

コマンドリファレンス

Rev.1.03.01

目次

序文：はじめに	11
第1章：コマンドリファレンスの見方	12
1.1 対応するプログラムのリビジョン	12
1.2 コマンドリファレンスの見方	12
1.3 インタフェース名について	12
1.4 no で始まるコマンドの入力形式について	12
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	13
1.6 工場出荷設定値について	13
第2章：コマンドの使い方	14
2.1 コンソールについて	14
2.1.1 コンソールによる設定手順	14
2.1.2 CONSOLE ポートからの設定	15
2.1.3 TELNET による設定	15
2.2 SSH サーバーについて	16
2.2.1 SSH サーバー機能の使用に当たっての注意事項	16
2.2.2 SSH サーバーの設定	16
2.3 TFTP について	16
2.3.1 TFTP による設定手順	16
2.3.2 設定ファイルの読み出し	17
2.3.3 設定ファイルの書き込み	17
2.4 コンソール使用時のキーボード操作について	17
2.5 「show」で始まるコマンド	18
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	18
2.5.2 show コマンドの表示内容を見やすくする	20
2.5.3 外部メモリへのリダイレクト機能	20
第3章：ヘルプ	22
3.1 コンソールに対する簡易説明の表示	22
3.2 コマンド一覧の表示	22
第4章：機器の設定	23
4.1 ログインパスワードの設定	23
4.2 ログインパスワードの暗号化保存	23
4.3 管理パスワードの設定	23
4.4 管理パスワードの暗号化保存	23
4.5 ログインユーザ名とログインパスワードの設定	23
4.6 ユーザーの属性を設定	24
4.7 他のユーザの接続の強制切断	26
4.8 セキュリティクラスの設定	26
4.9 タイムゾーンの設定	27
4.10 現在の日付けの設定	28
4.11 現在の時刻の設定	28
4.12 リモートホストによる時計の設定	28
4.13 NTP による時計の設定	28
4.14 NTP パケットを送信するときの始点 IP アドレスの設定	29
4.15 Stratum 0 の NTP サーバーとの時刻同期を許可する設定	29
4.16 コンソールのプロンプト表示の設定	29

4.17 コンソールの言語とコードの設定	30
4.18 コンソールの表示文字数の設定	30
4.19 コンソールの表示行数の設定	30
4.20 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	31
4.21 SYSLOG を受けるホストの IP アドレスの設定	31
4.22 SYSLOG ファシリティの設定	31
4.23 NOTICE タイプの SYSLOG を出力するか否かの設定	32
4.24 INFO タイプの SYSLOG 出力の設定	32
4.25 DEBUG タイプの SYSLOG を出力するか否かの設定	32
4.26 SYSLOG を送信する時の始点 IP アドレスの設定	33
4.27 SYSLOG パケットの始点ポート番号の設定	33
4.28 SYSLOG に実行コマンドを出力するか否かの設定	33
4.29 TELNET サーバー機能の ON/OFF の設定	33
4.30 TELNET サーバー機能の listen ポートの設定	34
4.31 TELNET サーバーへアクセスできるホストの設定	34
4.32 TELNET サーバーへ同時に接続できるユーザ数の設定	35
4.33 LAN インタフェースの動作設定	35
4.34 HUB IC での受信オーバーフロー数を取得するか否かの設定	35
4.35 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	36
4.36 LAN インタフェースの動作タイプの設定	36
4.37 ログインタイムの設定	38
4.38 TFTP によりアクセスできるホストの設定	38
4.39 インタフェースまたはシステムの説明の設定	39
4.40 TCP のコネクションレベルの syslog を出力するか否かの設定	39
4.41 HTTP リビジョンアップ実行を許可するか否かの設定	41
4.42 HTTP リビジョンアップ用 URL の設定	42
4.43 HTTP リビジョンアップ用 Proxy サーバーの設定	42
4.44 HTTP リビジョンアップ処理のタイムアウトの設定	42
4.45 リビジョンダウンを許可するか否かの設定	42
4.46 DOWNLOAD ボタンによるリビジョンアップ操作を許可するか否かの設定	43
4.47 リビジョンアップ実行のスケジュール	43
4.48 SSH サーバー機能の ON/OFF の設定	44
4.49 SSH サーバー機能の listen ポートの設定	44
4.50 SSH サーバーへアクセスできるホストの設定	45
4.51 SSH サーバーへ同時に接続できるユーザ数の設定	45
4.52 SSH サーバーホスト鍵の設定	45
4.53 SSH サーバーで利用可能な暗号アルゴリズムの設定	46
4.54 SSH クライアントの生存確認	46
4.55 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	47
4.56 SFTP サーバーへアクセスできるホストの設定	47
4.57 SSH クライアント	48
4.58 SCP クライアント	48
4.59 SSH クライアントで利用可能な暗号アルゴリズムの設定	49
4.60 SSH サーバーの公開鍵情報を保存するファイルの設定	50
4.61 パケットバッファのパラメータを変更する	50
4.62 有効になっているアラーム音を鳴らすか全く鳴らさないかの設定	51
4.63 USB ホスト機能に関連するアラーム音を鳴らすか否かの設定	51
4.64 microSD 機能に関連するアラームを鳴らすか否かの設定	51
4.65 バッチファイル実行機能に関連するアラーム音を鳴らすか否かの設定	52

4.66 起動時のアラーム音を鳴らすか否かの設定	52
4.67 HTTP リビジョンアップ機能に関連するアラームを鳴らすか否かの設定	52
4.68 環境変数の設定	53
4.69 監視情報を不揮発性メモリへ保存する	53
第 5 章 : ヤマハルーター用ファイルシステム RTFS	54
5.1 RTFS のフォーマット	54
5.2 RTFS のガベージコレクト	54
第 6 章 : 電話帳サーバー機能の設定	55
6.1 電話帳サーバードメイン名の設定	55
6.2 拠点情報の設定	55
6.3 連携する電話帳サーバーの設定	57
6.4 連携する電話帳サーバーが管理する番号の設定	57
6.5 冗長構成機能のための動作モードおよび冗長構成相手の設定	58
6.6 エラーレスポンスを転送するタイマーの設定	58
第 7 章 : IP の設定	60
7.1 インタフェース共通の設定	60
7.1.1 IP アドレスの設定	60
7.1.2 セカンダリ IP アドレスの設定	60
7.1.3 インタフェースの MTU の設定	61
7.1.4 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	61
7.1.5 echo,discard,time サービスを動作させるか否かの設定	62
7.1.6 IP の静的経路情報の設定	62
7.1.7 IP パケットのフィルタの設定	63
7.1.8 フィルタセットの定義	66
7.1.9 Source-route オプション付き IP パケットをフィルタアウトするか否かの設定	66
7.1.10 ディレクテッドブロードキャストパケットをフィルタアウトするか否かの設定	67
7.1.11 動的フィルタの定義	67
7.1.12 動的フィルタのタイムアウトの設定	68
7.1.13 侵入検知機能の動作の設定	69
7.1.14 1 秒間に侵入検知情報を通知する頻度の設定	70
7.1.15 重複する侵入検知情報の通知抑制の設定	70
7.1.16 侵入検知情報の最大表示件数の設定	71
7.1.17 TCP ウィンドウ・スケール・オプションを変更する	71
7.1.18 本機が端点となる TCP のセッション数の設定	71
7.1.19 IPv4 の経路情報に変化があった時にログに記録するか否かの設定	72
7.1.20 フィルタリングによるセキュリティの設定	72
7.1.21 ARP エントリの寿命の設定	73
7.1.22 静的 ARP エントリの設定	73
7.1.23 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	73
7.1.24 ARP エントリの変化をログに残すか否かの設定	74
7.2 RIP の設定	74
7.2.1 RIP を使用するか否かの設定	74
7.2.2 RIP に関して信用できるゲートウェイの設定	75
7.2.3 RIP パケットの受信に関する設定	75
7.2.4 RIP のフィルタリングの設定	75
7.2.5 RIP で加算するホップ数の設定	76
7.2.6 RIP2 での認証の設定	76
7.2.7 RIP2 での認証キーの設定	77

7.2.8 RIP で強制的に経路を広告する	77
7.2.9 RIP2 でのフィルタの比較方法	78
7.2.10 RIP のタイマーを調整する	78
7.3 VRRP の設定	79
7.3.1 インタフェース毎の VRRP の設定	79
7.3.2 シャットダウントリガの設定	80
7.4 バックアップの設定	80
7.4.1 ネットワーク監視機能の設定	80
第 8 章 : DHCP の設定	82
8.1 DHCP サーバー機能	82
8.1.1 DHCP の動作の設定	82
8.1.2 RFC2131 対応動作の設定	82
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	84
8.1.4 DHCP スコープの定義	84
8.1.5 DHCP 予約アドレスの設定	85
8.1.6 DHCP アドレス割り当て動作の設定	87
8.1.7 DHCP 割り当て情報を元にした予約設定の生成	87
8.1.8 DHCP オプションの設定	88
8.1.9 DHCP リース情報の手動追加	89
8.1.10 DHCP リース情報の手動削除	89
8.1.11 インタフェース毎の DHCP の動作の設定	90
第 9 章 : ICMP の設定	91
9.1 IPv4 の設定	91
9.1.1 ICMP Echo Reply を送信するか否かの設定	91
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	91
9.1.3 ICMP Parameter Problem を送信するか否かの設定	91
9.1.4 ICMP Time Exceeded を送信するか否かの設定	92
9.1.5 ICMP Timestamp Reply を送信するか否かの設定	92
9.1.6 ICMP Destination Unreachable を送信するか否かの設定	92
9.1.7 受信した ICMP のログを記録するか否かの設定	93
9.1.8 ステルス機能の設定	93
9.2 IPv6 の設定	94
9.2.1 ICMP Echo Reply を送信するか否かの設定	94
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	94
9.2.3 ICMP Parameter Problem を送信するか否かの設定	94
9.2.4 ICMP Time Exceeded を送信するか否かの設定	95
9.2.5 ICMP Destination Unreachable を送信するか否かの設定	95
9.2.6 受信した ICMP のログを記録するか否かの設定	96
9.2.7 ICMP Packet-Too-Big を送信するか否かの設定	96
9.2.8 ステルス機能の設定	96
第 10 章 : SNMP の設定	98
10.1 SNMPv1 によるアクセスを許可するホストの設定	98
10.2 SNMPv1 の読み出し専用のコミュニティ名の設定	99
10.3 SNMPv1 の読み書き可能なコミュニティ名の設定	99
10.4 SNMPv1 トラップの送信先の設定	99
10.5 SNMPv1 トラップのコミュニティ名の設定	99
10.6 SNMPv2c によるアクセスを許可するホストの設定	100
10.7 SNMPv2c の読み出し専用のコミュニティ名の設定	100

10.8 SNMPv2c の読み書き可能なコミュニティ名の設定	100
10.9 SNMPv2c トラップの送信先の設定	101
10.10 SNMPv2c トラップのコミュニティ名の設定	101
10.11 SNMPv3 エンジン ID の設定	101
10.12 SNMPv3 コンテキスト名の設定	101
10.13 SNMPv3 USM で管理するユーザの設定	102
10.14 SNMPv3 によるアクセスを許可するホストの設定	103
10.15 SNMPv3 VACM で管理する MIB ビューファミリの設定	103
10.16 SNMPv3 VACM で管理するアクセスポリシーの設定	104
10.17 SNMPv3 トラップの送信先の設定	104
10.18 SNMP 送信パケットの始点アドレスの設定	105
10.19 sysContact の設定	105
10.20 sysLocation の設定	105
10.21 sysName の設定	105
10.22 SNMP 標準トラップを送信するか否かの設定	106
10.23 SNMP の linkDown トラップの送信制御の設定	106
10.24 LAN インタフェースの各ポートのリンクが up/down したときにトラップを送信するか否かの設定	107
第 11 章 : DNS の設定	108
11.1 DNS を利用するか否かの設定	108
11.2 DNS サーバーの IP アドレスの設定	108
11.3 DNS ドメイン名の設定	108
11.4 SYSLOG 表示で DNS により名前解決するか否かの設定	109
11.5 DNS 問い合わせの内容に応じた DNS サーバーの選択	109
11.6 静的 DNS レコードの登録	110
11.7 DNS 問い合わせパケットの始点ポート番号の設定	111
11.8 DNS サーバーへアクセスできるホストの設定	112
11.9 DNS キャッシュを使用するか否かの設定	112
11.10 DNS キャッシュの最大エントリ数の設定	113
11.11 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	113
第 12 章 : IPv6	115
12.1 共通の設定	115
12.1.1 IPv6 インタフェースのリンク MTU の設定	115
12.1.2 TCP ウィンドウ・スケール・オプションを変更する	115
12.1.3 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	115
12.2 IPv6 アドレスの管理	116
12.2.1 インタフェースの IPv6 アドレスの設定	116
12.2.2 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	117
12.2.3 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	118
12.2.4 DAD(Duplicate Address Detection) の送信回数の設定	118
12.2.5 自動的に設定される IPv6 アドレスの最大数の設定	119
12.2.6 始点 IPv6 アドレスを選択する規則の設定	119
12.3 経路制御	119
12.3.1 IPv6 の経路情報の追加	119
12.4 RIPng	120
12.4.1 RIPng の使用の設定	120
12.4.2 インタフェースにおける RIPng の受信ポリシーの設定	120
12.4.3 RIPng の加算ホップ数の設定	121
12.4.4 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	121

12.4.5 RIPng で送受信する経路に対するフィルタリングの設定	121
12.4.6 RIPng による経路の優先度の設定	122
12.5 VRRPv3 の設定	122
12.5.1 インタフェース毎の VRRPv3 の設定	122
12.5.2 シャットダウントリガの設定	123
12.6 フィルタの設定	123
12.6.1 IPv6 フィルタの定義	124
12.6.2 IPv6 フィルタの適用	124
12.6.3 IPv6 動的フィルタの定義	125
12.7 近隣要請	126
12.7.1 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	126
第 13 章：トリガによるメール通知機能	128
13.1 メール設定識別名の設定	128
13.2 SMTP メールサーバーの設定	128
13.3 POP メールサーバーの設定	129
13.4 メール処理のタイムアウト値の設定	129
13.5 メールの送信時に使用するテンプレートの設定	130
13.6 メール通知のトリガの設定	131
13.7 パケットログ情報の保存方法の設定	133
第 14 章：HTTP サーバー機能	134
14.1 共通の設定	134
14.1.1 HTTP サーバー機能の有無の設定	134
14.1.2 HTTP サーバーへアクセスできるホストの設定	134
14.1.3 HTTP サーバーのセッションタイムアウト時間の設定	135
14.1.4 HTTP サーバー機能の listen ポートの設定	135
14.1.5 設定・管理ページで表示する装置名称の設定	135
第 15 章：スケジュール	136
15.1 スケジュールの設定	136
第 16 章：SNTP サーバー機能	138
16.1 SNTP サーバー機能を有効にするか否かの設定	138
16.2 SNTP サーバーへのアクセスを許可するホストの設定	138
第 17 章：外部メモリ機能	140
17.1 USB ホスト機能を使うか否かの設定	140
17.2 USB バスで過電流保護機能が働くまでの時間の設定	141
17.3 microSD カードスロットを使うか否かの設定	141
17.4 外部メモリ用キャッシュメモリの動作モードの設定	141
17.5 ファイルアクセス高速化用キャッシュメモリのサイズの設定	142
17.6 外部メモリに保存する SYSLOG ファイル名の指定	142
17.7 外部メモリボタンと DOWNLOAD ボタンの同時押下による設定ファイル、ファームウェアファイルのコピー操作を許可するか否かの設定	144
17.8 外部メモリ内のファイルからの起動を許可するか否かの設定	144
17.9 ルーター起動時に外部メモリを検出するまでのタイムアウトを設定する	145
17.10 起動時、あるいは外部メモリボタンと DOWNLOAD ボタン同時押下により読み込まれる、ファームウェアファイル名の指定	145
17.11 起動時、あるいは外部メモリボタンと DOWNLOAD ボタン同時押下により読み込まれる、設定ファイル名の指定	146
17.12 ファイル検索時のタイムアウトを設定する	147
17.13 バッチファイルを実行する	147

17.14	バッチファイルと実行結果ファイルの設定	147
17.15	外部メモリ性能測定コマンド	148
17.16	DOWNLOAD ボタンを押した時に実行する機能の設定	149
17.17	DOWNLOAD ボタンによるバッチファイルの実行を許可するか否かの設定	149
17.18	監視情報を書き出すファイル名のプレフィックスの設定	150
第 18 章	Lua スクリプト機能	152
18.1	Lua スクリプト機能を有効にするか否かの設定	152
18.2	Lua スクリプトの実行	152
18.3	Lua コンパイラの実行	153
18.4	Lua スクリプトの走行状態の表示	153
18.5	Lua スクリプトの強制終了	154
18.6	Lua スクリプト機能に関連するアラーム音を鳴らすか否かの設定	154
第 19 章	操作	156
19.1	設定に関する操作	156
19.1.1	管理ユーザへの移行	156
19.1.2	終了	156
19.1.3	設定内容の保存	156
19.1.4	設定ファイルの複製	157
19.1.5	ファームウェアファイルを内蔵フラッシュ ROM にコピー	158
19.1.6	設定ファイルの削除	159
19.1.7	デフォルト設定ファイルの設定	159
19.1.8	設定の初期化	159
19.2	動的情報のクリア操作	159
19.2.1	ARP テーブルのクリア	159
19.2.2	IP の動的経路情報のクリア	159
19.2.3	ログのクリア	160
19.2.4	DNS キャッシュのクリア	160
19.2.5	インタフェースのカウンター情報のクリア	160
19.2.6	IPv6 の動的経路情報の消去	160
19.2.7	近隣キャッシュの消去	160
19.2.8	起動情報の履歴を削除する	160
19.2.9	外部メモリに保存された SYSLOG のクリアとバックアップファイルの削除	160
19.2.10	パケットログ情報のクリア	161
19.2.11	通話履歴の消去	161
19.2.12	障害履歴の消去	161
19.2.13	統計情報の消去	161
19.3	ファイル、ディレクトリの操作	161
19.3.1	ディレクトリの作成	161
19.3.2	ファイルまたはディレクトリの削除	162
19.3.3	ファイルまたはディレクトリの複製	162
19.3.4	ファイル名またはディレクトリ名の変更	162
19.4	その他の操作	163
19.4.1	再起動	163
19.4.2	インタフェースの再起動	163
19.4.3	ping	163
19.4.4	ping6 の実行	164
19.4.5	tracert	165
19.4.6	tracert6 の実行	165
19.4.7	nslookup	165

19.4.8 IPv4 動的フィルタのコネクション管理情報の削除	165
19.4.9 TELNET クライアント	166
19.4.10 IPv6 動的フィルタのコネクション管理情報の削除	167
19.4.11 スイッチングハブ MAC アドレステーブルの消去	167
19.4.12 HTTP を利用したファームウェアのチェックおよびリビジョンアップの実行	167
19.4.13 メール通知の実行	168
19.4.14 外部メモリに保存された SYSLOG ファイルのローテート (バックアップ)	168
19.4.15 SIP 呼の切断	168
19.4.16 電話帳サーバーメンテナンス状態の設定	168
19.4.17 監視情報を不揮発性メモリへ保存する	169
第 20 章 : 設定の表示	170
20.1 機器設定の表示	170
20.2 すべての設定内容の表示	170
20.3 設定ファイルの一覧	170
20.4 ファイル情報の一覧の表示	170
20.5 インタフェースに付与されている IPv6 アドレスの表示	171
20.6 SSH サーバー公開鍵の表示	171
20.7 指定したインタフェースのフィルタ内容の表示	172
20.8 ファームウェアファイルの一覧	172
第 21 章 : 状態の表示	173
21.1 ARP テーブルの表示	173
21.2 インタフェースの状態の表示	173
21.3 IP の経路情報テーブルの表示	173
21.4 RIP で得られた経路情報の表示	174
21.5 IPv6 の経路情報の表示	174
21.6 IPv6 の RIP テーブルの表示	174
21.7 近隣キャッシュの表示	174
21.8 VRRP の情報の表示	174
21.9 DHCP サーバーの状態の表示	175
21.10 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	175
21.11 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	175
21.12 ネットワーク監視機能の状態の表示	176
21.13 侵入情報の履歴の表示	176
21.14 スイッチングハブ MAC アドレステーブルの表示	176
21.15 トリガによるメール通知機能の状態の表示	177
21.16 ログインしているユーザー情報の表示	177
21.17 パケットバッファの状態の表示	177
21.18 USB ホスト機能の動作状態を表示	178
21.19 技術情報の表示	178
21.20 microSD スロットの動作状態を表示	179
21.21 外部メモリの動作状態を表示	179
21.22 RTFS の状態の表示	179
21.23 起動情報を表示する	179
21.24 起動情報の履歴の詳細を表示する	180
21.25 起動情報の履歴の一覧を表示する	180
21.26 DNS キャッシュの表示	180
21.27 STATUS LED の情報の表示	180
21.28 コピーライトの表示	180
21.29 拠点登録状況の表示	180

21.30 通信中の呼情報の表示	181
21.31 通話履歴の表示	181
21.32 障害履歴の表示	181
21.33 統計情報の表示	182
21.34 拠点情報の表示	182
21.35 拠点情報の概略表示	183
21.36 電話帳サーバー VRRP 冗長構成機能の状態表示	183
第 22 章: ログイン	184
22.1 ログの表示	184

序文

はじめに

- 本書の記載内容の一部または全部を無断で転載することを禁じます。
- 本書の記載内容は将来予告なく変更されることがあります。
- 本製品を使用した結果発生した情報の消失等の損失については、当社では責任を負いかねます。保証は本製品物損の範囲に限ります。予めご了承ください。
- 本書の内容については万全を期して作成致しておりますが、記載漏れやご不審な点がございましたらご一報くださいますようお願い致します。
- イーサネットは富士ゼロックス株式会社の登録商標です。
- Microsoft、Windows は米国 Microsoft 社の米国およびその他の国における登録商標です。
- microSDHC ロゴは商標です。

第 1 章

コマンドリファレンスの見方

1.1 対応するプログラムのリビジョン

このコマンドリファレンスは、YSL-V810 のファームウェア、Rev.1.03.01 に対応しています。
このコマンドリファレンスの印刷より後にリリースされた最新のファームウェアや、マニュアル類および差分については以下に示す URL の WWW サーバーにある情報を参照してください。

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

1.2 コマンドリファレンスの見方

このコマンドリファレンスは、電話帳サーバ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。

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、電話帳サーバ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

ポートの名称	インタフェースの種類	インタフェース名
LAN ポート	LAN インタフェース	lan1
SETUP ポート	設定専用 LAN インタフェース	lan2

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

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多い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 工場出荷設定値について

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

```
ip lan2 address 10.0.0.1/24
telnetd service off
dhcp service server
dhcp server rfc2131 compliant except remain-silent
dhcp scope 1 10.0.0.2-10.0.0.9/24
```

第 2 章

コマンドの使い方

YSL-V810 に直接コマンドを 1 つ 1 つ送って機能を設定したり操作したりする方法と、必要なコマンド一式を記述したファイルを送信して設定する方法の 2 種類をサポートしています。LAN インタフェースが使用できない場合は、CONSOLE または SERIAL ポートを使ってコマンドを実行し、復旧などの必要な操作を行うことができます。

対話的に設定する手段をコンソールと呼び、コマンドを 1 つ 1 つ実行して設定や操作を行うことができます。必要なコマンド一式を記述したファイルを設定ファイル (Config) と呼び、TFTP により YSL-V810 にアクセスできる環境から設定ファイルを送信したり受信したりすることが可能です。

2.1 コンソールについて

各種の設定を行うためには、YSL-V810 の CONSOLE ポートにシリアル端末を接続する方法と、LAN 上のホストから TELNET、または SSH でログインする方法の 2 つがあります。

YSL-V810 へのアクセス方法
CONSOLE ポートに接続した端末からアクセス
LAN 上のホストから TELNET または SSH でログイン

YSL-V810 へは、それぞれに対して 1 ユーザがアクセスすることができます。またその中で管理ユーザになれるのは同時に 1 ユーザだけです。例えば、シリアル端末でアクセスしているユーザが管理ユーザとして設定を行っている場合には、別のユーザが一般ユーザとしてアクセスすることはできても管理ユーザになって設定を行うことはできません。

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

2.1.1 コンソールによる設定手順

CONSOLE ポートから設定を行う場合は、まず YSL-V810 の CONSOLE ポートとパソコンをクロスタイプのシリアルケーブルで接続します。シリアルケーブルの両端のコネクタはパソコンに適合したタイプをご使用ください。パソコンではターミナルソフトを使います。Windows をお使いの場合は OS に付属の『ハイパーターミナル』などのソフトウェアを使用します。MacOS X をお使いの場合は、OS に付属の『ターミナル』アプリケーションを使用します。

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

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

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

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

設定手順のおおまかな流れは次のようになります。

1. 一般ユーザとしてログインした後、`administrator` コマンドで管理ユーザとしてアクセスします。この時管理パスワードが設定してあれば、管理パスワードの入力が必要です。
2. 冗長構成のとき、メイン動作中の電話帳サーバーを設定変更する場合は、`sip proxy maintenance on` コマンドを実行して動作状態をメンテナンス状態に変更します。メイン動作中の電話帳サーバーの設定を変更すると、通話中の呼が切断される可能性があります。
3. 各種コマンドを使用して、相手先情報の内容を変更します。
4. `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。
5. もし 2. で動作状態を変更していた場合、`sip proxy maintenance off` コマンドを実行して動作状態を通常状態に戻します。

- 👉 **注:** Ctrl キーを押しながら S キーを押すと、コンソール出力を一時停止します。この状態でキーを押しても画面上は無反応に見えますが、キー入力処理は行われます。コンソール出力を再開するには Ctrl キーを押しながら Q キーを押します。

セキュリティの観点から、コンソールにキー入力がない時には、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。この時間は **login timer** コマンドを使用して変更することができます。

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

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

2.1.2 CONSOLE ポートからの設定

ターミナルソフトウェアの使用方法については、各ソフトウェアの取扱説明書をご覧ください。シリアルケーブルの接続は事前にすませておきます。

1. 「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。

設定したユーザ一名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、ユーザ名を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。

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

3. 「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。

4. コンソールコマンドを入力して、設定を行います

5. 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。

6. 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。

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

2.1.3 TELNET による設定

YSL-V810 の IP アドレスは 10.0.0.1 とした場合の例です。

1. [スタート]メニューから[ファイル名を指定して実行]を選びます。

2. 「telnet 10.0.0.1」と入力してから、[OK]をクリックします。

本機の IP アドレスを変更している場合には、「10.0.0.1」のかわりにその IP アドレスを入力します。

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

※TELNET 複数セッション機能対応機種で設定した名前ありユーザでログインする場合は、何も入力せずに Enter キーを押します。次に「Username:」と表示され、ユーザ名を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。

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

5. 「Password:」と表示されたら、管理パスワードを入力します。

「#」が表示されると、各種のコンソールコマンドを入力できます。

6. コンソールコマンドを入力して、設定を行います

7. 設定が終わったら、**save** と入力してから Enter キーを押します。

コンソールコマンドで設定した内容が、本機の不揮発性メモリに保存されます。

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

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

2.2 SSH サーバーについて

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

2.2.1 SSH サーバー機能の使用に当たっての注意事項

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

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

2.2.2 SSH サーバーの設定

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

1. **login user** コマンドで名前ありユーザを登録します。SSH ではログイン時のユーザ名の入力が必要となるため、事前に必ず名前ありユーザを登録しなければなりません。
2. 次に、**sshd host key generate** コマンドで SSH サーバーのホスト鍵を生成します。このコマンドによって DSA または RSA の公開鍵、および秘密鍵のペアが生成されます。ただし機種によってはこのコマンドの処理に数十秒ほど時間がかかる場合があります。
3. 最後に **sshd service** コマンドで SSH サーバー機能を有効にします。

2.3 TFTP について

YSL-V810 に設定した項目は、TFTP により LAN 上のホストから設定ファイルとして読み出すことができます。またホスト上の設定ファイルを本機に読み込ませて設定を行うこともできます。

TFTP は、Windows XP や MacOS X の『ターミナル』アプリケーション、UNIX 環境で標準的に搭載されており、実行することができます。TFTP が搭載されていない環境では、フリーソフトなどで TFTP クライアント機能のあるものを用意してください。この時、YSL-V810 は TFTP サーバーとして動作します。

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

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



注意:

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

2.3.1 TFTP による設定手順

TFTP により設定ファイルをやりとりするためには、YSL-V810 側にあらかじめアクセス許可するための設定が必要です。まず **tftp host** コマンドを使用し、本機にアクセスできるホストを設定します。工場出荷設定ではどのホストからもアクセスできない設定になっていることに注意してください。

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

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

2.3.2 設定ファイルの読み出し

ここでは、Windows から設定ファイルを読み出す場合の例を示します。YSL-V810 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、YSL-V810 の IP アドレスを 10.0.0.1、管理パスワードは“himitsu”、Windows に新しくできるファイルの名称を“OLDconfig.txt”とします。

1. [スタート]メニューから[すべてのプログラム]-[アクセサリ]-[コマンドプロンプト]を選びます。
2. 設定ファイルを保存するディレクトリに移動します。
3. **tftp 10.0.0.1 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 10.0.0.1 get config-encryption-aes128/himitsu OLDconfig.txt

と入力してから、Enter キーを押します

2.3.3 設定ファイルの書き込み

ここでは、Windows から設定ファイルを書き込む場合の例を示します。YSL-V810 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、YSL-V810 の IP アドレスを 10.0.0.1、管理パスワードは“himitsu”、書き込むべき Windows 上のファイルの名称を“NEWconfig.txt”とします。

1. [スタート]メニューから[すべてのプログラム]-[アクセサリ]-[コマンドプロンプト]を選びます。
2. 設定ファイルを保存するディレクトリに移動します。
3. **tftp 10.0.0.1 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 10.0.0.1 put NEWconfig.rtf config/himitsu

と入力してから、Enter キーを押します。

2.4 コンソール使用時のキーボード操作について

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

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

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

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

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

show config、**show config list**、**show 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 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

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

説明：

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

2.5 「show」で始まるコマンド

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

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

[書式]

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

[設定値及び初期値]

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

- [初期値]: -
- *pattern*
 - [設定値]: 検索パターン
 - [初期値]: -

[説明]

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

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

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

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 address
Searching ...
clear switching-hub macaddress: スイッチングハブの MAC アドレステーブルをクリア
^C
#
```

[設定例]

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

2.5.2 show コマンドの表示内容を見やすくする

[書式]

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

[説明]

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

表示内容が 1 画面に満たない場合には、すべての内容を表示して終了する。

コマンドは、数値プレフィ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 <code>grep</code> 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 <code>grep</code> コマンドと同じものである。
n	最後に入力された /、あるいは ? と同じ検索パターンで同じ方向に検索する。
N	最後に入力された /、あるいは ? と同じ検索パターンで逆方向に検索する。

2.5.3 外部メモリへのリダイレクト機能

[書式]

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

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

[設定値及び初期値]

- `name`: ファイル名
 - [設定値]:

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

- [初期値]: -

[説明]

show コマンドの実行結果を外部メモリに保存させることができるリダイレクト (>) により指定されたファイルは、常に新規ファイルとして生成される。このため、同名のファイルが外部メモリ中に存在している場合、ファイルは置き換えられる。

保存ファイルの暗号化には対応していない。

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

```
# show log | grep IPv6 > usb1:log.txt
```

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

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

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

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

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

[ノート]

リダイレクトの後にパイプ (|) は指定できない。

リダイレクトを複数回指定できない。

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

外部メモリについて、以下の状態では本機能は実行できない。

- 接続されていない状態
- ボタンを押された状態
- 使用を禁止されている状態

メモリの容量が不足している場合、書き込みに成功したサイズ分のファイルが生成される。

filename は半角 64 文字以内。

[設定例]

show log の内容を USB メモリに保存

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

show techinfo の内容を microSD カードに保存

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

第3章

ヘルプ

3.1 コンソールに対する簡易説明の表示

[書式]

help

[説明]

コンソールの使用方法の簡単な説明を表示する。

3.2 コマンド一覧の表示

[書式]

show command

[説明]

コマンドの名称とその簡単な説明を一覧表示する。

第 4 章

機器の設定

4.1 ログインパスワードの設定

[書式]

login password

[説明]

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

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

4.2 ログインパスワードの暗号化保存

[書式]

login password encrypted

[説明]

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

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

[ノート]

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

4.3 管理パスワードの設定

[書式]

administrator password

[説明]

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

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

4.4 管理パスワードの暗号化保存

[書式]

administrator password encrypted

[説明]

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

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

[ノート]

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

4.5 ログインユーザ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]

ログインユーザ名とパスワードを設定する。

登録できるユーザは最大 32 人。

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

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

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

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

[ノート]

同一のユーザ名を複数登録することはできない。

既に登録されているユーザ名で設定を行った場合は、元の設定が上書きされる。

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

4.6 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
ユーザ名	登録されているユーザ名
*	すべてのユーザ

- [初期値]: -
- *attribute=value*: ユーザー属性
 - [設定値]:
 - **administrator**: 管理者モードを使えるかどうかを示す属性

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

- *connection*: ルーターへのアクセス方法を示す属性

設定値	説明
off	すべての接続を禁止する。

設定値	説明
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。
http	GUI 設定画面への接続を許可する。

- host : ルーターへのアクセスホストを指定する属性

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

- multi-session : 複数接続を許可するかどうかを示す属性

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

- login-timer : ログインタイマーの指定

設定値	説明
120..21474836	キー入力がない場合に自動的にログアウトするまでの秒数。
clear	ログインタイマーを設定しない。

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

[説明]

ユーザーの属性を設定する。

user を省略した場合は、無名ユーザーの属性を設定する。

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

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

connection 属性では、*off*、*all* 以外の値はコンマ (,) でつないで複数指定することができる。

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

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

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

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

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

無名ユーザーに対しては TELNET での複数接続はできない。

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

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

[ノート]

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

4.7 他のユーザの接続の強制切断

[書式]

```
disconnect user user [/connection[no]]
```

```
disconnect user [user]/connection[no]
```

[設定値及び初期値]

- *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
ssh	SSH による接続
sftp	SFTP による接続
http	GUI 設定画面への接続

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

[説明]

他ユーザの接続を切断する。

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

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

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

[ノート]

自分自身のセッションを切断することはできない。

[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
```

4.8 セキュリティクラスの設定

[書式]

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

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

[設定値及び初期値]• *level*

- [設定値]:

設定値	説明
1	シリアルでも、TELNET、SSH でもログインできる
2	シリアルと TELNET と SSH からは設定できる
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 ssh コマンドが使用できる
off	ssh コマンドは使用できない

- [初期値]: off

[説明]

セキュリティクラスを設定する。

[ノート]

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

4.9 タイムゾーンの設定**[書式]**

timezone *timezone*

no timezone [*timezone*]

[設定値及び初期値]

-
- timezone*
- : その地域と世界標準時との差

- [設定値]:

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

- [初期値]: jst

[説明]

タイムゾーンを設定する。

4.10 現在の日付けの設定

[書式]

date *date*

[設定値及び初期値]

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

[説明]

現在の日付けを設定する。

4.11 現在の時刻の設定

[書式]

time *time*

[設定値及び初期値]

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

[説明]

現在の時刻を設定する。

4.12 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]

YSL-V810 の時計を、パラメータで指定したホストの時間に合わせる。
このコマンドが実行されるとホストの TCP の 37 番ポートに接続する。

[ノート]

YSL-V810 および、多くの UNIX コンピュータをリモートホストに指定できる。
syslog キーワードを指定した場合には、コマンドの出力結果を INFO レベルの SYSLOG へ出力する。

4.13 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 YSL-V810 の時計を設定する。このコマンドが実行されるとホストの UDP の 123 番ポートに接続する。

[ノート]

インターネットに接続している場合には、`rddate` コマンドを使用した場合よりも精密な時計合わせが可能になる。NTP サーバーはできるだけ近くのを指定した方が良い。利用可能な NTP サーバーについてはプロバイダに問い合わせること。

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

4.14 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。

4.15 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
<code>accept-stratum-0</code>	Stratum 0 の NTP サーバーとの時刻同期を許可する

- [初期値]:-

[説明]

Stratum 0 の NTP サーバーとの時刻同期を許可する。

[ノート]

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

4.16 コンソールのプロンプト表示の設定

[書式]

```
console prompt prompt
```

no console prompt [*prompt*]

[設定値及び初期値]

- *prompt*
 - [設定値]: コンソールのプロンプトの先頭文字列 (64 文字以内)
 - [初期値]: -

[説明]

コンソールのプロンプト表示を設定する。空文字列も設定できる。

4.17 コンソールの言語とコードの設定

[書式]

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

[設定値及び初期値]

- *code*
 - [設定値]:

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

- [初期値]: sjis

[説明]

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

4.18 コンソールの表示文字数の設定

[書式]

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

[設定値及び初期値]

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

[説明]

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

4.19 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。

4.20 コンソールにシステムメッセージを表示するか否かの設定**[書式]**

```
console info info
no console info [info]
```

[設定値及び初期値]

- *info*
- [設定値]:

設定値	説明
on	表示する
off	表示しない

- [初期値]: off

[説明]

コンソールにシステムメッセージを表示するか否かを設定する。

[ノート]

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

4.21 SYSLOG を受けるホストの IP アドレスの設定**[書式]**

```
syslog host host
no syslog host [host]
```

[設定値及び初期値]

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

[説明]

SYSLOG を受けるホストの IP アドレスを設定する。

IP アドレスは IPv4/IPv6 いずれのアドレスも設定できる。

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

4.22 SYSLOG ファシリティの設定**[書式]**

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

[設定値及び初期値]

- *facility*
- [設定値]:

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

- [初期値]: user

[説明]

SYSLOG のファシリティを設定する。

[ノート]

ファシリティ番号の意味づけは、各 SYSLOG サーバーで独自に行う。

4.23 NOTICE タイプの SYSLOG を出力するか否かの設定

[書式]

```
syslog notice notice
```

```
no syslog notice [notice]
```

[設定値及び初期値]

- *notice*

- [設定値]:

設定値	説明
on	出力する
off	出力しない

- [初期値]: off

[説明]

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

4.24 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]

SIP の呼制御情報等を SYSLOG で出力するか否か設定する。

[ノート]

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

4.25 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]

デバッグ情報を SYSLOG で出力するか否かを設定する。

[ノート]

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

4.26 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。

4.27 SYSLOG パケットの始点ポート番号の設定

[書式]

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

[設定値及び初期値]

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

[説明]

本機が送信する SYSLOG パケットの始点ポート番号を設定する。

4.28 SYSLOG に実行コマンドを出力するか否かの設定

[書式]

```
syslog execute command switch
no syslog execute command [switch]
```

[設定値及び初期値]

- *switch*
 - [設定値]:

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

- [初期値]: off

[説明]

実行されたコマンドを SYSLOG で出力するか否かを設定する。

[ノート]

コマンド実行に成功した場合、そのコマンド入力をログに出力する。

4.29 TELNET サーバー機能の ON/OFF の設定

[書式]

```
telnetd service service
no telnetd service
```

[設定値及び初期値]

- *service*
 - [設定値]:

設定値	説明
on	TELNET サーバー機能を有効にする
off	TELNET サーバー機能を停止させる

- [初期値]: on

[説明]

TELNET サーバー機能の利用を選択する。

[ノート]

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

4.30 TELNET サーバー機能の listen ポートの設定

[書式]

telnetd listen port

no telnetd listen

[設定値及び初期値]

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

[説明]

TELNET サーバー機能の listen ポートを選択する。

[ノート]

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

4.31 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

no telnetd host

[設定値及び初期値]

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

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

- [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]: -

[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。

4.32 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。

4.33 LAN インタフェースの動作設定

[書式]

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

[設定値及び初期値]

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

[説明]

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

4.34 HUB IC での受信オーバーフロー数を取得するか否かの設定

[書式]

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

[設定値及び初期値]

- *switch*
 - [設定値]:

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

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

[説明]

HUB IC での受信オーバーフロー数を定期的に取得するか否かを設定する。

[ノート]

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

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

4.35 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。

4.36 LAN インタフェースの動作タイプの設定

[書式]

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

[設定値及び初期値]

- *interface_with_swhub*
 - [設定値]: lan1
 - [初期値]: -
- *interface_without_swhub*
 - [設定値]: lan2
 - [初期値]: -
- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *speed*: LAN 速度および動作モード
 - [設定値]:

設定値	説明
auto	速度自動判別
1000-fdx	1000BASE-T 全二重
100-fdx	100BASE-TX 全二重
100-hdx	100BASE-TX 半二重
10-fdx	10BASE-T 全二重
10-hdx	10BASE-T 半二重
省略	省略時は auto

- [初期値]: auto
- *port*

- [設定値]: スイッチングハブのポート番号
- [設定値]:
 - 省略時は全ポート
- [初期値]: -
- `option=value`: オプション機能
- [設定値]:
 - `mtu`
 - インタフェースで送受信できる最大データ長
 - `auto-crossover`
 - オートクロスオーバー機能

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

- `macaddress-aging`
 - MAC アドレスエージング機能

設定値	説明
秒数	エージング時間
off	MAC アドレスエージング機能を無効にする

- `speed-downshift`
 - 速度ダウンシフト機能

設定値	説明
on	速度ダウンシフト機能を有効にする
off	速度ダウンシフト機能を無効にする

- [初期値]:
 - `mtu=1500`
 - `auto-crossover=on`
 - `macaddress-aging=300`
 - `speed-downshift=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。スイッチングハブを持つ LAN インタフェースについては、ポート毎に速度と動作モードを指定できる。

○`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。

○MAC アドレスエージング機能

スイッチングハブを持つ LAN インタフェースでのみ利用できる。

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

設定値に秒数 (1~3551) を指定することができる。ただし、コマンドの設定値と実際に消去されるまでの時間に誤差が生じる場合がある。

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

MAC アドレステーブルの大きさは 1024。

○速度ダウンシフト機能

on に設定すると 1000BASE-T で使用できないケーブルを接続された時に、速度を落としてリンクを試みる。

[ノート]

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

[設定例]

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

```
# lan type lan1 100-fdx 1 2
```

4.37 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 または SSH でログインした場合、clear が設定されていてもタイマ値は 300 秒として扱う。

4.38 TFTP によりアクセスできるホストの設定

[書式]

tftp host *ipaddr*

tftp host *any*

tftp host *none*

no tftp host

[設定値及び初期値]

• *ipaddr*

• [設定値]: IP アドレス

• [初期値]: -

• *any*

• [設定値]: すべてのホストからのアクセスを許可する

• [初期値]: -

• *none*

• [設定値]: すべてのホストからのアクセスを禁止する

• [初期値]: none

[説明]

TFTP サーバーへのアクセスを許可するホストを設定する。

[ノート]

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

4.39 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
 - [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。

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

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

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

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

[書式]

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

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	TCP コネクションの syslog を出力する
off	TCP コネクションの syslog を出力しない

- [初期値]: off
- *src_addr*: 始点 IP アドレス
 - [設定値]:
 - xxx.xxx.xxx.xxx は
 - 10 進数
 - *(ネットマスクの対応するビットが 8 ビットとも 0 と同じ)

- 間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定
- *(すべての IP アドレス)
- [初期値]:-
- *dst_addr*: 終点 IP アドレス
- [設定値]:
 - *src_addr* と同じ形式
 - 省略時は 1 個の * と同じ
- [初期値]:-
- *mask*: IP アドレスのビットマスク。*src_addr* および *dst_addr* がネットワークアドレスの場合にのみ指定可能。
- [設定値]:
 - "0xffffffff" のような 16 進表記
 - "/24" のようなビット数表記
 - 省略時は 0xffffffff と同じ
- [初期値]:-
- *tcpflag*: フィルタリングする TCP パケットの種類
- [設定値]:
 - プロトコルを表す 10 進数 (6 のみ)
 - プロトコルを表すニーモニック

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

- *tcpflag=flag_value/flag_mask*、または *tcpflag!=flag_value/flag_mask*
 - *flag_value*, *flag_mask* は 16 進表記
 - 参考フラグ値

0x0001	FIN
0x0002	SYN
0x0004	RST
0x0008	PSH
0x0010	ACK
0x0020	URG

- *(すべての TCP パケット。ニーモニックに tcp を指定したときと同じ)
- 省略時は * と同じ
- [初期値]:-
- *src_port_list*: TCP のソースポート番号
- [設定値]:
 - ポート番号、タイプを表す 10 進数
 - ポート番号を表すニーモニック

ニーモニック	ポート番号
ftp	20,21
ftpdata	20
telnet	23
smtp	25

ニーモニック	ポート番号
domain	53
gopher	70
finger	79
www	80
pop3	110
sunrpc	111
ident	113
ntp	123
nntp	119
snmp	161
syslog	514
printer	515
talk	517
route	520
uucp	540
submission	587

- 間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。
- 上項目のカンマで区切った並び (10 個以内)
- *(すべてのポート、タイプ)
- 省略時は * と同じ
- [初期値]: -
- *dest_port_list*: TCP のデスティネーションポート番号
 - [設定値]: *src_port_list* と同じ形式
 - [初期値]: -

[説明]

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

[設定例]

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

4.41 HTTP リビジョンアップ実行を許可するか否かの設定

[書式]

```
http revision-up permit permit
no http revision-up permit [permit]
```

[設定値及び初期値]

- *permit*
 - [設定値]:

設定値	説明
on	許可する
off	許可しない

- [初期値]: on

[説明]

HTTP リビジョンアップを許可するか否かを設定する。

[ノート]

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

4.42 HTTP リビジョンアップ用 URL の設定

[書式]

```
http revision-up url url
no http revision-up url [url]
```

[設定値及び初期値]

- *url*
 - [設定値]: ファームウェアが置いてある URL を設定する
 - [初期値]: `http://www.rtpro.yamaha.co.jp/firmware/revision-up/v810.bin`

[説明]

HTTP リビジョンアップとしてファームウェアが置いてある URL を設定する。

入力形式は“`http://サーバーの IP アドレスあるいはホスト名/パス名`”という形式となる。

サーバーのポート番号が 80 以外の場合は、“`http://サーバーの IP アドレスあるいはホスト名:ポート番号/パス名`”という形式で、URL の中に指定する必要がある。

4.43 HTTP リビジョンアップ用 Proxy サーバーの設定

[書式]

```
http revision-up proxy proxy_server [port]
no http revision-up proxy [proxy_server [port]]
```

[設定値及び初期値]

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

[説明]

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

4.44 HTTP リビジョンアップ処理のタイムアウトの設定

[書式]

```
http revision-up timeout time
no http revision-up timeout [time]
```

[設定値及び初期値]

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

[説明]

HTTP リビジョンアップ処理のタイムアウト時間を設定する。

4.45 リビジョンダウンを許可するか否かの設定

[書式]

```
http revision-down permit permit
no http revision-down permit [permit]
```

[設定値及び初期値]

- *permit*
 - [設定値]:

設定値	説明
on	現在のリビジョンより古いリビジョンへのリビジョンダウンを許可する
off	現在のリビジョンより古いリビジョンへのリビジョンダウンを許可しない

- [初期値]: off

[説明]

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

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

[書式]

```
operation http revision-up permit permit
no operation http revision-up permit [permit]
```

[設定値及び初期値]

- *permit*
- [設定値]:

設定値	説明
on	DOWNLOAD ボタンによるリビジョンアップ操作を許可する
off	DOWNLOAD ボタンによるリビジョンアップ操作を許可しない

- [初期値]: off

[説明]

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

[ノート]

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

4.47 リビジョンアップ実行のスケジュール

[書式]

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

[設定値及び初期値]

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

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

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

[説明]

ファームウェアのリビジョンアップを試みるスケジュールを設定する。

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

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

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

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

http revision-up permit コマンドで HTTP リビジョンアップを許可されていない時は、ファームウェアのリビジョンアップは行わない。

http revision-down permit コマンドでリビジョンダウンが許可されている場合は、WEB サーバーにおいてあるファームウェアが現在のファームウェアよりも古いリビジョンであってもファームウェアの書き換えを行う。

なお、WEB サーバーにおいてあるファームウェアが現在のファームウェアと同一リビジョンの場合には、ファームウェアの書き換えは行わない。

[設定例]

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

4.48 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。

4.49 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。

4.50 SSH サーバーへアクセスできるホストの設定

[書式]

```
sshd host ip_range [ip_range...]
sshd host any
sshd host none
no sshd host
```

[設定値及び初期値]

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

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

- [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] : -

[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。

4.51 SSH サーバーへ同時に接続できるユーザ数の設定

[書式]

```
sshd session num
no sshd session [num]
```

[設定値及び初期値]

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

[説明]

SSH に同時に接続できるユーザ数を設定する。

[ノート]

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

4.52 SSH サーバーホスト鍵の設定

[書式]

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

[設定値及び初期値]

- *bit*
 - [設定値] : 鍵のビット長(1024, 2048)
 - [初期値] : 1024

[説明]

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

[ノート]

SSH サーバー機能を利用する場合は、事前に本コマンドを実行してホスト鍵を生成する必要がある。
既にホスト鍵が設定されている状態で本コマンドを実行した場合、ユーザに対してホスト鍵を更新するか否かを確認する。

ホスト鍵の生成には、機種によって異なるが、1024 ビット鍵では数秒から 数分程度、2048 ビット鍵では数分から十数分程度の時間がかかる。

TFTP で設定を取得した場合は、**sshd host key generate [bit=bit] KEY1 KEY2 KEY3** という形式で保存される。
KEY1 ? KEY3 は、秘密鍵を機器固有の方式で暗号化した文字列である。

4.53 SSH サーバーで利用可能な暗号アルゴリズムの設定**[書式]**

```
sshd encrypt algorithm algorithm [algorithm ...]
no sshd encrypt algorithm [...]
```

[設定値及び初期値]

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

設定値	説明
aes128-ctr	AES128-CTR
aes192-ctr	AES192-CTR
aes256-ctr	AES256-CTR
aes128-cbc	AES128-CBC
aes192-cbc	AES192-CBC
aes256-cbc	AES256-CBC
3des-cbc	3DES-CBC
blowfish-cbc	Blowfish-CBC
cast128-cbc	CAST-128-CBC
arcfour	Arcfour

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

[説明]

SSH サーバーで利用可能な暗号アルゴリズムを設定する。
algorithm で指定した暗号アルゴリズムのリストを SSH 接続時にクライアントへ提案する。

[ノート]

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

4.54 SSH クライアントの生存確認**[書式]**

```
sshd client alive switch [interval [count]]
no sshd client alive [switch ...]
```

[設定値及び初期値]

- *switch*
- [設定値]:

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

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

[説明]

クライアントの生存確認を行うか否かを設定する。

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

4.55 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]

```
sshhd hide openssh version use
no sshhd 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。

4.56 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
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

設定値	説明
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]: 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 **sshd host** コマンドでもアクセスが許可されていな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。

4.57 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、YSL-V810 にログインした際に入力したユーザ名を使用して SSH サーバーへのアクセスを試みる。

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

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

実行例は以下の通り。

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

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

リモートホスト (2001:1::1) へアクセスする。

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

4.58 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 YSL-V810 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 YSL-V810 のファイルシステムにあるファイルを指定することはできない。

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

YSL-V810 の設定ファイル (config、config0~config1) 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。

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

実行例は以下の通り。

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

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

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

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

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

[設定値及び初期値]

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

設定値	説明
aes128-ctr	AES128-CTR
aes192-ctr	AES192-CTR
aes256-ctr	AES256-CTR
aes128-cbc	AES128-CBC
aes192-cbc	AES192-CBC
aes256-cbc	AES256-CBC
3des-cbc	3DES-CBC
blowfish-cbc	Blowfish-CBC
cast128-cbc	CAST-128-CBC

設定値	説明
arcfour	Arcfour

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

[説明]

SCP クライアントで利用可能な暗号アルゴリズムを設定する。

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

[ノート]

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

4.60 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。

4.61 パケットバッファのパラメータを変更する

[書式]

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

[設定値及び初期値]

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

設定値	説明
max-buffer	パケットバッファの最大割り当て数
max-free	フリーリストの最大値
min-free	フリーリストの最小値
buffer-in-chunk	チャンク内のパケットバッファ数
init-chunk	起動時に確保するチャンク数

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

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

[説明]

パケットバッファの管理パラメータを変更する。

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

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

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

[設定例]

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

4.62 有効になっているアラーム音を鳴らすか全く鳴らさないかの設定

[書式]

alarm entire *switch*
no alarm entire

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	鳴らす
off	鳴らさない

- [初期値]: on

[説明]

有効になっているアラーム音を鳴らすか全く鳴らさないかを選択する。

4.63 USB ホスト機能に関連するアラーム音を鳴らすか否かの設定

[書式]

alarm usbhost *switch*
no alarm usbhost

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	鳴らす
off	鳴らさない

- [初期値]: on

[説明]

USB ホスト機能に関連するアラーム音を鳴らすか否かを選択する。

4.64 microSD 機能に関連するアラームを鳴らすか否かの設定

[書式]

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

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	鳴らす
off	鳴らさない

- [初期値]: on

[説明]

microSD 機能に関連するアラームを鳴らすかどうかを設定する。

4.65 バッチファイル実行機能に関連するアラーム音を鳴らすか否かの設定

[書式]

alarm batch switch

no alarm batch

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
on	鳴らす
off	鳴らさない

- [初期値]: on

[説明]

バッチファイル実行機能に関連するアラーム音を鳴らすか否かを選択する。

4.66 起動時のアラーム音を鳴らすか否かの設定

[書式]

alarm startup switch [pattern]

no alarm startup [switch]

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
on	鳴らす
off	鳴らさない

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

[説明]

起動時にアラーム音を鳴らすか否かを選択する。

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

[書式]

alarm http revision-up switch

no alarm http revision-up [switch]

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
on	鳴らす

設定値	説明
off	鳴らさない

- [初期値]: on

[説明]

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

4.68 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]

YSL-V810 の環境変数を設定する。

環境変数名の命名規則は次の通りである。

半角の英数字とアンダースコア '_' が使用できるが、アンダースコアまたは数字を最初の文字にすることはできない。

変数名の長さに制限はないが、**set** コマンドはコマンドラインの最大長 (4095 文字) を超えて実行できない。英字の大文字、小文字を区別する。例えば、abc と Abc は別の変数として扱われる。

4.69 監視情報を不揮発性メモリへ保存する

[書式]

```
save report at time
```

[設定値及び初期値]

- *time*
 - [設定値]: 時:分 (0..23 : 0..59)
 - [初期値]: 3:00

[説明]

不揮発性メモリに対し、統計情報の保存領域の確保、障害履歴の保存、通話履歴の保存を行う時刻を指定する。

不揮発性メモリに保存する前の情報は揮発性メモリに記録されており、電源を切ると消えてしまう。

上記の処理は、毎日 1 回ここで設定した時刻に行う。不揮発性メモリへの保存処理を行っている間、呼処理など保存以外の処理が遅くなるので、例えば深夜など処理速度が低下しても影響の少ない時刻を指定することが望ましい。設定した時刻に対し、実際に処理が始まる時刻は最大で +60 秒後になる可能性がある。また処理に要する時間は不定であるが、呼処理を行っていない場合で最大 2 分程度の時間を要する。

external-memory sip-proxy filename prefix コマンド設定があれば、この設定時刻に外部メモリへの保存も行なう。

[ノート]

time の指定は、スケジュールコマンドの指定形式と異なり、'*' は指定できない。

第 5 章

ヤマハルーター用ファイルシステム RTFS

RTFS は、YSL-V810 の内蔵フラッシュ ROM に構築されるファイルシステムです。一般的な PC のファイルシステムと同様、内蔵フラッシュ ROM に任意のデータを保存しファイル名を付けて管理することができます。またディレクトリ構造も実現されています。内蔵フラッシュ ROM にはファームウェア (exec) や設定ファイル (config) など様々なデータが保存されていますが、それらとは独立した特定の領域を RTFS として使用します。

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

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

5.1 RTFS のフォーマット

[書式]

`rtfs format`

[説明]

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

[ノート]

フォーマットを実行するとデータは完全に削除され、復元することができない。

5.2 RTFS のガベージコレクション

[書式]

`rtfs garbage-collect`

[説明]

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

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

[ノート]

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

第 6 章

電話帳サーバー機能の設定

6.1 電話帳サーバードメイン名の設定

[書式]

sip proxy domain *domain*

no sip proxy domain

[設定値及び初期値]

- *domain*
 - [設定値]: ドメイン名
 - [初期値]: -

[説明]

電話帳サーバーで使用するドメイン名を設定する。

ドメイン名を設定しない場合はすべてのドメイン名について許容する。

ドメイン名を設定した場合は設定したドメイン名のみのアクセスを許す。

複数登録することはできない。

6.2 拠点情報の設定

[書式]

sip user *uri numberin* [*name=name*] [*auth=type*] [[*username*] [*password*]]

sip user *uri_top - uri_end numberin* [*name=name*] [*auth=type*] [[*username*] [*password*]]

sip user * *numberin* [*name=name*] [*auth=type*] [[*username*] [*password*]]

no sip user *uri*

no sip user *uri_top - uri_end*

no sip user *

[設定値及び初期値]

- *uri*
 - [設定値]: 個別 URI
 - [初期値]: -
- *uri_top*
 - [設定値]: 範囲 URI の始まり
 - [初期値]: -
- *uri_end*
 - [設定値]: 範囲 URI の終わり
 - [初期値]: -
- *numberin*: 事業所番号 + 内線番号の着番号から事業所番号を削除するかどうかの設定
 - [設定値]:

設定値	説明
all	削除しない
ext	削除する

- [初期値]: -
- *name*
 - [設定値]: 登録名
 - [初期値]: -
- *type*
 - [設定値]: 認証種類
 - [設定値]:

設定値	説明
none	認証不要
digest	ダイジェスト認証

- [初期値] : digest
- *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]

拠点情報を設定または削除する。

uri は、以下のように記述ができる。URI のスキームまたはホスト部の入力を省略することができる。

指定 URI の形式	認証時に使用される URI
sip:user@host	sip:user@host
user@host	sip:user@host とみなす。
sip:user	認証時に sip proxy domain 設定がされている場合 : sip:user@ (認証時に設定されているドメイン名) とみなす。 認証時に sip proxy domain 設定がされていない場合 : 認証対象の URI のうち、スキーム+ユーザ部のみ sip:user と照合し、ホスト部の比較は行わない。
tel:user	tel:user
user	認証時に sip proxy domain 設定がされている場合 : sip:user@ (認証時に設定されているドメイン名) とみなす。 認証時に sip proxy domain 設定がされていない場合 : 認証対象の URI のうち、スキーム+ユーザ部のみ sip:user と照合し、ホスト部の比較は行わない。

なお、URI のスキーム、ユーザ、ホスト部以外のエレメントは入力する意味がなく、含んでいたら無視する。また URI として * (アスタリスク) を指定した場合、上記個別または下記範囲指定で指定した URI 以外の URI すべてに適用する設定となる。削除時にアスタリスクを指定した場合、その他の URI に適用する設定のみを削除する。

uri_top と *uri_end* は、スキームまたはホスト部の入力を省略することができるのは個別に URI を指定する場合と同様。

uri_top - *uri_end* 形式の指定は、URI のうちのユーザ部に対し、末尾の数字列 (0,1,2,3,4,5,6,7,8,9 から成る文字列) を数値とみなして、数値範囲の複数のユーザ部を指定する。数字列以前の文字列および数字列の桁数は、*uri_top* と *uri_end* で完全に一致している必要がある。

例えば "008 - 011" を指定した場合は、"008", "009", "010", "011" を指定したことになる。

username は、*type* が none のときは、入力しても無視される。省略した場合は、もしくは * (アスタリスク) を指定した場合は、認証時に URI のユーザ部と同じ文字列とみなされる。

password は、*type* が none のときは、入力しても無視される。省略した場合は、空文字列とみなされる。

[ノート]

認証対象 URI の照合は、数値の大小だけでなく、数字列長とユーザ部末尾の数字列以外の文字列も照合する。すなわち先の例では、"008" にはマッチするが、"0008" や "user008" にはマッチしない。

URI の範囲指定において、数字列は { '0' '1' '2' '3' '4' '5' '6' '7' '8' '9' } だけから成る文字列である。また数値とみなす数字列長は最大 18 文字までであり、18 文字を超える場合は、末尾の 18 文字だけが使用される。範囲の重なる複数の範囲指定認証情報を登録することはできない。登録しようとした場合はエラーとする。個別指定と範囲指定が重なる場合は登録できる。

sip user uri_top - uri_end で登録された情報の削除は、**no sip user uri_top - uri_end** で全く同じ範囲指定を行うことのみ可能。例えば、"001 - 005" で登録した場合、"003" や "003 - 004" を指定して、一部の範囲のみ削除することはできない。

個別指定 URI で登録した認証情報は、範囲指定した認証情報より優先する。例えば "003" に対する個別指定認証情報と "001 - 005" に対する範囲指定認証情報があったとき、"003" を認証する場合は、個別認証情報の方が使用される。

事業所番号の削除において、内線番号がない場合に削除した場合には、機器の型番が入る。

登録名に非 ASCII 文字を指定する場合は、設定・管理ページから入力する。

6.3 連携する電話帳サーバーの設定

[書式]

```

sip proxy forwarding server num addr [primary=primary] [secondary=secondary] [domain=domain] [name=name]
no sip proxy forwarding server num

```

[設定値及び初期値]

- *num*
 - [設定値]: 連携サーバー番号 (1..4)
 - [初期値]: -
- *addr*
 - [設定値]: 転送先 IP アドレス (仮想アドレス)
 - [初期値]: -
- *primary*
 - [設定値]: 連携サーバーのプライマリサーバーの実アドレス
 - [初期値]: -
- *secondary*
 - [設定値]: 連携サーバーのセカンダリサーバーの実アドレス
 - [初期値]: -
- *domain*
 - [設定値]: ドメイン名
 - [初期値]: -
- *name*
 - [設定値]: 設定名
 - [初期値]: -

[説明]

連携する電話帳サーバーの設定をする。

連携する電話帳サーバーが冗長構成の場合に、仮想アドレスを転送先 IP アドレスに設定し、それぞれの実アドレスをプライマリ・セカンダリに設定する。

連携する電話帳サーバーが単体動作の場合には、プライマリ・セカンダリの設定は不要となる。

転送先 IP アドレスのみ設定する。

また、ドメイン名には連携する電話帳サーバーのドメイン名を設定する。

6.4 連携する電話帳サーバーが管理する番号の設定

[書式]

```

sip proxy forwarding address num uri
sip proxy forwarding address num uri_top - uri_end
no sip proxy forwarding address num uri
no sip proxy forwarding address num uri_top - uri_end

```

[設定値及び初期値]

- *num*
 - [設定値]: 連携サーバー番号 (1..4)
 - [初期値]: -
- *uri*
 - [設定値]: **sip user** コマンドを参照
 - [初期値]: -
- *uri_top*

- [設定値]: **sip user** コマンドを参照
- [初期値]: -
- *uri_end*
 - [設定値]: **sip user** コマンドを参照
 - [初期値]: -

[説明]

連携する電話帳サーバーで管理している電話番号を設定する。

設定された番号または範囲内宛の発信を受信すると、連携する電話帳サーバーの設定で登録した転送先 IP アドレスへ発信を転送する。

範囲指定は重ならないように設定する必要がある。

6.5 冗長構成機能のための動作モードおよび冗長構成相手の設定

[書式]

sip proxy redundancy mode mode [vrid ip-addr]

no sip proxy redundancy mode

[設定値及び初期値]

- *mode*: 電話帳サーバー VRRP 冗長構成におけるモードを設定する
 - [設定値]:

設定値	説明
standalone	単独動作サーバーであることを設定
primary	プライマリサーバーであることを設定
secondary	セカンダリサーバーであることを設定

- [初期値]: standalone
- *vrid*
 - [設定値]: primary / secondary の場合、電話帳サーバー VRRP 冗長構成に使用する VRRP グループ ID (1..255)
 - [初期値]: -
- *ip-addr*
 - [設定値]: 電話帳サーバー VRRP 冗長構成を形成する相手の IP アドレス
 - [初期値]: -

[説明]

電話帳サーバー VRRP 冗長構成の設定を行う。プライマリ / セカンダリサーバーの場合、VRRP 動作における VRRP グループ ID と、冗長構成を形成する相手のサーバーの IP アドレスを設定する必要がある。

冗長構成に使用される VRRP の IP プロトコルについては *ip-addr* で設定されたものと同一のものの設定が選択される。

プライマリサーバーとセカンダリサーバーにおける VRRP グループ ID、IP プロトコルを一致させるように設定を行う必要がある。VRRP の設定においては、プライマリサーバーの優先度をセカンダリサーバーの優先度より高く設定する必要がある。メンテナンス状態での優先度との兼ね合いがあるため、VRRP 優先度は必ず 3 以上を設定しなければならない。

これらの設定に矛盾があった場合の動作は予測できない。

6.6 エラーレスポンスを転送するタイマーの設定

[書式]

sip proxy error response timeout sec

no sip proxy error response timeout

[設定値及び初期値]

- *sec*
 - [設定値]: 秒数 (0..60)
 - [初期値]: 3

[説明]

この設定値を越えて initial-INVITE に対するエラーレスポンスを受信した場合は、ハントグループにより次の着信先

があっても **initial-INVITE** の転送を新たに行わず、この受信したエラーレスポンスを発信元に転送する。
initial-INVITE に対するレスポンスが無い場合にはこの設定値を参照せず、ハントグループによる新しい着信先へ **initial-INVITE** を転送する。
これは、ハントグループ全体での設定値ではない。着信先毎にタイマーはクリアする。

第 7 章

IP の設定

7.1 インタフェース共通の設定

7.1.1 IP アドレスの設定

[書式]

```
ip interface address ip_address/mask [broadcast broadcast_ip]
ip loopback address ip_address[/mask]
no ip interface address [ip_address/mask [broadcast broadcast_ip]]
no ip loopback 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]: -
- *loopback*
 - [設定値]: LOOPBACK 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]: -
- *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]: -

[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。

[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。

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

7.1.2 セカンダリ IP アドレスの設定

[書式]

```
ip interface secondary address ip_address[/mask]
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]: -
- *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。

[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。

7.1.3 インタフェースの MTU の設定**[書式]**

```
ip interface mtu mtu0
no ip interface mtu [mtu0]
```

[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*
 - [設定値]: MTU の値 (64..1500)
 - [初期値]:
 - mtu0=1500

[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。

7.1.4 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
no ip interface 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]:
 - on

[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。

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

[書式]

```
ip simple-service service
no ip simple-service [service]
```

[設定値及び初期値]

- *service*
- [設定値]:

設定値	説明
on	TCP/UDP の各種サービスを動作させる
off	サービスを停止させる

- [初期値]: off

[説明]

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

7.1.6 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)
 - 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)
<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
hide	出力インタフェースが LAN インタフェースの場合のみ有効なオプションで、相手先が接続されている場合だけ経路が有効になることを意味する
<i>weight weight</i>	異なる経路間の比率を表す値 <ul style="list-style-type: none"> • <i>weight</i>

設定値	説明
	<ul style="list-style-type: none"> 経路への重み (1..2147483647) 省略時は 1

- [初期値]: -

[説明]

IP の静的経路を設定する。

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

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

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

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

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

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

[ノート]

既に存在する経路を上書きすることができる。

[設定例]

- デフォルトゲートウェイを 192.168.0.1 とする。

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

7.1.7 IP パケットのフィルタの設定

[書式]

```
ip filter filter_num pass_reject src_addr[/mask] [dest_addr[/mask] [protocol [src_port_list [dest_port_list]]]]
no ip filter filter_num [pass_reject]
```

[設定値及び初期値]

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

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)

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

- [初期値]: -
- *src_addr*: IP パケットの始点 IP アドレス
 - [設定値]:
 - IP アドレス
 - A.B.C.D (A~D: 0~255 もしくは*)
 - 上記表記で A~D を*とすると、該当する 8 ビット分についてはすべての値に対応する
 - 間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。
 - , を区切りとして複数設定する事が出来る。
 - *(すべての IP アドレスに対応)
 - [初期値]: -
- *dest_addr*: IP パケットの終点 IP アドレス
 - [設定値]:
 - *src_addr* と同じ形式
 - 省略した場合は一個の * と同じ
 - [初期値]: -
- *mask*: IP アドレスのビットマスク (*src_addr* および *dest_addr* がネットワークアドレスの場合のみ指定可)
 - [設定値]:
 - A.B.C.D (A~D: 0~255)
 - 0x に続く十六進数
 - マスクビット数
 - 省略時は 0xffffffff と同じ
 - [初期値]: -
- *protocol*: フィルタリングするパケットの種類
 - [設定値]:
 - プロトコルを表す十進数 (0..255)
 - プロトコルを表すニーモニック

ニーモニック	十進数	説明
icmp	1	ICMP パケット
tcp	6	TCP パケット
udp	17	UDP パケット
ipv6	41	IPv6 パケット
gre	47	GRE パケット
esp	50	ESP パケット
ah	51	AH パケット
icmp6	58	ICMP6 パケット

- 上項目のカンマで区切った並び (5 個以内)
- 特殊指定

icmp-error	TYPE が 3、4、5、11、12、31、32 のいずれかである ICMP パケット
icmp-info	TYPE が 0、8~10、13~18、30、33~36 のいずれかである ICMP パケット
tcpsyn	SYN フラグの立っている tcp パケット

tcpfin	FIN フラグの立っている tcp パケット
tcprst	RST フラグの立っている tcp パケット
established	ACK フラグの立っている tcp パケット内から外への接続は許可するが、外から内への接続は拒否する機能
tcpflag=value/mask	TCP フラグの値と <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を設定する。本コマンドで設定されたフィルタは **ip filter directed-broadcast**、**ip filter dynamic**、**ip filter set**、**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** を使ったフィルタは、回線が接続されている時だけ通せば十分で、そのために回線に発信するまでもないようなパケットに有効である。例えば、時計を合わせるための NTP パケットがこれに該当する。ICMP パケットに対して、ICMP タイプと ICMP コードをフィルタでチェックしたい場合には、*protocol* には 'icmp' だけを単独で指定する。*protocol* が 'icmp' 単独である場合にのみ、*src_port_list* は ICMP タイプ、*dest_port_list* は ICMP コードと見なされる。*protocol* に 'icmp' と他のプロトコルを列挙した場合には *src_port_list* と *dest_port_list* の指定は TCP/UDP のポート番号と見なされ、ICMP パケットとの比較は行われぬ。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が比較される。パケットがその他のプロトコル (ICMP を含む) の場合には、*src_port_list* と *dest_port_list* の指定は存在しないものとしてフィルタと比較される。

[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 * *
```

7.1.8 フィルタセットの定義**[書式]**

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

[設定値及び初期値]

- *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、**ip interface secure filter** コマンドによりインタフェースに適用される。

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

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

[設定値及び初期値]

- *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。

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

[書式]

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

[設定値及び初期値]

- *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 パケットの扱いを設定する。

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]

いわゆる smurf 攻撃を防止するためには on にしておく。

7.1.11 動的フィルタの定義

[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]: 動的フィルタ番号 (1..21474836)
 - [初期値]: -
- *srcaddr*
 - [設定値]: 始点 IP アドレス
 - [初期値]: -
- *dstaddr*
 - [設定値]: 終点 IP アドレス
 - [初期値]: -
- *mask*: IP アドレスのビットマスク (*src_addr* および *dest_addr* がネットワークアドレスの場合のみ指定可)
 - [初期値]: -
- *protocol*: プロトコルのニーモニック
 - [設定値]:

- tcp/udp/ftp/tftp/domain/www/smtp/pop3/telnet/netmeeting
- 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
- [初期値] : -
- *filter_list*
 - [設定値] : **ip 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	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]

動的フィルタを定義する。第 1 書式では、あらかじめ本装置に登録されているアプリケーション名を指定する。第 2 書式では、ユーザがアクセス制御のルールを記述する。キーワードの *filter*、*in*、*out* の後には、**ip filter** コマンドで定義されたフィルタ番号を設定する。
filter キーワードの後に記述されたフィルタに該当するコネクション (トリガ) を検出したら、それ以降 *in* キーワードと *out* キーワードの後に記述されたフィルタに該当するコネクションを通過させる。*in* キーワードはトリガの方向に対して逆方向のアクセスを制御し、*out* キーワードは動的フィルタと同じ方向のアクセスを制御する。なお、**ip filter** コマンドの IP アドレスは無視される。*pass/reject* の引数も同様に無視される。
 プロトコルとして *tcp* や *udp* を指定した場合には、アプリケーションに固有な処理は実施されない。特定のアプリケーションを扱う必要がある場合には、アプリケーション名を指定する。

[設定例]

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

7.1.12 動的フィルタのタイムアウトの設定

[書式]

```
ip filter dynamic timer option=timeout [option=timeout...]  

no ip filter dynamic timer
```

[設定値及び初期値]

- *option* : オプション名
- [設定値] :

設定値	説明
tcp-syn-timeout	SYN を受けてから設定された時間内にコネクションが確立しなければセッションを切断する
tcp-fin-timeout	FIN を受けてから設定された時間が経てばコネクションを強制的に解放する

設定値	説明
tcp-idle-time	設定された時間内に TCP コネクションのデータが流れなければコネクションを切断する
udp-idle-time	設定された時間内に UDP コネクションのデータが流れなければコネクションを切断する
dns-timeout	DNS の要求を受けてから設定された時間内に応答を受けなければコネクションを切断する

- [初期値]:
 - tcp-syn-timeout=30
 - tcp-fin-timeout=5
 - tcp-idle-time=3600
 - udp-idle-time=30
 - dns-timeout=5

- *timeout*

- [設定値]: 待ち時間 (秒)
- [初期値]: -

[説明]

動的フィルタのタイムアウトを設定する。

[ノート]

本設定はすべての検査において共通に使用される。

7.1.13 侵入検知機能の動作の設定

[書式]

ip interface intrusion detection direction [type] switch [option]

no ip interface 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・コネクションの方向
 - [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・コネクションの種類
 - [設定値]:

設定値	説明
ip	IP ヘッダ
ip-option	IP オプションヘッダ
fragment	フラグメント
icmp	ICMP
udp	UDP
tcp	TCP
ftp	FTP
winny	Winny
share	Share

設定値	説明
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。

7.1.14 1 秒間に侵入検知情報を通知する頻度の設定

[書式]

```
ip interface intrusion detection notice-interval frequency
no ip interface 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。

7.1.15 重複する侵入検知情報の通知抑制の設定

[書式]

```
ip interface intrusion detection repeat-control time
no ip interface 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。

7.1.16 侵入検知情報の最大表示件数の設定**[書式]**

```
ip interface intrusion detection report num
no ip interface 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。

7.1.17 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
no ip interface 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。

7.1.18 本機が端点となる TCP のセッション数の設定**[書式]**

```
tcp session limit limit
no tcp session limit [limit]
```

[設定値及び初期値]

- *limit*: 制限値
 - [設定値]:

設定値	説明
32~65535	セッション数
none	制限しない

- [初期値]:
 - 1000

[説明]

本機が端点となる TCP のセッション数を制限する。

none を選択した場合には制限を設けない。

[ノート]

本機と直接通信しない場合にはこの制限は適用されない。

7.1.19 IPv4 の経路情報に変化があった時にログに記録するか否かの設定**[書式]**

```
ip route change log log
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。

7.1.20 フィルタリングによるセキュリティの設定**[書式]**

```
ip interface secure filter direction [filter_list...] [dynamic filter_list...]
ip interface secure filter name set_name
no ip interface secure filter direction [filter_list]
no ip interface 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
 - [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]: -
- *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。

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。

7.1.21 ARP エントリの寿命の設定

[書式]

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

[設定値及び初期値]

- *timer*
 - [設定値]: ARP エントリの寿命秒数 (30..32767)
 - [初期値]: 1200

[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。

7.1.22 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。

7.1.23 ARP が解決されるまでの間に送信を保留しておくパケットの数を制御する

[書式]

```
ip interface arp queue length len
no ip interface arp queue length [len]
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *len*
 - [設定値]: キュー長 (0..10000)
 - [初期値]:
 - 200

[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。

7.1.24 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。

7.2 RIP の設定**7.2.1 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。

7.2.2 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...]
no ip interface 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。

7.2.3 RIP パケットの受信に関する設定

[書式]

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

[設定値及び初期値]

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

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

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

[説明]

指定したインタフェースに対し、RIP パケットを受信するか否かを設定する。

"`version version`" で受信する RIP のバージョンを指定できる。指定しない場合は、RIP1/2 ともに受信する。

7.2.4 RIP のフィルタリングの設定

[書式]

```
ip interface rip filter direction filter_list
no ip interface 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。

7.2.5 RIP で加算するホップ数の設定**[書式]**

```
ip interface rip hop direction hop
no ip interface 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。

7.2.6 RIP2 での認証の設定**[書式]**

```
ip interface rip auth type type
no ip interface 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。

7.2.7 RIP2 での認証キーの設定

[書式]

```
ip interface rip auth key hex_key
ip interface rip auth key text text_key
no ip interface rip auth key
no ip interface 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
```

7.2.8 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]
no ip interface 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
```

7.2.9 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	

7.2.10 RIP のタイマーを調整する

[書式]

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

[設定値及び初期値]

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

[説明]

RIP のタイマー値を設定する。

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

$$\begin{aligned} update \times 3 &\leq invalid \leq update \times 6 \\ update \times 2 &\leq holddown \leq update \times 4 \end{aligned}$$

7.3 VRRP の設定**7.3.1 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冗長化構成の電話帳サーバ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。

7.3.2 シャットダウントリガの設定

[書式]

```
ip interface vrrp shutdown trigger vrid sip-proxy
ip interface vrrp shutdown trigger vrid ip keepalive number
no ip interface vrrp shutdown trigger vrid sip-proxy
no ip interface vrrp shutdown trigger vrid ip keepalive number
```

[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]: -
- *number*
 - [設定値]: **ip keepalive** 設定の番号
 - [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
sip-proxy	電話帳サーバーとしての動作に問題が発生した場合
ip keepalive	ip keepalive 設定によりダウンが検出された場合

[ノート]

電話帳サーバー動作において、sip-proxy のシャットダウントリガが発生するのは、SIP 動作自己診断において異常を検出した場合である。

7.4 バックアップの設定

7.4.1 ネットワーク監視機能の設定

[書式]

```
ip keepalive num kind interval count gateway [gateway ...] [option=value ...]
no ip keepalive num
```

[設定値及び初期値]

- *num*
 - [設定値]: このコマンドの識別番号 (1..100)
 - [初期値]: -
- *kind*: 監視方式
 - [設定値]:

設定値	説明
icmp-echo	ICMP Echo を使用する

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

- [設定値]:
 - IP アドレス
 - xxx.xxx.xxx.xxx (xxx は十進数)
- [初期値]: -
- *option=value* 列
- [設定値]:

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

- [初期値]:
 - log=off
 - upwait=5
 - downwait=5
 - length=64

[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。

第 8 章

DHCP の設定

本機は DHCP(*1) 機能として、DHCP サーバー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。

YSL-V810 が DHCP サーバーとして機能するか機能させないかは **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 **dhcscope 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。

(*1)Dynamic Host Configuration Protocol; RFC1541 , RFC2131

URL 参照 : <http://rfc.netvolante.jp/rfc/rfc1541.txt> ([rfc2131.txt](http://rfc.netvolante.jp/rfc/rfc2131.txt))

8.1 DHCP サーバー機能

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

- [初期値]: -

[説明]

DHCP に関する機能を設定する。

[ノート]

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

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。

[ノート]

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

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。

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]:

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 アドレスの範囲を設定する。除外 IP アドレスは複数指定できる。リース期間としては無期限を指定できるほか、DHCP クライアントから要求があった場合の許容最大リース期間を指定できる。

[ノート]

ひとつのネットワークについて複数の DHCP スコープを設定することはできない。複数の DHCP スコープで同一の IP アドレスを含めることはできない。IP アドレス範囲にネットワークアドレス、ブロードキャストアドレスを含む場合、割り当て可能アドレスから除外される。

DHCP リレーエージェントを経由しない DHCP クライアントに対して gateway キーワードによる設定パラメータが省略されている場合にはルーター自身の IP アドレスを通知する。

DHCP スコープを上書きした場合、以前のリース情報および予約情報は消去される。

expire の設定値は maxexpire の設定値以下でなければならない。

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

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
no dhcp scope bind scope_num ip_address
```

[設定値及び初期値]

- *scope_num*
 - [設定値]: スコープ番号 (1..65535)
 - [初期値]: -
- *ip_address*
 - [設定値]:

設定値	説明
xxx.xxx.xxx.xxx	(xxx は十進数) 予約する IP アドレス
*	割り当てる IP アドレスを指定しない

- [初期値]: -
- *type*: Client-Identifier オプションの *type* フィールドを決定する
 - [設定値]:

設定値	説明
text	0x00
ethernet	0x01

- [初期値]: -
- *id*
 - [設定値]:

設定値	説明
<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
 - [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。

dhcp scope コマンドを実行した場合、関連する予約はすべて消去される。

ipcp の指定は、同時に接続できる B チャ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いなければならない。また **dhcp server rfc2131 compliant off** あるいは **use-clientid** 機能を使用されないよう設定された時点で、コマンドの第 2 書式によるもの以外の予約は消去される。

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

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

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

[設定例]

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

1. **dhcp server rfc2131 compliant on** あるいは **use-clientid** 機能を使用する設定の場合

- A. B. C. の書式では、クライアントの識別に Client-Identifier オプションを使用する。
- D. の書式では DHCP パケットの *chaddr* フィールドを使用する。ただし、Client-Identifier オプションが存在する場合、この設定は無視される。

DHCP サーバーは *chaddr* フィールドの値より Client-Identifier オプションの値の方が優先して使用される。

show status dhcp コマンドを実行してクライアントの識別子を確認することで、クライアントが Client-Identifier オプションを使っているか否かを判別することも可能である。

- リースしているクライアントとして MAC アドレスが表示されていれば Client-Identifier オプションは使用していない
- リースしているクライアントとして十六進数の文字列、あるいは文字列が表示されていれば、Client-Identifier オプションが使われている Client-Identifier オプションを使うクライアントへの予約は、ここに表示される十六進数の文字列あるいは文字列を使用する

2. **dhcp server rfc2131 compliant off** あるいは **use-clientid** 機能を使用しない場合

- A. B. C. の書式では指定できない。Client-Identifier オプションは無視される。
- D. の書式では DHCP パケットの chaddr フィールドを使用する。

なお、クライアントとの相互動作に関して以下の留意点がある。

- 個々の機能を単独で用いるとクライアント側で思わぬ動作を招く可能性があるため、**dhcp server rfc2131 compliant on** あるいは **dhcp server rfc2131 compliant off** で使用することを推奨する。
- ルーターの再起動やスコープの再設定によりリース情報が消去されている場合、アドレスの延長要求をした時やリース期間内のクライアントを再起動した時にクライアントが使用する IP アドレスは変わることがある。
これを防ぐためには **dhcp server rfc2131 compliant on** (あるいは remain-silent 機能を有効にする) 設定がある。
この設定にすると、ヤマハルーターがリース情報を持たないクライアントからの DHCPREQUEST に対して DHCPNAK を返さず無視するようになる。
この結果、リース期限満了時にクライアントが出す DHCPDISCOVER に Requested IP Address オプションが含まれていれば、そのクライアントには引き続き同じ IP アドレスをリースすることができる。

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
no dhcp scope lease type scope_num [type ...]
```

[設定値及び初期値]

- *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。

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	show status dhcp summary コマンドで表示されるインデックス番号、最大 100 個
all	割り当て中の情報全てを対象とする
省略	省略時は all

- [初期値]: -

[説明]

現在の割り当て情報を元に予約設定を作成する。except キーワードを指示すると、指定した番号以外の情報が予約設定に反映される。

[ノート]

以下の変換規則で IP アドレス割り当て情報が予約設定に変換される。

IP アドレス割り当て情報のクライアント識別種別 (show status dhcp で表示される名称)	クライアント識別情報例	予約設定情報例
クライアントイーサネットアドレス	00:a0:de:01:02:03	ethernet 00:a0:de:01:02:03 ※1
		00:a0:de:01:02:03 ※2
クライアント ID	(01) 00 a0 de 01 02 03	ethernet 00:a0:de:01:02:03
	(01) 00 a0 de 01 02 03 04	01 00 a0 de 01 02 03 04
	(01) 31 32 33	00 31 32 33

※1 : rfc2131 compliant on あるいは use-clientid ありの場合、このような IP アドレス割り当て情報の表示は ARP チェックの結果である可能性が高く、通常の割り当て時にはクライアント ID オプションが使われるため、この形式で予約設定をする。ただし、MAC アドレスと異なるクライアント ID を使うホストが存在する場合はこの自動変換による予約は有効に機能しないため、そのようなホストに対する予約設定は別途、手動で行う必要がある

※2 : rfc2131 compliant off あるいは use-clientid なしの場合、chaddr フィールドを使用する

コマンド実行時点での割り当て情報を元に予約設定を作成する。サマリ表示からこの変換コマンドの実行までに時間が経過した場合には、本コマンド実行後に意図したペアの予約が作成されていることを **show config** で確認すべきである

8.1.8 DHCP オプションの設定

[書式]

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

[設定値及び初期値]

- *scope_num*
 - [設定値]: スコープ番号 (1..65535)
 - [初期値]: -
- *option*
 - [設定値]:
 - オプション番号
 - 1..49,62..254
 - ニーモニック
 - 主なニーモニック

router	3
dns	6
hostname	12
domain	15
wins_server	44

- [初期値]: -
- *value*: オプション値
 - [設定値]:
 - 値としては以下の種類があり、どれが使えるかはオプション番号で決まる。例えば、'router','dns','wins_server' は IP アドレスの配列であり、'hostname','domain' は文字列である。

1 オクテット整数	0..255
2 オクテット整数	0..65535
2 オクテット整数の配列	2 オクテット整数をコンマ (,) で並べたもの
4 オクテット整数	0..2147483647
IP アドレス	IP アドレス

IP アドレスの配列	IP アドレスをコンマ (,) で並べたもの
文字列	文字列
スイッチ	"on","off","1","0" のいずれか
バイナリ	2 桁十六進数をコンマ (,) で並べたもの

- [初期値]:-

[説明]

スコープに対して送信する DHCP オプションを設定する。**dns server** コマンドや **wins server** コマンドなどでも暗黙のうちに DHCP オプションを送信していたが、それを明示的に指定できる。また、暗黙の DHCP オプションではスコープでオプションの値を変更することはできないが、このコマンドを使えばそれも可能になる。

[ノート]

no dhcp scope コマンドでスコープが削除されるとオプションの設定もすべて消える。

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、使用すべきではない。

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。

8.1.11 インターフェース毎の DHCP の動作の設定**[書式]**

```
ip interface dhcp service type
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
 - [初期値]: -
- *type*
 - [設定値]:

設定値	説明
off	DHCP サーバーとして機能しない
server	DHCP サーバーとして機能させる

- [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。

off に設定した場合には、DHCP サーバーとして動作しない。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。

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。

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。

9.1.3 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。

9.1.4 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。

9.1.5 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。

9.1.6 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。

9.1.7 受信した ICMP のログを記録するか否かの設定

[書式]

```
ip icmp log log
no ip icmp log [log]
```

[設定値及び初期値]

- *log*
- [設定値] :

設定値	説明
on	記録する
off	記録しない

- [初期値] : off

[説明]

受信した ICMP を debug タイプのログに記録するか否かを設定する。

9.1.8 ステルス機能の設定

[書式]

```
ip stealth all
ip stealth interface [interface...]
no ip stealth [...]
```

[設定値及び初期値]

- *all* : すべての論理インタフェースからのパケットに対してステルス動作を行う
 - [初期値] : -
- *interface*
 - [設定値] : 指定した論理インタフェースからのパケットに対してステルス動作を行う
 - [初期値] : -

[説明]

このコマンドを設定すると、指定されたインタフェースから自分宛に来たパケットが原因で発生する ICMP および TCP リセットを返さないようになる。

自分がサポートしていないプロトコルや IPv6 ヘッダ、あるいはオープンしていない TCP/UDP ポートに対して指定されたインタフェースからパケットを受信した時に、通常であれば ICMP unreachable や TCP リセットを返送する。しかし、このコマンドを設定しておくそれを禁止することができ、ポートスキャナーなどによる攻撃を受けた時にルーターの存在を隠すことができる。

[ノート]

指定されたインタフェースからの PING にも答えなくなるので注意が必要である。

自分宛ではないパケットが原因で発生する ICMP はこのコマンドでは制御できない。それらを送信しないようにするには、`ip icmp *` コマンド群を用いる必要がある。

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。

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。

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。

9.2.4 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。

9.2.5 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。

9.2.6 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。

9.2.7 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。

9.2.8 ステルス機能の設定

[書式]

```
ipv6 stealth all
ipv6 stealth interface [interface...]
no ipv6 stealth [...]
```

[設定値及び初期値]

- *all*: すべての論理インタフェースからのパケットに対してステルス動作を行う
 - [初期値]: -
- *interface*
 - [設定値]: 指定した論理インタフェースからのパケットに対してステルス動作を行う
 - [初期値]: -

[説明]

このコマンドを設定すると、指定されたインタフェースから自分宛にきたパケットが原因で発生する ICMP および TCP リセットを返さないようになる。

自分がサポートしていないプロトコルや IPv6 ヘッダ、あるいはオープンしていない TCP/UDP ポートに対して指定されたインタフェースからパケットを受信した時に、通常であれば ICMP unreachable や TCP リセットを返送する。しかし、このコマンドを設定しておくことでそれを禁止することができ、ポートスキャナーなどによる攻撃を受けた時にルーターの存在を隠すことができる。

[ノート]

指定されたインタフェースからの PING にも答えなくなるので注意が必要である。

自分宛ではないパケットが原因で発生する ICMP はこのコマンドでは制御できない。それらを送信しないようにするには、**ipv6 icmp *** コマンド群を用いる必要がある。

第 10 章

SNMP の設定

SNMP (Simple Network Management Protocol) の設定を行うことにより、SNMP 管理ソフトウェアに対してネットワーク管理情報のモニタと変更を行うことができますようになります。このとき YSL-V810 は SNMP エージェントとなります。

YSL-V810 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。

YSL-V810 の状態を通知する SNMP メッセージをトラップと呼びます。YSL-V810 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。

10.1 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。

10.2 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。

10.3 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。

10.4 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。

10.5 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。

10.6 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。

10.7 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。

10.8 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。

10.9 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。

10.10 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。

10.11 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 (00a0deXXXXXX)

[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。

10.12 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。

10.13 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。

10.14 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。

10.15 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
```

10.16 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
<code>view_id</code>	読み出し可能なアクセス権を設定するビュー番号
<code>none</code>	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
<code>view_id</code>	書き込み可能なアクセス権を設定するビュー番号
<code>none</code>	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。

10.17 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
<code>trap</code>	トラップを送信する
<code>inform</code>	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。

10.18 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。

10.19 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"
```

10.20 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"
```

10.21 sysName の設定

[書式]

```
snmp sysname name
no snmp sysname
```

[設定値及び初期値]

- *name*
 - [設定値]: sysName として登録する名称 (255 文字以内)
 - [初期値]: -

[説明]

MIB 変数 sysName を設定する。空白を含ませるためには、パラメータ全体をダブルクォート (")、もしくはシングルクォート (') で囲む。

sysName は一般的に、機器の名称を記入しておく変数である。

[設定例]

```
# snmp sysname "RTX3000 with BRI module"
```

10.22 SNMP 標準トラップを送信するか否かの設定

[書式]

```
snmp trap enable snmp trap [trap...]
snmp trap enable snmp all
no snmp trap enable snmp
```

[設定値及び初期値]

- *trap*: 標準トラップの種類
 - [設定値]:

設定値	説明
coldstart	全設定初期化時
warmstart	再起動時
linkdown	リンクダウン時
linkup	リンクアップ時
authenticationfailure	認証失敗時

- [初期値]: -
- *all*: 全ての標準トラップを送信する
 - [初期値]: -

[初期設定]

```
snmp trap enable snmp all
```

[説明]

SNMP 標準トラップを送信するか否かを設定する。

all を設定した場合には、すべての標準トラップを送信する。個別にトラップを設定した場合には、設定されたトラップだけが送信される。

[ノート]

authenticationFailure トラップを送信するか否かはこのコマンドによって制御される。

coldStart トラップは、電源投入、再投入による起動後およびファームウェアリビジョンアップによる再起動後に *coldStart* トラップを送信する。

linkDown トラップは、**snmp trap send linkdown** コマンドによってインタ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。

10.23 SNMP の linkDown トラップの送信制御の設定

[書式]

```
snmp trap send linkdown interface switch
no snmp trap send linkdown 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]: -
- *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。

10.24 LAN インタフェースの各ポートのリンクが up/down したときにトラップを送信するか否かの設定

[書式]

```
snmp trap link-updown separate-l2switch-port interface switch
no snmp trap link-updown separate-l2switch-port interface
```

[設定値及び初期値]

- *interface*: インタフェース (現状では 'lan1' のみ設定可能)
 - [設定値]:
 - lan1
 - [初期値]: -
- *switch*
 - [設定値]:

設定値	説明
on	トラップを送信する
off	トラップを送信しない

- [初期値]: off

[説明]

各ポートのリンクが up/down したときにトラップを送信するか否かを設定する。

第 11 章

DNS の設定

本機は、DNS(Domain Name Service) 機能として名前解決、上位 DNS サーバーの選択機能、簡易 DNS サーバー機能 (静的 DNS レコードの登録) を持ちます。

名前解決の機能としては、**ping** や **traceroute**、**rdate**、**ntpdate**、**telnet** コマンドなどの IP アドレスパラメータの代わりに名前を指定したり、SYSLOG などの表示機能において IP アドレスを名前解決したりします。

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

11.1 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。

11.2 DNS サーバーの IP アドレスの設定

[書式]

```
dns server ip_address [ip_address...]
no dns server [ip_address...]
```

[設定値及び初期値]

- *ip_address*
- [設定値]: DNS サーバーの IP アドレス (空白で区切って最大 4 ヶ所まで設定可能)
- [初期値]: -

[説明]

DNS サーバーの IP アドレスを指定する。

この IP アドレスはルーターが DHCP サーバーとして機能する場合に DHCP クライアントに通知するためや、IPCP の MS 拡張オプションで相手に通知するためにも使用される。

他のコマンドでも DNS サーバーが設定されている場合は、最も優先順位の高いコマンドの設定が使用される。DNS サーバーを設定する各種コマンドの優先順位は、本章冒頭の説明を参照。

11.3 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。

11.4 SYSLOG 表示で DNS により名前解決するか否かの設定

[書式]

```
dns syslog resolv resolv
```

```
no dns syslog resolv [resolv]
```

[設定値及び初期値]

- *resolv*
 - [設定値]:

設定値	説明
on	解決する
off	解決しない

- [初期値]: off

[説明]

SYSLOG 表示で DNS により名前解決するか否かを設定する。

11.5 DNS 問い合わせの内容に応じた DNS サーバーの選択

[書式]

```
dns server select id server [server2] [type] query [original-sender]
```

```
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

設定値	説明
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</i> [/ <i>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]: -

[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。

11.6 静的 DNS レコードの登録

[書式]

```
ip host fqdn value [ttl=ttl]
dns static type name value [ttl=ttl]
no ip host fqdn [value]
no dns static type name [value]
```

[設定値及び初期値]

- *type*: 名前のタイプ
- [設定値]:

設定値	説明
a	ホストの IPv4 アドレス
aaaa	ホストの IPv6 アドレス
ptr	IP アドレスの逆引き用のポインタ
mx	メールサーバー

設定値	説明
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
```

11.7 DNS 問い合わせパケットの始点ポート番号の設定

[書式]

```
dns srcport port[port]
no dns srcport [port-[port]]
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号 (1..65535)
 - [初期値]:
 - 10000-10999

[説明]

YSL-V810 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ことを考慮しておく必要がある。

11.8 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]

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。

11.9 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、YSL-V810 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 YSL-V810 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。

YSL-V810 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。YSL-V810 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 YSL-V810 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。

11.10 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、YSL-V810 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。

11.11 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 YSL-V810 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。YSL-V810 自身が問い合わせる場合、IPv4 を優先するか IPv6 を優先するかは機能ごとにまちまちであった。具体的には、以下の機能では DNS フォールバック動作では IPv6 が優先されるが、その他の機能では IPv4 が優先されている。

- HTTP リビジョンアップ機能
- HTTP アップロード機能

このコマンドを on に設定すると、YSL-V810 のすべての機能で IPv6 が優先されるようになる。

[ノート]

DNS リカーシブサーバーとして、LAN 内の PC 等の問い合わせを上位の DNS サーバーに転送する際には、PC 等の問い合わせ内容をそのまま上位サーバーに転送するため、DNS フォールバックの動作も PC 等の実装がそのまま反映され、このコマンドの設定には影響を受けない。

第 12 章

IPv6

12.1 共通の設定

12.1.1 IPv6 インタフェースのリンク MTU の設定

[書式]

```
ipv6 interface mtu mtu
no ipv6 interface mtu [mtu]
```

[設定値及び初期値]

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

[説明]

IPv6 インタフェースの MTU の値を設定する

12.1.2 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
no ipv6 interface 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。

12.1.3 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

設定値	説明
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。

12.2 IPv6 アドレスの管理

12.2.1 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 proxy
no ipv6 interface address ipv6_address/prefix_len [address_type]
no ipv6 interface address auto
no ipv6 interface 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
 - [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]: -
- *proxy*: プロキシ
 - [設定値]:
 - *prefix_type@prefix_interface*[*interface_id/prefix_len*]
 - *prefix_type*

設定値	説明
ra-prefix	RA プロキシ

- *prefix_interface*

設定値	説明
<i>prefix_interface</i>	転送元のインタフェース名

- *interface_id*

設定値	説明
<i>interface_id</i>	インタフェース ID

- *prefix_len*

設定値	説明
<i>prefix_len</i>	IPv6 プレフィックス長

- [初期値]: -

[説明]

インタフェースに IPv6 アドレスを付与する。

[ノート]

このコマンドで付与したアドレスは、**show ipv6 address** コマンドで確認することができる。
 複数の LAN インタフェースでアドレスを自動で設定する機能を利用することができる。
 具体的には、RA で取得したプレフィックスとインタフェース ID から IPv6 アドレスを生成する機能が利用できる。
 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*、*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。

[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
```

12.2.2 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
no ipv6 interface prefix ipv6_prefix/prefix_len
no ipv6 interface prefix proxy
```

[設定値及び初期値]

- *interface*
 - [設定値]: LAN 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]*
 - *prefix_type*

設定値	説明
ra-prefix	RA プロキシ

- *prefix_interface*

設定値	説明
<i>prefix_interface</i>	転送元のインタフェース名

- *interface_id*

設定値	説明
<i>interface_id</i>	インタフェース ID

- *prefix_len*

設定値	説明
<i>prefix_len</i>	IPv6 プレフィックス長

- [初期値]: -

[説明]

インタフェースに IPv6 アドレスを付与する。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。

[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
```

12.2.3 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
no ipv6 interface 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
 - [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。

12.2.4 DAD(Duplicate Address Detection) の送信回数の設定**[書式]**

```
ipv6 interface dad retry count count
no ipv6 interface 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
 - [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。

12.2.5 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。

12.2.6 始点 IPv6 アドレスを選択する規則の設定**[書式]**

```
ipv6 source address selection rule rule
no ipv6 source address selection rule [rule]
```

[設定値及び初期値]

- *rule*: 始点 IPv6 アドレスを選択する規則
 - [設定値]:

設定値	説明
prefix	プレフィックスの最長一致
lifetime	寿命の長い方を優先

- [初期値]: lifetime

[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。

12.3 経路制御**12.3.1 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
 - 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
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。LAN インタフェースが複数ある機種ではスコープ識別子でインタフェースを指定する必要がある。インタフェースに対応するスコープ識別子は **show ipv6 address** コマンドで表示される。LAN インタフェースがひとつである機種に関しては、スコープ識別子が省略されると LAN1 が指定されたものとして扱う。

なお LOOPBACK インタフェース、NULL インタフェースは常にアップ状態なので、hide オプションは指定はできないものの意味はない。

12.4 RIPng

12.4.1 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。

12.4.2 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
no ipv6 interface 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。

12.4.3 RIPng の加算ホップ数の設定**[書式]**

```
ipv6 interface rip hop direction hop
no ipv6 interface rip hop direction
```

[設定値及び初期値]

- *direction*
 - [設定値]:

設定値	説明
in	受信時に加算する
out	送信時に加算する

- [初期値]: -
- *hop*
 - [設定値]: 加算ホップ数 (0..15)
 - [初期値]: 0

[説明]

PP インタ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。

12.4.4 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...]
no ipv6 interface 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。

12.4.5 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...]
no ipv6 interface 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。

12.4.6 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。スタティックなど複数のプロトコルで得られた経路が食い違う場合には、優先度が高い方が採用される。優先度が同じ場合には時間的に先に採用された経路が有効となる。

[ノート]

静的経路の優先度は 10000 で固定である。

12.5 VRRPv3 の設定

12.5.1 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電話帳サーバーの間では、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 電話帳サーバ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。

12.5.2 シャットダウントリガの設定

[書式]

```
ipv6 interface vrrp shutdown trigger vrid sip-proxy
ipv6 interface vrrp shutdown trigger vrid ip keepalive number
no ipv6 interface vrrp shutdown trigger vrid sip-proxy
no ipv6 interface vrrp shutdown trigger vrid $ip keepalive number
```

[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]: -
- *number*
 - [設定値]: **ip keepalive** 設定の番号
 - [初期値]: -

[説明]

設定した VRRPv3 グループでマス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
sip-proxy	電話帳サーバーとしての動作に問題が発生した場合
ip keepalive	ip keepalive 設定によりダウンが検出された場合

[ノート]

電話帳サーバー動作において、sip-proxy のシャットダウントリガが発生するのは、SIP 動作自己診断において異常を検出した場合である。

12.6 フィルタの設定

12.6.1 IPv6 フィルタの定義

[書式]

```
ipv6 filter filter_num pass_reject src_addr[/prefix_len] [dest_addr[/prefix_len] [protocol [src_port_list [dest_port_list]]]]
no ipv6 filter filter_num [pass_reject]
```

[設定値及び初期値]

- *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

12.6.2 IPv6 フィルタの適用

[書式]

```
ipv6 interface secure filter direction [filter_list...] [dynamic filter_list]
no ipv6 interface 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
 - [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。

12.6.3 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]:
 - tcp/udp/ftp/tftp/domain/www/smtp/pop3/telnet
 - echo/discard/daytime/chargen/ftp/ssh/telnet/smtp/time/whois/dns/domain/dhcps/
 - dhcpc/tftp/gopher/finger/http/www/pop3/sunrpc/ident/nntp/ntp/ms-rpc/
 - netbios_ns/netbios_dgm/netbios_ssn/imap/snmp/snmptrap/bgp/imap3/ldap/
 - https/ms-ds/ike/rlogin/rwho/rsh/syslog/printer/rip/ripng/
 - dhcpv6c/dhcpv6s/ms-sql/radius/l2tp/pptp/nfs/msblast/ipsec-nat-t/sip/
 - ping/ping6/tcp/udp
 - [初期値]: -
- *filter_list*
 - [設定値]: **ipv6 filter** コマンドで登録されたフィルタ番号のリスト
 - [初期値]: -
- *option*
 - [設定値]:
 - syslog=*switch*

設定値	説明
on	コネクションの通信履歴を syslog に残す
off	コネクションの通信履歴を syslog に残さない

- `timeout=time`

設定値	説明
time	データが流れなくなったときにコネクション情報を解放するまでの秒数

- [初期値]:
 - `syslog=on`
 - `timeout=60`

[説明]

IPv6 の動的フィルタを定義する。第 1 書式では、あらかじめルーターに登録されているアプリケーション名を指定する。第 2 書式では、ユーザがアクセス制御のルールを記述する。キーワードの `filter`、`in`、`out` の後には、**ipv6 filter** コマンドで定義されたフィルタ番号を設定する。

`filter` キーワードの後に記述されたフィルタに該当するコネクション (トリガ) を検出したら、それ以降 `in` キーワードと `out` キーワードの後に記述されたフィルタに該当するコネクションを通過させる。`in` キーワードはトリガの方向に対して逆方向のアクセスを制御し、`out` キーワードは動的フィルタと同じ方向のアクセスを制御する。なお、**ipv6 filter** コマンドの IP アドレスは無視される。`pass/reject` の引数も同様に無視される。

ここに記載されていないアプリケーションについては、`filter` キーワードを使って定義することで扱える可能性がある。特に `snmp` のように動的にポート番号が変化しないプロトコルの扱いは容易である。

`tcp` か `udp` を設定することで扱える可能性がある。特に、`telnet` のように動的にポート番号が変化しないプロトコルは `tcp` を指定することで扱うことができる。

12.7 近隣要請

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

- [初期値]: `na-proxy=all`

[初期設定]

```
ipv6 nd ns-trigger-dad off
```

[説明]

RA プロキシにおいて、下流よりアドレス重複チェックの近隣要請を受信した際に、そのグローバルアドレスを送信元とした近隣要請を上流に送信するか否かを設定する。

第 13 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。

13.1 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。

13.2 SMTP メールサーバーの設定

[書式]

mail server smtp *id address [port=port] [smtp-auth username password [auth_protocol]] [pop-before-smtp]*

no mail server smtp *id [...]*

[設定値及び初期値]

- *id*
 - [設定値]: メールサーバー設定 ID (1..10)
 - [初期値]: -
- *address*
 - [設定値]: サーバーの IP アドレスまたはホスト名
 - [初期値]: -
- *port*
 - [設定値]: サーバーのポート番号 (省略時は 25)
 - [初期値]: -
- *username*
 - [設定値]: 認証用ユーザ名
 - [初期値]: -
- *password*
 - [設定値]: 認証用パスワード
 - [初期値]: -
- *auth_protocol*: SMTP-AUTH 認証プロトコル
 - [設定値]:

設定値	説明
cram-md5	CRAM-MD5
digest-md5	DIGEST-MD5
plain	PLAIN 認証

- [初期値]: -

- `pop-before-smtp`
 - [設定値]: POP before SMTP の使用
 - [初期値]: -

[説明]

メール送信に使用するサーバー情報を設定する。

`smtp-auth` パラメータでは、メール送信の際の SMTP 認証のためのデータ (ユーザ名、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。

13.3 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。

13.4 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。

13.5 メール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]: -
- *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。Rev.8.03 系のすべてのリビジョンで使用可能。

[表示例]

```
mail template 1 1 From:test@test.com To:test1@test.com,test2@test.com
"Subject:Test Mail" notify-log=on
mail template 1 2 From:test@test.com To:test1@test.com
"Subject:RTX1500 test" "Date:Mon, 23 Feb 2004 09:54:20 +0900"
MIME-Version:1.0 "Content-Type:text/plain; charset=iso-2022-jp"
```

13.6 メール通知のトリガの設定

[書式]

- mail notify** *id template_id* trigger sip level=*level* [packet-log=*sw*]
- mail notify** *id template_id* trigger sip-proxy-redundancy
- 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]: -
- *level*
 - [設定値]: 障害度レベル (1..5)
 - [初期値]: -
- *sw*: SIP の詳細なログを通知するか設定する。
 - [設定値]:

設定値	説明
on	SIP の詳細なログを通知する
off	SIP の詳細なログを通知しない

- [初期値]: off
- *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
firewall	ファイアウォールの情報

設定値	説明
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
lanN	LAN 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)
- [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]

障害時にメール通知を行う条件の設定を行う。

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。

一つのテンプレート ID に異なる設定が入力された場合は、設定を有効にする方を優先する。

(例えば同一のテンプレート ID に `packet_log=on` と `packet_log=off` が設定された場合は `on` の設定が優先される)

障害度レベルを設定すると、設定した障害度レベル以上の障害に関する情報を通知する。障害度レベルは以下の 5 段階。

		拠点障害内容	電話帳サーバー障害内容
1	一時的に使用不可	ビジー (486)	ビジー (486)
2	操作ミス	ダイヤル操作ミス (404)	ダイヤル操作ミス (404)
3	設定ミス	-	4xx 系のエラーを返す場合 (404, 408, 486 は除く)
4	拠点が使用不可	エラーレスポンスを返す場合、 487,422 は除く Register の expires が満了した場合	408 エラーを返す場合 再送エラーを検知した場合
5	システム全体が使用不可	-	5xx,6xx 系のエラーを返す場合

`packet-log=on` を指定した場合は、SIP の詳細なパケットログ情報をファイルで添付する。電話帳サーバーにおいて保存されるパケットログの保存方法は、**sip packet-log** コマンドで設定された方法になる。

`sip-proxy-redundancy` を指定した場合は、冗長構成のセカンダリーサーバーにおいて、動作状態の変化に応じたメール通知が行われる。

メール通知の行うトリガ動作の設定を行う。**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。

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 sip level=3 packet_log=on
mail notify 2 3 trigger sip-proxy-redundancy
mail notify 4 1 trigger status all
mail notify 5 1 trigger intrusion lan1 in/out pp * in tunnel 1-3,5 out
```

13.7 パケットログ情報の保存方法の設定

[書式]

sip packet-log level=*level* mode

no sip packet-log level=*level*

[設定値及び初期値]

- *level*
 - [設定値]: 障害度レベル (1..5)
 - [初期値]: -
- *mode*
 - [設定値]:

設定値	説明
overwrite	上書き可能
write-once	空き領域のみ書き込み可能

- [初期値]: overwrite

[説明]

パケットログ情報の保存方法を設定する。

パケットログ情報は、**mail notify** コマンドで **packet-log=on** と設定した場合に保存する。

第 14 章

HTTP サーバー機能

14.1 共通の設定

14.1.1 HTTP サーバー機能の有無の設定

[書式]

```
httpd service switch
no httpd service
```

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
on	HTTP サーバー機能を有効にする
off	HTTP サーバー機能を無効にする

- [初期値]: on

[説明]

HTTP サーバーを有効にするか否かを選択する。

14.1.2 HTTP サーバーへアクセスできるホストの設定

[書式]

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

[設定値及び初期値]

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

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

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

[説明]

HTTP サーバーへのアクセスを許可するホストを設定する。

[ノート]

このコマンドで LAN インターフェースを指定した場合には、ネットワークアドレスとリミテッドブロードキャストアドレスを除く IP アドレスからのアクセスを許可する。指定した LAN インターフェースにプライマリアドレスもセカンダリアドレスも設定していなければ、アクセスを許可しない。

14.1.3 HTTP サーバーのセッションタイムアウト時間の設定

[書式]

```
httpd timeout time  
no httpd timeout [time]
```

[設定値及び初期値]

- *time*
 - [設定値]: 秒数 (1..180)
 - [初期値]: 5

[説明]

HTTP サーバーのタイムアウト時間を設定する。

[ノート]

インターネット経由で本装置にアクセスするときに、通信タイムアウトが発生するならば、このコマンドで大きな値を設定する。

14.1.4 HTTP サーバー機能の listen ポートの設定

[書式]

```
httpd listen port  
no httpd listen
```

[設定値及び初期値]

- *port*
 - [設定値]: ポート番号 (1..65535)
 - [初期値]: 80

[説明]

HTTP サーバーの待ち受けるポートを設定する。

14.1.5 設定・管理ページで表示する装置名称の設定

[書式]

```
httpd sysname name  
no httpd sysname
```

[設定値及び初期値]

- *name*
 - [設定値]: 設定・管理ページで表示する装置名称
 - [初期値]: -

[説明]

設定・管理ページで表示する装置名称を設定します。

第 15 章

スケジュール

15.1 スケジュールの設定

[書式]

```
schedule at id [date] time * command...
```

```
no schedule at id [[date]...]
```

[設定値及び初期値]

- *id*
 - [設定値]: スケジュール番号
 - [初期値]: -
- *date*: 日付 (省略可)
 - [設定値]:
 - 月/日
 - 省略時は */* とみなす

月の設定例	設定内容
1,2	1月と2月
2-	2月から12月まで
2-7	2月から7月まで
-7	1月から7月まで
*	毎月

日の設定例	設定内容
1	1日のみ
1,2	1日と2日
2-	2日から月末まで
2-7	2日から7日まで
-7	1日から7日まで
mon	月曜日のみ
sat,sun	土曜日と日曜日
mon-fri	月曜日から金曜日
-fri	日曜日から金曜日
*	毎日

- [初期値]: -
- *time*: 時刻
- [設定値]:

設定値	説明
hh:mm[:ss]	時 (0..23 または *): 分 (0..59 または *): 秒 (0..59)、秒は省略可
startup	起動時
usb-attached	USB デバイス認識時
sd-attached	microSD デバイス認識時

- [初期値]: -
- *command*
 - [設定値]: 実行するコマンド (制限あり)

- [初期値]:-

[説明]

time で指定した時刻に *command* で指定されたコマンドを実行する。

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**、**cold start**、**console info** と **console prompt** を除く **console** で始まるコマンド、**copy**、**copy exec**、**date**、**delete**、**exit**、**external-memory performance-test go**、**help**、**http revision-up go**、**http revision-up schedule**、**interface reset**、**less** で始まるコマンド、**login password**、**login password encrypted**、**login timer**、**login user**、**luac**、**make directory**、**nslookup**、**packetdump**、**ping**、**ping6**、**quit**、**rename**、**rtfs format**、**rtfs garbage collect**、**save**、**schedule at**、**scp**、**show** で始まるコマンド、**ssh**、**sshd host key generate**、**sshd session**、**system packet-buffer**、**telnet**、**telnetd session**、**time**、**timezone**、**traceroute**、**traceroute6**、**user attribute**

[ノート]

入力時、*command* パラメータに対して TAB キーによるコマンド補完は行いが、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]

- 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
```

第 16 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 YSL-V810 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。

16.1 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。

16.2 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]: 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。

第 17 章

外部メモリ機能

本機能は、YSL-V810 本体へ外部メモリ (USB メモリ、microSD カード) を接続することにより、YSL-V810 と外部メモリ間で各種データの操作を行います。

使用できる外部メモリは機種によって異なります。

本機能により、以下の動作が可能となります。

- コマンド設定、あるいは実行コマンドによる動作
 - 外部メモリへ SYSLOG メッセージを出力する。
 - 外部メモリへ設定ファイルをコピーする。
 - 外部メモリから設定ファイルをコピーする。
 - 外部メモリからファームウェアファイルをコピーする。
 - 外部メモリへ 監視情報を出力する。
- YSL-V810 本体の外部メモリボタンおよび DOWNLOAD ボタンの操作による動作
 - 外部メモリボタンと DOWNLOAD ボタンを同時に 3 秒以上押し続け、外部メモリから設定ファイルおよびファームウェアファイルをコピーする。
- 外部メモリからの起動
- バッチファイル実行機能

バッチファイル実行機能

外部メモリの中に、コマンドを羅列したファイル (バッチファイルと呼びます) を入れておき、そのファイルに記述されたコマンドを実行する機能です。

設定によって DOWNLOAD ボタンを押して実行させることができます。コンソールでの **execute batch** コマンドによって実行することもできます。

コマンドの実行結果やログは、ファイルとして外部メモリに書き出します。

本機能を用いると、PC がない環境でも PING での疎通確認などを行うことができます。例えばルーターの設置作業時に、必要な装置や作業手順を大幅に減らすことができます。実行結果や設定内容、YSL-V810 の状態などは、外部メモリにファイルとして書き出されます。書き出されたファイルは、外部メモリを取り出して携帯電話で確認することができます。作業ログとして利用することもできます。

本機能に関する技術情報は以下に示す URL で公開されています。

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

17.1 USB ホスト機能を使うか否かの設定

[書式]

usbhost use switch

no usbhost use [switch]

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	USB ホスト機能を使用する
off	USB ホスト機能を使用しない

- [初期値]: on

[説明]

USB ホスト機能を使用するか否かを設定する。

このコマンドが **off** に設定されているときは USB メモリをルーターに接続しても認識されない。

また、過電流により USB ホスト機能に障害が発生した場合、USB メモリが接続されていない状態で本コマンドを再設定すると復旧させることができる。

17.2 USB バスで過電流保護機能が働くまでの時間の設定

[書式]

```
usbhost overcurrent duration duration
no usbhost overcurrent duration [duration]
```

[設定値及び初期値]

- *duration*
 - [設定値]: 時間 (5..100、1 単位が 10 ミリ秒)
 - [初期値]: 5 (50 ミリ秒)

[説明]

過電流保護機能が働くまでの時間を設定する。ここで設定した時間、連続して過電流が検出されたら、過電流保護機能が働く。

17.3 microSD カードスロットを使うか否かの設定

[書式]

```
sd use switch
no sd use [switch]
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	microSD カードスロットを使用する
off	microSD カードスロットを使用しない

- [初期値]: on

[説明]

microSD カードスロットを使用するか否かを設定する。このコマンドが off に設定されているときは microSD カードをカードスロットに差し込んでも認識されない。

17.4 外部メモリ用キャッシュメモリの動作モードの設定

[書式]

```
external-memory cache mode mode
no external-memory cache mode [mode]
```

[設定値及び初期値]

- *mode*
 - [設定値]:

設定値	説明
write-through	ライトスルーモード
copy-back1	コピーバックモード 1
copy-back2	コピーバックモード 2

- [初期値]: copy-back1

[説明]

外部メモリ用キャッシュメモリの動作モードを設定する。ライトスルーモード、コピーバックモード 1、及びコピーバックモード 2 の 3 種類の動作モードをサポートしており、各モードによって FAT、DIR、FILE の各キャッシュ上のデータを外部メモリへ書き出すタイミングが異なる。

各動作モードについて、以下に説明する。

write-through を指定した場合、FAT、DIR、FILE に割り当てられていたキャッシュは、ライトスルーモードで動作し、常に外部メモリへ書き出される。最も安全性が高い。

copy-back1 を指定した場合、FAT と DIR キャッシュはコピーバックモードで動作し、FILE キャッシュは、ライトスルーモードで動作する。ライトスルーモードより高速に動作させることができる。

copy-back2 を指定した場合、FAT、DIR、FILE キャッシュがコピーバックモードで動作する。この設定では、外部メモリへの書き出しが抑制されるので、最も高速に動作する。しかし、外部メモリへ書き出しが完了していない状態が続く為、予期しない電源断が発生すると外部メモリのファイルシステムがダメージを受ける可能性が高くなる。

FAT : File Allocation Table の略

DIR : Directory Entry の略

[ノート]

本コマンドの変更は、外部メモリを接続した時に反映される。外部メモリが既に接続されている状態でコマンドを入力した場合は、一旦、取り外した後に再接続する必要がある。

17.5 ファイルアクセス高速化用キャッシュメモリのサイズの設定

[書式]

external-memory accelerator cache size interface size

no external-memory accelerator cache size interface [size]

[設定値及び初期値]

- *interface*

- [設定値]:

設定値	説明
usb1	USB ポート 1
sd1	microSD カードスロット

- [初期値]: -

- *size*

- [設定値]:

設定値	説明
1-5	キャッシュメモリのサイズ (数値が大きいほどメモリサイズが大きい)
off	ファイルアクセス高速化機構を使用しない

- [初期値]: 1

[説明]

ファイルアクセスを高速化するために使用するキャッシュメモリのサイズを設定する。

size に数値を指定した場合は、ファイルアクセスを高速化するための機構が働き、特にディレクトリ数やファイル数の多い構成での外部メモリへのアクセス性能が向上する。アクセス性能が向上しない場合は、*size* を大きくすることで向上することがある。ただし、*size* が大きいほど、外部メモリを接続してから使用可能になるまでの時間が長くなる可能性がある。

size に off を指定した場合は、ファイルアクセスを高速化するためのキャッシュメモリは確保されない。

なお、すべてのインタフェースに対して *size* に最大値を設定した状態で、同時にすべてのインタフェースに外部メモリを接続して使用すると、システム全体の性能に影響を与える可能性があるため、本コマンドを設定してファイルアクセスを高速化するインタフェースは一つに限定することを推奨する。

[ノート]

本コマンドの変更は、外部メモリを接続した時に反映される。外部メモリが既に接続されている状態でコマンドを入力した場合は、一旦、取り外した後に再接続する必要がある。

また、本コマンドで、*size* を大きくしてもアクセス性能が向上しない場合は、下記に示す操作を行うことで、改善されることがある。

- 可能であれば、外部メモリ内のディレクトリやファイルを減らす
- 外部メモリ内の総ディレクトリ数を 2,000 個以内となるように調整する
- 頻繁にアクセスするディレクトリ内の総ファイル数 (ディレクトリ含む) を 20,000 個以内となるように調整する
- ファイル名やディレクトリ名をなるべく短くする (32 文字以内を推奨)

17.6 外部メモリに保存する SYSLOG ファイル名の指定

[書式]

external-memory syslog filename name [crypto password] [limit=size] [backup=num] [interval=interval] [line=line]

no external-memory syslog filename [name]

[設定値及び初期値]

- *name* : SYSLOG ファイル名

- [設定値] :

設定値	説明
<i>usb1:filename</i>	USB メモリ内のファイル名 (.bak 拡張子を含む名前は指定できない)
<i>sd1:filename</i>	microSD カード内のファイル名 (.bak 拡張子を含む名前は指定できない)

- [初期値] : -

- *crypto* : SYSLOG を暗号化して保存する場合の暗号アルゴリズムの選択

- [設定値] :

設定値	説明
aes128	AES128 で暗号化する
aes256	AES256 で暗号化する

- [初期値] : -

- *password*

- [設定値] : ASCII 文字列で表したパスワード (半角 8 文字以上、32 文字以内)

- [初期値] : -

- *size*

- [設定値] : SYSLOG ファイルの上限サイズ (1 - 1024 単位:MB)

- [初期値] : 10

- *num*

- [設定値] : バックアップファイルの上限数 (1 - 100)

- [初期値] : 10

- *interval*

- [設定値] : SYSLOG を外部メモリに書き出す間隔 (2 - 86400 単位:秒)

- [初期値] : 2

- *line*

- [設定値] : SYSLOG を外部メモリに書き出す行数 (1000 - 3000 単位:行)

- [初期値] : 1000

[説明]

外部メモリ内に保存する SYSLOG ファイル名を指定する。

name に .bak 拡張子を含むファイル名は指定できない。また、暗号化しない場合、*name* に .rtfg 拡張子を含むファイル名は指定できない。

crypto および *password* を指定した場合、SYSLOG は暗号化してから外部メモリに書き込まれる。暗号化する場合、*name* に .rtfg 拡張子を含めるか、拡張子を省略した名前を指定する必要がある。拡張子を省略した場合、自動的にファイル名に rtfg 拡張子が追加される。

SYSLOG ファイルが上限サイズに達すると、SYSLOG ファイルのバックアップが行われる。このとき作成されるバックアップファイルの名前はファームウェアによって異なる。

バックアップファイル名は *name* で指定されたファイル名の後にバックアップが行われた日時を表す `_yyyymmdd_hhmmss` 形式の文字列が付加されたものとなる。

- yyyy ... 西暦 (4 桁)
- mm ... 月 (2 桁)
- dd ... 日 (2 桁)
- hh ... 時 (2 桁)
- mm ... 分 (2 桁)
- ss ... 秒 (2 桁)

バックアップファイル数が *num* で指定される上限数に達した場合、もしくは外部メモリに空き容量がなくなった場合は、最も古いバックアップファイルを削除してから新しいバックアップファイルが作成される。

name に拡張子が含まれている場合

- 暗号化しないで保存する ... 拡張子を `.bak` に置き換える
- 暗号化して保存する ... 拡張子の前に `_bak` を追加する

name に拡張子が含まれていない場合 ... `.bak` という拡張子を追加する

interval で指定した時間が経過した場合、もしくは *line* で指定した行数だけ `SYSLOG` が出力された場合に、外部メモリに `SYSLOG` を書き出す。

本コマンドが設定されていないときは `SYSLOG` は外部メモリに書き込まれない。

[ノート]

以下の変更を行う場合、*name* を変更しなければならない。

- `SYSLOG` を暗号化しないで保存するから、暗号化して保存するに変更する場合
- `SYSLOG` を暗号化して保存するから、暗号化しないで保存するに変更する場合
- 暗号アルゴリズムまたは、パスワードを変更する場合

外部メモリに暗号化して保存したファイルは、PC 上で RT-FileGuard を使用して復号することができる。

name は半角 99 文字以内。

17.7 外部メモリボタンと **DOWNLOAD** ボタンの同時押下による設定ファイル、ファームウェアファイルのコピー操作を許可するか否かの設定

[書式]

`operation external-memory download permit switch`

`no operation external-memory download permit [switch]`

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
on	許可する
off	許可しない

- [初期値]: on

[説明]

外部メモリボタンと **DOWNLOAD** ボタンの同時押下による、設定ファイルとファームウェアファイルのコピー操作を許可するか否かを設定する。

17.8 外部メモリ内のファイルからの起動を許可するか否かの設定

[書式]

`external-memory boot permit switch`

`no external-memory boot permit [switch]`

[設定値及び初期値]

- *switch*
- [設定値]:

設定値	説明
on	許可する
off	許可しない

- [初期値]: on

[説明]

外部メモリ内のファイルからの起動を許可するか否かを設定する。この設定を `OFF` に設定すると外部メモリ内のファイルからの起動はできなくなる。

起動時に読み込む設定ファイルとファームウェアファイルの名前はそれぞれ、**external-memory config filename** コマンドと **external-memory exec filename** コマンドで設定できる。

17.9 ルーター起動時に外部メモリを検出するまでのタイムアウトを設定する

[書式]

external-memory boot timeout *time*

no external-memory boot timeout [*time*]

[設定値及び初期値]

- *time*
 - [設定値]: タイムアウト秒数 (1..30)
 - [初期値]: 1

[説明]

ルーター起動時に外部メモリを検出するまでのタイムアウト時間を設定する。

external-memory boot permit on コマンドによって、外部メモリ内のファイルからの起動を許可するに設定されている場合に有効である。

接続認識が遅いデバイスの場合、タイムアウト時間を大きくすることで認識されるようになることがある。

[ノート]

外部メモリ性能測定コマンドで、**boot device attach** で表示される時間を目安にして設定するとよい。

17.10 起動時、あるいは外部メモリボタンと DOWNLOAD ボタン同時押下により読み込まれる、ファームウェアファイル名の指定

[書式]

external-memory exec filename *from* [*to*]

external-memory exec filename off

no external-memory exec filename [*from*] [*to*]

no external-memory exec filename [off]

[設定値及び初期値]

- *from*: 外部メモリとファームウェアファイル名
 - [設定値]:

設定値	説明
usb1: <i>filename</i>	USB メモリ内のファームウェアファイル名
sd1: <i>filename</i>	microSD カード内のファームウェアファイル名
*: <i>filename</i>	USB メモリおよび microSD カード内のファームウェアファイル名

- [初期値]:
 - *:v810.bin
- *to*: コピー先ファイル名
 - [設定値]:

設定値	説明
0~1	内蔵フラッシュ ROM の実行形式ファームウェアファイル番号 (省略時は 0)

- [初期値]: 0

[説明]

外部メモリを差して起動した時、あるいは外部メモリボタンと DOWNLOAD ボタンを同時に押下した時に読み込まれる、外部メモリ上のファームウェアファイル名を指定する。

外部メモリボタンと DOWNLOAD ボタンを同時に押下した時は、ファームウェアファイルは内蔵フラッシュ ROM にコピーされるが、その時のコピー先の内蔵フラッシュ ROM のファームウェアファイル番号も指定できる。

外部メモリに "*" を指定した場合、指定するファイルの検索はまず microSD カードから行われ、指定したファイルがなければ USB メモリが検索される。ボタン操作の場合は該当するボタンの外部メモリだけがファイル検索の対象となる。

filename は絶対パスを使って指定するかファイル名のみを指定する。ファイル名のみを指定した場合は指定された外部メモリ内から検索される。

検索の結果複数のファイルが該当する場合、ディレクトリ階層上最もルートディレクトリに近く、アルファベット順に先のディレクトリにあるファイルが選ばれる。

off に指定した場合、ファームウェアファイルの検索と読み込みを行わない。

[ノート]

外部メモリのディレクトリ構成やファイル数によっては、ファイルの検索に時間がかかることがある。

検索時間を短くするためには、階層の深いディレクトリの作成は避けてルートに近い位置にファイルを格納したり、ファイルを絶対パスで直接指定することが望ましい。

自動検索のタイムアウトの時間は **external-memory auto-search time** コマンドで設定できる。

filename は半角 99 文字以内。

[設定例]

- microSD カード内から "v810.bin" を検索し、ファームウェアファイルとして読み込む

```
# external-memory exec filename sd1:v810.bin
```

- microSD カード内のディレクトリ "test" から "v810.bin" を検索し、ファームウェアファイルとして読み込む

```
# external-memory exec filename sd1:/test/v810.bin
```

17.11 起動時、あるいは外部メモリボタンと DOWNLOAD ボタン同時押下により読み込まれる、設定ファイル名の指定

[書式]

```
external-memory config filename from [from] [to] [password]
```

```
external-memory config filename off
```

```
no external-memory config filename [from] [to] [password]
```

```
no external-memory config filename [off]
```

[設定値及び初期値]

- from* : 外部メモリと設定ファイル名
 - [設定値]:

設定値	説明
usb1: <i>filename</i>	USB メモリ内の設定ファイル名
sd1: <i>filename</i>	microSD カード内の設定ファイル名
*: <i>filename</i>	USB メモリおよび microSD カード内の設定ファイル名

- [初期値]:
 - *:config.rtf, *:config.txt
- to* : コピー先ファイル名
 - [設定値]:

設定値	説明
0~4	内蔵フラッシュ ROM の設定ファイル番号 (省略時は 0)

- [初期値]: 0
- password*
 - [設定値]: 復号パスワード (ASCII 文字列で半角 8 文字以上、32 文字以内)
 - [初期値]: -

[説明]

外部メモリを差して起動した時、あるいは外部メモリボタンと DOWNLOAD ボタンを同時に押下した時に読み込まれる、外部メモリ上の設定ファイル名を指定する。

また外部メモリボタンと DOWNLOAD ボタンを同時に押下した時は、設定ファイルは内蔵フラッシュ ROM にコピーされるが、その時のコピー先の内蔵フラッシュ ROM の設定ファイル番号も指定できる。

外部メモリに "*" を指定した場合、指定するファイルの検索はまず microSD カードから行われ、指定したファイルがなければ USB メモリが検索される。ボタン操作の場合は該当するボタンの外部メモリだけがファイル検索の対象となる。

filename は絶対パスを使って指定するかファイル名のみを指定する。ファイル名のみを指定した場合は指定された外部メモリ内から検索される。

検索の結果複数のファイルが該当する場合、ディレクトリ階層上最もルートディレクトリに近く、アルファベット順に先のディレクトリにあるファイルが選ばれる。

パスワードを指定して暗号化されている設定ファイルを復号して読み込む場合は、*password* に暗号化したときのパスワードを設定する。

off に指定した場合、設定ファイルの検索と読み込みを行わない。

[ノート]

外部メモリのディレクトリ構成やファイル数によっては、ファイルの検索に時間がかかることがある。

検索時間を短くするためには、階層の深いディレクトリの作成は避けてルートに近い位置にファイルを格納したり、ファイルを絶対パスで直接指定することが望ましい。

自動検索のタイムアウトの時間は **external-memory auto-search time** コマンドで設定できる。

外部メモリに暗号化して保存したファイルは、PC 上で RT-FileGuard を使用して復号することができる。

filename は半角 99 文字以内。

[設定例]

- microSD カード内から "config.txt" を検索し、設定ファイルとして読み込む

```
# external-memory config filename sd1:config.txt
```

- microSD カード内のディレクトリ "test" から "config.txt" を検索し、設定ファイルとして読み込む

```
# external-memory config filename sd1:/test/config.txt
```

17.12 ファイル検索時のタイムアウトを設定する

[書式]

```
external-memory auto-search time time
no external-memory auto-search time [time]
```

[設定値及び初期値]

- time*
 - [設定値]:
 - 秒数 (1..600)
 - [初期値]: 300

[説明]

外部メモリに格納されているファイルを検索する時のタイムアウト時間を設定する。

17.13 バッチファイルを実行する

[書式]

```
execute batch
```

[説明]

外部メモリのバッチファイルを実行する。実行されるバッチファイル名は **external-memory batch filename** コマンドで指定する。

[ノート]

実行中のバッチファイルを中断したい場合は Ctrl+C を入力する。

17.14 バッチファイルと実行結果ファイルの設定

[書式]

```
external-memory batch filename batchfile [logfile]
no external-memory batch filename [batchfile [logfile]]
```

[設定値及び初期値]

- batchfile*: バッチファイル名

- [設定値]:

設定値	説明
usb1:filename	USB メモリ内のバッチファイル名
sd1:filename	microSD カード内のバッチファイル名
*:filename	USB メモリおよび microSD カード内のバッチファイル名

- [初期値]:
 - *:command.txt

- logfile

- [設定値]:

設定値	説明
filename	実行結果ファイル名

- [初期値]: command-log.txt

[説明]

外部メモリ内のバッチファイル名と実行結果ファイル名を指定する。

外部メモリに "*" を指定した場合、指定するファイルの検索はまず microSD カードから行われ、指定したファイルがなければ USB メモリが検索される。

filename は絶対パスを使ってファイルを指定するかファイル名のみを指定する。バッチファイルの filename にファイル名のみを指定した場合は外部メモリ内から自動検索する。複数のファイルがある場合、ディレクトリ階層上最もルートディレクトリに近く、アルファベット順に先のディレクトリにあるファイルが選ばれる。

logfile を省略した場合、"バッチファイル名 -log.txt" という名前で実行結果ファイルが作成される。

[ノート]

batchfile に指定可能な文字数は logfile を指定した場合は、半角 99 文字以内。logfile を省略した場合は、拡張子を除いて半角 91 文字以内。filename に指定可能な文字数は半角 99 文字以内。

[設定例]

- microSD カードのファイルから "command_test.txt" をバッチファイルとして検索する。

```
# external-memory batch filename sd1:command_test.txt
```

- microSD カードのディレクトリ "test" から "command_test.txt" を読み込む。

```
# external-memory batch filename sd1:/test/command_test.txt
```

17.15 外部メモリ性能測定コマンド

[書式]

external-memory performance-test go interface

[設定値及び初期値]

- interface
 - [設定値]:

設定値	説明
usb1	USB インタフェース
sd1	microSD インタフェース

- [初期値]: -

[説明]

外部メモリ機能の使用に耐えうる性能を持つメモリであるか否かを確認する。

外部メモリの認識に要する時間やデータの読み書き速度を確認し、一連のテスト終了後、使用に耐えうる性能を持つと判断されれば、

- OK:succeeded

そうでないものは

- NG:failed

と表示する。

[ノート]

外部メモリはフォーマット直後の状態のものを対象とする。
本機能は他の機能を使用していない状態で実行する必要がある。

本コマンド実行中は **syslog debug on, no syslog host** が設定される。そのため、**syslog debug off** にしていても DEBUG タイプの SYSLOG が出力されることがある。また、**syslog host** コマンドを設定していても SYSLOG サーバーにログが転送されない。

YSL-V810 の外部メモリ機能を利用する際に外部メモリに求められる最低限の性能を確認するものであり、本機能の結果はその外部メモリの全ての動作を保証するものではない。
外部メモリ機能を使用する際は、**show status external-memory** コマンドで外部メモリへの書き込みエラーなどが発生していないことを定期的に確認することを推奨する。

17.16 DOWNLOAD ボタンを押した時に実行する機能の設定

[書式]

```
operation button function download function [script_file [args ...]]
no operation button function download [function [script_file [args ...]]]
```

[設定値及び初期値]

- *function* : DOWNLOAD ボタンを押した時に実行する機能
 - [設定値]:

設定値	説明
http revision-up	HTTP リビジョンアップ
execute batch	バッチファイルの実行
execute lua	Lua スクリプトの実行

- [初期値]: http revision-up
- *script_file*
 - [設定値]: スクリプトファイル名またはバイトコードファイル名を絶対パスもしくは相対パスで指定する
 - [初期値]: -
- *args*
 - [設定値]: *script_file* に渡す可変個引数
 - [初期値]: -

[説明]

DOWNLOAD ボタンを押した時に実行する機能を設定する。機能実行中は DOWNLOAD ボタンの下のランプが点灯し、機能の実行が完了すると消灯する。

function に execute lua を設定した場合、*script_file* を必ず指定する必要がある。*script_file* に相対パスを指定した場合、環境変数 PWD を基点としたパスと解釈される。PWD は **set** コマンドで変更可能であり、初期値は "/" である。

[ノート]

Lua スクリプトを実行させる場合、環境変数 LUA_INIT が設定されていれば *script_file* よりも先に LUA_INIT のスクリプトが実行される。

17.17 DOWNLOAD ボタンによるバッチファイルの実行を許可するか否かの設定

[書式]

```
operation execute batch permit permit
no operation execute batch permit [permit]
```

[設定値及び初期値]

- *permit*
 - [設定値]:

設定値	説明
on	DOWNLOAD ボタンによるバッチファイルの実行を許可する

設定値	説明
off	DOWNLOAD ボタンによるバッチファイルの実行を許可しない

- [初期値]: off

[説明]

DOWNLOAD ボタンによりバッチファイルの実行機能を使用するか否かを設定する。

17.18 監視情報を書き出すファイル名のプレフィックスの設定

[書式]

external-memory sip-proxy filename prefix *prefix* [*crypto password*]

no external-memory sip-proxy filename prefix [*prefix* [*crypto password*]]

[設定値及び初期値]

- *prefix*: ファイル名のプレフィックス
- [設定値]:

設定値	説明
usb1: <i>filename</i>	ファイル名のプレフィックス ("usb1:"を含めずに半角 15 文字以内)
sd1: <i>filename</i>	ファイル名のプレフィックス ("sd1:"を含めずに半角 15 文字以内)

- [初期値]: -
- *crypto*: 暗号化して保存するときの暗号アルゴリズム
- [設定値]:

設定値	説明
aes128	AES128 で暗号化する
aes256	AES256 で暗号化する

- [初期値]: -
- *password*
- [設定値]: 暗号化して保存するときの暗号鍵 ASCII 文字列で表したパスワード (半角 8 文字以上、32 文字以内)
- [初期値]: -

[説明]

監視情報を書き出すファイル名のプレフィックス (接頭語) を設定する。

実際のファイル名は、このプレフィックスをもとにして自動的に決まる。

例えば、プレフィックスを「yamaha」と設定した場合、統計情報を書き出すファイル名は、`yamaha_statistics_20170210.csv` のようになる。

また、保存先ディレクトリは、`/v810_statistics/201702/` となり、この配下に保存される。

暗号化をしないときには、*crypto*、*password* パラメータを指定してはならない。

save report at コマンドで設定された時刻に、統計情報、通話履歴および障害履歴の 3 つが CSV ファイル形式で書き出される。

または、**save report now** コマンドが実行されたときに、書き出される。ファイル名が同じ場合は上書きされるので、コマンド実行時には注意が必要である。

いずれの場合も保持できる最大数か、または直前の 24 時間分のデータが書き出される。

[ノート]

実際のファイル名は、*prefix* の後に種別や日付を表す文字列が加わる。

ファイル名の書式は以下に従う。 *prefix_type_yyyymmdd.ext*

ディレクトリ名の書式は以下に従う。 */v810_type/yyyymm/*

- *prefix*
 - 本コマンドにより設定される任意の文字列

- *type*
 - 監視情報の種類

statistics	統計情報
call	通話履歴
error	障害履歴

- *yyyy*
 - 西暦 (4 桁)
- *mm*
 - 月 (2 桁)
- *dd*
 - 日 (2 桁)
- *ext*
 - 拡張子

csv	CSV
rftg	暗号化されたファイル

外部メモリに暗号化して保存したファイルは、PC 上で RT-FileGuard を使用して復号することができる。

第 18 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。

18.1 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。

18.2 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。

18.3 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。

18.4 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

18.5 Lua スクリプトの強制終了

[書式]

```
terminate lua task_id
```

```
terminate lua file script_file
```

[設定値及び初期値]

- *task_id*: 強制終了する Lua タスクの番号
 - [設定値]:

設定値	説明
all	すべての Lua タスク番号
1..10 (DOWNLOAD ボタン非搭載の機種では 1..9)	Lua タスクの番号

- [初期値]: -
- *script_file*
 - [設定値]: 強制終了するスクリプトファイル名またはバイトコードファイル名を絶対パスもしくは相対パスで指定する
 - [初期値]: -

[説明]

指定した Lua タスク、または、Lua スクリプトを強制終了する。

第 1 書式では、*task_id* で指定された Lua タスクを強制終了する。Lua タスクの番号や実行しているスクリプトについては **show status lua** コマンドで確認できる。

第 2 書式では、*script_file* で指定されたパスとファイル名が完全に一致するスクリプトを実行しているすべての Lua タスクを強制終了する。*script_file* に相対パスを指定した場合、環境変数 PWD を基点とする絶対パスに置換された後で対象の Lua タスクの検索が行われる。

lua コマンドの **-e** オプションを使用して、スクリプトファイルを使用せずに実行されているような Lua スクリプトを強制終了させる場合は、第 1 書式を使用する。

18.6 Lua スクリプト機能に関連するアラーム音を鳴らすか否かの設定

[書式]

```
alarm lua switch
```

```
no alarm lua [switch]
```

[設定値及び初期値]

- *switch*
 - [設定値]:

設定値	説明
on	鳴らす
off	鳴らさない

- [初期値] : on

[説明]

Lua スクリプト機能に関連するアラーム音を鳴らすか否かを選択する。

[ノート]

本コマンドでは、DOWNLOAD ボタンによる Lua スクリプトの実行に関するアラーム音を鳴らすか否かの設定ができる。ハードウェアライブラリでの制御によるアラーム音を鳴らすか否かは、**alarm entire** コマンドの設定に従う。

第 19 章

操作

19.1 設定に関する操作

19.1.1 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。

19.1.2 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]

本装置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。

19.1.3 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
0~1	内蔵フラッシュ ROM の設定ファイル番号
usb1:filename	USB メモリ内の設定ファイル名
sd1:filename	microSD カード内の設定ファイル名

- [初期値]: -
- **comment**
 - [設定値]: 設定ファイルのコメント (半角 200 文字以内)
 - [初期値]: -

[説明]

現在の設定内容を不揮発性メモリに保存する。ファイル指定を省略すると、起動時に使用した設定ファイルに保存する。

[ノート]

filename は半角 99 文字以内。

19.1.4 設定ファイルの複製

[書式]

copy config *from to*

copy config *from to crypto* [*password*]

copy config *from to* [*password*]

[設定値及び初期値]

- *from* : コピー元ファイル名

- [設定値] :

設定値	説明
0~1.1	内蔵フラッシュ ROM の設定ファイル番号
usb1: <i>filename</i>	USB メモリ内の設定ファイル名
sd1: <i>filename</i>	microSD カード内の設定ファイル名
*: <i>filename</i>	USB メモリおよび microSD カード内の設定ファイル名

- [初期値] :-

- *to* : コピー先ファイル名

- [設定値] :

設定値	説明
0~1	内蔵フラッシュ ROM の設定ファイル番号
usb1: <i>filename</i>	USB メモリ内の設定ファイル名、 <i>filename</i> は半角 64 文字以内
sd1: <i>filename</i>	microSD カード内の設定ファイル名、 <i>filename</i> は半角 64 文字以内

- [初期値] :-

- *crypto* : 暗号アルゴリズムの選択

- [設定値] :

設定値	説明
aes128	AES128 で暗号化する。
aes256	AES256 で暗号化する。

- [初期値] :-

- *password*

- [設定値] : ASCII 文字列で表したパスワード (半角 8 文字以上、32 文字以内)

- [初期値] :-

[説明]

保存されている設定ファイルを複製する。

コピー元、コピー先の両方に外部メモリのファイルを指定することはできない。

cold start 直後は設定ファイルが存在しないので内蔵フラッシュ ROM から外部メモリへ設定ファイルのコピーはできない。この場合、一度 **save** コマンドで設定を保存してから実行する必要がある。

内蔵フラッシュ ROM へコピーした内容を、実際の動作に反映させるためには、本コマンドの実行後にルーターを再起動する必要がある。

外部メモリに "*" を指定した場合、指定するファイルの検索はまず microSD カードから行われ、指定したファイルがなければ USB メモリが検索される。 *filename* は絶対パスを使ってファイルを指定するかファイル名のみを指定する。 *filename* にファイル名のみを指定した場合は外部メモリ内から自動検索する。

複数のファイルがある場合、ディレクトリ階層上最もルートディレクトリに近く、アルファベット順に先のディレクトリにあるファイルが選ばれる。

コピー先に外部メモリを指定する場合、 *filename* に絶対パスを使ってファイルを指定する。

外部メモリを対象として暗号化機能を利用することができる。

CRYPTO を指定した場合、設定ファイルを暗号化してから外部メモリにコピーする。暗号化してコピーする場合、ファイル名には *.rtfg* 拡張子を含めるか、拡張子を省略した名前を指定する必要がある。拡張子を省略した場合、自

動的にファイル名に.rtfg 拡張子を追加する。
パスワードを省略した暗号化を行うことができる。

[ノート]

外部メモリ上の暗号化された設定ファイルを復号しないで内蔵フラッシュ ROM にコピーすることはできない。
第2書式は、内蔵フラッシュ ROM の設定ファイルを外部メモリへ暗号化してコピーする場合にのみ利用できる。
第3書式は、外部メモリ内の暗号化された設定ファイルを復号化して内蔵フラッシュ ROM 内にコピーする場合にのみ利用できる。復号するときの暗号アルゴリズムは自動的に判別するので、復号時には暗号アルゴリズムを指定する必要はない。

外部メモリ内のファイルを指定できるのは、外部メモリインタフェースを持つ機種に限られる。
内蔵フラッシュ ROM の設定ファイル番号をコピー先ファイルとした場合、元のコピー先ファイルはこのコマンドの実行後は退避ファイルとなる。

ファイルの自動検索は、外部メモリのディレクトリ構成やファイル数によっては、ファイルの検索に時間がかかることがある。

検索時間を短くするためには、階層の深いディレクトリの作成は避けてルートに近い位置にファイルを格納したり、ファイルを絶対パスで直接指定することが望ましい。

自動検索のタイムアウトの時間は **external-memory auto-search time** コマンドで設定できる。

外部メモリに暗号化して保存したファイルは、PC 上で RT-FileGuard を使用して復号することができる。

filename は半角 99 文字以内。

19.1.5 ファームウェアファイルを内蔵フラッシュ ROM にコピー

[書式]

copy exec from to

[設定値及び初期値]

- *from* : コピー元ファイル名
 - [設定値]:

設定値	説明
番号	0 のみ指定可
usb1: <i>filename</i>	USB メモリ内のファームウェアファイル名
sd1: <i>filename</i>	microSD カード内のファームウェアファイル名
*: <i>filename</i>	USB メモリおよび microSD カード内のファームウェアファイル名

- [初期値]: -
- *to* : コピー先ファイル名
 - [設定値]:

設定値	説明
番号	0 のみ指定可

- [初期値]: -

[説明]

実行形式ファームウェアファイルを内蔵フラッシュ ROM にコピーする。

内蔵フラッシュ ROM へコピーした内容を、実際の動作に反映させるためには、本コマンドの実行後にルーターを再起動する必要がある。

外部メモリに "*" を指定した場合、指定するファイルの検索はまず microSD カードから行われ、指定したファイルがなければ USB メモリが検索される。

filename は絶対パスを使ってファイルを指定するかファイル名のみを指定する。

filename にファイル名のみを指定した場合は外部メモリ内から自動検索する。

複数のファイルがある場合、ディレクトリ階層上最もルートディレクトリに近く、アルファベット順に先のディレクトリにあるファイルが選ばれる。

[ノート]

ファイルの自動検索は、外部メモリのディレクトリ構成やファイル数によっては、ファイルの検索に時間がかかる

ことがある。

検索時間を短くするためには、階層の深いディレクトリの作成は避けてルートに近い位置にファイルを格納したり、ファイルを絶対パスで直接指定することが望ましい。

自動検索のタイムアウトの時間は **external-memory auto-search time** コマンドで設定できる。

filename は半角 99 文字以内。

19.1.6 設定ファイルの削除

[書式]

delete config *filename*

[設定値及び初期値]

- *filename* : 削除するファイル名
 - [設定値]:

設定値	説明
all	内蔵フラッシュ ROM の全ての設定ファイル
0~1.1	内蔵フラッシュ ROM の設定ファイル番号

- [初期値]:-

[説明]

保存されている設定ファイルを削除する。

19.1.7 デフォルト設定ファイルの設定

[書式]

set-default-config *filename*

[設定値及び初期値]

- *filename*
 - [設定値]: 設定ファイル番号 (0..1.1)
 - [初期値]:-

[説明]

起動時に使用する設定ファイルを設定する。

19.1.8 設定の初期化

[書式]

cold start

[説明]

工場出荷時の設定に戻し、再起動する。
コマンド実行時に管理パスワードを入力する必要がある。

[ノート]

内蔵フラッシュ ROM の設定ファイルがすべて削除されることに注意。

19.2 動的情報のクリア操作

19.2.1 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。

19.2.2 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。

19.2.3 ログのクリア

[書式]

clear log [saved]

[設定値及び初期値]

- saved
 - [設定値]: リブート直前のログをクリアする
 - [初期値]: -

[説明]

ログをクリアする。

19.2.4 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。

19.2.5 インタフェースのカウンター情報のクリア

[書式]

clear status 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のカウンター情報をクリアする。

19.2.6 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。

19.2.7 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。

19.2.8 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。

19.2.9 外部メモリに保存された SYSLOG のクリアとバックアップファイルの削除

[書式]

clear external-memory syslog

[説明]

外部メモリに保存された現在書き込み中の SYSLOG ファイル内のログのクリアとすべての SYSLOG のバックアップファイルの削除を行う。
 削除の対象となる SYSLOG のバックアップファイルは、**external-memory syslog filename** コマンドで指定されたパス内に存在するファイルが対象となる。
 なお、本コマンドは、**external-memory syslog filename** コマンドで SYSLOG ファイル名が設定されており、かつ、指定された外部ストレージインタフェースに外部メモリが接続されている場合にのみ動作する。

19.2.10 パケットログ情報のクリア

[書式]

```
clear sip packet-log level=level
```

[設定値及び初期値]

- *level*
 - [設定値]: 障害度レベル (1..5)
 - [初期値]: -

[説明]

パケットログ情報を消去する。

19.2.11 通話履歴の消去

[書式]

```
clear history call
```

[説明]

通話履歴の全件を消去する。

19.2.12 障害履歴の消去

[書式]

```
clear history error
```

[説明]

障害履歴の全件を消去する。

19.2.13 統計情報の消去

[書式]

```
clear statistics
```

[説明]

統計情報の全件を消去する。

19.3 ファイル、ディレクトリの操作

19.3.1 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。

19.3.2 ファイルまたはディレクトリの削除

[書式]

`delete path`

[設定値及び初期値]

- *path*
 - [設定値]: 相対パスまたは絶対パス
 - [初期値]: -

[説明]

指定したファイルまたはディレクトリを削除する。

ディレクトリが空でない場合は配下のファイルとディレクトリも同時に削除される。

path に相対パスを指定した場合、環境変数 `PWD` を基点としたパスと解釈される。`PWD` は `set` コマンドで変更可能であり、初期値は `"/"` である。

[ノート]

path に相対パスで `"config"` または `"exec"` を指定した場合、本コマンドではなく、`delete config` コマンドまたは `delete exec` コマンドが実行される。このような場合には相対パスを使用せず、絶対パスでファイルまたはディレクトリを指定する。

19.3.3 ファイルまたはディレクトリの複製

[書式]

`copy path1 path2`

[設定値及び初期値]

- *path1*
 - [設定値]: コピー元となるファイルまたはディレクトリの相対パスまたは絶対パス
 - [初期値]: -
- *path2*
 - [設定値]: コピー先の相対パスまたは絶対パス
 - [初期値]: -

[説明]

ファイルまたはディレクトリを複製する。コピー元がディレクトリの場合は、配下のすべてのファイルとディレクトリが再帰的に複製される。

path1 がファイルの場合の動作は以下の通りとなる。

path2 と同名のファイルが存在する場合は *path2* のデータが *path1* のデータで上書きされる。

path2 と同名のディレクトリが存在する場合は、そのディレクトリの配下に *path1* と同名のファイルが作成される。

path2 と同名のファイルやディレクトリが存在しない場合には *path2* が作成される。

path1 がディレクトリの場合の動作は以下の通りとなる。

path2 と同名のファイルが存在する場合は複製を実行できない。

path2 と同名のディレクトリが存在する場合は、そのディレクトリの配下に *path1* と同名のディレクトリが作成される。

path2 と同名のファイルやディレクトリが存在しない場合には *path2* が作成される。

path1、*path2* に相対パスを指定した場合、環境変数 `PWD` を基点としたパスと解釈される。`PWD` は `set` コマンドで変更可能であり、初期値は `"/"` である。

[ノート]

path1 に相対パスで `"config"` または `"exec"` を指定した場合、本コマンドではなく、`copy config` コマンドまたは `copy exec` コマンドが実行される。このような場合には相対パスを使用せず、絶対パスでファイルまたはディレクトリを指定する。

19.3.4 ファイル名またはディレクトリ名の変更

[書式]

`rename path name`

[設定値及び初期値]

- *path*

- [設定値]: 変更対象のファイルまたはディレクトリの相対パスまたは絶対パス
- [初期値]: -
- *name*
 - [設定値]: 変更後の名前
 - [初期値]: -

[説明]

指定したファイルまたはディレクトリの名前を変更する。

path に相対パスを指定した場合、環境変数 *PWD* を基点としたパスと解釈される。*PWD* は **set** コマンドで変更可能であり、初期値は "/" である。

[ノート]

name パラメータに新しい名前を指定する場合、スラッシュ "/" を含む名前を指定することはできない。

19.4 その他の操作

19.4.1 再起動

[書式]

restart [*config*]

[設定値及び初期値]

- *config*
 - [設定値]: 内蔵フラッシュ ROM の設定ファイル番号 (0~1.1)
 - [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。

19.4.2 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
 - USB インタフェース名
 - SD インタフェース名
 - [初期値]: -

[説明]

指定したインタフェースを再起動する。

LAN インタフェースでは、オートネゴシエーションする設定になっていればオートネゴシエーション手順が起動される。

USB と SD インタフェースでは、ポートの給電が OFF,ON され、USB デバイスや microSD カードの再アタッチが行われる。

[ノート]

lan1 または lan2 に対してこのコマンドを実行すると、lan1 および lan2 インタフェースが同時にリセットされる。

19.4.3 ping

[書式]

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

[設定値及び初期値]

- *datalen*
 - [設定値]: データ長 (1..65535 バイト)
 - [初期値]: 64

- *count*
 - [設定値]: 実行回数 (1..21474836)
 - [初期値]: Ctrl+c キーが入力されるまで繰り返す
- *ip_address*
 - [設定値]: 始点 IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))
 - [初期値]: ルーターのインタフェースに付与されたアドレスの中から選択する
- *wait*
 - [設定値]: 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。

19.4.4 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
```

[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*
 - [設定値]: 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]: -

[説明]

指定した宛先に対して ICMPv6 Echo Request を送信する。

スコープ識別子は、**show ipv6 address** コマンドで表示できる。

count パラメータを省略すると、Ctrl+c キーを入力するまで実行を継続する。

-w オプションを指定した時には、次のパケットを送信するまでの間に相手からの返事を確認できなかった時にはその旨のメッセージを表示する。-w オプションを指定していない時には、パケットが受信できなくても何もメッセージを表示しない。

19.4.5 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。

19.4.6 traceroute6 の実行

[書式]

traceroute6 *destination*

[設定値及び初期値]

- *destination*
 - [設定値]: 送信する宛先の IPv6 アドレス、または名前
 - [初期値]: -

[説明]

指定した宛先までの経路を調べて表示する。

19.4.7 nslookup

[書式]

nslookup *host*

[設定値及び初期値]

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

[説明]

DNS による名前解決を行う。

[ノート]

IPv4 のみ対応。

19.4.8 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。

19.4.9 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、またはホスト名
 - [初期値]: -
- *port*: 使用するポート番号
 - [設定値]:
 - 十進数
 - ポート番号のニーモニック
 - 省略時は 23 (TELNET)
 - [初期値]: 23
- *mode*: TELNET 通信 (送信) の動作モード
 - [設定値]:

設定値	説明
character	文字単位で通信する
line	行単位で通信する
auto	<i>port</i> パラメータの設定値により character/line を選択
省略	省略時は auto

- [初期値]: auto
- *negotiation*: TELNET オプションのネゴシエーションの選択
 - [設定値]:

設定値	説明
on	ネゴシエーションする
off	ネゴシエーションしない
auto	<i>port</i> パラメータの設定値により on/off を選択
省略	省略時は auto

- [初期値]: auto
- *abort*: TELNET クライアントを強制的に終了させるためのアボートキー
 - [設定値]:
 - 十進数の ASCII コード
 - 省略時は 29(^)
 - [初期値]: 29

[説明]

TELNET クライアントを実行する。

[ノート]

ホスト名による接続は A レコード(IPv4)のみ対応している。

character モードは、通常の TELNET サーバーなどへの接続のための透過的な通信を行う。

line モードは、入力行を編集して行単位の通信を行う。行編集の終了は、改行コード (CR:0x0d または LF:0x0a) の入力で判断する。

ポート番号による機能自動選択について

1. TELNET 通信の動作モードの自動選択
port 番号が 23 の場合は文字単位モードとなり、そうでない場合は行単位モードとなる。
2. TELNET オプションのネゴシエーションの自動選択

port 番号が 23 の場合はネゴシエーションし、そうでない場合はネゴシエーションしない。

19.4.10 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]: チャネルの識別子
 - [初期値]: -

[説明]

指定したセッションに属する特定のチャネルを削除する。チャネルを指定しないときには、そのセッションに属するすべてのチャネルを削除する。

19.4.11 スイッチングハブ MAC アドレステーブルの消去

[書式]

```
clear switching-hub macaddress [interface]
```

[設定値及び初期値]

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

[説明]

スイッチングハブ LSI 内部に保持している動的 MAC アドレステーブルを消去する。

[ノート]

lan type コマンドの *macaddress-aging* パラメータが **off** の場合にこのコマンドを実行してもテーブルエントリ情報は消去されず、次に *macaddress-aging* パラメータが **on** にされた時点で消去される。

19.4.12 HTTP を利用したファームウェアのチェックおよびリビジョンアップの実行

[書式]

```
http revision-up go [no-confirm [prompt]]
```

[設定値及び初期値]

- **no-confirm**: 書き換え可能なリビジョンのファームウェアが存在するときに、ファームウェアの更新を行うかどうかを確認しない
 - [初期値]: -
- **prompt**: コマンド実行後、すぐにプロンプトを表示させ、他のコマンドを実行できるようにする
 - [初期値]: -

[説明]

WEB サーバーに置いているファームウェアと現在実行中のファームウェアのリビジョンをチェックし、書き換え可能であればファームウェアのリビジョンアップを行う。書き換え可能なリビジョンのファームウェアが存在すると、「更新しますか? (Y/N)」という確認を求めてくるので、更新する場合は "Y" を、更新しない場合は "N" を入力する必要がある。

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

http revision-up permit コマンドで HTTP リビジョンアップを許可されていない時は、ファームウェアの書き換えは行わない。

http revision-down permit コマンドでリビジョンダウンが許可されている場合は、WEB サーバーにおいてあるファームウェアが現在のファームウェアよりも古いリビジョンであってもファームウェアの書き換えを行う。

なお、WEB サーバーにおいてあるファームウェアが現在のファームウェアと同一リビジョンの場合には、ファームウェアの書き換えは行わない。

19.4.13 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。

19.4.14 外部メモリに保存された SYSLOG ファイルのローテート (バックアップ)

[書式]

rotate external-memory syslog

[説明]

外部メモリに保存された SYSLOG ファイルのローテート (バックアップ) を行う。

現在書き込み中の SYSLOG ファイルをバックアップファイルに退避し、新たに書き込み用の SYSLOG ファイルを作成する。既に同名のバックアップファイルが存在する場合には実行されない。

また、バックアップファイルを作成する際、バックアップファイル数が **external-memory syslog filename** コマンドで指定される上限数に達した場合、もしくは外部メモリに空き容量がなくなった場合は、最も古いバックアップファイルを削除してから新しいバックアップファイルが作成される。

バックアップファイル名の書式については、**external-memory syslog filename** コマンドを参照のこと。

なお、本コマンドは、**external-memory syslog filename** コマンドで SYSLOG ファイル名が設定されており、かつ、指定された外部ストレージインタフェースに外部メモリが接続されている場合にのみ動作する。

[ノート]

schedule at コマンドで定期的に本コマンドを実行するようにしておくと、日毎、週毎、あるいは月毎の SYSLOG のバックアップファイルを自動で作成することが可能になる。

[設定例]

```
schedule at 1 */* 00:00 * rotate external-memory syslog # 毎日バックアップを実行する
schedule at 1 */mon 00:00 * rotate external-memory syslog # 毎週月曜日にバックアップを実行する
schedule at 1 */1 00:00 * rotate external-memory syslog # 毎月 1 日にバックアップを実行する
```

19.4.15 SIP 呼の切断

[書式]

disconnect sip proxy

[説明]

電話帳サーバー機能によるすべての SIP 呼を切断する。

19.4.16 電話帳サーバーメンテナンス状態の設定

[書式]

sip proxy maintenance sw

[設定値及び初期値]

- *sw*: SIP サーバー動作状態を設定する
 - [設定値]:

設定値	説明
on	メンテナンス状態であることを設定
off	通常状態であることを設定

- [初期値]: -

[説明]

電話帳サーバー機能の設定を変更する場合、一旦メンテナンス状態に移行してから設定の変更を行い、変更後に通

常状態に戻す。

プライマリサーバーまたはセカンダリサーバーでメンテナンス状態に移行すると、自己の VRRP 優先度をプライマリでは 2、セカンダリでは 1 に設定する。

メンテナンス状態に移行しても、冗長構成のもう一台の状態によっては `initial-INIVITE` または `REGISTER` メッセージを受信する可能性があるが、そのメッセージに対しては `480 Temporarily Unavailable` を返す。

[ノート]

ダウンロードボタンを押してダウンロード待ち状態になった場合も、`sip proxy maintenance on` が設定された状態となる。

19.4.17 監視情報を不揮発性メモリへ保存する

[書式]

`save report now`

[説明]

不揮発性メモリに対し、統計情報の保存領域の確保、障害履歴の保存、通話履歴の保存を行う。

不揮発性メモリに保存する前の情報は揮発性メモリに記録されており、電源を切ると消えてしまう。1 日 1 回決まった時刻 (`save report at` コマンドで指定) に不揮発性メモリへの保存処理を行うが、本コマンドにより、その処理を即時に行うことができる。

`external-memory sip-proxy filename prefix` コマンド設定があれば、外部メモリへの保存も行なう。

[ノート]

保存処理中は呼処理など保存処理以外の処理が非常に遅くなるので、運用中に実行すべきではない。冗長化構成であれば、メンテナンス状態で実行するのが望ましい。

また保存処理が終了するまでの時間は不定であるが、最大で 2 分程度の時間を要する。

第 20 章

設定の表示

20.1 機器設定の表示

[書式]

show environment

[説明]

以下の項目が表示される。

- システムのリビジョン
- CPU、メモリの使用量 (%)
- 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ファームウェアと設定ファイル
- 起動時刻、現在時刻、起動してから現在までの経過時間
- セキュリティクラス

20.2 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..1.1)
 - [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。

20.3 設定ファイルの一覧

[書式]

show config list
less config list

[説明]

内蔵フラッシュ ROM に保存されている設定ファイルのファイル名、日時、コメントの一覧を表示する。

20.4 ファイル情報の一覧の表示

[書式]

show file list location [all] [file-only]
less file list location [all] [file-only]

[設定値及び初期値]

- *location*: 表示するファイルのある位置
 - [設定値]:

設定値	説明
internal	内蔵フラッシュ ROM に格納されている config 一覧

設定値	説明
絶対パスまたは相対パス	内蔵フラッシュ ROM の RTFS 領域および外部メモリ

- [初期値]:-
- all: 配下の全ディレクトリを対象にする
 - [初期値]:-
- file-only: ファイル名のみを表示する
 - [初期値]:-

[説明]

指定した場所に格納されているファイル情報の一覧を表示する。

location に相対パスを指定した場合、環境変数 PWD を基点としたパスと解釈される。PWD は **set** コマンドで変更可能であり、初期値は "/" である。

[ノート]

location に絶対パスまたは相対パスを指定した場合のみ、all と file-only を使用できる。

20.5 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]
```

[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]:-

[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。

20.6 SSH サーバー公開鍵の表示

[書式]

```
show sshd public key [fingerprint]
```

[設定値及び初期値]

- fingerprint: 鍵指紋を表示することを示すキーワード
 - [初期値]:-

[説明]

SSH サーバーの公開鍵を表示する。

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

[表示例]

```
> show sshd public key
ssh-dss XXXXXXXXXXXX1kc3MAAAEBAPTb9YYdgvE+4bbhF4mtoIJri+ujdAIfr4hL/0w7Jlvc50eXg
sXJoCqIPlsLRGHOOzxVYbOouPCUV/jPFCatgOIi8eJNzUqSB1e6MOFtGjmESrdYiafyIUhps+YWqd
TIIo0AFnVUKMqAbYODA3Cy7kNVptYRK8rcKwK1ChbatWnT/Z7RcmEVEou0q1Oyp79b3DcpFM7ofa4d
9ySb6mj06Y/Ok8IL5qFhCHmGOGtqJTKZsqb5VnPz8FYC8t1s6/tpyrUa5aG2af/yTEa5U5BDYAuc88
wNIUG9alGo/8WIHiBJAm432o7UPqTHWO/5nYEQu44gmEPQrPGJ65GT8AAAAVAOpjE0Jyei+4c5qWSF
PXUgrLf5HAAABAQCnnPO+ZjWZcZwGa6LxTGMczAjDy5uwD4DWBbRxsPKaXlsicJGC0aridnTthIGa8
ARypDjhpL1a37SDezx8yCIQ5vh+4SPLdS1hdSSzXXE+MXIICXnOVPdiKC4ia10n81tMxW/EPw4SqFP
77r7VvCE/JpXv82AN2JTJ/HAN3X7lvMyCsKZLoWrEcEcBH5anvAQKByVt7RefToZ4vSgodskv7nyXX
XXXXXXXXX
ssh-rsa XXXXXXXXXXXX1yc2EAAAABlWAAQEAwvAZK18jKTCHIHQfrV4r7UOYChX0oeKjBbuuLSDhSH
WmhpG3xxJO0pDIedSF3KnB7LX2SfymQYJ7XYIqMjmU0oziv/zi+De/z3M7wJHQUwfMZEDAdR6Mx39w
6Q04/ehQcaszjXi+0A12wG/kk56IAU23CW/i21o//5GZTzKFKyEJUWauHWEW9glF5Yy7F64PesqoH
6h5oDNK7LhIT7s4QXRnUJphIINrW278Dnvyry3liR+tgTJAq3cGHfYsaQCdankDilIQhUazUY0vJO
/gjYcJMuWH6Ek/cst+PCtgnt0XV5Bl079uRUmcACs2pDX5EWrwPXXXXXXXXXX==

> show sshd public key fingerprint
ssh-dss 2048 XX:XX:77:c5:f9:48:fd:62:85:fb:27:a8:0a:c1:XX:XX
ssh-rsa 2048 XX:XX:58:89:e2:0b:ec:d9:6b:49:11:d2:a3:9d:XX:XX
```

20.7 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]
```

[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]: -
- *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。

20.8 ファームウェアファイルの一覧

[書式]

```
show exec list
```

```
less exec list
```

[説明]

内蔵フラッシュ ROM に保存されている実行形式ファームウェアファイルの情報を表示する。起動中の実行形式ファームウェアファイルには '*' 印が表示される。実行形式ファームウェアファイルが保存されている外部メモリが接続されている場合には、そのファームウェアファイルの情報も表示される。

第 21 章

状態の表示

21.1 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。

21.2 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
 - [初期値]: -

[説明]

インタフェースの状態を表示する。

21.3 IP の経路情報テーブルの表示

[書式]

```
show ip route [destination]
```

```
show ip route detail
```

```
show ip route summary
```

[設定値及び初期値]

- *destination*
 - [設定値]:
 - 相手先 IP アドレス
 - 省略時、経路情報テーブル全体を表示する
 - [初期値]: -
- *detail*: 現在有効な IPv4 経路に加えて、動的経路制御プロトコルによって得られた経路により隠されている静的経路も表示する
 - [初期値]: -
- *summary*: IPv4 の経路数をプロトコル毎に合計して表示する
 - [初期値]: -

[説明]

IP の経路情報テーブルまたは相手先 IP アドレスへのゲートウェイを表示する。ネットマスクは設定時の表現に関わらず連続するビット数で表現される。

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

summary を指定した時には、IPv4 の経路数をプロトコル毎に合計して表示する。

[ノート]

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

プロトコル	メトリック値
RIP	メトリック値

21.4 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。

21.5 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。

21.6 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。

21.7 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。

21.8 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。

21.9 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)

21.10 動的フィルタによって管理されているコネクションの表示**[書式]**

```
show ip connection
show ip connection [interface [direction] [ip_address]]
show ip connection summary
```

[設定値及び初期値]

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

[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。

21.11 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** summary

[設定値及び初期値]

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

[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。

21.12 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。

21.13 侵入情報の履歴の表示

[書式]

show ip intrusion detection**show ip intrusion detection** *interface* [*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	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。

21.14 スイッチングハブ MAC アドレステーブルの表示

[書式]

show status switching-hub macaddress [*interface* [*port*]] [*mac_address*]

[設定値及び初期値]

- *interface*
 - [設定値]: LAN インタフェース名
 - [初期値]: -
- *port*
 - [設定値]: ポート番号 1..4
 - [初期値]: -
- *mac_address*
 - [設定値]: MAC アドレス
 - [初期値]: -

[説明]

スイッチングハブ LSI 内部に保持しているポート毎の動的 MAC アドレステーブルを表示する。ポート番号を指定するとそのポートに関する情報のみが表示される。LAN インタフェース名にはスイッチングハブを持つインタフェースだけが指定可能である。

21.15 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。

21.16 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

21.17 パケットバッファの状態の表示**[書式]**

```
show status packet-buffer [group]
```

[設定値及び初期値]

- *group*: 表示するパケットバッファのグループを指定する
 - [設定値]:

設定値	説明
グループ名 (small, middle, large, huge)	指定したグループの状態を表示する
省略	すべてのグループの状態を表示する

- [初期値]:-

[説明]

パケットバッファの状態を表示する。表示する項目は以下の通り：

- グループ名
- 格納できるパケットサイズ
- 管理パラメータ
- 現在、割り当て中のパケットバッファ数
- 現在、フリーリストにつながれているパケットバッファ数
- 現在、確保しているチャンク数
- パケットバッファの割り当て要求を受けた回数
- パケットバッファの割り当てに成功した回数
- パケットバッファの割り当てに失敗した回数
- パケットバッファが解放された回数
- チャンクを確保した回数
- チャンクを確保しようとして失敗した回数
- チャンクを解放した回数

[表示例]

```
# show status packet-buffer large
large group: 2048 bytes length
parameters: max-buffer=10000 max-free=2812 min-free=62
             buffers-in-chunk=625 initial-chunk=4
2372 buffers in free list
128 buffers are allocated, req/succ/fail/rel = 137/137/0/9
4 chunks are allocated, req/succ/fail/rel = 4/4/0/0
```

21.18 USB ホスト機能の動作状態を表示

[書式]

```
show status usbhost
```

[説明]

USB ホスト機能の動作状態を表示する。

21.19 技術情報の表示

[書式]

```
show techinfo
```

[説明]

技術サポートに必要な情報を一度に出力する。

他の **show** コマンドとは異なり、**show techinfo** コマンドの出力は **console columns/lines** コマンドの設定を無視して一度に出力される。一画面ごとに出力が停止するページ動作は行わない。そのため、ターミナルソフトのログ機能を用いて、出力を PC のファイルとして保存することが望ましい。

また、**console character** コマンドの設定も無視され、常に英語モードで出力される。

一画面ごとに内容を確認しながら出力したいときには、以下のように **less** コマンドを併用するとよい。ただし、**less** コマンドは画面制御シーケンスを多数出力するため、ログを記録しながら **less** コマンドを使用すると、ログファイルがわかりにくくなる。

```
show techinfo | less
```

[ノート]

ルーターに対して PC で動作する TFTP クライアントからアクセスし、ファイル名 'techinfo' を GET すると、**show techinfo** コマンドの出力と同じものが得られる。

Windows XP の TFTP.EXE を使用した例：

```
C:\>tftp 192.168.0.1 get techinfo techinfo.txt
```

21.20 microSD スロットの動作状態を表示

[書式]

```
show status sd
```

[説明]

microSD スロットの動作状態を表示する。

21.21 外部メモリの動作状態を表示

[書式]

```
show status external-memory
```

[説明]

USB ポートと microSD スロットに接続されている外部メモリの状態や共通情報を表示する。

[ノート]

USB ポートに携帯端末が接続されている場合は、USB ポートについては「外部メモリが接続されていません」と表示される。

21.22 RTFS の状態の表示

[書式]

```
show status rtfs
```

[説明]

内蔵フラッシュ ROM の RTFS 領域の状態を表示する。表示する内容は次の通り。

- 容量
- 空き容量
- 作成可能エントリ数
- ファイル数
- ディレクトリ数

実行例は以下の通り。

```
# show status rtfs
容量      : 1572864 バイト
空き容量  : 1566025 バイト
作成可能エントリ数 : 995
ファイル数   : 2
ディレクトリ数 : 3
#
```

21.23 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。

21.24 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。

21.25 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。

21.26 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。

21.27 STATUS LED の情報の表示

[書式]

```
show status status-led [history]
```

[設定値及び初期値]

- history : STATUS LED の状態変化の履歴を表示
 - [初期値] :-

[説明]

STATUS LED の情報を表示する。

点灯していた場合は、点灯の原因となったキープアライブが設定されているインターフェースの一覧が表示される。

history オプションを指定した場合は状態変化の履歴も表示される。

21.28 コピーライトの表示

[書式]

```
show copyright [detail]
```

[設定値及び初期値]

- detail
 - [設定値] : 条文を含めたソフトウェアの著作権情報を表示する
 - [初期値] :-

[説明]

ソフトウェアの著作権情報を表示する。

detail を指定することで、条文を含めたソフトウェアの著作権情報を表示することができる。

21.29 拠点登録状況の表示

[書式]

```
show status sip location
```

[説明]

端末の登録状況を表示する。
SIP アドレス、IP アドレス、q 値、残り登録有効時間を表示する。

21.30 通信中の呼情報の表示**[書式]**

```
show status sip proxy
```

[説明]

通信中の呼の情報を表示する。
通話開始時間、発信者番号、着信者番号を表示する。

21.31 通話履歴の表示**[書式]**

```
show history call [offset=offset] [print=print] [top=top] [end=end] [caller=caller] [callee=callee] [time=time] [state=state]
```

[設定値及び初期値]

- *offset*: 絞り込み対象とする履歴の先頭位置。最新の履歴の位置を 0 とし、そこから新しい順に数えて絞り込み対象としたい履歴の先頭位置を指定する。省略時は 0 とみなす。
 - [初期値]: -
- *print*: 表示件数 (1...100)。省略時は 100 とみなす。
 - [初期値]: -
- *top*: 発信日時で絞り込む。絞り込み開始日時 (yyyy-mm-dd または yyyy/mm/dd)。
 - [初期値]: -
- *end*: 発信日時で絞り込む。絞り込み終了日時 (yyyy-mm-dd または yyyy/mm/dd)。
 - [初期値]: -
- *caller*: 発信者番号で絞り込む。
 - [初期値]: -
- *callee*: 着信者番号で絞り込む。
 - [初期値]: -
- *time*: 通話時間で絞り込む (hh:mm:ss)。
 - [初期値]: -
- *state*: 呼の終了時の状態で絞り込む。
 - [設定値]:

設定値	説明
1	正常終了
2	本装置ビジー
3	拠点ビジー
4	エラー

- [初期値]: -

[説明]

通話履歴を表示する。
発信日時、発信者番号、着信者番号、通話時間、呼の終了時の状態、呼の終了時の着信側の通話数を表示する。
通話履歴は最大で 26000 件記録されているが、同時に表示できるのは最大 100 件まで。必要な情報を得るためには絞り込み条件を指定する。

21.32 障害履歴の表示**[書式]**

```
show history error [offset=offset] [print=print] [top=top] [end=end] [caller=caller] [callee=callee] [error=state] [log]
```

[設定値及び初期値]

- *offset*: 絞り込み対象とする履歴の先頭位置。最新の履歴の位置を 0 とし、そこから新しい順に数えて絞り込み対象としたい履歴の先頭位置を指定する。省略時は 0 とみなす。
 - [初期値]: -
- *print*: 表示件数 (1...100)。省略時は 100 とみなす。
 - [初期値]: -
- *top*: 障害発生日時で絞り込む。絞り込み開始日時 (yyyy-mm-dd または yyyy/mm/dd)。
 - [初期値]: -
- *end*: 障害発生日時で絞り込む。絞り込み終了日時 (yyyy-mm-dd または yyyy/mm/dd)。
 - [初期値]: -
- *caller*: 発信者番号で絞り込む。
 - [初期値]: -
- *callee*: 着信者番号で絞り込む。
 - [初期値]: -
- *state*: 障害内容で絞り込む。
 - [設定値]:

設定値	説明
1	本装置ビジー
2	拠点ビジー
3	エラー

- [初期値]: -
- *log*: 指定すると、対応する SIP パケットログが存在する履歴のみ表示。
 - [初期値]: -

[説明]

障害履歴を表示する。

障害発生日時、発信者番号、着信者番号、障害内容、対応する SIP パケットログの有無を表示する。

障害履歴は最大で 1500 件記録されているが、同時に表示できるのは最大 100 件まで。必要な情報を得るためには絞り込み条件を指定する。

21.33 統計情報の表示

[書式]

show statistics [*offset=offset*] [*print=print*] [*top=top*] [*end=end*] [*period=period*]

[設定値及び初期値]

- *offset*: 絞り込み対象とする統計情報の先頭位置。最新の記録位置を 0 とし、そこから新しい順に数えて絞り込み対象としたい記録の先頭位置を指定する。省略時は 0 とみなす。
 - [初期値]: -
- *print*: 表示件数 (1...100)。省略時は 100 とみなす。
 - [初期値]: -
- *top*: 統計記録日時で絞り込む。絞り込み開始日時 (yyyy-mm-dd または yyyy/mm/dd)。
 - [初期値]: -
- *end*: 統計記録日時で絞り込む。絞り込み終了日時 (yyyy-mm-dd または yyyy/mm/dd)。
 - [初期値]: -
- *period*: 集計時間 (1...24)。指定すると、集計時間ごとに再集計して表示する。
 - [初期値]: -

[説明]

統計情報を表示する。

統計記録日時と、記録日時ごとの各統計値を表示する。

同時に表示できるのは最大 100 件まで。必要な情報を得るためには絞り込み条件を指定する。

21.34 拠点情報の表示

[書式]

```
show status sip user [user=user] [status=status]
```

[設定値及び初期値]

- *user* : 事業所番号で絞り込む。
 - [初期値] :-
- *status* : 拠点の状態で絞り込む。
 - [設定値] :

設定値	説明
1	登録済み
2	登録切れ
3	未登録
4	ビジー
5	エラー

- [初期値] :-

[説明]

拠点情報を表示する。

事業所番号、名称、登録 IP アドレス、登録 q 値、拠点の状態を表示する。

21.35 拠点情報の概略表示

[書式]

```
show status sip user summary
```

[説明]

拠点情報の概略を表示する。

登録拠点数、同時通話数、エラー拠点数、ビジー拠点数を表示する。

21.36 電話帳サーバー VRRP 冗長構成機能の状態表示

[書式]

```
show status sip proxy redundancy
```

[説明]

電話帳サーバー VRRP 冗長構成機能の状態を表示する。

第 22 章

ログイン

22.1 ログの表示

[書式]

```
show log [saved] [reverse]
show log external-memory [backup [fileid]]
less log [saved] [reverse]
```

[設定値及び初期値]

- saved
 - [設定値]: リブート直前のログを表示する
 - [初期値]: -
- reverse
 - [設定値]: ログを逆順に表示する
 - [初期値]: -
- external-memory
 - [設定値]: **external-memory syslog filename** コマンドで設定している SYSLOG ファイルの中身を表示する
 - [初期値]: -
- backup
 - [設定値]: SYSLOG バックアップファイルの中身を表示する、もしくは、SYSLOG バックアップファイルの一覧を表示する
 - [初期値]: -
- fileid: 指定した SYSLOG バックアップファイルの中身を表示する
 - [設定値]: `yyyymmdd_hhmmss`
 - [初期値]: -

[説明]

ルーターの動作状況を記録したログを表示する。

ログの最大保持件数は 3000。

最大数を越えた場合には、発生時刻の古いものから消去されていく。最大数以上のログを保存する場合には、**syslog host** コマンドでログを SYSLOG サーバーに転送して、そちらで保存する必要がある。

意図しないリブートが発生したときは、'saved' を指定することでリブート直前のログを表示することができる。

このコマンドでは、通常は発生時刻の古いものからログを順に表示するが、'reverse' を指定することで新しいものから表示させることができる。

パワーオフ・ログ保存機能に対応していない機種では、本機の電源を切るとログは消去される。

external-memory を指定した場合は、外部メモリ内の SYSLOG ファイルを表示する。

external-memory backup を指定した場合は、バックアップファイルの一覧を古いものから順に表示する。バックアップファイルの中身を表示するには、表示されたファイル名の日時データ (`yyyymmdd_hhmmss` 形式で表される文字列の 15 桁) を **fileid** に指定すると表示させることができる。

[ノート]

restart コマンドや TFTP によるファームウェアのバージョンアップなどで電源を入れたままルーターが再起動した場合でも、電源を切らない限りはログは保存される。

saved オプションを指定することで表示されるログは電源を切ると消去される。

external-memory を指定した場合は以下の制限がある。

- 外部メモリ内の暗号化したログファイルは表示できない
- リダイレクトを指定できない

external-memory を指定して、**external-memory syslog filename** コマンドが設定されていない場合は実行エラーとなる。

索引

記号

> 20
>> 20

A

administrator 156
administrator password 23
administrator password encrypted 23
alarm batch 52
alarm entire 51
alarm http revision-up 52
alarm lua 154
alarm sd 51
alarm startup 52
alarm usbhost 51

C

clear arp 159
clear boot list 160
clear dns cache 160
clear external-memory syslog 160
clear history call 161
clear history error 161
clear ip dynamic routing 159
clear ipv6 dynamic routing 160
clear ipv6 neighbor cache 160
clear log 160
clear sip packet-log 161
clear statistics 161
clear status 160
clear switching-hub macaddress 167
cold start 159
console character 30
console columns 30
console info 31
console lines 30
console prompt 29
copy 162
copy config 157
copy exec 158

D

date 28
delete 162
delete config 159
description 39
dhcp convert lease to bind 87
dhcp duplicate check 84
dhcp manual lease 89
dhcp manual release 89
dhcp scope 84
dhcp scope bind 85
dhcp scope lease type 87
dhcp scope option 88
dhcp server rfc2131 compliant 82
dhcp service 82
disconnect ip connection 165
disconnect ipv6 connection 167

disconnect sip proxy 168
disconnect user 26
dns cache max entry 113
dns cache use 112
dns domain 108
dns host 112
dns server 108
dns server select 109
dns service 108
dns service fallback 113
dns srport 111
dns static 110
dns syslog resolv 109

E

execute batch 147
exit 156
external-memory accelerator cache size 142
external-memory auto-search time 147
external-memory batch filename 147
external-memory boot permit 144
external-memory boot timeout 145
external-memory cache mode 141
external-memory config filename 146
external-memory exec filename 145
external-memory performance-test go 148
external-memory sip-proxy filename prefix 150
external-memory syslog filename 142

G

grep 18

H

help 22
http revision-down permit 42
http revision-up go 167
http revision-up permit 41
http revision-up proxy 42
http revision-up schedule 43
http revision-up timeout 42
http revision-up url 42
httpd host 134
httpd listen 135
httpd service 134
httpd sysname 135
httpd timeout 135

I

interface reset 163
ip arp timer 73
ip filter 63
ip filter directed-broadcast 67
ip filter dynamic 67
ip filter dynamic timer 68
ip filter set 66
ip filter source-route 66
ip host 110
ip icmp echo-reply send 91

- ip icmp echo-reply send-only-linkup 91
- ip icmp log 93
- ip icmp parameter-problem send 91
- ip icmp time-exceeded send 92
- ip icmp timestamp-reply send 92
- ip icmp unreachable send 92
- ip interface address 60
- ip interface arp log 74
- ip interface arp queue length 73
- ip interface arp static 73
- ip interface dhcp service 90
- ip interface intrusion detection 69
- ip interface intrusion detection notice-interval 70
- ip interface intrusion detection repeat-control 70
- ip interface intrusion detection report 71
- ip interface mtu 61
- ip interface rebound 61
- ip interface rip auth key 77
- ip interface rip auth key text 77
- ip interface rip auth type 76
- ip interface rip filter 75
- ip interface rip force-to-advertise 77
- ip interface rip hop 76
- ip interface rip receive 75
- ip interface rip trust gateway 75
- ip interface secondary address 60
- ip interface secure filter 72
- ip interface secure filter name 72
- ip interface tcp window-scale 71
- ip interface vrrp 79
- ip interface vrrp shutdown trigger 80
- ip keepalive 80
- ip route 62
- ip route change log 72
- ip simple-service 62
- ip stealth 93
- ipv6 filter 124
- ipv6 filter dynamic 125
- ipv6 icmp echo-reply send 94
- ipv6 icmp echo-reply send-only-linkup 94
- ipv6 icmp log 96
- ipv6 icmp packet-too-big send 96
- ipv6 icmp parameter-problem send 94
- ipv6 icmp time-exceeded send 95
- ipv6 icmp unreachable send 95
- ipv6 interface address 116
- ipv6 interface dad retry count 118
- ipv6 interface mtu 115
- ipv6 interface prefix 117
- ipv6 interface prefix change log 118
- ipv6 interface rip filter 121
- ipv6 interface rip hop 121
- ipv6 interface rip receive 120
- ipv6 interface rip trust gateway 121
- ipv6 interface secure filter 124
- ipv6 interface tcp window-scale 115
- ipv6 interface vrrp 122
- ipv6 interface vrrp shutdown trigger 123
- ipv6 max auto address 119
- ipv6 nd ns-trigger-dad 126
- ipv6 rh0 discard 115
- ipv6 rip preference 122
- ipv6 rip use 120
- ipv6 route 119
- ipv6 source address selection rule 119
- ipv6 stealth 96

L

- lan count-hub-overflow 35
- lan linkup send-wait-time 36
- lan shutdown 35
- lan type 36
- less 20
- less config 170
- less config list 170
- less exec list 172
- less file list 170
- less log 184
- login password 23
- login password encrypted 23
- login timer 38
- login user 23
- lua 152
- lua use 152
- luac 153

M

- mail notify 131
- mail notify status exec 168
- mail server name 128
- mail server pop 129
- mail server smtp 128
- mail server timeout 129
- mail template 130
- make directory 161

N

- nslookup 165
- ntp backward-compatibility 29
- ntp local address 29
- ntpdate 28

O

- operation button function download 149
- operation execute batch permit 149
- operation external-memory download permit 144
- operation http revision-up permit 43

P

- ping 163
- ping6 164

Q

- quit 156

R

- rdate 28
- rename 162
- restart 163
- rip filter rule 78
- rip timer 78
- rip use 74
- rotate external-memory syslog 168
- rtfs format 54
- rtfs garbage-collect 54

S

save 156
 save report at 53
 save report now 169
 schedule at 136
 scp 48
 sd use 141
 security class 26
 set 53
 set-default-config 159
 sftpd host 47
 show arp 173
 show command 22
 show config 170
 show config list 170
 show copyright 180
 show dns cache 180
 show environment 170
 show exec list 172
 show file list 170
 show history call 181
 show history error 181
 show ip connection 175
 show ip intrusion detection 176
 show ip rip table 174
 show ip route 173
 show ip secure filter 172
 show ipv6 address 171
 show ipv6 connection 175
 show ipv6 neighbor cache 174
 show ipv6 rip table 174
 show ipv6 route 174
 show log 184
 show sshd public key 171
 show statistics 182
 show status 173
 show status boot 179
 show status boot all 180
 show status boot list 180
 show status dhcp 175
 show status external-memory 179
 show status ip keepalive 176
 show status lua 153
 show status mail service 177
 show status packet-buffer 177
 show status rdfs 179
 show status sd 179
 show status sip location 180
 show status sip proxy 181
 show status sip proxy redundancy 183
 show status sip user 182
 show status sip user summary 183
 show status status-led 180
 show status switching-hub macaddress 176
 show status usbhost 178
 show status user 177
 show status vrrp 174
 show techinfo 178
 sip packet-log 133
 sip proxy domain 55
 sip proxy error response timeout 58
 sip proxy forwarding address 57
 sip proxy forwarding server 57
 sip proxy maintenance 168
 sip proxy redundancy mode 58

sip user 55
 snmp community read-only 99
 snmp community read-write 99
 snmp host 98
 snmp local address 105
 snmp syscontact 105
 snmp syslocation 105
 snmp sysname 105
 snmp trap community 99
 snmp trap enable snmp 106
 snmp trap host 99
 snmp trap link-updown separate-l2switch-port 107
 snmp trap send linkdown 106
 snmpv2c community read-only 100
 snmpv2c community read-write 100
 snmpv2c host 100
 snmpv2c trap community 101
 snmpv2c trap host 101
 snmpv3 context name 101
 snmpv3 engine id 101
 snmpv3 host 103
 snmpv3 trap host 104
 snmpv3 usm user 102
 snmpv3 vacm access 104
 snmpv3 vacm view 103
 sntpd host 138
 sntpd service 138
 ssh 48
 ssh encrypt algorithm 49
 ssh known hosts 50
 sshd client alive 46
 sshd encrypt algorithm 46
 sshd hide openssh version 47
 sshd host 45
 sshd host key generate 45
 sshd listen 44
 sshd service 44
 sshd session 45
 syslog debug 32
 syslog execute command 33
 syslog facility 31
 syslog host 31
 syslog info 32
 syslog local address 33
 syslog notice 32
 syslog srport 33
 system packet-buffer 50

T

tcp log 39
 tcp session limit 71
 telnet 166
 telnetd host 34
 telnetd listen 34
 telnetd service 33
 telnetd session 35
 terminate lua 154
 terminate lua file 154
 tftp host 38
 time 28
 timezone 27
 traceroute 165
 traceroute6 165

U

usbhost overcurrent duration [141](#)

usbhost use [140](#)

user attribute [24](#)