなかった場合には名前解決は行われぬ。他のコマンドでも DNS サーバーが設定されている場合は、最も優先順位の高いコマンドの設定が使用される。DNS サーバーを設定する各種コマンドの優先順位は、本章冒頭の説明を参照。

edns オプションを省略、または edns=off を指定すると、対象の DNS サーバーへの名前解決は DNS で通信を行う。

edns=on を指定すると、対象の DNS サーバーへの名前解決は EDNS で通信を行う。

edns=on で名前解決ができない場合、edns=off に変更すると名前解決できる場合がある。

EDNS はバージョン 0 に対応。

[ノート]

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

edns オプションは vRX VMware ESXi 版で指定可能。

[設定例]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

18.5 DNS サーバーアドレスを取得するインタフェースの設定**[書式]**

```
dns server dhcp interface [edns=sw]
no dns server dhcp [interface [edns=sw]]
```

[設定値及び初期値]

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

設定値	説明
on	対象の DNS サーバーへの通信は EDNS で行う
off	対象の DNS サーバーへの通信は DNS で行う

- [初期値]: off

[説明]

DNS サーバーアドレスを取得するインタフェースを設定する。このコマンドでインタフェース名が設定されていると、DNS で名前解決を行うときに、指定したインタフェースで DHCP サーバーから取得した DNS サーバーアドレスに対して問い合わせを行う。DHCP サーバーから DNS サーバーアドレスを取得できなかった場合は名前解決を行わない。

他のコマンドでも DNS サーバーが設定されている場合は、最も優先順位の高いコマンドの設定が使用される。DNS サーバーを設定する各種コマンドの優先順位は、本章冒頭の説明を参照。

edns オプションを省略、または edns=off を指定すると、対象の DNS サーバーへの名前解決は DNS で通信を行う。

edns=on を指定すると、対象の DNS サーバーへの名前解決は EDNS で通信を行う。

edns=on で名前解決ができない場合、edns=off に変更すると名前解決できる場合がある。

EDNS はバージョン 0 に対応。

[ノート]

この機能は指定したインタフェースが DHCP クライアントとして動作していなければならない。

デプロイ時の状態および **cold start** コマンド実行後の本コマンドの設定値については「1.6 デプロイ時の設定値について」を参照してください。

edns オプションは vRX VMware ESXi 版で指定可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

18.6 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
dhcpv6	DHCPv6 による通知
msex	IPCP MS 拡張による通知

- [初期値]: dhcp および msex

- *server*

- [設定値]:

設定値	説明
none	一切通知しない
me	本機自身
server	dns server コマンドに設定したサーバー群、protocol に dhcpv6 を指定した場合は DHCPv6 で割り当てられたサーバー群

- [初期値]:

- me server (protocol が dhcp または msex の場合)
- me (protocol が dhcpv6 の場合)

[説明]

DHCP や 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。protocol に dhcpv6 を指定した場合は、IPv6 網から DHCPv6 で通知された DNS 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。

[ノート]

protocol の dhcpv6 パラメータは vRX VMware ESXi 版で指定可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

18.7 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

18.8 DNS サーバーへの AAAA レコードの問い合わせを制限するか否かの設定

[書式]

```
dns service aaaa filter switch
no dns service aaaa filter [switch]
```

[設定値及び初期値]

- *switch*
- [設定値] :

設定値	説明
on	AAAA レコードの問い合わせを制限する
off	AAAA レコードの問い合わせを制限しない

- [初期値] : off

[説明]

DNS サーバーへの AAAA レコードの問い合わせを制限するか否かを設定する。

IPv6 での接続環境がないのに AAAA レコードが引けてしまうことで、接続に失敗するような場合は、このコマンドにより AAAA レコードの問い合わせに対して、AAAA レコードを回答しないようにする。

本機が DNS リレーサーバーになっている通信及び本機発の通信が影響を受ける。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

18.9 SYSLOG 表示で DNS により名前解決するか否かの設定

[書式]

```
dns syslog resolv resolve
no dns syslog resolv [resolve]
```

[設定値及び初期値]

- *resolve*
- [設定値] :

設定値	説明
on	解決する
off	解決しない

- [初期値] : off

[説明]

SYSLOG 表示で DNS により名前解決するか否かを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

18.10 DNS 問い合わせの内容に応じた DNS サーバーの選択

[書式]

```
dns server select id server [edns=sw] [server2 [edns=sw]] [type] query [original-sender] [restrict pp connection-pp]
```

dns server select id pp peer_num [edns=sw] [default-server [edns=sw]] [type] query [original-sender] [restrict pp connection-pp]

dns server select id dhcp interface [edns=sw] [default-server [edns=sw]] [type] query [original-sender] [restrict pp connection-pp]

dns server select id reject [type] query [original-sender]

no dns server select id

[設定値及び初期値]

- *id*
 - [設定値]: DNS サーバー選択テーブルの番号
 - [初期値]: -
- *server*
 - [設定値]: プライマリ DNS サーバーの IP アドレス
 - [初期値]: -
- *server2*
 - [設定値]: セカンダリ DNS サーバーの IP アドレス
 - [初期値]: -
- *type*: DNS レコードタイプ
 - [設定値]:

設定値	説明
a	ホストの IP アドレス
aaaa	ホストの IPv6 アドレス
ptr	IP アドレスの逆引き用のポインタ
mx	メールサーバー
ns	ネームサーバー
cname	別名
any	すべてのタイプにマッチする
省略	省略時は a

- [初期値]: -
- *query*: DNS 問い合わせの内容
 - [設定値]:

設定値	説明
<i>type</i> が a、aaaa、mx、ns、cname の場合	<i>query</i> はドメイン名を表す文字列であり、後方一致とする。例えば、"yamaha.co.jp" であれば、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。
<i>type</i> が ptr の場合	<i>query</i> は IP アドレス (<i>ip_address[/masklen]</i>) であり、 <i>masklen</i> を省略したときは IP アドレスにのみマッチし、 <i>masklen</i> を指定したときはネットワークアドレスに含まれるすべての IP アドレスにマッチする。DNS 問い合わせに含まれる.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	<i>query</i> は完全一致とし、前方一致、及び後方一致には "*" を用いる。つまり、前方一致では、"NetVolante.*" であれば、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]: -
- *sw*
 - [設定値]:

設定値	説明
on	対象の DNS サーバーへの通信は EDNS で行う
off	対象の DNS サーバーへの通信は DNS で行う

- [初期値]: off

[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はサーバーの選択条件に追加される。相手先がアップしていないとサーバーは選択されない。相手先がアップしていて、かつ、他の条件もマッチしている場合に指定したサーバーが選択される。*edns* オプションを省略、または *edns=off* を指定すると、対象の DNS サーバーへの名前解決は DNS で通信を行う。*edns=on* を指定すると、対象の DNS サーバーへの名前解決は EDNS で通信を行う。*edns=on* で名前解決ができない場合、*edns=off* に変更すると名前解決できる場合がある。EDNS はバージョン 0 に対応。

[ノート]

edns オプションは vRX VMware ESXi 版で指定可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

18.11 静的 DNS レコードの登録

[書式]

```
ip host fqdn value [ttl=ttl]
dns static type name value [ttl=ttl]
no ip host fqdn [value]
no dns static type name [value]
```

[設定値及び初期値]

- *type*: 名前のタイプ
 - [設定値]:

設定値	説明
a	ホストの IPv4 アドレス
aaaa	ホストの IPv6 アドレス
ptr	IP アドレスの逆引き用のポインタ

設定値	説明
mx	メールサーバー
ns	ネームサーバー
cname	別名

- [初期値]: -
- *name*、*value*
- [設定値]:
type パラメータによって以下のように意味が異なる

<i>type</i> パラメータ	<i>name</i>	<i>value</i>
a	FQDN	IPv4 アドレス
aaaa	FQDN	IPv6 アドレス
ptr	IPv4 アドレス	FQDN
mx	FQDN	FQDN
ns	FQDN	FQDN
cname	FQDN	FQDN

- [初期値]: -
- *fqdn*
 - [設定値]: ドメイン名を含んだホスト名
 - [初期値]: -
- *ttl*
 - [設定値]: 秒数 (1..4294967295)
 - [初期値]: -

[説明]

静的な DNS レコードを定義する。

ip host コマンドは、**dns static** コマンドで **a** と **ptr** を両方設定することを簡略化したものである。

[ノート]

問い合わせに対して返される DNS レコードは以下のような特徴を持つ。

- TTL フィールドには、*ttl* パラメータの設定値がセットされる。*ttl* パラメータが省略された時には 1 がセットされる。
- Answer セクションに回答となる DNS レコードが 1 つセットされるだけで、Authority/Additional セクションには DNS レコードがセットされない
- MX レコードの *preference* フィールドは 0 にセットされる

[設定例]

```
# ip host pc1.rtpro.yamaha.co.jp 133.176.200.1
# dns static ptr 133.176.200.2 pc2.yamaha.co.jp
# dns static cname mail.yamaha.co.jp mail2.yamaha.co.jp
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

18.12 DNS 問い合わせパケットの始点ポート番号の設定

[書式]

```
dns sreport port[-port]
no dns sreport [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で扱うとき、始点番号がランダムに変化するという点を考慮しておく必要がある。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

18.13 DNS サーバーへアクセスできるホストの設定

[書式]

dns host ip_range [ip_range...]

dns host any

dns host none

dns host lan

no dns host

[設定値及び初期値]

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

設定値	説明
1 個の IP アドレスまたは間にハイフン (-) をはさんだ IP アドレス (範囲指定)、およびこれらを任意に並べたもの	指定したホストからのアクセスを許可する
lanN	LAN インターフェースからのアクセスを許可する

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

[説明]

DNS サーバー機能へのアクセスを許可するホストを設定する。

[ノート]

IP アドレスとニーモニックの混在指定および複数のニーモニックの指定が可能。このコマンドで LAN インタフェースを指定した場合には、ネットワークアドレスと limited broadcast address を除く IP アドレスからのアクセスを許可する。指定した LAN インタフェースにプライマリアドレスもセカンダリアドレスも設定していなければ、アクセスを許可しない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

18.14 DNS キャッシュを使用するか否かの設定

[書式]

dns cache use switch

no dns cache use [switch]

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
on	DNS キャッシュを利用する
off	DNS キャッシュを利用しない

- [初期値]: on

[説明]

DNS キャッシュを利用するか否かを設定する。

switch を on に設定した場合、DNS キャッシュを利用する。すなわち、ルーターが送信した DNS 問い合わせパケットに対する上位 DNS サーバーからの返答をルーター内部に保持し、次に同じ問い合わせが発生したときでも、サーバーには問い合わせず、キャッシュの内容を返す。

上位 DNS サーバーから得られた返答には複数の RR レコードが含まれているが、DNS キャッシュの保持時間は、それらの RR レコードの TTL のうちもっとも短い時間になる。また、まったく RR レコードが存在しない場合には、60 秒となる。

ルーター内部に保持する DNS エントリの数は **dns cache max entry** コマンドで設定する。

switch を off にした場合、DNS キャッシュは利用しない。ルーターが送信した DNS 問い合わせパケットに対する上位 DNS サーバーからの返答はルーター内部に保持せず、同じ問い合わせがあっても毎回 DNS サーバーに問い合わせを行う。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

18.15 DNS キャッシュの最大エントリ数の設定

[書式]

```
dns cache max entry num
no dns cache max entry [num]
```

[設定値及び初期値]

- *num*
- [設定値]: 最大エントリ数 (1..1024)
- [初期値]: 256

[説明]

DNS キャッシュの最大エントリ数を設定する。

設定した数だけ、ルーター内部に DNS キャッシュとして上位 DNS サーバーからの返答を保持できる。設定した数を超えた場合、返答が返ってきた順で古いものから破棄される。

上位 DNS サーバーから得られた返答には複数の RR レコードが含まれているが、DNS キャッシュの保持時間は、それらの RR レコードの TTL のうちもっとも短い時間になる。また、まったく RR レコードが存在しない場合には、60 秒となる。返答が得られてから保持時間を経過したエントリは、DNS キャッシュから削除される。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

18.16 DNS フォールバック動作をルーター全体で統一するか否かの設定

[書式]

```
dns service fallback switch
no dns service fallback [switch]
```

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
on	DNS フォールバック動作を IPv6 優先に統一する
off	DNS フォールバック動作は機能ごとにまちまちである

- [初期値]: off

[説明]

DNS フォールバック動作をルーターのすべての機能で統一するか否かを設定する。

DNS でホスト名を IP アドレスに変換する場合、IPv4/IPv6 いずれかを DNS サーバーに先に問い合わせ、アドレスが解決できない場合に他方のアドレスを問い合わせる動作を、DNS フォールバックと呼ぶ。ルーター自身が問い合わせる場合、すべての機能で IPv4 が優先されている。

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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

第 19 章

優先制御 / 帯域制御

優先制御と帯域制御の機能は、インタフェースに入力されたパケットの順序を入れ換えて別のインタフェースに出力します。これらの機能を使用しない場合には、パケットは入力した順番に処理されます。

優先制御は、クラス分けしたキューに優先順位をつけ、まず高位のキューのパケットを出力し、そのキューが空になると次の順位のキューのパケットを出力する、という処理を行います。

帯域制御は、クラス分けしたキューをラウンドロビン方式で監視しますが、監視頻度に差を与えてキューごとに利用できる帯域に差をつけます。

クラスは、**queue class filter** コマンドにより、パケットのフィルタリングと同様な定義でパケットを分類します。vRX では、クラスは 1 から 100 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。

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
1..16	1..100

クラスは番号が大きいほど優先順位が高くなります。

パケットの処理アルゴリズムは、**queue interface type** コマンドにより、優先制御、帯域制御、単純 FIFO の中から選択します。

これはインタフェースごとに選択することができます。

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

[説明]

指定したインタフェースに対して、インタフェースの速度を設定する。**queue interface type** コマンドで優先制御および帯域制御の設定が必要。

[ノート]

speed パラメータの後ろに 'k'、'M' または 'G' をつけると、それぞれ kbit/s、Mbit/s、Gbit/s として扱われる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

19.2 クラス分けのためのフィルター設定

[書式]

```
queue class filter num class ip src_addr [dest_addr [protocol [src_port [dest_port]]]]
queue class filter num class ipv6 src_addr [dest_addr [protocol [src_port [dest_port]]]]
queue class filter num precedence [mapping=prec:class [,prec:class...]] ip src_addr [dest_addr [protocol [src_port [dest_port]]]]
queue class filter num precedence [mapping=prec:class [,prec:class...]] ipv6 src_addr [dest_addr [protocol [src_port [dest_port]]]]
queue class filter num dscp ip src_addr [dest_addr [protocol [src_port [dest_port]]]]
queue class filter num dscp ipv6 src_addr [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
- [初期値]: -

- *class*

- [設定値]:

設定値	説明
1..100	クラス

- [初期値]: -

- *prec*

- [設定値]: precedence 値 (0..7)
- [初期値]: -

- *src_addr*: IP パケットの始点アドレス

- [設定値]:

- IP アドレス
 - A.B.C.D (A~D: 0~255 もしくは*)
 - 上記表記で A~D を*とすると、該当する 8 ビット分についてはすべての値に対応する
 - IPv6 アドレス
 - 間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。
 - , を区切りとして複数設定することができる。
- FQDN
 - 任意の文字列 (半角 255 文字以内。/ : は使用できない。 , は区切り文字として使われるため、使用できない)
 - * から始まる FQDN は * より後ろの文字列を後方一致条件として判断する 例えば *.example.co.jp は www.example.co.jp、mail.example.co.jp などと一致する
 - , を区切りとして複数設定することができる。
 - * (すべての IP アドレスまたは IPv6 アドレスに対応)

- [初期値]: -

- *dest_addr*: IP パケットの終点アドレス

- [設定値]:

- *src_addr* と同じ形式
- 省略した場合は一個の * と同じ

- [初期値]: -

- *protocol*: フィルタリングするパケットの種類

- [設定値]:

- プロトコルを表す十進数
- プロトコルを表すニーモニック

icmp	1
tcp	6
udp	17

- 上項目のカンマで区切った並び (5 個以内)
- *(すべてのプロトコル)
- established
- 省略時は * と同じ

- [初期値]: -

- *src_port*: UDP、TCP のソースポート番号

- [設定値]:

- ポート番号を表す十進数
- ポート番号を表すニーモニック (一部)

ニーモニック	ポート番号
ftp	20,21
ftpdata	20

ニーモニック	ポート番号
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 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

dscp 形式の場合、転送するパケットの DS フィールドの DSCP 値により定義される PHB に応じてクラス (1..9) を分けて優先制御もしくはシェーピングや Dynamic Traffic Control による帯域制御を行う。

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。

[設定例]

```
# queue class filter 1 4 ip ** udp 5004-5060 *
```

```
# queue class filter 2 10 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 ip * 172.16.6.0/24 tcp * *
# queue class filter 10 dscp ip 172.16.10.0/24 *
# queue class filter 11 dscp ip * 172.16.11.0/24
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

19.3 キューイングアルゴリズムタイプの選択

[書式]

queue interface type type [shaping-level=level]**queue pp type type****no queue interface type** [type]**no queue pp type** [type]

[設定値及び初期値]

• interface

- [設定値]: LAN インタフェース名
- [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 インタフェースに対する帯域制御を行う。LAN インタフェースにだけ設定できる。

shaping-level オプションは type パラメーターに priority および shaping を指定しているときのみ指定可能。

shaping-level に 1 を設定した場合、帯域速度の計算をプリアンブル、SFD (Start Frame Delimiter)、IFG (Inter Frame Gap) を含んだフレームサイズでおこなう。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

19.4 クラス分けフィルタの適用

[書式]

queue interface class filter list filter_list**queue pp class filter list filter_list****queue tunnel class filter list filter_list****no queue interface class filter list** [filter_list]

```
no queue pp class filter list [filter_list]
no queue tunnel class filter list [filter_list]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *filter_list*
 - [設定値]: 空白で区切られたクラスフィルタの並び
 - [初期値]: -

[説明]

指定した LAN インタフェースまたは選択されている PP、トンネルに対して、**queue class filter** コマンドで設定したフィルタを適用する順番を設定する。フィルタにマッチしなかったパケットは、**queue interface default class** コマンドで指定したデフォルトクラスに分類される。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

19.5 クラス毎のキュー長の設定

[書式]

```
queue interface length len1 [len2...lenN] [drop-threshold=dthreshold-mid[,dthreshold-high]]
queue pp length len1 [len2...len16]
no queue interface length [len1...]
no queue pp length [len1...]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *len1..lenN*
 - [設定値]:
 - クラス 1 からクラス 100 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
- *dthreshold-mid*
 - [設定値]: AF PHB の廃棄優先度が中の場合のキューサイズの閾値 (1%..100%)
 - [初期値]: 75%
- *dthreshold-high*
 - [設定値]: AF PHB の廃棄優先度が高の場合のキューサイズの閾値 (1%..100%)
 - [初期値]: 50%

[説明]

インタフェースに対して、指定したクラスのキューに入れることができるパケットの個数を指定する。指定を省略したクラスに関しては、最後に指定されたキュー長が残りのクラスにも適用される。

DiffServ ベース QoS の場合、*dthreshold-mid*、*dthreshold-high* パラメータで指定した値が AF PHB の廃棄優先度が中と高に対応するキューに積むことができる閾値となる。閾値は、クラスのキュー長に対する割合 (%) として表す。

dthreshold-high を省略した場合は、*dthreshold-mid* と同じ値となる。廃棄優先度が低に対応する閾値は常に 100% である。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

19.6 デフォルトクラスの設定

[書式]

```
queue interface default class class0
queue pp default class class1
```

```
queue tunnel default class class1
no queue interface default class [class0]
no queue pp default class [class1]
no queue tunnel default class [class1]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *class0*
 - [設定値]: クラス (1..100)
 - [初期値]: 2
- *class1*
 - [設定値]: クラス (1..16)
 - [初期値]: 2

[説明]

インタフェースに対して、フィルタにマッチしないパケットをどのクラスに分類するかを指定する。

[ノート]

第三書式は vRX VMware ESXi 版で使用可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

19.7 クラスの属性の設定

[書式]

```
queue interface class property class bandwidth=bandwidth
queue interface class property class type=type
no queue interface class property class [...]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *class*
 - [設定値]: クラス (1..100)
 - [初期値]: -
- *bandwidth*
 - [設定値]:
 - クラスに割り当てる帯域 (bit/s)
 - 数値の後ろに 'k'、'M' または 'G' をつけるとそれぞれ kbit/s、Mbit/s、Gbit/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。
 - [初期値]: -
- *type*
 - [設定値]:

設定値	説明
priority	優先制御クラスとして使用することを明示する。

- [初期値]: -

[説明]

指定したクラスの属性を設定する。

[ノート]

bandwidth パラメータで各クラスに割り当てる帯域の合計は、回線全体の帯域を越えてはいけません。回線全体の帯域は、**speed** コマンドで設定される。

queue interface type コマンドで **shaping** が指定されている場合は、Dynamic Traffic Control による帯域制御を行うことが可能である。Dynamic Traffic Control を行うためには、*bandwidth* パラメータに「,」（コンマ）でつないだ 2 つの速

度を指定することで、保証帯域と上限帯域を設定する。記述順に関係なく、常に値の小さな方が保証帯域となる。なお、保証帯域の合計が回線全体の帯域を越えてはいけない。

type パラメータは **queue interface type** コマンドで **shaping** が指定されている場合のみ有効である。インタフェースにおいて帯域制御による速度配分がされている場合でも、*type* パラメータに **priority** を指定することで、そのクラスは優先制御クラスとなり、帯域制御クラスよりも優先してパケットの転送が行われる。*type* パラメータに **priority** を指定したクラスが複数ある場合は、クラス番号が大きいほど優先順位が高くなる。

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

19.8 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 インタフェース名
 - [初期値]: -
- *class*
 - [設定値]: DCC を有効にするクラス (1..100)
 - [初期値]: -
- *ip_address*
 - [設定値]:

設定値	説明
IP アドレス	サーバーなどの監視対象から除外するホストの IP アドレスを設定する (空白で区切って複数指定可能、ハイフン「-」を使用して範囲指定も可能)

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

option	value	説明
forwarding	reject, 1..16	過剰送信と見なしたトラフィックの転送先のクラス
watch	source	送信元 IP アドレス単位で帯域を監視する
	destination	宛先 IP アドレス単位で帯域を監視する
threshold	占有率, 秒数	過剰送信と見なす閾値を帯域の占有率と占有時間をカンマ「,」で結び設定する (占有率 1%..100%、秒数 10..86400)
time	infinity	過剰送信と見なしたトラフィックを遮断する時間、または、使用するクラスを変更する時間 (秒)
	10..604800	
mode	forced	動作モードを強制制御モードにする
	adaptive	動作モードを適応制御モードにする

option	value	説明
trigger	winsky	Winsky 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]

指定したインタフェースについて、同一のホストが過剰な送信/受信を行い、帯域を逼迫していないか監視をする。監視対象のインタフェースに適用されている QoS 種別が `shaping` の場合は、`queue interface class property` コマンドで設定されたクラス帯域に対する占有率 (クラス帯域に保証値と上限値を指定している場合は保証値に対する占有率) を監視する。QoS 種別が `priority` の場合は、インタフェース帯域に対する占有率を監視する。監視時は 10 秒毎に占有率を求め、その占有率が指定秒数を越えたときに閾値超過と判定される。例えば、`threshold=70%,30` と設定した場合、帯域使用率 70% 以上である 10 秒間が連続して 3 回続いたときに閾値超過と判定される。

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

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

`mode` パラメータは動作モードを指定する。`forced` を指定した場合は、`threshold` パラメータで指定した占有時間が経過したら直ちに当該フローの制御を実行する。また、`time` パラメータで指定した制御時間が経過したら直ちに当該フローの制御を解除する。`adaptive` を指定した場合は、`threshold` パラメータで指定した占有時間が経過しても当該クラスの使用帯域が保証帯域の 90% 未満である間は制御を保留する。また、`time` パラメータで指定した制御時間が経過しても当該クラスの使用帯域が保証帯域の 90% 以上である間は制御解除を保留する。

制御が保留されているホストは `show status qos` コマンドで表示されず、制御が保留されている間に `threshold` の占有率を割ったらその時点で制御は解除される。

`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。

[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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

第 20 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。

20.1 OSPF の有効設定

[書式]

```
ospf configure refresh
```

[説明]

OSPF 関係の設定を有効にする。OSPF 関係の設定を変更したら、ルーターを再起動するか、あるいはこのコマンドを実行しなくてはならない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

20.2 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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

20.3 OSPF による経路の優先度設定

[書式]

```
ospf preference preference
no ospf preference [preference]
```

[設定値及び初期値]

- *preference*
 - [設定値]: OSPF による経路の優先度 (1 以上の数値)
 - [初期値]: 2000

[説明]

OSPF による経路の優先度を設定する。優先度は 1 以上の数値で表され、数字が大きい程優先度が高い。OSPF と RIP など複数のプロトコルで得られた経路が食い違う場合には、優先度が高い方が採用される。優先度が同じ場合には時間的に先に採用された経路が有効となる。

[ノート]

静的経路の優先度は 10000 で固定である。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

20.4 OSPF のルーター ID 設定

[書式]

ospf router id *router-id***no ospf router id** [*router-id*]

[設定値及び初期値]

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

[説明]

OSPF のルーター ID を指定する。

[ノート]

ルーター ID が本コマンドで設定されていないときは、以下のインタフェースに付与されているプライマリ IPv4 アドレスのいずれかが自動的に選択され、ルーター ID として使用させれる。

- LAN インタフェース
- LOOPBACK インタフェース
- PP インタフェース

なお、プライマリ IPv4 アドレスが付与されたインタフェースがない場合は初期値は設定されない。意図しない IP アドレスがルーター ID として使用されることを防ぐため、本コマンドにより明示的にルーター ID を指定することが望ましい。

OSPF と BGP-4 とを併用する場合、本コマンドか **bgp router id** コマンドのいずれか一方を設定する。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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

20.5 OSPF で受け取った経路をルーティングテーブルに反映させるか否かの設定

[書式]

ospf export from ospf [*filter filter_num...*]**no ospf export from ospf** [*filter filter_num...*]

[設定値及び初期値]

- *filter_num*
 - [設定値]: **ospf export filter** コマンドのフィルタ番号
 - [初期値]: すべての経路がルーティングテーブルに反映される

[説明]

OSPF で受け取った経路をルーティングテーブルに反映させるかどうかを設定する。指定したフィルタに一致する経路だけがルーティングテーブルに反映される。コマンドが設定されていない場合または **filter** キーワード以降を省略した場合には、すべての経路がルーティングテーブルに反映される。

[ノート]

フィルタ番号は 100 個まで設定できる。

このコマンドは OSPF のリンク状態データベースには影響を与えない。つまり、OSPF で他のルーターと情報をやり取りする動作としては、このコマンドがどのように設定されていても変化は無い。OSPF で計算した経路が、実際にパケットをルーティングするために使われるかどうかだけが変化する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

20.6 外部プロトコルによる経路導入

[書式]

ospf import from protocol [*filter filter_num...*]

no ospf import from protocol [filter filter_num...]

[設定値及び初期値]

- *protocol* : OSPF の経路テーブルに導入する外部プロトコル
 - [設定値] :

設定値	説明
static	静的経路
rip	RIP
bgp	BGP

- [初期値] :-
- *filter_num*
 - [設定値] : フィルタ番号
 - [初期値] :-

[説明]

OSPF の経路テーブルに外部プロトコルによる経路を導入するかどうかを設定する。導入された経路は外部経路として他の OSPF ルーターに広告される。

filter_num は **ospf import filter** コマンドで定義したフィルタ番号を指定する。外部プロトコルから導入されようとする経路は指定したフィルタにより検査され、フィルタに該当すればその経路は OSPF に導入される。該当するフィルタがない経路は導入されない。また、**filter** キーワード以降を省略した場合には、すべての経路が OSPF に導入される

経路を広告する場合のパラメータであるメトリック値、メトリックタイプ、タグは、フィルタの検査で該当した **ospf import filter** コマンドで指定されたものを使う。**filter** キーワード以降を省略した場合には、以下のパラメータを使用する。

- metric=1
- type=2
- tag=1

[ノート]

フィルタ番号は 300 個まで設定できる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

20.7 OSPF で受け取った経路をどう扱うかのフィルタの設定

[書式]

ospf export filter filter_num [*nr*] *kind ip_address/mask...*
no ospf export filter filter_num [...]

[設定値及び初期値]

- *filter_num*
 - [設定値] : フィルタ番号
 - [初期値] :-
- *nr* : フィルタの解釈の方法
 - [設定値] :

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

- [初期値] :-
- *kind* : フィルタ種別
 - [設定値] :

設定値	説明
include	指定したネットワークアドレスに含まれる経路 (ネットワークアドレス自身を含む)
refines	指定したネットワークアドレスに含まれる経路 (ネットワークアドレス自身を含まない)
equal	指定したネットワークアドレスに一致する経路

- [初期値] :-
- `ip_address/mask`
 - [設定値] : ネットワークアドレスをあらわす IP アドレスとマスク長
 - [初期値] :-

[説明]

OSPF により他の OSPF ルーターから受け取った経路を経路テーブルに導入する際に適用するフィルタを定義する。このコマンドで定義したフィルタは、**ospf export from ospf** コマンドの `filter` 項で指定されてはじめて効果を持つ。`ip_address/mask` では、ネットワークアドレスを設定する。これは、複数設定でき、経路の検査時にはそれぞれのネットワークアドレスに対して検査を行う。

`nr` が省略されている場合には、一つでも該当するフィルタがある場合には経路が導入される。

`not` 指定時には、すべての検査でフィルタに該当しなかった場合に経路が導入される。`reject` 指定時には、一つでも該当するフィルタがある場合には経路が導入されない

`kind` では、経路の検査方法を設定する。

include	ネットワークアドレスと一致する経路および、ネットワークアドレスに含まれる経路が該当となる
refines	ネットワークアドレスに含まれる経路が該当となるが、ネットワークアドレスと一致する経路が含まれない
equal	ネットワークアドレスに一致する経路だけが該当となる

[ノート]

`not` 指定のフィルタを **ospf export from** コマンドで複数設定する場合には注意が必要である。`not` 指定のフィルタに合致するネットワークアドレスは、そのフィルタでは導入するかどうか決定しないため、次のフィルタで検査されることになる。そのため、例えば、以下のような設定ではすべての経路が導入されることになり、フィルタの意味が無い。

```
ospf export from ospf filter 1 2
ospf export filter 1 not equal 192.168.1.0/24
ospf export filter 2 not equal 192.168.2.0/24
```

1 番のフィルタでは、192.168.1.0/24 以外の経路を導入し、2 番のフィルタで 192.168.2.0/24 以外の経路を導入している。つまり、経路 192.168.1.0/24 は 2 番のフィルタにより、経路 192.168.2.0/24 は 1 番のフィルタにより導入されるため、導入されない経路は存在しない。

経路 192.168.1.0/24 と経路 192.168.2.0/24 を導入したくない場合には以下のような設定を行う必要がある。

```
ospf export from ospf filter 1
ospf export filter 1 not equal 192.168.1.0/24 192.168.2.0/24
```

あるいは

```
ospf export from ospf filter 1 2 3
ospf export filter 1 reject equal 192.168.1.0/24
ospf export filter 2 reject equal 192.168.2.0/24
ospf export filter 3 include 0.0.0.0/0
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

20.8 外部経路導入に適用するフィルタ定義

[書式]

```
ospf import filter filter_num [nr] kind ip_address/mask... [parameter...].
no ospf import filter filter_num [[not] kind ip_address/mask... [parameter...]]
```

[設定値及び初期値]

- *filter_num*
 - [設定値]: フィルタ番号
 - [初期値]: -
- *nr*: フィルタの解釈の方法
 - [設定値]:

設定値	説明
not	フィルタに該当しない経路を広告する
reject	フィルタに該当した経路を広告しない
省略時	フィルタに該当した経路を広告する

- [初期値]: -
- *kind*
 - [設定値]:

設定値	説明
include	指定したネットワークアドレスに含まれる経路 (ネットワークアドレス自身を含む)
refines	指定したネットワークアドレスに含まれる経路 (ネットワークアドレス自身は含まない)
equal	指定したネットワークアドレスに一致する経路

- [初期値]: -
- *ip_address/mask*
 - [設定値]: ネットワークアドレスをあらわす IP アドレスとマスク長
 - [初期値]: -
- *parameter*: 外部経路を広告する場合のパラメータ
 - [設定値]:

設定値	説明
metric	メトリック値 (0..16777215)
type	メトリックタイプ (1..2)
tag	タグの値 (0..4294967295)

- [初期値]: -

[説明]

OSPF の経路テーブルに外部経路を導入する際に適用するフィルタを定義する。このコマンドで定義したフィルタは、**ospf import from** コマンドの *filter* 項で指定されてはじめて効果を持つ。

ip_address/mask では、ネットワークアドレスを設定する。これは、複数設定でき、経路の検査時にはそれぞれのネットワークアドレスに対して検査を行い、1 つでも該当するものがあればそれが適用される。

nr が省略されている場合には、一つでも該当するフィルタがある場合には経路を広告する。not 指定時には、すべての検査でフィルタに該当しなかった場合に経路を広告する。reject 指定時には、一つでも該当するフィルタがある場合には経路を広告しない。

kind では、経路の検査方法を設定する。

include	ネットワークアドレスと一致する経路および、ネットワークアドレスに含まれる経路が該当となる
refines	ネットワークアドレスに含まれる経路が該当となるが、ネットワークアドレスと一致する経路が含まれない

equal	ネットワークアドレスに一致する経路だけが該当となる
-------	---------------------------

kind の前に **not** キーワードを置くと、該当/非該当の判断が反転する。例えば、**not equal** では、ネットワークアドレスに一致しない経路が該当となる

parameter では、該当した経路を OSPF の外部経路として広告する場合のパラメータとして、メトリック値、メトリックタイプ、タグがそれぞれ **metric**、**type**、**tag** により指定できる。これらを省略した場合には、以下の値が採用される。

- **metric**=1
- **type**=2
- **tag**=1

[ノート]

not 指定のフィルタを **ospf import from** コマンドで複数設定する場合には注意が必要である。**not** 指定のフィルタに合致するネットワークアドレスは、そのフィルタでは導入するかどうかが決まらないため、次のフィルタで検査されることになる。そのため、例えば、以下のような設定ではすべての経路が広告されることになり、フィルタの意味が無い。

```
ospf import from static filter 1 2
ospf import filter 1 not equal 192.168.1.0/24
ospf import filter 2 not equal 192.168.2.0/24
```

1 番のフィルタでは、192.168.1.0/24 以外の経路を広告し、2 番のフィルタで 192.168.2.0/24 以外の経路を広告している。つまり、経路 192.168.1.0/24 は 2 番のフィルタにより、経路 192.168.2.0/24 は 1 番のフィルタにより広告されるため、広告されない経路は存在しない。

経路 192.168.1.0/24 と経路 192.168.2.0/24 を広告したくない場合には以下のような設定を行う必要がある。

```
ospf import from static filter 1
ospf import filter 1 not equal 192.168.1.0/24 192.168.2.0/24
```

あるいは

```
ospf import from static filter 1 2 3
ospf import filter 1 reject equal 192.168.1.0/24
ospf import filter 2 reject equal 192.168.2.0/24
ospf import filter 3 include 0.0.0.0/0
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

20.9 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

設定値	説明
md5	MD5 認証

- [初期値]: 認証は行わない
- `stub`: スタブエリアであることを指定する。
 - [初期値]: スタブエリアではない
- `cost`
 - [設定値]: 1 以上の数値
 - [初期値]: -

[説明]

OSPF エリアを設定する。

`cost` は 1 以上の数値で、エリア境界ルーターがエリア内に広告するデフォルト経路のコストとして使われる。`cost` を指定しないとデフォルト経路の広告は行われぬ。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

20.10 エリアへの経路広告

[書式]

ospf area network area network/mask [restrict]

no ospf area network area network/mask [restrict]

[設定値及び初期値]

- `area`
 - [設定値]:

設定値	説明
backbone	バックボーンエリア
1 以上の数値	非バックボーンエリア
IP アドレス表記 (0.0.0.0 は不可)	非バックボーンエリア

- [初期値]: -
- `network`
 - [設定値]: IP アドレス
 - [初期値]: -
- `mask`
 - [設定値]: ネットマスク長
 - [初期値]: -

[説明]

エリア境界ルーターが他のエリアに経路を広告する場合に、`network/mask` で指定したネットワーク範囲内の個々の経路を `network/mask` に要約して広告する。`restrict` キーワードを指定した場合は、`network/mask` の範囲内の経路は要約した経路も含めて一切他のエリアに広告しなくなる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

20.11 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

設定値	説明
1 以上の数値	非バックボーンエリア
IP アドレス表記 (0.0.0.0 は不可)	非バックボーンエリア

- [初期値]: -
- *host*
 - [設定値]: IP アドレス
 - [初期値]: -
- *cost*
 - [設定値]: 1 以上の数値
 - [初期値]: -

[説明]

指定したホストが指定したコストでスタブ的に接続されていることをエリア内に広告する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

20.12 仮想リンク設定

[書式]

```
ospf virtual-link router_id area [parameters...]
no ospf virtual-link router_id [area [parameters...]]
```

[設定値及び初期値]

- *router_id*
 - [設定値]: 仮想リンクの相手のルーター ID
 - [初期値]: -
- *area*
 - [設定値]:

設定値	説明
1 以上の数値	非バックボーンエリア
IP アドレス表記 (0.0.0.0 は不可)	非バックボーンエリア

- [初期値]: -
- *parameters*
 - [設定値]: NAME=VALUE の列
 - [初期値]:
 - retransmit-interval = 5 秒
 - transmit-delay = 1 秒
 - hello-interval = 10 秒
 - dead-interval = 40 秒
 - authkey=なし
 - md5key=なし
 - md5-sequence-mode=second

[説明]

仮想リンクを設定する。仮想リンクは *router_id* で指定したルーターに対して、*area* で指定したエリアを経由して設定される。*parameters* では、仮想リンクのパラメータが設定できる。パラメータは NAME=VALUE の形で指定され、以下の種類がある。

NAME	VALUE	説明
retransmit-interval	秒数	LSA を連続して送る場合の再送間隔を秒単位で設定する。(1..)
transmit-delay	秒数	リンクの状態が変わってから LSA を送信するまでの時間を秒単位で設定する。(1..)

NAME	VALUE	説明
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、そのインタフェースから直接通信できるすべての近隣ルーターとの間で同じ値でなくてはならない。これらのパラメータの値が設定値とは異なっている OSPFHELLO パケットを受信した場合には、それは無視される。

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

20.13 指定インタフェースの OSPF エリア設定

[書式]

```
ip interface ospf area area [parameters...]
ip pp ospf area area [parameters...]
ip tunnel ospf area area [parameters...]
no ip interface ospf area [area [parameters...]]
no ip pp ospf area [area [parameters...]]
no ip tunnel ospf area [area [parameters...]]
```

[設定値及び初期値]

- interface
 - [設定値]: LAN インタフェース名、LOOPBACK インタフェース名
 - [初期値]: -
- area
 - [設定値]:

設定値	説明
backbone	バックボーンエリア

設定値	説明
1 以上の数値	非バックボーンエリア
IP アドレス表記 (0.0.0.0 は不可)	非バックボーンエリア

- [初期値]: インタフェースは OSPF エリアに属していない
- *parameters*
 - [設定値]: NAME=VALUE の列
 - [初期値]:
 - type=broadcast (LAN インタフェース設定時)
 - type=point-to-point (PP または TUNNEL インタフェース設定時)
 - type=loopback (LOOPBACK インタフェース設定時)
 - passive=インタフェースは passive ではない
 - cost=1 (LAN インタフェース、LOOPBACK インタフェース設定時)、pp は回線速度に依存
 - priority=1
 - retransmit-interval=5 秒
 - transmit-delay=1 秒
 - hello-interval=10 秒 (type=broadcast 設定時)
 - hello-interval=10 秒 (point-to-point 設定時)
 - dead-interval=hello-interval の 4 倍
 - poll-interval=120 秒
 - authkey=なし
 - md5key=なし
 - md5-sequence-mode=second

[説明]

指定したインタフェースの属する OSPF エリアを設定する。

NAME パラメータの type はインタフェースのネットワークがどのようなタイプであるかを設定する。

parameters では、リンクパラメータを設定する。パラメータは NAME=VALUE の形で指定され、以下の種類がある。

NAME	VALUE	説明
type	broadcast	ブロードキャスト
	point-to-point	ポイント・ポイント
passive		インタフェースに対して、OSPF パケットを送信しない。該当インタフェースに他の OSPF ルーターがない場合に設定する。
cost	コスト	<p>インタフェースのコストを設定する。初期値は、インタフェースの種類と回線速度によって決定される。LAN インタフェースの場合は 1、PP インタフェースの場合は、バインドされている回線の回線速度を S[kbit/s] とすると、以下の計算式で決定される。例えば、64kbit/s の場合は 1562、1.536Mbit/s の場合には 65 となる。(0.65535)</p> <ul style="list-style-type: none"> • $COST=100000/S$ <p>TUNNEL インタフェースの場合は、1562 がデフォルト値となる。</p>
priority	優先度	指定ルーターの選択の際の優先度を設定する。PRIORITY 値が大きいルーターが指定ルーターに選ばれる。0 を設定すると、指定ルーターに選ばれなくなる。(0..255)

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	近隣ルーターから HELLO を受け取れない場合に、近隣ルーターがダウンしたと判断するまでの時間を秒単位で設定する。(1..)
poll-interval	秒数	非ブロードキャストリンクでのみ有効なパラメータで、近隣ルーターがダウンしている場合の HELLO パケットの送信間隔を秒単位で設定する。(1..)
authkey	文字列	プレーンテキスト認証の認証鍵を表す文字列を設定する。(8 文字以内)
md5key	"(ID),(KEY)"	MD5 認証の認証鍵を表す ID と鍵文字列 KEY を設定する。ID は十進数で 0~255、KEY は文字列で 16 文字以内。MD5 認証鍵は 2 つまで設定できる。複数の MD5 認証鍵が設定されている場合には、送信パケットは同じ内容のパケットを複数個、それぞれの鍵による認証データを付加して送信する。受信時には鍵 ID が一致する鍵が比較対象となる。
md5-sequence-mode	"second"	送信時刻の秒数
	"increment"	単調増加

LOOPBACK インタフェースに設定する場合は、NAME パラメータの type でインタフェースタイプを、cost でインタフェースのコストを指定できる。LOOPBACK インタフェースのタイプで指定できるのは、以下の 2 種類だけとなる。

NAME	VALUE	広告される経路の種類	OSPF 的なインタフェースの扱い	
			タイプ	状態
type	loopback	LOOPBACK インタフェースの IP アドレスのみのホスト経路	point-to-point	Loopback
	loopback-network	LOOPBACK インタフェースの implicit なネットワーク経路	non-broadcast(NBMA)	DROther

[ノート]

- NAME パラメータの type について
NAME パラメータの type として、LAN インタフェースは broadcast のみが許される。PP インタフェースは、PPP を利用する場合は point-to-point が設定できる。
- passive について
passive は、インタフェースが接続しているネットワークに他の OSPF ルーターが存在しない場合に指定する。passive を指定しておく、インタフェースから OSPF パケットを送信しなくなるので、無駄なトラフィックを抑制したり、受信側で誤動作の原因になるのを防ぐことができる。

LAN インタフェース (type=broadcast であるインタフェース) の場合には、インタフェースが接続しているネットワークへの経路は、**ip interface ospf area** コマンドを設定していないと他の OSPF ルーターに広告されない。そのため、OSPF を利用しないネットワークに接続する LAN インタフェースに対しては、**passive** を付けた **ip interface ospf area** コマンドを設定しておくことでそのネットワークでは OSPF を利用しないまま、そこへの経路を他の OSPF ルーターに広告することができる。

PP インタフェースに対して **ip interface ospf area** コマンドを設定していない場合は、インタフェースが接続するネットワークへの経路は外部経路として扱われる。外部経路なので、他の OSPF ルーターに広告するには **ospf import** コマンドの設定が必要である。

- hello-interval/dead-interval について

hello-interval/dead-interval の値は、そのインタフェースから直接通信できるすべての近隣ルーターとの間で同じ値でなくてはならない。これらのパラメータの値が設定値とは異なっている OSPF HELLO パケットを受信した場合には、それは無視される。

- MD5 認証鍵について

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

20.14 非ブロードキャスト型ネットワークに接続されている OSPF ルーターの指定

[書式]

```
ip interface ospf neighbor ip_address [eligible]
ip pp ospf neighbor ip_address [eligible]
ip tunnel ospf neighbor ip_address [eligible]
no ip interface ospf neighbor ip_address [eligible]
no ip pp ospf neighbor ip_address [eligible]
no ip tunnel ospf neighbor ip_address [eligible]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *ip_address*
 - [設定値]: 近隣ルーターの IP アドレス
 - [初期値]: -

[説明]

非ブロードキャスト型のネットワークに接続されている OSPF ルーターを指定する。eligible キーワードが指定されたルーターは指定ルーターとして適格であることを表す。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

20.15 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

設定値	説明
off	イコールコストになるスタブを他の経路とマージしない

- [初期値]: on

[説明]

他の経路と同じコストになるスタブをどう扱うかを設定する。

on の場合にはスタブへの経路を他の経路とマージして、イコールコストマルチパス動作をする。これは、RFC2328 の記述に沿うものである。

off の場合にはスタブへの経路を無視する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

20.16 OSPF の状態遷移とパケットの送受信をログに記録するか否かの設定

[書式]

```
ospf log log [log...]
```

```
no ospf log [log...]
```

[設定値及び初期値]

- *log*
- [設定値]:

設定値	説明
interface	インタフェースの状態遷移
neighbor	近隣ルーターの状態遷移
packet	送受信したパケット

- [初期値]: OSPF のログは記録しない。

[説明]

指定した種類のログを INFO レベルで記録する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

20.17 インタフェースの状態変化時、OSPF に外部経路を反映させる時間間隔の設定

[書式]

```
ospf reric interval time
```

```
no ospf reric interval [time]
```

[設定値及び初期値]

- *time*
- [設定値]: 秒数 (1 以上の数値)
- [初期値]: 1

[説明]

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

OSPF ではインタフェースの状態変化を 1 秒間隔で監視し、変化があれば最新の外部経路を自身に反映させるが、インタフェースの状態変化が連続して発生するときは、複数の外部経路の反映処理が *time* で指定した秒数の間隔でまとめて行われるようになる。

[ノート]

複数のトンネルが一斉にアップすることがあるような環境では、本コマンドの値を適切に設定することで、OSPF や BGP の外部経路の導入によるシステムへの負荷を軽減することができる。

本コマンドの設定値は、BGP への外部経路の反映にも影響する。本コマンドと **bgp reric interval** コマンドの設定値が食い違う場合には、本コマンドの設定値が優先して適用される。

本コマンドの設定は、経路の変化や IP アドレスの変化に対する OSPF や BGP の動作には関係しない。また本コマンドの設定値は、**ospf configure refresh** コマンドを実行しなくても即時反映される。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

第 21 章

BGP

21.1 BGP の起動の設定

[書式]

```
bgp use use
no bgp use [use]
```

[設定値及び初期値]

- *use*
 - [設定値]:

設定値	説明
on	起動する
off.	起動しない

- [初期値]: off

[説明]

BGP を起動するか否かを設定する

[ノート]

いずれかのインタフェースにセカンダリアドレスを割り当てた場合、BGP を使用することはできない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

21.2 経路の集約の設定

[書式]

```
bgp aggregate ip_address/mask filter filter_num ...
no bgp aggregate ip_address/mask [filter filter_num... ]
```

[設定値及び初期値]

- *ip_address/mask*
 - [設定値]: IP アドレス/ネットマスク
 - [初期値]: -
- *filter_num*
 - [設定値]: フィルタ番号 (1..2147483647)
 - [初期値]: -

[説明]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

21.3 経路を集約するためのフィルタの設定

[書式]

```
bgp aggregate filter filter_num protocol [reject] kind ip_address/mask ...
no bgp aggregate filter filter_num [protocol [reject] kind ip_address/mask ...]
```

[設定値及び初期値]

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

設定値	説明
static	静的経路
rip	RIP
ospf	OSPF
bgp	BGP
all	すべてのプロトコル

- [初期値]: -
- *kind*
- [設定値]:

設定値	説明
include	指定したネットワークに含まれる経路 (ネットワークアドレス自身を含む)
refines	指定したネットワークに含まれる経路 (ネットワークアドレス自身を含まない)
equal	指定したネットワークに一致する経路

- [初期値]: -
- *ip_address/mask*
 - [設定値]: IP アドレス/ネットマスク
 - [初期値]: -

[説明]

BGP で広告する経路を集約するためのフィルタを定義する。このコマンドで定義したフィルタは、**bgp aggregate** コマンドの *filter* 節で指定されてはじめて効果を持つ。

ip_address/mask では、ネットワークアドレスを設定する。これは複数設定でき、そのうち、一致するネットワーク長が長い設定が採用される。

kind の前に *reject* キーワードを置くと、その経路は集約されない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

21.4 AS 番号の設定

[書式]

```
bgp autonomous-system as
no bgp autonomous-system [as]
```

[設定値及び初期値]

- *as*
 - [設定値]: AS 番号 (1..65535)
 - [初期値]: -

[説明]

ルーターの AS 番号を設定する。

[ノート]

AS 番号を設定するまで BGP は動作しない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

21.5 ルーター ID の設定

[書式]

```
bgp router id ip_address
no bgp router id [ip_address]
```

[設定値及び初期値]

- *ip_address*

- [設定値]: IP アドレス
- [初期値]: インタフェースに付与されているプライマリアドレスから自動的に選択する。

[説明]

ルーター ID を設定する。

[ノート]

ルーター ID が本コマンドで設定されていないときは、以下のインタフェースに付与されているプライマリ IPv4 アドレスのいずれかが自動的に選択され、ルーター ID として使用させれる。

- LAN インタフェース
- LOOPBACK インタフェース
- PP インタフェース

なお、プライマリ IPv4 アドレスが付与されたインタフェースがない場合は初期値は設定されない。意図しない IP アドレスがルーター ID として使用されることを防ぐため、本コマンドにより明示的にルーター ID を指定することが望ましい。

OSPF と BGP-4 とを併用する場合、本コマンドか **ospf router id** コマンドのいずれか一方を設定する。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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

21.6 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。

プロトコル名	初期値
スタティック	10000
RIP	1000
OSPF	2000
BGP	500

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

21.7 BGP で受信した経路に対するフィルタの適用

[書式]

```
bgp export remote_as filter filter_num ...
bgp export aspath seq "aspath_regex" filter filter_num ...
no bgp export remote_as [filter filter_num ...]
no bgp export aspath seq ["aspath_regex"] [filter filter_num ...]
```

[設定値及び初期値]

- *remote_as*

- [設定値]: 相手の AS 番号 (1..65535)
- [初期値]: -
- *seq*
 - [設定値]: AS パスを指定したときの評価順序 (1..65535)
 - [初期値]: -
- *aspath_regexp*
 - [設定値]: 正規表現
 - [初期値]: -
- *filter_num*
 - [設定値]: フィルタ番号 (1..2147483647)
 - [初期値]: -

[説明]

BGP で受けた経路に対してフィルタを設定する。*remote_as* を指定してフィルタを設定した場合、接続先から受けた経路についてフィルタに該当した経路が実際のルーティングテーブルに導入され、RIP や OSPF のような他のプロトコルにも通知される。フィルタに該当しない経路はルーティングには適用されず、他のプロトコルに通知されることもない。フィルタの番号には **bgp export filter** コマンドで定義した番号を指定する。

aspath_regexp を指定してフィルタを設定した場合、*remote_as* を指定した場合と同様に、AS パスが正規表現と一致する経路についてフィルタに該当した経路が導入される。*aspath_regexp* には **grep** コマンドで使用できる検索パターンを指定する。

aspath_regexp を指定したフィルタを複数設定した場合、*seq* の小さい順に評価される。また、*aspath_regexp* を指定したフィルタを設定した場合、*remote_as* を指定したフィルタよりも優先して評価される。

[ノート]

正規表現によって AS パスを表す例

- すべての AS パスと一致する

```
# bgp export aspath 10 ".*" filter 1
```

- AS 番号が 1000 または 1100 で始まる AS パスと一致する

```
# bgp export aspath 20 "^1[01]00.*" filter 1
```

- AS 番号に 2000 を含む AS パスと一致する

```
# bgp export aspath 30 "2000" filter 1
```

- AS パスが 3000 3100 3200 であるパスと完全一致する

```
# bgp export aspath 40 "^3000 3100 3200$" filter 1
```

- AS パスに AS_SET を含むパスと一致する

```
# bgp export aspath 50 "{.*}" filter 1
```

フィルタ番号は、100 個まで設定できる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

21.8 BGP で受信する経路に適用するフィルタの設定

[書式]

```
bgp export filter filter_num [reject] kind ip_address/mask ... [parameter ]
no bgp export filter filter_num [[reject] kind ip_address/mask ... [parameter]]
```

[設定値及び初期値]

- *filter_num*
 - [設定値]: フィルタ番号 (1..2147483647)
 - [初期値]: -
- *kind*
 - [設定値]:

設定値	説明
include	指定したネットワークに含まれる経路 (ネットワークアドレス自身を含む)
refines	指定したネットワークに含まれる経路 (ネットワークアドレス自身を含まない)
equal	指定したネットワークに一致する経路

- [初期値]: -
- *ip_address/mask*
- [設定値]:

設定値	説明
ip_address/mask	IP アドレス/ネットマスク
all	すべてのネットワーク

- [初期値]: -
- *parameter*: TYPE=VALUE の組
- [設定値]:

TYPE	VALUE	説明
preference	0..255	同じ経路を複数の相手から受信したときに、一方を選択するための優先度

- [初期値]: 0

[説明]

BGP で受信する経路に適用するフィルタを定義する。このコマンドで定義したフィルタは、**bgp export** コマンドの *filter* 節で指定されてはじめて効果を持つ。

ip_address/mask では、ネットワークアドレスを設定する。複数の設定があるときには、プレフィックスが最も長く一致する設定が採用される。

kind の前に *reject* キーワードを置くと、その経路が拒否される。

[ノート]

preference の設定は BGP 経路の間で優先順位をつけるために使用される。BGP 経路の全体の優先度は、**bgp preference** コマンドで設定する。

[設定例]

```
# bgp export filter 1 include 10.0.0.0/16 172.16.0.0/16
# bgp export filter 2 reject equal 192.168.0.0/24
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

21.9 BGP に導入する経路に対するフィルタの適用

[書式]

```
bgp import remote_as protocol [from_as] filter filter_num ...
no bgp import remote_as protocol [from_as] [filter filter_num ...]
```

[設定値及び初期値]

- *remote_as*
 - [設定値]: 相手の AS 番号 (1..65535)
 - [初期値]: -
- *protocol*
 - [設定値]:

設定値	説明
static	静的経路

設定値	説明
rip	RIP
ospf	OSPF
bgp	BGP
aggregate	集約経路

- [初期値]: -
- *from_as*
 - [設定値]: 導入する経路を受信した AS(*protocol* で **bgp** を指定したときのみ)(1..65535)
 - [初期値]: -
- *filter_num*
 - [設定値]: フィルタ番号 (1..2147483647)
 - [初期値]: -

[説明]

RIP や OSPF のような BGP 以外の経路を導入するときに適用するフィルタを設定する。フィルタに該当しない経路は導入されない。フィルタの番号には、**bgp import filter** コマンドで定義した番号を指定する。BGP の経路を導入するときには、その経路を受信した AS 番号を指定する必要がある。

[ノート]

このコマンドが設定されていないときには、外部経路は導入されない。
フィルタ番号は、100 個まで設定できる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

21.10 BGP の設定の有効化

[書式]

bgp configure refresh

[説明]

BGP の設定を有効にする。BGP の設定を変更したら、ルーターを再起動するか、このコマンドを実行する必要がある。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

21.11 BGP に導入する経路に適用するフィルタの設定

[書式]

bgp import filter *filter_num* [*reject*] *kind ip_address/mask ... [parameter ...]*
no bgp import filter *filter_num* [[*reject*] *kind ip_address/mask ... [parameter ...]*]

[設定値及び初期値]

- *filter_num*
 - [設定値]: フィルタ番号 (1..2147483647)
 - [初期値]: -
- *kind*
 - [設定値]:

設定値	説明
include	指定したネットワークに含まれる経路 (ネットワークアドレス自身を含む)
refines	指定したネットワークに含まれる経路 (ネットワークアドレス自身を含まない)
equal	指定したネットワークに一致する経路

- [初期値]: -
- *ip_address/mask*
 - [設定値]:

設定値	説明
ip_address/mask	IP アドレス/ネットマスク
all	すべてのネットワーク

- [初期値]: -
- *parameter*: TYPE=VALUE の組
- [設定値]:

TYPE	VALUE	説明
metric	1..16777215	MED(Multi-Exit Discriminator) で通知するメトリック値 (指定しないときは MED を送信しない)
preference	0..255	同じ経路を複数の相手から受信したときに、一方を選択するための優先度

- [初期値]:
 - preference=100

[説明]

BGP に導入する経路に適用するフィルタを定義する。このコマンドで定義したフィルタは、**bgp import** コマンドの *filter* 節で指定されてはじめて効果を持つ。

ip_address/mask では、ネットワークアドレスを設定する。複数の設定があるときには、プレフィックスが最も長く一致する設定が採用される。

kind の前に *reject* キーワードを置くと、その経路が拒否される。

[設定例]

```
# bgp import filter 1 include 10.0.0.0/16 172.16.0.0/16
# bgp import filter 2 reject equal 192.168.0.0/24
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

21.12 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

TYPE	VALUE	説明
passive	on または off	能動的な BGP コネクションの接続を抑制するか否か
gateway	IP アドレス/インタフェース	接続先に対するゲートウェイ
local-address	IP アドレス	BGP コネクションの自分のアドレス
ignore-capability	on または off	capability を無視するか否か

- [初期値]:
 - hold-time=180
 - metric は送信されない
 - passive=off
 - gateway は指定されない
 - local-address は指定されない
 - ignore-capability=off

[説明]

BGP コネクションを接続する近隣ルーターを定義する。

[ノート]

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

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

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。

キープアライブを有効にすることで近隣ルーターおよび経路情報の更新が行われるため、hold-time パラメータは 'off' 以外に設定する必要がある。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

21.13 BGP のログの設定

[書式]

```
bgp log log [log]
no bgp log [log ...]
```

[設定値及び初期値]

- log
 - [設定値]:

設定値	説明
neighbor	近隣ルーターに対する状態遷移
packet	送受信したパケット

- [初期値]: ログを記録しない。

[説明]

指定した種類のログを INFO レベルで記録する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

21.14 BGP で強制的に経路を広告する

[書式]

```
bgp force-to-advertise remote_as ip_address/mask [parameter ...]
no bgp force-to-advertise remote_as ip_address/mask [parameter ...]
```

[設定値及び初期値]

- remote_as
 - [設定値]: 相手の AS 番号

- [初期値]: -
- *ip_address/mask*
 - [設定値]: IP アドレス/ネットマスク
 - [初期値]: -
- *parameter*
 - [設定値]:
 - TYPE=VALUE の組

TYPE	VALUE	説明
metric	1..16777215	MED (Multi-Exit Discriminator) で通知するメトリック値
preference	0..255	同じ経路を複数の相手から受信したときに、一方を選択するための優先度

- [初期値]: preference=100

[説明]

本コマンドで設定した経路がルーティングテーブルに存在しない場合でも、指定された AS 番号のルーターに対して BGP で経路を強制的に広告する。経路として 'default' を指定した場合にはデフォルト経路が広告される。設定したコマンドは **bgp configure refresh** コマンドを実行したときに有効になる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

21.15 インタフェースの状態変化時、BGP に外部経路を反映させる時間間隔の設定

[書式]

```
bgp reric interval time
no bgp reric interval [time]
```

[設定値及び初期値]

- *time*
 - [設定値]: 秒数 (1 以上の数値)
 - [初期値]: 1

[説明]

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

BGP ではインタフェースの状態変化を 1 秒間隔で監視し、変化があれば最新の外部経路を自身に反映させるが、インタフェースの状態変化が連続して発生するときは、複数の外部経路の反映処理が *time* で指定した秒数の間隔でまとめて行われるようになる。

[ノート]

複数のトンネルが一斉にアップすることがあるような環境では、本コマンドの値を適切に設定することで、OSPF や BGP の外部経路の導入によるシステムへの負荷を軽減することができる。本コマンドの設定値は、OSPF への外部経路の反映にも影響する。本コマンドと **ospf reric interval** コマンドの設定値が食い違う場合には、**ospf reric interval** コマンドの設定値が優先して適用される。本コマンドの設定は、経路の変化や IP アドレスの変化に対する OSPF や BGP の動作には関係しない。また本コマンドの設定値は、**bgp configure refresh** コマンドを実行しなくても即時反映される。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

21.16 BGP の最適経路選択における MED 属性が付加されていない経路のデフォルトの MED 値の設定

[書式]

```
bgp default med med
no bgp default med [med]
```

[設定値及び初期値]

- *med*
 - [設定値]: MED 値 (1..2147483647)
 - [初期値]: 2147483647

[説明]

BGP の最適経路選択で、MED 属性が付加されていない経路に対するデフォルトの MED 値を設定する。本コマンドが設定されていない場合、MED 属性が付加されていない経路は最大の MED 値(2147483647)を持つことになり、優先度は最低となる。

本コマンドの設定は、MED 属性が付加されている経路には影響しない。

[適用モデル]

vRX VMware ESXi 版

第 22 章

IPv6

22.1 共通の設定

22.1.1 IPv6 パケットを扱うか否かの設定

[書式]

```
ipv6 routing routing
no ipv6 routing [routing]
```

[設定値及び初期値]

- *routing*
 - [設定値]:

設定値	説明
on	処理対象として扱う
off	処理対象として扱わない

- [初期値]: on

[説明]

IPv6 パケットをルーティングするか否かを設定する。本スイッチを on にしないと PP 側の IPv6 関連は一切動作しない。

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.1.2 IPv6 インタフェースのリンク MTU の設定

[書式]

```
ipv6 interface mtu mtu0
ipv6 pp mtu mtu1
ipv6 tunnel mtu mtu2
no ipv6 interface mtu [mtu0]
no ipv6 pp mtu [mtu1]
no ipv6 tunnel mtu [mtu2]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *mtu*
 - [設定値]: MTU の値 (1280..1500)
 - [初期値]:
 - mtu0=1500
 - mtu1=1500
 - mtu2=1280

[説明]

IPv6 インタフェースの MTU の値を設定する

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.1.3 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 tep mss limit mss
no ipv6 interface tcp mss limit [mss]
no ipv6 pp tcp mss limit [mss]
no ipv6 tunnel tcp mss limit [mss]

```

[設定値及び初期値]

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

設定値	説明
536..1440	MSS の最大長
auto	自動設定
off	設定しない

- [初期値]:
 - auto

[説明]

インタフェースを通過する TCP セッションの MSS を制限する。インタフェースを通過する TCP パケットを監視し、MSS オプションの値が設定値を越えている場合には、設定値に書き換える。キーワード **auto** を指定した場合には、インタフェースの MTU、もしくは PP インタフェースの場合で相手の MRU 値が分かる場合にはその MRU 値から計算した値に書き換える。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.1.4 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 tep window-scale sw
no ipv6 interface tcp window-scale [...]
no ipv6 pp tcp window-scale [...]
no ipv6 tunnel tcp window-scale [...]

```

[設定値及び初期値]

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

設定値	説明
off	何もしない
remove	TCP ウィンドウ・スケール・オプションを削除する

- [初期値]: off

[説明]

インターフェースを通過する TCP パケットのウィンドウ・スケール・オプションを強制的に変更する。remove を指定すると、ウィンドウ・スケール・オプションが有効になっていた場合には、無効にして転送する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.1.5 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.1.6 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.1.7 ICMPv6 でアドレス解決が完了するまでに送信を保留しておくことのできるパケット数の設定

[書式]

```
ipv6 interface icmp-nd queue length len
no ipv6 interface icmp-nd queue length [len]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インターフェース名
 - [初期値]: -
- *len*
 - [設定値]: キュー長 (0..10000)
 - [初期値]: 200

[説明]

ICMPv6 の Neighbor Discovery のアドレス解決が完了していないホストに対してパケットを送信しようとした時に、アドレス解決が完了するかタイムアウトにより解決できないことが確定するまで、インターフェース毎に送信を保留しておくことのできるパケットの最大数を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.1.8 近隣キャッシュの最大エントリー数の設定**[書式]**

```
ipv6 interface neighbor cache max entry num
no ipv6 interface neighbor cache max entry [num]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *num*
 - [設定値]: 最大エントリー数 (256...20480)
 - [初期値]:
 - 1024

[説明]

インターフェースごとに近隣キャッシュの最大エントリー数を設定する。近隣キャッシュのエントリー数が、設定した最大エントリー数に達した場合は、古い近隣キャッシュを削除する。本コマンド実行時、現在の近隣キャッシュのエントリー数が最大エントリー数を超える場合は、古い近隣キャッシュを削除する。

[適用モデル]

vRX VMware ESXi 版

22.1.9 IPv6 のフラグメントパケットを再構成するために保持しておく時間を設定**[書式]**

```
ipv6 reassembly hold-time sec
no ipv6 reassembly hold-time [sec]
```

[設定値及び初期値]

- *sec*
 - [設定値]:

設定値	説明
秒数 (1..60)	IPv6 のフラグメントパケットを再構成するために保持しておく時間

- [初期値]: 60 秒

[説明]

IPv6 のフラグメントパケットを再構成するために保持しておく時間。設定した時間が経過しても再構成ができなかった場合、保持していたパケットは破棄される。コマンド実行時にすでに保持していたパケットについては変更しない。

[適用モデル]

vRX VMware ESXi 版

22.2 IPv6 アドレスの管理**22.2.1 インタフェースの IPv6 アドレスの設定****[書式]**

```
ipv6 interface address ipv6_address/prefix_len [address_type]
ipv6 interface address auto
ipv6 interface address dhcp
```

```

ipv6 interface address proxy
ipv6 pp address ipv6_address/prefix_len [address_type]
ipv6 pp address auto
ipv6 pp address dhcp
ipv6 pp address proxy
ipv6 tunnel address ipv6_address/prefix_len [address_type]
ipv6 tunnel address auto
ipv6 tunnel address dhcp
ipv6 tunnel address proxy
no ipv6 interface address ipv6_address/prefix_len [address_type]
no ipv6 interface address auto
no ipv6 interface address dhcp
no ipv6 interface address proxy
no ipv6 pp address ipv6_address/prefix_len [address_type]
no ipv6 pp address auto
no ipv6 pp address dhcp
no ipv6 pp address proxy
no ipv6 tunnel address ipv6_address/prefix_len [address_type]
no ipv6 tunnel address auto
no ipv6 tunnel address dhcp
no ipv6 tunnel address proxy
    
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、LOOPBACK インタフェース名、ブリッジインタフェース名
 - [初期値]: -
- *ipv6_address*
 - [設定値]: IPv6 アドレス部分
 - [初期値]: -
- *prefix_len*
 - [設定値]: IPv6 プレフィックス長
 - [初期値]: -
- *address_type*
 - [設定値]:

設定値	説明
unicast	ユニキャスト
anycast	エニーキャスト

- [初期値]: unicast
- *auto*: RA で取得したプレフィックスとインタフェースの MAC アドレスから IPv6 アドレスを生成することを示すキーワード
 - [初期値]: -
- *dhcp*: DHCPv6 で取得したプレフィックスとインタフェースの MAC アドレスから IPv6 アドレスを生成することを示すキーワード
 - [初期値]: -
- *proxy*: プロキシ
 - [設定値]:
 - *prefix_type@prefix_interface[interface_id/prefix_len]*
 - *prefix_type*

設定値	説明
dhcp-prefix	DHCPv6 プロキシ
ra-prefix	RA プロキシ

- *prefix_interface*

設定値	説明
<i>prefix_interface</i>	転送元のインタフェース名

- *interface_id*

設定値	説明
<i>interface_id</i>	インタフェース ID

- *prefix_len*

設定値	説明
<i>prefix_len</i>	IPv6 プレフィックス長

- [初期値]: -

[説明]

インタフェースに IPv6 アドレスを付与する。

[ノート]

このコマンドで付与したアドレスは、**show ipv6 address** コマンドで確認することができる。

複数の LAN インタフェースでアドレスを自動で設定する機能を利用することができる。

具体的には、RA で取得したプレフィックスとインタフェース ID から IPv6 アドレスを生成する機能と、DHCPv6 で取得したプレフィックスとインタフェース ID から IPv6 アドレスを生成する機能が利用できる。

これらを設定する場合、デフォルト経路は最後に設定が完了したインタフェースに向く。

LOOPBACK インタフェースを指定した場合は、*auto*、*dhcp*、*address_type*、*proxy* は指定できない。

prefix_interface には LOOPBACK インタフェースは指定できない。

ブリッジインタフェースは vRX VMware ESXi 版で指定可能。

[設定例]

- LAN2 で受信した RA のプレフィックスに::1 を付け足して IPv6 アドレスを作り、それを LAN1 に付与する

```
# ipv6 lan1 address ra-prefix@lan2::1/64
```

- LAN2 が DHCPv6 で取得した /56 のプレフィックス (XXXX:XXXX:XXXX:XX00::/56) を分割し、LAN1 と LAN3 に異なる /64 のプレフィックスの IPv6 アドレスを付与する

```
LAN1 に付与する IPv6 アドレス : XXXX:XXXX:XXXX:XX01::1/64
```

```
LAN3 に付与する IPv6 アドレス : XXXX:XXXX:XXXX:XX02::1/64
```

```
# ipv6 lan1 address dhcp-prefix@lan2::1:0:0:1/64
```

```
# ipv6 lan3 address dhcp-prefix@lan2::2:0:0:1/64
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.2.2 インタフェースのプレフィックスに基づく IPv6 アドレスの設定

[書式]

```
ipv6 interface prefix ipv6_prefix/prefix_len
```

```
ipv6 interface prefix proxy
```

```
ipv6 pp prefix ipv6_prefix/prefix_len
```

```
ipv6 pp prefix proxy
```

```
ipv6 tunnel prefix ipv6_prefix/prefix_len
```

```
ipv6 tunnel prefix proxy
```

```
no ipv6 interface prefix ipv6_prefix/prefix_len
```

```
no ipv6 interface prefix proxy
```

```
no ipv6 pp prefix ipv6_prefix/prefix_len
```

```
no ipv6 pp prefix proxy
```

```
no ipv6 tunnel prefix ipv6_prefix/prefix_len
```

```
no ipv6 tunnel prefix proxy
```

[設定値及び初期値]

- *interface*

- [設定値]: LAN インタフェース名、ブリッジインタフェース名

- [初期値]: -
- *ipv6_prefix*
 - [設定値]: IPv6 プレフィックスのアドレス部分
 - [初期値]: -
- *prefix_len*
 - [設定値]: IPv6 プレフィックス長
 - [初期値]: -
- *proxy*: プロキシ
 - [設定値]:
 - *prefix_type@prefix_interface[interface_id/prefix_len]*

設定値	説明
dhcp-prefix	DHCPv6 プロキシ
ra-prefix	RA プロキシ

- *prefix_interface*

設定値	説明
<i>prefix_interface</i>	転送元のインタフェース名

- *interface_id*

設定値	説明
<i>interface_id</i>	インタフェース ID

- *prefix_len*

設定値	説明
<i>prefix_len</i>	IPv6 プレフィックス長

- [初期値]: -

[説明]

インタフェースに IPv6 アドレスを付与する。類似のコマンドに **ipv6 interface address** コマンドがあるが、このコマンドではアドレスではなくプレフィックスのみを指定する。プレフィックス以降の部分は MAC アドレスに基づいて自動的に補完する。このときに使用する MAC アドレスは、設定しようとするインタフェースに割り当てられているものが使われる。ただし、MAC アドレスを持たない PP インタフェースやトンネルインタフェースでは LAN1 インタフェースの MAC アドレスを使用する。

なお、類似の名前を持つ **ipv6 prefix** コマンドはルーター広告で通知するプレフィックスを定義するものであり、IPv6 アドレスを付与するものではない。しかしながら、通常の運用では、インタフェースに付与する IPv6 アドレスのプレフィックスとルーター広告で通知するプレフィックスは同じであるから、双方のコマンドに同じプレフィックスを設定することが多い。

[ノート]

このコマンドで付与したアドレスは、**show ipv6 address** コマンドで確認することができる。

prefix_interface には LOOPBACK インタフェースは指定できない。

ブリッジインタフェースは vRX VMware ESXi 版で指定可能。

[設定例]

- LAN2 で受信した RA のプレフィックスを LAN1 に付与する

```
# ipv6 lan1 prefix ra-prefix@lan2::/64
```

- LAN2 が DHCPv6 で取得した /56 のプレフィックス (XXXX:XXXX:XXXX:XX00::/56) を分割し、LAN1 と LAN3 に異なる /64 のプレフィックスを付与する

```
LAN1 に付与するプレフィックス : XXXX:XXXX:XXXX:XX01::/64
LAN3 に付与するプレフィックス : XXXX:XXXX:XXXX:XX02::/64
```

```
# ipv6 lan1 prefix dhcp-prefix@lan2::1:0:0:0:1/64
# ipv6 lan3 prefix dhcp-prefix@lan2::2:0:0:0:1/64
```

(注：内部動作の関係上「dhcp-prefix@lan2::1:0:0:0/64」ではなく、「dhcp-prefix@lan2::1:0:0:0/64」と設定してください。)

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.2.3 IPv6 プレフィックスに変化があった時にログに記録するか否かの設定

[書式]

```

ipv6 interface prefix change log log
ipv6 pp prefix change log log
ipv6 tunnel prefix change log log
no ipv6 interface prefix change log log
no ipv6 pp prefix change log log
no ipv6 tunnel prefix change log log

```

[設定値及び初期値]

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

設定値	説明
on	IPv6 プレフィックスの変化をログに記録する
off	IPv6 プレフィックスの変化をログに記録しない

- [初期値]: off

[説明]

IPv6 プレフィックスに変化があった時にそれをログに記録するか否かを設定する。
ログは INFO レベルで記録される。

同じプレフィックスに対するアドレスを複数設定した場合、同じログが複数回表示される。

[ノート]

ブリッジインタフェースは vRX VMware ESXi 版で指定可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.2.4 DHCPv6 の動作の設定

[書式]

```

ipv6 interface dhcp service type
ipv6 interface dhcp service client [ir=value]
ipv6 pp dhcp service type
ipv6 pp dhcp service client [ir=value]
ipv6 tunnel dhcp service type
ipv6 tunnel dhcp service client [ir=value]
no ipv6 interface dhcp service
no ipv6 pp dhcp service
no ipv6 tunnel dhcp service

```

[設定値及び初期値]

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

設定値	説明
off	DHCPv6 を使わない
client	クライアント
server	サーバー

- [初期値]: off
- *value*
- [設定値]:

設定値	説明
on	クライアントとして動作する時、Inform-Request を送信する
off	クライアントとして動作する時、Solicit を送信する

- [初期値]: off

[説明]

各インタフェースにおける DHCPv6 の動作を設定する。

[ノート]

ir オプションは vRX VMware ESXi 版で指定可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.2.5 DAD(Duplicate Address Detection) の送信回数の設定

[書式]

ipv6 interface dad retry count count

ipv6 pp dad retry count count

no ipv6 interface dad retry count [count]

no ipv6 pp dad retry count [count]

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、ブリッジインタフェース名
 - [初期値]: -
- *count*
 - [設定値]: 選択したインタフェースでの DAD の再送回数 (0..10)
 - [初期値]: 1

[説明]

インタフェースに IPv6 アドレスが設定されたときに、アドレスの重複を検出するために送信する DAD の送信回数を設定する。ただし、0 を設定した場合は、DAD を送信せずにアドレスを有効なものとして扱う。

[ノート]

ブリッジインタフェースは vRX VMware ESXi 版で指定可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.2.6 自動的に設定される IPv6 アドレスの最大数の設定

[書式]

ipv6 max auto address max

no ipv6 max auto address [max]

[設定値及び初期値]

- *max*
 - [設定値]: 自動的に設定される IPv6 アドレスの 1 インタフェースあたりの最大数 (1~256)
 - [初期値]: 16

[説明]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.2.7 始点 IPv6 アドレスを選択する規則の設定**[書式]**

ipv6 source address selection rule

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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.3 近隣探索**22.3.1 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

設定値	説明
ra-prefix	RA プロキシ

- *prefix_interface*

設定値	説明
<i>prefix_interface</i>	転送元のインタフェース名

- *interface_id*

設定値	説明
<i>interface_id</i>	インタフェース ID

- *prefix_len*

設定値	説明
<i>prefix_len</i>	IPv6 プレフィックス長

- [初期値]: -
- *preferred_lifetime*: プレフィックスの推奨寿命 (0..4294967295)
 - [初期値]: 604800
- *valid_lifetime*: プレフィックスの有効寿命 (0..4294967295)
 - [初期値]: 2592000
- *time*: 時間設定
 - [設定値]:
 - yyyy-mm-dd[,hh:mm[:ss]]

設定値	説明
yyyy	年 (1980..2079)
mm	月 (01..12)
dd	日 (01..31)
hh	時 (00..23)
mm	分 (00..59)
ss	秒 (00..59、省略時は 00)

- [初期値]: -
- *l_flag*: on-link フラグ
 - [初期値]: on
- *a_flag*: autonomous address configuration フラグ
 - [初期値]: on
- *switch*
 - [設定値]:
 - on
 - off
 - [初期値]: -

[説明]

ルーター広告で配布するプレフィックスを定義する。実際に広告するためには、**ipv6 interface rtadv send** コマンドの設定が必要である。

time では寿命を秒数または寿命が尽きる時刻のいずれかを設定できる。*time* として数値 (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::1:0:0:0:1/64」ではなく、「dhcp-prefix@lan2::1:0:0:0:1/64」と設定してください。)

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.3.2 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、DHCPv6 に代表されるルーター広告以外の手段によるアドレス自動設定をホストに許可させるか否かの設定。
o_flag	on、off	other stateful configuration フラグ。ルーター広告以外の手段により IPv6 アドレス以外のオプション情報をホストに自動的に取得させるか否かの設定。
max-rtr-adv-interval	秒数	ルーター広告を送信する最大間隔 (4..1800 秒)
min-rtr-adv-interval	秒数	ルーター広告を送信する最小間隔 (3..1350 秒)
adv-default-lifetime	秒数	ルーター広告によって設定される端末のデフォルト経路の有効時間 (0..9000 秒)

NAME	VALUE	説明
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..3600000 ミリ秒)
adv-retrans-time	ミリ秒数	ルーター広告を再送する間隔 (0..4294967295 ミリ秒)
adv-cur-hop-limit	ホップ数	ルーター広告の限界ホップ数 (0..255)
mtu	auto、off、バイト数	ルーター広告に MTU オプションを含めるか否かと、含める場合の値の設定。auto の場合はインタフェースの MTU を採用する。

- [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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.3.3 ルーター要請の再送機能の設定

[書式]

```

ipv6 interface rtsol max-retransmit mrt=mrt mrd=mrd mrc=mrc
ipv6 pp rtsol max-retransmit mrt=mrt mrd=mrd mrc=mrc
no ipv6 interface rtsol max-retransmit [...]
no ipv6 pp rtsol max-retransmit [...]

```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *mrt*
 - [設定値]: 最大再送間隔 (4..3600 (秒))
 - [初期値]: 3600
- *mrd*
 - [設定値]: 最大再送継続時間 (4..2147483647 (秒) または infinity)
 - [初期値]: infinity
- *mrc*
 - [設定値]: 最大再送回数 (0..2147483647 または infinity)
 - [初期値]: infinity

[説明]

再送間隔は初期値 4 秒から 2 倍ずつ増加していく。初期値は +10% 幅、倍率は ±10% 幅でランダムな値を取る。
 >*mrd* と >*mrc* の両方を infinity 以外に設定している場合は、>*mrd* と >*mrc* のどちらかの条件が満たされたら再送はストップする。
 >*mrc* を 0 に設定している場合は再送を行わない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.4 経路制御

22.4.1 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
<i>name</i>	PAP/CHAP による名前

• *dhcp interface*

設定値	説明
<i>interface</i>	DHCP にて与えられるデフォルトゲートウェイを使う場合の、DHCP クライアントとして動作する LAN インタフェース名 (送り先が Default の時のみ有効)

• *tunnel tunnel_num*: トンネルインタフェースへの経路

• LOOPBACK インタフェース名、NULL インタフェース名

• [初期値]: -

• *parameter*: 以下のパラメータを空白で区切り複数設定可能

• [設定値]:

設定値	説明
<i>metric metric</i>	メトリックの指定 <ul style="list-style-type: none"> • <i>metric</i> <ul style="list-style-type: none"> • メトリック値 (1..15) • 省略時は 1
<i>hide</i>	出力インタフェースが PP インタフェースの場合のみ有効なオプションで、回線が接続されている場合だけ経路が有効になることを意味する

• [初期値]: -

[説明]

IPv6 の経路情報を追加する。スコープ識別子には LAN インタフェース名を用いる。

なお LOOPBACK インタフェース、NULL インタフェースは常にアップ状態なので、hide オプションは指定はできるものの意味はない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.5 RIPng

22.5.1 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.5.2 インタフェースにおける RIPng の送信ポリシーの設定

[書式]

```
ipv6 interface rip send send
ipv6 pp rip send send
ipv6 tunnel rip send send
no ipv6 interface rip send
no ipv6 pp rip send
no ipv6 tunnel rip send
```

[設定値及び初期値]

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

設定値	説明
on	RIPng を送信する
off	RIPng を送信しない

- [初期値]: on

[説明]

RIPng の送信ポリシーを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.5.3 インタフェースにおける RIPng の受信ポリシーの設定

[書式]

```
ipv6 interface rip receive receive
ipv6 pp rip receive receive
ipv6 tunnel rip receive receive
```

no ipv6 interface rip receive**no ipv6 pp rip receive****no ipv6 tunnel rip receive****[設定値及び初期値]**

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

設定値	説明
on	受信した RIPng パケットを処理する
off	受信した RIPng パケットを無視する

- [初期値]: on

[説明]

RIPng の受信ポリシーを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.5.4 RIPng の加算ホップ数の設定**[書式]****ipv6 interface rip hop direction hop****ipv6 pp rip hop direction hop****no ipv6 interface rip hop direction****no ipv6 pp rip hop direction****[設定値及び初期値]**

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

設定値	説明
in	受信時に加算する
out	送信時に加算する

- [初期値]: -
- *hop*
 - [設定値]: 加算ホップ数 (0..15)
 - [初期値]: 0

[説明]

PP インタフェースで送受信する RIPng のメトリックに対して加算するホップ数を設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.5.5 インタフェースにおける信頼できる RIPng ゲートウェイの設定**[書式]****ipv6 interface rip trust gateway [except] gateway [gateway...]****ipv6 pp rip trust gateway [except] gateway [gateway...]****no ipv6 interface rip trust gateway [[except] gateway [gateway...]]****no ipv6 pp rip trust gateway [[except] gateway [gateway...]]****[設定値及び初期値]**

- *interface*
 - [設定値]: LAN インタフェース名

- [初期値]: -
- *gateway*
 - [設定値]: IPv6 アドレス
 - [初期値]: -

[説明]

信頼できる RIPng ゲートウェイを設定する。

except キーワードを指定していない場合には、列挙したゲートウェイを信用できるゲートウェイとし、それらからの RIP だけを受信する。

except キーワードを指定した場合は、列挙したゲートウェイを信用できないゲートウェイとし、それらを除いた他のゲートウェイからの RIP だけを受信する。

gateway は 10 個まで指定可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.5.6 RIPng で送受信する経路に対するフィルタリングの設定

[書式]

```
ipv6 interface rip filter direction filter_list [filter_list...]
```

```
ipv6 pp rip filter direction filter_list [filter_list...]
```

```
ipv6 tunnel rip filter direction filter_list [filter_list...]
```

```
no ipv6 interface rip filter direction
```

```
no ipv6 pp rip filter direction
```

```
no ipv6 tunnel rip filter direction
```

[設定値及び初期値]

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

設定値	説明
in	内向きのパケットを対象にする
out	外向きのパケットを対象にする

- [初期値]: -
- *filter_list*
 - [設定値]: フィルタ番号
 - [初期値]: -

[説明]

インタフェースで送受信する RIPng パケットに対して適用するフィルタを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.5.7 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

設定値	説明
interval	ipv6 pp rip connect interval コマンドで設定された時間間隔で RIPng を送出する
update	経路情報が変わった時にのみ RIPng を送出する

- [初期値]: update

[説明]

選択されている相手について回線接続時に RIPng を送出する条件を設定する。

[設定例]

```
# ipv6 pp rip connect interval 60
# ipv6 pp rip connect send interval
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.5.8 回線接続時の PP 側の RIPng 送出の時間間隔の設定

[書式]

```
ipv6 pp rip connect interval time
no ipv6 pp rip connect interval
```

[設定値及び初期値]

- *time*
 - [設定値]: 秒数 (30..21474836)
 - [初期値]: 30

[説明]

選択されている相手について回線接続時に RIPng を送出する時間間隔を設定する。

[設定例]

```
# ipv6 pp rip connect interval 60
# ipv6 pp rip connect send interval
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.5.9 回線切断時の PP 側の RIPng の動作の設定

[書式]

```
ipv6 pp rip disconnect send action
no ipv6 pp rip disconnect send
```

[設定値及び初期値]

- *action*
 - [設定値]:

設定値	説明
none	RIPng を送信しない
interval	ipv6 pp rip connect interval コマンドで設定された時間間隔で RIPng を送出する
update	経路情報が変わった時にのみ RIPng を送信する

- [初期値]: none

[説明]

選択されている相手について回線切断時に RIPng を送出する条件を設定する。

[設定例]

```
# ipv6 pp rip disconnect interval 1800
# ipv6 pp rip disconnect send interval
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.5.10 回線切断時の PP 側の RIPng 送出の時間間隔の設定

[書式]

```
ipv6 pp rip disconnect interval time
no ipv6 pp rip disconnect interval
```

[設定値及び初期値]

- *time*
 - [設定値]: 秒数 (30..21474836)
 - [初期値]: 3600

[説明]

選択されている相手について回線切断時に RIPng を送出する時間間隔を設定する。

[設定例]

```
# ipv6 pp rip disconnect interval 1800
# ipv6 pp rip disconnect send interval
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.5.11 RIPng による経路を回線切断時に保持するか否かの設定

[書式]

```
ipv6 pp rip hold routing hold
no ipv6 pp rip hold routing
```

[設定値及び初期値]

- *hold*
 - [設定値]:

設定値	説明
on	保持する
off	保持しない

- [初期値]: off

[説明]

PP インタフェースから RIPng で得られた経路を、回線が切断されたときに保持するか否かを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.5.12 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.6 VRRPv3 の設定

22.6.1 インタフェース毎の VRRPv3 の設定

[書式]

```
ipv6 interface vrrp vrid ipv6_address [priority=priority] [preempt=preempt] [auth=auth] [advertise-interval=time1] [down-interval=time2]
```

```
no ipv6 interface vrrp vrid [vrid...]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *vrid*
 - [設定値]: VRRPv3 グループ ID (1..255)
 - [初期値]: -
- *ipv6_address*
 - [設定値]: 仮想ルーターの IPv6 アドレス
 - [初期値]: -
- *priority*
 - [設定値]: 優先度 (1..254)
 - [初期値]: 100
- *preempt*: プリエンプトモード
 - [設定値]:

設定値	説明
on	使用する
off	使用しない

- [初期値]: on
- *auth*
 - [設定値]: テキスト認証文字列 (8 文字以内)
 - [初期値]: -
- *time1*
 - [設定値]: VRRPv3 広告の送信間隔 (1..60 秒)
 - [初期値]: 1
- *time2*
 - [設定値]: マスターがダウンしたと判定するまでの時間 (3..180 秒)
 - [初期値]: 3

[説明]

指定した VRRPv3 グループを利用することを設定する。

同じ VRRPv3 グループに所属するルーターの間では、VRID および仮想ルーターの IPv6 アドレスを一致させておかななくてはならない。これらが食い違った場合の動作は予測できない。

auth パラメータを指定しない場合には、認証なしとして動作する。

time1 および *time2* パラメータで、マスターが VRRPv3 広告を送信する間隔と、バックアップがそれを監視してダウンと判定するまでの時間を設定する。トラフィックが多いネットワークではこれらの値を初期値より長めに設定すると動作が安定することがある。これらの値はすべての VRRPv3 ルーターで一致している必要がある。

[ノート]

priority および *preempt* パラメータの設定は、仮想ルーターの IPv6 アドレスとして自分自身の LAN インタフェースに付与されているアドレスを指定している場合には無視される。この場合、優先度は最高の 255 となり、常にプリエンプトモードで動作する。

[適用モデル]

vRX VMware ESXi 版

22.6.2 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 tunnel tunnel_num
ipv6 interface vrrp shutdown trigger vrid route network [nexthop]
no ipv6 interface vrrp shutdown trigger vrid interface
no ipv6 interface vrrp shutdown trigger vrid pp peer_num
no ipv6 interface vrrp shutdown trigger vrid tunnel tunnel_num
no ipv6 interface vrrp shutdown trigger vrid route network
    
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *vrid*
 - [設定値]: VRRPv3 グループ ID (1..255)
 - [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: tunnel インターフェース番号
 - [初期値]: -
- *network*
 - [設定値]:
 - IPv6 プレフィックス/プレフィックス長
 - default
 - [初期値]: -
- *nexthop*
 - [設定値]:
 - インタフェース名
 - IPv6 アドレス
 - [初期値]: -

[説明]

設定した VRRPv3 グループでマスタールーターとして動作している場合に、指定した条件によってシャットダウンすることを設定する。

形式	説明
LAN インタフェース形式	指定した LAN インタフェースがリンクダウンするか、あるいは lan keepalive でダウンが検知されると、シャットダウンする。
pp 形式	指定した相手先情報番号に該当する回線で通信できなくなった場合にシャットダウンする。通信できなくなるとは、ケーブルが抜けるなどレイヤ 1 が落ちた場合と、以下の場合である。 <ul style="list-style-type: none"> • 回線が専用線である時には、LCP キープアライブによって通信相手が落ちたと判断した場合 • pp keepalive use 設定によりダウンが検出された場合
tunnel 形式	指定した tunnel インターフェースが以下の条件によりダウンした場合にシャットダウンする。 <ul style="list-style-type: none"> • IPsec トンネルで、ipsec ike keepalive use 設定によりダウンが検出された場合

形式	説明
	<ul style="list-style-type: none"> L2TP/IPsec、L2TPv3、L2TPv3/IPsec のいずれかのトンネルで、l2tp keepalive use 設定によりダウンが検出された場合 IPIP トンネルで、ipip keepalive use 設定によりダウンが検出された場合
route 形式	指定した経路が経路テーブルに存在しないか、 <i>nexthop</i> で指定したインタフェースもしくは 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。 <i>nexthop</i> を省略した場合には、経路がどのような先に向いていても存在する限りはシャットダウンしない。

[適用モデル]

vRX VMware ESXi 版

22.7 フィルタの設定

22.7.1 IPv6 フィルタの定義

[書式]

```
ipv6 filter filter_num pass_reject src_addr[/prefix_len] [dest_addr[/prefix_len] [protocol [src_port_list [dest_port_list]]]]
no ipv6 filter filter_num [pass_reject]
```

[設定値及び初期値]

- filter_num*
 - [設定値]: 静的フィルタ番号 (1..21474836)
 - [初期値]: -
- pass_reject*
 - [設定値]: フィルタのタイプ (**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 のフィルタを定義する。

[ノート]

近隣探索に関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

[設定例]

PP 1 で送受信される IPv6 Packet Too Big を記録する

```
# pp select 1
# ip pp secure filter in 1 100
# ip pp secure filter out 1 100
# ipv6 filter 1 pass-log * * icmp6 2
# ipv6 filter 100 pass * *
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.7.2 IPv6 フィルタの適用

[書式]

```
ipv6 interface secure filter direction [filter_list...] [dynamic filter_list]
ipv6 pp secure filter direction [filter_list...] [dynamic filter_list]
ipv6 tunnel secure filter direction [filter_list...] [dynamic filter_list]
no ipv6 interface secure filter direction
no ipv6 pp secure filter direction
no ipv6 tunnel secure filter direction
```

[設定値及び初期値]

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

設定値	説明
in	受信したパケットのフィルタリング
out	送信するパケットのフィルタリング

- [初期値]: -
- *filter_list*
 - [設定値]: 空白で区切られたフィルタ番号の並び (静的フィルタと動的フィルタの数の合計として 128 個以内)
 - [初期値]: -
- *dynamic*: キーワード後に動的フィルタの番号を記述する
 - [初期値]: -

[説明]

IPv6 フィルタをインタフェースに適用する。

[ノート]

LOOPBACK インタフェースと NULL インタフェースでは動的フィルタは使用できない。
 NULL インタフェースで *direction* に 'in' は指定できない。
 ブリッジインタフェースは vRX VMware ESXi 版で指定可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.7.3 IPv6 動的フィルタの定義

[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/
 - dhcpcv6c/dhcpcv6s/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番号のリスト
 - [初期値]: -
- *option*
 - [設定値]:
 - syslog=switch

設定値	説明
on	接続の通信履歴を syslog に残す
off	接続の通信履歴を syslog に残さない

- timeout=*time*

設定値	説明
1..2147483647	データが流れなくなったときに接続情報を解放するまでの秒数

- [初期値]:
 - syslog=on
 - timeout=60

[説明]

IPv6 の動的フィルタを定義する。第 1 書式では、あらかじめルーターに登録されているアプリケーション名を指定する。第 2 書式では、ユーザがアクセス制御のルールを記述する。キーワードの **filter**、**in**、**out** の後には、**ipv6 filter** コマンドで定義されたフィルタ番号を設定する。

filter キーワードの後に記述されたフィルタに該当する接続 (トリガ) を検出したら、それ以降 **in** キーワードと **out** キーワードの後に記述されたフィルタに該当する接続を通過させる。**in** キーワードはトリガの方向に対して逆方向のアクセスを制御し、**out** キーワードは動的フィルタと同じ方向のアクセスを制御する。なお、**ipv6 filter** コマンドの IP アドレスは無視される。pass/reject の引数も同様に無視される。

ここに記載されていないアプリケーションについては、filter キーワードを使って定義することで扱える可能性がある。特に snmp のように動的にポート番号が変化しないプロトコルの扱いは容易である。

tcp か udp を設定することで扱える可能性がある。特に、telnet のように動的にポート番号が変化しないプロトコルは tcp を指定することで扱うことができる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

22.8 近隣要請

22.8.1 アドレス重複チェックをトリガに近隣要請を行うか否かの設定

[書式]

```
ipv6 nd ns-trigger-dad on [option=value]
ipv6 nd ns-trigger-dad off
no ipv6 nd ns-trigger-dad [...]
```

[設定値及び初期値]

- on
 - [設定値]: 近隣要請を行う
 - [初期値]: -
- off
 - [設定値]: 近隣要請を行わない
 - [初期値]: -
- option=value 列: MLD の動作方式
 - [設定値]:

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

- [初期値]: na-proxy=all

[初期設定]

```
ipv6 nd ns-trigger-dad off
```

[説明]

RA プロキシにおいて、下流よりアドレス重複チェックの近隣要請を受信した際に、そのグローバルアドレスを送信元とした近隣要請を上流に送信するか否かを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

第 23 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。

23.1 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

23.2 SMTP メールサーバーの設定

[書式]

mail server smtp *id address [port=port] [smtp-auth username password [auth_protocol]] [pop-before-smtp] [smtps]*

no mail server smtp *id [...]*

[設定値及び初期値]

- *id*
 - [設定値]: メールサーバー設定 ID (1..10)
 - [初期値]: -
- *address*
 - [設定値]: サーバーの IP アドレスまたはホスト名
 - [初期値]: -
- *port*
 - [設定値]: サーバーのポート番号 (省略時は 25、または、465)
 - [初期値]: -
- *username*
 - [設定値]: 認証用ユーザ名
 - [初期値]: -
- *password*
 - [設定値]: 認証用パスワード
 - [初期値]: -
- *auth_protocol*: SMTP-AUTH 認証プロトコル
 - [設定値]:

設定値	説明
cram-md5	CRAM-MD5

設定値	説明
digest-md5	DIGEST-MD5
plain	PLAIN 認証

- [初期値]: -
- `pop-before-smtp`
 - [設定値]: POP before SMTP の使用
 - [初期値]: -
- `smtps`
 - [設定値]: SMTPS の使用
 - [初期値]: -

[説明]

メール送信に使用するサーバー情報を設定する。

`smtp-auth` パラメータでは、メール送信の際の SMTP 認証のためのデータ (ユーザ名、パスワード) を指定する。

SMTP サーバーで認証が必要ない場合は `smtp-auth` の設定は必要ない。

SMTP 認証でサポートしている認証プロトコルは、CRAM-MD5、DIGEST-MD5 および PLAIN 認証の 3 種類である。

`smtp-auth` パラメータでプロトコルを指定した場合にはそれを用い、プロトコルが省略された場合には SMTP サーバーとの前記の順で認証交渉を行う。

`pop-before-smtp` パラメータを設定すると、メール送信時に POP before SMTP 動作を行う。ここで行う POP 動作は、**mail server pop** コマンドで同じ ID で設定したものを利用する。`pop-before-smtp` パラメータが設定されているのに、対応する **mail server pop** コマンドの設定がないと、メールは送信できない。

`smtps` パラメーターが設定されている場合、SMTPS を使用してメールを送信する。`smtps` パラメーターと `pop-before-smtp` パラメーターは同時に設定できない。

`port` パラメーターを省略した場合、`smtps` パラメーターの設定によって、メールサーバーのポート番号として使用する値が変わる。`smtps` パラメーターの設定と、メールサーバーのポート番号の対応は以下のとおり。

<code>smtps</code> パラメーター	使用するポート番号
設定しない (省略)	25
設定する	465

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

23.3 POP メールサーバーの設定

[書式]

`mail server pop id address [port=port] protocol username password`

`no mail server pop id [...]`

[設定値及び初期値]

- `id`
 - [設定値]: メールサーバー設定 ID (1..10)
 - [初期値]: -
- `address`
 - [設定値]: サーバーの IP アドレスまたはホスト名
 - [初期値]: -
- `port`
 - [設定値]: サーバーのポート番号 (省略時は 110)
 - [初期値]: -
- `protocol`
 - [設定値]:

設定値	説明
pop3	POP3
apop	APOP

- [初期値]: -

- *username*
 - [設定値]: 認証用ユーザ名
 - [初期値]: -
- *password*
 - [設定値]: 認証用パスワード
 - [初期値]: -

[説明]

メール受信に使用するサーバー情報を設定する。

mail server smtp コマンドで *pop-before-smtp* パラメータを設定したときに必要な設定である。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

23.4 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

23.5 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/QAC/TM Info
- *date*

- [設定値]: メールヘッダに表示する時刻
- [初期値]: 送信時の時刻
- *mime_version*
 - [設定値]: メールヘッダに表示する MIME-Version
 - [初期値]: 1.0
- *content_type*
 - [設定値]: メールヘッダに表示する 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:vRX test" "Date:Mon, 23 Feb 2004 09:54:20 +0900"
MIME-Version:1.0 "Content-Type:text/plain; charset=iso-2022-jp"
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

23.6 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フェース
 - [設定値]:

設定値	説明
pp	PP バックアップ
lanN	LAN バックアップ
tunnel	TUNNEL バックアップ

- [初期値]: -
- *range_b*
 - [設定値]:
 - インタフェース番号および範囲指定
 - pp,tunnel のみ (*,xx-yy,zz etc)
 - [初期値]: -
- *route*
 - [設定値]:
 - ネットマスク付きの経路
 - default
 - [初期値]: -
- *if_f*
 - [設定値]: メール通知を行うイーサネットフィルタの設定された LAN インタフェース
 - [初期値]: -
- *dir_f*: フィルタ設定の方向
 - [設定値]:

設定値	説明
in	受信方向
out	送信方向

- [初期値]: -
- *type*: メール通知で通知する情報
 - [設定値]:

設定値	説明
all	全ての内容
interface	インタフェースの情報
routing	ルーティングの情報
vpn	VPN の情報
nat	NAT の情報
firewall	ファイアウォールの情報
config-log	設定情報とログ

- [初期値]: -
- *if_i*: 不正アクセス検知設定のインタフェース
 - [設定値]:

設定値	説明
pp	PP インタフェース
lanN(N,M)	LAN インタフェース

設定値	説明
tunnel	TUNNEL インタフェース
*	全てのインタフェース

- [初期値]: -
- *range_i*
 - [設定値]:
 - インタフェース番号および範囲指定
 - 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についてはログ表示されるものが対象となる。

イーサネットフィルタ..... **pass-log, reject-log** パラメータの定義

内部状態を通知する場合は、**mail notify status exec** コマンドを実行する必要がある。

不正アクセス検知については **ip interface intrusion detection** コマンドの設定により検出されたものが通知対象となる。

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

[設定例]

```
mail notify 1 1 trigger backup pp * lan2 lan3 tunnel 1-10,12
mail notify 2 1 trigger route 192.168.1.0/24 172.16.0.0/16
mail notify 3 1 trigger filter ethernet lan1 in
mail notify 4 1 trigger status all
mail notify 5 1 trigger intrusion lan1 in/out pp * in tunnel 1-3,5 out
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

第 24 章

スケジュール

24.1 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 +timer * command...
schedule at id +timer pp peer_num command...
schedule at id +timer tunnel tunnel_num 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

- [初期値]: -

- *timer* : *command* を実行するまでの時間 (秒、1..3600)
 - [初期値] :-
- *peer_num*
 - [設定値] :
 - 相手先情報番号
 - anonymous
 - [初期値] :-
- *tunnel_num*
 - [設定値] : トンネルインタフェースの番号
 - [初期値] :-
- *command*
 - [設定値] : 実行するコマンド (制限あり)
 - [初期値] :-

[説明]

time で指定した時刻、または *timer* で指定した時間後に、*command* で指定されたコマンドを実行する。

第 2、第 3 書式で指定された場合には、それぞれあらかじめ指定された相手先情報番号/トンネル番号での、**pp select/tunnel select** コマンドが発行済みであるように動作する。

schedule at コマンドは複数指定でき、同じ時刻に指定されたものは *id* の小さな順に実行される。

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**、**clear vrx license**、**cold start**、**confirm**、**console info** と **console prompt** を除く **console** で始まるコマンド、**copy**、**date**、**delete**、**echo**、**embedded file**、**exit**、**export vrx license**、**help**、**import vrx license**、**interface reset**、**ipsec transport template**、**ipv6 ospf configure refresh**、**less** で始まるコマンド、**load**、**login password**、**login password encrypted**、**login timer**、**login user**、**luac**、**macro**、**make directory**、**nslookup**、**ospf configure refresh**、**packetdump**、**ping**、**ping6**、**pp select**、**quit**、**rename**、**rollback timer**、**save**、**schedule at**、**scp**、**show** で始まるコマンド、**ssh**、**sshd host key generate**、**sshd session**、**system packet-buffer**、**telnet**、**telnetd session**、**time**、**timezone**、**traceroute**、**traceroute6**、**tunnel select**、**tunnel template**、**user attribute**、**vrx license update schedule**

[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いが、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]

- 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
```

- コマンド設定時から 10 分後に再起動する

```
# schedule at 1 +600 * restart
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

第 25 章

生存通知機能

25.1 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ず。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

25.2 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]:

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

- [初期値]:
 - log=off
 - monitor=off

[説明]

受信した生存通知の内容を syslog に出力するか否かを設定する。

monitor オプションで指定した監視時間内に生存通知が届かないとき、syslog を出力し SNMP トラップを送出する。

[ノート]

本コマンドを設定する前に、**heartbeat pre-shared-key** コマンドで、送信側ルーターとの共有鍵を設定する必要がある。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

25.3 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

第 26 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、動作には互換性がない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 at** コマンドと組み合わせることで実現していた通知の定期送信は、送信設定コマンドのみで実施できるようになります。
- 通知する IP アドレスは原則として生存通知パケットの送出インタフェースに設定されている IP アドレスとなります。ここで、当該インタフェースに NAT や IP マスカレードが設定されていれば、送出する通知パケットに NAT / IP マスカレード設定を適用した場合の IP アドレスが使用されます。ただし、**unnumbered** 接続の回線を使用して生存通知パケットを送信する場合は、IP アドレスが設定されている LAN インタフェースの中で、若番のインタフェースから優先的に IP アドレスを選択して通知します (通知パケットの IP ヘッダの始点アドレスと同期)。
- 受信した生存通知の情報を **show status heartbeat2** コマンドで表示することができます。

26.1 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 **ja.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。

また、vRX VMware ESXi 版では、VMware ESXi の Web コンソールを使用しているときには、**console character** コマンドの設定が **ja.sjis** の場合でも、意図した通りに処理されない場合がある。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

26.2 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)。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

26.3 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

26.4 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

26.5 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

26.6 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、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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

26.7 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

26.8 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

26.9 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

26.10 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..10000)
 - [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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

26.11 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 *ja.sjis* の場合にのみ正しく動作し、他の設定では誤動作する可能性がある。

また、vRX VMware ESXi 版では、VMware ESXi の Web コンソールを使用しているときには、**console character** コマンドの設定が *ja.sjis* の場合でも、誤動作する可能性がある。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

26.12 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 *ja.sjis* の場合にのみ正しく動作し、他の設定では誤動作する可能性がある。

また、vRX VMware ESXi 版では、VMware ESXi の Web コンソールを使用しているときには、**console character** コマンドの設定が *ja.sjis* の場合でも、誤動作する可能性がある。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

第 27 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。

27.1 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

27.2 SNTP サーバーへのアクセスを許可するホストの設定

[書式]

`sntpd host ip_range [ip_range...]`

`sntpd host any`

`sntpd host none`

`sntpd host lan`

`no sntpd host`

[設定値及び初期値]

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

- [設定値]:

設定値	説明
1 個の IP アドレスまたは間にハイフン (-) をはさんだ IP アドレス (範囲指定)、およびこれらを任意に並べたもの	指定したホストからのアクセスを許可する
lanN	LAN インターフェースからのアクセスを許可する

- [初期値]: -

- any

- [設定値]: すべてのホストからのアクセスを許可する

- [初期値]: -

- none

- [設定値]: すべてのホストからのアクセスを禁止する

- [初期値]: -

- lan

- [設定値]: すべての LAN 側ネットワーク内からのアクセスを許可する
- [初期値]: -

[初期設定]

```
sntpd host lan
```

[説明]

SNTP サーバーへのアクセスを許可するホストを設定する。

[ノート]

このコマンドで LAN インタフェースを指定した場合には、ネットワークアドレスとディレクテッドブロードキャストアドレスを除く IPv4 アドレスからのアクセスを許可する。

指定した LAN インタフェースにプライマリアドレスもセカンダリアドレスも設定していなければアクセスを許可しない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

第 28 章

ブリッジインタフェース (ブリッジ機能)

ブリッジインタフェースは複数のインタフェースを 1 つの仮想インタフェースに收容し、收容したインタフェース間でブリッジングを行う機能です。

收容された各インタフェースが接続する物理的なセグメントは 1 つのセグメントとして扱います。

注意事項

- 本機能におけるブリッジ処理はワイヤレートを保証するものではありません。
- QoS 機能には対応していません。そのため、QoS 機能を利用した Dynamic Traffic Control 機能を利用することはできません。
- スパニングツリープロトコルには対応していません。
- BPDU フレームは透過します。

28.1 ブリッジインタフェースに收容するインタフェースを設定する

[書式]

```
bridge member bridge_interface interface interface [...]
```

```
no bridge member bridge_interface [interface ...]
```

[設定値及び初期値]

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

設定値	説明
lanN	LAN インタフェース名
tunnelN	TUNNEL インタフェース名
tunnelN-tunnelM	TUNNEL インタフェースの範囲

- [初期値]: -

[説明]

仮想インタフェースであるブリッジインタフェースに收容するインタフェースを指定する。

收容したインタフェース間でブリッジ動作が行われる。

トンネルインタフェースを收容した場合、L2TPv3 トンネルが確立しているトンネルインタフェースでのみブリッジ動作が行われる。

[ノート]

- 收容する LAN インタフェースについて

收容した実インタフェースに IPv4, IPv6 アドレスを付与してはならない。

收容した実インタフェースの IPv6 リンクローカルアドレスは削除される。

收容する LAN インタフェースの MTU はすべて同一の値でなければならない。

いずれかのブリッジインタフェースに收容した実インタフェースは、他のブリッジインタフェースに收容することはできない。

- 收容するトンネルインタフェースについて

收容するトンネルインタフェースの MTU は無効となり、トンネルインタフェースでフラグメントは行われず、カプセル化されたパケットの送信インタフェースの MTU に従ってフラグメントが発生する。

いずれかのブリッジインタフェースに收容したインタフェースは、他のブリッジインタフェースに收容することはできない。

- ブリッジインタフェースについて

ブリッジインタフェースのリンク状態は收容した LAN インタフェースまたはトンネルインタフェースのリンク状態に応じて変化する。

いずれかの収容したインタフェースがアップ状態だった場合、ブリッジインタフェースはアップ状態になる。すべてのインタフェースがダウン状態だった場合、ブリッジインタフェースもダウン状態になる。ブリッジインタフェースの MAC アドレスは、収容した LAN インタフェースのうち、インタフェース番号がもっとも小さいインタフェースのアドレスを使用する。

[適用モデル]

vRX VMware ESXi 版

28.2 自動的なラーニングを行うか否かの設定

[書式]

```
bridge learning bridge_interface switch
no bridge learning bridge_interface [switch]
```

[設定値及び初期値]

- *bridge_interface*
 - [設定値]: ブリッジインタフェース名
 - [初期値]: -
- *switch*
 - [設定値]:

設定値	説明
on	ラーニングする
off	ラーニングしない

- [初期値]: on

[説明]

ブリッジ機能で自動的な MAC アドレスのラーニングを行うか否かを設定する。

bridge_interface には対象となるブリッジインタフェース名を指定する。

ラーニングを行う場合、ブリッジインタフェースに収容したインタフェースでパケットを受信すると、そのパケットの始点 MAC アドレスと受信インタフェースを学習してラーニングテーブルに登録する。

学習した情報はブリッジ処理が行われるときに参照され、パケットが不要なインタフェースに出力されることを抑制する。

[ノート]

学習時にラーニングテーブルが上限に達していた場合、もっとも古いエントリ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、一致するエントリが存在しなかった場合、受信インタフェースを除くすべての収容インタフェースにパケットが出力される。これはリピーターと同様の動作である。

[適用モデル]

vRX VMware ESXi 版

28.3 ブリッジがラーニングした情報の消去タイマーの設定

[書式]

```
bridge learning bridge_interface timer time
no bridge learning bridge_interface timer [time]
```

[設定値及び初期値]

- *bridge_interface*
 - [設定値]: ブリッジインタフェース名
 - [初期値]: -
- *time*
 - [設定値]:

設定値	説明
30..32767	秒数
off	タイマを設定しない

- [初期値]: 300

[説明]

ブリッジが自動的にラーニングした情報の寿命を設定する。

bridge_interface には対象となるブリッジインタフェース名を指定する。

指定した時間内に、ある始点 MAC アドレスからパケットを受信しなかった場合はその MAC アドレスに関する学習した情報を消去する。

off を指定した場合には、学習した情報が自動的に消去されることはなくなる。

[適用モデル]

vRX VMware ESXi 版

28.4 静的なラーニング情報の設定

[書式]

```
bridge learning bridge_interface static mac_address interface
no bridge learning bridge_interface static mac_address [interface]
```

[設定値及び初期値]

- *bridge_interface*
 - [設定値]: ブリッジインタフェース名
 - [初期値]: -
- *mac_address*
 - [設定値]: MAC アドレス
 - [初期値]: -
- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -

[説明]

ブリッジが参照する静的な登録情報を設定する。

bridge_interface には対象となるブリッジインタフェース名を指定する。

mac_address に指定した MAC アドレスが宛先であるパケットは、*interface* で指定したインタフェースに出力されるようになる。

interface には *bridge_interface* に収容された LAN インタフェースを指定する。

[ノート]

静的に登録した情報は自動的に学習した情報よりも優先して参照される。

interface で指定した LAN インタフェースが *bridge_interface* に収容されていない場合、登録した情報は無視される。

[適用モデル]

vRX VMware ESXi 版

第 29 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。

29.1 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

29.2 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

29.3 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

29.4 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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

29.5 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..9	Lua タスクの番号

- [初期値]: -
- script_file*
 - [設定値]: 強制終了するスクリプトファイル名またはバイトコードファイル名を絶対パスもしくは相対パスで指定する
 - [初期値]: -

[説明]

指定した Lua タスク、または、Lua スクリプトを強制終了する。

第 1 書式では、*task_id* で指定された Lua タスクを強制終了する。Lua タスクの番号や実行しているスクリプトについては **show status lua** コマンドで確認できる。

第 2 書式では、*script_file* で指定されたパスとファイル名が完全に一致するスクリプトを実行しているすべての Lua タスクを強制終了する。*script_file* に相対パスを指定した場合、環境変数 PWD を基点とする絶対パスに置換された後で対象の Lua タスクの検索が行われる。

lua コマンドの -e オプションを使用して、スクリプトファイルを使用せずに実行されているような Lua スクリプトを強制終了させる場合は、第 1 書式を使用する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

第 30 章

操作

30.1 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.2 トンネルインタフェース番号の選択

[書式]

```
tunnel select tunnel_num
no tunnel select
```

[設定値及び初期値]

- *tunnel_num*
 - [設定値]:

設定値	説明
番号	トンネルインタフェース番号
none	トンネルインタフェースを選択しない

- [初期値]: -

[説明]

トンネルモードの設定や表示の対象となるトンネルインタフェース番号を選択する。

[ノート]

本コマンドの操作は、一般ユーザでも実行できる。

プロンプトが tunnel の場合は、pp 関係のコマンドは入力できない。

no tunnel select コマンドは **tunnel select none** コマンドと同じ動作をする。

選択できるトンネルインタフェース番号のモデルによる違いは [IPsec の設定](#) (177 ページ) を参照

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.3 設定に関する操作

30.3.1 管理ユーザへの移行

[書式]

administrator

[説明]

このコマンドを発行してからでないと、ルーターの設定は変更できない。また操作コマンドも実行できない。パラメータはなく、コマンド入力後にプロンプトに応じて改めて管理パスワードを入力する。入力されるパスワードは画面には表示されない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.3.2 終了

[書式]

quit

quit save

exit

exit save

[設定値及び初期値]

- **save**: 管理ユーザから抜ける際に指定すると、設定内容を不揮発性メモリに保存して終了
 - [初期値]: -

[説明]

ルーターへのログインを終了、または管理ユーザーから抜ける。

設定を変更して保存せずに管理ユーザーから抜けようとする、新しい設定内容を不揮発性メモリに保存するか否かを問い合わせる。不揮発性メモリに保存されれば、再起動を経ても同じ設定での起動が可能となる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.3.3 設定内容の保存

[書式]

save *[filename [comment]]*

[設定値及び初期値]

- **filename**: 設定を保存するファイル名
 - [設定値]:

設定値	説明
0~4	設定ファイル番号

- [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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.3.4 設定ファイルの複製

[書式]

copy config *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
0..4.2	設定ファイル番号
prefix:filename	外部ストレージ内の設定ファイル名
emfs:filename	EMFS 内の設定ファイル名

- [初期値]: -

- *to* : コピー先ファイル名

- [設定値]:

設定値	説明
0..4	設定ファイル番号
prefix:filename	外部ストレージ内の設定ファイル名

- [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ストレージのファイルを指定することはできない。

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。

コピー先に外部ストレージを指定する場合、*filename* に絶対パスを使ってファイルを指定する。

prefix には *mount* コマンドでマウントした外部ストレージのプレフィックスを指定し、*filename* には絶対パスを使用して対象とするファイルを指定する。

絶対パスのディレクトリ名及びファイル名長は最大 255 文字で指定する。

マウントされている外部ストレージは *show status storage interface* コマンドで確認できる。

[ノート]

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。外部ストレージおよび暗号アルゴリズムは vRX VMware ESXi 版で指定可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.3.5 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	全ての設定ファイル
0..4.2	設定ファイル番号

- [初期値]: -

[説明]

保存されている設定ファイルを削除する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.3.6 デフォルト設定ファイルの設定

[書式]

```
set-default-config filename
```

[設定値及び初期値]

- *filename*
 - [設定値]: 設定ファイル番号 (0..4.2)
 - [初期値]: -

[説明]

起動時に使用する設定ファイルを設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.3.7 設定の初期化

[書式]

```
cold start
```

[説明]

デプロイ時の設定に戻し、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]

設定ファイルがすべて削除されることに注意。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.3.8 遠隔地のルーターからの設定に対する制限

[書式]

```
remote setup accept tel_num [tel_num_list]
remote setup accept any
remote setup accept none
no remote setup accept
```

[設定値及び初期値]

- *tel_num*
 - [設定値]: 電話番号
 - [初期値]: -
- *tel_num_list*
 - [設定値]: 電話番号を空白で区切った並び
 - [初期値]: -
- *any*: すべての遠隔地のルーターからの設定を許可することを示すキーワード
 - [初期値]: *any*
- *none*: すべての遠隔地のルーターからの設定を拒否することを示すキーワード
 - [初期値]: -

[説明]

自分のルーターの設定を許可する相手先を設定する。

[適用モデル]

vRX VMware ESXi 版

30.4 動的情報のクリア操作

30.4.1 アカウントのクリア

[書式]

```
clear account
```

[説明]

アカウント情報をクリアする。

[適用モデル]

vRX VMware ESXi 版

30.4.2 PP アカウントのクリア

[書式]

```
clear account pp [peer_num]
```

[設定値及び初期値]

- *peer_num*
 - [設定値]:
 - 相手先情報番号
 - 省略時は現在選択している相手先
 - [初期値]:-

[説明]

指定した PP インタフェースに関するアカウントをクリアする。

[適用モデル]

vRX VMware ESXi 版

30.4.3 TUNNEL アカウントのクリア

[書式]

```
clear account tunnel [tunnel_num]
```

[設定値及び初期値]

- *tunnel_num*
 - [設定値]:
 - 相手先情報番号
 - 省略時、選択されている相手について表示する
 - [初期値]:-

[説明]

指定したデータコネクタ接続設定がされているトンネルインタフェースに関するアカウントをクリアする。

[適用モデル]

vRX VMware ESXi 版

30.4.4 データコネクタのアカウントのクリア

[書式]

```
clear account ngn data
```

[説明]

データコネクタのアカウントをクリアする。

[適用モデル]

vRX VMware ESXi 版

30.4.5 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.4.6 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.4.7 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。

[適用モデル]

vRX VMware ESXi 版

30.4.8 ログのクリア

[書式]

clear log [saved]

[設定値及び初期値]

- saved
 - [設定値]: リポ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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.4.9 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.4.10 インタフェースのカウンター情報のクリア

[書式]

clear status *interface***clear status pp *peer_num*****clear status tunnel *tunnel_num***

[設定値及び初期値]

- *interface*

- [設定値]: LAN インタフェース名、ブリッジインタフェース名
- [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -

[説明]

指定したインタフェースのカウンター情報をクリアする。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.4.11 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.4.12 インタフェースの NAT アドレステーブルのクリア**[書式]**

```
clear nat descriptor interface dynamic interface
clear nat descriptor interface dynamic pp [peer_num]
clear nat descriptor interface dynamic tunnel [tunnel_num]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]:
 - 相手先情報番号
 - anonymous
 - 省略時は現在選択している相手先
 - [初期値]: -
- *tunnel_num*
 - [設定値]:
 - トンネルインタフェース番号
 - 省略時は現在選択されているトンネルインタフェース
 - [初期値]: -

[説明]

インタフェースに適用されている NAT アドレステーブルをクリアする。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.4.13 IP マスカレードで管理しているセッションの統計情報のクリア

[書式]

clear nat descriptor masquerade session statistics [*nat_descriptor*]

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]:
 - NAT ディスクリプタ番号 (1..2147483647)
 - *nat_descriptor* 省略時はすべての NAT ディスクリプタについて統計情報のクリアを行う。
 - [初期値]: -

[説明]

IP マスカレードで管理しているセッションの統計情報をクリアする。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.4.14 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.4.15 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.4.16 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.5 ファイル、ディレクトリの操作

30.5.1 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。

path には **mount** コマンドでマウントした外部ストレージを指定できる。外部ストレージのパスは、マウント時に設定したプレフィックスを先頭に付与して指定する。例えば、プレフィックスが "storage:" である外部ストレージの "/" *dir* を指定する場合は、"storage:/dir" と指定する。マウントされている外部ストレージは **show status storage interface** コマンドで確認できる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.5.2 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。

path には **mount** コマンドでマウントした外部ストレージを指定できる。外部ストレージのパスは、マウント時に設定したプレフィックスを先頭に付与して指定する。例えば、プレフィックスが "storage:" である外部ストレージの "/" *dir* を指定する場合は、"storage:/dir" と指定する。マウントされている外部ストレージは **show status storage interface** コマンドで確認できる。

[ノート]

path に相対パスで "config" を指定した場合、本コマンドではなく、**delete config** 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.5.3 ファイルまたはディレクトリの複製

[書式]

copy from to

[設定値及び初期値]

- *from*
 - [設定値]: コピー元のファイル名またはディレクトリ名
 - [初期値]: -
- *to*
 - [設定値]: コピー先のファイル名またはディレクトリ名
 - [初期値]: -

[説明]

ファイルまたはディレクトリを複製する。*from* がディレクトリの場合は、配下のすべてのファイルとディレクトリが再帰的に複製される。

from と *to* は、それぞれ相対パスまたは絶対パスで指定する。

from がファイルの場合の動作は以下の通りとなる。

to と同名のファイルが存在する場合は *to* のデータが *from* のデータで上書きされる。

to と同名のディレクトリが存在する場合は、そのディレクトリの配下に *from* と同名のファイルが作成される。

to と同名のファイルやディレクトリが存在しない場合には *to* が作成される。

from がディレクトリの場合の動作は以下の通りとなる。

to と同名のファイルが存在する場合は複製を実行できない。

to と同名のディレクトリが存在する場合は、そのディレクトリの配下に *from* と同名のディレクトリが作成される。

to と同名のファイルやディレクトリが存在しない場合には *to* が作成される。

from、*to* に相対パスを指定した場合、環境変数 PWD を基点としたパスと解釈される。PWD は **set** コマンドで変更可能であり、初期値は "/" である。

from、*to* には **mount** コマンドでマウントした外部ストレージを指定できる。外部ストレージのパスは、マウント時に設定したプレフィックスを先頭に付与して指定する。例えば、プレフィックスが "storage:" である外部ストレージの "/dir" を指定する場合は、"storage:/dir" と指定する。マウントされている外部ストレージは **show status storage interface** コマンドで確認できる。

[ノート]

from に相対パスで "config" を指定した場合、本コマンドではなく、**copy config** コマンドが実行される。このような場合には相対パスを使用せず、絶対パスでファイルまたはディレクトリを指定する。

本コマンドでは、必要に応じた親ディレクトリ作成が行われないため、*to* のパス中に存在しないディレクトリが含まれているとエラーになる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.5.4 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。

path には **mount** コマンドでマウントした外部ストレージを指定できる。外部ストレージのパスは、マウント時に設定したプレフィックスを先頭に付与して指定する。例えば、プレフィックスが "storage:" である外部ストレージの "/dir" を指定する場合は、"storage:/dir" と指定する。マウントされている外部ストレージは **show status storage interface** コマンドで確認できる。

[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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.6 外部ストレージの操作

30.6.1 外部ストレージをマウントする

[書式]

```
mount nfs_if [prefix]
mount smb_if username=username password=password [prefix]
```

[設定値及び初期値]

- *nfs_if*
 - [設定値]: NFS の接続先
 - [初期値]: -
- *smb_if*
 - [設定値]: SMB の接続先
 - [初期値]: -
- *username*
 - [設定値]: SMB のユーザー名
 - [初期値]: -
- *password*

- [設定値]: SMB のパスワード
- [初期値]: -
- *prefix*
 - [設定値]: ヤマハルーターのコマンドでパスの先頭に付与するプレフィックス (半角 1 文字以上、20 文字以下)
 - [初期値]: -

[説明]

外部ストレージ (NFS、または SMB) をマウントする。

外部ストレージを NFS でマウントする場合は、第 1 書式で指定する。*nfs_if* は以下のフォーマットで指定する。

- `nfs://<SERVER>/<PATH>`
 - <SERVER> ... 外部ストレージの IPV4 アドレス
 - <PATH> ... 外部ストレージのパス

外部ストレージを SMB でマウントする場合は、第 2 書式で指定する。*smb_if* は以下のフォーマットで指定する。

- `smb://<SERVER>/<PATH>`
 - <SERVER> ... 外部ストレージの IPV4 アドレス
 - <PATH> ... 外部ストレージのパス

ヤマハルーターのコマンドで、マウントした外部ストレージにアクセスする場合は、*prefix* に指定したプレフィックスを先頭に付与したパスを指定する。例えば、*prefix* に "server:" を指定したとき、**show file list** コマンドで外部ストレージの /temp ディレクトリの内容を表示する場合は以下のように入力する。

```
# show file list server:/temp
```

prefix に使用できる文字は、半角英数字、ハイフン (-)、アンダースコア (_)、ピリオド (.) である。

prefix に指定した文字列の末尾には、自動的にコロン (:) が付与される。

prefix を省略した場合は、自動的にプレフィックスが決定される。外部ストレージごとのプレフィックスは、**show status storage interface** コマンドで確認することができる。

外部ストレージは最大で 10 個までマウントできる。

[設定例]

外部ストレージ (192.168.100.100) の /share ディレクトリを NFS でマウント、プレフィックスに server: を指定する

```
# mount nfs://192.168.100.100/share server:
```

外部ストレージ (10.10.10.10) の /example ディレクトリを SMB (ユーザー名: user、パスワード: pass) でマウント、プレフィックスは自動で設定する

```
# mount smb://10.10.10.10/example username=user password=pass
```

上記でマウントした外部ストレージのプレフィックスを確認する

```
# show status storage interface
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.6.2 外部ストレージをアンマウントする**[書式]**

```
unmount prefix
```

[設定値及び初期値]

- *prefix*
 - [設定値]: 外部ストレージをマウントしたときに指定したプレフィックス
 - [初期値]: -

[説明]

外部ストレージ (NFS、または SMB) をアンマウントする。

prefix は **mount** コマンドで外部ストレージをマウントしたときに設定したプレフィックスを指定する。

外部ストレージごとのプレフィックスは、**show status storage interface** コマンドで確認することができる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.7 その他の操作

30.7.1 相手先の使用許可の設定

[書式]

```
pp enable peer_num [peer_num ...]
no pp enable peer_num
```

[設定値及び初期値]

- *peer_num*
- [設定値]:

設定値	説明
番号	相手先情報番号
番号 1-番号 2	番号 1 から番号 2 までの相手先情報番号
番号 1-	番号 1 以上のすべての相手先情報番号
-番号 1	番号 1 以下のすべての相手先情報番号
anonymous	anonymous インターフェース
all	すべての相手先情報番号

- [初期値]:-

[説明]

相手先を使用できる状態にする。工場出荷時、すべての相手先は **disable** 状態なので、使用する場合は必ずこのコマンドで **enable** 状態にしなければならない。
複数指定した場合には、その全てで使用できる状態になる。

[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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.7.2 相手先の使用不許可の設定

[書式]

```
pp disable peer_num [peer_num ...]
```

[設定値及び初期値]

- *peer_num*
- [設定値]:

設定値	説明
番号	相手先情報番号
番号 1-番号 2	番号 1 から番号 2 までの相手先情報番号
番号 1-	番号 1 以上のすべての相手先情報番号
-番号 1	番号 1 以下のすべての相手先情報番号
anonymous	anonymous インターフェース
all	すべての相手先情報番号

- [初期値]:-

[説明]

相手先を使用できない状態にする。

相手先の設定を行う場合は `disable` 状態であることが望ましい。
複数指定した場合には、その全てで使用できない状態になる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.7.3 再起動

[書式]

```
restart [config]
```

[設定値及び初期値]

- *config*
 - [設定値]: 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。
config は、デフォルト設定ファイルに設定される。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.7.4 電源オフ

[書式]

```
shutdown
```

[説明]

ルーターの電源を切る。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.7.5 インタフェースの再起動

[書式]

```
interface reset interface [interface ...]
```

[設定値及び初期値]

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

[説明]

指定したインタフェースを再起動する。
LAN インタフェースでは、オートネゴシエーションする設定になっていればオートネゴシエーション手順が起動される

[ノート]

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

`pp bind` コマンド、経路情報などすべての設定を整えた後に実行する。対象とするインタフェースがバインドされているすべての相手先情報番号の通信を停止した状態で、また回線種別を変更する場合には回線を抜いた状態で実行すること。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.7.6 発信

[書式]

```
connect peer_num  
connect pp peer_num
```


connect tunnel *tunnel_num*

[設定値及び初期値]

- *peer_num*
 - [設定値]: 発信相手の相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: NGN 網を介したトンネル番号または L2TPv3 トンネル番号
 - [初期値]: -

[説明]

手動で発信する。

[ノート]

connect tunnel コマンドは、データコネクトを使用した拠点間接続以外のトンネルには使用できない。データコネクト接続機能を実装していないモデルでは、**connect pp** コマンドは使用できない。データコネクト接続機能と L2TPv3 機能を実装していないモデルでは、**connect tunnel** コマンドは使用できない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.7.7 切断

[書式]

disconnect *peer_num*

disconnect pp *peer_num*

disconnect tunnel *tunnel_num*

[設定値及び初期値]

- *peer_num*
 - [設定値]:

設定値	説明
番号	切断する相手先情報番号
all	すべての相手先情報番号
anonymous	anonymous のすべて
anonymous1 ..	指定した anonymous

- [初期値]: -
- *tunnel_num*
 - [設定値]: NGN 網を介したトンネル番号または L2TPv3 トンネル番号
 - [初期値]: -

[説明]

手動で切断する。

[ノート]

disconnect tunnel コマンドは、データコネクトを使用した拠点間接続以外のトンネルには使用できない。データコネクト接続機能を実装していないモデルでは、**disconnect pp** コマンドは使用できない。データコネクト接続機能と L2TPv3 機能を実装していないモデルでは、**disconnect tunnel** コマンドは使用できない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.7.8 ping

[書式]

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

[設定値及び初期値]

- *datalen*: データ長 (1..65535)
 - [初期値]: 64
- *count*

- [設定値]: 実行回数 (1..21474836)
- [初期値]: Ctrl-C キーが入力されるまで繰り返す
- *ip_address*
 - [設定値]: 始点 IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))
 - [初期値]: ルーターのインタフェースに付与されたアドレスの中から選択する
- *wait*: パケット送信間隔秒数 (0.1 .. 3600.0)
 - [初期値]: 1
- *host*
 - [設定値]:
 - ping をかけるホストの IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))
 - ping をかけるホストの名称
 - [初期値]: -

[説明]

ICMP Echo を指定したホストに送出し、ICMP Echo Reply が送られてくるのを待つ。送られてきたら、その旨表示する。コマンドが終了すると簡単な統計情報を表示する。

count パラメータを省略すると、Ctrl-C キーを入力するまで実行を継続する。

-w オプションを指定した時には、次のパケットを送信するまでの間に相手からの返事を確認できなかった時にはその旨のメッセージを表示する。-w オプションを指定していない時には、パケットが受信できなくても何もメッセージを表示しない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.7.9 ping6 の実行

[書式]

```
ping6 [-s datalen] [-c count] [-sa ipv6_address] [-w wait] destination
ping6 [-s datalen] [-c count] [-sa ipv6_address] [-w wait] destination%scope_id
ping6 [-s datalen] [-c count] [-sa ipv6_address] [-w wait] destination interface
ping6 [-s datalen] [-c count] [-sa ipv6_address] [-w wait] destination pp peer_num
ping6 [-s datalen] [-c count] [-sa ipv6_address] [-w wait] destination tunnel tunnel_num
ping6 destination [count]
ping6 destination%scope_id [count]
ping6 destination interface [count]
ping6 destination pp peer_num [count]
ping6 destination tunnel tunnel_num [count]
```

[設定値及び初期値]

- *datalen*
 - [設定値]: データ長 (1..65535 バイト)
 - [初期値]: 64
- *count*
 - [設定値]: 実行回数 (1..21474836)
 - [初期値]: Ctrl-C キーが入力されるまで繰り返す
- *ipv6_address*
 - [設定値]: 始点 IPv6 アドレス
 - [初期値]: ルーターのインタフェースに付与されたアドレスの中から選択する
- *wait*: パケット送信間隔秒数 (0.1 .. 3600.0)
 - [初期値]: 1
- *destination*
 - [設定値]: 送信する宛先の IPv6 アドレス、または名前
 - [初期値]: -
- *scope_id*
 - [設定値]: スコープ識別子
 - [初期値]: -
- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *peer_num*

- [設定値]: 相手先情報番号
- [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -

[説明]

指定した宛先に対して ICMPv6 Echo Request を送信する。

スコープ識別子には LAN インタフェース名または LOOPBACK インタフェース名を指定する。

count パラメータを省略すると、Ctrl-C キーを入力するまで実行を継続する。

-w オプションを指定した時には、次のパケットを送信するまでの間に相手からの返事を確認できなかった時にはその旨のメッセージを表示する。-w オプションを指定していない時には、パケットが受信できなくても何もメッセージを表示しない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.7.10 traceroute

[書式]

```
traceroute host [noresolv] [-sa source]
```

[設定値及び初期値]

- *host*
 - [設定値]:
 - traceroute をかけるホストの IP アドレス (xxx.xxx.xxx.xxx)
 - traceroute をかけるホストの名称
 - [初期値]: -
- *noresolv*: DNS による解決を行わないことを示すキーワード
 - [初期値]: -
- *source*
 - [設定値]: 始点 IP アドレス
 - [初期値]: -

[説明]

指定したホストまでの経路を調べて表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.7.11 traceroute6 の実行

[書式]

```
traceroute6 destination [noresolv] [-sa source]
```

[設定値及び初期値]

- *destination*
 - [設定値]: 送信する宛先の IPv6 アドレス、または名前
 - [初期値]: -
- *noresolv*
 - [設定値]: DNS による解決を行わないことを示すキーワード
 - [初期値]: -
- *source*
 - [設定値]: 始点 IPv6 アドレス
 - [初期値]: -

[説明]

指定した宛先までの経路を調べて表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.7.12 nslookup

[書式]

nslookup *host*

[設定値及び初期値]

- *host*
 - [設定値]:
 - IP アドレス
 - IPv6 アドレス
 - ホスト名
 - [初期値]: -

[説明]

DNS による名前解決を行う。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.7.13 IPv4 動的フィルタの接続管理情報の削除

[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]: チャンネルの識別子
 - [初期値]: -

[説明]

指定したセッションに属する特定のチャンネルを削除する。チャンネルを指定しないときには、そのセッションに属するすべてのチャンネルを削除する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.7.14 TELNET クライアント

[書式]

telnet *host* [*port* [*mode* [*negotiation* [*abort*]]]]

[設定値及び初期値]

- *host*
 - [設定値]: TELNET をかける相手の IP アドレス、ホスト名、または NGN 網電話番号
 - [初期値]: -
- *port*: 使用するポート番号
 - [設定値]:
 - 十進数
 - ポート番号のニーモニック
 - 省略時は 23 (TELNET)
 - [初期値]: 23
- *mode*: TELNET 通信 (送信) の動作モード
 - [設定値]:

設定値	説明
character	文字単位で通信する
line	行単位で通信する
auto	<i>port</i> パラメータの設定値により character/line を選択

設定値	説明
省略	省略時は auto

- [初期値]: auto
- *negotiation*: TELNET オプションのネゴシエーションの選択
- [設定値]:

設定値	説明
on	ネゴシエーションする
off	ネゴシエーションしない
auto	<i>port</i> パラメータの設定値により on/off を選択
省略	省略時は auto

- [初期値]: auto
- *abort*: TELNET クライアントを強制的に終了させるためのアボートキー
- [設定値]:
 - 十進数の ASCII コード
 - 省略時は 29(^)
- [初期値]: 29

[説明]

TELNET クライアントを実行する。

[ノート]

ホスト名による接続は A レコード (IPv4) のみ対応している。

character モードは、通常の TELNET サーバーなどへの接続のための透過的な通信を行う。

line モードは、入力行を編集して行単位の通信を行う。行編集の終了は、改行コード (CR:0x0d または LF:0x0a) の入力で判断する。

ポート番号による機能自動選択について

1. TELNET 通信の動作モードの自動選択

port 番号が 23 の場合は文字単位モードとなり、そうでない場合は行単位モードとなる。

2. TELNET オプションのネゴシエーションの自動選択

port 番号が 23 の場合はネゴシエーションし、そうでない場合はネゴシエーションしない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.7.15 IPv6 動的フィルタのコネクション管理情報の削除

[書式]

```
disconnect ipv6 connection session_id [channel_id]
```

[設定値及び初期値]

- *session_id*
 - [設定値]: セッションの識別子
 - [初期値]: -
- *channel_id*
 - [設定値]: チャンネルの識別子
 - [初期値]: -

[説明]

指定したセッションに属する特定のチャンネルを削除する。チャンネルを指定しないときには、そのセッションに属するすべてのチャンネルを削除する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.7.16 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 インタフェース名
 - [初期値]: -
- *mac_address*
 - [設定値]: MAC アドレス
 - [初期値]: -
- *ip_address*
 - [設定値]: IPv4 アドレス
 - [初期値]: -
- *port*
 - [設定値]: UDP ポート番号
 - [初期値]: -
- *type*
 - [設定値]: イーサネットタイプフィールドの値 (1501..65535)
 - [初期値]: -

[説明]

指定した LAN インタフェースに Magic Packet を送信する。

第 1 書式では、IPv4 UDP パケットとして UDP ペイロードに Magic Packet データシーケンスを格納したパケットを送信する。終点 IP アドレスと、終点 UDP ポート番号を指定できるが、省略した場合には、終点 IP アドレスとしてはインタフェースのディレクティッドブロードキャストアドレスが、終点ポート番号には 9(discard) が使われる。また、終点 IP アドレスを指定した場合にはユニキャストでパケットを送信する。その場合、通常のルーティングや ARP の手順は踏まず、終点 MAC アドレスはコマンドで指定したものになる。終点 IP アドレスを省略した場合にはブロードキャストでパケットを送信する。

第 2 書式では、Ethernet ヘッダの直後から Magic Packet のデータシーケンスが始まるパケットを送信する。

どちらの形式でも、-i、-c オプションで Magic Packet の送信間隔および回数を指定できる。パケットの送信中でも、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 インタフェース以外には Magic Packet を送信できない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.7.17 メール通知の実行

[書式]

mail notify status exec *id*

[設定値及び初期値]

- *id*
 - [設定値]: 設定番号 (1..10)
 - [初期値]: -

[説明]

状態情報をメールで送信する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.7.18 設定の一括更新

[書式]

```
load [config-type] config [difference] [silent | interactive] [no-configure-refresh] [no-key-generate] [rollback-timer=timer]
```

[設定値及び初期値]

- *config-type* : 引数 *config* の種類を表す
 - [設定値] :

設定値	説明
config	config 番号
file	EMFS に保存されているファイルのファイル名

- [初期値] :-
- *config*
 - [設定値] : config 番号、またはファイル名
 - [初期値] :-
- *timer*
 - [設定値] : 復元タイマーの値 (120..21474836)
 - [初期値] :-

[説明]

指定された設定ファイルへ設定を復元・更新する。

config-type を省略した書き方をした場合、*config* は以下の順で解釈される。

- 保存されている config 番号に一致する場合はその設定
- 存在するファイル名と一致する場合はそのファイル

更新方法には、置換と差分の 2 種類がある。

- 置換 : 現在の設定内容をいったんすべて消去し、設定ファイルの設定内容に置き換える。
- 差分 : 現在の設定内容を設定ファイルの設定内容に変更する、最小限のコマンドを実行する。

デフォルト動作は置換更新であり、*difference* オプションを指定することで差分更新となる。

デフォルトでは、設定を置き換えるために実行するコマンドがコンソールに表示される。*silent* オプションを指定すると、コマンドの表示はせずに設定を書き換える。*interactive* オプションを指定すると、コマンドを一つずつ実行するかどうか確認しながら設定を更新できる。*interactive* オプションは、対話的ではないインターフェースからは利用できない。*silent* オプションと *interactive* オプションを同時に指定することはできない。

load コマンドで設定を置き換えた場合、必要に応じて '**ospf configure refresh**'、'**bgp configure refresh**' あるいは '**ipv6 ospf configure refresh**' コマンドが追加で実行される。*no-configure-refresh* オプションを指定すると、この動作を抑止することができる。

更新前後の設定ファイルに **sshd host key generate** コマンドが設定されていた場合、*no-key-generate* オプションを指定するとホスト鍵の再生成は実行されず、更新前のホスト鍵の設定を引き継ぐことができる。

rollback-timer オプションで復元タイマーが設定できる。以下の場合に、自動的に設定が **load** コマンド実行前の内容に復元される。

- 復元タイマーがタイムアウトした。
- ログインタイマーがタイムアウトした。

復元タイマーを停止するには以下のいずれかの操作が必要である。

- **confirm** コマンドを実行する。
- **save** コマンドで設定を不揮発性メモリーに保存する。
- **quit**、または **exit** コマンドでログアウトする。
- **restart** コマンドで機器を再起動する。
- *rollback-timer* オプション無しの **load** コマンドを実行する。

一つのコンソールあたり、復元タイマーは一つしか動作しない。*rollback-timer* オプション付きの **load** コマンドあるいは **rollback timer** コマンドを複数回実行した場合には、最後のコマンドの復元タイマーのみが有効となる。

rollback-timer オプションを省略した場合には、復元タイマーは動作しない。

[ノート]

暗号化された設定ファイルには対応していない。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.7.19 ロールバックタイマーの起動

[書式]

rollback timer timer

[設定値及び初期値]

- *timer*
 - [設定値]: 復元タイマーの値 (秒、1.21474836)
 - [初期値]: -

[説明]

復元タイマーのみを設定する。以下の場合に、自動的に設定が **rollback timer** コマンド実行前の内容に復元される。

- 復元タイマーがタイムアウトした。
- ログインタイマーがタイムアウトした。

以下の場合に、復元タイマーは停止する。

- **confirm** コマンドを実行する。
- **save** コマンドで設定を不揮発性メモリーに保存する。
- **quit**、または **exit** コマンドでログアウトする。
- **restart** コマンドで機器を再起動する。
- rollback-timer オプション無しの **load** コマンドを実行する。

一つのコンソールあたり、復元タイマーは一つしか動作しない。rollback-timer オプション付きの **load** コマンドあるいは **rollback timer** コマンドを複数回実行した場合には、最後のコマンドの復元タイマーのみが有効となる。

[ノート]

このコマンドは、手動で設定を変更するときのセーフネットとして利用することができる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.7.20 設定の確認

[書式]

confirm

[説明]

load コマンドあるいは **rollback timer** コマンドで起動した復元タイマーを停止し、設定変更の内容を確定させる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.7.21 ファイルをマクロとして実行する

[書式]

call [-v] [-x] *filename* [*parameter..*]

[設定値及び初期値]

- *filename*
 - [設定値]: ファイル名
 - [初期値]: -
- *parameter*
 - [設定値]: マクロ引数
 - [初期値]: -

[説明]

filename で指定したファイルをマクロとして実行する。

マクロには引数を渡すことができる。引数が、NAME=VALUE の形をしている場合、マクロ内では変数 NAME として VALUE を参照できる。他の形の引数は位置引数として、指定された順番に、\$1、\$2 等でアクセスできる。\$0 はファイル名、\$* はすべての位置引数を空白で結合した文字列となる。引数はすべてマクロ内でのみ利用可能な変数である。

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

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

30.7.22 echo

[書式]

echo [*string*]

[設定値及び初期値]

- *string*
 - [設定値]: 表示したい文字列
 - [初期値]: -

[説明]

指定された文字列を表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

第 31 章

設定の表示

31.1 機器設定の表示

[書式]

show environment [detail]

[設定値及び初期値]

- detail
 - [設定値]: 全体の平均 CPU 使用率に加えて、各コア毎の CPU 使用率を表示する
 - [初期値]: -

[説明]

以下の項目が表示される。

- システムのリビジョン
- CPU、メモリの使用量 (%)
- パケットバッファの使用量 (%)
- 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設定ファイル

detail オプションを省略した場合は全体の平均 CPU 使用率が表示され、detail オプションを指定した場合は全体の平均 CPU 使用率に加え、各コア毎の CPU 使用率が表示される。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

31.2 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。
ファイルを指定した場合には、ログインパスワードと管理パスワードを問い合わせられる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

31.3 指定した PP の設定内容の表示

[書式]

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

[設定値及び初期値]

- *peer_num*
 - [設定値]:
 - 相手先情報番号
 - anonymous
 - 省略時、選択されている相手について表示する

- [初期値]:-

[説明]

show config、**less config** コマンドの表示の中から、指定した相手先情報番号に関するものだけを表示する。

相手先情報番号の間にハイフン (-) を挟んで範囲指定すると、指定した範囲の相手先情報番号に関するものを表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

31.4 指定したトンネルの設定内容の表示

[書式]

```
show config tunnel [tunnel_num] [expand]
```

```
show config tunnel [tunnel_num-tunnel_num] [expand]
```

```
less config tunnel [tunnel_num] [expand]
```

```
less config tunnel [tunnel_num-tunnel_num] [expand]
```

[設定値及び初期値]

- *tunnel_num*
 - [設定値]:
 - トンネル番号
 - 省略時は、選択されているトンネルについて表示する
 - [初期値]:-

[説明]

show config、**less config** コマンドの表示の中から、指定したトンネル番号に関するものだけを表示する。

トンネル番号の間にハイフン (-) を挟んで範囲指定すると、指定した範囲のトンネル番号に関するものを表示する。

expand キーワードを指定すると、**tunnel template** コマンドにて指定したトンネルテンプレートが適用された後の、実際にルーターの動作時に参照される設定を表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

31.5 設定の差分の表示

[書式]

```
show config difference [[config-type1] config1] [config-type2] config2
```

[設定値及び初期値]

- *config-type1/2*: 引数 *config1*, *config2* の種類を表す
 - [設定値]:

設定値	説明
config	config 番号
file	EMFS に保存されているファイルのファイル名

- [初期値]:-
- *config1/2*
 - [設定値]: '!' (現在動作中の設定)、config 番号、またはファイル名のいずれか
 - [初期値]:-

[説明]

config1 と *config2* の差分を、*config1* を *config2* へ変換するためのコマンド列という形で表示する。

config1 にあり、*config2* にないコマンドは **no** 形式で表示され、*config1* になく、*config2* にあるコマンドは通常形式で表示される。*config1*、*config2* とともに、**show config** コマンドでの表示に沿った形でインデント (段付け) されていないことはない。

config1 を省略した場合は、'!' (現在動作中の設定) が指定されたものとする。

config-type1/2 を省略した場合、*config1/2* は以下の順で解釈される。

- 保存されている config 番号に一致する場合は、その設定
- 存在するファイル名と一致する場合は、そのファイル

[ノート]

`config1/2` に `config` 番号を指定した場合で、保存されている設定に **login password**、**login password encrypted**、**administrator password**、**administrator password encrypted** コマンドが含まれている場合には、動作前にそれらのパスワードを入力する必要がある。

このコマンドは、管理者モードでのみ動作する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

31.6 設定ファイルの一覧

[書式]

show config list

less config list

[説明]

設定ファイルのファイル名、日時、コメントの一覧を表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

31.7 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	config 一覧
絶対パスまたは相対パス	ユーザ領域および外部ストレージ

- [初期値] : -
- `all` : 配下の全ディレクトリを対象にする
 - [初期値] : -
- `file-only` : ファイル名のみを表示する
 - [初期値] : -

[説明]

指定した場所に格納されているファイル情報の一覧を表示する。`location` に指定可能なパラメータは、以下の通りとなる。

設定値	説明
internal	config 一覧
絶対パスまたは相対パス	ユーザ領域および外部ストレージ

`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。

`location` には `mount` コマンドでマウントした外部ストレージを指定できる。外部ストレージのパスは、マウント時に設定したプレフィックスを先頭に付与して指定する。例えば、プレフィックスが `"storage:"` である外部ストレージの `"/dir"` を指定する場合は、`"storage:/dir"` と指定する。マウントされている外部ストレージは `show status storage interface` コマンドで確認できる。

[ノート]

`location` に絶対パスまたは相対パスを指定した場合のみ、`all` と `file-only` を使用できる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

31.8 インタフェースに付与されている IPv6 アドレスの表示

[書式]

```
show ipv6 address [interface]
show ipv6 address pp [peer_num]
show ipv6 address tunnel [tunnel_num]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名、LOOPBACK インタフェース名、NULL インタフェース
 - [初期値]: -
- *peer_num*
 - [設定値]:
 - 相手先情報番号
 - anonymous
 - 省略時、選択されている相手について表示する
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -

[説明]

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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

31.9 指定したインタフェースのフィルタ内容の表示

[書式]

```
show ip secure filter interface [dir]
show ip secure filter pp [peer_num] [dir]
show ip secure filter tunnel [tunnel_num] [dir]
```

[設定値及び初期値]

- *interface*
 - [設定値]: フィルタの適用されたインタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -
- *dir*
 - [設定値]: フィルタの適用された方向、'in' または 'out'
 - [初期値]: -

[説明]

指定したインタフェースに適用されているフィルタ定義の内容を表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

31.10 指定したインターフェースの IPv6 フィルター内容の表示

[書式]

```
show ipv6 secure filter interface [dir]
show ipv6 secure filter pp [peer_num] [dir]
show ipv6 secure filter tunnel [tunnel_num] [dir]
```

[設定値及び初期値]

- *interface*
 - [設定値]: フィルターの適用されたインターフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインターフェース番号
 - [初期値]: -
- *dir*
 - [設定値]: フィルターの適用された方向、'in' または 'out'
 - [初期値]: -

[説明]

指定したインターフェースに適用されている IPv6 フィルター定義の内容を表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

31.11 環境変数の表示

[書式]

show set [*name*]

[設定値及び初期値]

- *name*
 - [設定値]: 環境変数名
 - [初期値]: -

[説明]

指定した環境変数の値を表示する。

name を省略した場合には、設定されている環境変数をすべて表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

31.12 エイリアスの表示

[書式]

show alias [*name*]

[設定値及び初期値]

- *name*
 - [設定値]: エイリアス名
 - [初期値]: -

[説明]

指定したエイリアスの値を表示する。

name を省略した場合には、設定されているエイリアスをすべて表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

31.13 マクロの表示

[書式]

show macro [*name*]

[設定値及び初期値]

- *name*
 - [設定値]: マクロ名
 - [初期値]: -

[説明]

指定したマクロの値を表示する。

name を省略した場合には、設定されているマクロをすべて表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

第 32 章

状態の表示

32.1 ARP テーブルの表示

[書式]

```
show arp [interface]
```

[設定値及び初期値]

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

[説明]

ARP テーブルを表示する。インタフェース名を指定した場合、そのインタフェース経由で得られた ARP テーブル情報だけを表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.2 インタフェースの状態の表示

[書式]

```
show status interface
```

[設定値及び初期値]

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

[説明]

インタフェースの状態を表示する。

[ノート]

ブリッジインタフェースは vRX VMware ESXi 版で指定可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.3 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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.4 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 [detail]
```

[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、さらに *detail* を指定した時は隠されている経路も表示する
 - [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。さらに *detail* を指定した時は、隠されている経路についても経路数の合計を表示する。

[ノート]

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

プロトコル	メトリック値
RIP	メトリック値
OSPF	内部/外部経路の別、コスト値、メトリック値 (外部経路のみ) Type 1 の外部経路の場合、コスト値はメトリック値を含んだ経路へのコスト値となる。 Type 2 の外部経路の場合、コスト値は ASBR へのコスト値となる。
BGP	無し

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.5 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.6 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.7 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.8 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.9 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。

[適用モデル]

vRX VMware ESXi 版

32.10 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・ゲートウェイの識別子
 - 省略時はすべてのセキュリティ・ゲートウェイの SA のサマリを表示する。
 - [初期値]: -
- detail: SA の詳細な情報を表示する。
 - [初期値]: -

[説明]

IPsec の SA の状態を表示する。
id で与えられた識別子を持つ SA の情報を表示する。

[ノート]

該当の SA の生成時に XAUTH 認証を行った場合、認証に使用したユーザ名

- RADIUS 認証を行ったか否か
- 通知した内部 IP アドレス
- 追加した経路情報
- 適用したフィルタの情報

を同時に表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.11 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]:
- [初期値]: -

設定値	説明
1..8	証明書ファイルの識別子

[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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.12 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]:

設定値	説明
1..8	CRL ファイルの識別子

- [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

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.13 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 インタフェース名
 - [初期値]:-
- `vrid`
 - [設定値]: VRRP グループ ID(1..255)
 - [初期値]:-

[説明]

VRRP の情報を表示する。

[適用モデル]

vRX VMware ESXi 版

32.14 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 マスカレードのエントリが大量に存在する場合は、*detail* オプションを指定すると全エントリの表示に時間がかかり通信に影響を及ぼすことがあるため、IP マスカレードで使用中のポートの個数またはセッション数を確認したいときは、*detail* オプションを指定しないようにするか、**show nat descriptor masquerade port summary** コマンド、または **show nat descriptor masquerade session summary** コマンドを使うことを推奨する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.15 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 インタフェース名
 - [初期値]: -

[説明]

NAT ディスクリプタと適用インタフェースのリストを表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.16 LAN インタフェースの NAT ディスクリプタのアドレスマップの表示

[書式]

```
show nat descriptor interface address interface
show nat descriptor interface address pp peer_num
show nat descriptor interface address tunnel tunnel_num
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -

[説明]

インタフェースに適用されている NAT ディスクリプタのアドレスマップを表示する。

[ノート]

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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.17 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。

[ノート]

nat descriptor backward-compatibility コマンドで、*type* パラメータを 2 に設定した場合は本コマンドは使用できない。

代わりに、**show nat descriptor masquerade session summary** コマンドで、管理しているセッション数を表示することができる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.18 IP マスカレードで使用しているセッション数の表示

[書式]

```
show nat descriptor masquerade session [nat_descriptor] summary
```

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]:
 - NAT ディスクリプタ番号 (1..2147483647)
 - *nat_descriptor* 省略時はすべての NAT ディスクリプタについて表示する。
 - [初期値]: -

[説明]

IP マスカレードで管理しているセッション数およびセッション数のピーク値を表示する。セッション数のピーク値は NAT ディスクリプタの設定変更やルーターの再起動によってクリアされ、**clear nat descriptor dynamic** コマンドによるセッションの削除ではクリアされない。

[ノート]

本コマンドは、**nat descriptor backward-compatibility** コマンドで、*type* パラメータを 2 に設定した場合のみ使用可能である。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.19 IP マスカレードで管理しているセッションの統計情報の表示

[書式]

```
show nat descriptor masquerade session statistics [nat_descriptor]
```

[設定値及び初期値]

- *nat_descriptor*
 - [設定値]:
 - NAT ディスクリプター番号 (1..2147483647)
 - *nat_descriptor* 省略時はすべての NAT ディスクリプターについて表示する。
 - [初期値]: -

[説明]

IP マスカレードで管理しているセッションの統計情報として始点 IP アドレスで識別されるホスト毎にセッション数、ピーク値、制限された回数と時刻を表示する。セッション数の制限値は、**nat descriptor masquerade session limit** コマンドの設定値に従う。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.20 L2TP の状態の表示

[書式]

```
show status l2tp [tunnel tunnel_num]
```

[設定値及び初期値]

- *tunnel_num*
 - [設定値]: トンネル番号
 - [初期値]: -

[説明]

L2TP の状態を表示します。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.21 IPIP トンネリングの状態の表示

[書式]

```
show status ipip [tunnel tunnel_num]
```

[設定値及び初期値]

- *tunnel_num*
 - [設定値]: トンネル番号
 - [初期値]: -

[説明]

IPIP トンネリングの状態を表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.22 OSPF 情報の表示

[書式]

```
show status ospf info
```

[設定値及び初期値]

- *info*: 表示する情報の種類
 - [設定値]:

設定値	説明
database	OSPF のデータベース
neighbor	近隣ルーター
interface	各インタフェースの状態
virtual-link	バーチャルリンクの状態

- [初期値]: -

[説明]

OSPF の各種情報を表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.23 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** などを受け入れられた経路だけを表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.24 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)

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.25 DHCP クライアントの状態の表示

[書式]**show status dhcpc****[説明]**

DHCP クライアントの状態を表示する。

- クライアントの状態
 - インタフェース
 - IP アドレス (取得できないときはその状態)
 - DHCP サーバー
 - リース残時間
 - クライアント ID
 - ホスト名 (設定時)
- 共通情報
 - DNS サーバー
 - ゲートウェイ

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.26 DHCPv6 の状態の表示

[書式]**show status ipv6 dhcp****[説明]**

DHCPv6 に関する状態を表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.27 バックアップ状態の表示

[書式]**show status backup****[説明]**

バックアップ設定されたインタフェースについて、バックアップの状態を表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.28 動的フィルタによって管理されている接続の表示

[書式]

```

show ip connection [interface [direction] [ip_address]]
show ip connection pp [peer_num [direction] [ip_address]]
show ip connection tunnel [tunnel_num [direction] [ip_address]]
show ip connection summary
show ip connection detail [interface [direction]]
show ip connection detail pp [peer_num [direction]]
show ip connection detail tunnel [tunnel_num [direction]]

```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -
- *direction*

- [設定値]:

設定値	説明
in	入力方向
out	出力方向

- [初期値]: -
- *ip_address*
 - [設定値]: IP アドレス xxx.xxx.xxx.xxx(xxx は十進数)
 - [初期値]: -
- *summary*: インタフェース/方向単位の管理コネクション数、および全体の合計を表示する
 - [初期値]: -
- *detail*: 動的フィルタによって管理されているすべてのコネクションを表示する
 - [初期値]: -

[説明]

指定したインタフェースについて、動的なフィルタによって管理されているコネクションを表示する。インタフェースを指定しないときには、すべてのインタフェースの情報を表示する。

detail を指定しない場合は管理されているコネクションを送信元 IP アドレスごとに集約して表示する。ただし、*ip_address* が指定された場合には *detail* を指定した場合の情報のうちソースアドレスが *ip_address* に一致するものを表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.29 IPv6 の動的フィルタによって管理されているコネクションの表示

[書式]

```
show ipv6 connection
show ipv6 connection interface [direction] [ipv6_address]
show ipv6 connection pp [peer_num [direction] [ipv6_address]]
show ipv6 connection tunnel [tunnel_num [direction] [ipv6_address]]
show ipv6 connection summary
show ipv6 connection detail [interface [direction]]
show ipv6 connection detail pp [peer_num [direction]]
show ipv6 connection detail tunnel [tunnel_num [direction]]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *peer_num*
 - [設定値]: 相手先情報番号
 - [初期値]: -
- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -
- *direction*
 - [設定値]:

設定値	説明
in	入力方向
out	出力方向

- [初期値]: -
- *ipv6_address*
 - [設定値]: IPv6 アドレス部分
 - [初期値]: -
- *summary*: インタフェース/方向単位の管理コネクション数、および全体の合計を表示する
 - [初期値]: -

- detail : 動的フィルタによって管理されているすべてのコネクションを表示する
 - [初期値] :-

[説明]

指定したインタフェースについて、動的なフィルタによって管理されているコネクションを表示する。インタフェースを指定しないときには、すべてのインタフェースの情報を表示する。

detail を指定しない場合は管理されているコネクションを送信元 IP アドレスごとに集約して表示する。ただし、*ipv6_address* が指定された場合には detail を指定した場合の情報のうちソースアドレスが *ipv6_address* に一致するものを表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.30 ネットワーク監視機能の状態の表示

[書式]

```
show status ip keepalive
```

[説明]

ネットワーク監視機能の状態を表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.31 侵入情報の履歴の表示

[書式]

```
show ip intrusion detection
show ip intrusion detection interface [direction]
show ip intrusion detection pp [peer_num [direction]]
show ip intrusion detection tunnel [tunnel_num [direction]]
```

[設定値及び初期値]

- *interface*
 - [設定値] : LAN インタフェース名
 - [初期値] :-
- *peer_num*
 - [設定値] : 相手先情報番号
 - [初期値] :-
- *tunnel_num*
 - [設定値] : トンネルインタフェース番号
 - [初期値] :-
- *direction*
 - [設定値] :

設定値	説明
in	入力方向
out	出力方向

- [初期値] :-

[説明]

最近の侵入情報を表示する。侵入情報は各インタフェースの各方向ごとに表示され、表示される最大件数は、**ip interface intrusion detection report** コマンドで設定した件数となる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.32 トンネルインタフェースの状態の表示

[書式]

```
show status tunnel [tunnel_num]
show status tunnel [state]
show status tunnel [name=name]
```

[設定値及び初期値]

- *tunnel_num*
 - [設定値]: トンネルインタフェース番号
 - [初期値]: -
- *state*: 接続状態
 - [設定値]:

設定値	説明
up	接続されているトンネルインタフェース一覧を表示する
down	接続されていないトンネルインタフェース一覧を表示する

- [初期値]: -
- *name*
 - [設定値]: 接続相手の名前
 - [初期値]: -

[説明]

トンネルインタフェースの状態を表示する。

L2TP/IPsec 機能では、L2TP トンネルは IPsec トンネルの状態に応じて接続状態が判定される。

第 3 書式では、マルチポイントトンネルインタフェースで接続している相手の中から *name* に指定した文字列を含む名前が付与されている接続相手の情報を抽出して表示する。なお、接続相手の名前は相手側の **tunnel multipoint local name** コマンドで設定する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.33 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.34 ルーターにマウントされている外部ストレージの一覧を表示する

[書式]

show status storage interface [detail]

[設定値及び初期値]

- *detail*
 - [設定値]: すべての情報を表示する
 - [初期値]: -

[説明]

ルーターに接続されている外部ストレージ (NFS、または SMB) の一覧を表示する。表示する情報は以下のとおり。

情報	説明
INTERFACE	外部ストレージの接続先

情報	説明
FILESYSTEM	外部ストレージのファイルシステム
PREFIX	ヤマハルーターのコマンドで、パスの先頭に付与するプレフィックス

文字数の多い項目は省略される。

detail オプションを付与すると、すべての情報を表示する。

[表示例]

```
# show status storage interface
INTERFACE          FILESYSTEM PREFIX
-----
192.168.100.100:/share    nfs      server:
//10.10.10.10/example    cifs     smb001:
```

```
# show status storage interface detail
INTERFACE: 192.168.100.100:/share
FILESYSTEM: nfs
PREFIX: server:
-----
INTERFACE: //10.10.10.10/example
FILESYSTEM: cifs
PREFIX: smb001:
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.35 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
(*: current user, +: administrator mode, @: authenticated via RADIUS)
username      connection login time idle   IP address
-----
user-local    ssh1      09/16 10:21 0:02:08
*+@user-radius1 telnet1 09/16 10:22 0:00:00 192.168.0.100
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.36 ログインしたユーザーのログイン履歴の表示

[書式]**show status user history****[説明]**

ルーターにログインしたユーザーのログイン履歴を最大で 50 件まで表示する。以下の項目が表示される。

- ユーザー名
- 接続種別
- ログインした日時
- アイドル時間
- 接続相手の IP アドレス

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.37 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
- 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

[表示例]

```
# show status packet-buffer large
large group: 2048 bytes length
parameters: max-buffer=40000
39491 buffers in free list
509 buffers are allocated, req/succ/fail/rel = 22992/22992/0/22483
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.38 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

設定値	説明
length	キューイングしているパケット数
dcc	Dynamic Class Control の制御状況
all	すべての情報

- [初期値]: -
- *interface*
 - [設定値]: LAN インタフェース名 (省略時、全ての LAN インタフェースについて表示する)
 - [初期値]: -
- *class*
 - [設定値]: クラス (1..100)
 - [初期値]: -

[説明]

インタフェースに対して、QoS の設定情報や各クラスの使用状況を表示する。

- LAN インタフェース名
- キューイングアルゴリズム
- インタフェース速度
- クラス数
- 各クラスの設定帯域、使用帯域、使用帯域のピーク値と記録日時
- 設定帯域の合計
- 各クラスのエンキュー成功回数/失敗回数、デキュー回数、保持しているパケット数、パケット数のピーク値と記録日時
- Dynamic Class Control により制御されているホストの情報と制御内容

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.39 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)

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.40 技術情報の表示

[書式]

```
show techinfo
```

[説明]

技術サポートに必要な情報を一度に出力する。

他の **show** コマンドとは異なり、**show techinfo** コマンドの出力は **console columns/lines** コマンドの設定を無視して一度に出力される。一画面ごとに出力が停止するページ動作は行わない。そのため、ターミナルソフトのログ機能を用いて、出力を PC のファイルとして保存することが望ましい。

また、**console character** コマンドの設定も無視され、常に英語モードで出力される。

一画面ごとに内容を確認しながら出力したいときには、以下のように **less** コマンドを併用するとよい。ただし、**less** コマンドは画面制御シーケンスを多数出力するため、ログを記録しながら **less** コマンドを使用すると、ログファイルがわかりにくくなる。

```
show techinfo | less
```

[ノート]

ルーターに対して PC で動作する TFTP クライアントからアクセスし、ファイル名 'techinfo' を GET すると、**show techinfo** コマンドの出力と同じものが得られる。

Windows の TFTP.EXE を使用した例：

```
C:\>tftp 192.168.0.1 get techinfo techinfo.txt
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.41 起動情報を表示する

[書式]

```
show status boot [num]
```

[設定値及び初期値]

- *num* : 履歴番号
- [設定値] :

設定値	説明
0..4	指定した番号の履歴を表示する
省略	省略時は 0

- [初期値] : -

[説明]

起動の情報を表示する。

show status boot list コマンドで表示される履歴番号を指定すると、その履歴の詳細が表示される。
num を省略した場合は、履歴番号=0 の履歴が表示される。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.42 起動情報の履歴の詳細を表示する

[書式]

```
show status boot all
```

[説明]

起動情報の履歴の詳細を最大で 5 件まで表示する。

cold start コマンド、**clear boot list** コマンドを実行すると、この履歴はクリアされる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.43 起動情報の履歴の一覧を表示する

[書式]

```
show status boot list
```

[説明]

起動情報の履歴を最大で 5 件まで表示する。

cold start コマンド、**clear boot list** コマンドを実行すると、この履歴はクリアされる。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.44 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。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.45 ライセンス情報の表示

[書式]

`show status license [vrx [all]]`

[設定値及び初期値]

- vrx
 - [設定値]: 仮想ルーターのソフトウェアライセンスの詳細な情報を表示
 - [初期値]: -
- all
 - [設定値]: 有効期限切れとなったライセンスを含めた詳細な情報を表示
 - [初期値]: -

[説明]

ライセンスの情報を表示する。表示する情報は以下のとおり。

項目	説明
品番	ライセンス製品の品番 仮想ルーターのソフトウェアライセンスでは基本ライセンスが「vRX-<速度制限>」で表記され、オプションライセンスがある場合は当該ライセンスの種類と機能制限が併記される 仮想ルーターのソフトウェアライセンスの正式な品番は vrx オプションを付与することで確認可能
状態	ライセンスの状態 仮想ルーターのソフトウェアライセンスでは常に「有効」と表記される
有効期限	ライセンスの有効期限

vrx オプションを付与すると、仮想ルーターのソフトウェアライセンスの詳細な情報を表示する。all オプションを付与すると、有効期限切れとなったライセンスを含めた詳細な情報を表示する。表示する情報は以下のとおり。

項目	説明
ユーザー ID	ライセンスと紐づくユーザーの ID
インスタンス ID	ライセンスと紐づくインスタンスの ID
基本ライセンス	ルーターにインポートされている基本ライセンスの内訳 現在有効になっているライセンスの先頭にアスタリスク (*) が付与される
オプションライセンス	ルーターにインポートされているオプションライセンスの内訳

[表示例]

```
# show status license
```

```
=====
品番          状態          有効期限
-----
vRX-10G      有効          2020/11/30
VPN (対地数:3000)
```

```
# show status license vrx
```

```
ユーザー ID:      vrx_user
インスタンス ID:  12345678
基本ライセンス:
```

```
=====
品番          速度          有効期限
```

```
-----
*vRX-1Y10G      10G   2019/11/01 - 2020/11/30
オプションライセンス:
vRX-VPN1K x 3
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.46 CPU スケジューリング (パケット転送) 機能の状態の表示**[書式]****show status packet-scheduling****[説明]**

現在の CPU スケジューリング (パケット転送) 機能の状態を表示する。

- CPU スケジューリング方式
 - 動作中の CPU スケジューリング方式

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

- CPU 使用率
 - CPU コアごとの CPU コア全体の使用率
- フロー (IPv4/IPv6)
 - 全体の IPv4/IPv6 フロー数
 - CPU コアごとの IPv4/IPv6 フロー数
- 受信パケット
 - CPU コアごとの受信パケット数

CPU スケジューリング方式がロードバランス方式である場合、CPU コアごとの IPv4/IPv6 フロー数は表示されない。受信パケット数は、**system packet-scheduling** コマンドを実行するとクリアされる。

[表示例]

```
# show status packet-scheduling
CPU スケジューリング方式:      hash
CPU 使用率:
  CPU0:      57%(5sec) 56%(1min) 56%(5min)
  CPU1:      62%(5sec) 62%(1min) 62%(5min)
  CPU2:      88%(5sec) 89%(1min) 88%(5min)
  CPU3:      54%(5sec) 54%(1min) 54%(5min)
フロー(IPv4/IPv6):      2 エントリ / 2 エントリ
  CPU0:      0 エントリ / 1 エントリ
  CPU1:      1 エントリ / 0 エントリ
  CPU2:      1 エントリ / 0 エントリ
  CPU3:      0 エントリ / 1 エントリ
受信パケット:
  CPU0:      23155524 パケット
  CPU1:      14018842 パケット
  CPU2:      23624407 パケット
  CPU3:      22886347 パケット
```

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.47 サードパーティー製ソフトウェアの著作権情報を表示**[書式]****show copyright** [detail [*software*]]**show copyright** [detail [*license* [*version*]]]

[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]: -
- *software*
 - [設定値]: 表示対象とするソフトウェア名
 - [初期値]: -
- *license*
 - [設定値]: ライセンス条文表示するライセンス名
 - [初期値]: -
- *version*
 - [設定値]: ライセンスのバージョン番号
 - [初期値]: -

[説明]

搭載されているサードパーティー製ソフトウェアの著作権情報を表示する。

detail を指定するとライセンス条文を合わせて表示する。

一部ソフトウェアの著作権情報およびライセンス条文を表示するには *software* を指定する必要がある。対象のソフトウェア名は **show copyright detail** を実行すると表示される。

license を指定することで、ライセンスの条文を表示することができる。*version* は *license* パラメータで指定したライセンスのバージョンを指定することができる。

[ノート]

サードパーティー製ソフトウェアに適用される一般的なライセンスの条文は **show copyright common-license** または第2書式で確認できる。

第2書式は vRX Amazon EC2 版 Rev.19.00.01 のみで使用可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

32.48 サードパーティー製ソフトウェアに適用される一般的なライセンスの条文を表示

[書式]

show copyright common-license [*license*]

[設定値及び初期値]

- *license*
 - [設定値]:

設定値	説明
agpl-3.0-only	GNU Affero General Public License v3.0 only を表示する
apache-2.0	Apache License 2.0 を表示する
artistic-1.0-perl	Artistic License 1.0 (Perl) を表示する
cc-by-sa-3.0	Creative Commons Attribution Share Alike 3.0 Unported を表示する
cc0-1.0	Creative Commons Zero v1.0 Universal を表示する
gfdl-1.2-no-invariants-or-later	GNU Free Documentation License v1.2 or later - no invariants を表示する
gfdl-1.2-only	GNU Free Documentation License v1.2 only を表示する
gfdl-1.3-no-invariants-or-later	GNU Free Documentation License v1.3 or later - no invariants を表示する
gfdl-1.3-or-later	GNU Free Documentation License v1.3 or later を表示する
gpl-1.0-only	GNU General Public License v1.0 only を表示する
gpl-1.0-or-later	GNU General Public License v1.0 or later を表示する

設定値	説明
gpl-2.0-only	GNU General Public License v2.0 only を表示する
gpl-2.0-or-later	GNU General Public License v2.0 or later を表示する
gpl-3.0-only	GNU General Public License v3.0 only を表示する
gpl-3.0-or-later	GNU General Public License v3.0 or later を表示する
lgpl-2.0-only	GNU Library General Public License v2 only を表示する
lgpl-2.0-or-later	GNU Library General Public License v2 or later を表示する
lgpl-2.1-only	GNU Lesser General Public License v2.1 only を表示する
lgpl-2.1-or-later	GNU Lesser General Public License v2.1 or later を表示する
lgpl-3.0-only	GNU Lesser General Public License v3.0 only を表示する
lgpl-3.0-or-later	GNU Lesser General Public License v3.0 or later を表示する
oldap-2.8	Open LDAP Public License v2.8 を表示する
psf-2.0	Python Software Foundation License 2.0 を表示する
sisssl	Sun Industry Standards Source License v1.1 を表示する

- [初期値] :-

[説明]

サードパーティー製ソフトウェアに適用される一般的なライセンスの条文を表示する。

[ノート]

ソフトウェア別のライセンス条文は **show copyright** で確認できる。

vRX Amazon EC2 版は Rev.19.00.07 以降で使用可能。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

第 33 章

ログイン

33.1 ログの表示

[書式]

```
show log [saved] [reverse]
show log file [backup [fileid]]
less log [saved] [reverse]
```

[設定値及び初期値]

- saved
 - [設定値]: リポート直前のログを表示する
 - [初期値]: -
- reverse
 - [設定値]: ログを逆順に表示する
 - [初期値]: -
- file
 - [設定値]: /yamaha_sys ディレクトリ内の 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: ファイルの中身を表示させたい SYSLOG バックアップファイルのファイル名に付加されている日時データを指定する
 - [設定値]: yyyyymmdd_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 20,000 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。

意図しないリポートが発生したときは、'saved' を指定することでリポート直前のログを表示することができる。

このコマンドでは、通常は発生時刻の古いものからログを順に表示するが、'reverse' を指定することで新しいものから表示させることができる。

file を指定した場合は、/yamaha_sys ディレクトリ内の SYSLOG ファイルを表示する。

file backup を指定した場合は、SYSLOG 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は、表示されたファイル名の日時データ (yyyyymmdd_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]

clear log コマンドを実行するとログは消去される。

file を指定した場合は以下の制限がある。

- /yamaha_sys ディレクトリ内の暗号化した SYSLOG ファイルは表示できない

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

33.2 アカウントの表示

[書式]

```
show account
```

[説明]

以下の項目を表示

- 発信回数
- 着信回数

- 課金料金の総計

[ノート]

電源 OFF や再起動により、それまでの課金情報がクリアされる。

[適用モデル]

vRX VMware ESXi 版

33.3 PP アカウントの表示

[書式]

```
show account pp [peer_num]
```

[設定値及び初期値]

- *peer_num*
 - [設定値]:
 - 相手先情報番号
 - anonymous
 - 省略時、選択されている相手について表示する
 - [初期値]:-

[説明]

指定した PP インタフェースに関するアカウントを表示する。

[適用モデル]

vRX VMware ESXi 版

33.4 TUNNEL アカウントの表示

[書式]

```
show account tunnel [tunnel_num]
```

[設定値及び初期値]

- *tunnel_num*
 - [設定値]:
 - 相手先情報番号
 - 省略時、選択されている相手について表示する
 - [初期値]:-

[説明]

指定したデータコネクタ接続設定がされているトンネルインタフェースについて発着信回数や料金情報を表示する。発着回数、着信回数は切断時にカウントされる。料金情報は再起動によりクリアされる。**account threshold** コマンドで設定される閾値を超えたか否かの計算には、データコネクタ分の料金は含まれない。

[適用モデル]

vRX VMware ESXi 版

33.5 データコネクタのアカウントの表示

[書式]

```
show account ngn data
```

[説明]

データコネクタの発着信回数や課金情報を表示する。

[ノート]

課金情報は接続時間と設定した帯域幅から計算しているため、最終的に請求される料金とは異なる場合がある。

[適用モデル]

vRX VMware ESXi 版

33.6 コマンド履歴の表示

[書式]

```
show command history [num]
```

[設定値及び初期値]

- *num*
 - [設定値]: ヒストリー番号 (1..21474836)
 - [初期値]: -

[説明]

コマンドヒストリーを表示する。

num を指定した場合は、指定した番号のコマンドから直前のコマンドまで表示する。*num* を省略した場合には、新しいものからさかのぼって最大 20 個のコマンドを表示する。

[適用モデル]

vRX Amazon EC2 版, vRX VMware ESXi 版

索引

記号

> [34](#)
>> [34](#)

A

administrator [357](#)
 administrator password [36](#)
 administrator password encrypted [36](#)
 administrator radius auth [38](#)
 alias [73](#)
 auth user [195](#)
 auth user attribute [196](#)
 auth user group [197](#)
 auth user group attribute [197](#)

B

bgp aggregate [297](#)
 bgp aggregate filter [297](#)
 bgp autonomous-system [298](#)
 bgp configure refresh [302](#)
 bgp default med [305](#)
 bgp export [299](#)
 bgp export aspath [299](#)
 bgp export filter [300](#)
 bgp force-to-advertise [304](#)
 bgp import [301](#)
 bgp import filter [302](#)
 bgp log [304](#)
 bgp neighbor [303](#)
 bgp preference [299](#)
 bgp reric interval [305](#)
 bgp router id [298](#)
 bgp use [297](#)
 bridge learning [351](#)
 bridge learning bridge_interface static [352](#)
 bridge learning bridge_interface timer [351](#)
 bridge member [350](#)

C

call [376](#)
 clear account [360](#)
 clear account ngn data [360](#)
 clear account pp [360](#)
 clear account tunnel [360](#)
 clear arp [360](#)
 clear boot list [363](#)
 clear bridge learning [361](#)
 clear dns cache [361](#)
 clear heartbeat2 [347](#)
 clear heartbeat2 id [347](#)
 clear heartbeat2 name [347](#)
 clear ip dynamic routing [361](#)
 clear ip traffic list [121](#)
 clear ip traffic list pp [121](#)
 clear ip traffic list tunnel [121](#)
 clear ipv6 dynamic routing [363](#)
 clear ipv6 neighbor cache [363](#)
 clear log [361](#)

clear nat descriptor dynamic [362](#)
 clear nat descriptor interface dynamic [362](#)
 clear nat descriptor interface dynamic pp [362](#)
 clear nat descriptor interface dynamic tunnel [362](#)
 clear nat descriptor masquerade session statistics [363](#)
 clear status [361](#)
 clear vrx license [40](#)
 cold start [359](#)
 confirm [376](#)
 connect [368](#)
 connect pp [368](#)
 connect tunnel [368](#)
 console character [47](#)
 console columns [47](#)
 console info [48](#)
 console lines [47](#)
 console prompt [46](#)
 copy [364](#)
 copy config [357](#)

D

date [44](#)
 delete [364](#)
 delete config [358](#)
 description [60](#)
 dhcp client client-identifier [159](#)
 dhcp client client-identifier pool [159](#)
 dhcp client client-identifier pp [159](#)
 dhcp client hostname [158](#)
 dhcp client hostname pool [158](#)
 dhcp client hostname pp [158](#)
 dhcp client option [160](#)
 dhcp client option pool [160](#)
 dhcp client option pp [160](#)
 dhcp client release linkdown [161](#)
 dhcp convert lease to bind [153](#)
 dhcp duplicate check [149](#)
 dhcp manual lease [155](#)
 dhcp manual release [155](#)
 dhcp relay select [156](#)
 dhcp relay server [156](#)
 dhcp relay srcport [156](#)
 dhcp relay threshold [157](#)
 dhcp scope [149](#)
 dhcp scope bind [150](#)
 dhcp scope lease type [152](#)
 dhcp scope option [154](#)
 dhcp server rfc2131 compliant [148](#)
 dhcp service [147](#)
 disconnect [369](#)
 disconnect ip connection [372](#)
 disconnect ipv6 connection [373](#)
 disconnect pp [369](#)
 disconnect tunnel [369](#)
 disconnect user [42](#)
 dns cache max entry [273](#)
 dns cache use [272](#)
 dns domain [265](#)
 dns host [272](#)
 dns notice order [267](#)
 dns private address spoof [267](#)

dns server 264
 dns server dhcp 266
 dns server pp 265
 dns server select 268
 dns service 264
 dns service aaaa filter 268
 dns service fallback 273
 dns sreport 271
 dns static 270
 dns syslog resolv 268

E

echo 377
 embedded file 74
 ethernet filter 125
 ethernet interface filter 126
 exit 357
 export vrx license file 40

G

grep 32

H

heartbeat pre-shared-key 340
 heartbeat receive 340
 heartbeat send 341
 heartbeat2 myname 342
 heartbeat2 receive 344
 heartbeat2 receive enable 345
 heartbeat2 receive log 345
 heartbeat2 receive monitor 345
 heartbeat2 receive record limit 346
 heartbeat2 transmit 342
 heartbeat2 transmit enable 343
 heartbeat2 transmit interval 343
 heartbeat2 transmit log 344
 help 35

I

import sshd authorized-keys 67
 import vrx license 39
 interface reset 368
 ip arp timer 96
 ip filter 83
 ip filter directed-broadcast 87
 ip filter dynamic 87
 ip filter dynamic timer 88
 ip filter fqdn timer 89
 ip filter set 86
 ip filter source-route 86
 ip flow limit 99
 ip flow timer 98
 ip forward filter 123
 ip fragment remove df-bit 95
 ip host 270
 ip icmp echo-reply send 162
 ip icmp echo-reply send-only-linkup 162
 ip icmp error-decrypted-ipsec send 165
 ip icmp log 166
 ip icmp mask-reply send 162
 ip icmp parameter-problem send 163
 ip icmp redirect receive 163

ip icmp redirect send 163
 ip icmp time-exceeded send 164
 ip icmp timestamp-reply send 164
 ip icmp unreachable send 165
 ip implicit-route preference 98
 ip interface address 77
 ip interface arp log 98
 ip interface arp queue length 97
 ip interface arp static 97
 ip interface dhcp auto default-route-add 82
 ip interface dhcp auto interface-route-add 82
 ip interface dhcp lease time 158
 ip interface dhcp retry 159
 ip interface dhcp service 157
 ip interface forward filter 124
 ip interface intrusion detection 90
 ip interface intrusion detection notice-interval 91
 ip interface intrusion detection repeat-control 91
 ip interface intrusion detection report 92
 ip interface mtu 79
 ip interface nat descriptor 254
 ip interface ospf area 291
 ip interface ospf neighbor 294
 ip interface proxyarp 96
 ip interface proxyarp vrrp 96
 ip interface rebound 79
 ip interface rip auth key 107
 ip interface rip auth key text 107
 ip interface rip auth type 107
 ip interface rip filter 106
 ip interface rip force-to-advertise 111
 ip interface rip hop 106
 ip interface rip receive 105
 ip interface rip send 105
 ip interface rip trust gateway 104
 ip interface secondary address 78
 ip interface secure filter 93
 ip interface secure filter name 93
 ip interface tcp mss limit 92
 ip interface tcp window-scale 93
 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 60
 ip keepalive 119
 ip local forward filter 124
 ip pp address 77
 ip pp forward filter 124
 ip pp intrusion detection 90
 ip pp intrusion detection notice-interval 91
 ip pp intrusion detection repeat-control 91
 ip pp intrusion detection report 92
 ip pp mtu 79
 ip pp nat descriptor 254
 ip pp ospf area 291
 ip pp ospf neighbor 294
 ip pp rebound 79
 ip pp remote address 100
 ip pp remote address pool 100
 ip pp rip auth key 107
 ip pp rip auth key text 107
 ip pp rip auth type 107
 ip pp rip backup interface 110
 ip pp rip connect interval 109
 ip pp rip connect send 109

- ip pp rip disconnect interval 110
- ip pp rip disconnect send 110
- ip pp rip filter 106
- ip pp rip force-to-advertise 111
- ip pp rip hold routing 108
- ip pp rip hop 106
- ip pp rip receive 105
- ip pp rip send 105
- ip pp rip trust gateway 104
- ip pp secure filter 93
- ip pp secure filter name 93
- ip pp tcp mss limit 92
- ip pp tcp window-scale 93
- ip pp traffic list 121
- ip pp traffic list threshold 122
- ip reassembly hold-time 99
- ip route 80
- ip route change log 93
- ip routing 77
- ip routing process 56
- ip tos supersede 95
- ip tunnel address 173
- ip tunnel forward filter 124
- ip tunnel intrusion detection 90
- ip tunnel intrusion detection notice-interval 91
- ip tunnel intrusion detection repeat-control 91
- ip tunnel intrusion detection report 92
- ip tunnel mtu 79
- ip tunnel nat descriptor 254
- ip tunnel ospf area 291
- ip tunnel ospf neighbor 294
- ip tunnel rebound 79
- ip tunnel remote address 173
- ip tunnel rip auth key 107
- ip tunnel rip auth key text 107
- ip tunnel rip auth type 107
- ip tunnel rip filter 106
- ip tunnel rip force-to-advertise 111
- ip tunnel rip hop 106
- ip tunnel rip receive 105
- ip tunnel rip send 105
- ip tunnel rip trust gateway 104
- ip tunnel secure filter 93
- ip tunnel secure filter name 93
- ip tunnel tcp mss limit 92
- ip tunnel tcp window-scale 93
- ip tunnel traffic list 121
- ip tunnel traffic list threshold 122
- ipip keepalive log 224
- ipip keepalive use 224
- ipsec auto refresh 182
- ipsec ike always-on 183
- ipsec ike auth method 178
- ipsec ike backward-compatibility 194
- ipsec ike child-exchange type 204
- ipsec ike duration 205
- ipsec ike eap myname 180
- ipsec ike eap request 181
- ipsec ike eap send certreq 181
- ipsec ike encryption 190
- ipsec ike esp-encapsulation 202
- ipsec ike group 191
- ipsec ike hash 192
- ipsec ike keepalive log 189
- ipsec ike keepalive use 188
- ipsec ike license-key 200
- ipsec ike license-key use 201
- ipsec ike local address 187
- ipsec ike local id 187
- ipsec ike local name 186
- ipsec ike log 202
- ipsec ike message-id-control 203
- ipsec ike mode-cfg address 200
- ipsec ike mode-cfg address pool 199
- ipsec ike mode-cfg method 199
- ipsec ike nat-traversal 209
- ipsec ike negotiate-strictly 182
- ipsec ike negotiation receive 204
- ipsec ike payload type 193
- ipsec ike pfs 194
- ipsec ike pki file 180
- ipsec ike pre-shared-key 179
- ipsec ike proposal-limitation 203
- ipsec ike queue length 191
- ipsec ike remote address 185
- ipsec ike remote id 185
- ipsec ike remote name 184
- ipsec ike restrict-dangling-sa 208
- ipsec ike retry 183
- ipsec ike send info 194
- ipsec ike version 178
- ipsec ike xauth myname 195
- ipsec ike xauth request 198
- ipsec ipcomp type 212
- ipsec log illegal-spi 192
- ipsec refresh sa 208
- ipsec sa delete 210
- ipsec sa policy 206
- ipsec transport 215
- ipsec transport template 215
- ipsec tunnel 211
- ipsec tunnel fastpath-fragment-function follow df-bit 210
- ipsec tunnel outer df-bit 211
- ipsec use 177
- ipv6 filter 328
- ipv6 filter dynamic 330
- ipv6 icmp echo-reply send 166
- ipv6 icmp echo-reply send-only-linkup 166
- ipv6 icmp error-decrypted-ipsec send 169
- ipv6 icmp log 169
- ipv6 icmp packet-too-big send 169
- ipv6 icmp parameter-problem send 167
- ipv6 icmp redirect receive 167
- ipv6 icmp redirect send 167
- ipv6 icmp time-exceeded send 168
- ipv6 icmp unreachable send 168
- ipv6 interface address 310
- ipv6 interface dad retry count 315
- ipv6 interface dhcp service 314
- ipv6 interface icmp-nd queue length 309
- ipv6 interface mtu 307
- ipv6 interface neighbor cache max entry 310
- ipv6 interface prefix 312
- ipv6 interface prefix change log 314
- ipv6 interface rip filter 323
- ipv6 interface rip hop 322
- ipv6 interface rip receive 321
- ipv6 interface rip send 321
- ipv6 interface rip trust gateway 322
- ipv6 interface rtadv send 318
- ipv6 interface rtsol max-retransmit 319
- ipv6 interface secure filter 329

ipv6 interface tcp mss limit 307
 ipv6 interface tcp window-scale 308
 ipv6 interface vrrp 326
 ipv6 interface vrrp shutdown trigger 327
 ipv6 max auto address 315
 ipv6 nd ns-trigger-dad 331
 ipv6 pp address 310
 ipv6 pp dad retry count 315
 ipv6 pp dhcp service 314
 ipv6 pp mtu 307
 ipv6 pp prefix 312
 ipv6 pp prefix change log 314
 ipv6 pp rip connect interval 324
 ipv6 pp rip connect send 323
 ipv6 pp rip disconnect interval 325
 ipv6 pp rip disconnect send 324
 ipv6 pp rip filter 323
 ipv6 pp rip hold routing 325
 ipv6 pp rip hop 322
 ipv6 pp rip receive 321
 ipv6 pp rip send 321
 ipv6 pp rip trust gateway 322
 ipv6 pp rtadv send 318
 ipv6 pp rtsol max-retransmit 319
 ipv6 pp secure filter 329
 ipv6 pp tcp mss limit 307
 ipv6 pp tcp window-scale 308
 ipv6 prefix 316
 ipv6 reassembly hold-time 310
 ipv6 rh0 discard 309
 ipv6 rip preference 325
 ipv6 rip use 321
 ipv6 route 320
 ipv6 routing 307
 ipv6 routing process 309
 ipv6 source address selection rule 316
 ipv6 tunnel address 310
 ipv6 tunnel dhcp service 314
 ipv6 tunnel mtu 307
 ipv6 tunnel prefix 312
 ipv6 tunnel prefix change log 314
 ipv6 tunnel rip filter 323
 ipv6 tunnel rip receive 321
 ipv6 tunnel rip send 321
 ipv6 tunnel secure filter 329
 ipv6 tunnel tcp mss limit 307
 ipv6 tunnel tcp window-scale 308

L

l2tp always-on 221
 l2tp hostname 221
 l2tp keepalive log 220
 l2tp keepalive use 219
 l2tp local router-id 221
 l2tp remote end-id 222
 l2tp remote router-id 222
 l2tp service 218
 l2tp syslog 220
 l2tp tunnel auth 218
 l2tp tunnel disconnect time 219
 lan backup 116
 lan backup recovery time 117
 lan keepalive interval 118
 lan keepalive log 118
 lan keepalive use 117

lan linkup send-wait-time 57
 lan receive-buffer-size 58
 lan shutdown 57
 lan type 57
 less 33
 less config 378
 less config list 380
 less config pp 378
 less config tunnel 379
 less file list 380
 less log 405
 load 375
 login password 36
 login password encrypted 36
 login radius use 37
 login timer 59
 login user 37
 lua 353
 lua use 353
 luac 354

M

macro 73
 mail notify 335
 mail notify status exec 374
 mail server name 332
 mail server pop 333
 mail server smtp 332
 mail server timeout 334
 mail template 334
 make directory 363
 mount 365

N

nat descriptor address inner 256
 nat descriptor address outer 255
 nat descriptor backward-compatibility 254
 nat descriptor ftp port 260
 nat descriptor log 261
 nat descriptor masquerade incoming 259
 nat descriptor masquerade port range 260
 nat descriptor masquerade remove df-bit 262
 nat descriptor masquerade rlogin 257
 nat descriptor masquerade session limit 262
 nat descriptor masquerade session limit total 263
 nat descriptor masquerade static 258
 nat descriptor masquerade unconvertible port 261
 nat descriptor sip 261
 nat descriptor static 257
 nat descriptor timer 259
 nat descriptor type 255
 ngn radius account callee 235
 ngn radius account caller 234
 ngn radius auth password 234
 ngn renumbering link-refresh 235
 ngn type 231
 nslookup 372
 ntp backward-compatibility 46
 ntp local address 46
 ntpdate 45

O

ospf area 288

ospf area network [289](#)
ospf area stubhost [289](#)
ospf configure refresh [283](#)
ospf export filter [285](#)
ospf export from ospf [284](#)
ospf import filter [286](#)
ospf import from [284](#)
ospf log [295](#)
ospf merge equal cost stub [294](#)
ospf preference [283](#)
ospf reric interval [295](#)
ospf router id [284](#)
ospf use [283](#)
ospf virtual-link [290](#)

P

packetdump [53](#)
packetdump pp [53](#)
ping [369](#)
ping6 [370](#)
pki certificate file [216](#)
pki crl file [217](#)
pp always-on [130](#)
pp auth accept [128](#)
pp auth multi connect prohibit [130](#)
pp auth myname [129](#)
pp auth request [129](#)
pp auth username [128](#)
pp backup [115](#)
pp backup pp [115](#)
pp backup recovery time [116](#)
pp backup tunnel [115](#)
pp bind [222](#)
pp disable [367](#)
pp enable [367](#)
pp keepalive interval [101](#)
pp keepalive log [103](#)
pp keepalive use [102](#)
pp select [356](#)
ppp bacp maxconfigure [141](#)
ppp bacp maxfailure [141](#)
ppp bacp maxterminate [141](#)
ppp bacp restart [140](#)
ppp bap maxretry [142](#)
ppp bap restart [141](#)
ppp ccp maxconfigure [139](#)
ppp ccp maxfailure [140](#)
ppp ccp maxterminate [139](#)
ppp ccp restart [139](#)
ppp ccp type [138](#)
ppp chap maxchallenge [135](#)
ppp chap restart [134](#)
ppp ipcp ipaddress [135](#)
ppp ipcp maxconfigure [136](#)
ppp ipcp maxfailure [136](#)
ppp ipcp maxterminate [136](#)
ppp ipcp msxt [137](#)
ppp ipcp remote address check [137](#)
ppp ipcp restart [136](#)
ppp ipcp vjc [135](#)
ppp ipv6cp use [140](#)
ppp lcp acfc [131](#)
ppp lcp magicnumber [131](#)
ppp lcp maxconfigure [133](#)
ppp lcp maxfailure [133](#)

ppp lcp maxterminate [133](#)
ppp lcp mru [132](#)
ppp lcp pfc [132](#)
ppp lcp restart [132](#)
ppp lcp silent [133](#)
ppp msccp maxretry [138](#)
ppp msccp restart [138](#)
ppp pap maxauthreq [134](#)
ppp pap restart [134](#)
pppoe access concentrator [142](#)
pppoe auto connect [142](#)
pppoe auto disconnect [143](#)
pppoe disconnect time [144](#)
pppoe invalid-session forced close [145](#)
pppoe padi maxretry [143](#)
pppoe padi restart [143](#)
pppoe padr maxretry [144](#)
pppoe padr restart [144](#)
pppoe service-name [145](#)
pppoe tcp mss limit [145](#)
pppoe use [142](#)

Q

queue class filter [275](#)
queue interface class control [281](#)
queue interface class filter list [278](#)
queue interface class property [280](#)
queue interface default class [279](#)
queue interface length [279](#)
queue interface type [278](#)
queue pp class filter list [278](#)
queue pp default class [279](#)
queue pp length [279](#)
queue pp type [278](#)
queue tunnel class filter list [278](#)
queue tunnel default class [279](#)
quit [357](#)

R

radius account [250](#)
radius account port [252](#)
radius account server [251](#)
radius auth [250](#)
radius auth port [252](#)
radius auth server [251](#)
radius retry [253](#)
radius secret [252](#)
radius server [251](#)
rdate [45](#)
remote setup accept [359](#)
rename [365](#)
restart [368](#)
rip advertise mode [108](#)
rip filter rule [112](#)
rip preference [104](#)
rip timer [112](#)
rip use [103](#)
rollback timer [376](#)

S

save [357](#)
schedule at [338](#)
scp [69](#)

security class 43
 set 72
 set-default-config 359
 sftpd host 68
 show account 405
 show account ngn data 406
 show account pp 406
 show account tunnel 406
 show alias 382
 show arp 384
 show bridge learning 386
 show command 35
 show command history 406
 show config 378
 show config difference 379
 show config list 380
 show config pp 378
 show config tunnel 379
 show copyright 402
 show copyright common-license 403
 show dns cache 400
 show environment 378
 show file list 380
 show ip connection 393
 show ip connection pp 393
 show ip connection tunnel 393
 show ip intrusion detection 395
 show ip intrusion detection pp 395
 show ip intrusion detection tunnel 395
 show ip rip table 386
 show ip route 385
 show ip secure filter 381
 show ip secure filter pp 381
 show ip secure filter tunnel 381
 show ip traffic list 122
 show ip traffic list pp 122
 show ip traffic list tunnel 122
 show ipsec sa 387
 show ipsec sa gateway 387
 show ipv6 address 381
 show ipv6 address pp 381
 show ipv6 address tunnel 381
 show ipv6 connection 394
 show ipv6 connection pp 394
 show ipv6 connection tunnel 394
 show ipv6 neighbor cache 386
 show ipv6 rip table 386
 show ipv6 route 386
 show ipv6 secure filter 381
 show ipv6 secure filter pp 381
 show ipv6 secure filter tunnel 381
 show log 405
 show macro 382
 show nat descriptor address 388
 show nat descriptor interface address 389
 show nat descriptor interface address pp 389
 show nat descriptor interface address tunnel 389
 show nat descriptor interface bind 389
 show nat descriptor interface bind pp 389
 show nat descriptor interface bind tunnel 389
 show nat descriptor masquerade port summary 390
 show nat descriptor masquerade session statistics 390
 show nat descriptor masquerade session summary 390
 show pki certificate summary 387
 show pki crl 388
 show set 382
 show sshd authorized-keys 67
 show sshd host key 63
 show status 384
 show status backup 393
 show status bgp neighbor 391
 show status boot 400
 show status boot all 400
 show status boot list 400
 show status dhcp 392
 show status dhcpc 392
 show status ethernet filter 127
 show status heartbeat 399
 show status heartbeat2 346
 show status heartbeat2 id 346
 show status heartbeat2 name 346
 show status ip keepalive 395
 show status ipip 391
 show status ipv6 dhcp 393
 show status l2tp 391
 show status license 401
 show status lua 354
 show status mail service 396
 show status ngn 236
 show status ospf 391
 show status packet-buffer 398
 show status packet-scheduling 402
 show status pp 384
 show status qos 398
 show status storage interface 396
 show status tunnel 395
 show status user 397
 show status user history 397
 show status vrrp 388
 show techinfo 399
 shutdown 368
 sip 100rel 227
 sip arrive address check 229
 sip arrive ringing p-n-uatype 228
 sip arrive session timer method 229
 sip arrive session timer refresher 228
 sip ip protocol 227
 sip log 230
 sip outer address 230
 sip response code busy 230
 sip session timer 226
 sip use 226
 sip user agent 228
 snmp community read-only 238
 snmp community read-write 238
 snmp display ipcp force 249
 snmp host 237
 snmp local address 244
 snmp syscontact 244
 snmp syslocation 245
 snmp sysname 245
 snmp trap community 238
 snmp trap cpu threshold 246
 snmp trap delay-timer 247
 snmp trap enable snmp 246
 snmp trap host 238
 snmp trap memory threshold 247
 snmp trap send linkdown 247
 snmp trap send linkdown pp 247
 snmp trap send linkdown tunnel 247
 snmp yrifppdisplayatmib2 248
 snmp yrifunneldisplayatmib2 248

- snmpv2c community read-only [239](#)
- snmpv2c community read-write [240](#)
- snmpv2c host [239](#)
- snmpv2c trap community [240](#)
- snmpv2c trap host [240](#)
- snmpv3 context name [241](#)
- snmpv3 engine id [241](#)
- snmpv3 host [242](#)
- snmpv3 trap host [244](#)
- snmpv3 usm user [241](#)
- snmpv3 vacm access [243](#)
- snmpv3 vacm view [243](#)
- sntpd host [348](#)
- sntpd service [348](#)
- speed [275](#)
- ssh [69](#)
- ssh encrypt algorithm [70](#)
- ssh known hosts [71](#)
- sshd auth method [65](#)
- sshd authorized-keys filename [66](#)
- sshd client alive [64](#)
- sshd encrypt algorithm [64](#)
- sshd hide openssh version [65](#)
- sshd host [62](#)
- sshd host key generate [63](#)
- sshd listen [61](#)
- sshd service [61](#)
- sshd session [62](#)
- syslog debug [50](#)
- syslog execute command [52](#)
- syslog facility [48](#)
- syslog file [50](#)
- syslog host [48](#)
- syslog info [49](#)
- syslog local address [52](#)
- syslog mount-server_filename [51](#)
- syslog notice [49](#)
- syslog srcreport [52](#)
- system cpu threshold [55](#)
- system memory threshold [56](#)
- system packet-buffer [71](#)
- system packet-scheduling [75](#)

T

- telnet [372](#)
- telnetd host [54](#)
- telnetd listen [54](#)

- telnetd service [53](#)
- telnetd session [55](#)
- terminate lua [355](#)
- terminate lua file [355](#)
- tftp host [59](#)
- time [44](#)
- timezone [44](#)
- traceroute [371](#)
- traceroute6 [371](#)
- tunnel backup [212](#)
- tunnel backup pp [212](#)
- tunnel backup tunnel [212](#)
- tunnel disable [171](#)
- tunnel enable [171](#)
- tunnel encapsulation [172](#)
- tunnel endpoint address [174](#)
- tunnel endpoint local address [174](#)
- tunnel endpoint name [175](#)
- tunnel endpoint remote address [173](#)
- tunnel multipoint limit [176](#)
- tunnel multipoint local name [176](#)
- tunnel multipoint server [175](#)
- tunnel ngn arrive permit [232](#)
- tunnel ngn bandwidth [231](#)
- tunnel ngn call permit [232](#)
- tunnel ngn disconnect time [231](#)
- tunnel ngn fallback [233](#)
- tunnel ngn interface [233](#)
- tunnel ngn radius auth [234](#)
- tunnel select [356](#)
- tunnel template [213](#)
- tunnel type [172](#)

U

- unmount [366](#)
- user attribute [40](#)

V

- vrx license file directory [38](#)
- vrx license update schedule [39](#)
- vrx user [38](#)

W

- wins server [137](#)
- wol send [373](#)