

Biz Box ルーター「N58i」



コマンドリファレンス

本製品をお使いになる前に本書をよくお読みになり、
正しく設置や設定を行なってください。

本書中の警告や注意を必ず守り、正しく安全にお使いください。

本書はなくさないように、大切に保管してください。

- 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。
- コマンドラインで設定した内容は GUI に上書きされます。

- ※ 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。
- ※ Stac LZS は米国 Hi/fn 社の登録商標です。

目次

1. コマンドリファレンスの見方	21
1.1 コマンドリファレンスの見方	21
1.2 インタフェース名について	21
1.3 no で始まるコマンドの入力形式について	21
1.4 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	22
1.5 工場出荷設定値について	22
2. コマンドの使い方	23
2.1 コンソールについて	23
2.1.1 コンソールによる設定手順	24
2.1.2 CONSOLE ポートからの設定	25
2.1.3 TELNET による設定	27
2.1.4 リモートセットアップ	29
2.2 SSH サーバーについて	30
2.2.1 使用に当たっての注意事項	30
2.2.2 SSH サーバーの設定	30
2.3 TFTP について	31
2.3.1 TFTP による設定手順	31
2.3.2 設定ファイルの読み出し	32
2.3.3 設定ファイルの書き込み	33
2.4 コンソール使用時のキーボード操作について	33
2.5 「show」で始まるコマンド	34
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	34
2.5.2 show コマンドの表示内容を見やすくする	35
3. ヘルプ	36
3.1 コンソールに対する簡易説明の表示	36
3.2 コマンド一覧の表示	36
4. 機器の設定	37
4.1 ログインパスワードの設定	37
4.2 無名ユーザのパスワードを暗号化して保存する	37
4.3 管理パスワードの設定	37
4.4 管理ユーザのパスワードを暗号化して保存する	37
4.5 ログインユーザ名とログインパスワードの設定	37
4.6 ユーザの属性を設定	38
4.7 セキュリティクラスの設定	39
4.8 コンソールのプロンプト表示の設定	39
4.9 ログインタイマの設定	40
4.10 タイムゾーンの設定	40
4.11 現在の日付けの設定	40
4.12 現在の時刻の設定	40
4.13 リモートホストによる時計の設定	40
4.14 NTP による時計の設定	41
4.15 コンソールの言語とコードの設定	41
4.16 コンソールの表示文字数の設定	41
4.17 コンソールの表示行数の設定	41
4.18 コンソールにシステムメッセージを表示するか否かの設定	42
4.19 SYSLOG を受けるホストの IP アドレスの設定	42
4.20 SYSLOG ファシリティの設定	42
4.21 NOTICE タイプの SYSLOG を出力するか否かの設定	42
4.22 INFO タイプの SYSLOG を出力するか否かの設定	42
4.23 DEBUG タイプの SYSLOG を出力するか否かの設定	43

4.24	SYSLOG を送信する時の始点 IP アドレスの設定	43
4.25	SYSLOG パケットの始点ポート番号の設定	43
4.26	TELNET サーバー機能の ON/OFF の設定	43
4.27	TELNET サーバーへアクセスできるホストの IP アドレスの設定	44
4.28	TELNET サーバー機能の listen ポートの設定	44
4.29	TELNET に同時に接続できるユーザ数を設定する	44
4.30	TFTP によりアクセスできるホストの IP アドレスの設定	45
4.31	ファストパス機能の設定	45
4.32	LAN インタフェースの動作設定	45
4.33	LAN インタフェースの動作タイプの設定	45
4.34	インタフェースの説明	46
4.35	TEL ポートでの接続・切断時にアラーム音を鳴らすか否かの設定	46
4.36	データ通信での接続・切断時にアラーム音を鳴らすか否かの設定	47
4.37	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	47
4.38	攻撃を検知した時にアラーム音を鳴らすか否かの設定	47
4.39	MP 通信でリンク数が増えた時にアラーム音を鳴らすか否かの設定	47
4.40	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	47
4.41	HTTP リビジョンアップ実行を許可するか否かの設定	48
4.42	HTTP リビジョンアップ用 URL の設定	48
4.43	HTTP リビジョンアップ用 Proxy サーバーの設定	48
4.44	HTTP リビジョンアップ処理のタイムアウトの設定	48
4.45	リビジョンダウンを許可するか否かの設定	49
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	49
4.47	電話機からのリビジョンアップ操作を許可するか否かの設定	49
4.48	INIT スイッチによるパスワード再入力機能の設定	49
4.49	エコーキャンセル制御方法の設定	50
4.50	エコーキャンセルの NLP 閾値の設定	51
4.51	エコーキャンセルを無効にする音の設定	51
4.52	Magic Packet を LAN に中継するか否かの設定	51
4.53	TCP のログを記録するか否かの設定	52
4.54	SSH サーバー機能の ON/OFF の設定	53
4.55	SSH サーバー機能の listen ポートの設定	53
4.56	SSH サーバーへアクセスできるホストの IP アドレスの設定	54
4.57	SSH に同時に接続できるユーザ数を設定する	54
4.58	SSH サーバー ホスト鍵の設定	54
4.59	SSH クライアントの生存確認	55
4.60	パケットバッファのパラメータを変更する	55
4.61	他のユーザの接続を強制切断する	56
5.	ISDN 関連の設定	57
5.1	共通の設定	57
5.1.1	BRI インタフェースの使用制限の設定	57
5.1.2	BRI 回線の種類の指定	57
5.1.3	自分の ISDN 番号の設定	57
5.1.4	PP で使用するインタフェースの設定	58
5.1.5	課金額による発信制限の設定	58
5.1.6	PIAFS の発信方式の設定	58
5.1.7	PIAFS の着信を許可するか否かの設定	59
5.1.8	PIAFS 接続時の起動側の指定	59
5.1.9	常時接続の設定	59
5.2	相手側の設定	60
5.2.1	相手 ISDN 番号の設定	60
5.2.2	自動接続の設定	60
5.2.3	自動切断の設定	60
5.2.4	着信許可の設定	60

5.2.5	発信許可の設定	61
5.2.6	相手への発信順序の設定	61
5.2.7	再発信抑制タイマの設定	61
5.2.8	エラー切断後の再発信禁止タイマの設定	62
5.2.9	相手にコールバック要求を行なうか否かの設定	62
5.2.10	コールバック要求タイプの設定	62
5.2.11	相手からのコールバック要求に応じるか否かの設定	62
5.2.12	コールバック受け入れタイプの設定	62
5.2.13	MS コールバックでユーザからの番号指定を許可するか否かの設定	63
5.2.14	コールバックタイマの設定	63
5.2.15	コールバック待機タイマの設定	63
5.2.16	ISDN 回線を切断するタイマ方式の指定	63
5.2.17	切断タイマの設定 (ノーマル)	64
5.2.18	入力切断タイマの設定 (ノーマル)	64
5.2.19	出力切断タイマの設定 (ノーマル)	64
5.2.20	課金単位時間方式での課金単位時間と監視時間の設定	65
5.2.21	切断タイマの設定 (ファスト)	65
5.2.22	切断タイマの設定 (強制)	65
5.2.23	同じ相手に対して連続して認証に失敗できる回数の設定	66
5.2.24	MP が失敗できる最大回数の設定	66
5.2.25	相手先毎の累積接続時間による発信制限の設定	66
5.2.26	相手先毎の累積接続回数による発信制限の設定	66
5.2.27	i-ナンバーサービスのポート番号の設定	67
6.	IP の設定	68
6.1	インタフェース共通の設定	68
6.1.1	IP パケットを扱うか否かの設定	68
6.1.2	IP アドレスの設定	68
6.1.3	セカンダリ IP アドレスの設定	69
6.1.4	IP の静的経路情報の設定	69
6.1.5	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	70
6.1.6	IP パケットのフィルタの設定	70
6.1.7	フィルタセットの定義	71
6.1.8	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	72
6.1.9	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	72
6.1.10	動的フィルタの定義	72
6.1.11	TCP セッションの MSS 制限の設定	73
6.1.12	動的フィルタのタイムアウトの設定	74
6.1.13	侵入検知機能の動作の設定	74
6.1.14	1 秒間に侵入検知情報を通知する頻度の設定	74
6.1.15	重複する侵入検知情報の通知抑制の設定	75
6.1.16	侵入検知情報の最大表示件数の設定	75
6.1.17	侵入検知で用いる閾値の設定	75
6.1.18	echo, discard, time サービスを動作させるか否かの設定	75
6.1.19	フィルタに一致する IP パケットの DF ビットを 0 に書き換えるか否かの設定	76
6.1.20	フィルタリングによるセキュリティの設定	76
6.1.21	インタフェースの MTU の設定	77
6.1.22	ARP が解決されるまで送信を保留するパケットの数の設定	77
6.2	代理 ARP の設定	77
6.2.1	ARP エントリの寿命の設定	78
6.2.2	静的 ARP エントリの設定	78
6.3	PP 側の設定	78
6.3.1	相手の PP 側 IP アドレスの設定	78
6.3.2	リモート IP アドレスプールの設定	79
6.3.3	PP 経由のキープアライブの時間間隔の設定	79

6.3.4	PP 経由のキープアライブを使用するか否かの設定	80
6.3.5	PP 経由のキープアライブのログをとるか否かの設定	80
6.3.6	専用線ダウン検出時の動作の設定	81
6.4	RIP の設定	81
6.4.1	RIP を使用するかどうかの設定	81
6.4.2	RIP に関して信用できるゲートウェイの設定	81
6.4.3	RIP パケットの送信に関する設定	81
6.4.4	RIP パケットの受信に関する設定	82
6.4.5	RIP のフィルタリングの設定	82
6.4.6	RIP で加算するホップ数の設定	82
6.4.7	RIP2 での認証の設定	83
6.4.8	RIP2 での認証キーの設定	83
6.4.9	回線切断時の経路保持の設定	83
6.4.10	回線接続時の PP 側の RIP の動作の設定	84
6.4.11	回線接続時の PP 側の RIP 送出の時間間隔の設定	84
6.4.12	回線切断時の PP 側の RIP の動作の設定	84
6.4.13	回線切断時の PP 側の RIP 送出の時間間隔の設定	84
6.4.14	ネットワーク監視機能の設定	85
7.	イーサネットフィルタの設定	86
7.1	フィルタ定義の設定	86
7.2	インタフェースでのイーサネットフィルタリングの設定	87
8.	PPP の設定	88
8.1	相手の名前とパスワードの設定	88
8.2	要求する認証タイプの設定	88
8.3	受け入れる認証タイプの設定	89
8.4	自分の名前とパスワードの設定	89
8.5	同一 username を持つ相手からの二重接続を禁止するか否かの設定	89
8.6	LCP 関連の設定	89
8.6.1	Address and Control Field Compression オプション使用の設定	89
8.6.2	Magic Number オプション使用の設定	90
8.6.3	Maximum Receive Unit オプション使用の設定	90
8.6.4	Protocol Field Compression オプション使用の設定	90
8.6.5	lcp-restart パラメータの設定	90
8.6.6	lcp-max-terminate パラメータの設定	91
8.6.7	lcp-max-configure パラメータの設定	91
8.6.8	lcp-max-failure パラメータの設定	91
8.6.9	Configure-Request をすぐに送信するか否かの設定	91
8.7	PAP 関連の設定	91
8.7.1	pap-restart パラメータの設定	91
8.7.2	pap-max-authreq パラメータの設定	92
8.8	CHAP 関連の設定	92
8.8.1	chap-restart パラメータの設定	92
8.8.2	chap-max-challenge パラメータの設定	92
8.9	IPCP 関連の設定	92
8.9.1	Van Jacobson Compressed TCP/IP 使用の設定	92
8.9.2	PP 側 IP アドレスのネゴシエーションの設定	92
8.9.3	ipcp-restart パラメータの設定	93
8.9.4	ipcp-max-terminate パラメータの設定	93
8.9.5	ipcp-max-configure パラメータの設定	93
8.9.6	ipcp-max-failure パラメータの設定	93
8.9.7	WINS サーバーの IP アドレスの設定	93
8.9.8	IPCP の MS 拡張オプションを使うか否かの設定	94
8.9.9	ホスト経路が存在する相手側 IP アドレスを受け入れるか否かの設定	94

8.10	MSCBCP 関連の設定	94
8.10.1	mscbcp-restart パラメータの設定	94
8.10.2	mscbcp-maxretry パラメータの設定	94
8.11	CCP 関連の設定	95
8.11.1	全パケットの圧縮タイプの設定	95
8.11.2	ccp-restart パラメータの設定	95
8.11.3	ccp-max-terminate パラメータの設定	95
8.11.4	ccp-max-configure パラメータの設定	95
8.11.5	ccp-max-failure パラメータの設定	96
8.12	IPV6CP 関連の設定	96
8.12.1	IPV6CP を使用するか否かの設定	96
8.13	MP 関連の設定	96
8.13.1	MP を使用するか否かの設定	96
8.13.2	MP の制御方法の設定	96
8.13.3	MP のための負荷閾値の設定	96
8.13.4	MP の最大リンク数の設定	97
8.13.5	MP の最小リンク数の設定	97
8.13.6	MP のための負荷計測間隔の設定	97
8.13.7	MP のパケットを分割するか否かの設定	97
8.14	PPPoE 関連の設定	98
8.14.1	PPPoE で使用する LAN インタフェースの指定	98
8.14.2	アクセスコンセントレータ名の設定	98
8.14.3	セッションの自動接続の設定	98
8.14.4	セッションの自動切断の設定	98
8.14.5	PADI パケットの最大再送回数の設定	98
8.14.6	PADI パケットの再送時間の設定	99
8.14.7	PADR パケットの最大再送回数の設定	99
8.14.8	PADR パケットの再送時間の設定	99
8.14.9	PPPoE セッションの切断タイマの設定	99
8.14.10	TCP パケットの MSS の制限の有無とサイズの指定	99
8.14.11	サービス名の指定	100
8.14.12	認証失敗の最大回数を設定する	100
9.	DHCP の設定	101
9.1	DHCP サーバー・リレーエージェント機能	101
9.1.1	DHCP の動作の設定	101
9.1.2	RFC2131 対応動作の設定	102
9.1.3	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	102
9.1.4	DHCP スコープの定義	103
9.1.5	DHCP 予約アドレスの設定	103
9.1.6	DHCP 割り当て情報を元にした予約設定の生成	105
9.1.7	DHCP オプションの設定	105
9.1.8	DHCP アドレス割り当て動作の設定	106
9.1.9	DHCP リース情報の手動追加	107
9.1.10	DHCP リース情報の手動削除	107
9.1.11	DHCP サーバーの指定の設定	107
9.1.12	DHCP サーバーの選択方法の設定	107
9.1.13	DHCP BOOTREQUEST パケットの中継基準の設定	108
9.2	DHCP クライアント機能	108
9.2.1	要求する IP アドレスリース期間の設定	108
9.2.2	IP アドレス取得要求の再送回数と間隔の設定	108
9.2.3	DHCP クライアント ID オプションの設定	109
9.2.4	DHCP クライアントのホスト名の設定	109
9.2.5	DHCP クライアントが DHCP サーバーへ送るメッセージ中に格納するオプションの設定	110
10.	ICMP の設定	111

10.1	IPv4 の設定	111
10.1.1	ICMP Echo Reply を送信するか否かの設定	111
10.1.2	ICMP Echo Reply をリンクダウン時に送信するか否かの設定	111
10.1.3	ICMP Mask Reply を送信するか否かの設定	111
10.1.4	ICMP Parameter Problem を送信するか否かの設定	111
10.1.5	ICMP Redirect を送信するか否かの設定	112
10.1.6	ICMP Redirect 受信時の処理の設定	112
10.1.7	ICMP Time Exceeded を送信するか否かの設定	112
10.1.8	ICMP Timestamp Reply を送信するか否かの設定	112
10.1.9	ICMP Destination Unreachable を送信するか否かの設定	112
10.1.10	受信した ICMP のログを記録するか否かの設定	113
10.1.11	ステルス機能の設定	113
10.2	IPv6 の設定	113
10.2.1	ICMP Echo Reply を送信するか否かの設定	113
10.2.2	ICMP Echo Reply をリンクダウン時に送信するか否かの設定	114
10.2.3	ICMP Parameter Problem を送信するか否かの設定	114
10.2.4	ICMP Redirect を送信するか否かの設定	114
10.2.5	ICMP Redirect 受信時の処理の設定	114
10.2.6	ICMP Time Exceeded を送信するか否かの設定	114
10.2.7	ICMP Destination Unreachable を送信するか否かの設定	115
10.2.8	受信した ICMP のログを記録するか否かの設定	115
10.2.9	ICMP Packet-Too-Big を送信するか否かの設定	115
10.2.10	ステルス機能の設定	115
11.	トンネリング	116
11.1	トンネルインタフェースの使用許可の設定	116
11.2	トンネルインタフェースの使用不許可の設定	116
11.3	トンネルインタフェースの種別の設定	116
11.4	トンネルインタフェースの端点 IP アドレスの設定	116
11.5	トンネルインタフェースの IPv4 アドレスの設定	117
11.6	トンネルインタフェースの相手側の IPv4 アドレスの設定	117
11.7	トンネル接続する DTCP サーバーへの認証情報の設定	117
12.	PPTP 機能の設定	118
12.1	共通の設定	118
12.1.1	PPTP サーバーを動作させるか否かの設定	118
12.1.2	相手先情報番号にバインドされるトンネルインタフェースの設定	118
12.1.3	PPTP ホスト名の設定	118
12.1.4	PPTP の動作タイプの設定	118
12.1.5	PPTP パケットのウィンドウサイズの設定	119
12.1.6	PPTP の動作モードの設定	119
12.1.7	PPTP のコネクション制御の syslog を出力するか否かの設定	119
12.1.8	PPTP 暗号鍵生成のための要求する認証方式の設定	119
12.1.9	PPTP 暗号鍵生成のための受け入れ可能な認証方式の設定	120
12.2	リモートアクセス VPN 機能	120
12.2.1	PPTP トンネルの切断タイムの設定	120
12.2.2	PPTP トンネルの端点の名前の設定	120
12.2.3	PPTP キープアライブの設定	120
12.2.4	PPTP キープアライブのログ設定	121
12.2.5	PPTP 接続において暗号化の有無により接続を許可するか否かの設定	121
12.2.6	PPTP キープアライブを出すインターバルとカウントの設定	121
13.	NAT 機能	122
13.1	インタフェースへの NAT ディスクリプタ適用の設定	122
13.2	NAT ディスクリプタの動作タイプの設定	122
13.3	NAT 処理の外側 IP アドレスの設定	123

13.4	NAT 処理の内側 IP アドレスの設定	123
13.5	NAT のアドレス割当をログに記録するか否かの設定	123
13.6	静的 NAT エントリの設定	123
13.7	IP マスカレード使用時に rlogin,rcp と ssh を使用するか否かの設定	124
13.8	外側から受信したパケットに該当する変換テーブルが存在しないときの動作の設定	124
13.9	静的 IP マスカレードエントリの設定	124
13.10	NAT の IP アドレスマップの消去タイマの設定	125
13.11	IP マスカレードで利用するポートの範囲の設定	125
13.12	FTP として認識するポート番号の設定	125
13.13	IP マスカレードで変換しないポート番号の範囲の設定	126
13.14	IP マスカレード変換時に DF ビットを削除するか否かの設定	126
13.15	SIP メッセージに含まれる IP アドレスを書き換えるか否かの設定	126
14.	DNS の設定	128
14.1	DNS を利用するか否かの設定	128
14.2	ルータ自身の FQDN の設定	128
14.3	DNS ドメイン名の設定	128
14.4	DNS サーバーの IP アドレスの設定	128
14.5	DNS サーバーを通知してもらう相手先情報番号の設定	129
14.6	DNS サーバーアドレスを取得する LAN インタフェースの設定	129
14.7	プライベートアドレスに対する問い合わせを処理するか否かの設定	129
14.8	DHCP/IPCP MS 拡張で DNS サーバーを通知する順序の設定	130
14.9	SYSLOG 表示で DNS により名前解決するか否かの設定	130
14.10	DNS 問い合わせの内容に応じた DNS サーバーの選択	130
14.11	静的 DNS レコードの登録	131
14.12	DNS 問い合わせパケットの始点ポート番号の設定	132
14.13	DNS サーバーへアクセスできるホストの IP アドレス設定	132
15.	優先制御	133
15.1	インタフェース速度の設定	133
15.2	キューイングアルゴリズムタイプの選択	133
15.3	クラス分けのためのフィルタ設定	133
15.4	デフォルトクラスの設定	134
15.5	クラス分けフィルタの適用	135
15.6	クラス毎のキュー長の設定	135
15.7	MP インタリーブの設定	135
16.	連携機能	137
16.1	連携動作を行なうか否かの設定	137
16.2	連携動作で使用するポート番号の設定	137
16.3	帯域測定で連携動作を行なう相手毎の動作の設定	137
16.4	負荷監視通知で連携動作を行なう相手毎の動作の設定	138
16.5	負荷監視サーバーとしての動作トリガの設定	139
16.6	負荷監視クライアントとしての動作の設定	140
16.7	連携動作の手動実行	140
17.	IPv6	141
17.1	共通の設定	141
17.1.1	IPv6 パケットを扱うか否かの設定	141
17.1.2	IPv6 インタフェースのリンク MTU の設定	141
17.1.3	TCP セッションの MSS 制限の設定	141
17.2	IPv6 アドレスの管理	142
17.2.1	インタフェースの IPv6 アドレスの設定	142
17.2.2	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	142
17.2.3	DHCPv6 の動作の設定	143
17.2.4	IPv6 で DAD(Duplicate Address Detection) の送信回数を設定する	143

17.3	近隣探索	143
17.3.1	ルータ広告で配布するプレフィックスの定義	143
17.3.2	ルータ広告の送信の制御	144
17.4	経路制御	145
17.4.1	IPv6 の経路情報の追加	145
17.5	RIPng	146
17.5.1	RIPng の使用の設定	146
17.5.2	インタフェースにおける RIPng の送信ポリシーの設定	146
17.5.3	インタフェースにおける RIPng の受信ポリシーの設定	146
17.5.4	RIPng の加算ホップ数の設定	147
17.5.5	インタフェースにおける信頼できる RIPng ゲートウェイの設定	147
17.5.6	RIPng で送受信する経路に対するフィルタリングの設定	147
17.5.7	回線接続時の PP 側の RIPng の動作の設定	147
17.5.8	回線接続時の PP 側の RIPng 送出の時間間隔の設定	148
17.5.9	回線切断時の PP 側の RIPng の動作の設定	148
17.5.10	回線切断時の PP 側の RIPng 送出の時間間隔の設定	148
17.5.11	RIPng による経路を回線切断時に保持するか否かの設定	148
17.6	フィルタの設定	149
17.6.1	IPv6 フィルタの定義	149
17.6.2	IPv6 フィルタの適用	149
17.6.3	IPv6 動的フィルタの定義	150
17.7	IPv6 マルチキャストパケットの転送の設定	150
17.7.1	MLD の動作の設定	151
17.7.2	MLD の静的な設定を登録するコマンド	152
18.	アナログ通信機能の設定	153
18.1	キー操作とコンソールコマンドの対応	153
18.2	TEL ポートごとの設定	154
18.2.1	TEL ポートを使うか否かの設定	154
18.2.2	TEL ポートのダイヤルイン番号の設定	154
18.2.3	TEL ポートに接続する機器の設定	155
18.2.4	TEL ポートの発信者番号を通知するか否かの設定	155
18.2.5	相手先番号による即時発信を許可するか否かの設定	155
18.2.6	ダイヤル完了ボタンの設定	156
18.2.7	グローバル着信を許可するか否かの設定	156
18.2.8	TEL ポートでの識別着信をするか否かの設定	156
18.2.9	識別着信リストの登録	157
18.2.10	サブアドレス無し着信を許可するか否かの設定	157
18.2.11	異なる種類の通信機器からの着信を許可するか否かの設定	157
18.2.12	話中着信を許可するか否かの設定	157
18.2.13	着信ベルリストの登録	158
18.2.14	ナンバー・ディスプレイの設定	158
18.2.15	指定した TEL ポートの優先着信順位を設定	159
18.2.16	ダイヤル桁間タイマの設定	159
18.2.17	フッキングを判定する時間の設定	159
18.2.18	フッキング後にキー操作を受け入れる時間の設定	159
18.2.19	フッキング及びオンフック検出を無効と判断する時間の設定	160
18.2.20	保留音の種類の設定	160
18.2.21	TEL ポートの再呼出時間設定	160
18.2.22	フレックスホン機能の使用パターンの設定	160
18.2.23	着信転送先アドレスの設定	161
18.2.24	着信転送を起動するタイミングの設定	161
18.2.25	着信転送トーキの設定	161
18.2.26	着信転送が拒否された時の動作の設定	162
18.2.27	送話 PAD の設定	162

18.2.28	受話 PAD の設定	162
18.2.29	MP 時に電話発着信のために 1B チャンネルに落とすか否かの設定	163
18.2.30	TEL ポートへの切断信号の送出の設定	163
18.2.31	DTMF 検出レベルの設定	163
18.2.32	アザーダイヤルトーンを出すか否かの設定	164
18.2.33	着信時の着信ベル鳴動モードの設定	164
18.2.34	i・ナンバーサービスのポート番号の設定	164
18.2.35	アナログダイヤルインと無鳴動着信機能の設定	164
18.2.36	PB ダイヤルインの一次応答検出タイミングの設定	165
18.2.37	発番号情報なし着信機能の設定	165
18.2.38	ポーズを判定する時間の設定	166
18.2.39	TEL ポートに対する電力供給の設定	166
18.3	アナログ回線の設定	166
18.3.1	ダイヤルの種別を選択	166
18.3.2	フッキング時間の設定	167
18.3.3	アナログ回線のモデム信号を検出するまでの時間を設定する	167
18.3.4	ナンバーディスプレイ (ダイヤルイン) の着信の識別設定	167
18.3.5	アナログ回線に対する受話 PAD の設定	167
18.3.6	アナログ回線に対する送話 PAD の設定	168
18.3.7	アナログ回線に対するポーズ時間の設定	168
18.3.8	付加サービス機能の設定	168
18.3.9	アナログ回線を使用するか否かの設定	168
19.	メール着信確認、メール転送、メール通知機能の設定	169
19.1	メール着信確認機能	169
19.1.1	メールサーバーの設定	169
19.1.2	メールチェックの実行	169
19.1.3	メールチェックの実行を許可するか否かの設定	169
19.1.4	メールチェックタイムアウトの設定	169
19.2	メール転送機能	170
19.2.1	送信メールサーバーの設定	170
19.2.2	送信先サーバーの設定	170
19.2.3	受信メッセージサーバーの設定	170
19.2.4	受信メッセージの最大長の設定	170
19.2.5	メール転送タイムアウトの設定	171
19.2.6	転送メッセージの最大長の設定	171
19.2.7	メール転送の実行	171
19.2.8	受信メッセージサーバー制限の設定	171
19.2.9	転送メッセージのフィルタ設定	172
19.2.10	メッセージ転送を禁止するか否かの設定	172
19.3	メール通知機能	172
19.3.1	送信情報の文字コードの設定	172
19.3.2	メール送信時のサブジェクトの指定	172
19.3.3	メール送信の実行	173
19.3.4	不正アクセス検知時のメール通知設定	173
19.3.5	不正アクセス検知時に通知されるメールのサブジェクト設定	173
19.3.6	不正アクセス検知情報をメールで通知する	173
20.	HTTP サーバー機能 (かんたん設定 / プロバイダ設定) の設定	174
20.1	プロバイダ接続タイプの設定	174
20.2	プロバイダ名称の設定	174
20.3	トンネル接続の名称の設定	174
20.4	プロバイダ情報の PP との関連付けと名前の設定	174
20.5	プロバイダの接続設定	175
20.6	プロバイダの DNS サーバーのアドレス設定	175
20.7	LAN インタフェースの DNS サーバーのアドレスの設定	175

20.8	DNS サーバーを通知してくれる相手の相手先情報番号の設定	175
20.9	フィルタ型ルーティングの形式の設定	176
20.10	LAN 側のプロバイダ名称の設定	176
20.11	プロバイダに対する昼間課金単位時間の設定	176
20.12	プロバイダに対する昼間課金単位時間方式での単位時間と監視時間の設定	177
20.13	プロバイダに対する夜間課金単位時間の設定	177
20.14	プロバイダに対する夜間課金単位時間方式での単位時間と監視時間の設定	177
20.15	NTP サーバーの設定	178
20.16	プロバイダに対する自動切断タイマ無効時間の設定	178
20.17	プロバイダに対する夜間料金時間の設定	178
20.18	プロバイダの NTP サーバーのアドレス設定	178
20.19	MP 使用時間帯の設定	179
20.20	かんたん設定ページの切断ボタンを押した後に自動接続するか否かの設定	179
20.21	かんたん設定ページで IPv6 接続を行なうか否かの設定	179
20.22	プロバイダ情報とトンネルとの関連付け	179
20.23	LAN インターフェースのプロバイダ情報とトンネルとの関連付け	179
20.24	HTTP サーバー機能の有無の設定	180
20.25	HTTP サーバーへアクセスできるホストの IP アドレス設定	180
20.26	HTTP サーバーのセッションタイムアウト時間の設定	180
20.27	HTTP サーバー機能の listen ポートの設定	180
21.	UPnP の設定	181
21.1	UPnP を使用するか否かの設定	181
21.2	UPnP に使用する IP アドレスを取得するインターフェースの設定	181
21.3	UPnP のポートマッピング用消去タイマのタイプの設定	181
21.4	UPnP のポートマッピングの消去タイマの設定	181
21.5	UPnP の syslog を出力するか否かの設定	182
22.	USB の設定	183
22.1	USB ホスト機能を使うか否かの設定	183
22.2	USB メモリに保存する SYSLOG ファイル名の指定	183
22.3	USB ボタンと DOWNLOAD ボタン同時押下による設定ファイル、ファームウェアファイルのコピー操作を許可するか否かの設定 ..	183
22.4	USB ボタンと DOWNLOAD ボタン同時押下によりコピーする設定ファイル名の指定	183
22.5	USB ボタンと DOWNLOAD ボタン同時押下によりコピーするファームウェアファイル名の指定 ..	184
23.	スケジュール	185
23.1	スケジュールの設定	185
24.	操作	187
24.1	相手先情報番号の選択	187
24.2	トンネルインターフェース番号の選択	187
24.3	設定に関する操作	187
24.3.1	管理ユーザへの移行	187
24.3.2	終了	187
24.3.3	設定内容の保存	188
24.3.4	設定ファイルの複製	188
24.3.5	ファームウェアファイルを内蔵フラッシュ ROM にコピー	188
24.3.6	設定ファイルの削除	188
24.3.7	設定ファイルの一覧	188
24.3.8	設定の初期化	189
24.3.9	遠隔地のルータの設定	189
24.3.10	遠隔地のルータからの設定に対する制限	189
24.4	動的情報のクリア操作	189
24.4.1	ARP テーブルのクリア	189
24.4.2	IP の動的経路情報のクリア	189
24.4.3	ログのクリア	190

24.4.4	アカウントのクリア	190
24.4.5	TEL ポートに関するアカウントのクリア	190
24.4.6	DNS キャッシュのクリア	190
24.4.7	NAT アドレステーブルのクリア	190
24.4.8	インタフェースの NAT アドレステーブルのクリア	191
24.4.9	IPv6 の動的経路情報の消去	191
24.4.10	近隣キャッシュの消去	191
24.5	その他の操作	191
24.5.1	相手先の使用許可の設定	191
24.5.2	相手先の使用不許可の設定	191
24.5.3	再起動	191
24.5.4	インタフェースの再起動	192
24.5.5	PP インタフェースの再起動	192
24.5.6	発信	192
24.5.7	切断	192
24.5.8	DTCP セッションの手動接続	192
24.5.9	DTCP セッションの手動切断	193
24.5.10	ping の実行	193
24.5.11	ping6 の実行	193
24.5.12	traceroute の実行	193
24.5.13	traceroute6 の実行	194
24.5.14	nslookup	194
24.5.15	メールチェックの結果の消去	194
24.5.16	TELNET クライアント	194
24.5.17	IPv4 動的フィルタのコネクション管理情報の削除	195
24.5.18	IPv6 動的フィルタのコネクション管理情報の削除	195
24.5.19	ファームウェアのチェックおよびリビジョンアップ	195
24.5.20	Magic Packet の送信	195
25.	設定の表示	197
25.1	機器設定の表示	197
25.2	すべての設定内容の表示	197
25.3	指定した PP の設定内容の表示	197
25.4	指定したトンネルの設定内容の表示	197
25.5	設定ファイルの一覧	197
25.6	ファイル情報の一覧の表示	198
25.7	インタフェースに付与されている IPv6 アドレスの表示	198
25.8	SSH サーバー 公開鍵の表示	198
26.	状態の表示	199
26.1	ARP テーブルの表示	199
26.2	IP の経路情報テーブルの表示	199
26.3	RIP で得られた経路情報の表示	199
26.4	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	199
26.5	侵入情報の履歴の表示	200
26.6	IPv6 の経路情報の表示	200
26.7	近隣キャッシュの表示	200
26.8	IPv6 の RIP テーブルの表示	200
26.9	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	201
26.10	ネットワーク監視機能の状態の表示	201
26.11	相手先ごとの接続時間情報の表示	201
26.12	動的 NAT ディスクリプタのアドレスマップの表示	201
26.13	動作中の NAT ディスクリプタの適用リストの表示	201
26.14	LAN インタフェースの NAT ディスクリプタのアドレスマップの表示	202
26.15	起動時の情報の表示	202
26.16	インタフェースの状態の表示	202

26.17	各相手先の状態の表示	202
26.18	トンネルインタフェース情報の表示	202
26.19	DTCP セッション情報の表示	203
26.20	DHCP サーバーの状態の表示	203
26.21	DHCP クライアントの状態の表示	203
26.22	DHCPv6 の状態の表示	203
26.23	MLD の状態の表示	203
26.24	PPTP の状態の表示	204
26.25	アナログ関係の状態の表示	204
26.26	音声通話の接続状態の表示	204
26.27	メールチェックの状態表示	204
26.28	UPnP に関するステータス情報の表示	204
26.29	パケットバッファの状態を表示する	204
26.30	QoS ステータスの表示	205
26.31	連携動作の状態の表示	205
26.32	ルータにログインしているユーザの情報を表示する	206
26.33	USB ホスト機能の動作状態を表示	206
27.	ロギング	207
27.1	ログの表示	207
27.2	アカウントの表示	207
27.3	アナログ関係のアカウントの表示	207
27.4	アナログ回線のアカウントの表示	208
27.5	通信履歴の表示	208

コマンド索引

A

account threshold	58
account threshold pp	58
administrator	24, 187
administrator password	37
administrator password encrypted	37
alarm connection analog	46
alarm connection data	47
alarm entire	47
alarm intrusion	47
alarm mp	47
alarm ushhost	47
analog arrive another-device permit	157
analog arrive global permit	156
analog arrive incoming-signal	164
analog arrive incoming-signal timing pb	165
analog arrive inumber-port	164
analog arrive number display	158
analog arrive priority	159
analog arrive restrict	156
analog arrive restrict list	157
analog arrive ringer-type list	158
analog arrive ring-while-talking permit	157
analog arrive without-calling-number	165
analog arrive without-subaddress permit	157
analog device type	155
analog disc-signal	163
analog dtmf level	163
analog end-of-dialing-code	156
analog extension incoming ringer	164
analog extension other-dial-tone	164
analog hooking inhibit timer	160
analog hooking timer	159
analog hooking wait timer	159
analog http revision-up permit	49
analog local address	154
analog local address notice	155
analog mp prior	163
analog pad receive	162
analog pad send	162
analog pause timer	166
analog power	166
analog rapid call	155
analog re-ringing-timer	160
analog supplementary-service	160
analog supplementary-service call-deflection address	161
analog supplementary-service call-deflection reject	162
analog supplementary-service call-deflection ringer	161
analog supplementary-service call-deflection talkie	161
analog use	154
analog wait dial timer	159
audio echo-canceller	50
audio echo-canceller disabler	51

audio echo-canceller nlp threshold	51
audio hold-tone type	160

C

clear account	190
clear account analog	190
clear account pp	190
clear account pstn	190
clear arp	189
clear dns cache	190
clear ip dynamic routing	189
clear ipv6 dynamic routing	191
clear ipv6 neighbor cache	191
clear log	190
clear mail-check info	194
clear nat descriptor dynamic	190
clear nat descriptor interface dynamic	191
clear nat descriptor interface dynamic pp	191
clear nat descriptor interface dynamic tunnel	191
cold start	22, 189
connect	192
console character	24, 41
console columns	41
console info	42
console lines	41
console prompt	39
cooperation	137, 140
cooperation bandwidth-measuring remote	137
cooperation load-watch control	140
cooperation load-watch remote	138
cooperation load-watch trigger	139
cooperation port	137
copy config	188
copy exec	188

D

date	40
delete config	188
description	46
dhcp client client-identifier	109
dhcp client client-identifier pool	109
dhcp client client-identifier pp	109
dhcp client hostname	109
dhcp client option	110
dhcp convert lease to bind	105
dhcp duplicate check	102
dhcp manual lease	107
dhcp manual release	107
dhcp relay select	107
dhcp relay server	107
dhcp relay threshold	108
dhcp scope	103
dhcp scope bind	103
dhcp scope lease type	106
dhcp scope option	105
dhcp server rfc2131 compliant	102

dhcp service	101
disconnect	24, 192
disconnect ip connection	195
disconnect ipv6 connection	195
disconnect user	56
dns domain	128
dns host	132
dns notice order	130
dns private address spoof	129
dns private name	128
dns server	128
dns server dhcp	129
dns server pp	129
dns server select	130
dns service	128
dns srcport	132
dns static	131
dns syslog resolv	130
E	
ethernet filter	86
ethernet interface filter	87
exit	187
H	
help	36
http revision-down permit	49
http revision-up go	195
http revision-up permit	48
http revision-up proxy	48
http revision-up timeout	48
http revision-up url	48
httpd host	180
httpd listen	180
httpd service	180
httpd timeout	180
I	
interface reset	192
interface reset pp	192
ip arp timer	78
ip filter	70
ip filter directed-broadcast	72
ip filter dynamic	72
ip filter dynamic timer	74
ip filter set	71
ip filter source-route	72
ip fragment remove df-bit filter	76
ip host	131
ip icmp echo-reply send	111
ip icmp echo-reply send-only-linkup	111
ip icmp log	113
ip icmp mask-reply send	111
ip icmp parameter-problem send	111
ip icmp redirect receive	112
ip icmp redirect send	112
ip icmp time-exceeded send	112
ip icmp timestamp-reply send	112
ip icmp unreachable send	112
ip interface address	68
ip interface arp queue length	77
ip interface arp static	78
ip interface dhcp lease time	108
ip interface dhcp retry	108
ip interface intrusion detection	74
ip interface intrusion detection notice-interval	74
ip interface intrusion detection repeat-control	75
ip interface intrusion detection report	75
ip interface intrusion detection threshold	75
ip interface mtu	77
ip interface nat descriptor	122
ip interface proxyarp	77
ip interface rip auth key	83
ip interface rip auth type	83
ip interface rip filter	82
ip interface rip hop	82
ip interface rip receive	82
ip interface rip send	81
ip interface rip trust gateway	81
ip interface secondary address	69
ip interface secure filter	76
ip interface tcp mss limit	73
ip interface wol relay	51
ip keepalive	85
ip pp address	68
ip pp intrusion detection	74
ip pp intrusion detection notice-interval	74
ip pp intrusion detection repeat-control	75
ip pp intrusion detection report	75
ip pp intrusion detection threshold	75
ip pp mtu	77
ip pp nat descriptor	122
ip pp remote address	78
ip pp remote address pool	79
ip pp rip auth key	83
ip pp rip auth type	83
ip pp rip connect interval	84
ip pp rip connect send	84
ip pp rip disconnect interval	84
ip pp rip disconnect send	84
ip pp rip filter	82
ip pp rip hold routing	83
ip pp rip hop	82
ip pp rip receive	82
ip pp rip send	81
ip pp rip trust gateway	81
ip pp secure filter	76
ip pp tcp mss limit	73
ip route	69
ip route change log	70
ip routing	68
ip routing process	45
ip simple-service	75
ip stealth	113
ip tunnel address	117
ip tunnel intrusion detection	74
ip tunnel intrusion detection notice-interval	74
ip tunnel intrusion detection repeat-control	75
ip tunnel intrusion detection report	75

ip tunnel intrusion detection threshold	75	ipv6 rip use	146
ip tunnel mtu	77	ipv6 route	145
ip tunnel nat descriptor	122	ipv6 routing	141
ip tunnel remote address	117	ipv6 stealth	115
ip tunnel rip auth key	83	ipv6 tunnel address	142
ip tunnel rip auth type	83	ipv6 tunnel dhcp service	143
ip tunnel rip filter	82	ipv6 tunnel mld	151
ip tunnel rip hop	82	ipv6 tunnel mld static	152
ip tunnel rip receive	82	ipv6 tunnel prefix	142
ip tunnel rip send	81	ipv6 tunnel rip filter	147
ip tunnel rip trust gateway	81	ipv6 tunnel rip receive	146
ip tunnel secure filter	76	ipv6 tunnel rip send	146
ip tunnel tcp mss limit	73	ipv6 tunnel secure filter	149
ipv6 filter	149	ipv6 tunnel tcp mss limit	141
ipv6 filter dynamic	150	isdn arrive inumber-port	67
ipv6 icmp echo-reply send	113	isdn arrive permit	60
ipv6 icmp echo-reply send-only-linkup	114	isdn auto connect	60
ipv6 icmp log	115	isdn auto disconnect	60
ipv6 icmp packet-too-big send	115	isdn call block time	61
ipv6 icmp parameter-problem send	114	isdn call permit	61
ipv6 icmp redirect receive	114	isdn call prohibit auth-error count	66
ipv6 icmp redirect send	114	isdn call prohibit mp-error count	66
ipv6 icmp time-exceeded send	114	isdn call prohibit time	62
ipv6 icmp unreachable send	115	isdn callback mscbcip user-specify	63
ipv6 interface address	142	isdn callback permit	62
ipv6 interface dad retry count	143	isdn callback permit type	62
ipv6 interface dhcp service	143	isdn callback request	62
ipv6 interface mld	151	isdn callback request type	62
ipv6 interface mld static	152	isdn callback response time	63
ipv6 interface mtu	141	isdn callback wait time	63
ipv6 interface prefix	142	isdn disconnect input time	64
ipv6 interface rip filter	147	isdn disconnect interval time	65
ipv6 interface rip hop	147	isdn disconnect output time	64
ipv6 interface rip receive	146	isdn disconnect policy	63
ipv6 interface rip send	146	isdn disconnect time	64
ipv6 interface rip trust gateway	147	isdn fast disconnect time	65
ipv6 interface rtadv send	144	isdn forced disconnect time	65
ipv6 interface secure filter	149	isdn local address	57
ipv6 interface tcp mss limit	141	isdn piafs arrive	59
ipv6 pp address	142	isdn piafs call	58
ipv6 pp dad retry count	143	isdn piafs control	59
ipv6 pp dhcp service	143	isdn remote address	60
ipv6 pp mld	151	isdn remote call order	61
ipv6 pp mld static	152	isdn use	57
ipv6 pp mtu	141		
ipv6 pp prefix	142		
ipv6 pp rip connect interval	148	L	
ipv6 pp rip connect send	147	lan shutdown	45
ipv6 pp rip disconnect interval	148	lan type	45
ipv6 pp rip disconnect send	148	leased keepalive down	81
ipv6 pp rip filter	147	less config	197
ipv6 pp rip hold routing	148	less config list	188, 197
ipv6 pp rip hop	147	less config pp	197
ipv6 pp rip receive	146	less config tunnel	197
ipv6 pp rip send	146	less file list	198
ipv6 pp rip trust gateway	147	less log	207
ipv6 pp rtadv send	144	line type	31, 57
ipv6 pp secure filter	149	login password	37
ipv6 pp tcp mss limit	141	login password encrypted	37
ipv6 prefix	143	login timer	24, 40

login user	37	pp connect time threshold	66
M		pp disable	24, 191
mail-check go	169	pp enable	24, 191
mail-check prohibit	169	pp keepalive interval	79
mail-check server	169	pp keepalive log	80
mail-check timeout	169	pp keepalive use	80
mail-notify charset	172	pp name	174
mail-notify go	173	pp select	187
mail-notify intrusion	173	ppp ccp maxconfigure	95
mail-notify intrusion go	173	ppp ccp maxfailure	96
mail-notify intrusion subject	173	ppp ccp maxterminate	95
mail-notify subject	172	ppp ccp no-encryption	121
mail-transfer filter	172	ppp ccp restart	95
mail-transfer go	171	ppp ccp type	95, 118
mail-transfer prohibit	172	ppp chap maxchallenge	92
mail-transfer receive from	170	ppp chap restart	92
mail-transfer receive maxlength	170	ppp ipcp ipaddress	92
mail-transfer receive restrict	171	ppp ipcp maxconfigure	93
mail-transfer send maxlength	171	ppp ipcp maxfailure	93
mail-transfer send to	170	ppp ipcp maxterminate	93
mail-transfer server	170	ppp ipcp msexit	94
mail-transfer timeout	171	ppp ipcp remote address check	94
		ppp ipcp restart	93
		ppp ipcp vjc	92
N		ppp ipv6cp use	96
nat descriptor address inner	123	ppp lcp acfc	89
nat descriptor address outer	123	ppp lcp magicnumber	90
nat descriptor ftp port	125	ppp lcp maxconfigure	91
nat descriptor log	123	ppp lcp maxfailure	91
nat descriptor masquerade incoming	124	ppp lcp maxterminate	91
nat descriptor masquerade port range	125	ppp lcp mru	90
nat descriptor masquerade remove df-bit	126	ppp lcp pfc	90
nat descriptor masquerade rlogin	124	ppp lcp restart	90
nat descriptor masquerade static	124	ppp lcp silent	91
nat descriptor masquerade unconvertible port	126	ppp mp control	96
nat descriptor sip	126	ppp mp divide	97
nat descriptor static	123	ppp mp interleave	135
nat descriptor timer	125	ppp mp load threshold	96
nat descriptor type	122	ppp mp maxlink	97
nslookup	194	ppp mp minlink	97
ntpdate	41	ppp mp timer	97
		ppp mp use	96
		ppp mscbcx maxretry	94
O		ppp mscbcx restart	94
operation http revision-up permit	49	ppp pap maxauthreq	92
operation usb-download permit	183	ppp pap restart	91
		pppoe	100
P		pppoe access concentrator	98
password reenter	49	pppoe auto connect	98
ping	193	pppoe auto disconnect	98
ping6	193	pppoe call prohibit auth-error count	100
pp always-on	59	pppoe disconnect time	99
pp auth accept	89, 120	pppoe padi maxretry	98
pp auth multi connect prohibit	89	pppoe padi restart	99
pp auth myname	89	pppoe padr maxretry	99
pp auth request	88, 119	pppoe padr restart	99
pp auth username	88	pppoe service-name	100
pp bind	58, 118	pppoe tcp mss limit	99
pp connect count threshold	66	pppoe use	98
		pptp call-id mode	119

pptp hostname	118
pptp keepalive interval	121
pptp keepalive log	121
pptp keepalive use	120
pptp service	118
pptp service type	118
pptp syslog	119
pptp tunnel disconnect time	120
pptp window size	119
provider auto connect forced disable	179
provider bind	179
provider dns server	175
provider dns server pp	175
provider filter routing	176
provider interface dns server	175
provider interface name	176
provider ipv6 connect pp	179
provider isdn account nighttime	178
provider isdn auto disconnect off	178
provider isdn disconnect daytime	176
provider isdn disconnect interval daytime	177
provider isdn disconnect interval nighttime	177
provider isdn disconnect nighttime	177
provider ntp server	178
provider ntpdate	178
provider pp bind	179
provider ppp mp use on	179
provider select	175
provider set	174
provider type	174
pstn dial type	166
pstn hooking timer	167
pstn modem signal timer	167
pstn number display	167
pstn pad receive	167
pstn pad send	168
pstn pause timer	168
pstn supplementary-service	168
pstn use	168

Q

queue class filter	133
queue interface class filter list	135
queue interface default class	134
queue interface length	135
queue interface type	133
queue pp class filter list	135
queue pp default class	134
queue pp length	135
queue pp type	133
quit	187

R

rdate	40
remote setup	189
remote setup accept	189
restart	31, 191
rip use	81

S

save	24, 188
schedule at	185
security class	39
show	34, 35
show account	207
show account analog	207
show account pp	207
show account pstn	208
show arp	199
show command	36
show config	197
show config list	188, 197
show config pp	197
show config tunnel	197
show environment	197
show file list	198
show history	208
show ip connection	199
show ip connection pp	199
show ip connection tunnel	199
show ip intrusion detection	200
show ip intrusion detection pp	200
show ip intrusion detection tunnel	200
show ip rip table	199
show ip route	199
show ipv6 address	198
show ipv6 connection	201
show ipv6 connection pp	201
show ipv6 connection tunnel	201
show ipv6 neighbor cache	200
show ipv6 rip table	200
show ipv6 route	200
show log	207
show nat descriptor address	201
show nat descriptor interface address	202
show nat descriptor interface address pp	202
show nat descriptor interface address tunnel	202
show nat descriptor interface bind	201
show nat descriptor interface bind pp	201
show nat descriptor interface bind tunnel	201
show pp connect time	201
show sshd public key	198
show status	202
show status analog	204
show status boot	202
show status cooperation	205
show status dhcp	203
show status dhcpc	203
show status dtcp	203
show status ip keepalive	201
show status ipv6 dhcp	203
show status ipv6 mld	203
show status mail-check	204
show status packet-buffer	204
show status pp	202
show status pptp	204
show status qos	205
show status tunnel	202

show status upnp	204
show status usbhost	206
show status user	206
show status voice call	204
speed	133
sshd client alive	55
sshd host	54
sshd host key generate	54
sshd listen	53
sshd service	53
sshd session	54
syslog debug	43
syslog facility	42
syslog host	42
syslog info	42
syslog local address	43
syslog notice	42
syslog srcport	43
system packet-buffer	55

T

tcp log	52
telnet	194
telnetd host	44
telnetd listen	44
telnetd service	43
telnetd session	44
tftp host	31, 45
time	40
timezone	40
traceroute	193
traceroute6	194
tunnel disable	116
tunnel dtcp	117
tunnel dtcp connect	192
tunnel dtcp disconnect	193
tunnel enable	116
tunnel encapsulation	116, 118
tunnel endpoint address	116, 118
tunnel endpoint name	120
tunnel name	174
tunnel select	187

U

upnp external address refer	181
upnp external address refer pp	181
upnp port mapping timer	181
upnp port mapping timer type	181
upnp syslog	182
upnp use	181
usbhost config filename	183
usbhost exec filename	184
usbhost syslog filename	183
usbhost use	183
user attribute	38

W

wins server	93
wol send	195

1. コマンドリファレンスの見方

1.1 コマンドリファレンスの見方

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

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

1.2 インタフェース名について

コマンドの入力形式において、ルータの各インタフェースを指定するためにインタフェース名を利用します。インタフェース名は、インタフェース種別とインタフェース番号を間に空白をおかずに続けて表記します。インタフェース種別には、"lan"、"bri" があります。

ポートの名称	インタフェースの種別	インタフェース名
LAN ポート	LAN インタフェース	lan1
WAN ポート	LAN インタフェース	lan2
ISDN U ポート	BRI インタフェース	bri1
ISDN S/T ポート	BRI インタフェース	bri1

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

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

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

1.4 コマンドの入力文字数とエスケープシーケンスについて

1つのコマンドとして入力できる文字数は、コマンド本体とパラメータ部分を含めて最大 4095 文字以内、キーワードの合計が 1024 以内です。

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

特殊文字	入力	特殊文字	入力
?	\? '?' "?"	,	\, ''''
#	\# '#' "#"	"	\" ''''
\	\\	空白	¥の後ろに空白 ' ' " "

1.5 工場出荷設定値について

本製品をお買いあげ頂いた状態及び **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。

本製品の工場出荷設定：

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

2. コマンドの使い方

本製品に直接コマンドを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식을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 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なうことができます。

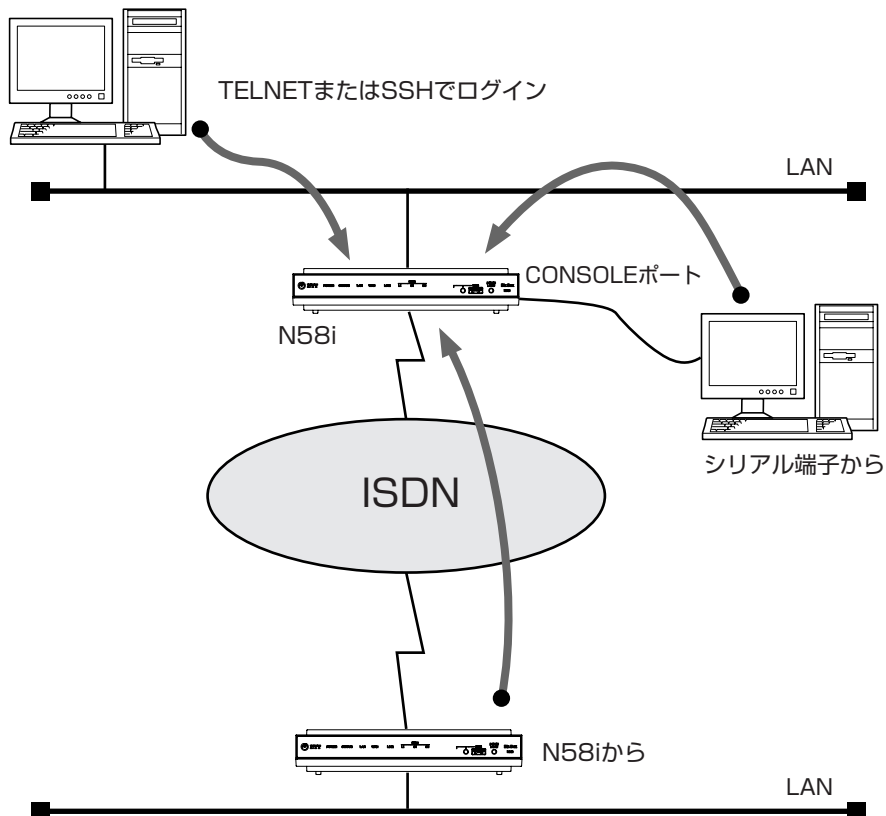
対話的に設定する手段をコンソールと呼び、コマンドを1つ1つ実行して設定や操作を行なうことができます。必要なコマンド一식을記述したファイルを設定ファイル (Config) と呼び、TFTP により本製品にアクセスできる環境から設定ファイルを送信したり受信することが可能です。

2.1 コンソールについて

各種の設定を行なうためには、本製品の 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、ISDN 回線や専用線を介して別の N58i からログインする方法の3つがあります。

本製品へのアクセス方法
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
ISDN 回線や専用線を介して別の N58i からログイン

本製品へは、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なうこともできます。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なう場合は、まず本製品の 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 で設定を行なう場合は、パソコンでは TELNET アプリケーションを使います。Windows をお使いの場合は OS に付属の『TELNET』ソフトウェアを使用します。MacOS X をお使いの場合は、OS に付属の『ターミナル』アプリケーションで telnet コマンドを実行します。

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

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

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

設定手順のおおまかな流れは次のようになります。

1. 一般ユーザとしてログインした後、**administrator** コマンドで管理ユーザとしてアクセスします。この時管理パスワードが設定してあれば、管理パスワードの入力が必要です。
2. 回線を接続していない相手の相手先情報を変更する場合には、**pp disable** コマンドを実行してから相手先情報の内容を変更してください。回線が接続されている場合には、**disconnect** コマンドでまず回線を手動切断しておきます。
3. 相手先情報の内容を各種コマンドを使用して変更します。
4. **pp enable** コマンドを実行します。
5. **save** コマンドを実行して、不揮発性メモリに設定内容を保存します。

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

セキュリティの観点から、コンソールにキー入力がない一定時間無き時には、自動的に 300 秒（初期値）でログアウトするように設定されています。この時間は **login timer** コマンドを使用して変更することができます。

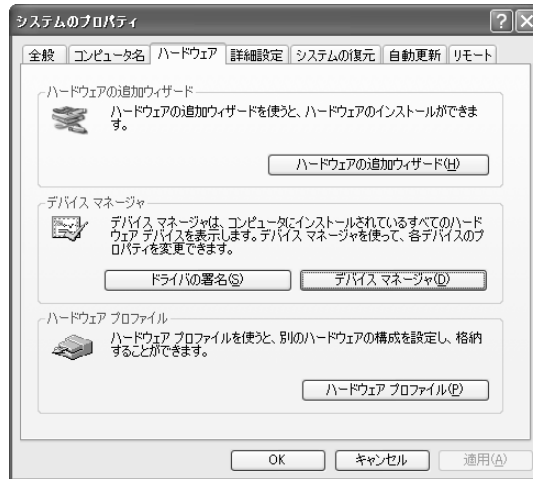
新たに管理ユーザになって設定コマンドを実行すると、その内容はすぐに動作に反映されますが、**save** コマンドを実行しないと不揮発性メモリに書き込まれません。

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

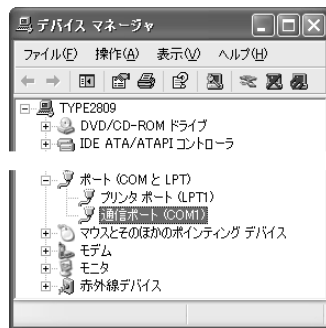
2.1.2 CONSOLE ポートからの設定

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

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



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



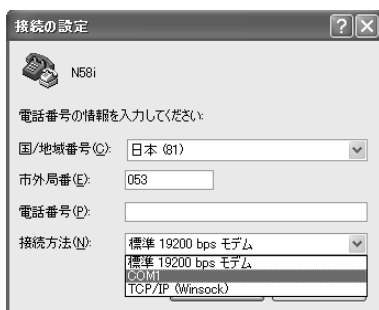
3. 「デバイス マネージャ」ウィンドウを閉じます。

2. コマンドの使い方

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



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



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



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

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

```

Password:
N58i BootROM Ver. 1.01
N58i Rev.9.01.36 (Thu Nov 20 10:07:08 2008)
Copyright (c) 1994-2008 Yamaha Corporation.
Copyright (c) 1998-2000 Tokyo Institute of Technology.
Copyright (c) 2000 Japan Advanced Institute of Science and Technology, HOKURIK
U.
Copyright (c) 2002 RSA Security Inc. All rights reserved.
Copyright (c) 1997-2004 University of Cambridge. All rights reserved.
Copyright (C) 1997 - 2002, Makoto Matsumoto and Takuji Nishimura, All rights r
eserved.
Copyright (c) 1995 Tatu Ylonen, Espoo, Finland All rights reserved.
Copyright (c) 1998-2004 The OpenSSL Project. All rights reserved.
Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.
00:a0:de:3d:64:5e, 00:a0:de:3d:64:5f
Memory 32Mbytes, 2LAN, 1BRI
> administrator
Password:
#
# quit
> -

```

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

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

2.1.3 TELNET による設定

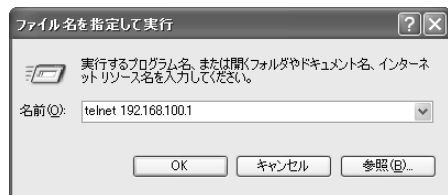
ここでは、Windows XP の TELNET を使用する場合を例に説明します。本製品の IP アドレスは 192.168.100.1 とした場合の例です。

1. [スタート] メニューから [ファイル名を指定して実行] を選びます。



2. コマンドの使い方

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



- 「Password:」と表示されたら、ログインパスワードを入力してから Enter キーを押します。
※設定した名前ありユーザでログインする場合は、何も入力せずに Enter キーを押します。次に「Username:」と表示され、ユーザ名の入力待ち状態となります。ここで、設定したユーザ名を入力して Enter キーを押し、続いてユーザパスワードを入力します。
何も表示されないときは、1 度 Enter キーを押します。
「>」が表示されると、コンソールコマンドを入力できるようになります。

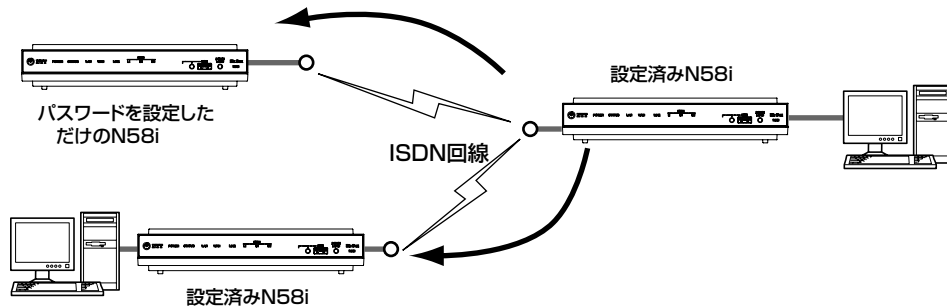


- 【ノート】
- ・「**help**」と入力してから Enter キーを押すと、キー操作の説明が表示されます。
 - ・「**show command**」と入力してから Enter キーを押すと、コマンド一覧が表示されます。

- 「**administrator**」と入力してから、Enter キーを押します。
- 「Password:」と表示されたら、管理パスワードを入力します。
「#」が表示されると、各種のコンソールコマンドを入力できます。
- コンソールコマンドを入力して、設定を行いません。
- 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、本製品の不揮発性メモリに保存されます。
- 設定を終了するには、「**quit**」と入力してから Enter キーを押します。
- コンソール画面を終了するには、もう 1 度「**quit**」と入力してから Enter キーを押します。

2.1.4 リモートセットアップ

N58i を使えば、ISDN 回線や専用線経由で離れた場所の N58i を設定することができます。これを「リモートセットアップ」といいます。パスワードが設定された N58i であれば、リモートセットアップで設定することが可能です。ISDN 回線や専用線経由で相手の N58i に直接接続するので、プロバイダに契約していなくても、インターネット接続できない状態でも設定できます。



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

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

相手の N58i へのログインが完了すると、コンソールコマンドで設定できるようになります。

【ご注意】 ・ FTTH や CATV、ADSL などの WAN ポート経由で、リモートセットアップすることはできません。

2.2 SSH サーバーについて

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

2.2.1 使用に当たっての注意事項

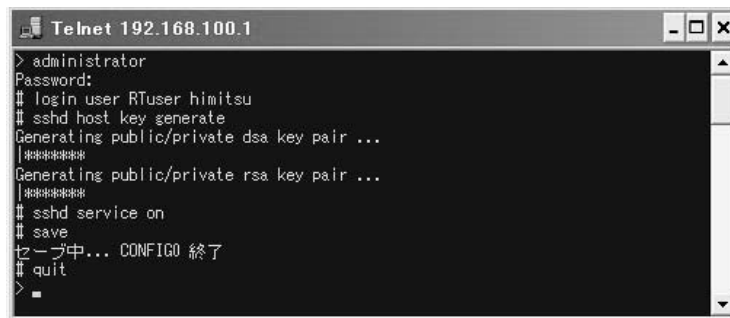
SSH サーバー機能では以下の機能をサポートしていないことに注意してください。

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

2.2.2 SSH サーバーの設定

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

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



```
Telnet 192.168.100.1
> administrator
Password:
# login user RTuser himitsu
# sshd host key generate
Generating public/private dsa key pair ...
*****
Generating public/private rsa key pair ...
*****
# sshd service on
# save
セーブ中... CONFIGO 終了
# quit
>
```

2.3 TFTP について

本製品に設定した項目は、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製品に読み込ませて設定を行なうこともできます。

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、本製品は TFTP サーバーとして動作します。

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

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

2.3.1 TFTP による設定手順

TFTP により設定ファイルをやりとりするためには、本製品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、本製品にアクセスできるホストを設定します。工場出荷設定ではどのホストからもアクセスできない設定になっていることに注意してください。



```
Telnet 192.168.100.1
> administrator
Password:
# tftp host 192.168.100.25
# save
セーブ中... CONFIGO 終了
# quit
>
```

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

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

2.3.2 設定ファイルの読み出し

ここでは、Windows XP から設定ファイルを読み出す場合の例を示します。本製品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、本製品の IP アドレスを 192.168.100.1、管理パスワードは “himitsu”、Windows に新しくできるファイルの名称を “OLDconfig.txt” とします。

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



```
コマンド プロンプト
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>cd N58i
C:\N58i>tftp 192.168.100.1 get config/himitsu OLDconfig.txt
Transfer successful: 2643 bytes in 1 second, 2643 bytes/s
C:\N58i>
```


2.3.3 設定ファイルの書き込み

ここでは、Windows XP から設定ファイルを書き込む場合の例を示します。本製品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、本製品の IP アドレスを 192.168.100.1、管理パスワードは “himitsu”、書き込むべき Windows 上のファイルの名称を “NEWconfig.txt” とします。

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

```

コマンド プロンプト
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>
C:\>cd N58i

C:\N58i>tftp 192.168.100.1 put NEWconfig.txt config/himitsu
Transfer successful: 2643 bytes in 1 second, 2643 bytes/s

C:\N58i>

```

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い場合は、**console lines infinity** コマンドを実行します。

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

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

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

説明：

n 数字のキー入力で整数値を表します。省略時は '1' です。

Ctrl-X [Ctrl] キーを押しながら [X] キーを押すことを示します。

2.5 「show」で始まるコマンド

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

これらの機能は「show」で始まるすべてのコマンドで利用できます。

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

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

[設定値]

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

【説明】

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

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

また、grep は一行に繰り返し指定することもできる。更に、**less** コマンドと同時に使用することもできる。

pattern 中の文字として '\$','?','|' を使用する場合は、それらの文字の前に '\$' をもう一つ重ねて入力しなければならない。

【設定例】

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

2.5.2 show コマンドの表示内容を見やすくする

【書式】

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

【説明】

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

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

3. ヘルプ

3.1 コンソールに対する簡易説明の表示

〔書式〕	help
〔設定値〕	なし
〔説明〕	コンソールの使用方法の簡単な説明を表示する。

3.2 コマンド一覧の表示

〔書式〕	show command
〔設定値〕	なし
〔説明〕	コマンドの名称とその簡単な説明を一覧表示する。

4. 機器の設定

4.1 ログインパスワードの設定

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

4.2 無名ユーザのパスワードを暗号化して保存する

- [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。
- [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**
- [設定値] なし
- [説明] 管理ユーザとしてルータの設定を変更する為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。

4.4 管理ユーザのパスワードを暗号化して保存する

- [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。
- [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] ◦ *user* ユーザ名 (32 文字以内)
 ◦ *password* パスワード (32 文字以内)
- [説明] ログインユーザ名とパスワードを設定する。

登録できるユーザは最大 32 人。

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

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

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

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

[ノート] 同一のユーザ名を複数登録することはできない。

既に登録されているユーザ名で設定を行った場合は、元の設定が上書きされる。

[初期値] 設定ユーザなし

4.6 ユーザの属性を設定

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

[設定値]

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

[説明] ユーザの属性を設定する。属性には、以下のものがある。

<i>attribute</i>	<i>value</i>	説明
administrator	on	administrator コマンドにより管理ユーザに昇格することができる。
	off	administrator コマンドにより管理ユーザに昇格することができない。
connection	off	すべての接続を禁止する。
	all	すべての接続を許可する。
	serial	シリアルコンソールからの接続を許可する。
	telnet	TELNET による接続を許可する。
	ssh	SSH による接続を許可する。
	remote	リモートセットアップによる接続を許可する。
host	IP アドレス	指定したホストからの接続を許可する。
	any	すべてのホストからの接続を許可する。
multi-session	on	同一ユーザ名による TELNET または、SSH での複数接続を許可する。
	off	同一ユーザ名による TELNET または、SSH での複数接続を禁止する。
login-timer	30..21474836, clear	ログインタイマを設定する。

[ノート] *user* を省略した場合は、無名ユーザの属性を設定する。

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

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

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

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

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

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

無名ユーザに対しては SSH による接続を許可することができない。

無名ユーザに対しては TELNET での複数接続はできない。

TELNET または SSH 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。

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

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

4.7 セキュリティクラスの設定

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

[設定値]

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

[説明] セキュリティクラスを設定する。

[ノート] **remote setup accept** コマンドにより、遠隔地のルータからのログイン (**remote setup**) を細かくアクセス制限することができる。遠隔地のルータからのログイン機能は、回線交換あるいは専用線を利用するため、それらに接続できる環境でのみ有効である。

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

4.8 コンソールのプロンプト表示の設定

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

[設定値] ○ *prompt*..... コンソールのプロンプトの先頭文字列 (16 文字以内)

[説明] コンソールのプロンプト表示を設定する。空文字列も設定できる。

[初期値] 空文字列

4.9 ログインタイマの設定

- [書式] **login timer time**
no login timer [time]
- [設定値] ○ *time*
- キー入力がない場合に自動的にログアウトするまでの秒数 (30..21474836)
 - clear ログインタイマを設定しない
- [説明] キー入力がない場合に自動的にログアウトするまでの時間を設定する。
- [ノート] TELNET 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。
- [初期値] 300

4.10 タイムゾーンの設定

- [書式] **timezone timezone**
no timezone [timezone]
- [設定値] ○ *timezone* その地域と世界標準時との差
- jst 日本標準時 (+09:00)
 - utc 世界標準時 (+00:00)
 - 時刻 : 分 (-12:00 .. +11:59)
- [説明] タイムゾーンを設定する。
- [初期値] jst

4.11 現在の日付けの設定

- [書式] **date date**
- [設定値] ○ *date* yyyy-mm-dd または yyyy/mm/dd
- [説明] 現在の日付けを設定する。

4.12 現在の時刻の設定

- [書式] **time time**
- [設定値] ○ *time* hh:mm:ss
- [説明] 現在の時刻を設定する。

4.13 リモートホストによる時計の設定

- [書式] **rdate bost [syslog]**
- [設定値] ○ *bost*
- リモートホストの IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))
 - ホストの名称
- *syslog* 出力結果を SYSLOG へ出力することを示すキーワード
- [説明] ルータの時計を、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] 本製品および多くの 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。

4.14 NTP による時計の設定

- [書式] **ntpdate** *ntp_server* [syslog]
- [設定値] ◦ *ntp_server*
- NTP サーバーの IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))
 - NTP サーバーの名称
- *syslog* 出力結果を SYSLOG へ出力することを示すキーワード
- [説明] NTP を利用してルータの時計を設定する。このコマンドが実行されるとホストの UDP の 123 番ポートに接続する。
- [ノート] インターネットに接続している場合には、**rdate** コマンドを使用した場合よりも精密な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。
本製品は NTP サーバーになれない。
syslog キーワードを指定した場合には、コマンドの出力結果を INFO レベルの SYSLOG へ出力する。

4.15 コンソールの言語とコードの設定

- [書式] **console character** *code*
no console character [*code*]
- [設定値] ◦ *code*
- *ascii* 英語で表示する、文字コードは ASCII
 - *sjis* 日本語で表示する、文字コードはシフト JIS
 - *euc* 日本語で表示する、文字コードは EUC
- [説明] コンソールに表示する言語とコードを設定する。
本コマンドは一般ユーザでも実行できる。
- [ノート] 本コマンドの設定は、**save** コマンドで保存するまで **show config** コマンドによる設定の表示に反映されない。
- [初期値] *sjis*

4.16 コンソールの表示文字数の設定

- [書式] **console columns** *col*
no console columns [*col*]
- [設定値] ◦ *col* コンソールの表示文字数 (80..200)
- [説明] コンソールの 1 行あたりの表示文字数を設定する。
本コマンドは一般ユーザでも実行できる。
- [ノート] 本コマンドの設定は、**save** コマンドで保存するまで **show config** コマンドによる設定の表示に反映されない。
- [初期値] 80

4.17 コンソールの表示行数の設定

- [書式] **console lines** *lines*
no console lines [*lines*]
- [設定値] ◦ *lines*
- 整数 (10..100)
 - *infinity* スクロールを止めない
- [説明] コンソールの表示行数を設定する。
このコマンドは一般ユーザでも実行できる。
- [ノート] 本コマンドの設定は、**save** コマンドで保存するまで **show config** コマンドによる設定の表示に反映されない。

[初期値] 24

4.18 コンソールにシステムメッセージを表示するか否かの設定

[書式] **console info** *info*
no console info *info*[設定値] ◦ *info*
• on..... 表示する
• off..... 表示しない

[説明] コンソールにシステムのメッセージを表示するか否かを設定する。

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

[初期値] off

4.19 SYSLOG を受けるホストの IP アドレスの設定

[書式] **syslog host** *host*
no syslog host [*host*][設定値] ◦ *host*..... SYSLOG を受けるホストの IP アドレス (IPv6 アドレス可)[説明] SYSLOG を受けるホストの IP アドレスを設定する。
syslog debug コマンドが on に設定されている場合、大量のデバッグメッセージが送信されるので、このコマンドで設定するホストには十分なディスク領域を確保しておくことが望ましい。

[初期値] SYSLOG ホストは設定されない

4.20 SYSLOG ファシリティの設定

[書式] **syslog facility** *facility*
no syslog facility [*facility*][設定値] ◦ *facility*
• 0..23
• user..... 1
• local0..local7..... 16..23

[説明] SYSLOG のファシリティを設定する。

[初期値] user

4.21 NOTICE タイプの SYSLOG を出力するか否かの設定

[書式] **syslog notice** *notice*
no syslog notice [*notice*][設定値] ◦ *notice*
• on..... 出力する
• off..... 出力しない

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

[初期値] off

4.22 INFO タイプの SYSLOG を出力するか否かの設定

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

- [設定値] ◦ *info*
- on..... 出力する
 - off..... 出力しない
- [説明] ISDN の呼制御情報等を SYSLOG で出力するか否か設定する。
- [初期値] on

4.23 DEBUG タイプの SYSLOG を出力するか否かの設定

- [書式] **syslog debug** *debug*
no syslog debug [*debug*]
- [設定値] ◦ *debug*
- on..... 出力する
 - off..... 出力しない
- [説明] ISDN および、PPP のデバッグ情報等を SYSLOG で出力するか否かを設定する。
- [ノート] *debug* パラメータを on にすると、大量のデバッグメッセージを送信するため、**syslog host** コマンドで設定するホスト側には十分なディスク領域を確保しておき、必要なデータが得られたらすぐに off にする。
- [初期値] off

4.24 SYSLOG を送信する時の始点 IP アドレスの設定

- [書式] **syslog local address** *address*
no syslog local address [*address*]
- [設定値] ◦ *address*..... 始点 IP アドレス
- [説明] SYSLOG パケットを送信する時の始点 IP アドレスを設定する。始点 IP アドレスが設定されていない時は、通常の UDP パケット送信ルールに従い、出力インタフェースの IP アドレスを利用する。
- [初期値] 始点 IP アドレスは設定されていない。

4.25 SYSLOG パケットの始点ポート番号の設定

- [書式] **syslog srcport** *port*
no syslog srcport [*port*]
- [設定値] ◦ *port*..... ポート番号 (1..65535)
- [説明] 本製品が送信する SYSLOG パケットの始点ポート番号を設定する。
- [初期値] 514

4.26 TELNET サーバー機能の ON/OFF の設定

- [書式] **telnetd service** *service*
no telnetd service [*service*]
- [設定値] ◦ *service*
- on..... TELNET サーバー機能を有効にする
 - off..... TELNET サーバー機能を停止させる
- [説明] TELNET サーバー機能の利用を選択する。
- [ノート] TELNET サーバーが停止している場合、TELNET サーバーはアクセス要求に一切応答しない。
- [初期値] on

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

- [書式] **telnetd host ip_range [ip_range...]**
no telnetd host [ip_range...]
- [設定値] ◦ *ip_range*
- LAN インタフェース名
 - TELNET サーバーへアクセスを許可するホストの IP アドレス範囲のリストまたはニーモニック
 - 1 個の IP アドレスまたは間にマイナス (-) をはさんだ IP アドレス (範囲指定)、及びこれらを任意に並べたもの
 - any すべてのホストからのアクセスを許可する
 - none すべてのホストからのアクセスを禁止する
- [説明] TELNET でこのルータにアクセスできるホストを指定する。
any の場合にはすべてのホストがアクセスできる。
none を指定すると、すべてのホストからのアクセスを拒否する。
IP アドレスを指定した場合には、指定された IP アドレスのホストだけがアクセスできる。IP アドレスはハイフン「-」により範囲指定が可能である。
LAN インタフェース名を指定した場合には、指定した LAN インタフェースに直結されたホストだけがアクセスできる。
IP アドレス範囲と LAN インタフェース名は複数指定できる。その場合、いずれかの設定に合致すればアクセスは受け入れられる。
- [ノート] LAN インタフェース名の指定は IPv4 によるアクセスだけに適用される。LAN インタフェース名だけが設定されている場合、IPv6 でアクセスすることはできない。
ニーモニックをリストにすることはできない。
設定後の新しい TELNET 接続から適用される。
- [初期値] any

4.28 TELNET サーバー機能の listen ポートの設定

- [書式] **telnetd listen port**
no telnetd listen [port]
- [設定値] ◦ *port* TELNET サーバー機能の待ち受け (listen) ポート番号 (1..65535)
- [説明] TELNET サーバー機能の listen ポートを選択する。
- [ノート] telnetd は、TCP の 23 番ポートで待ち受けしているが、本コマンドにより待ち受けポートを変更することができる。
ただし、待ち受けポートを変更した場合には、ポート番号が変更されても、TELNET オプションのネゴシエーションが行える TELNET クライアントを用いる必要がある。
- [初期値] 23

4.29 TELNET に同時に接続できるユーザ数を設定する

- [書式] **telnetd session num**
no telnetd session
- [設定値] ◦ *num* 同時接続数 (1..8)
- [説明] TELNET に同時に接続できるユーザ数を設定する。
- [ノート] 設定を変更したときに変更した値よりも多くのユーザが接続している場合は、接続しているユーザはそれを維持することができるが、接続しているユーザ数が設定値より少なくなるまで新たな接続は許可しない。
- [初期値] 8

4.30 TFTP によりアクセスできるホストの IP アドレスの設定

[書式]	tftp host <i>host</i> no tftp host [<i>host</i>]
[設定値]	○ <i>host</i> <ul style="list-style-type: none"> • IP アドレス TFTP によりアクセスできるホストの IP アドレス (IPv6 アドレス可) • any すべてのホストから TFTP によりアクセスできる • none すべてのホストから TFTP によりアクセスできない
[説明]	TFTP によりアクセスできるホストの IP アドレスを設定する。
[ノート]	セキュリティの観点から、プログラムのリビジョンアップや設定ファイルの読み書きが終了したらすぐに none にする。
[初期値]	none

4.31 ファストパス機能の設定

[書式]	ip routing process <i>process</i> no ip routing process
[設定値]	○ <i>process</i> <ul style="list-style-type: none"> • fast ファストパス機能を利用する • normal ファストパス機能を利用せず、すべてのパケットをノーマルパスで処理する
[説明]	パケット転送をファストパス機能で処理するか、ノーマルパス機能で処理するかを設定する。
[ノート]	fast を設定した場合でも、以下の場合にはノーマルパスで処理される。 <ul style="list-style-type: none"> • IPv4 でも IPv6 でもないパケット • 終点 IP アドレスがブロードキャストまたはマルチキャストになっているパケット • 終点 IP アドレスがルータ自身の IP アドレスになっているパケット • フラグメントする必要があるパケット • フラグメントされているパケット • IP オプションが付いているパケット • ICMP エラーを送る必要があるパケット • SYN/FIN/RST ビットがセットされている TCP パケット • DHCP 関連のパケット • FTP の制御セッションのパケット • パケットを転送する先のホストやゲートウェイの ARP がまだ解決できていない時 • フローテーブルが一杯になってしまい、新たにフローテーブルに追加できないフローのパケット
[初期値]	fast

4.32 LAN インタフェースの動作設定

[書式]	lan shutdown <i>interface</i> [<i>port...</i>] no lan shutdown <i>interface</i> [<i>port...</i>]
[設定値]	○ <i>interface</i> LAN インタフェース名 ○ <i>port</i> ポート番号
[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。

4.33 LAN インタフェースの動作タイプの設定

[書式]	lan type <i>interface</i> <i>speed_type</i> [<i>port ...</i>] [<i>speed_type ...</i>] [auto-crossover= <i>switch</i>] lan type <i>interface</i> auto-crossover= <i>switch</i> no lan type <i>interface</i>
------	--

- [設定値]
- *interface* LAN インタフェース名
 - *speed_type* LAN 動作タイプ
 - *auto* 自動判別
 - *10-hdx* 10BASE-T 半二重
 - *10-fdx* 10BASE-T 全二重
 - *100-hdx* 100BASE-TX 半二重
 - *100-fdx* 100BASE-TX 全二重
 - 省略時は *auto*
 - *port*
 - スイッチングハブのポート番号 (1..4)
 - 省略時は全ポート
 - *switch*
 - *on* クロスストレート自動判別機能を使用する
 - *off* クロスストレート自動判別機能を使用しない

[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を設定する。正しく通信できる組み合わせは以下の表のとおり。

相手側設定	本製品の設定				
	自動判別	100BASE-TX 全二重	100BASE-TX 半二重	10BASE-T 全二重	10BASE-T 半二重
自動判別	○	×	○	×	○
100BASE-TX 全二重	×	○	×	×	×
100BASE-TX 半二重	○	×	○	×	×
10BASE-T 全二重	×	×	×	○	×
10BASE-T 半二重	○	×	×	×	○

- [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、その終了後に設定が有効となる。
- [初期値] *speed_type* = *auto*
auto-crossover = *on*
- [設定例] ○ 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

4.34 インタフェースの説明

- [書式] **description interface description**
description pp description
description tunnel description
no description interface [description]
no description pp description
no description tunnel description
- [設定値] ○ *interface* LAN インタフェース名
○ *description* 説明の文字列
- [説明] インタフェースの説明を設定しておく。'pp'、'tunnel' を指示した時にはそれぞれ、**pp select** あるいは **tunnel select** で選択したインタフェースの説明となる。
設定内容は、インタフェースに対する **show status** コマンドで表示される。
- [初期値] なし

4.35 TEL ポートでの接続・切断時にアラーム音を鳴らすか否かの設定

- [書式] **alarm connection analog switch**
no alarm connection analog

- [設定値] ◦ *switch*
- on 鳴らす
 - off 鳴らさない
- [説明] TEL ポートでの内線通話を除く接続・切断時にアラーム音を鳴らすか否かを選択する。
- [初期値] off

4.36 データ通信での接続・切断時にアラーム音を鳴らすか否かの設定

- [書式] **alarm connection data** *switch*
no alarm connection data
- [設定値] ◦ *switch*
- on 鳴らす
 - off 鳴らさない
- [説明] データ通信での接続・切断時にアラーム音を鳴らすか否かを選択する。
- [初期値] on

4.37 有効になっているアラーム音を鳴らすか全く鳴らさないかの設定

- [書式] **alarm entire** *switch*
no alarm entire
- [設定値] ◦ *switch*
- on 鳴らす
 - off 鳴らさない
- [説明] 有効になっているアラーム音を鳴らすか全く鳴らさないかを選択する。
- [初期値] on

4.38 攻撃を検知した時にアラーム音を鳴らすか否かの設定

- [書式] **alarm intrusion** *switch*
no alarm intrusion
- [設定値] ◦ *switch*
- on 鳴らす
 - off 鳴らさない
- [説明] 攻撃を検知した時にアラーム音を鳴らすか否かを選択する。
- [初期値] on

4.39 MP 通信でリンク数が増えた時にアラーム音を鳴らすか否かの設定

- [書式] **alarm mp** *switch*
no alarm mp
- [設定値] ◦ *switch*
- on 鳴らす
 - off 鳴らさない
- [説明] MP 通信でリンク数が増えた時にアラーム音を鳴らすか否かを選択する。
- [初期値] on

4.40 USB ホスト機能に関連するアラーム音を鳴らすか否かの設定

- [書式] **alarm usbhost** *switch*
no alarm usbhost

- [設定値] ◦ *switch*
- on 鳴らす
 - off 鳴らさない
- [説明] USB ホスト機能に関連するアラーム音を鳴らすか否かを選択する。
- [初期値] on

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] ◦ *permit*
- on 許可する
 - off 許可しない
- [説明] HTTP リビジョンアップを許可するか否かを設定する。
- [ノート] このコマンドの設定は、コマンドによる直接の HTTP リビジョンアップ、かんたん設定によるリビジョンアップ、電話機からのリビジョンアップに影響する。
- [初期値] on

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

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] ◦ *proxy-server* HTTP リビジョンアップ時に使用する Proxy サーバー
◦ *port* Proxy サーバーのポート番号
- [説明] Proxy サーバーのホスト名または、IP アドレスとポート番号を指定する。
- [初期値] Proxy サーバーは設定されていない

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] ◦ *time* タイムアウト時間 (秒)
- [説明] HTTP リビジョンアップ処理のタイムアウト時間を設定する。
- [初期値] 30

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 <i>permit</i> no http revision-down permit [<i>permit</i>]
[設定値]	<ul style="list-style-type: none"> ◦ <i>permit</i> • on.....現在のリビジョンより古いリビジョンへのリビジョンダウンを許可する • off.....現在のリビジョンより古いリビジョンへのリビジョンダウンを許可しない
[説明]	HTTP リビジョンアップ機能にて、現在のリビジョンよりも古いリビジョンへのファームウェアのリビジョンダウンを許可するか否かを設定する。
[初期値]	off

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 <i>permit</i> no operation http revision-up permit [<i>permit</i>]
[設定値]	<ul style="list-style-type: none"> ◦ <i>permit</i> • on.....DOWNLOAD ボタンによるリビジョンアップ操作を許可する • off.....DOWNLOAD ボタンによるリビジョンアップ操作を許可しない
[説明]	DOWNLOAD ボタンによりファームウェアのリビジョンアップ機能を使用するか否かを設定する。
[ノート]	リビジョンアップ機能は HTTP リビジョンアップ機能に準ずる。 STATUS ランプがエラーを表示している状態で本コマンドを off に設定すると、エラー表示が解除される。
[初期値]	off

4.47 電話機からのリビジョンアップ操作を許可するか否かの設定

[書式]	analog http revision-up permit <i>permit</i> no analog http revision-up permit
[設定値]	<ul style="list-style-type: none"> ◦ <i>permit</i> ◦ on.....許可する ◦ off.....許可しない
[説明]	電話機からのリビジョンアップ操作を許可するか否かを設定する。
[初期値]	on

4.48 INIT スイッチによるパスワード再入力機能の設定

[書式]	password reenter <i>reenter</i> no password reenter
[設定値]	<ul style="list-style-type: none"> ◦ <i>reenter</i> • enable.....パスワード再入力機能を許可する • disable.....パスワード再入力機能を許可しない
[説明]	起動完了後に INIT スイッチを 10 秒以上押し続けると、その後 10 分間はパスワードを再入力可能にする機能を許可するか否かを設定する。再入力可能な 10 分間は、TELENT やシリアル経由でもパスワードなしでログインが可能。 なお、パスワードを再入力可能にする機能は、電源投入後 1 回のみ実行可能。
[初期値]	enable

4.49 エコーキャンセラ制御方法の設定

[書式] **audio echo-canceller** port=*port* [route=*route*] mode [*length* [nlp=*nlp*] [cng=*cng*]]
no audio echo-canceller port=*port* [route=*route* mode [*length* [nlp=*nlp*] [cng=*cng*]]]

[設定値]

- *port*
 - tel1 TEL1 ポート
 - tel2 TEL2 ポート
- *route*
 - BRI インタフェース名
 - pstn LINE ポート
- *mode*
 - auto 自動設定
 - off エコーキャンセラ OFF
- *length* エコーキャンセラテール長
 - 8 8 ミリ秒
 - 16 16 ミリ秒
- *nlp*
 - on NLP 機能有効
 - off NLP 機能無効
 - 省略時は on
- *cng*
 - on CNG 機能有効
 - off CNG 機能無効
 - 省略時は on

[説明] ポート毎のエコーキャンセラ制御方法を設定する。

mode パラメータを *auto* に指定した場合、通常はエコーキャンセラ機能が ON で動作して、ファックスの開始音を検出したときには、その呼が終了するまではエコーキャンセラ機能が OFF で動作する。

port パラメータに TEL ポートを指定して、*route* パラメータを *bri1* または *pstn*、*mode* パラメータを *off* と指定すると、TEL ポートから ISDN ポートまたは LINE ポートを經由する通話におけるエコーキャンセラ機能を OFF にできる。

NLP (NonLinear Processing) 機能を *on* に指定すると、対向からの音声がある場合には、TEL ポートから対向に送られる音声を抑制する。

CNG (Comfort Noise Generation) 機能を *on* に指定すると、対向からの音声があるときに TEL ポートから対向に送られる音声を抑制した場合に、対向に送られる音声に環境雑音と同程度のノイズを加えることによって、音声抑制切替による不自然さを軽減することができる。

[ノート] *nlp* のパラメータを省略した場合、*nlp=on* で設定される。
cng のパラメータを省略した場合、*cng=on* で設定される。

[初期値]

```
port=tel1 auto 8 nlp=on cng=on
port=tel1 route=bri1 auto
port=tel1 route=pstn off
port=tel2 auto 8 nlp=on cng=on
port=tel2 route=bri1 auto
port=tel2 route=pstn off
```

[設定例]

- TEL1 ポートのエコーキャンセラを OFF とする
audio echo-canceller port=tel1 off
- TEL1 ポートの *bri1* 経由の通話についてエコーキャンセラをオフとする
audio echo-canceller port=tel1 route=bri1 off
- tel1 ポートのエコーキャンセラの設定値をデフォルト値に戻す
no audio echo-canceller port=tel1

4.50 エコーキャンセラの NLP 閾値の設定

- [書式] **audio echo-canceller nlp threshold** port=*port threshold*
no audio echo-canceller nlp threshold port=*port*
- [設定値] ◦ *threshold*
- -15dB -15dB
 - -18dB -18dB
 - -21dB -21dB
 - -24dB -24dB
 - -27dB -27dB
 - -30dB -30dB
 - -33dB -33dB
 - -36dB -36dB
 - -39dB -39dB
 - -42dB -42dB
- *port*
- tel1 TEL1 ポート
 - tel2 TEL2 ポート
- [説明] エコーキャンセラの NLP(NonLinear Processing) 閾値を設定する。
- [入力例] TEL1 のエコーキャンセラの NLP 閾値を -27dB に設定する。
 audio echo-canceller nlp threshold port=tel1 -27dB
- [ノート] NLP 閾値はポート毎の設定となる。
- [初期値] -30dB

4.51 エコーキャンセラを無効にする音の設定

- [書式] **audio echo-canceller disabler mode**
- [設定値] ◦ *mode*
- 2100hz 2100Hz 検出でエコーキャンセラ無効
 - with-phase-reversal 位相反転ありの 2100Hz 検出でエコーキャンセラ無効
- [説明] エコーキャンセラを無効にする音の種類を設定する。
- [ノート] 音の種類は機器全体で単一の設定となる。
- [初期値] 2100hz

4.52 Magic Packet を LAN に中継するか否かの設定

- [書式] **ip interface wol relay relay**
no ip interface wol relay
- [設定値] ◦ *interface* LAN インタフェース名
- *relay*
- broadcast Magic Packet をブロードキャストパケットとして中継する
 - unicast Magic Packet をユニキャストパケットとして中継する
 - off Magic Packet かどうか検査しない
- [説明] 遠隔地から送信された、ディレクティッドブロードキャスト宛の IPv4 パケットとして構成された Magic Packet を指定した LAN インタフェースに中継する。IPv4 パケットの終点 IP アドレスは指定した LAN インタフェースのディレクティッドブロードキャスト宛でなくてはならない。
- broadcast または unicast を指定した場合には、受信したパケットの内容をチェックし、Magic Packet データシーケンスが存在する場合にのみパケットを中継する。

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

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

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

[ノート] いずれの場合も、Magic Packet として中継されなかった場合の packets は、`ip filter directed-broadcast` コマンドの設定に基づき処理される。

[初期値] `off`

4.53 TCP のログを記録するか否かの設定

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

[設定値]

- `switch`
 - `on`..... TCP コネクションの syslog を出力する
 - `off`..... TCP コネクションの syslog を出力しない
- `src_addr` 始点パケットの IP アドレス
 - xxx.xxx.xxx.xxx (xxx は十進数)
 - * (ネットマスクの対応するビットが 8 ビットとも 0 と同じ。すべての IP アドレスに対応)
 - 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
- `dst_addr`
 - 終点 IP アドレス (`src_addr` と同じ形式)
 - 省略時は 1 個の * と同じ
- `mask` IP アドレスのビットマスク
 - 省略時は 0xffffffff と同じ
 - `src_addr` 及び `dst_addr` がネットワークアドレスの場合にのみ指定可能
- `tcpflag` フィルタリングする TCP パケットの種類
 - プロトコルを表す 10 進数 (6 のみ)
 - プロトコルを表すニーモニック

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

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

○ *src_port_list*..... TCP のソースポート番号

- ポート番号を表す 10 進数
- ポート番号を表す二ーモニック

二ーモニック	ポート番号	二ーモニック	ポート番号
ftp	20,21	ident	113
ftpdata	20	ntp	123
telnet	23	nntp	119
smtp	25	snmp	161
domain	53	syslog	514
gopher	70	printer	515
finger	73	talk	517
www	80	route	520
pop3	110	uucp	540
sunrpc	111		

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

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

- [説明] TCP のログを記録する。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。
- [ノート] 本設定により処理負荷が高くなるため、通常の運用においては本設定をせずに運用することを推奨する。
- [初期値] off
- [設定例] PPTP のポートに SYN が来ているか
 # tcp log on ** tcpsyn * 1723
 FIN,RST,SYN の立った TCP パケット
 # tcp log on ** tcpflag!=0x0000/0x0007
 すべての TCP パケット (tcp log on ***** と同じ)
 # tcp log on

4.54 SSH サーバー機能の ON/OFF の設定

- [書式] **sshd service service**
no sshd service [service]
- [設定値] ○ *service*
- on..... SSH サーバー機能を有効にする
 - off..... SSH サーバー機能を停止させる
- [説明] SSH サーバー機能の利用を選択する。
- [ノート] SSH サーバー機能が停止している場合、SSH サーバーはアクセス要求に一切応答しない。
- [初期値] off

4.55 SSH サーバー機能の listen ポートの設定

- [書式] **sshd listen port**
no sshd listen [port]
- [設定値] ○ *port*..... SSH サーバー機能の待ち受け (listen) ポート番号 (1..65535)
- [説明] SSH サーバーの listen ポートを選択する。
- [ノート] SSH サーバーは、TCP の 22 番ポートで待ち受けしているが、本コマンドにより待ち受けポートを変更することができる。
- [初期値] 22

4.56 SSH サーバーへアクセスできるホストの IP アドレスの設定

- [書式] **sshd host** *ip_range* [*ip_range* ...]
no sshd host [*ip_range* ...]
- [設定値] ○ *ip_range*
- SSH サーバーへアクセスを許可するホストの IP アドレス範囲のリストまたはニーモニック
 - 1 個の IP アドレスまたは間にハイフン (-) をはさんだ IP アドレス (範囲指定)、およびこれらを任意に並べたもの
 - any すべてのホストからのアクセスを許可する
 - none すべてのホストからのアクセスを禁止する
- [説明] SSH サーバーへアクセスできるホストの IP アドレスを設定する。
- [ノート] ニーモニックをリストにすることはできない。
- 設定後の新しい SSH 接続から適用される。
- [初期値] any

4.57 SSH に同時に接続できるユーザ数を設定する

- [書式] **sshd session** *num*
no sshd session [*num*]
- [設定値] ○ *num* 同時接続数 (1..8)
- [説明] SSH に同時に接続できるユーザ数を設定する。
- [ノート] 設定を変更したときに変更した値よりも多くのユーザが接続している場合は、接続しているユーザはそれを維持することができるが、接続しているユーザ数が設定値より少なくなるまで新たな接続は許可しない。
- [初期値] 8

4.58 SSH サーバー ホスト鍵の設定

- [書式] **sshd host key generate** [*seed*]
no sshd host key generate [*seed*]
- [設定値] ○ *seed* ホスト鍵の元になる数 (0...4294967295)
- [説明] SSH サーバーのホスト鍵を設定する。
- seed* を省略した場合は、ランダムな値が *seed* として自動的に設定される。
- [ノート] SSH サーバー機能を利用する場合は、事前に本コマンドを実行してホスト鍵を生成する必要がある。
- seed* によって生成されるホスト鍵が一意に決まるため、*seed* を指定する場合は機器毎に異なる値を設定すべきである。
- 既にホスト鍵が設定されている状態で本コマンドを実行した場合、ユーザに対してホスト鍵を更新するか否かを確認する。
- ホスト鍵の生成には、機種によって異なるが 30 秒から 1 分程度の時間がかかる。
- TFTP で設定を取得した場合は、**sshd host key generate** *seed* KEY1 KEY2 という形式で保存される。KEY1 と KEY2 は、それぞれ RSA 秘密鍵と DSA 秘密鍵を機器固有の方式で暗号化した文字列である。そのため、保存した設定を他の機器に適用する場合、*seed* からホスト鍵を生成し、機器固有の方式で暗号化して保存するため、入力した KEY1、KEY2 とは同一の文字列にはならない。

4.59 SSH クライアントの生存確認

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

[設定値]

- *switch*
 - *on*..... クライアントの生存確認を行なう
 - *off*..... クライアントの生存確認を行なわない
- *interval*..... 送信間隔の秒数 (1..2147483647)
- *count*..... 試行回数 (1..2147483647)

[説明] クライアントの生存確認を行なうか否かを設定する。

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

[初期値]

- *switch* off
- *interval* 100
- *count* 3

4.60 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]

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

[説明] パケットバッファの管理パラメータを変更する。

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

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

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。

[初期値]

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

[設定例]

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

4.61 他のユーザの接続を強制切断する

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

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

[説明] 他ユーザの接続を切断する。

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

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

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

[ノート] 自分自身のセッションを切断することはできない。

[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
```


5. ISDN 関連の設定

5.1 共通の設定

5.1.1 BRI インタフェースの使用制限の設定

- [書式] **isdn use interface use**
no isdn use interface
- [設定値] ◦ *interface*
 • BRI インタフェース名
- *use*
 • off 発着信禁止
 • on 発着信可
 • call-only 発信専用 (着信規制)
 • arrive-only 着信専用 (発信規制)
- [説明] BRI インタフェースの発着信を制限する。
- [初期値] on

5.1.2 BRI 回線の種類の指定

- [書式] **line type interface line [channels]**
no line type interface line [channels]
- [設定値] ◦ *interface* BRI インタフェース名
- *line*
 • isdn, isdn-ntt ISDN 回線交換
 • 164 デジタル専用線、64kbit/s
 • 1128 デジタル専用線、128kbit/s
- *channels* *line* パラメータが isdn、isdn-ntt の場合のみ指定可
 • 1b B チャンネルは 1 チャンネルだけ使用
 • 2b B チャンネルは 2 チャンネルとも使用する
- [説明] BRI 回線の種類を指定する。設定の変更は、再起動か、あるいは該当インタフェースに対する **interface reset** コマンドの発行により反映される。
- [ノート] 別の通信機器の発着信のために 1B チャンネルを確保したい場合は *channels* パラメータを 1b に設定する。
- [初期値] line = isdn
 channels = 2b

5.1.3 自分の ISDN 番号の設定

- [書式] **isdn local address interface isdn_num[/sub_address]**
isdn local address interface /sub_address
no isdn local address interface
- [設定値] ◦ *interface*
 • BRI インタフェース名
- *isdn_num* ISDN 番号
- *sub_address* ISDN サブアドレス (0x21 から 0x7e の ASCII 文字列)
- [説明] 自分の ISDN 番号とサブアドレスを設定する。ISDN 番号、サブアドレスとも完全に設定して運用することが推奨される。また、ISDN 番号は市外局番も含めて設定する。
- [ノート] 他機種との相互接続のために、ISDN サブアドレスに英文字や記号を使わず数字だけにしなければいけないことがある。

5.1.4 PP で使用するインタフェースの設定

- [書式] **pp bind interface** [interface]
no pp bind [interface]
- [設定値] ◦ *interface* BRI インタフェース名の並び
- [説明] 選択されている相手先に対して実際に使用するインタフェースを設定する。
- [初期値] どのインタフェースともバインドされていない

5.1.5 課金額による発信制限の設定

- [書式] **account threshold** [interface] *yen*
account threshold pp *yen*
no account threshold interface [yen]
no account threshold [yen]
no account threshold pp [yen]
- [設定値] ◦ *interface* BRI インタフェース名
◦ *yen*
 - 課金額 円 (10..21474836)
 - off 発信制限機能を使わない
- [説明] 網から通知される課金の合計 (これは **show account** コマンドで表示される) の累計が指定した金額に達したらそれ以上の発信を行なわないようにする。
account threshold コマンドではルータ全体の合計金額を設定し、*interface* パラメータを指定した場合には、それぞれのインタフェースでの合計金額、**account threshold pp** コマンドでは選択している相手先に対する発信での合計金額で制御を行なう。
課金が網から通知されるのは通信切断時なので、長時間の接続の途中切断することはできず、この場合は制限はできない。この場合に対処するには、**isdn forced disconnect time** コマンドで通信中でも時間を監視して強制的に回線を切るような設定しておく方法がある。また、課金合計は **clear account** コマンドで 0 にリセットでき、**schedule at** コマンドで定期的に **clear account** を実行するようにしておく、毎月一定額以内に課金を抑えるといったことが自動で可能になる。
- [ノート] 課金額は通信の切断時に ISDN 回線を通じて通知される料金情報に基づくため、割引サービスなどを利用している場合には、最終的に請求される料金とは異なる場合がある。また、弊社以外の通信事業者を利用して通信した場合には料金情報は通知されない。
- [初期値] off

5.1.6 PIAFS の発信方式の設定

- [書式] **isdn piafs call speed** [64kmode]
no isdn piafs call [speed [64kmode]]
- [設定値] ◦ *speed*
 - off 発信を同期 PPP とする
 - 32k 発信を PIAFS 32k とする
 - 64k 発信を PIAFS 64k とする
◦ *64kmode*
 - *guarantee* PIAFS 64k の発信ではギャランティー方式を使用する
 - *best-effort* PIAFS 64k の発信ではベストエフォート方式を使用する
- [説明] PIAFS モードの発信を可能にするか否かを設定する。また、PIAFS モードの速度を選択する。
speed が off に設定されている場合には発信は同期 PPP になり、32k に設定されている場合には発信は PIAFS 32k に、64k に設定されている場合には発信は PIAFS 64k になる。
speed が 64k に設定されている場合には、*64kmode* の設定が有効になる。
64kmode が設定されていない、または *guarantee* に設定されている場合には、発信はギャランティー方式の PIAFS 64k になる。
64kmode が *best-effort* に設定されている場合には、発信はベストエフォート方式になる。
- [ノート] PIAFS 64k では特別なサブアドレスが用いられるため、ユーザがコマンドで設定した発サブアドレスは無視される。

[初期値] off

5.1.7 PIAFS の着信を許可するか否かの設定

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

[設定値] ○ *arrive*

- on..... 許可する
- off..... 拒否する

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

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

[初期値] on

5.1.8 PIAFS 接続時の起動側の指定

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

[設定値] ○ *switch*

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

[説明] PIAFS を制御する側を選択する。

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

<i>switch</i> パラメータの設定	call	both	arrive
発信時	起動側	起動側	被起動側
着信時	被起動側	起動側	起動側

[初期値] call

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

5.1.9 常時接続の設定

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

[設定値] ○ *switch*

- on..... 常時接続する
- off..... 常時接続しない

○ *time*..... 再接続を要求するまでの秒数 (60..21474836)

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

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

[初期値] off

5.2 相手側の設定

5.2.1 相手 ISDN 番号の設定

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

[設定値] ○ *call_arrive*

- *call* 発着信用
- *arrive* 着信専用

○ *isdn_num* ISDN 番号

○ *sub_address*..... ISDN サブアドレス (0x21 から 0x7e の ASCII 文字)

○ *isdn_num_list* ISDN 番号だけまたは ISDN 番号とサブアドレスの組を空白で区切った並び

[説明] 選択されている相手の ISDN 番号とサブアドレスを設定する。ISDN 番号には市外局番も含めて設定する。選択されている相手が *anonymous* の場合は無意味である。

複数の ISDN 番号が設定されている場合、まず先頭の ISDN 番号での接続に失敗すると次に指定された ISDN 番号が使われる。同様に、それに失敗すると次の ISDN 番号を使うという動作を続ける。

MP のように相手先に対して複数チャンネルで接続しようとする際に発信する順番は、**isdn remote call order** コマンドで設定する。

5.2.2 自動接続の設定

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

[設定値] ○ *auto*

- *on*..... 自動接続する
- *off* 自動接続しない

[説明] 選択されている相手について自動接続するか否かを設定する。

[初期値] on

5.2.3 自動切断の設定

[書式] **isdn auto disconnect** *auto*
no isdn auto disconnect [*auto*]

[設定値] ○ *auto*

- *on*..... 自動切断する
- *off* 自動切断しない

[説明] 選択されている相手について自動切断するか否かを設定する。

各種切断タイマの設定を変更せずに、自動切断を無効にしたい場合に使用する。

[ノート] **schedule at** コマンドと併用して、テレホーダイ時間中に自動切断しないようにしたい場合等に有効。
anonymous に対して使用する事はできない。

[初期値] on

5.2.4 着信許可の設定

[書式] **isdn arrive permit** *arrive*
no isdn arrive permit [*arrive*]

[設定値] ○ *arrive*

- *on*..... 許可する
- *off* 許可しない

[説明] 選択されている相手からの着信を許可するか否かを設定する。

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

[初期値] on

5.2.5 発信許可の設定

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

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

[説明] 選択されている相手への発信を許可するか否かを設定する。

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

[初期値] on

5.2.6 相手への発信順序の設定

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

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

[説明] **isdn remote address call** コマンドで複数の ISDN 番号が設定されている場合に意味を持つ。MP を使用する場合などのように、相手先に対して同時に複数のチャンネルで接続しようとする際に、どのような順番で ISDN 番号を選択するかを設定する。

round を指定した場合は、**isdn remote address call** コマンドで最初に設定した ISDN 番号で発信した次の発信時に、このコマンドで次に設定された ISDN 番号を使う。このように順次ずれていき、最後に設定された番号で発信した次には、最初に設定された ISDN 番号を使い、これを繰り返す。

serial を指定した場合は、発信時には必ず最初に設定された ISDN 番号を使い、何らかの理由で接続できなかった場合は次に設定された ISDN 番号で発信し直す。

なお round、serial いずれの設定の場合でも、どこも接続されていない状態や相手先とすべてのチャンネルで切断された後では、最初に設定された ISDN 番号から発信に使用される。

[ノート] MP を使用する場合は、round にした方が効率がよい。

[初期値] serial

5.2.7 再発信抑制タイマの設定

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

[設定値] ◦ *time*..... 秒数 (0..15.0)

[説明] 選択されている相手との通信が切断された後、同じ相手に対し再度発信するのを禁止する時間を設定する。秒数は 0.1 秒単位で設定できる。

isdn call prohibit time コマンドによるタイマはエラーで切断された場合だけに適用されるが、このコマンドによるタイマは正常切断でも適用される点が異なる。

[ノート] 切断後すぐに発信ということを繰り返す状況では適当な値を設定すべきである。

isdn forced disconnect time コマンドと併用するとよい。

[初期値] 0

5.2.8 エラー切断後の再発信禁止タイマの設定

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

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

[説明] 選択されている相手に発信しようとして失敗した場合に、同じ相手に対し再度発信するのを禁止する時間を設定する。秒数は 0.1 秒単位で設定できる。

isdn call block time コマンドによるタイマは切断後に常に適用されるが、このコマンドによるタイマはエラー切断にのみ適用される点異なる。

[初期値] 60

5.2.9 相手にコールバック要求を行なうか否かの設定

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

[設定値] ○ *callback_request*

- on 要求する
- off 要求しない

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

[初期値] off

5.2.10 コールバック要求タイプの設定

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

[設定値] ○ *type*

- yamaha ヤマハ方式
- msbcpc MS コールバック

[説明] コールバックを要求する場合のコールバック方式を設定する。

[初期値] yamaha

5.2.11 相手からのコールバック要求に応じるか否かの設定

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

[設定値] ○ *callback_permit*

- on 応じる
- off 応じない

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

[初期値] off

5.2.12 コールバック受け入れタイプの設定

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

[設定値] ○ *type1, type2*

- yamaha ヤマハ方式
- msbcpc MS コールバック

[説明] 受け入れることのできるコールバック方式を設定する。

[初期値] type1 = yamaha
type2 = mscbcp

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

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

[設定値] ○ *specify*
• on..... 許可する
• off..... 拒否する

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

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

[初期値] off

5.2.14 コールバックタイムの設定

[書式] **isdn callback response time** *type time*
no isdn callback response time

[設定値] ○ *type*
• 1b..... 1B でコールバックする
○ *time*..... 秒数 (0..15.0)

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

[初期値] *time* = 0

5.2.15 コールバック待機タイムの設定

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

[設定値] ○ *time*..... 秒数 (1.0..60.0)

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

[初期値] 60

5.2.16 ISDN 回線を切断するタイム方式の指定

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

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

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

- [初期値] 1
- [設定例] # isdn disconnect policy 2
isdn disconnect interval time 240 6 2

5.2.17 切断タイマの設定 (ノーマル)

- [書式] **isdn disconnect time** *time*
no isdn disconnect time [*time*]
- [設定値] ○ *time*
- 秒数 (1.0..21474836.0)
 - off タイマを設定しない
- [説明] 選択されている相手について PP 側のデータ送受信がない場合の切断までの時間を設定する。秒数は 0.1 秒単位で設定できる。
- [ノート] 本コマンドの設定値を X 秒、**isdn disconnect input time** コマンドの設定値を IN 秒、**isdn disconnect output time** コマンドの設定値を OUT 秒とする。
X>IN または X>OUT のように設定した場合、パケットの入出力が観測されないと X 秒で切断される。外部へパケットを送信していない状態でも、外部からパケットを受信し続けていると、本コマンドの設定通りに切断されないことがある。
- [初期値] 60

5.2.18 入力切断タイマの設定 (ノーマル)

- [書式] **isdn disconnect input time** *time*
no isdn disconnect input time [*time*]
- [設定値] ○ *time*
- 秒数 (1.0..21474836.0)
 - off タイマを設定しない
- [説明] 選択されている相手について PP 側からデータ受信がない場合の切断までの時間を設定する。秒数は 0.1 秒単位で設定できる。
- [ノート] 例えば、UDP パケットを定期的に出すようなプログラムが暴走したような場合、本タイマを設定しておくことにより回線を切断することができる。
5.2.17 切断タイマの設定 (ノーマル) のノート参照。
- [初期値] 120

5.2.19 出力切断タイマの設定 (ノーマル)

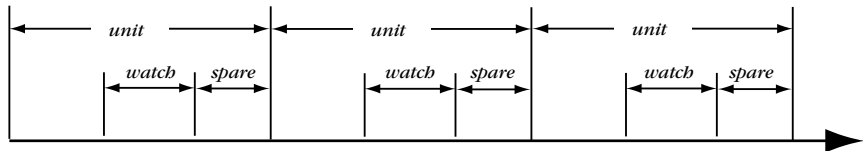
- [書式] **isdn disconnect output time** *time*
no isdn disconnect output time [*time*]
- [設定値] ○ *time*
- 秒数 (1.0..21474836.0)
 - off タイマを設定しない
- [説明] 選択されている相手について PP 側へのデータ送信がない場合の切断までの時間を設定する。秒数は 0.1 秒単位で設定できる。
- [ノート] 例えば、接続先を経由して外部から不正な UDP パケットを受信し続けるような場合、本タイマを設定しておくことにより回線を切断することができる。
5.2.17 切断タイマの設定 (ノーマル) のノート参照。
- [初期値] 120

5.2.20 課金単位時間方式での課金単位時間と監視時間の設定

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

[設定値] ◦ *unit* 課金単位時間
 • 秒数 (1.0..21474836.0)
 • off
 ◦ *watch* 監視時間
 • 秒数 (1.0..21474836.0)
 • off
 ◦ *spare* 切断余裕時間
 • 秒数 (1.0..21474836.0)
 • off

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



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

[ノート] 外部へパケットを送信していない状態でも、外部からパケットを受信し続けていると、本コマンドの設定通りに切断されないことがある。

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

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

5.2.21 切断タイマの設定 (ファスト)

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

[設定値] ◦ *time*
 • 秒数 (1.0..21474836.0)
 • off タイマを設定しない

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

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

[初期値] 20

5.2.22 切断タイマの設定 (強制)

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

- [設定値] ◦ *time*
- 秒数 (1.0..21474836.0)
 - off タイマを設定しない
- [説明] 選択されている相手に接続する最大時間を設定する。秒数は 0.1 秒単位で設定できる。パケットをやりとりしていても、このコマンドで設定した時間が経過すれば強制的に回線を切断する。ダイヤルアップ接続でインターネット側からの無効なパケット (ping アタック等) が原因で回線が自動切断できない場合に有効。 **isdn call block time** コマンドと併用するとよい。
- [初期値] off

5.2.23 同じ相手に対して連続して認証に失敗できる回数の設定

- [書式] **isdn call prohibit auth-error count** *count*
no isdn call prohibit auth-error count
- [設定値] ◦ *count*
- 連続して認証に失敗できる回数 (1..21474836)
 - off 発信制限をかけない
- [説明] 連続して認証に失敗できる回数を設定する。ここで設定した回数だけ連続して認証に失敗したときには、その後は、同じ相手に対して発呼しない。
- なお、以下のコマンドを実行すると、再び発呼が可能となる。
pp auth accept / pp auth request / pp auth myname / pp auth username / no pp auth myname / no pp auth username
- [初期値] 5

5.2.24 MP が失敗できる最大回数の設定

- [書式] **isdn call prohibit mp-error count** *times*
no isdn call prohibit mp-error count
- [設定値] ◦ *times*
- 失敗できる最大回数 (1..21474836)
 - off 発信制限をかけない
- [説明] 選択されている相手に対し、MP が失敗できる最大回数を設定する。最大回数を越えた場合、**ppp mp use**、**ppp mp minlink**、**ppp mp maxlink** コマンドで設定を直さないと同じ相手に MP で発呼できない。
- [初期値] 5

5.2.25 相手先毎の累積接続時間による発信制限の設定

- [書式] **pp connect time threshold** *time*
no pp connect time threshold
- [設定値] ◦ *time*..... 秒数 (1..21474836)
- [説明] 選択された相手先に対する累計接続時間の閾値を設定する。
 なお、発信時の接続時間の累計を累積接続時間として使用する。
- [ノート] 累積接続時間は本製品の通信時間算出方式により計算された通信時間の累計のため、プロバイダ独自の通信時間算出方法により計算された累積接続時間とは異なることがある。
- [初期値] なし

5.2.26 相手先毎の累積接続回数による発信制限の設定

- [書式] **pp connect count threshold** *count*
no pp connect count threshold

- [設定値] ◦ *count*回数 (1..21474836)
- [説明] 選択された相手先に対する累計接続回数の閾値を設定する。
 なお、発信時の接続回数の累計を累積接続回数として使用する。
 累積接続回数は **clear account** コマンドにより 0 に設定される。
- [初期値] なし

5.2.27 i・ナンバーサービスのポート番号の設定

- [書式] **isdn arrive inumber-port interface inum_port [inum_port...]**
 no isdn arrive inumber-port interface
- [設定値] ◦ *interface*
 • BRI インタフェース名
- *inum_port* i・ナンバーサービスのポート番号
- 1..... ポート番号 1 で着信する
 - 2..... ポート番号 2 で着信する
 - 3..... ポート番号 3 で着信する
 - all すべてのポート番号で着信する
 - none..... 着信しない
- [説明] ルータで着信する i・ナンバーサービスのポート番号を選択する。
- [初期値] all

6. IP の設定

6.1 インタフェース共通の設定

6.1.1 IP パケットを扱うか否かの設定

- [書式] **ip routing** *routing*
no ip routing [*routing*]
- [設定値] ◦ *routing*
- on..... IP パケットを処理対象として扱う
 - off..... IP パケットを処理対象として扱わない
- [説明] IP パケットをルーティングするかどうかを設定する。
- [ノート] off の場合でも TELNET による設定や TFTP によるアクセス、PING 等は可能。
- [初期値] on

6.1.2 IP アドレスの設定

- [書式] **ip interface address** *ip_address/mask* [*broadcast broadcast_ip*]
ip interface address *dhcp*
ip pp address *ip_address/mask* [*broadcast broadcast_ip*]
no ip interface address [*ip_address/mask*]
no ip pp address [*ip_address/mask*]
- [設定値] ◦ *interface* LAN インタフェース名
- *ip_adddres*..... IP アドレス xxx.xxx.xxx.xxx (xxx は十進数)
 - *dhcp* DHCP クライアントとして IP アドレスを取得することを示すキーワード
 - *mask*
 - xxx.xxx.xxx.xxx (xxx は十進数)
 - 0x に続く十六進数
 - マスクビット数 - *broadcast_ip* ブロードキャスト IP アドレス
- [説明] インタフェースの IP アドレスとネットマスクを設定する。“*broadcast broadcast_ip*” を指定すると、ブロードキャストアドレスを指定できる。省略した場合には、ディレクティッドブロードキャストアドレスが使われる。*dhcp* を指定すると、設定直後に DHCP クライアントとして IP アドレスを取得する。また *dhcp* を指定している場合に **no ip interface address** を入力すると、取得していた IP アドレスの開放メッセージを DHCP サーバーに送る。
- [ノート] LAN インタフェースに IP アドレスを設定していない場合には、RARP により IP アドレスを得ようとする。
PP インタフェースに IP アドレスを設定していない場合には、そのインタフェースは unnumbered として動作する。
DHCP クライアントとして動作させた場合に取得したクライアント ID は、**show status dhcpc** コマンドで確認することができる。
- [初期値] IP アドレスは設定されていない
ディレクティッドブロードキャストアドレスが使われる

6.1.3 セカンダリ IP アドレスの設定

- [書式] **ip interface secondary address** *ip_address*[/*mask*]
ip interface secondary address dhcp
no ip interface secondary address [*ip_address*/*mask*]
- [設定値]
- *interface* LAN インタフェース名
 - *ip_address* セカンダリ IP アドレス xxx.xxx.xxx.xxx (xxx は十進数)
 - *dhcp* DHCP クライアントとして IP アドレスを取得することを示すキーワード
 - *mask*
 - xxx.xxx.xxx.xxx (xxx は十進数)
 - 0x に続く十六進数
 - マスクビット数
- [説明] LAN 側のセカンダリ IP アドレスとネットマスクを設定する。
 dhcp を指定すると、設定直後に DHCP クライアントとして IP アドレスを取得する。
- [ノート] セカンダリのネットワークでのブロードキャストアドレスは必ずディレクティッドブロードキャストアドレスが使われる。

6.1.4 IP の静的経路情報の設定

- [書式] **ip route network gateway gateway** [*parameter*] [*gateway gateway* [*parameter*]]
no ip route network [*gateway*...]
- [設定値]
- *network*
 - default..... デフォルト経路
 - IP アドレス 送り先のホスト / マスクビット数 (省略時は 32)
 - *gateway*
 - IP アドレス xxx.xxx.xxx.xxx (xxx は十進数)
 - *pp peer_num* PP インタフェースへの経路
 - *peer_num*
 - 相手先情報番号
 - anonymous
 - *pp anonymous name=name*
 - *name*..... PAP/CHAP による名前
 - *dhcp interface*
 - *interface* DHCP で与えられるデフォルトゲートウェイを使う場合の DHCP クライアントとして動作する LAN インタフェース名 (送り先が Default の時のみ有効)
 - *tunnel tunnel_num* トンネルインタフェースへの経路
 - *parameter*..... 以下のパラメータを空白で区切り複数設定可能
 - *filter number* [*number*...]... フィルタ型経路の指定
 - *number*..... フィルタの番号 (1..21474836) (空白で区切り複数設定可能)
 - *metric metric* メトリックの指定
 - *metric*
 - メトリック値 (1..15)
 - 省略時は 1
 - *hide*..... 出力インタフェースが PP インタフェースまたは TUNNEL インタフェースの場合のみ有効なオプションで、回線が接続されている場合だけ経路が有効になることを意味する
 - *weight weight* 異なる経路間の比率を表す値
 - *weight*
 - 経路への重み (1..2147483647)
 - 省略時は 1
- [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。

[ノート] 既に存在する経路を上書きすることができる。

[設定例] ◦ デフォルトゲートウェイを 192.168.0.1 とする
ip route default gateway 192.168.0.1

◦ PP1 で接続している相手のネットワークは 192.168.1.0/24 である
ip route 192.168.1.0/24 gateway pp 1

6.1.5 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

[設定値] ◦ log
• on..... IPv4 経路の変化をログに記録する
• off..... IPv4 経路の変化をログに記録しない

[説明] IPv4 の経路情報に変化があった時にそれをログに記録するか否かを設定する。ログは INFO レベルで記録される。

[初期値] off

6.1.6 IP パケットのフィルタの設定

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

[設定値] ◦ filter_num 静的フィルタ番号 (1..21474836)
◦ pass_reject
• pass-log..... 一致すれば通す (ログに記録する)
• pass-nolog..... 一致すれば通す (ログに記録しない)
• reject-log..... 一致すれば破棄する (ログに記録する)
• reject-nolog..... 一致すれば破棄する (ログに記録しない)
• restrict-log..... 回線が接続されていれば通し、切断されていれば破棄する (ログに記録する)
• restrict-nolog..... 回線が接続されていれば通し、切断されていれば破棄する (ログに記録しない)
◦ src_addr IP パケットの始点 IP アドレス
• xxx.xxx.xxx.xxx xxx は
▪ 十進数
▪ * (ネットマスクの対応するビットが 8 ビットとも 0 と同じ)
• 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 アドレスに対応)
◦ dest_addr IP パケットの終点 IP アドレス (src_addr と同じ形式)。
省略時は 1 個の * と同じ。
◦ mask IP アドレスのビットマスク、省略時は 0xfffff と同じ。
src_addr 及び dest_addr がネットワークアドレスの場合にのみ指定可。
• xxx.xxx.xxx.xxx (xxx は十進数)
• 0x に続く十六進数
• マスクビット数

◦ *protocol* フィルタリングするパケットの種類

- プロトコルを表す十進数 (0..255)
- プロトコルを表すニーモニック

ニーモニック	十進数	説明
icmp	1	icmp パケット
icmp-error	-	特定のTYPE コードの icmp パケット
icmp-info	-	特定のTYPE コードの icmp パケット
tcp	6	tcp パケット
tcpfin	-	FIN フラグの立っている tcp パケット
tcprst	-	RST フラグの立っている tcp パケット
established	-	ACK フラグの立っている tcp パケット 内から外への接続は許可するが、 外から内への接続は拒否する機能
udp	17	udp パケット
esp	50	IPsec の esp パケット
ah	51	IPsec の ah パケット

- 上項目のカンマで区切った並び (5 個以内)
- `tcpflag=flag_value/flag_mask` または `tcpflag!=flag_value/flag_mask`
 - ◻ `flag_value`(0xに続く十六進数 0x0000 .. 0xffff)
 - ◻ `flag_mask`(0xに続く十六進数 0x0000 .. 0xffff)
- * (すべてのプロトコル)
- 省略時は * と同じ。

◦ *src_port_list*..... UDP、TCP のソースポート番号

- ポート番号を表す十進数
- ポート番号を表すニーモニック (一部)

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

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

◦ *dest_port_list*.....UDP、TCP のデスティネーションポート番号

[説明] IP パケットのフィルタを設定する。本コマンドで設定されたフィルタは **ip interface secure filter**、**ip filter set**、**ip filter dynamic**、及び **ip interface rip filter** コマンドで用いられる。

[ノート] `restrict-log` 及び `restrict-nolog` を使ったフィルタは、回線が接続されている場合だけ通せば十分で、そのため回線に発信するまでもないようなパケットに対して有効。例えば、時計をあわせる NTP パケット。
"ip filter pass * * icmp,tcp telnet" などのように、TCP/UDP 以外のプロトコルとポート番号の両方が指定されている場合、TCP/UDP 以外のパケットに関しては、ポート番号の指定をチェックしない。
"ip filter pass * * * telnet" などのように、TCP/UDP と明記せずにポート番号を指定していた場合、TCP/UDP 以外もフィルタに該当する。

[設定例] `# ip filter 3 pass-nolog 172.20.10.* 172.21.192.0/18 tcp ftp`

6.1.7 フィルタセットの定義

[書式] **ip filter set** *name direction filter_list* [*filter_list* ...]
no ip filter set *name* [*direction* ...]

- [設定値]
- *name*..... フィルタセットの名前を表す文字列
 - *direction*
 - *in* 入力方向のフィルタ
 - *out* 出力方向のフィルタ
 - *filter_list*..... 空白で区切られたフィルタ番号の並び (100 個以内)
- [説明]
- フィルタセットを定義する。フィルタセットは、in/out のフィルタをそれぞれ定義し、**ip interface secure filter** コマンドによりインタフェースに適用される。

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

- [書式]
- ```
ip filter source-route filter_out
no ip filter source-route [filter_out]
```
- [設定値]
- *filter\_out*
    - *on*..... フィルタアウトする
    - *off* ..... フィルタアウトしない
- [説明]
- Source-route オプション付き IP パケットをフィルタアウトするか否かを設定する。
- [初期値]
- on

### 6.1.9 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]
no ip filter directed-broadcast
```
- [設定値]
- *filter_out*
 - *on*..... フィルタアウトする
 - *off* フィルタアウトしない
 - *filter_num* 静的フィルタ番号 (1..21474836)
- [説明]
- 終点アドレスがディレクティッドブロードキャストアドレスである IPv4 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]
- このコマンドでのチェックよりも、**wol relay** コマンドのチェックの方が優先される。wol relay コマンドでのチェックにより通過させることができなかったパケットのみが、このコマンドでのチェックを受ける。
- いわゆる smurf 攻撃を防止するためには *on* にしておく。
- [初期値]
- on

6.1.10 動的フィルタの定義

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



- [ 設定値 ]
- *dyn\_filter\_num* ..... 動的フィルタ番号 (1..21474836)
  - *srcaddr* ..... 始点 IP アドレス
  - *dstaddr* ..... 終点 IP アドレス
  - *protocol* ..... プロトコル
    - tcp
    - udp
    - ftp
    - tftp
    - domain
    - www
    - smtp
    - pop3
    - telnet
    - netmeeting
  - *filter\_list*..... **ip filter** コマンドで登録されたフィルタ番号のリスト
  - *option*
    - *syslog=switch*
      - *on*.....コネクションの通信履歴を SYSLOG に残す
      - *off*.....コネクションの通信履歴を SYSLOG に残さない
    - *timeout=time*
      - *time*.....データが流れなくなったときにコネクション情報を解放するまでの時間 ( 秒 )
- [ 説明 ]
- 動的フィルタを定義する。第 1 書式では、あらかじめルータに登録されているアプリケーション名を指定する。第 2 書式では、ユーザがアクセス制御のルールを記述する。キーワードの **filter**、**in**、**out** の後には、**ip filter** コマンドで定義されたフィルタ番号を設定する。
- filter** キーワードの後に記述されたフィルタに該当するコネクション (トリガ) を検出したら、それ以降 **in** キーワードと **out** キーワードの後に記述されたフィルタに該当するコネクションを通過させる。**in** キーワードはトリガの方向に対して逆方向のアクセスを制御し、**out** キーワードは動的フィルタと同じ方向のアクセスを制御する。なお、**ip filter** コマンドの IP アドレスは無視される。**pass/reject** の引数も同様に無視される。
- プロトコルとして **tcp** や **udp** を指定した場合には、アプリケーションに固有な処理は実施されない。特定のアプリケーションを扱う必要がある場合には、アプリケーション名を指定する。
- [ 初期値 ]
- syslog* = on  
*timeout* = 60
- [ 設定例 ]
- ```
# ip filter 10 * * udp * snmp
# ip filter dynamic 1 * * filter 10
```

6.1.11 TCP セッションの MSS 制限の設定

- [書式]
- ```
ip interface tcp mss limit mss
ip pp tcp mss limit mss
ip tunnel tcp mss limit mss
no ip interface tcp mss limit [mss]
no ip pp tcp mss limit [mss]
no ip tunnel tcp mss limit [mss]
```
- [ 設定値 ]
- *interface* ..... LAN インタフェース名
  - *mss*
    - MSS の最大長 (536 .. 1460)
    - *auto*..... 自動設定
    - *off*..... 設定しない
- [ 説明 ]
- インタフェースを通過する TCP セッションの MSS を制限する。インタフェースを通過する TCP パケットを監視し、MSS オプションの値が設定値を越えている場合には、設定値に書き換える。キーワード **auto** を指定した場合には、インタフェースの MTU、もしくは PP インタフェースの場合で相手の MRU 値が分かる場合にはその MRU 値から計算した値に書き換える。
- [ ノート ]
- PPPoE 用の PP インタフェースに対しては、**pppoe tcp mss limit** コマンドでも TCP セッションの MSS を制限することができる。このコマンドと **pppoe tcp mss limit** コマンドの両方が有効な場合は、MSS はどちらかより小さな方の値に制限される。
- [ 初期値 ]
- off

### 6.1.12 動的フィルタのタイムアウトの設定

- [書式] **ip filter dynamic timer** [*option=timeout* [*option...*]]  
**no ip filter dynamic timer**
- [設定値]
- *option* ..... オプション名
    - tcp-syn-timeout ..... SYN を受けてから設定された時間内にコネクションが確立しなければセッションを切断する
    - tcp-fin-timeout ..... FIN を受けてから設定された時間が経てばコネクションを強制的に解放する
    - tcp-idle-time ..... 設定された時間内に TCP コネクションのデータが流れなければコネクションを切断する
    - udp-idle-time ..... 設定された時間内に UDP コネクションのデータが流れなければコネクションを切断する
    - dns-timeout ..... DNS の要求を受けてから設定された時間内に応答を受けなければコネクションを切断する
  - *timeout* ..... 待ち時間 (秒)
- [説明] 動的フィルタのタイムアウトを設定する。
- [ノート] 本設定はすべての検査において共通に使用される。
- [初期値]
- ```
tcp-syn-timeout=30
tcp-fin-timeout=5
tcp-idle-time=3600
udp-idle-time=30
dns-timeout=5
```

6.1.13 侵入検知機能の動作の設定

- [書式] **ip interface intrusion detection direction switch** [*option*]
ip pp intrusion detection direction switch [*option*]
ip tunnel intrusion detection direction switch [*option*]
no ip interface intrusion detection
no ip pp intrusion detection
no ip tunnel intrusion detection
- [設定値]
- *interface* LAN インタフェース名
 - *direction* 観察するパケットの方向
 - in インタフェース側から内側へ
 - out インタフェース側から外側へ
 - *switch*
 - on 実行する
 - off 実行しない
 - *option* オプション
 - reject=*rjt*
 - on 不正なパケットを破棄する
 - off 不正なパケットを破棄しない
- [説明] 指定したインタフェースで、指定された向きのパケットについて侵入を検知する。
- [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。
- [初期値]
- ```
switch = off
reject = off
```

### 6.1.14 1 秒間に侵入検知情報を通知する頻度の設定

- [書式] **ip interface intrusion detection notice-interval frequency**  
**ip pp intrusion detection notice-interval frequency**  
**ip tunnel intrusion detection notice-interval frequency**  
**no ip interface intrusion detection notice-interval**  
**no ip pp intrusion detection notice-interval**  
**no ip tunnel intrusion detection notice-interval**
- [設定値]
- *frequency* ..... 頻度 (1..1000)

[ 説明 ] 1 秒間に侵入検知情報を通知する頻度を設定する。

[ 初期値 ] 1

### 6.1.15 重複する侵入検知情報の通知抑制の設定

[ 書式 ] **ip interface intrusion detection repeat-control time**  
**ip pp intrusion detection repeat-control time**  
**ip tunnel intrusion detection repeat-control time**  
**no ip interface intrusion detection repeat-control**  
**no ip pp intrusion detection repeat-control**  
**no ip tunnel intrusion detection repeat-control**

[ 設定値 ] ◦ *time*..... 秒数 (1..1000)

[ 説明 ] 同じホストに対する同じ種類の攻撃を、*time* 秒に 1 回のみ通知するよう抑制する。

[ 初期値 ] 60

### 6.1.16 侵入検知情報の最大表示件数の設定

[ 書式 ] **ip interface intrusion detection report num**  
**ip pp intrusion detection report num**  
**ip tunnel intrusion detection report num**  
**no ip interface intrusion detection report**  
**no ip pp intrusion detection report**  
**no ip tunnel intrusion detection report**

[ 設定値 ] ◦ *num* ..... 件数 (1..1000)

[ 説明 ] **show ip intrusion detection** コマンドで表示される侵入検知情報の最大件数を設定する。

[ 初期値 ] 50

### 6.1.17 侵入検知で用いる閾値の設定

[ 書式 ] **ip interface intrusion detection threshold type count**  
**ip pp intrusion detection threshold type count**  
**ip tunnel intrusion detection threshold type count**  
**no ip interface intrusion detection threshold type**  
**no ip pp intrusion detection threshold type**  
**no ip tunnel intrusion detection threshold type**

[ 設定値 ] ◦ *type*..... 閾値を設定する攻撃の種類

- port-scan..... ポートスキャン
- syn-flood..... SYN フラッド

◦ *count*..... 閾値 (1..65535)

[ 説明 ] 侵入検知で用いる閾値を設定する。攻撃のタイプと設定する数値の意味は以下のようになる。

| <i>type</i> | <i>count</i> 値の意味                                              |
|-------------|----------------------------------------------------------------|
| port-scan   | 同じホストに対して、1 秒間に <i>count</i> 種類の異なるポートへのアクセスを検出したらポートスキャンと判定する |
| syn-flood   | 同じホストに対する SYN パケットを、1 秒間に <i>count</i> 回以上検出したら SYN フラッドと判定する  |

[ 初期値 ] port-scan = 64  
syn-flood = 100

### 6.1.18 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] | <ul style="list-style-type: none"> <li>◦ <i>service</i> <ul style="list-style-type: none"> <li>• on.....TCP/UDP の各種サービスを動作させる</li> <li>• off .....サービスを停止させる</li> </ul> </li> </ul> |
| [説明]  | TCP/UDP の echo(7)、discard(9)、time(37) の各種サービスを動作させるか否かを設定する。サービスを停止すると該当のポートも閉じる。                                                                                                   |
| [ノート] | 本製品を指定して rdate により時計を合わせている機器がある場合には、ip simple-service on と設定しなければならない。                                                                                                             |
| [初期値] | off                                                                                                                                                                                 |

### 6.1.19 フィルタに一致する IP パケットの DF ビットを 0 に書き換えるか否かの設定

|       |                                                                                                                                                                                                                                                                                                    |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [書式]  | <b>ip fragment remove df-bit filter</b> <i>filter_num ...</i><br><b>no ip fragment remove df-bit filter</b> [ <i>filter_num ...</i> ]                                                                                                                                                              |
| [設定値] | ◦ <i>filter_num</i> ..... <b>ip filter</b> コマンドで登録されたフィルタ番号                                                                                                                                                                                                                                        |
| [説明]  | フォワーディングする IP パケットの内、フィルタに一致するものは DF ビットを 0 に書き換える。                                                                                                                                                                                                                                                |
| [ノート] | DF ビットは経路 MTU 探索アルゴリズムで利用されるが、経路の途中で ICMP パケットをフィルタするファイアウォールなどがあるとアルゴリズムがうまく動作せず、特定の通信相手とだけは通信ができないなどの現象になることがある。この様な現象は、「経路 MTU 探索ブラックホール (Path MTU Discovery Blackhole)」と呼ばれている。この経路 MTU 探索ブラックホールがある場合には、このコマンドでそのような相手との通信に関して DF ビットを 0 に書き換えてしまえば、経路 MTU 探索は正しく動作しなくなるものの、通信できなくなるということはない。 |

### 6.1.20 フィルタリングによるセキュリティの設定

|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [書式]  | <b>ip interface secure filter</b> <i>direction</i> [ <i>filter_list...</i> ] [ <i>dynamic filter_list...</i> ]<br><b>ip pp secure filter</b> <i>direction</i> [ <i>filter_list...</i> ] [ <i>dynamic filter_list...</i> ]<br><b>ip tunnel secure filter</b> <i>direction</i> [ <i>filter_list...</i> ] [ <i>dynamic filter_list...</i> ]<br><b>ip interface secure filter</b> <i>name set_name</i><br><b>ip pp secure filter</b> <i>name set_name</i><br><b>ip tunnel secure filter</b> <i>name set_name</i><br><b>no ip interface secure filter</b> <i>direction</i> [ <i>filter_list</i> ]<br><b>no ip pp secure filter</b> <i>direction</i> [ <i>filter_list</i> ]<br><b>no ip tunnel secure filter</b> <i>direction</i> [ <i>filter_list</i> ]<br><b>no ip interface secure filter</b> [ <i>name</i> [ <i>set_name</i> ]]<br><b>no ip pp secure filter</b> [ <i>name</i> [ <i>set_name</i> ]]<br><b>no ip tunnel secure filter</b> [ <i>name</i> [ <i>set_name</i> ]] |
| [設定値] | <ul style="list-style-type: none"> <li>◦ <i>interface</i> ..... LAN インタフェース名</li> <li>◦ <i>direction</i> <ul style="list-style-type: none"> <li>• in .....受信したパケットのフィルタリング</li> <li>• out .....送信するパケットのフィルタリング</li> </ul> </li> <li>◦ <i>filter_list</i>..... 空白で区切られたフィルタ番号の並び (128 個以内)</li> <li>◦ <i>set_name</i> ..... フィルタセットの名前を表す文字列</li> <li>◦ <i>dynamic</i> ..... キーワード後に動的フィルタの番号を記述する</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| [説明]  | <b>ip filter</b> コマンドによるパケットのフィルタを組み合わせて、インタフェースで送受信するパケットの種類を制限する。<br>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 / 廃棄が決定する。それ以降のフィルタは調べられない。すべてのフィルタにマッチしないパケットは廃棄される。<br>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 での検査は行われぬ。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。
- [初期値] フィルタは設定されていない

### 6.1.21 インタフェースの MTU の設定

- [書式] **ip interface mtu mtu0**  
**ip pp mtu mtu1**  
**ip tunnel mtu mtu2**  
**no ip interface mtu [mtu0]**  
**no ip pp mtu [mtu1]**  
**no ip tunnel mtu [mtu2]**
- [設定値] ○ *interface* ..... LAN インタフェース名  
 ○ *mtu0, mtu1, mtu2*..... MTU の値 (64..1500)
- [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、それらでは初期値のまま 1500 の MTU となる。
- [初期値] mtu0 = 1500  
 mtu1 = 1500  
 mtu2 = 1280

### 6.1.22 ARP が解決されるまで送信を保留するパケットの数の設定

- [書式] **ip interface arp queue length len**  
**no ip interface arp queue length [len]**
- [設定値] ○ *interface* ..... LAN インタフェース名  
 ○ *len* ..... キュー長 (0..10000)
- [説明] ARP が解決していないホストに対してパケットを送信しようとした時に、ARP が解決するか、タイムアウトにより ARP が解決できないことが確定するまで、インタフェース毎に送信を保留しておくことのできるパケットの最大数を設定する。  
 0 を設定するとパケットを保留しなくなるため、例えば ARP が解決していない相手に ping を実行すると必ず最初の 1 パケットは失敗するようになる。
- [ノート] 本コマンドが実装される以前のバージョンでは、送信を保留する数の上限は設定されておらず、いくらでも保留することができた。
- [初期値] 40

## 6.2 代理 ARP の設定

- [書式] **ip interface proxyarp proxyarp**  
**no ip interface proxyarp [proxyarp]**
- [設定値] ○ *interface* ..... LAN インタフェース名  
 ○ *proxyarp*  
 ● *on*.....代理 ARP 動作をする  
 ● *off*.....代理 ARP 動作をしない
- [説明] 代理 ARP 動作をするか否か設定する。
- [初期値] off

### 6.2.1 ARP エントリの寿命の設定

---

- [書式]           **ip arp timer timer**  
**no ip arp timer [timer]**
- [設定値]           ◦ *timer* ..... ARP エントリの寿命秒数 (30..32767)
- [説明]            ARP エントリの寿命を設定する。ARP 手順で得られた IP アドレスと MAC アドレスの組は ARP エントリとして記憶されるが、このコマンドで設定した時間だけ経過すると、再度 ARP 手順が実行される。その時点で ARP に応答が無い場合にはエントリは消される。
- [初期値]           1200

### 6.2.2 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 [mac\_address]**
- [設定値]           ◦ *interface* ..... LAN インタフェース名  
◦ *ip\_address* ..... IP アドレス  
◦ *mac\_address* ..... MAC アドレス
- [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。

## 6.3 PP 側の設定

### 6.3.1 相手の PP 側 IP アドレスの設定

---

- [書式]           **ip pp remote address ip\_address**  
**ip pp remote address dhcp [interface]**  
**no ip pp remote address [ip\_address]**
- [設定値]           ◦ *ip\_address*  
• IP アドレス ..... xxx.xxx.xxx.xxx (xxx は十進数)  
• dhcp ..... 自分自身の DHCP サーバー機能より IP アドレスを割り当てる  
◦ dhcp ..... DHCP クライアントを利用することを示すキーワード  
◦ *interface*  
• DHCP クライアントとして動作する LAN インタフェース名  
• 省略時は lan1
- [説明]            選択されている相手の PP 側の IP アドレスを設定する。  
dhcp を設定した場合は、自分自身が DHCP サーバーとして動作している必要がある。自分で管理している DHCP スコープの中から、IP アドレスを割り当てる。  
最大 8 つまで設定できる。
- dhcp を設定した場合は、*interface* で指定した LAN インタフェースが DHCP クライアントとして IP アドレスを取得し、そのアドレスを PP 側に割り当てる。取得できなかった場合は、0.0.0.0 を割り当てる。
- [初期値]           相手側 IP アドレスは設定されていない
- [設定例]           例えば、ルータ A 側が "no ip pp remote address"、"ppp ipcp ipaddress on" と設定し、接続するルータ B 側が "ip pp address yyy.yyy.yyy.yyy" と設定している場合には、実際のルータ A での相手の PP 側の IP アドレスは "yyy.yyy.yyy.yyy" になることを意味する。

### 6.3.2 リモート IP アドレスプールの設定

- [ 書式 ]     **ip pp remote address pool** *ip\_address* [*ip\_address...*]  
**ip pp remote address pool** *ip\_address-ip\_address*  
**ip pp remote address pool** dhcp  
**ip pp remote address pool** dhcpc [*interface*]  
**no ip pp remote address pool**
- [ 設定値 ]     ◦ *ip\_address* ..... anonymous のためにプールする IP アドレス  
◦ *ip\_address-ip\_address* ..... IP アドレスの範囲  
◦ dhcp ..... 自分自身の DHCP サーバー機能を利用することを示すキーワード  
◦ dhcpc ..... DHCP クライアントを利用することを示すキーワード  
◦ *interface*  
    • DHCP クライアントとして動作する LAN インタフェース名  
    • 省略時は lan1
- [ 説明 ]     anonymous で相手に割り当てるための IP アドレスプールを設定する。PP として anonymous が選択された場合のみ有効である。  
dhcp を設定した場合は、自分自身が DHCP サーバーとして動作している必要がある。自分で管理している DHCP スコープの中から、IP アドレスを割り当てる。  
dhcpc を設定した場合は、*interface* で指定した LAN インタフェースが DHCP クライアントとして IP アドレス情報のみを取得し、そのアドレスを割り当てる。取得できなかった場合は、0.0.0.0 を割り当てる。2 個まで設定できる。

### 6.3.3 PP 経由のキープアライブの時間間隔の設定

- [ 書式 ]     **pp keepalive interval** *interval* [*retry-interval=retry-interval*] [*count=count*] [*time=time*]  
**no pp keepalive interval** [*interval* [*count*]]
- [ 設定値 ]     ◦ *interval* ..... キープアライブパケットを送出する時間間隔 [ 秒 ] (1..65535)  
◦ *retry-interval* ..... キープアライブパケットの確認に一度失敗した後の送信間隔。単位は秒。キープアライブパケットが確認できれば、送信間隔はまた *interval* に戻る。  
◦ *count* ..... この回数連続して応答がなければ相手側のルータをダウンしたと判定する (3..100)  
◦ *time* ..... キープアライブパケットの確認に失敗するようになってから回線断と判断するまでの時間。単位は秒。*count* パラメータとは同時には指定できない。
- [ 説明 ]     PP インタフェースでのキープアライブパケットの送信間隔と、回線断と判定するまでの再送回数および時間を設定する。
- 送信したキープアライブパケットに対して返事が返って来ている間は *interval* で指定した間隔でキープアライブパケットを送信する。一度、返事が確認できなかった時には送信間隔が *retry-interval* パラメータの値に変更される。*count* パラメータに示された回数だけ連続して返事が確認できなかった時には回線断と判定する。
- 回線断判定までの時間を *time* パラメータで指定した場合には、少なくとも指定した時間の間、キープアライブパケットの返事が連続して確認できない時に回線断と判定する。
- [ ノート ]     *time* パラメータを指定した場合には、その値はキープアライブの間隔と再送回数によって再計算されるため、設定値とは異なる値が **show config** で表示されることがある。
- [ 初期値 ]     *interval* = 30  
*retry-interval* = 1  
*count* = 6

### 6.3.4 PP 経由のキープアライブを使用するか否かの設定

[書式] **pp keepalive use** lcp-echo  
**pp keepalive use** icmp-echo *dest\_ip* [*option=value...*] [*dest\_ip* [*option=value...*]...]  
**pp keepalive use** lcp-echo icmp-echo *dest\_ip* [*option=value...*] [*dest\_ip* [*option=value...*]...]  
**pp keepalive use** off  
**no pp keepalive use**

[設定値] ○ lcp-echo ..... LCP Echo Request/Reply を用いる  
○ icmp-echo ..... ICMP Echo Reply を用いる  
○ *dest\_ip* ..... キープアライブ確認先の IP アドレス  
○ *option=value* 列

| <i>option</i>     | <i>value</i> | 説明                          |
|-------------------|--------------|-----------------------------|
| <i>upwait</i>     | ミリ秒          | アップ検知のための許容応答時間 (1..10000)  |
| <i>downwait</i>   | ミリ秒          | ダウン検知のための許容応答時間 (1..10000)  |
| <i>disconnect</i> | 秒            | 無応答切断時間 (1..21474836)       |
| <i>length</i>     | バイト          | ICMP Echo パケットの長さ (64-1500) |

○ off ..... キープアライブを使用しない

[説明] 選択した相手先に対する接続のキープアライブ動作を設定する。  
lcp-echo 指定で LCP Echo Request/Reply を用い、icmp-echo も指定すれば ICMP Echo/Reply も同時に用いる。icmp-echo を使用する場合には IP アドレスの設定が必要である。

[ノート] このコマンドを設定していない場合でも、**pp always-on** コマンドで on と設定していれば、LCP Echo によるキープアライブが実行される。

icmp-echo で確認する IP アドレスに対する経路は、設定される PP インタフェースが送出先となるよう設定される必要がある。

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

*disconnect* オプションは、PPPoE で使用する場合に PPPoE レベルでの再接続が必要な場合に使用する。*disconnect* オプションが設定されている場合に、設定時間内に icmp-echo の応答がないと、PPPoE レベルで一度切断操作を行なうため、**pp always-on** コマンドとの併用により再接続を行なうことができる。他のパラメータがデフォルト値の場合、*disconnect* オプションは 70 秒程度に設定しておく、ダウン検出後の切断動作が確実に行われる。

*length* オプションで指定するのは 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。

[初期値] off

### 6.3.5 PP 経由のキープアライブのログをとるか否かの設定

[書式] **pp keepalive log** *log*  
**no pp keepalive log** [*log*]

[設定値] ○ *log*  
• on ..... ログをとる  
• off ..... ログをとらない

[説明] PP 経由のキープアライブをログにとるか否かを設定する。

[ノート] この設定は、すべての PP で共通に用いられる。

[初期値] off



### 6.3.6 専用線ダウン検出時の動作の設定

|         |                                                                                                                                                                             |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ 書式 ]  | <b>leased keepalive down action</b><br><b>no leased keepalive down</b> [action]                                                                                             |
| [ 設定値 ] | <ul style="list-style-type: none"> <li>◦ action           <ul style="list-style-type: none"> <li>• silent .....何もしない</li> <li>• reset .....ルータを再起動する</li> </ul> </li> </ul> |
| [ 説明 ]  | キープアライブによって専用線ダウンを検出した場合のルータの動作を設定する。                                                                                                                                       |
| [ 初期値 ] | silent                                                                                                                                                                      |

## 6.4 RIP の設定

### 6.4.1 RIP を使用するか否かの設定

|         |                                                                                                                                                                             |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ 書式 ]  | <b>rip use rip_use</b><br><b>no rip use rip_use</b>                                                                                                                         |
| [ 設定値 ] | <ul style="list-style-type: none"> <li>◦ rip_use           <ul style="list-style-type: none"> <li>• on .....RIP を使用する</li> <li>• off .....RIP を使用しない</li> </ul> </li> </ul> |
| [ 説明 ]  | RIP を使用するか否かを設定する。この機能を OFF にすると、すべてのインタフェースに対して RIP パケットを送信することはなくなり、受信した RIP パケットは無視される。                                                                                  |
| [ 初期値 ] | off                                                                                                                                                                         |

### 6.4.2 RIP に関して信用できるゲートウェイの設定

|         |                                                                                                                                                                                                                                                                                                                                                                                   |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ 書式 ]  | <b>ip interface rip trust gateway</b> [except] gateway_list<br><b>ip pp rip trust gateway</b> [except] gateway_list<br><b>ip tunnel rip trust gateway</b> [except] gateway_list<br><b>no ip interface rip trust gateway</b> [[except] gateway_list]<br><b>no ip pp rip trust gateway</b> [[except] gateway_list]<br><b>no ip tunnel rip trust gateway</b> [[except] gateway_list] |
| [ 設定値 ] | <ul style="list-style-type: none"> <li>◦ interface ..... LAN インタフェース名</li> <li>◦ gateway_list ..... IP アドレスの並び (10 個以内)</li> </ul>                                                                                                                                                                                                                                                |
| [ 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。<br>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。<br>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。                                                                                                                                                                                   |
| [ 初期値 ] | 信用できる、あるいは信用できないゲートウェイは設定されておらず、すべてのホストからの RIP を信用できるものとして扱う                                                                                                                                                                                                                                                                                                                      |

### 6.4.3 RIP パケットの送信に関する設定

|        |                                                                                                                                                                                                                                                                                                                                                  |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ 書式 ] | <b>ip interface rip send rip_send</b> [version version [broadcast]]<br><b>ip pp rip send rip_send</b> [version version [broadcast]]<br><b>ip tunnel rip send rip_send</b> [version version [broadcast]]<br><b>no ip interface rip send</b> [rip_send...]<br><b>no ip pp rip send</b> [rip_send...]<br><b>no ip tunnel rip send</b> [rip_send...] |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

- [設定値]
- *interface* ..... LAN インタフェース名
  - *rip\_send*
    - *on*..... RIP パケットを送信する
    - *off* ..... RIP パケットを送信しない
  - *version* ..... 送信する RIP のバージョン (1,2)
  - *broadcast*..... **ip interface address** コマンドで指定したブロードキャストアドレス
- [説明]
- 指定したインタフェースに対し、RIP パケットを送信するか否かを設定する。  
"version *version*" で送信する RIP のバージョンを指定できる。
- [初期値]
- off (トンネルインタフェースの場合)  
on version 1 (その他のインタフェースの場合)

#### 6.4.4 RIP パケットの受信に関する設定

- [書式]
- ```
ip interface rip receive rip_receive [version version [version]]
ip pp rip receive rip_receive [version version [version]]
ip tunnel rip receive rip_receive [version version [version]]
no ip interface rip receive [rip_receive...]
no ip pp rip receive [rip_receive...]
no ip tunnel rip receive [rip_receive...]
```
- [設定値]
- *interface* LAN インタフェース名
 - *rip_receive*
 - *on*..... RIP パケットを受信する
 - *off* RIP パケットを受信しない
 - *version* 受信する RIP のバージョン (1,2)
- [説明]
- 指定したインタフェースに対し、RIP パケットを受信するか否かを設定する。
"version *version*" で受信する RIP のバージョンを指定できる。指定しない場合は、RIP1/2 ともに受信する。
- [初期値]
- off (トンネルインタフェースの場合)
on version 1 2 (その他のインタフェースの場合)

6.4.5 RIP のフィルタリングの設定

- [書式]
- ```
ip interface rip filter direction filter_list
ip pp rip filter direction filter_list
ip tunnel rip filter direction filter_list
no ip interface rip filter direction filter_list
no ip pp rip filter direction filter_list
no ip tunnel rip filter direction filter_list
```
- [設定値]
- *interface* ..... LAN インタフェース名
  - *direction*
    - *in* ..... 受信した RIP のフィルタリング
    - *out* ..... 送信する RIP のフィルタリング
  - *filter\_list*..... 空白で区切られた静的フィルタ番号の並び (100 個以内)
- [説明]
- インタフェースで送受信する RIP のフィルタリングを設定する。  
**ip filter** コマンドで設定されたフィルタの始点 IP アドレスが、送受信する RIP の経路情報にマッチする場合は、フィルタが *pass* であればそれを処理し、*reject* であればその経路情報だけを破棄する。
- [初期値]
- フィルタは設定されていない

#### 6.4.6 RIP で加算するホップ数の設定

- [書式]
- ```
ip interface rip hop direction hop
ip pp rip hop direction hop
ip tunnel rip hop direction hop
no ip interface rip hop direction hop
no ip pp rip hop direction hop
no ip tunnel rip hop direction hop
```

- [設定値]
- *interface* LAN インタフェース名
 - *direction*
 - *in* 受信した RIP に加算する
 - *out* 送信する RIP に加算する
 - *hop* 加算する値 (0..15)
- [説明] インタフェースで送受信する RIP に加算するホップ数を設定する。
- [初期値] 0

6.4.7 RIP2 での認証の設定

- [書式]
- ```
ip interface rip auth type type
ip pp rip auth type type
ip tunnel rip auth type type
no ip interface rip auth type [type]
no ip pp rip auth type [type]
no ip tunnel rip auth type [type]
```
- [ 設定値 ]
- *interface* ..... LAN インタフェース名
  - *type*
    - *none* ..... 認証しない
    - *text* ..... テキスト型の認証を行なう
- [ 説明 ]            RIP2 を使用する場合のインタフェースでの認証の設定をする。  
none の場合は認証なし。text の場合はテキスト型の認証を行なう。
- [ 初期値 ]            none

#### 6.4.8 RIP2 での認証キーの設定

---

- [ 書式 ]
- ```
ip interface rip auth key hex_key
ip pp rip auth key hex_key
ip tunnel rip auth key hex_key
ip interface rip auth key text text_key
ip pp rip auth key text text_key
ip tunnel rip auth key text text_key
no ip interface rip auth key
no ip pp rip auth key
no ip tunnel rip auth key
no ip interface rip auth key text
no ip pp rip auth key text
no ip tunnel rip auth key text
```
- [設定値]
- *interface* LAN インタフェース名
 - *hex_key* 十六進数の列で表現された認証キー
 - *text* 文字列を示すキーワード
 - *text_key* 文字列で表現された認証キー
- [説明] RIP2 を使用する場合のインタフェースの認証キーを設定する。
- [設定例]
- ```
ip lan1 rip auth key text testing123
ip pp rip auth key text "hello world"
ip lan2 rip auth key 01 02 ff 35 8e 49 a8 3a 5e 9d
```

#### 6.4.9 回線切断時の経路保持の設定

---

- [ 書式 ]
- ```
ip pp rip hold routing rip_bold
no ip pp rip hold routing [rip_bold]
```
- [設定値]
- *rip_bold*
 - *on* 回線が切断されても RIP による経路を保持し続ける
 - *off* 回線が切断されたら RIP による経路を破棄する

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

6.4.10 回線接続時の PP 側の RIP の動作の設定

[書式]	ip pp rip connect send rip_action no ip pp rip connect send [rip_action]
[設定値]	○ rip_action <ul style="list-style-type: none"> • interval ip pp rip connect interval コマンドで設定された時間間隔で RIP を送出する • update..... 経路情報が変わった場合にのみ RIP を送出する • none..... RIP を送出しない
[説明]	選択されている相手について回線接続時に RIP を送出する条件を設定する。
[初期値]	update
[設定例]	# ip pp rip connect interval 60 # ip pp rip connect send interval

6.4.11 回線接続時の PP 側の RIP 送出の時間間隔の設定

[書式]	ip pp rip connect interval time no ip pp rip connect interval [time]
[設定値]	○ time..... 秒数 (30..21474836)
[説明]	選択されている相手について回線接続時に RIP を送出する時間間隔を設定する。 ip pp rip send と ip pp rip receive コマンドが on、 ip pp rip connect send コマンドが interval の時に有効である。
[初期値]	30
[設定例]	# ip pp rip connect interval 60 # ip pp rip connect send interval

6.4.12 回線切断時の PP 側の RIP の動作の設定

[書式]	ip pp rip disconnect send rip_action no ip pp rip disconnect send [rip_action]
[設定値]	○ rip_action <ul style="list-style-type: none"> • none..... 回線切断時に RIP を送出しない • interval ip pp rip disconnect interval コマンドで設定された時間間隔で RIP を送出 • update..... 経路情報が変わった時にのみ RIP を送出する
[説明]	選択されている相手について回線切断時に RIP を送出する条件を設定する。
[初期値]	none
[設定例]	# ip pp rip disconnect interval 1800 # ip pp rip disconnect send interval

6.4.13 回線切断時の PP 側の RIP 送出の時間間隔の設定

[書式]	ip pp rip disconnect interval time no ip pp rip disconnect interval [time]
[設定値]	○ time..... 秒数 (30..21474836)
[説明]	選択されている相手について回線切断時に RIP を送出する時間間隔を設定する。 ip pp rip send と ip pp rip receive コマンドが on、 ip pp rip disconnect send コマンドで interval 設定に有効である。

- [初期値] 3600
- [設定例] # ip pp rip disconnect interval 1800
ip pp rip disconnect send interval

6.4.14 ネットワーク監視機能の設定

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

- [設定値]
- *num*このコマンドの識別番号 (1..100)
 - *kind*監視方式
 - icmp-echoICMP Echo を使用する
 - *interval*キープアライブの送信間隔秒数 (1..65535)
 - *count*到達性がないと判断するまでに送信する回数 (3..100)
 - *gateway*
 - IP アドレス xxx.xxx.xxx.xxx(xxx は十進数)
 - dhcp interface
 - interfaceDHCP にて与えられるデフォルトゲートウェイを使う場合の、DHCP クライアントとして動作する LAN インタフェース名
 - *option = value* 列

<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)

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

7. イーサネットフィルタの設定

7.1 フィルタ定義の設定

- [書式] **ethernet filter** *filter_num* *pass_reject* *src_mac* [*dst_mac* [*offset* *byte_list*]]
ethernet filter *filter_num* *pass_rejec* *type* [*scope*] [*offset* *byte_list*]
no ethernet filter *filter_num* [*pass_reject*...]
- [設定値] ◦ *filter_num* 静的フィルタの番号 (1..100)
 ◦ *pass_rejec*
 • *pass-log* 一致すれば通す (ログに記録する)
 • *pass-nolog* 一致すれば通す (ログに記録しない)
 • *reject-log* 一致すれば破棄する (ログに記録する)
 • *reject-nolog* 一致すれば破棄する (ログに記録しない)
 ◦ *src_mac* 始点 MAC アドレス
 • *xx:xx:xx:xx:xx:xx* (*xx* は十六進数、または *)
 • * (すべての MAC アドレスに対応)
 ◦ *dst_mac* 終点 MAC アドレス
 • 始点 MAC アドレス *src_mac* と同じ形式
 • 省略時は 1 つの * と同じ
 ◦ *type*
 • *dhcp-bind* 指定された DHCP スコープで予約設定されているホストを対象にする
 • *dhcp-not-bind* 指定された DHCP スコープで予約設定されていないホストを対象にする
 ◦ *scope* DHCP スコープ
 • 1..65535 の整数
 • DHCP スコープのリース範囲に含まれる IP アドレス
 ◦ *offset* オフセットを表す十進数 (イーサネットフレームの始点 MAC アドレスの直後をお
 とする)
 ◦ *byte_list* バイト列
 • *xx* (二桁の十六進数) あるいは * (任意のバイト) をカンマで区切った並び (16 個以内)
- [説明] イーサネットフレームのフィルタを設定する。
 本コマンドで設定されたフィルタは、**ethernet lan filter** コマンドで用いられる。
 通常型のフィルタでは、始点 MAC アドレス、終点 MAC アドレスなどで送受信するイーサネットフレーム
 にフィルタを適用する。
 dhcp-bind 型のフィルタでは、以下のイーサネットフレームにフィルタを適用する。対象とならない
 イーサネットフレームはフィルタに合致しないものとして扱う。
- 以下のいずれかに該当する、IPv4 パケットの場合
 - イーサネットタイプが IPv4 (0x0800)
 - PPPoE 環境で、イーサネットタイプが PPPoE データフレーム (0x8864)、プロトコル ID が
IPv4 (0x0800)
 - 802.1Q タグ VLAN 環境で、TPID が 802.1Q タグ (0x8100)、イーサネットタイプが
IPv4 (0x0800)
- イーサネットフレームの始点 MAC アドレスと始点 IP アドレスの組が、対象となる DHCP スコープで
 予約されているならフィルタに合致するとみなす。
- イーサネットタイプが、以下のいずれかの場合
 - ARP (0x0806)
 - RARP (0x8035)
 - PPPoE 制御パケット (0x8863)
 - MAC レイヤ制御パケット (0x8808)
- イーサネットフレームの始点 MAC アドレスが、対象となる DHCP スコープで予約されているならフィ
 ルタに合致するとみなす。
dhcp-not-bind 型のフィルタでは、以下のイーサネットフレームにフィルタを適用する。
 対象とならないイーサネットフレームはフィルタに合致しないものとして扱う。
- イーサネットタイプが IPv4 (0x0800) である場合
 イーサネットフレームの始点 IP アドレスが、対象となる DHCP スコープのリース範囲に含まれていて、
 かつ、始点 MAC アドレスが DHCP スコープで予約されていない時にフィルタに合致するとみなす。

dhcp-bind、dhcp-not-bind 型のフィルタで対象とする DHCP スコープは、SCOPE パラメータで指定する。

SCOPE パラメータとしては DHCP スコープ番号を指定することもできるし、DHCP スコープが定義されているサブネットに含まれる IP アドレスで指定することもできる。

IP アドレスで DHCP スコープを指定する場合に、複数の DHCP スコープが該当する時には、その中で最も長いネットマスク長を持つ DHCP スコープを選択する。

SCOPE パラメータを省略した場合には、フィルタが適用されるインタフェースで使用される DHCP スコープがすべて対象となる。

dhcp-bind、dhcp-not-bind 型のフィルタが DHCP リレーエージェントとして動作しているルータに設定された場合、DHCP サーバーから DHCP スコープとその DHCP スコープにおけるクライアントの予約情報を取得し、フィルタの適用時に参照する。DHCP サーバーからの DHCP スコープおよび予約情報の取得は、DHCP メッセージをリレーする際、DHCP メッセージのオプション部に予約情報を書き込んで通知することにより行なわれる。

- [ノート] LAN 分割機能を使用する場合には、ルータ内部でイーサネットタイプとして 0x8100 ~ 0x810f の値を使用しているため、それらのイーサネットフレームをフィルタして送受信できないようにすると、LAN 分割機能を使用しているポートで通信できなくなるので注意が必要である。
- dhcp-bind、dhcp-not-bind 型のフィルタでは、イーサネットフレームの始点 MAC アドレスや始点 IP アドレスを用いてフィルタの判定をするため、**ethernet lan filter** コマンドでは通常 in 方向にのみ使用することになる。out 方向の場合、始点 MAC アドレスはルータ自身の MAC アドレスになるため、DHCP の予約情報と一致することはない。
- dhcp-bind 型フィルタは、予約されているクライアントだけを通過させる、という形になるため、通常は pass 等と組み合わせて使用する。
- 一方、dhcp-not-bind 型フィルタは、予約されていないクライアントを破棄する、という形になるため、通常は reject 等と組み合わせて使用することになる。

7.2 インタフェースでのイーサネットフィルタリングの設定

- [書式] **ethernet interface filter dir list**
no ethernet interface filter dir [list]
- [設定値]
- *interface* LAN インタフェース名
 - *dir*
 - *in* LAN 側から入ってくるパケットのフィルタリング
 - *out* LAN 側に出ていくパケットのフィルタリング
 - *list* 空白で区切られた静的フィルタ番号の並び (100 個以内)
- [説明] LAN 側を通るパケットについて、**ethernet filter** コマンドによるパケットのフィルタを組み合わせて、通過するパケットの種類を制限する。
- [ノート] LAN インタフェース名に指定できるのは物理的な LAN だけであり、VLAN インタフェースは指定できない。
- [初期値] フィルタは設定されていない

8. PPP の設定

8.1 相手の名前とパスワードの設定

[書式] **pp auth username** *username password* [*myname myname mypass*] [*isdn1*] [*clid* [*isdn2*]] [*msscbcp*] [*ip_address*]

pp auth username *username password*
no pp auth username *username* [*password...*]

- [設定値]
- *username* 名前 (64 文字以内)
 - *password* パスワード (64 文字以内)
 - *myname* 自分側の設定を入力することを示すキーワード
 - *myname* 自分側のユーザ名
 - *mypass* 自分側のパスワード
 - *isdn1* 相手の ISDN アドレス
 - *clid* 発番号認証を利用することを示すキーワード
 - *isdn2* 発番号認証に用いられる ISDN アドレス
 - *msscbcp* MS コールバックを許可することを示すキーワード
 - *ip_address* 相手に割り当てる IP アドレス

[説明] 第一書式は、PP として `anonymous` が選択されたときにのみ有効である。相手の名前とパスワードを設定する。複数の設定が可能。オプションで自分側の設定も入力ができる。

双方向で認証を行なう場合には、相手のユーザ名が確定してから自分を相手に認証させるプロセスが動き始める。

これらのパラメータが設定されていない場合には、**pp auth myname** コマンドの設定が参照される。オプションで ISDN 番号が設定でき、名前と結びついたルーティングやリモート IP アドレスに対しての発信を可能にする。*isdn1* は発信用の ISDN アドレスである。*isdn1* を省略すると、この相手には発信しなくなる。

名前に '*' を与えた場合にはワイルドカードとして扱い、他の名前とマッチしなかった相手に対してその設定を使用する。

clid キーワードは発番号認証を利用することを指示する。このキーワードがない場合は発番号認証は行われない。発番号認証は *isdn2* があれば *isdn2* を用い、または *isdn2* がなければ *isdn1* を用い、一致したら認証は成功したとみなす。

msscbcp キーワードは MS コールバックを許可することを指示する。このユーザからの着信に対しては、同時に **isdn callback permit on** としてあれば MS コールバックの動作を行なう。

8.2 要求する認証タイプの設定

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

- [設定値]
- *auth*
 - *none* 何も要求しない
 - *pap* PAP による認証を要求する
 - *chap* CHAP による認証を要求する
 - *mschap* MSCHAP による認証を要求する
 - *mschap-v2* MSCHAP Version2 による認証を要求する
 - *chap-pap* CHAP もしくは PAP による認証を要求する
 - *arrive-only* 着信時にのみ PPP による認証を要求するキーワード

[説明] 選択された相手について PAP と CHAP による認証を要求するかどうかを設定する。発信時には常に適用される。`anonymous` でない着信の場合には発番号により PP が選択されてから適用される。`anonymous` での着信時には、発番号による PP の選択が失敗した場合に適用される。

chap-pap キーワードの場合には、最初 CHAP を要求し、それが相手から拒否された場合には改めて PAP を要求するよう動作する。これにより、相手が PAP または CHAP の片方しかサポートしていない場合でも容易に接続できるようになる。

arrive-only キーワードが指定された場合には、着信時のみ PPP による認証を要求するようになり、発信時には要求しない。

[初期値] none

8.3 受け入れる認証タイプの設定

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

[設定値] ○ *accept*

- pap PAP による認証を受け入れる
- chap CHAP による認証を受け入れる
- mschap MSCHAP による認証を受け入れる
- mschap-v2 MSCHAP Version2 による認証を受け入れる

[説明] 相手からの PPP 認証要求を受け入れるかどうかを設定する。発信時には常に適用される。anonymous でない着信の場合には発番号により PP が選択されてから適用される。anonymous での着信時には、発番号による PP の選択が失敗した場合に適用される。
このコマンドで認証を受け入れる設定になっても、**pp auth myname** コマンドで自分の名前とパスワードが設定されていなければ、認証を拒否する。
PP 毎のコマンドである。

[初期値] 認証を受け入れない

8.4 自分の名前とパスワードの設定

[書式] **pp auth myname** *myname password*
no pp auth myname [*myname password*]

[設定値] ○ *myname* 名前 (64 文字以内)
○ *password* パスワード (64 文字以内)

[説明] PAP または CHAP で相手に送信する自分の名前とパスワードを設定する。
PP 毎のコマンドである。

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

[書式] **pp auth multi connect prohibit** *prohibit*
no pp auth multi connect prohibit [*prohibit*]

[設定値] ○ *prohibit*

- on 禁止する
- off 禁止しない

[説明] **pp auth username** で登録した同一 *username* を持つ相手からの二重接続を禁止するか否かを設定する。

[初期値] off

8.6 LCP 関連の設定

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

[書式] **ppp lcp acfc** *acfc*
no ppp lcp acfc [*acfc*]

[設定値] ○ *acfc*

- on 用いる
- off 用いない

- [説明] 選択されている相手について [PPP, LCP] の Address and Control Field Compression オプションを用いるか否かを設定する。
- [ノート] on を設定していても相手に拒否された場合は用いない。また、このオプションを相手から要求された場合には、このコマンドの設定に関わらず常にアクセプトする。
- [初期値] off

8.6.2 Magic Number オプション使用の設定

- [書式] **ppp lcp magicnumber** *magicnumber*
no ppp lcp magicnumber [*magicnumber*]
- [設定値] ◦ *magicnumber*
 • on.....用いる
 • off.....用いない
- [説明] 選択されている相手について [PPP,LCP] の Magic Number オプションを用いるか否かを設定する。
- [ノート] on を設定していても相手に拒否された場合は用いない。
- [初期値] on

8.6.3 Maximum Receive Unit オプション使用の設定

- [書式] **ppp lcp mru** *mru* [*length*]
no ppp lcp mru [*mru* [*length*]]
- [設定値] ◦ *mru*
 • on.....用いる
 • off.....用いない
 ◦ *length*.....MRU の値 (1280..1792)
- [説明] 選択されている相手について [PPP,LCP] の Maximum Receive Unit オプションを用いるか否かと、MRU の値を設定する。
- [ノート] on を設定していても相手に拒否された場合は用いない。一般には on でよいが、このオプションをつけると接続できないルータに接続する場合には off にする。
データ圧縮を利用する設定の場合には、*length* パラメータの設定は常に 1792 として動作する。
- [初期値] mru = on
 length = 1792

8.6.4 Protocol Field Compression オプション使用の設定

- [書式] **ppp lcp pfc** *pfc*
no ppp lcp pfc [*pfc*]
- [設定値] ◦ *pfc*
 • on.....用いる
 • off.....用いない
- [説明] 選択されている相手について [PPP,LCP] の Protocol Field Compression オプションを用いるか否かを設定する。
- [ノート] on を設定していても相手に拒否された場合は用いない。また、このオプションを相手から要求された場合には、このコマンドの設定に関わらず常にアクセプトする。
- [初期値] off

8.6.5 lcp-restart パラメータの設定

- [書式] **ppp lcp restart** *time*
no ppp lcp restart [*time*]

[設定値]	◦ <i>time</i> ミリ秒 (20..10000)
[説明]	選択されている相手について [PPP,LCP] の <i>configure-request</i> 、 <i>terminate-request</i> の再送時間を設定する。
[初期値]	3000

8.6.6 lcp-max-terminate パラメータの設定

[書式]	ppp lcp maxterminate <i>count</i> no ppp lcp maxterminate [<i>count</i>]
[設定値]	◦ <i>count</i> 回数 (1..10)
[説明]	選択されている相手について [PPP,LCP] の <i>terminate-request</i> の送信回数を設定する。
[初期値]	2

8.6.7 lcp-max-configure パラメータの設定

[書式]	ppp lcp maxconfigure <i>count</i> no ppp lcp maxconfigure [<i>count</i>]
[設定値]	◦ <i>count</i> 回数 (1..10)
[説明]	選択されている相手について [PPP,LCP] の <i>configure-request</i> の送信回数を設定する。
[初期値]	10

8.6.8 lcp-max-failure パラメータの設定

[書式]	ppp lcp maxfailure <i>count</i> no ppp lcp maxfailure [<i>count</i>]
[設定値]	◦ <i>count</i> 回数 (1..10)
[説明]	選択されている相手について [PPP,LCP] の <i>configure-nak</i> の送信回数を設定する。
[初期値]	10

8.6.9 Configure-Request をすぐに送信するか否かの設定

[書式]	ppp lcp silent <i>switch</i> no ppp lcp silent
[設定値]	◦ <i>switch</i> <ul style="list-style-type: none"> • on..... PPP/LCP で、回線接続直後の <i>Configure-Request</i> の送信を、相手から <i>Configure-Request</i> を受信するまで遅らせる • off..... PPP/LCP で、回線接続直後に <i>Configure-Request</i> を送信する
[説明]	PPP/LCP で、回線接続後 <i>Configure-Request</i> をすぐに送信するか、あるいは相手から <i>Configure-Request</i> を受信するまで遅らせるかを設定する。通常は回線接続直後に <i>Configure-Request</i> を送信して構わないが、接続相手によってはこれを遅らせた方がよいものがある。
[初期値]	off

8.7 PAP 関連の設定

8.7.1 pap-restart パラメータの設定

[書式]	ppp pap restart <i>time</i> no ppp pap restart [<i>time</i>]
[設定値]	◦ <i>time</i> ミリ秒 (20..10000)

- [説明] 選択されている相手について [PPP,PAP] authenticate-request の再送時間を設定する。
- [初期値] 3000

8.7.2 pap-max-authreq パラメータの設定

- [書式] **ppp pap maxauthreq count**
no ppp pap maxauthreq [count]
- [設定値] ◦ *count*.....回数 (1..10)
- [説明] 選択されている相手について [PPP,PAP] authenticate-request の送信回数を設定する。
- [初期値] 10

8.8 CHAP 関連の設定

8.8.1 chap-restart パラメータの設定

- [書式] **ppp chap restart time**
no ppp chap restart [time]
- [設定値] ◦ *time*.....ミリ秒 (20..10000)
- [説明] 選択されている相手について [PPP,CHAP] challenge の再送時間を設定する。
- [初期値] 3000

8.8.2 chap-max-challenge パラメータの設定

- [書式] **ppp chap maxchallenge count**
no ppp chap maxchallenge [count]
- [設定値] ◦ *count*.....回数 (1..10)
- [説明] 選択されている相手について [PPP,CHAP] challenge の送信回数を設定する。
- [初期値] 10

8.9 IPCP 関連の設定

8.9.1 Van Jacobson Compressed TCP/IP 使用の設定

- [書式] **ppp ipcp vjc compression**
no ppp ipcp vjc [compression]
- [設定値] ◦ *compression*
- on.....使用する
 - off.....使用しない
- [説明] 選択されている相手について [PPP,IPCP] Van Jacobson Compressed TCP/IP を使用するか否かを設定する。
- [ノート] on を設定していても相手に拒否された場合は用いない。
- [初期値] off

8.9.2 PP 側 IP アドレスのネゴシエーションの設定

- [書式] **ppp ipcp ipaddress negotiation**
no ppp ipcp ipaddress [negotiation]

- [設定値] ◦ *negotiation*
- on.....ネゴシエーションする
 - off.....ネゴシエーションしない
- [説明] 選択されている相手について PP 側 IP アドレスのネゴシエーションをするか否かを設定する。
- [初期値] off

8.9.3 ipcp-restart パラメータの設定

- [書式] **ppp ipcp restart time**
no ppp ipcp restart [time]
- [設定値] ◦ *time*..... ミリ秒 (20..10000)
- [説明] 選択されている相手について [PPP,IPCP] の configure-request、 terminate-request の再送時間を設定する。
- [初期値] 3000

8.9.4 ipcp-max-terminate パラメータの設定

- [書式] **ppp ipcp maxterminate count**
no ppp ipcp maxterminate [count]
- [設定値] ◦ *count*..... 回数 (1..10)
- [説明] 選択されている相手について [PPP,IPCP] の terminate-request の送信回数を設定する。
- [初期値] 2

8.9.5 ipcp-max-configure パラメータの設定

- [書式] **ppp ipcp maxconfigure count**
no ppp ipcp maxconfigure [count]
- [設定値] ◦ *count*..... 回数 (1..10)
- [説明] 選択されている相手について [PPP,IPCP] の configure-request の送信回数を設定する。
- [初期値] 10

8.9.6 ipcp-max-failure パラメータの設定

- [書式] **ppp ipcp maxfailure count**
no ppp ipcp maxfailure [count]
- [設定値] ◦ *count*..... 回数 (1..10)
- [説明] 選択されている相手について [PPP,IPCP] の configure-nak の送信回数を設定する。
- [初期値] 10

8.9.7 WINS サーバーの IP アドレスの設定

- [書式] **wins server server1 [server2]**
no wins server [server1 [server2]]
- [設定値] ◦ *server1, server2*..... IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))
- [説明] WINS (Windows Internet Name Service) サーバーの IP アドレスを設定する。
- [ノート] IPCP の MS 拡張オプションおよび DHCP でクライアントに渡すための WINS サーバーの IP アドレスを設定する。ルータはこのサーバーに対し WINS クライアントとしての動作は一切行なわない。

[初期値] WINS サーバーは設定されていない

8.9.8 IPCP の MS 拡張オプションを使うか否かの設定

[書式] **ppp ipcp msex** *msex*
no ppp ipcp msex [*msex*]

[設定値] ◦ *msex*
 • on..... 使用する
 • off 使用しない

[説明] 選択されている相手について、[PPP,IPCP] の MS 拡張オプションを使うか否かを設定する。
 on の場合は、DNS サーバーの IP アドレスと WINS (Windows Internet Name Service) サーバーの IP アドレスを、接続した相手である Windows マシンに渡すことができる。渡すための DNS サーバーや WINS サーバーの IP アドレスはそれぞれ、**dns server** コマンドおよび **wins server** コマンドで設定する。
 off の場合は、DNS サーバーや WINS サーバーのアドレスを渡されても受け取らない。

[初期値] off

8.9.9 ホスト経路が存在する相手側 IP アドレスを受け入れるか否かの設定

[書式] **ppp ipcp remote address check** *sw*
no ppp ipcp remote address check [*sw*]

[設定値] ◦ *sw*
 • on..... 通知された相手の PP 側 IP アドレスを拒否する
 • off 通知された相手の PP 側 IP アドレスを受け入れる

[説明] 他の PP 経由のホスト経路が既に存在している IP アドレスを PP 接続時に相手側 IP アドレスとして通知されたときに、その IP アドレスを受け入れるか否かを設定する。

[初期値] on

8.10 MSCBCP 関連の設定

8.10.1 mscbcpr-start パラメータの設定

[書式] **ppp mscbcpr restart** *time*
no ppp mscbcpr restart [*time*]

[設定値] ◦ *time*..... ミリ秒 (20..10000)

[説明] 選択されている相手について [PPP, MSCBCP] の Request/Response の再送時間を設定する。

[初期値] 1000

8.10.2 mscbcpr-maxretry パラメータの設定

[書式] **ppp mscbcpr maxretry** *count*
no ppp mscbcpr maxretry [*count*]

[設定値] ◦ *count*..... 回数 (1..30)

[説明] 選択されている相手について [PPP, MSCBCP] の request/Response の再送回数を設定する。

[初期値] 30

8.11 CCP 関連の設定

8.11.1 全パケットの圧縮タイプの設定

[書式] **ppp ccp type** *type*
no ppp ccp type [*type*]

[設定値] ○ *type*

- stac0 Stac LZS で圧縮する
- stac Stac LZS で圧縮する
- cstac Stac LZS で圧縮する (接続相手が Cisco ルータの場合)
- mppe-40 40bit MPPE で暗号化する
- mppe-128 128bit MPPE で暗号化する
- mppe-any 40bit, 128bit MPPE いずれかの暗号化を行なう
- none 圧縮しない

[説明] 選択されている相手について [PPP,CCP] 圧縮方式を選択する。

[ノート] Van Jacobson Compressed TCP/IP との併用も可能である。
type に stac を指定した時、回線状態が悪い場合や、高負荷で、パケットロスが頻繁に起きると、通信が正常に行えなくなることがある。このような場合、自動的に「圧縮なし」になる。その後、リスタートまで「圧縮なし」のままである。このような状況が改善できない時は、stac0 を指定すればよい。ただしその時は接続先も stac0 に対応していなければならない。stac0 は stac よりも圧縮効率は落ちる。

接続相手が Cisco ルータの場合に stac を適用する通信できないことがある。そのような場合には、設定を cstac に変更すると通信が可能になることがある。

mppe-40, mppe-128, mppe-any の場合には 1 パケット毎に鍵交換される。MPPE は Microsoft Point-To-Point Encryption (Protocol) の略で CCP を拡張したものであり、暗号アルゴリズムとして RC4 を採用し、鍵長 40bit または 128bit を使う。暗号鍵生成のために認証プロトコルの MS-CHAP または MS-CHAPv2 と合わせて設定する。

[初期値] stac

8.11.2 ccp-restart パラメータの設定

[書式] **ppp ccp restart** *time*
no ppp ccp restart [*time*]

[設定値] ○ *time* ミリ秒 (20..10000)

[説明] 選択されている相手について [PPP, CCP] の configure-request、terminate-request の再送時間を設定する。

[初期値] 3000

8.11.3 ccp-max-terminate パラメータの設定

[書式] **ppp ccp maxterminate** *count*
no ppp ccp maxterminate [*count*]

[設定値] ○ *count* 回数 (1..10)

[説明] 選択されている相手について [PPP, CCP] の terminate-request の送信回数を設定する。

[初期値] 2

8.11.4 ccp-max-configure パラメータの設定

[書式] **ppp ccp maxconfigure** *count*
no ppp ccp maxconfigure [*count*]

[設定値] ○ *count* 回数 (1..10)

[説明] 選択されている相手について [PPP, CCP] の configure-request の送信回数を設定する。

[初期値] 10

8.11.5 ccp-max-failure パラメータの設定

[書式] **ppp ccp maxfailure count**
no ppp ccp maxfailure [count]

[設定値] ◦ *count*.....回数 (1..10)

[説明] 選択されている相手について [PPP, CCP] の configure-nak の送信回数を設定する。

[初期値] 10

8.12 IPV6CP 関連の設定

8.12.1 IPV6CP を使用するか否かの設定

[書式] **ppp ipv6cp use use**
no ppp ipv6cp use [use]

[設定値] ◦ *use*
 • on.....使用する
 • off.....使用しない

[説明] 選択されている相手について IPV6CP を使用するか否かを選択する。

[初期値] on

8.13 MP 関連の設定

8.13.1 MP を使用するか否かの設定

[書式] **ppp mp use use**
no ppp mp use [use]

[設定値] ◦ *use*
 • on.....使用する
 • off.....使用しない

[説明] 選択されている相手について MP を使用するか否かを選択する。
 on に設定していても、LCP の段階で相手とのネゴシエーションが成立しなければ MP を使わずに通信する。

[初期値] off

8.13.2 MP の制御方法の設定

[書式] **ppp mp control type**
no ppp mp control [type]

[設定値] ◦ *type*
 • arrive自分が 1B 目の着信側の場合に MP を制御する
 • both自分が 1B 目の発信着信いずれの場合でも MP を制御する
 • call自分が 1B 目の発信側の場合に MP を制御する

[説明] 選択されている相手について MP を制御して 2B 目の発信 / 切断を行なう場合を設定する。通常は初期値のように自分が 1B 目の発信側の場合だけ制御するようにしておく。

[初期値] call

8.13.3 MP のための負荷閾値の設定

[書式] **ppp mp load threshold call_load call_count disc_load disc_count**
no ppp mp load threshold [call_load call_count disc_load disc_count]

- [設定値] ◦ *call_load*..... 発信負荷閾値 %(1..100)
 ◦ *call_count*..... 回数 (1..100)
 ◦ *disc_load*..... 切断負荷閾値 %(0..50)
 ◦ *disc_count*..... 回数 (1..100)
- [説明] 選択されている相手について [PPP, MP] の 2B 目を発信したり切断したりする場合のデータ転送負荷の閾値を設定する。
 負荷は回線速度に対する % で評価し、送受信で大きい方の値を採用する。*call_load* を超える負荷が *call_count* 回繰り返されたら 2B 目の発信を行なう。逆に *disc_load* を下回る負荷が *disc_count* 回繰り返されたら 2B 目を切断する。
- [初期値] *call_load* = 70
 call_count = 1
 disc_load = 30
 disc_count = 2

8.13.4 MP の最大リンク数の設定

- [書式] **ppp mp maxlink** *number*
 no ppp mp maxlink [*number*]
- [設定値] ◦ *number*..... リンク数
- [説明] 選択されている相手について [PPP, MP] の最大リンク数を設定する。リンク数の最大値は、使用モデルで使用できる ISDN Bch の数までとなる。
- [初期値] 2

8.13.5 MP の最小リンク数の設定

- [書式] **ppp mp minlink** *number*
 no ppp mp minlink [*number*]
- [設定値] ◦ *number*..... リンク数
- [説明] 選択されている相手について [PPP,MP] の最小リンク数を設定する。
- [初期値] 1

8.13.6 MP のための負荷計測間隔の設定

- [書式] **ppp mp timer** *time*
 no ppp mp timer [*time*]
- [設定値] ◦ *time*..... 秒数 (1..21474836)
- [説明] 選択されている相手について [PPP, MP] のための負荷計測間隔を設定する。
 単位は秒。負荷計測だけでなく、すべての MP の動作はこのコマンドで設定した間隔で行われる。
- [初期値] 10

8.13.7 MP のパケットを分割するか否かの設定

- [書式] **ppp mp divide** *divide*
 no ppp mp divide [*divide*]
- [設定値] ◦ *divide*
 • on..... 分割する
 • off..... 分割しない

- [説明] 選択されている相手について [PPP, MP] に対して、MP パケットの送信時にパケットを分割するかかを設定する。
分割するとうまく接続できない相手に対してだけ off にする。
分割しないように設定した場合、特に TCP の転送効率に悪影響が出る可能性がある。
64 バイト以下のパケットは本コマンドの設定に関わらず分割されない。
- [初期値] on

8.14 PPPoE 関連の設定

8.14.1 PPPoE で使用する LAN インタフェースの指定

- [書式] **pppoe use interface**
no pppoe use
- [設定値] ◦ *interface* LAN インタフェース名
- [説明] 選択されている相手に対して、PPPoE で使用する LAN インタフェースを指定する。設定がない場合は、PPPoE は使われない。
- [初期値] PPPoE を使用しない

8.14.2 アクセスコンセントレータ名の設定

- [書式] **pppoe access concentrator name**
no pppoe access concentrator
- [設定値] ◦ *name* アクセスコンセントレータの名前を表す文字列
- [説明] 選択されている相手について PPPoE で接続するアクセスコンセントレータの名前を設定する。接続できるアクセスコンセントレータが複数ある場合に、どのアクセスコンセントレータに接続するのかを指定するために使用する。

8.14.3 セッションの自動接続の設定

- [書式] **pppoe auto connect switch**
no pppoe auto connect
- [設定値] ◦ *switch*
- on 自動接続する
 - off 自動接続しない
- [説明] 選択されている相手に対して、PPPoE のセッションを自動で接続するかかを設定する。
- [初期値] on

8.14.4 セッションの自動切断の設定

- [書式] **pppoe auto disconnect switch**
no pppoe auto disconnect
- [設定値] ◦ *switch*
- on 自動切断する
 - off 自動切断しない
- [説明] 選択されている相手に対して、PPPoE のセッションを自動で切断するかかを設定する。
- [初期値] on

8.14.5 PADI パケットの最大再送回数の設定

- [書式] **pppoe padi maxretry count**
no pppoe padi maxretry

- [設定値] ◦ *count*.....回数 (1..10)
- [説明] PPPoE プロトコルにおける PADI パケットの最大再送回数を設定する。
- [初期値] 5

8.14.6 PADI パケットの再送時間の設定

- [書式] **pppoe padi restart time**
 no pppoe padi restart
- [設定値] ◦ *time*..... ミリ秒 (20..10000)
- [説明] PPPoE プロトコルにおける PADI パケットの再送時間を設定する。
- [初期値] 3000

8.14.7 PADR パケットの最大再送回数の設定

- [書式] **pppoe padr maxretry times**
 no pppoe padr maxretry
- [設定値] ◦ *count*.....回数 (1..10)
- [説明] PPPoE プロトコルにおける PADR パケットの最大再送回数を設定する。
- [初期値] 5

8.14.8 PADR パケットの再送時間の設定

- [書式] **pppoe padr restart time**
 no pppoe padr restart
- [設定値] ◦ *time*..... ミリ秒 (20..10000)
- [説明] PPPoE プロトコルにおける PADR パケットの再送時間を設定する。
- [初期値] 3000

8.14.9 PPPoE セッションの切断タイマの設定

- [書式] **pppoe disconnect time time**
 no pppoe disconnect time
- [設定値] ◦ *time*
 • 秒数 (1..21474836)
 • off タイマを設定しない
- [説明] 選択されている相手に対して、タイムアウトにより PPPoE セッションを自動切断する時間を設定する。
- [ノート] LCP と NCP パケットは監視対象外。
- [初期値] off

8.14.10 TCP パケットの MSS の制限の有無とサイズの指定

- [書式] **pppoe tcp mss limit length**
 pppoe tcp mss limit
- [設定値] ◦ *length*
 • データ長 (1240..1452)
 • auto..... MSS を MTU の値に応じて制限する
 • off MSS を制限しない

- [説明] PPPoE セッション上で TCP パケットの MSS(Maximum Segment Size) を制限するかどうかを設定する。
- [ノート] このコマンドと **ip interface tcp mss limit** コマンドの両方が有効な場合は、MSS はどちらかより小さな方の値に制限される。
- [初期値] auto

8.14.11 サービス名の指定

- [書式] **pppoe service-name name**
no pppoe service-name
- [設定値] ◦ *name* サービス名を表す文字列
- [説明] 選択されている相手について PPPoE で要求するサービス名を設定する。
接続できるアクセスコンセントレータが複数ある場合に、要求するサービスを提供することが可能なアクセスコンセントレータを選択して接続するために使用する。
- [ノート] フレッツ・ADSL に接続する場合には、このコマンドでサービス名を指定してはいけない。
- [初期値] 指定なし

8.14.12 認証失敗の最大回数を設定する

- [書式] **pppoe call prohibit auth-error count count**
no pppoe call prohibit auth-error count
- [設定値] ◦ *count*
- 回数 (1..21474836)
 - off 発信制限をかけない
- [説明] 選択されている相手に対し、認証が失敗できる最大回数を設定する。
なお、以下のコマンドを実行すると、再び発呼が可能となる。
pp auth accept / pp auth request / pp auth myname / pp auth username / no pp auth myname / no pp auth username
- [初期値] 15

9. DHCP の設定

本製品は DHCP¹ 機能として、DHCP サーバー機能、DHCP リレーエージェント機能、DHCP クライアント機能を実装しています。DHCP 機能の利用により、基本的なネットワーク環境の自動設定を実現します。

DHCP クライアント機能は Windows 等で実装されており、これらと本製品の DHCP サーバー機能、DHCP リレーエージェント機能を組み合わせることにより DHCP クライアントの基本的なネットワーク環境の自動設定を実現します。

ルータが DHCP サーバーとして機能するか DHCP リレーエージェントとして機能するか、どちらとしても機能させないかは **dhcp service** コマンドにより設定します。現在の設定は、**show status dhcp** コマンドにより知ることができます。

DHCP サーバー機能は、DHCP クライアントからのコンフィギュレーション要求を受けて IP アドレスの割り当て（リース）や、ネットマスク、DNS サーバーの情報等を提供します。

割り当てる IP アドレスの範囲とリース期間は **dhcp scope** コマンドにより設定されたものが使用されます。

IP アドレスの範囲は複数の設定が可能であり、それぞれの範囲を DHCP スコープ番号で管理します。DHCP クライアントからの設定要求があると DHCP サーバーは DHCP スコープの中で未割り当ての IP アドレスを自動的に通知します。なお、特定の DHCP クライアントに特定の IP アドレスを固定的にリースする場合には、**dhcp scope** コマンドで定義したスコープ番号を用いて **dhcp scope bind** コマンドで予約します。予約の解除は **no dhcp scope bind** コマンドで行ないます。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** 及び **maxexpire** キーワードのパラメータで指定します。リース状況は **show status dhcp** コマンドにより知ることができます。DHCP クライアントに通知する DNS サーバーの IP アドレス情報は、**dns server** コマンドで設定されたものを通知します。

DHCP リレーエージェント機能は、ローカルセグメントの DHCP クライアントからの要求を、予め設定されたリモートのネットワークセグメントにある DHCP サーバーへ転送します。リモートセグメントの DHCP サーバーは **dhcp relay server** コマンドで設定します。DHCP サーバーが複数ある場合には、**dhcp relay select** コマンドにより選択方式を指定することができます。

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

9.1 DHCP サーバー・リレーエージェント機能

9.1.1 DHCP の動作の設定

【書式】	dhcp service type no dhcp service [type]
【設定値】	○ <i>type</i> <ul style="list-style-type: none"> • server..... DHCP サーバーとして機能させる • relay DHCP リレーエージェントとして機能させる
【説明】	DHCP に関する機能を設定する。 DHCP リレーエージェント機能使用時には、NAT 機能を使用することはできない。
【初期値】	DHCP サービスは機能しない

1. Dynamic Host Configuration Protocol; RFC1541, RFC2131

9.1.2 RFC2131 対応動作の設定

[書式]	dhcp server rfc2131 compliant comp dhcp server rfc2131 compliant [except] <i>function</i> [<i>function..</i>] no dhcp server rfc2131 compliant ◦ <i>comp</i> • on RFC2131 準拠 • off RFC1541 準拠 ◦ <i>except</i> 指定した機能以外が RFC2131 対応となることを示すキーワード ◦ <i>function</i> • broadcast-nak DHCPNAK をブロードキャストで送る • none-domain-null ... ドメイン名の最後に NULL 文字を付加しない • remain-silent リース情報を持たないクライアントからの DHCPREQUEST を無視する • reply-ack DHCPNAK の代わりに許容値を格納した DHCPACK を返す • use-clientid クライアントの識別に Client-Identifier オプションを優先する
[説明]	DHCP サーバーの動作を指定する。on の場合には RFC2131 準拠となる。off の場合には、RFC1541 準拠の動作となる。 また RFC1541 をベースとして RFC2131 記述の個別機能のみを対応させる場合には以下のパラメータで指定する。これらのパラメータはスペースで区切り複数指定できる。except キーワードを指示すると、指定したパラメータ以外の機能が RFC2131 対応となる。
	<ul style="list-style-type: none"> • 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。
[初期値]	on

9.1.3 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]	◦ <i>check1</i> LAN 内を対象とするチェックの確認用の待ち時間 <ul style="list-style-type: none"> • ミリ秒 (1..1000) • off LAN 内を対象とするチェックを行なわない ◦ <i>check2</i> 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の待ち時間 <ul style="list-style-type: none"> • ミリ秒 (1..3000) • off LAN 外 (DHCP リレーエージェント経由) を対象とするチェックを行なわない
[説明]	DHCP サーバーとして機能する場合、IP アドレスを DHCP クライアントにリースする直前に、その IP アドレスを使っているホストが他にいないことをチェックするか否かを設定する。
[ノート]	LAN 内のスコープに対しては ARP を、DHCP リレーエージェント経由のスコープに対しては PING を使ってチェックする。
[初期値]	check1 = 100 check2 = 500

9.1.4 DHCP スコープの定義

- [書式] **dhcp scope** *scope_num ip_address-ip_address/netmask* [except *ex_ip ...*] [gateway *gw_ip*] [expire *time*] [maxexpire *time*]
no dhcp scope *scope_num [ip_address-ip_address/netmask* [except *ex_ip ...*] [gateway *gw_ip*] [expire *time*] [maxexpire *time*]]
- [設定値]
- *scope_num* スコープ番号 (1..65535)
 - *ip_address-ip_address* .. 対象となるサブネットで割り当てる IP アドレスの範囲
 - *netmask*
 - xxx.xxx.xxx.xxx (xxx は十進数)
 - 0x に続く十六進数
 - マスクビット数
 - *ex_ip* IP アドレス指定範囲の中で除外する IP アドレス
 - *gw_ip* IP アドレス対象ネットワークのゲートウェイの IP アドレス
 - *time*
 - 分 (1..21474836)
 - 時間:分
 - infinity 無期限リース
- [説明] DHCP サーバーとして割り当てる IP アドレスのスコープを設定する。
 複数の除外 IP アドレスを空白で区切って複数指定できる。
 また、"IP アドレス -IP アドレス" と指定することで除外 IP アドレス範囲を指定できる。
 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。
- [初期値] expire *time* = 72:00
 maxexpire *time* = 72:00

9.1.5 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 [[type] id]*
no dhcp scope bind *scope_num ip_address mac_address*
- [設定値]
- *scope_num* スコープ番号 (1..65535)
 - *ip_address* 予約する IP アドレス
 - xxx.xxx.xxx.xxx (xxx は十進数)
 - * (リースする IP アドレスを指定しない)
 - *type* Client-Identifier オプションの *type* フィールドを決定する
 - text 0x00
 - ethernet 0x01
 - *id*
 - *type* が ethernet の場合 MAC アドレス
 - *type* が text の場合 文字列
 - *type* が省略された場合 2 桁十六進数の列で先頭は *type* フィールド
 - *mac_address* 予約クライアントの MAC アドレス
 - xx:xx:xx:xx:xx:xx (xx は十六進数)
 - *ipcp* IPCP でリモート側に与えることを示すキーワード
- [説明] IP アドレスをリースする 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 * 指定としてクライアントだけを指定することもできる。
 この形式を削除する場合はクライアント識別子を省略できない。

[ノート]

IP アドレスは、*scope_num* パラメータで指定された DHCP スコープ範囲内でなければならない。1 つの DHCP スコープ内では、1 つの MAC アドレスに複数の IP アドレスを設定することはできない。他の DHCP クライアントにリース中の IP アドレスを予約設定した場合、リース終了後にその IP アドレスの割り当てが行われる。

dhcp scope コマンド、あるいは **no 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 チャネルの数に限られる。また、IPCP で与えるアドレスは LAN 側のスコープから選択される。

コマンドの第 1 書式を使う場合は、あらかじめ **dhcp server rfc2131 compliant on** あるいは **use-clientid** 機能を使用するよう設定されていなければならない。また **dhcp server rfc2131 compliant off** あるいは **use-clientid** 機能が使用されないよう設定された時点で、コマンドの第 2 書式によるもの以外の予約は消去される。

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

コマンドの第 2 書式による MAC アドレスでの予約は、クライアントの識別に DHCP パケットの *chaddr* フィールドを用いる。この形の予約機能は、ルータの設定が **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は動作しない。

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** 機能ありの場合

dhcp scope bind での指定方法	A. B. C.	D.
クライアントの識別に用いる情報	Client-Identifier オプション	chaddr(※ 1)

- ※ 1 Client-Identifier オプションが存在しない場合に限り、Client-Identifier オプションが存在する場合にはこの設定は無視される

dhcp server rfc2131 compliant on あるいは **use-clientid** 機能ありでアドレスをリースする場合、DHCP サーバーは *chaddr* に優先して Client-Identifier オプションを使用する。そのため、この場合の **show status dhcp** コマンド実行でクライアントの識別子を確認することで、クライアントが Client-Identifier オプションを使っているか否かを判別することも可能である。

すなわち、リースしているクライアントとして MAC アドレスが表示されていれば Client-Identifier オプションは使用されておらず、十六進文字列あるいは文字列でクライアントが表示されていれば、Client-Identifier オプションが使われている。この場合、Client-Identifier オプションを使うクライアントへの予約は、ここで表示される十六進文字列あるいは文字列を使用する。

2. **dhcp server rfc2131 compliant off** あるいは **use-clientid** 機能なしの場合

dhcp scope bind での指定方法	(※ 2)	D.
クライアントの識別に用いる情報	(※ 3)	chaddr

- ※ 2 他の方法での指定は出来ない
 ※ 3 Client-Identifier オプションは無視される

なお、クライアントとの相互動作に関して下記の留意点がある。

- 個々の機能を単独で用いるとクライアント側の思わぬ動作を招く可能性があるため、**dhcp server rfc2131 compliant** on あるいは **dhcp server rfc2131 compliant** off で使用することを推奨する。
- ルータの再起動、スコープの再設定などでリース情報が消去されている場合、アドレス延長要求時、あるいはリース期間内のクライアントの再起動時、クライアントの使用する IP アドレスが変わることがある。
- これを防ぐために **dhcp server rfc2131 compliant** on (あるいは remain-silent 機能) が有効である場合がある。この設定では、本製品がリース情報を持たないクライアントからの DHCPREQUEST に DHCPNAK を返さず無視する。
- この結果、リース期限満了時にクライアントが出す DHCPDISCOVER に Requested IP Address オプションが含まれていれば、そのクライアントには引き続き同じ IP アドレスをリースできる。

9.1.6 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_num** [except] [idx [...]]

[設定値] ◦ *scope_num* スコープ番号 (1-65535)

◦ *idx*

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

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

[ノート] 以下の変換規則で IP アドレス割り当て情報が予約設定に変換される。

IP アドレス割り当て情報のクライアント識別種別 (show status dhcp で表示される名称)	クライアント識別情報 例	予約設定情報 例
クライアントイーサネットアドレス	00:a0:de:01:02:03	ethernet 00:a0:de:01:02:03 ※ 1 00:a0:de:01:02:03 ※ 2
クライアント ID	(01) 00 a0 de 01 02 03	ethernet 00:a0:de:01:02:03
	(01) 00 a0 de 01 02 03 04	01 00 a0 de 01 02 03 04
	(00) 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、手動で行なう必要がある。

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

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

9.1.7 DHCP オプションの設定

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

[設定値]

- *scope_num* スコープ番号 (1..65535)
- *option* オプション番号 (1..49,64..76,128..254) またはニーモニック
 - 主なニーモニック

router	3
dns	6
hostname	12
domain	15
wins_server	44

- *value* オプション値

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

1 オクテット整数	0..255
2 オクテット整数	0..65535
2 オクテット数の配列	2 オクテット整数をコンマ (,) で並べたもの
4 オクテット整数	0..4294967295
IP アドレス	IP アドレス
IP アドレスの配列	IP アドレスをコンマ (,) で並べたもの
文字列	文字列
スイッチ	"on", "off", "1", "0" のいずれか
バイナリ	2 桁十六進数をコンマ (,) で並べたもの

[説明]

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

[ノート]

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

9.1.8 DHCP アドレス割り当て動作の設定

[書式]

dhcp scope lease type scope_num type [fallback=fallback_scope_num]
no dhcp scope lease type scope_num [type...]

[設定値]

- *scope_num*, *fallback_scope_num* スコープ番号 (1-65535)
- *type* 割り当ての動作
 - **bind-priority** 予約情報を優先して割り当てる
 - **bind-only** 予約情報だけに制限して割り当てる

[説明]

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

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

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

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

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

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

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

- (3a) フォールバックスコープに対する **dhcp scope lease type** コマンドの設定が `bind-priority` になっている時には、クライアントにはフォールバックスコープに空きアドレスがある限りそれを割り当てる。
- (3b) フォールバックスコープに対する **dhcp scope lease type** コマンドの設定が `bind-only` になっている時には、クライアントには IP アドレスは割り当てられない。

いずれの場合も、リース期間は各 DHCP スコープの定義に従う。

[初期値] `bind-priority`

9.1.9 DHCP リース情報の手動追加

[書式] **dhcp manual lease** *ip_address* [*type*] *id*
dhcp manual lease *ip_address* *mac_address*
dhcp manual lease *ip_address* *ipcp*

[設定値] ◦ *ip_address* リースする IP アドレス
 ◦ *type* Client-Identifier オプションの *type* フィールドを決定する
 • *text* 0x00
 • *ethernet* 0x01
 ◦ *id*
 • *type* が *text* の場合 文字列
 • *type* が *ethernet* の場合 MAC アドレス
 • *type* が省略された場合 2 桁十六進数の列で先頭は *type* フィールド
 ◦ *mac_address* XX:XX:XX:XX:XX:XX (XX は十六進数) DHCP クライアントの MAC アドレス
 ◦ *ipcp* IPCP でリモート側に与えたものとするキーワード

[説明] 手動で、特定 IP アドレスのリース情報を追加する。

[ノート] 本コマンドは自動で行われる DHCP のアドレス配布に影響を与えるため、意図して特定の IP アドレスのリース情報を追加したい場合を除いて、使用するべきではない。

9.1.10 DHCP リース情報の手動削除

[書式] **dhcp manual release** *ip_address*

[設定値] ◦ *ip_address* 解放する IP アドレス

[説明] 手動で、特定 IP アドレスのリース情報を削除する。

[ノート] 本コマンドは自動で行われる DHCP のアドレス配布に影響を与えるため、意図して特定の IP アドレスのリース情報を削除したい場合を除いて、使用するべきではない。

9.1.11 DHCP サーバーの指定の設定

[書式] **dhcp relay server** *host1* [*host2* [*host3* [*host4*]]]
no dhcp relay server

[設定値] ◦ *host1..host4* DHCP サーバーの IP アドレス

[説明] DHCP BOOTREQUEST パケットを中継するサーバーを最大 4 つまで設定する。サーバーが複数指定された場合は、BOOTREQUEST パケットを複製してすべてのサーバーに中継するか、あるいは 1 つだけサーバーを選択して中継するかは **dhcp relay select** コマンドの設定で決定される。

9.1.12 DHCP サーバーの選択方法の設定

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

- [設定値] ◦ *type*
- *hash* Hash 関数を利用して一つだけサーバーを選択する
 - *all* すべてのサーバーを選択する
- [説明] **dhcp relay server** コマンドで設定された複数のサーバーの取り扱いを設定する。
hash が指定された場合は、Hash 関数を利用して一つだけサーバーが選択されてパケットが中継される。この Hash 関数は、DHCP メッセージの *chaddr* フィールドを引数とするので、同一の DHCP クライアントに対しては常に同じサーバーが選択されるはずである。*all* が指定された場合は、パケットはすべてのサーバーに対し複写中継される。
- [初期値] *hash*

9.1.13 DHCP BOOTREQUEST パケットの中継基準の設定

- [書式] **dhcp relay threshold *time***
no dhcp relay threshold [*time*]
- [設定値] ◦ *time* 秒数 (0..65535)
- [説明] DHCP BOOTREQUEST パケットの *secs* フィールドとこのコマンドによる秒数を比較し、設定値より小さな *secs* フィールドを持つ DHCP BOOTREQUEST パケットはサーバーに中継しないようにする。これにより、同一 LAN 上に別の DHCP サーバーがあるにも関わらず遠隔地の DHCP サーバーにパケットを中継してしまうのを避けることができる。
- [初期値] 0

9.2 DHCP クライアント機能

9.2.1 要求する IP アドレスリース期間の設定

- [書式] **ip interface dhcp lease time *time***
no ip interface dhcp lease time [*time*]
- [設定値] ◦ *interface* LAN インタフェース名
- *time*
- 分数 (1..21474836)
 - 時間 : 分
- [説明] DHCP クライアントが要求する IP アドレスのリース期間を設定する。
- [ノート] リース期間の要求が受け入れられなかった場合、要求しなかった場合は、DHCP サーバーからのリース期間を利用する。
- [初期値] リース期間を要求しない

9.2.2 IP アドレス取得要求の再送回数と間隔の設定

- [書式] **ip interface dhcp retry *retry interval***
no ip interface dhcp retry [*retry interval*]
- [設定値] ◦ *interface* LAN インタフェース名
- *retry*
- 回数 (1..100)
 - *infinity* 無制限
- *interval* 秒数 (1..100)
- [説明] IP アドレスの取得に失敗したときにリトライする回数とその間隔を設定する。
- [初期値] *retry* = *infinity*
interval = 5

9.2.3 DHCP クライアント ID オプションの設定

- [書式]
- ```

dhcp client client-identifier interface primary [type type] id
dhcp client client-identifier interface secondary [type type] id
dhcp client client-identifier pp peer_num [type type] id
dhcp client client-identifier pool pool_num [type type] id
no dhcp client client-identifier interface primary
no dhcp client client-identifier interface secondary
no dhcp client client-identifier pp peer_num
no dhcp client client-identifier pool pool_num

```
- [ 設定値 ]
- *interface* ..... LAN インタフェース名
  - *type* ..... ID オプションの *type* フィールドの値を設定することを示すキーワード
  - *type* ..... ID オプションの *type* フィールドの値
  - *id*
    - ASCII 文字列で表した ID
    - 2 桁の十六進数列で表した ID
  - *peer\_num*
    - 相手先情報番号
    - anonymous
  - *pool\_num* ..... **ip pp remote address pool dhcpc** コマンドで取得する IP アドレスの番号。例えば、**ip pp remote address pool dhcpc** コマンドで IP アドレスを 2 個取得できる機種で、*pool\_num* に "1" または "2" を設定することで、それぞれのクライアント ID オプションに任意の ID を付けることができる。(1..**ip pp remote address pool dhcpc** コマンドで取得できる IP アドレスの最大数)
- [ 説明 ] DHCP クライアント ID オプションの *type* フィールドと ID を設定する。
- [ 初期値 ] *type* = 1

### 9.2.4 DHCP クライアントのホスト名の設定

- [ 書式 ]
- ```

dhcp client hostname interface primary host
dhcp client hostname interface secondary host
dhcp client hostname pp peer_num host
dhcp client hostname pool pool_num host
no dhcp client hostname interface primary [host]
no dhcp client hostname interface secondary [host]
no dhcp client hostname pp peer_num [host]
no dhcp client hostname pool pool_num [host]

```
- [設定値]
- *interface* LAN インタフェース名
 - *peer_num*
 - 相手先情報番号
 - anonymous
 - *pool_num* **ip pp remote address pool dhcpc** コマンドで取得する IP アドレスの番号。例えば、**ip pp remote address pool dhcpc** コマンドで IP アドレスを 2 個取得できる機種で、*pool_num* に "1" または "2" を設定することで、それぞれのクライアント ID オプションに任意の ID を付けることができる。(1..**ip pp remote address pool dhcpc** コマンドで取得できる IP アドレスの最大数)
 - *host* DHCP クライアントのホスト名
- [説明] DHCP クライアントのホスト名を設定する。
- [初期値] DHCP クライアントのホスト名は設定されていない

9.2.5 DHCP クライアントが DHCP サーバーへ送るメッセージ中に格納するオプションの設定

- [書式]
- ```

dhcp client option interface primary option=value
dhcp client option interface secondary option=value
dhcp client option pp peer_num option=value
dhcp client option pool pool_num option=value
no dhcp client option interface primary [option=value]
no dhcp client option interface secondary [option=value]
no dhcp client option pp peer_num [option=value]
no dhcp client option pool pool_num [option=value]

```
- [ 設定値 ]
- *interface* ..... LAN インタフェース名
  - *option* ..... オプション番号 (十進数)
  - *value* ..... 格納するオプション値 (十六進数、"." で区切って複数指定可能)  
なおオプション長情報は入力の必要はない
  - *peer\_num*
    - 相手先情報番号
    - anonymous
  - *pool\_num* ..... **ip pp remote address pool dhcpc** コマンドで取得する IP アドレスの番号。例えば、**ip pp remote address pool dhcpc** コマンドで IP アドレスを 2 個取得できる機種で、*pool\_num* に "1" または "2" を設定することで、それぞれのクライアント ID オプションに任意の ID を付けることができる。(1.. **ip pp remote address pool dhcpc** コマンドで取得できる IP アドレスの最大数)
- [ 説明 ] DHCP クライアントが DHCP サーバーへ送るメッセージ中に格納するオプションを設定する。
- [ ノート ] このコマンドはサーバーとの相互接続に必要な場合にのみ設定する。得られたオプション値は内部では利用されない。
- [ 初期値 ] 設定なし
- [ 設定例 ]
1. LAN2 プライマリアドレスを DHCP サーバーから得る場合に特定アドレス (192.168.0.128) を要求する。
 

```

dhcp client option lan2 primary 50=c0,a8,00,80
ip lan2 address dhcp

```

 (注: ただし、この場合でも要求アドレスがサーバーから与えられるか否かはサーバー次第である。)

## 10. ICMP の設定

### 10.1 IPv4 の設定

#### 10.1.1 ICMP Echo Reply を送信するか否かの設定

---

[書式] **ip icmp echo-reply send** *send*  
**no ip icmp echo-reply send** [*send*]

[設定値] ◦ *send*  
• on.....送信する  
• off.....送信しない

[説明] ICMP Echo を受信した場合に、ICMP Echo Reply を返すか否かを設定する。

[初期値] on

#### 10.1.2 ICMP Echo Reply をリンクダウン時に送信するか否かの設定

---

[書式] **ip icmp echo-reply send-only-linkup** *send*  
**no ip icmp echo-reply send-only-linkup** [*send*]

[設定値] ◦ *send*  
• on.....リンクアップしている時だけ ICMP Echo Reply を返す  
• off.....リンクの状態に関わらず ICMP Echo Reply を返す

[説明] リンクダウンしているインタフェースに付与された IP アドレスを終点 IP アドレスとする ICMP Echo を受信した時に、それに対して ICMP Echo Reply を返すかどうかを設定する。on に設定した時には、リンクアップしている時だけ ICMP Echo を返すので、リンクの状態を ping で調べることができるようになる。off に設定した場合には、リンクの状態に関わらず ICMP Echo を返す。

[初期値] off

#### 10.1.3 ICMP Mask Reply を送信するか否かの設定

---

[書式] **ip icmp mask-reply send** *send*  
**no ip icmp mask-reply send** [*send*]

[設定値] ◦ *send*  
• on.....送信する  
• off.....送信しない

[説明] ICMP Mask Request を受信した場合に、ICMP Mask Reply を返すか否かを設定する。

[初期値] on

#### 10.1.4 ICMP Parameter Problem を送信するか否かの設定

---

[書式] **ip icmp parameter-problem send** *send*  
**no ip icmp parameter-problem send** [*send*]

[設定値] ◦ *send*  
• on.....送信する  
• off.....送信しない

[説明] 受信した IP パケットの IP オプションにエラーを検出した場合に、ICMP Parameter Problem を送信するか否かを設定する。

[初期値] off

---

**10.1.5 ICMP Redirect を送信するか否かの設定**

---

[書式] **ip icmp redirect send** *send*  
**no ip icmp redirect send** [*send*]

[設定値] ◦ *send*  
• on.....送信する  
• off.....送信しない

[説明] 他のゲートウェイ宛の IP パケットを受信して、そのパケットを適切なゲートウェイに回送した場合に、同時にパケットの送信元に対して ICMP Redirect を送信するか否かを設定する。

[初期値] on

---

**10.1.6 ICMP Redirect 受信時の処理の設定**

---

[書式] **ip icmp redirect receive** *action*  
**no ip icmp redirect receive** [*action*]

[設定値] ◦ *action*  
• on.....処理する  
• off.....無視する

[説明] ICMP Redirect を受信した場合に、それを処理して自分の経路テーブルに反映させるか、あるいは無視するかを設定する。

[初期値] off

---

**10.1.7 ICMP Time Exceeded を送信するか否かの設定**

---

[書式] **ip icmp time-exceeded send** *send*  
**no ip icmp time-exceeded send** [*send*]

[設定値] ◦ *send*  
• on.....送信する  
• off.....送信しない

[説明] 受信した IP パケットの TTL が 0 になってしまったため、そのパケットを破棄した場合に、同時にパケットの送信元に対して ICMP Time Exceeded を送信するか否かを設定する。

[初期値] on

---

**10.1.8 ICMP Timestamp Reply を送信するか否かの設定**

---

[書式] **ip icmp timestamp-reply send** *send*  
**no ip icmp timestamp-reply send** [*send*]

[設定値] ◦ *send*  
• on.....送信する  
• off.....送信しない

[説明] ICMP Timestamp を受信した場合に、ICMP Timestamp Reply を返すか否かを設定する。

[初期値] on

---

**10.1.9 ICMP Destination Unreachable を送信するか否かの設定**

---

[書式] **ip icmp unreachable send** *send*  
**no ip icmp unreachable send** [*send*]

[設定値] ◦ *send*  
• on.....送信する  
• off.....送信しない



[説明] 経路テーブルに宛先が見つからない場合や、あるいは ARP が解決できなくて IP パケットを破棄することになった場合に、同時にパケットの送信元に対して ICMP Destination Unreachable を送信するかどうかを設定する。

[初期値] on

### 10.1.10 受信した ICMP のログを記録するか否かの設定

[書式] **ip icmp log** *log*  
**no ip icmp log** [*log*]

[設定値] ○ *log*  

- on..... 記録する
- off..... 記録しない

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

[初期値] off

### 10.1.11 ステルス機能の設定

[書式] **ip stealth** all  
**ip stealth** *interface* [*interface*...]  
**no ip stealth** [...]

[設定値] ○ all..... すべての論理インタフェースからのパケットに対してステルス動作を行なう  
 ○ *interface*  

- LAN インタフェース名
- *pp peer\_num*..... 相手先情報番号

[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て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。

自分宛て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。

[初期値] ステルス動作を行なわない

## 10.2 IPv6 の設定

### 10.2.1 ICMP Echo Reply を送信するか否かの設定

[書式] **ipv6 icmp echo-reply send** *send*  
**no ipv6 icmp echo-reply send** [*send*]

[設定値] ○ *send*  

- on..... 送信する
- off..... 送信しない

[説明] ICMP Echo Reply を送信するか否かを設定する。

[初期値] on

**10.2.2 ICMP Echo Reply をリンクダウン時に送信するか否かの設定**

---

[ 書式 ]        **ipv6 icmp echo-reply send-only-linkup** *send*  
**no ipv6 icmp echo-reply send-only-linkup** [*send*]

[ 設定値 ]        ◦ *send*  
                   • on..... リンクアップしている時だけ ICMP Echo Reply を返す  
                   • off..... リンクの状態に関わらず ICMP Echo Reply を返す

[ 説明 ]        リンクダウンしているインタフェースに付与された IP アドレスを終点 IP アドレスとする ICMP Echo を受信した時に、それに対して ICMP Echo Reply を返すかどうかを設定する。on に設定した時には、リンクアップしている時だけ ICMP Echo を返すので、リンクの状態を ping で調べることができるようになる。off に設定した場合には、リンクの状態に関わらず ICMP Echo を返す。

[ 初期値 ]        off

**10.2.3 ICMP Parameter Problem を送信するか否かの設定**

---

[ 書式 ]        **ipv6 icmp parameter-problem send** *send*  
**no ipv6 icmp parameter-problem send** [*send*]

[ 設定値 ]        ◦ *send*  
                   • on..... 送信する  
                   • off..... 送信しない

[ 説明 ]        ICMP Parameter Problem を送信するか否かを設定する。

[ 初期値 ]        off

**10.2.4 ICMP Redirect を送信するか否かの設定**

---

[ 書式 ]        **ipv6 icmp redirect send** *send*  
**no ipv6 icmp redirect send** [*send*]

[ 設定値 ]        ◦ *send*  
                   • on..... 送信する  
                   • off..... 送信しない

[ 説明 ]        ICMP Redirect を出すか否かを設定する。

[ 初期値 ]        on

**10.2.5 ICMP Redirect 受信時の処理の設定**

---

[ 書式 ]        **ipv6 icmp redirect receive** *action*  
**no ipv6 icmp redirect receive** [*action*]

[ 設定値 ]        ◦ *action*  
                   • on..... 処理する  
                   • off..... 無視する

[ 説明 ]        ICMP Redirect を受けた場合に処理するか無視するかを設定する。

[ 初期値 ]        off

**10.2.6 ICMP Time Exceeded を送信するか否かの設定**

---

[ 書式 ]        **ipv6 icmp time-exceeded send** *send*  
**no ipv6 icmp time-exceeded send** [*send*]

[ 設定値 ]        ◦ *send*  
                   • on..... 送信する  
                   • off..... 送信しない

[ 説明 ]        ICMP Time Exceeded を出すか否かを設定する。

[ 初期値 ]        on

### 10.2.7 ICMP Destination Unreachable を送信するか否かの設定

---

[ 書式 ]            **ipv6 icmp unreachable send** *send*  
                  **no ipv6 icmp unreachable send** [*send*]

[ 設定値 ]        ◦ *send*  
                  • on.....送信する  
                  • off.....送信しない

[ 説明 ]            ICMP Destination Unreachable を出すか否かを設定する。

[ 初期値 ]        on

### 10.2.8 受信した ICMP のログを記録するか否かの設定

---

[ 書式 ]            **ipv6 icmp log** *log*  
                  **no ipv6 icmp log** [*log*]

[ 設定値 ]        ◦ *log*  
                  • on.....記録する  
                  • off.....記録しない

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

[ 初期値 ]        off

### 10.2.9 ICMP Packet-Too-Big を送信するか否かの設定

---

[ 書式 ]            **ipv6 icmp packet-too-big send** *send*  
                  **no ipv6 icmp packet-too-big send** [*send*]

[ 設定値 ]        ◦ *send*  
                  • on.....送信する  
                  • off.....送信しない

[ 説明 ]            ICMP Packet-Too-Big を出すか否かを設定する。

[ 初期値 ]        on

### 10.2.10 ステルス機能の設定

---

[ 書式 ]            **ipv6 stealth** *all*  
                  **ipv6 stealth** *interface* [*interface...*]  
                  **no ipv6 stealth** [...]

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

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

自分がサポートしていないプロトコルや IPv6 ヘッダ、あるいはオープンしていない TCP/UDP ポートに対して指定されたインタフェースからパケットを受信した時に、通常であれば ICMP unreachable や TCP リセットを返送する。しかし、このコマンドを設定しておく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の存在を隠すことができる。

[ ノート ]        指定されたインタフェースからの PING にも答えなくなるので注意が必要である。  
自分宛ではないパケットが原因で発生する ICMP はこのコマンドでは制御できない。それらを送信しないようにするには、**ipv6 icmp \*** コマンド群を用いる必要がある。

[ 初期値 ]        ステルス動作を行なわない

## 11. トンネリング

### 11.1 トンネルインタフェースの使用許可の設定

---

- [書式]           **tunnel enable** *tunnel\_num*  
**no tunnel enable** *tunnel\_num*
- [設定値]        ◦ *tunnel\_num*
- トンネルインタフェース番号
  - all ..... すべてのトンネルインタフェース
- [説明]           トンネルインタフェースを使用できる状態にする。  
工場出荷時は、すべてのトンネルインタフェースは `disable` 状態であり、使用する場合は本コマンドにより、インタフェースを有効にしなければならない。

### 11.2 トンネルインタフェースの使用不許可の設定

---

- [書式]           **tunnel disable** *tunnel\_num*
- [設定値]        ◦ *tunnel\_num*
- トンネルインタフェース番号
  - all ..... すべてのトンネルインタフェース
- [説明]           トンネルインタフェースを使用できない状態にする。  
トンネル先の設定を行なう場合は、`disable` 状態で行なうのが望ましい。

### 11.3 トンネルインタフェースの種別の設定

---

- [書式]           **tunnel encapsulation** *type*  
**no tunnel encapsulation**
- [設定値]        ◦ *type*
- `ipip` ..... IPv6 over IPv4 トンネル、IPv4 over IPv6 トンネル、IPv4 over IPv4 トンネルまたは IPv6 over IPv6 トンネル
  - `pptp` ..... PPTP トンネル
- [説明]           トンネルインタフェースの種別を設定する。
- [ノート]         トンネリングと NAT を併用する場合には **tunnel endpoint address** コマンドにより始点 IP アドレスを設定することが望ましい。
- [初期値]         `ipip`

### 11.4 トンネルインタフェースの端点 IP アドレスの設定

---

- [書式]           **tunnel endpoint address** [*local*] *remote*  
**no tunnel endpoint address** [[*local*] *remote*]
- [設定値]        ◦ *local* ..... 自分側のトンネルインタフェース端点の IP アドレス
- *remote* ..... 相手側のトンネルインタフェース端点の IP アドレス
- [説明]           トンネルインタフェース端点の IP アドレスを設定する。IP アドレスは IPv4/IPv6 いずれのアドレスも設定できるが、*local* と *remote* では IPv4/IPv6 の種別が揃っていないといけない。トンネルインタフェース端点として IPv4 アドレスを設定した場合には、IPv4 over IPv4 トンネルと IPv6 over IPv4 トンネルが、IPv6 アドレスを設定した場合には IPv4 over IPv6 トンネルと IPv6 over IPv6 トンネルが利用できる。
- local* を省略した場合は、適当なインタフェースの IP アドレスが利用される。
- [ノート]         PPTP サーバーの Anonymous で受ける場合には設定する必要はない。
- [初期値]         IP アドレスは設定されていない

## 11.5 トンネルインタフェースの IPv4 アドレスの設定

- [書式]           **ip tunnel address** *ip\_address*[/*mask*]  
**no ip tunnel address** [*ip\_address*[/*mask*]]
- [設定値]       ○ *ip\_address* ..... IPv4 アドレス  
                  ○ *mask* ..... xxx.xxx.xxx.xxx (xxx は 10 進数)  
                                           0x に続く 16 進数  
                                           マスクビット数
- [説明]           トンネルインタフェースの IPv4 アドレスとネットマスクを設定する。

## 11.6 トンネルインタフェースの相手側の IPv4 アドレスの設定

- [書式]           **ip tunnel remote address** *ip\_address*  
**no ip tunnel remote address** [*ip\_address*]
- [設定値]       ○ *ip\_address* ..... IPv4 アドレス
- [説明]           トンネルインタフェースの相手側の IPv4 アドレスを設定する。

## 11.7 トンネル接続する DTCP サーバーへの認証情報の設定

- [書式]           **tunnel dtcp** *ip-address*[:*port*] **myname** *username password* [*retry*] [*local*]  
**no tunnel dtcp** *ip-address*[:*port*] **myname** *username password* [*retry*] [*local*]

- [設定値]       ○ *ip\_address* ..... DTCP サーバーの IP アドレスもしくはドメイン名  
                  ○ *port* ..... DTCP サーバー側のポート番号  
                  ○ *username* ..... 認証用ユーザ名  
                  ○ *password* ..... 認証用パスワード  
                  ○ *retry* ..... 認証に失敗した場合の再接続回数の上限  
                  ○ *local* ..... 認証確立時に利用する自分側の端点の IP アドレス

- [説明]           DTCP サーバーに接続するための認証情報を設定する。  
 このコマンドを設定すると、ルータ起動時もしくは設定完了時に自動的に認証動作が開始される。認証動作は自動的に行なわれ、認証が失敗した場合は、確立するまで再接続を繰り返す。一旦確立した後もキーブアライブによる接続維持の動作が行なわれる。  
*retry* パラメータを設定することにより再接続の上限回数を指定することができる。

*port* を指定しない場合には、ポート番号 20200 が使用される。

*retry* を指定しない場合には、再接続回数を制限しない。

*local\_address* を指定しない場合には、DTCP サーバーに最も近いインタフェースのアドレスを自分側の端点の IP アドレスとして使用する。

*tunnel dtcp connect* コマンドまたは *tunnel dtcp disconnect* コマンドを利用することにより、手動で接続または切断を行なう事もできる。

DTCP の認証が確立した場合、サーバーから利用する IPv6 のプレフィックスを伝達される。このプレフィックスを自動的に反映する場合のキーワードとして *dtcp-prefix* を利用できる。

- [初期値]       なし

- [設定例]       TUNNEL1 インタフェース経由で受信したプレフィックスを LAN1 インタフェースに設定し、同時に RA として広告する。

```
ipv6 lan1 prefix dtcp-prefix@tunnel1::/64
ipv6 prefix 1 dtcp-prefix@tunnel1::/64
ipv6 lan1 rtadv send 1
```

## 12. PPTP 機能の設定

本機能を使用して PC と接続するためには、PC 側には Microsoft 社の WindowsXP の「仮想プライベートネットワーク接続」などの設定が必要となります。

### 12.1 共通の設定

**tunnel encapsulation**、**tunnel endpoint address**、**ppp ccp type** コマンドも合わせて参照のこと。

#### 12.1.1 PPTP サーバーを動作させるか否かの設定

---

[書式] **pptp service** *service*  
**no ptp service** [*service*]

[設定値] ○ *service*

- on.....PPTP サーバーとして動作する
- off.....PPTP サーバーとして動作しない

[説明] PPTP サーバー機能を動作させるか否かを設定する。

[ノート] PPTP サーバーで使う TCP のポート番号 1723 を閉じる。初期値は off なので、PPTP サーバーを起動する場合には、**pptp service on** を設定する。

[初期値] off

#### 12.1.2 相手先情報番号にバインドされるトンネルインタフェースの設定

---

[書式] **pp bind** *tunnel\_num*  
**pp bind** *tunnel\_num-tunnel\_num*  
**no pp bind** [*tunnel\_num*]

[設定値] ○ *tunnel\_num* ..... トンネルインタフェース番号 (tunnel1 .. tunnel4)

[説明] 選択されている相手先情報番号にバインドされるトンネルインタフェースを指定する。  
第2書式は anonymous インタフェースを使って多数の接続先を登録するために複数連続したトンネルインタフェースをバインドする場合に用いる。

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

[初期値] 設定されていない

#### 12.1.3 PPTP ホスト名の設定

---

[書式] **pptp hostname** *name*  
**no ptp hostname** [*name*]

[設定値] ○ *name*..... ホスト名 (64 バイト以内)

[説明] PPTP ホスト名を設定する。

[ノート] コマンドで設定したユーザ定義の名前が相手先に通知される。何も設定していない場合には機種名が通知される。相手先のルータには、**show status pp** コマンドの '接続相手先:' で表示される。

[初期値] 機種名

#### 12.1.4 PPTP の動作タイプの設定

---

[書式] **pptp service type** *type*  
**no ptp service type** [*type*]

|         |                                                                                                                                                                                             |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ 設定値 ] | <ul style="list-style-type: none"> <li>◦ <i>type</i> <ul style="list-style-type: none"> <li>• <i>server</i>..... サーバーとして動作</li> <li>• <i>client</i>..... クライアントとして動作</li> </ul> </li> </ul> |
| [ 説明 ]  | PPTP サーバーとして動作するか、PPTP クライアントとして動作するかを設定する。                                                                                                                                                 |
| [ ノート ] | PPTP はサーバー、クライアント方式の接続で、ルータ間で接続する場合には必ず一方がサーバーで、もう一方がクライアントである必要がある。                                                                                                                        |
| [ 初期値 ] | <i>server</i>                                                                                                                                                                               |

### 12.1.5 PPTP パケットのウィンドウサイズの設定

|         |                                                                                 |
|---------|---------------------------------------------------------------------------------|
| [ 書式 ]  | <b>pptp window size <i>size</i></b><br><b>no pptp window size [<i>size</i>]</b> |
| [ 設定値 ] | ◦ <i>size</i> ..... パケットサイズ (1..128)                                            |
| [ 説明 ]  | 受信済みで無応答の PPTP パケットをバッファに入れることができるパケットの最大数を設定する。                                |
| [ 初期値 ] | 32                                                                              |

### 12.1.6 PPTP の動作モードの設定

|         |                                                                                                                                                                                                 |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ 書式 ]  | <b>pptp call-id mode <i>mode</i></b><br><b>no pptp call-id mode [<i>mode</i>]</b>                                                                                                               |
| [ 設定値 ] | <ul style="list-style-type: none"> <li>◦ <i>mode</i> <ul style="list-style-type: none"> <li>• <i>normal</i>..... 通常モード</li> <li>• <i>backward-compatibility</i> .....未対応</li> </ul> </li> </ul> |
| [ 説明 ]  | PPTP の動作モードを設定する。                                                                                                                                                                               |
| [ 初期値 ] | <i>normal</i>                                                                                                                                                                                   |

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

|         |                                                                                                                                                                             |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ 書式 ]  | <b>pptp syslog <i>syslog</i></b><br><b>no pptp syslog [<i>syslog</i>]</b>                                                                                                   |
| [ 設定値 ] | <ul style="list-style-type: none"> <li>◦ <i>syslog</i> <ul style="list-style-type: none"> <li>• <i>on</i>..... 出力する</li> <li>• <i>off</i>..... 出力しない</li> </ul> </li> </ul> |
| [ 説明 ]  | PPTP のコネクション制御の syslog を出力するか否かを設定する。同時に <b>syslog debug on</b> を設定する必要がある。<br>キーブアラライブ用の Echo-Request, Echo-Reply については出力されない。                                             |
| [ 初期値 ] | <i>off</i>                                                                                                                                                                  |

### 12.1.8 PPTP 暗号鍵生成のための要求する認証方式の設定

|         |                                                                                                                                                                                                                                                                                                                |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ 書式 ]  | <b>pp auth request <i>auth</i> [arrive-only]</b><br><b>no pp auth request [<i>auth</i>]</b>                                                                                                                                                                                                                    |
| [ 設定値 ] | <ul style="list-style-type: none"> <li>◦ <i>auth</i> <ul style="list-style-type: none"> <li>• <i>pap</i>..... PAP</li> <li>• <i>chap</i>..... CHAP</li> <li>• <i>mschap</i>..... MSCHAP</li> <li>• <i>mschap-v2</i> ..... MSCHAP-Version2</li> <li>• <i>chap-pap</i>..... CHAP と PAP 両方</li> </ul> </li> </ul> |
| [ 説明 ]  | 要求する認証方式を設定する。                                                                                                                                                                                                                                                                                                 |

- [ノート] PPTP 暗号鍵生成のために認証プロトコルの MS-CHAP または MS-CHAPv2 を設定する。通常サーバー側で設定する。
- [初期値] 設定されない

### 12.1.9 PPTP 暗号鍵生成のための受け入れ可能な認証方式の設定

---

- [書式] **pp auth accept *auth* [*auth*]**  
**no pp auth accept [*auth auth*]**
- [設定値] ○ *auth*
- pap..... PAP
  - chap..... CHAP
  - mschap..... MSCHAP
  - mschap-v2..... MSCHAP-Version2
- [説明] 受け入れ可能な認証方式を設定する。
- [ノート] PPTP 暗号鍵生成のために認証プロトコルの MS-CHAP または MS-CHAPv2 を設定する。通常クライアント側で設定する。  
 MacOS 10.2 以降のクライアントに対しては mschap-v2 を用いる。
- [初期値] 設定されない

## 12.2 リモートアクセス VPN 機能

### 12.2.1 PPTP トンネルの切断タイマの設定

---

- [書式] **pptp tunnel disconnect time *time***  
**no pptp tunnel disconnect time [*time*]**
- [設定値] ○ *time*
- 秒数 (1..21474836)
  - off..... タイマを設定しない
- [説明] 選択されている PPTP トンネルに対して、データパケット無入力・無送信時に、タイムアウトにより PPTP トンネルを切断する時間を設定する。
- [初期値] 60

### 12.2.2 PPTP トンネルの端点の名前の設定

---

- [書式] **tunnel endpoint name [*local\_name*] *remote\_name***  
**no tunnel endpoint name [*local\_name remote\_name*]**
- [設定値] ○ *local\_name*..... 自分側端点  
 ○ *remote\_name*..... 相手側端点
- [説明] トンネル端点の名前を指定する。
- [ノート] 名前にはドメイン名 (FQDN) を指定する。**tunnel endpoint address** コマンドが設定されている場合には、そちらが優先される。

### 12.2.3 PPTP キープアライブの設定

---

- [書式] **pptp keepalive use *use***  
**no pptp keepalive use [*use*]**
- [設定値] ○ *use*
- on..... 使用する
  - off..... 使用しない
- [説明] トンネルキープアライブを使用するか否かを選択する。



- [ノート] PPTP トンネルの端点に対して、PPTP 制御コネクション確認要求 (Echo-Request) を送出して、それに対する PPTP 制御コネクション確認要求への応答 (Echo-Reply) で相手先からの応答があるかどうかを確認する。応答がない場合には、**pptp keepalive interval** コマンドに従った切断処理を行なう。
- [初期値] on

#### 12.2.4 PPTP キープアライブのログ設定

- [書式] **pptp keepalive log** *log*  
**no ptp keepalive log** [*log*]
- [設定値] ○ *log*
- on..... ログにとる
  - off..... ログにとらない
- [説明] トンネルキープアライブをログに取るか否かを選択する。
- [初期値] off

#### 12.2.5 PPTP 接続において暗号化の有無により接続を許可するか否かの設定

- [書式] **ppp ccp no-encryption** *mode*  
**no ppp ccp no-encryption** [*mode*]
- [設定値] ○ *mode*
- reject..... 暗号化なしでは接続拒否
  - accept..... 暗号化なしでも接続許可
- [説明] MPPE(Microsoft Point-to-Point Encryption) の暗号化がネゴシエーションされないときの動作を設定する。
- [初期値] accept

#### 12.2.6 PPTP キープアライブを出すインターバルとカウントの設定

- [書式] **pptp keepalive interval** *interval* [*count*]  
**no ptp keepalive interval** [*interval* *count*]
- [設定値] ○ *interval*..... インターバル (1..65535)  
○ *count*..... カウント (3..100)
- [説明] トンネルキープアライブを出すインターバルとダウン検出用のカウントを設定する。
- [ノート] 一度 PPTP 制御コネクション確認要求 (Echo-Request) に対するリプライが返ってこないのを検出したら、その後の監視タイマは 1 秒に短縮される。
- [初期値] *interval* = 30  
*count* = 6

## 13. NAT 機能

NAT 機能は、ルータが転送する IP パケットの始点 / 終点 IP アドレスや、TCP/UDP のポート番号を変換することにより、アドレス体系の異なる IP ネットワークを接続することができる機能です。

NAT 機能を用いると、プライベートアドレス空間とグローバルアドレス空間との間でデータを転送したり、1 つのグローバル IP アドレスに複数のホストを対応させたりすることができます。

本製品では、始点 / 終点 IP アドレスの変換だけを行なうことを NAT と呼び、TCP/UDP のポート番号の変換を伴うものを IP マスカレードと呼んでいます。

アドレス変換規則を表す記述を NAT ディスクリプタと呼び、それぞれの NAT ディスクリプタには、アドレス変換の対象とすべきアドレス空間が定義されます。アドレス空間の記述には、**nat descriptor address inner**、**nat descriptor address outer** コマンドを用います。前者は NAT 処理の内側 (INNER) のアドレス空間を、後者は NAT 処理の外側 (OUTER) のアドレス空間を定義するコマンドです。原則的に、これら 2 つのコマンドを対で設定することにより、変換前のアドレスと変換後のアドレスとの対応づけが定義されます。

NAT ディスクリプタはインタフェースに対して適用されます。インタフェースに接続された先のネットワークが NAT 処理の外側であり、インタフェースから本製品を経由して他のインタフェースから繋がるネットワークが NAT 処理の内側になります。

NAT ディスクリプタは動作タイプ属性を持ちます。IP マスカレードやアドレスの静的割当てなどの機能を利用する場合には、該当する動作タイプを選択する必要があります。

### 13.1 インタフェースへの NAT ディスクリプタ適用の設定

**[書式]**

```
ip interface nat descriptor nat_descriptor_list [reverse nat_descriptor_list]
ip pp nat descriptor nat_descriptor_list [reverse nat_descriptor_list]
ip tunnel nat descriptor nat_descriptor_list [reverse nat_descriptor_list]
no ip interface nat descriptor [nat_descriptor_list [reverse nat_descriptor_list]]
no ip pp nat descriptor [nat_descriptor_list [reverse nat_descriptor_list]]
no ip tunnel nat descriptor [nat_descriptor_list [reverse nat_descriptor_list]]
```

**[設定値]**

- *interface* ..... LAN インタフェース名
- *nat\_descriptor\_list* ..... 空白で区切られた NAT ディスクリプタ番号 (1..21474836) の並び (16 個以内)

**[説明]** 適用されたインタフェースを通過するパケットに対して、リストに定義された順番で NAT ディスクリプタによって定義された NAT 変換を順番に処理する。

*reverse* の後ろに記述した NAT ディスクリプタでは、通常処理される IP アドレス、ポート番号とは逆向きの IP アドレス、ポート番号に対して NAT 変換を施す。

**[ノート]** LAN インタフェースの場合、NAT ディスクリプタの外側アドレスに対しては、同一 LAN の ARP 要求に対して応答する。

### 13.2 NAT ディスクリプタの動作タイプの設定

**[書式]**

```
nat descriptor type nat_descriptor type
no nat descriptor type [nat_descriptor type]
```

**[設定値]**

- *nat\_descriptor* ..... NAT ディスクリプタ番号 (1..21474836)
- *type*
  - *none* ..... NAT 変換機能を利用しない
  - *nat* ..... 動的 NAT 変換と静的 NAT 変換を利用
  - *masquerade* ..... 静的 NAT 変換と IP マスカレード変換
  - *nat-masquerade* ..... 動的 NAT 変換と静的 NAT 変換と IP マスカレード変換

**[説明]** NAT 変換の動作タイプを指定する。

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

**[初期値]** none

### 13.3 NAT 処理の外側 IP アドレスの設定

- [書式] **nat descriptor address outer** *nat\_descriptor outer\_ipaddress\_list*  
**no nat descriptor address outer** *nat\_descriptor [outer\_ipaddress\_list]*
- [設定値]
- *nat\_descriptor* ..... NAT ディスクリプタ番号 (1..21474836)
  - *outer\_ipaddress\_list* ... NAT 対象の外側 IP アドレス範囲のリストまたはニーモニック
    - 1 個の IP アドレスまたは間に - をはさんだ IP アドレス (範囲指定)、およびこれらを任意に並べたもの
    - *ipcp* ..... PPP の IPCP の IP-Address オプションにより接続先から通知される IP アドレス
    - *primary* ..... **ip interface address** コマンドで設定されている IP アドレス
    - *secondary* ..... **ip interface secondary address** コマンドで設定されている IP アドレス
- [説明] 動的 NAT 処理の対象である外側の IP アドレスの範囲を指定する。IP マスカレードでは、先頭の 1 個の外側の IP アドレスが使用される。
- [ノート] ニーモニックをリストにすることはできない。  
適用されるインタフェースにより使用できるパラメータが異なる。

| 適用インタフェース        | LAN | PP | トンネル |
|------------------|-----|----|------|
| <i>ipcp</i>      | ×   | ○  | ×    |
| <i>primary</i>   | ○   | ×  | ×    |
| <i>secondary</i> | ○   | ×  | ×    |
| IP アドレス          | ○   | ○  | ○    |

[初期値] *ipcp*

### 13.4 NAT 処理の内側 IP アドレスの設定

- [書式] **nat descriptor address inner** *nat\_descriptor inner\_ipaddress\_list*  
**no nat descriptor address inner** *nat\_descriptor [inner\_ipaddress\_list]*
- [設定値]
- *nat\_descriptor* ..... NAT ディスクリプタ番号 (1..21474836)
  - *inner\_ipaddress\_list* ... NAT 対象の内側 IP アドレス範囲のリストまたはニーモニック
    - 1 個の IP アドレス、または間に - をはさんだ IP アドレス (範囲指定)、およびこれらを任意に並べたもの
    - *auto* ..... すべて
- [説明] NAT/IP マスカレード処理の対象である内側の IP アドレスの範囲を指定する。
- [初期値] *auto*

### 13.5 NAT のアドレス割当をログに記録するか否かの設定

- [書式] **nat descriptor log** *switch*
- [設定値]
- *switch*
    - *on* ..... 記録する
    - *off* ..... 記録しない
- [説明] NAT のアドレス割当をログに記録するか否かを設定します。
- [初期値] *off*

### 13.6 静的 NAT エントリの設定

- [書式] **nat descriptor static** *nat\_descriptor id outer\_ip=inner\_ip [count]*  
**no nat descriptor static** *nat\_descriptor id [outer\_ip=inner\_ip [count]]*
- [設定値]
- *nat\_descriptor* ..... NAT ディスクリプタ番号 (1..21474836)
  - *id* ..... 静的 NAT エントリの識別情報 (1..21474836)
  - *outer\_ip* ..... 外側 IP アドレス (1 個)
  - *inner\_ip* ..... 内側 IP アドレス (1 個)

◦ *count*

- 連続設定する個数
- 省略時は 1

- [ 説明 ] NAT 変換で固定割り付けする IP アドレスの組み合わせを指定する。個数を同時に指定すると指定されたアドレスを始点とした範囲指定とする。
- [ ノート ] 外側アドレスが NAT 処理対象として設定されているアドレスである必要は無い。静的 NAT のみを使用する場合には、**nat descriptor address outer** コマンドと **nat descriptor address inner** コマンドの設定に注意する必要がある。初期値がそれぞれ *ipcp* と *auto* であるので、例えば何らかの IP アドレスをダミーで設定しておくことで動的動作しないようにする。

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

- [ 書式 ] **nat descriptor masquerade rlogin** *nat\_descriptor use*  
**no nat descriptor masquerade rlogin** *nat\_descriptor [use]*
- [ 設定値 ] ◦ *nat\_descriptor*.....NAT ディスクリプタ番号 (1..21474836)  
 ◦ *use*  
 • *on* ..... 使用する  
 • *off* ..... 使用しない
- [ 説明 ] IP マスカレード使用時に *rlogin*、*rcp*、*ssh* の使用を許可するか否かを設定する。
- [ ノート ] *on* にすると、*rlogin*、*rcp* と *ssh* のトラフィックに対してはポート番号を変換しなくなる。また *on* の場合に *rsh* は使用できない。
- [ 初期値 ] *off*

### 13.8 外側から受信したパケットに該当する変換テーブルが存在しないときの動作の設定

- [ 書式 ] **nat descriptor masquerade incoming** *nat\_descriptor action [ip\_address]*  
**no nat descriptor masquerade incoming** *nat\_descriptor*
- [ 設定値 ] ◦ *nat\_descriptor*.....NAT ディスクリプタ番号 (1..21474836)  
 ◦ *action*.....動作  
 • *through*..... 変換せずに通す  
 • *reject*..... 破棄して、TCP の場合は RST を返す  
 • *discard*..... 破棄して、何も返さない  
 • *forward*..... 指定されたホストに転送する  
 ◦ *ip\_address* ..... 転送先の IP アドレス
- [ 説明 ] IP マスカレードで外側から受信したパケットに該当する変換テーブルが存在しないときの動作を設定する。*action* が *forward* のときには *ip\_address* を設定する必要がある。
- [ 初期値 ] *reject*

### 13.9 静的 IP マスカレードエントリの設定

- [ 書式 ] **nat descriptor masquerade static** *nat\_descriptor id inner\_ip protocol [outer\_port=]inner\_port*  
**no nat descriptor masquerade static** *nat\_descriptor id [inner\_ip protocol [outer\_port=]inner\_port]*
- [ 設定値 ] ◦ *nat\_descriptor*.....NAT ディスクリプタ番号 (1..21474836)  
 ◦ *id*..... 静的 IP マスカレードエントリの識別情報 (1 以上の数値)  
 ◦ *inner\_ip*..... 内側 IP アドレス (1 個)  
 ◦ *protocol*  
 • *esp* ..... ESP  
 • *tcp* ..... TCP プロトコル  
 • *udp* ..... UDP プロトコル  
 • *icmp* ..... ICMP プロトコル  
 • プロトコル番号..... IANA で割り当てられている *protocol numbers*  
 ◦ *outer\_port*..... 固定する外側ポート番号 (ニーモニック)  
 ◦ *inner\_port*..... 固定する内側ポート番号 (ニーモニック)

- [ 説明 ] IP マスカレードによる通信でポート番号変換を行なわないようにポートを固定する。
- [ ノート ] *outer\_port* と *inner\_port* を指定した場合には IP マスカレード適用時にインタフェースの外側から内側へのパケットは *outer\_port* から *inner\_port* に、内側から外側へのパケットは *inner\_port* から *outer\_port* へとポート番号が変換される。  
*outer\_port* を指定せず、*inner\_port* のみの場合はポート番号の変換はされない。

### 13.10 NAT の IP アドレスマップの消去タイマの設定

---

- [ 書式 ] **nat descriptor timer** *nat\_descriptor* *time*  
**nat descriptor timer** *nat\_descriptor* protocol=*protocol* [port=*port\_range*] *time*  
**no nat descriptor timer** *nat\_descriptor* [*time*]  
**no nat descriptor timer** *nat\_descriptor* protocol=*protocol* [port=*port\_range*] [...]
- [ 設定値 ]
- *nat\_descriptor* ..... NAT ディスクリプタ番号 (1..21474836)
  - *time* ..... 消去タイマの秒数 (30..21474836)
  - *protocol* ..... プロトコル
  - *port\_range* ..... ポート番号の範囲、プロトコルが TCP または UDP の場合にのみ有効
- [ 説明 ] NAT や IP マスカレードのセッション情報を保持する期間を表す NAT タイマを設定する。IP マスカレードの場合には、プロトコルやポート番号別の NAT タイマを設定することもできる。指定されていないプロトコルの場合は、第一の形式で設定した NAT タイマの値が使われる。
- [ 初期値 ] 900  
プロトコル毎の設定はなし

### 13.11 IP マスカレードで利用するポートの範囲の設定

---

- [ 書式 ] **nat descriptor masquerade port range** *nat\_descriptor* *start* [*port\_num*]  
**no nat descriptor masquerade port range** *nat\_descriptor* [*start* [*port\_num*]]
- [ 設定値 ]
- *nat\_descriptor* ..... NAT ディスクリプタの識別番号 (1..21474836)
  - *start* ..... 開始ポート番号 (1024..65534)
  - *port\_num*
    - ポートの個数 (1 .. 4096)
    - 省略時は 4096 個
- [ 説明 ] IP マスカレードで利用するポート番号の範囲を設定する。  
*start+port\_num* <= 65535 でなくてはならない。
- [ 初期値 ] *start* = 60000  
*port\_num* = 4096

### 13.12 FTP として認識するポート番号の設定

---

- [ 書式 ] **nat descriptor ftp port** *nat\_descriptor* *port* [*port...*]  
**no nat descriptor ftp port** *nat\_descriptor* [*port...*]
- [ 設定値 ]
- *nat\_descriptor* ..... NAT ディスクリプタの識別番号 (1..21474836)
  - *port* ..... ポート番号 (1 .. 65535)
- [ 説明 ] TCP で、このコマンドにより設定されたポート番号を FTP の制御チャネルの通信とみなして処理をする。
- [ 初期値 ] 21

### 13.13 IP マスカレードで変換しないポート番号の範囲の設定

- [書式]        **nat descriptor masquerade unconvertible port** *nat\_descriptor* if-possible  
**nat descriptor masquerade unconvertible port** *nat\_descriptor protocol port*  
**no nat descriptor masquerade unconvertible port** *nat\_descriptor protocol* [*port*]
- [設定値]     ◦ *nat\_descriptor*..... NAT ディスクリプタの識別番号 (1..21474836)  
               ◦ *protocol*  
                   • tcp ..... TCP  
                   • udp ..... UDP  
               ◦ *port*..... ポート番号の範囲
- [説明]        IP マスカレードで変換しないポート番号の範囲を設定する。  
 if-possible が指定されている時には、処理しようとするポート番号が他の通信で使われていない場合には値を変換せずそのまま利用する。
- [初期値]     なし

### 13.14 IP マスカレード変換時に DF ビットを削除するか否かの設定

- [書式]        **nat descriptor masquerade remove df-bit** *remove*  
**no nat descriptor masquerade remove df-bit** [*remove*]
- [設定値]     ◦ *remove*  
               • on ..... IP マスカレード変換時に DF ビットを削除する  
               • off ..... IP マスカレード変換時に DF ビットを削除しない
- [説明]        IP マスカレード変換時に DF ビットを削除するか否かを設定する。
- DF ビットは経路 MTU 探索のために用いるが、そのためには長すぎるパケットに対する ICMP エラーを正しく発信元まで返さなくてはならない。しかし、IP マスカレード処理では IP アドレスなどを書き換えてしまうため、ICMP エラーを正しく発信元に返せない場合がある。そうすると、パケットを永遠に届けることができなくなってしまう。このように、経路 MTU 探索のための ICMP エラーが正しく届かない状況を、経路 MTU ブラックホールと呼ぶ。
- IP マスカレード変換時に同時に DF ビットを削除してしまうと、この経路 MTU ブラックホールを避けることができる。その代わりに、経路 MTU 探索が行なわれないことになるので、通信効率を下がる可能性がある。
- [ノート]      ファストパス処理は、一度ノーマルパス処理で通過させたパケットの情報を保存しておき、同じ種類のパケットであれば高速に転送するという処理を行なっている。そのため、例えば **ping** コマンドを実行した場合、最初の 1 回目はノーマルパス処理、2 回目以降はファストパス処理となる。そのため、最初の 1 回は DF ビットが削除されるが、2 回目以降は DF ビットが削除されないという状況だった。
- [初期値]     on

### 13.15 SIP メッセージに含まれる IP アドレスを書き換えるか否かの設定

- [書式]        **nat descriptor sip** *nat\_descriptor sw*  
**no nat descriptor sip** *nat\_descriptor*
- [設定値]     ◦ *nat\_descriptor*..... NAT ディスクリプタの識別番号 (1..21474836)  
               ◦ *sw*  
                   • on ..... 変換する  
                   • off ..... 変換しない  
                   • auto ..... **sip use** コマンドの設定値に従う
- [説明]        SIP メッセージに含まれる IP アドレスを NAT または IP マスカレードの変換ルールに従って書き換えるか否かを設定する。  
 auto と設定した場合には、sip use on と設定されていれば IP アドレスの変換を行ない、sip use off と設定されていれば IP アドレスの変換を行なわない。

[ノート] 静的 NAT または静的 IP マスカレードを設定して、LAN 内に SIP 対応機器を設置して使用する場合、その SIP 対応機器と LAN の外側に設置された機器との間で送受信される SIP メッセージに含まれる IP アドレスは、SIP-NAT 機能が有効なときに意図しない変換が行われる、また、SIP-NAT 機能が無効なときに意図した変換が行われない、ということがありうる。それらを原因として SIP 通信が正常に行えない場合には、本コマンドの設定を変更しなければならない。

[初期値] auto

## 14. DNS の設定

本製品は、DNS(Domain Name Service)機能として名前解決、リカーシブサーバー機能、上位 DNS サーバーの選択機能、簡易 DNS サーバー機能(静的 DNS レコードの登録)を持ちます。

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

リカーシブサーバー機能は、DNS サーバーとクライアントの間に入って、DNS パケットの中継を行いません。本製品宛にクライアントから届いた DNS 問い合わせパケットを **dns server** コマンドで設定された DNS サーバーに中継します。DNS サーバーからの回答は本製品宛に届くので、それをクライアントに転送します。最大 256 件のキャッシュを持ち、キャッシュにあるデータに関しては DNS サーバーに問い合わせることなく返事を返すため、DNS によるトラフィックを削減する効果があります。キャッシュは、DNS サーバーからデータを得た場合にデータに記されていた時間だけ保持されません。

DNS の機能を使用するためには、**dns server** コマンドを設定しておく必要があります。また、この設定は DHCP サーバー機能において、DHCP クライアントの設定情報にも使用されます。

### 14.1 DNS を利用するか否かの設定

---

|       |                                                                                                                                          |
|-------|------------------------------------------------------------------------------------------------------------------------------------------|
| 【書式】  | <b>dns service service</b><br><b>no dns service [service]</b>                                                                            |
| 【設定値】 | ○ <i>service</i> <ul style="list-style-type: none"> <li>• recursive..... DNS リカーシブサーバーとして動作する</li> <li>• off ..... サービスを停止させる</li> </ul> |
| 【説明】  | DNS リカーシブサーバーとして動作するかどうかを設定する。off を設定すると、DNS 的機能は一切動作しない。また、ポート 53/udp も閉じられる。                                                           |
| 【初期値】 | recursive                                                                                                                                |

### 14.2 ルータ自身の FQDN の設定

---

|       |                                                                   |
|-------|-------------------------------------------------------------------|
| 【書式】  | <b>dns private name name</b><br><b>no dns private name [name]</b> |
| 【設定値】 | ○ <i>name</i> ..... ルータの FQDN                                     |
| 【説明】  | ルータの DNS 名を指定する。                                                  |
| 【初期値】 | なし                                                                |

### 14.3 DNS ドメイン名の設定

---

|       |                                                                                                                                                                                                                                     |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 【書式】  | <b>dns domain domain_name</b><br><b>no dns domain [domain_name]</b>                                                                                                                                                                 |
| 【設定値】 | ○ <i>domain_name</i> ..... DNS ドメインを表す文字列                                                                                                                                                                                           |
| 【説明】  | ルータが所属する DNS ドメインを設定する。<br>ルータのホストとしての機能 ( <b>ping</b> 、 <b>traceroute</b> ) 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。 |

### 14.4 DNS サーバーの IP アドレスの設定

---

|      |                                                                                        |
|------|----------------------------------------------------------------------------------------|
| 【書式】 | <b>dns server ip_address [ip_address ...]</b><br><b>no dns server [ip_address ...]</b> |
|------|----------------------------------------------------------------------------------------|



- [設定値]    ◦ *ip\_address* ..... DNS サーバーの IP アドレス (空白で区切って最大 4ヶ所まで設定可能)
- [説明]        DNS サーバーの IP アドレスを指定する。  
この IP アドレスはルータが DHCP サーバーとして機能する場合に DHCP クライアントに通知するためや、IPCP の MS 拡張オプションで相手に通知するためにも使用される。
- [ノート]        DHCP サーバーから通知された DNS サーバーを使うときには、**dns server dhcp** コマンドを使う。
- [初期値]        DNS サーバーは設定されていない

#### 14.5 DNS サーバーを通知してもらう相手先情報番号の設定

- [書式]        **dns server pp peer\_num**  
**no dns server pp [peer\_num]**
- [設定値]        ◦ *peer\_num* ..... DNS サーバーを通知してもらう相手先情報番号
- [説明]        DNS サーバーを通知してもらう相手先情報番号を設定する。このコマンドで相手先情報番号が設定されていると、DNS での名前解決を行なう場合に、まずこの相手先に発信して、そこで PPP の IPCP MS 拡張機能で通知された DNS サーバーに対して問い合わせを行なう。  
相手先に接続できなかったり、接続できても DNS サーバーの通知がなかった場合には名前解決は行われ  
ない。  
**dns server** コマンドで DNS サーバーが明示的に指定されている場合には、そちらの設定が優先される。  
**dns server** コマンドに指定したサーバーから返事がない場合には、相手先への接続と DNS サーバーの通知取得が行われる。
- [ノート]        この機能を使用する場合には、**dns server pp** コマンドで指定された相手先情報に、**ppp ipcp msexton** の設定が必要である。  
DHCP サーバーから通知された DNS サーバーを使うときには、**dns server dhcp** コマンドを使う。
- [初期値]        DNS サーバーを通知してもらう相手先は設定されていない
- [設定例]        # pp select 2  
pp2# ppp ipcp msexton  
pp2# dns server pp 2

#### 14.6 DNS サーバーアドレスを取得する LAN インタフェースの設定

- [書式]        **dns server dhcp interface**  
**no dns server dhcp**
- [設定値]        ◦ *interface* ..... LAN インタフェース名
- [説明]        DNS サーバーアドレスを取得する LAN インタフェースを設定する。このコマンドで LAN インタフェース名が設定されていると、DNS で名前解決を行なうときに、指定した LAN インタフェースで DHCP サーバーから取得した DNS サーバーアドレスに対して問い合わせを行なう。DHCP サーバーから DNS サーバーアドレスを取得できなかった場合は名前解決を行なわない。  
**dns server** コマンドで DNS サーバーが明示的に指定されているか、**dns server select**、**dns server pp** コマンドの設定により問い合わせをする DNS サーバーが決められた場合には、その設定が優先される。
- [ノート]        この機能は指定した LAN インタフェースが DHCP クライアントとして動作していなければならない。
- [初期値]        LAN インタフェースは設定されていない

#### 14.7 プライベートアドレスに対する問い合わせを処理するか否かの設定

- [書式]        **dns private address spoof spoof**  
**no dns private address spoof [spoof]**
- [設定値]        ◦ *spoof*  
    • on ..... 処理する  
    • off ..... 処理しない

- [ 説明 ] on の場合、DNS リカーシブサーバー機能で、プライベートアドレスの PTR レコードに対する問い合わせに対し、上位サーバーに問い合わせを転送することなく、自分でその問い合わせに対し “NXDomain”、すなわち「そのようなレコードはない」というエラーを返す。
- [ 初期値 ] off

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

- [ 書式 ] **dns notice order protocol server [server]**  
**no dns notice order protocol [server [server]]**
- [ 設定値 ]
- *protocol*
    - dhcp ..... DHCP による通知
    - msxt ..... IPCP MS 拡張による通知
  - *server*
    - none ..... 一切通知しない
    - me ..... 本製品自身
    - server ..... **dns server** コマンドに設定したサーバー群
- [ 説明 ] DHCP や IPCP MS 拡張では DNS サーバーを複数通知できるが、それをどのような順序で通知するかを設定する。  
none を設定すれば、他の設定に関わらず DNS サーバーの通知を行わなくなる。me は本製品自身の DNS リカーシブサーバー機能を使うことを通知する。server では、**dns server** コマンドに設定したサーバー群を通知することになる。IPCP MS 拡張では通知できるサーバーの数が最大 2 に限定されているので、後ろに me が続く場合は先頭の 1 つだけと本製品自身を、server 単独で設定されている場合には先頭の 2 つだけを通知する。
- [ 初期値 ] dhcp me server  
msxt me server

#### 14.9 SYSLOG 表示で DNS により名前解決するか否かの設定

- [ 書式 ] **dns syslog resolv resolv**  
**no dns syslog resolv [resolv]**
- [ 設定値 ]
- *resolv*
    - on ..... 解決する
    - off ..... 解決しない
- [ 説明 ] SYSLOG 表示で DNS により名前解決するか否かを設定する。
- [ 初期値 ] off

#### 14.10 DNS 問い合わせの内容に応じた DNS サーバーの選択

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

- [ 設定値 ]
- *id* ..... DNS サーバー選択テーブルの番号
  - *server* ..... プライマリ DNS サーバーの IP アドレス
  - *server2* ..... セカンダリ DNS サーバーの IP アドレス
  - *type* ..... DNS レコードタイプ (省略時は a)
    - *a* ..... ホストの IP アドレス
    - *ptr* ..... IP アドレスの逆引き用のポインタ
    - *mx* ..... メールサーバー
    - *ns* ..... ネームサーバー
    - *cname* ..... 別名
    - *any* ..... すべてのタイプにマッチする
  - *query* ..... DNS 問い合わせの内容
    - *type* が a、mx、ns、cname の場合  
*query* はドメイン名を表す文字列であり、後方一致とする。例えば、"example.jp" であれば、www.example.jp などにマッチする。"." を指定するとすべてのドメイン名にマッチする。
    - *type* が ptr の場合  
*query* は IP アドレス (*ip\_address/masklen*) であり、*masklen* を省略したときは IP アドレスにのみマッチし、*masklen* を指定したときはネットワークアドレスに含まれるすべての IP アドレスにマッチする。DNS 問い合わせに含まれる .in-addr.arpa ドメインで記述された FQDN は、IP アドレスへ変換された後に比較される。すべての IP アドレスは指定できない。
  - *original-sender* ..... DNS 問い合わせの送信元の IP アドレスの範囲
  - *connection-pp* ..... DNS サーバーを選択する場合、接続状態を確認する接続相手先情報番号
  - *peer\_num* ..... IPCP により接続相手から通知される DNS サーバーを使う場合の接続相手先情報番号
  - *interface* ..... DHCP サーバーより取得する DNS サーバーを使う場合の LAN インタフェース名
  - *default-server* ..... *peer\_num* パラメータで指定した接続相手から DNS サーバーを獲得できなかったときに使う DNS サーバーの IP アドレス

[ 説明 ] DNS 問い合わせの解決を依頼する DNS サーバーとして、DNS 問い合わせの内容および DNS 問い合わせの送信元および回線の接続状態を確認する接続相手先情報番号と DNS サーバーとの組合せを複数登録しておき、DNS 問い合わせに応じてその組合せから適切な DNS サーバーを選択できるようにする。テーブルは小さい番号から検索され、DNS 問い合わせの内容に *query* がマッチしたら、その DNS サーバーを用いて DNS 問い合わせを解決しようとする。一度マッチしたら、それ以降のテーブルは検索しない。すべてのテーブルを検索してマッチするものがない場合には、**dns server** コマンドで指定された DNS サーバーを用いる。

reject キーワードを使用した書式の場合、*query* がマッチしたら、その DNS 問い合わせパケットを破棄し、DNS 問い合わせを解決しない。

restrict pp 節が指定されていると、*connection-pp* で指定した相手先が接続状態になっているかどうかサーバーの選択条件に追加される。相手先が接続状態になっていないとサーバーは選択されない。相手先が接続状態になっていて、かつ、他の条件もマッチしている場合に指定したサーバーが選択される。

## 14.11 静的 DNS レコードの登録

[ 書式 ]

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

- [ 設定値 ]
- *type* ..... 名前のタイプ
    - *a* ..... ホストの IPv4 アドレス
    - *aaaa* ..... ホストの IPv6 アドレス
    - *ptr* ..... IP アドレスの逆引き用のポインタ
    - *mx* ..... メールサーバー
    - *ns* ..... ネームサーバー
    - *cname* ..... 別名

○ *name, value*..... *type* パラメータによって以下のように意味が異なる

| <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               | IP アドレス     | FQDN         |
| mx                | FQDN        | FQDN         |
| ns                | FQDN        | FQDN         |
| cname             | FQDN        | FQDN         |

○ *fqdn* ..... ドメイン名を含んだホスト名

[ 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 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.example.jp 192.168.200.1
dns static ptr 192.168.200.2 pc2.example.jp
dns static cname mail.example.jp mail2.example.jp
```

## 14.12 DNS 問い合わせパケットの始点ポート番号の設定

[ 書式 ] **dns srcport** *srcport*  
**no dns srcport** [*srcport*]

[ 設定値 ] ○ *srcport* ..... 始点ポート番号 (1..65535)

[ 説明 ] DNS リカーシブサーバー機能で、自分が送信する DNS 問い合わせパケットの始点ポート番号を設定する。

[ 初期値 ] 53

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

[ 書式 ] **dns host** *host* [*host* [...]]  
**no dns host**

[ 設定値 ] ○ *host*

- any ..... すべてのホストからのアクセスを許可する
- lan ..... すべての LAN ポート側ネットワーク内ならば許可する
- lanN ..... ひとつの任意の LAN ポート側ネットワーク内ならば許可する (N はインタフェース番号)
- none ..... すべてのホストからのアクセスを禁止する
- DNS サーバーへアクセスを許可するホストの IP アドレス
- DNS サーバーへアクセスを許可するホストの IP アドレスの範囲 (ip\_address-ip\_address)

[ 説明 ] DNS サーバーへのアクセスを許可するホストを設定する。

[ ノート ] このコマンドで LAN インタフェースを指定した場合には、ネットワークアドレスと limited broadcast address を除く IP アドレスからのアクセスを許可する。  
指定した LAN インタフェースにプライマリアドレスもセカンダリアドレスも設定していなければ、アクセスを許可しない。

[ 初期値 ] any

## 15. 優先制御

優先制御の機能は、インタフェースに入力されたパケットの順序を入れ替えて別のインタフェースに出力します。これらの機能を使用しない場合には、パケットは入力した順番に処理されます。

優先制御は、クラス分けしたキューに優先順位をつけ、まず高位のキューを出力し、そのキューが空になると次の順位のキューのパケットを出力する、という処理を行ないます。

クラスは、**queue class filter** コマンドにより、パケットのフィルタリングと同様な定義でパケットを分類します。優先制御では 1 から 4 までのクラスが使用できます。クラスは番号が大きいくほど優先順位が高くなります。

パケットの処理アルゴリズムは、**queue interface type** コマンドにより、優先制御、単純 FIFOの中から選択します。これはインタフェースごとに選択することができます。

### 15.1 インタフェース速度の設定

|         |                                                                                                                                         |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------|
| [ 書式 ]  | <b>speed interface speed</b><br><b>no speed interface [speed]</b>                                                                       |
| [ 設定値 ] | <ul style="list-style-type: none"> <li>○ <i>interface</i> ..... LAN インタフェース名</li> <li>○ <i>speed</i> ..... インタフェース速度 (bit/s)</li> </ul> |
| [ 説明 ]  | 指定したインタフェースに対して、インタフェースの速度を設定する。                                                                                                        |
| [ ノート ] | <i>speed</i> パラメータの後ろに 'k' または 'M' をつけると、それぞれ kbit/s、Mbit/s として扱われる。                                                                    |
| [ 初期値 ] | なし                                                                                                                                      |

### 15.2 キューイングアルゴリズムタイプの選択

|         |                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ 書式 ]  | <b>queue interface type type</b><br><b>queue pp type type</b><br><b>no queue interface type type</b><br><b>no queue pp type [type]</b>                                                                                                                                                                                                                                                                                  |
| [ 設定値 ] | <ul style="list-style-type: none"> <li>○ <i>interface</i> ..... LAN インタフェース名</li> <li>○ <i>type</i> <ul style="list-style-type: none"> <li>• <i>fifo</i>..... First In, First Out 形式のキューイング</li> <li>• <i>priority</i> ..... 優先制御キューイング</li> </ul> </li> </ul>                                                                                                                                                          |
| [ 説明 ]  | 指定したインタフェースに対して、キューイングアルゴリズムタイプを選択する。<br><br><p><i>fifo</i> は最も基本的なキューである。<i>fifo</i> の場合、パケットは必ず先にルータに到着したのから送信される。パケットの順番が入れ替わることは無い。<i>fifo</i> キューにたまったパケットの数が <b>queue interface length</b> コマンドで指定した値を越えた場合、キューの再後尾、つまり最も最後に到着したパケットが破棄される。</p> <p><i>priority</i> は優先制御を行なう。<b>queue class filter</b> コマンドおよび <b>queue interface class filter list</b> コマンドでパケットをクラス分けし、送信待ちのパケットの中から最も優先順位の高いクラスのパケットを送信する。</p> |
| [ 初期値 ] | <i>fifo</i>                                                                                                                                                                                                                                                                                                                                                                                                             |

### 15.3 クラス分けのためのフィルタ設定

|        |                                                                                                                                                     |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| [ 書式 ] | <b>queue class filter num class ip src_addr [dest_addr [proto [src_port [dest_port]]]]</b><br><b>no queue class filter num class [protocol ...]</b> |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------|

## [ 設定値 ]

- *num* ..... クラスフィルタの識別番号 (1..100)
- *class* ..... クラス (1..16)
- *src\_addr* ..... IP パケットの始点 IP アドレス
  - xxx.xxx.xxx.xxx xxx
    - 十進数
    - \* (ネットマスクの対応するビットが 8 ビットとも 0 と同じ)
  - \* (すべての IP アドレスに対応)
- *dest\_addr*
  - IP パケットの終点 IP アドレス (*src\_addr* と同じ形式)
  - 省略時は一つの \* と同じ
- *proto* ..... フィルタリングするパケットの種類
  - プロトコルを表す十進数
  - プロトコルを表すニーモニック

|      |    |
|------|----|
| icmp | 1  |
| tcp  | 6  |
| udp  | 17 |

- 上項目のカンマで区切った並び (5 個以内)
- \* (すべてのプロトコル)
- established
- 省略時は \* と同じ。
- *src\_port* ..... UDP、TCP のソースポート番号
  - ポート番号を表す十進数
  - ポート番号を表すニーモニック (一部)

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

- 間に - をはさんだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。
- 上項目のカンマで区切った並び (10 個以内)
- \* (すべてのポート)
- 省略時は \* と同じ。
- *dest\_port* ..... UDP、TCP のデスティネーションポート番号

## [ 説明 ]

クラス分けのためのフィルタを設定する。

パケットフィルタに該当したパケットは、指定したクラスに分類される。このコマンドで設定したフィルタを使用するかどうか、あるいはどのような順番で適用するかは、各インタフェースにおける **queue interface class filter list** コマンドで設定する。

## 15.4 デフォルトクラスの設定

## [ 書式 ]

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

## [ 設定値 ]

- *interface* ..... LAN インタフェース名
- *class* ..... クラス (1..16)

## [ 説明 ]

インタフェースに対して、フィルタにマッチしないパケットをどのクラスに分類するかを指定する。

[ 初期値 ] 2

## 15.5 クラス分けフィルタの適用

---

- [ 書式 ]        **queue interface class filter list** *filter\_list*  
**queue pp class filter list** *filter\_list*  
**no queue interface class filter list** [*filter\_list*]  
**no queue pp class filter list** [*filter\_list*]
- [ 設定値 ]     ◦ *interface* ..... LAN インタフェース名  
◦ *filter\_list*..... 空白で区切られたクラスフィルタの並び
- [ 説明 ]        指定した LAN インタフェースまたは選択されている PP に対して、**queue class filter** コマンドで設定したフィルタを適用する順番を設定する。フィルタにマッチしなかったパケットは、**queue interface default class** コマンドで指定したデフォルトクラスに分類される。

## 15.6 クラス毎のキュー長の設定

---

- [ 書式 ]        **queue interface length** *len1* [*len2*..*len4*]  
**queue pp length** *len1* [*len2*..*len4*]  
**no queue interface length** [*len1* [*len2*..*len4*]]  
**no queue pp length** [*len1* [*len2*..*len4*]]
- [ 設定値 ]     ◦ *interface* ..... LAN インタフェース名  
◦ *len1*..*len4*..... クラス 1 からクラス 4 のキュー長 (1..10000)
- [ 説明 ]        インタフェースに対して、指定したクラスのキューに入ることのできるパケットの個数を指定する。設定を省略したクラスに関しては、最後に指定されたキュー長が残りのクラスにも適用される。
- [ 初期値 ]     40 (LAN)  
20 (PP)

## 15.7 MP インタリーブの設定

---

- [ 書式 ]        **ppp mp interleave** [*delay*] *switch*  
**no ppp mp interleave** [[*delay*] *switch*]
- [ 設定値 ]     ◦ *delay* ..... 遅延 (ミリ秒)  
◦ *switch*  
• **on**..... MP インタリーブを使用する  
• **off**..... MP インタリーブを使用しない
- [ 説明 ]        MP インタリーブを使用するかどうかを設定する。*delay* では、優先されるプロトコルで許容できる最大遅延を設定する。パケットをどのような大きさに分割するかは、*delay* の値と回線速度により決定される。
- [ ノート ]      *delay* で設定した遅延が保証されるわけではない。  
データの受信側でも同じ設定をしておかないと、効果が発揮されない。  
同時に圧縮は利用できない。圧縮を利用する設定の場合、この機能は無視されるので、以下の設定で圧縮を無効にしておく必要がある。
- ppp ccp type none**

```
[初期値] delay = 30
 switch = on

[設定例] # queue class filter 1 4 ip VOIP-GATEWAY * * * *
 # queue class filter 2 3 ip * * icmp * *
 # queue class filter 3 1 ip * * * * *
 # pp select 1
 # pp bind bri1
 # queue pp type priority
 # queue class filter list 1 2 3
 # isdn remote address call 03-123-4567
 # ppp mp use on
 # ppp mp interleave on
 # ppp mp maxlink 1
 # ppp ccp type none
 # pp enable 1
```



## 16. 連携機能

### 16.1 連携動作を行なうか否かの設定

- [書式]            **cooperation type role sw**  
**no cooperation type role [sw]**
- [設定値]        ◦ *type* ..... 連携動作タイプ
- *bandwidth-measuring* ..... 回線帯域検出
  - *load-watch* ..... 負荷監視通知
- *role* ..... 連携動作での役割
- *server* ..... サーバー側動作
  - *client* ..... クライアント側動作
- *sw*
- *on* ..... 機能を有効にする
  - *off* ..... 機能を無効にする
- [説明]            連携動作の機能毎の動作を設定する。
- [初期値]        すべての連携動作で *off*

### 16.2 連携動作で使用するポート番号の設定

- [書式]            **cooperation port port**  
**no cooperation port [port]**
- [設定値]        ◦ *port* ..... ポート番号
- [説明]            連携動作で使用する UDP のポート番号を設定する。連携動作で送出されるパケットの送信元ポート番号にこの番号を使用する。またこのポート番号宛のパケットを受信した場合には連携動作に関わるパケットとして処理する。
- [初期値]        59410

### 16.3 帯域測定で連携動作を行なう相手毎の動作の設定

- [書式]            **cooperation bandwidth-measuring remote id role address [option=value]**  
**no cooperation bandwidth-measuring remote id [role address [option=value]]**
- [設定値]        ◦ *id* ..... 相手先 ID 番号 (1-100)
- *role* ..... 連携動作での相手側の役割
- *server* ..... 相手側がサーバー側動作を行なう
  - *client* ..... 相手側がクライアント側動作を行なう
- *address* ..... 連携動作の相手側 IP アドレス
- *option* ..... オプション
- *apply* ..... 測定結果を LAN インタフェースの速度設定に反映させるか否か、'on' or 'off'
  - *port* ..... 相手側が使用する UDP のポート番号
  - *initial-speed* ..... 測定開始値 [bit/s]
  - *interval* ..... 定期監視間隔 (60-2147483647)[sec] or 'off'
  - *sensitivity* ..... 測定感度、'high', 'middle' or 'low'
  - *syslog* ..... 動作をログに残すか否か、'on' or 'off'
- [説明]            帯域測定で連携動作を行なう相手毎の動作を設定する。

[ノート] *role* パラメータで *client* を設定する場合には、オプションは *port* と *syslog* だけが設定できる。*server* を設定する場合にはすべてのオプションが設定できる。

*apply* オプションが *on* の場合、帯域測定の結果を相手先に向かう LAN インタフェースの **speed lan** コマンドの設定値に上書きする。

*initial-speed* オプションでは初期状態で測定を開始する速度を設定できる。パラメータの後ろに *'k'* または *'M'* をつけると、それぞれ *kbit/s*、*Mbit/s* として扱われる。

*interval* オプションでは、帯域測定が終了した後で帯域に変化がないか定期的に確認測定する間隔を設定できる。*'off'* を指定した場合には測定終了後の定期的な確認測定を行わない。

帯域の変動が頻繁にあったりパケットロスのある環境では、*sensitivity* オプションで測定感度を鈍くすることで、頻繁な設定変更を抑制したり測定完了までの時間を短縮することができる。

[初期値]

```

apply = on
port = 59410
initial-speed = 10000000
interval = 3600
sensitivity = high
syslog = off

```

## 16.4 負荷監視通知で連携動作を行なう相手毎の動作の設定

[書式] **cooperation load-watch remote id role address [option=value]**  
**no cooperation load-watch remote id role [address [option=value]]**

[設定値]

- *id* ..... 相手先 ID 番号 (1-100)
- *role* ..... 連携動作での相手側の役割
  - *server* ..... 相手側がサーバー側動作を行なう
  - *client* ..... 相手側がクライアント側動作を行なう
- *address* ..... 連携動作の相手側 IP アドレス
- *option* ..... オプション
  - *trigger* ..... サーバー動作として、クライアントに通知を行なう条件のトリガ定義番号、*'.'* で区切って複数の指定が可能、相手側動作をクライアントに設定する時にのみ可能
  - *control* ..... クライアント動作として、サーバーから通知を受けた時の制御動作定義番号、相手側動作をサーバーに設定する時にのみ可能
  - *port* ..... 相手側が使用する UDP のポート番号、相手側動作をクライアントに設定する時にのみ可能
  - *syslog* ..... 動作をログに残すか否か、*'on'* or *'off'*
  - *apply* ..... 負荷監視通知の結果を動作に反映させるかどうか、*'on'* or *'off'*

[説明] 負荷監視通知で連携動作を行なう相手毎の動作を設定する。

[ノート] *trigger* オプションと *port* オプションを利用できるのは *role* パラメータで *client* を設定する場合であり、*control* オプションが利用できるのは *role* パラメータで *server* を設定する場合である。複数のトリガを設定した場合、抑制要請の送信タイミングはそれぞれのトリガで個別に検出される。それらの送信タイミングが異なる時には抑制要請はそれぞれのタイミングで個別に送られ、送信タイミングが一致する時にはひとつの抑制要請となる。相手先に一度抑制解除が送られた後は、次に抑制要請を送信するまで抑制解除は送信しない。抑制要請を送信していないトリガ条件が抑制解除条件を満たしても抑制解除通知は送信しない。抑制制御を行っている最中に相手先情報が削除されると、制御対象のインタフェースの速度はその時点の設定が保持される。

## 16.5 負荷監視サーバーとしての動作トリガの設定

- [書式]            **cooperation load-watch trigger** *id point* high=*high* [, *count*] low=*low* [, *count*] [*option=value*]  
**no cooperation load-watch trigger** *id* [*point* high=*high* [, *count*] low=*low* [, *count*] [*option=value*]]
- [設定値]
- *id* ..... 相手先 ID 番号 (1-100)
  - *point* ..... 負荷監視対象ポイント
    - *interface* receive ..... インタフェースでの単位時間当たりの受信量を監視する  
値は 1 秒あたりのビット数で指定する
      - *interface* ..... LAN インタフェース名
    - *interface* overflow ..... LAN インタフェースでの単位時間当たりの受信オーバーフロー数と受信  
バッファエラー数の増加を監視し、値は回数で指定する
      - *interface* ..... LAN インタフェース名
  - *high* ..... 高負荷検出閾値
  - *low* ..... 負荷減少検出閾値
  - *count* ..... 通知を送出するに至る検出回数 (1-100)、省略時は 3
  - *option* ..... オプション
    - *interval* ..... 監視する間隔 (1-65535)[sec]、省略時は 10[sec]
    - *syslog* ..... 動作をログに残すか否か、'on' or 'off'、省略時は 'off'
- [説明]            機器の負荷を検出して相手側にトラフィック抑制要請を送出する条件を設定する。監視対象ポイントの負荷を単位時間毎に監視し、*high* に設定された閾値を上回ることを *count* 回数続けて検出すると抑制要請を送出する。この状態で閾値を上回る高負荷状態が続く限り、*count* の間隔で抑制要請を送出し続ける。同様に、*low* に設定された閾値を *count* 回数続けて下回って検出すると抑制解除を送出する。抑制解除は同じ相手に対して連続して送出不される。
- [ノート]            閾値を決定する際の参考値として、**show environment** や **show status lan** で表示される情報のほか、syslog オプションによりログに表示される値も利用できる。
- [設定例]
- ```
# cooperation load-watch trigger 2 lan2 receive high=80m,5 low=50m,1
```
- 単位時間内での LAN2 からの受信バイト数から受信速度を求め、その値が 80[Mbit/s] 以上であることが連続 5 回あれば抑制要請を送り、その後 50[Mbit/s] 以下であることが 1 度でも観測されれば抑制解除を送る。
- ```
cooperation load-watch trigger 3 lan2 overflow high=2,1 low=0,5
```
- 単位時間内での LAN2 での受信オーバーフロー数の増加を監視し、2 回検出されることが 1 度でもあれば抑制要請を送り、検出されないことが 5 回続けば抑制解除を送る。



## 17. IPv6

### 17.1 共通の設定

#### 17.1.1 IPv6 パケットを扱うか否かの設定

---

- [書式]        **ipv6 routing** *routing*  
**no ipv6 routing** [*routing*]
- [設定値]     ◦ *routing*
- on..... 処理対象として扱う
  - off..... 処理対象として扱わない
- [説明]        IPv6 パケットをルーティングするか否かを設定する。本スイッチを on にしないと PP 側の IPv6 関連は一切動作しない。  
off の場合でも TELNET による設定や TFTP によるアクセス、PING 等は可能。
- [初期値]     on

#### 17.1.2 IPv6 インタフェースのリンク MTU の設定

---

- [書式]        **ipv6 interface mtu** *mtu*  
**ipv6 pp mtu** *mtu*  
**no ipv6 interface mtu** *mtu*  
**no ipv6 pp mtu** *mtu*
- [設定値]     ◦ *interface* ..... LAN インタフェース名  
◦ *mtu* ..... MTU の値 (1280..1500)
- [説明]        IPv6 インタフェースのリンク MTU を設定する。
- [初期値]     1500

#### 17.1.3 TCP セッションの MSS 制限の設定

---

- [書式]        **ipv6 interface tcp mss limit** *mss*  
**ipv6 pp tcp mss limit** *mss*  
**ipv6 tunnel tcp mss limit** *mss*  
**no ipv6 interface tcp mss limit** [*mss*]  
**no ipv6 pp tcp mss limit** [*mss*]  
**no ipv6 tunnel tcp mss limit** [*mss*]
- [設定値]     ◦ *interface* ..... LAN インタフェース名  
◦ *mss*
- MSS の最大長 (536 .. 1440)
  - auto..... 自動設定
  - off..... 設定しない
- [説明]        インタフェースを通過する TCP セッションの MSS を制限する。インタフェースを通過する TCP パケットを監視し、MSS オプションの値が設定値を越えている場合には、設定値に書き換える。キーワード auto を指定した場合には、インタフェースの MTU、もしくは PP インタフェースの場合で相手の MRU 値が分かる場合にはその MRU 値から計算した値に書き換える。
- [ノート]      PPPoE 用の PP インタフェースに対しては、**pppoe tcp mss limit** コマンドでも TCP セッションの MSS を制限することができる。このコマンドと **pppoe tcp mss limit** コマンドの両方が有効な場合は、MSS はどちらかより小さな方の値に制限される。
- [初期値]     off

## 17.2 IPv6 アドレスの管理

## 17.2.1 インタフェースの IPv6 アドレスの設定

[ 書式 ]

```

ipv6 interface address address/prefix_len
ipv6 interface address auto
ipv6 pp address address/prefix_len
ipv6 tunnel address address/prefix_len
no ipv6 interface address address/prefix_len
no ipv6 interface address auto
no ipv6 pp address address/prefix_len
no ipv6 tunnel address address/prefix_len

```

[ 設定値 ]

- *interface* ..... LAN インタフェース名
- *address*
  - IPv6 アドレス
  - *prefix\_type@prefix\_interface:interface\_id*
    - *prefix\_type*
      - *ra-prefix* ..... RA で取得したプレフィックスを使用する
      - *dhcp-prefix* ..... DHCPv6-PD で取得したプレフィックスを使用する
      - *dtcp-prefix* ..... DTCP で取得したプレフィックスを使用する
    - *prefix\_interface* ..... プレフィックスを取得するインタフェース
    - *interface\_id* ..... インタフェース識別子
- *prefix\_len* ..... プレフィックス長
- *auto* ..... LAN インタフェースの自動設定を行なうことを示すキーワード

[ 説明 ]

インタフェースに IPv6 アドレスを付与する。  
*prefix\_type@prefix\_interface:interface\_id* が指定された場合には、取得したプレフィックスとインタフェース識別子により、IPv6 アドレスが決定される。

[ ノート ]

このコマンドで付与したアドレスは、**show ipv6 address** コマンドで確認することができる。  
 複数の LAN インタフェースで自動設定機能を利用することができる。その場合、デフォルト経路は最後に自動設定が完了したインタフェースに向く。

## 17.2.2 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 prefix/prefix_len
ipv6 pp prefix prefix/prefix_len
ipv6 tunnel prefix prefix/prefix_len
no ipv6 interface prefix prefix/prefix_len
no ipv6 pp prefix prefix/prefix_len
no ipv6 tunnel prefix prefix/prefix_len

```

[ 設定値 ]

- *interface* ..... LAN インタフェース名
- *prefix*
  - IPv6 プレフィックス
  - *prefix\_type@prefix\_interface::*
    - *prefix\_type*
      - *ra-prefix* ..... RA で取得したプレフィックスを使用する
      - *dhcp-prefix* ..... DHCPv6-PD で取得したプレフィックスを使用する
      - *dtcp-prefix* ..... DTCP で取得したプレフィックスを使用する
    - *prefix\_interface* ..... プレフィックスを取得するインタフェース
- *prefix\_len* ..... プレフィックス長

[ 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。

*prefix\_type@prefix\_interface::* が指定された場合には、取得したプレフィックスがインタフェースのプレフィックスとして使用される。

[ノート] このコマンドで設定された IPv6 アドレスは **show ipv6 address** コマンドで確認できる。

### 17.2.3 DHCPv6 の動作の設定

- [書式] **ipv6 interface dhcp service type**  
**ipv6 pp dhcp service type**  
**ipv6 tunnel dhcp service type**  
**no ipv6 interface dhcp service**  
**no ipv6 pp dhcp service**  
**no ipv6 tunnel dhcp service**
- [設定値]    ◦ *interface* ..... LAN インタフェース名  
               ◦ *type*  
               • *off* ..... DHCPv6 を使わない  
               • *client* ..... クライアント
- [説明]       各インタフェースにおける DHCPv6 の動作を設定する。
- [初期値]     *off*

### 17.2.4 IPv6 で DAD(Duplicate Address Detection) の送信回数を設定する

- [書式] **ipv6 interface dad retry count count**  
**ipv6 pp dad retry count count**  
**no ipv6 interface dad retry count [count]**  
**no ipv6 pp dad retry count [count]**
- [設定値]    ◦ *interface* ..... LAN インタフェース名  
               ◦ *count* ..... 選択したインタフェースでの DAD の再送回数 (0..10)
- [説明]       インタフェースに IPv6 アドレスが設定されたときに、アドレスの重複を検出するために送信する DAD の送信回数を設定する。ただし、0 を設定した場合は、DAD を送信せずにアドレスを有効なものとして扱う。
- [初期値]     1

## 17.3 近隣探索

### 17.3.1 ルータ広告で配布するプレフィックスの定義

- [書式] **ipv6 prefix prefix\_id prefix/prefix\_len [valid\_lifetime=time] [preferred\_lifetime=time] [l\_flag=switch] [a\_flag=switch]**  
**no ipv6 prefix prefix\_id**
- [設定値]    ◦ *prefix\_id* ..... プレフィックス番号  
               ◦ *prefix* ..... プレフィックス  
               • IPv6 プレフィックス

- *prefix\_type@prefix\_interface::*
  - *prefix\_type*
    - *ra-prefix* ..... RA で取得したプレフィックスを使用する
    - *dhcp-prefix* ..... DHCPv6-PD で取得したプレフィックスを使用する
    - *dtcp-prefix* ..... DTCP で取得したプレフィックスを使用する
  - *prefix\_interface* ..... プレフィックスを取得するインターフェース
- *prefix\_len* ..... プレフィックス長
- *valid\_lifetime* ..... プレフィックスの有効寿命 (60..15552000)
- *preferred\_lifetime* ..... プレフィックスの推奨寿命 (60..15552000)
- *time* ..... 時間設定
  - *YYYY-MM-DD,bh:mm[:ss]*
    - *YYYY* ..... 年 (1980..2079)
    - *MM* ..... 月 (01..12)
    - *DD* ..... 日 (01..31)
    - *hh* ..... 時 (00..23)
    - *mm* ..... 分 (00..59)
    - *ss* ..... 秒 (00..59、省略時は 00)
- *l\_flag* ..... on-link フラグ
- *a\_flag* ..... autonomous address configuration フラグ
- *switch*
  - on
  - off

[ 説明 ] ルータ広告で配布するプレフィックスを定義する。実際に広告するためには、**ipv6 interface rtadv prefix** コマンドの設定が必要である。  
*time* では寿命を秒数または寿命が尽きる時刻のいずれかを設定できる。*time* として数値 (60 以上 15552000 以下) を設定すると、その秒数を寿命として広告する。*time* として時刻を設定すると、その時刻に寿命が尽きるものとして寿命を計算し、広告する。時刻を設定する場合は、上記のフォーマットに従う。有効寿命とはアドレスが無効になるまでの時間であり、推奨寿命とはアドレスを新たな接続での使用が不可となる時間である。また、on-link フラグはプレフィックスがそのデータリンクに固有である時に on とする。autonomous address configuration フラグはプレフィックスを自律アドレス設定で使うことができる場合に on とする。

*prefix\_type@prefix\_interface::* が指定された場合には、取得したプレフィックスをルータ広告で配布する。

[ ノート ] リンクローカルのプレフィックスを設定することはできない。

[ 初期値 ]  
 valid\_lifetime = 2592000  
 preferred\_lifetime = 604800  
 l\_flag = on  
 a\_flag = on

### 17.3.2 ルータ広告の送信の制御

[ 書式 ]  
**ipv6 interface rtadv send prefix\_id [prefix\_id...] [parameters...]**  
**ipv6 pp rtadv send prefix\_id [prefix\_id...] [parameters...]**  
**ipv6 interface rtadv send**  
**no ipv6 interface rtadv send**

[ 設定値 ]  
 ◦ *interface* ..... LAN インタフェース名  
 ◦ *prefix\_id* ..... プレフィックス番号  
 ◦ *parameters* ..... NAME=VALUE の列

[ 説明 ] インタフェースごとにルータ広告の送信を制御する。  
 送信されるプレフィックスとして、**ipv6 prefix** コマンドで設定されたものが用いられる。  
*m\_flag* および *o\_flag* を指定することにより、管理するホストがルータ広告以外のステートフル自動設定情報をどのように解釈するかを設定できる。



また、`max-rtr-adv-interval` および `min-rtr-adv-interval` を指定することによりルータ広告の送信間隔の範囲を、`adv-default-lifetime` を指定することによりルータ広告を送信したルータをデフォルトルータとして使用できる有効時間を、`adv-reachable-time` を指定することによりノード間で確認する到達性の有効時間を、それぞれ設定できる。

これらのパラメータは `NAME=VALUE` の形で指定される。

| NAME                              | VALUE           | 説明                                                                                                                                                                                                                                       |
|-----------------------------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>m_flag</code>               | on/off          | managed address configuration フラグ。<br>ルータ広告 (RA) による自動設定とは別に、DHCPv6 に代表される RA 以外の手段によるアドレス自動設定をホストに許可するか否かを設定する。<br><ul style="list-style-type: none"> <li>• on ..... 許可しない</li> <li>• off ..... 許可する (許可しても RA による自動設定は行われる)</li> </ul> |
| <code>o_flag</code>               | on/off          | other stateful configuration フラグ。<br>ルータ広告以外の手段により IPv6 アドレス以外のオプション情報をホストに自動的に取得させるか否かを設定する。<br><ul style="list-style-type: none"> <li>• on ..... 取得させない</li> <li>• off ..... 取得させる</li> </ul>                                          |
| <code>max-rtr-adv-interval</code> | 秒数              | ルータ広告 (RA) の最大送信間隔を指定する。<br>設定可能範囲は 4 ~ 1800 秒。                                                                                                                                                                                          |
| <code>min-rtr-adv-interval</code> | 秒数              | ルータ広告 (RA) の最小送信間隔を指定する。<br>設定可能範囲は 3 ~ 1350 秒。                                                                                                                                                                                          |
| <code>adv-default-lifetime</code> | 秒数              | Router Lifetime フィールド。<br>ルータ広告を送信したルータをデフォルトルータとして使用できる有効時間を指定する。<br>設定可能範囲は 0 ~ 9000 秒。                                                                                                                                                |
| <code>adv-reachable-time</code>   | ミリ秒             | Reachable Time フィールド。<br>ノード間で確認する到達性の有効時間を指定する。<br>設定可能範囲は 0 ~ 3600000 ミリ秒。                                                                                                                                                             |
| <code>mtu</code>                  | auto, off, バイト数 | ルータ広告に MTU オプションを含めるか否かと、含める場合の設定。<br>auto の場合はインタフェースの MTU を採用する。                                                                                                                                                                       |

[初期値]

```

m_flag = off
o_flag = off
max-rtr-adv-interval=600
min-rtr-adv-interval=200
adv-default-lifetime=1800
adv-reachable-time=0
mtu=auto

```

## 17.4 経路制御

### 17.4.1 IPv6 の経路情報の追加

[書式] **ipv6 route** *network* gateway *gateway* [*parameter*] [*gateway gateway* [*parameter*]]  
**no ipv6 route** *network*

[説明]

- *network*
  - IPv6 アドレス / プレフィックス長
  - default..... デフォルト経路
- *gateway* ..... ゲートウェイ
  - IP アドレス % スコープ識別子
  - pp *peer\_num* ..... PP インタフェースへの経路
    - *peer\_num*
      - 相手先情報番号
      - anonymous
  - pp anonymous name=*name*
    - *name*..... PAP/CHAP による名前
  - tunnel *tunnel\_num* ..... トンネルインタフェースへの経路

- *parameter*.....以下のパラメータを空白で区切り複数設定可能
  - *metric metric*.....メトリックの指定
    - *metric* .....メトリック値 (1..15) (省略時は 1)
  - *hide*.....出力インタフェースが PP インタフェースの場合のみ有効なオプションで、回線が接続されている場合だけ経路が有効になることを意味する

[ 説明 ] IPv6 の経路情報を追加する。LAN インタフェースが複数ある機種ではスコープ識別子でインタフェースを指定する必要がある。インタフェースに対応するスコープ識別子は **show ipv6 address** コマンドで表示される。LAN インタフェースがひとつである機種に関しては、スコープ識別子が省略されると LAN1 が指定されたものとして扱う。

## 17.5 RIPng

### 17.5.1 RIPng の使用の設定

[ 書式 ] **ipv6 rip use use**  
**no ipv6 rip use**

[ 設定値 ] ○ *use*  
 • *on*.....RIPng を使う  
 • *off* .....RIPng を使わない

[ 説明 ] RIPng を使うか否かを設定する。

[ 初期値 ] off

### 17.5.2 インタフェースにおける RIPng の送信ポリシーの設定

[ 書式 ] **ipv6 interface rip send send**  
**ipv6 pp rip send send**  
**ipv6 tunnel rip send send**  
**no ipv6 interface rip send**  
**no ipv6 pp rip send**  
**no ipv6 tunnel rip send**

[ 設定値 ] ○ *interface* ..... LAN インタフェース名  
 ○ *send*  
 • *on*.....RIPng を送信する  
 • *off* .....RIPng を送信しない

[ 説明 ] RIPng の送信ポリシーを設定する。

[ 初期値 ] on

### 17.5.3 インタフェースにおける RIPng の受信ポリシーの設定

[ 書式 ] **ipv6 interface rip receive receive**  
**ipv6 pp rip receive receive**  
**ipv6 tunnel rip receive receive**  
**no ipv6 interface rip receive**  
**no ipv6 pp rip receive**  
**no ipv6 tunnel rip receive**

[ 設定値 ] ○ *interface* ..... LAN インタフェース名  
 ○ *receive*  
 • *on*.....受信した RIPng パケットを処理する  
 • *off* .....受信した RIPng パケットを無視する

[ 説明 ] RIPng の受信ポリシーを設定する。

[ 初期値 ] on

### 17.5.4 RIPng の加算ホップ数の設定

- [書式] **ipv6 interface rip hop direction hop**  
**ipv6 pp rip hop direction hop**  
**no ipv6 interface rip hop**  
**no ipv6 pp rip hop**
- [設定値] ○ *interface* ..... LAN インタフェース名  
 ○ *direction*  
   • *in* ..... 受信時に加算する  
   • *out* ..... 送信時に加算する  
 ○ *hop* ..... 加算ホップ数 (0..15)
- [説明] インタフェースで送受信する RIPng のメトリックに対して加算するホップ数を設定する。
- [初期値] 0

### 17.5.5 インタフェースにおける信頼できる RIPng ゲートウェイの設定

- [書式] **ipv6 interface rip trust gateway [except] gateway [gateway ...]**  
**ipv6 pp rip trust gateway [except] gateway [gateway ...]**  
**no ipv6 interface rip trust gateway**  
**no ipv6 pp rip trust gateway**
- [設定値] ○ *interface* ..... LAN インタフェース名  
 ○ *gateway* ..... IPv6 アドレス
- [説明] 信頼できる RIPng ゲートウェイを設定する。  
 except キーワードを指定していない場合には、列挙したゲートウェイを信用できるゲートウェイとし、それらからの RIP だけを受信する。  
 except キーワードを指定した場合は、列挙したゲートウェイを信用できないゲートウェイとし、それらを除いた他のゲートウェイからの RIP だけを受信する。

### 17.5.6 RIPng で送受信する経路に対するフィルタリングの設定

- [書式] **ipv6 interface rip filter direction filter\_list [filter\_list...]**  
**ipv6 pp rip filter direction filter\_list [filter\_list...]**  
**ipv6 tunnel rip filter direction filter\_list [filter\_list...]**  
**no ipv6 interface rip filter**  
**no ipv6 pp rip filter**  
**no ipv6 tunnel rip filter**
- [設定値] ○ *interface* ..... LAN インタフェース名  
 ○ *direction*  
   • *in* ..... 内向きのパケットを対象にする  
   • *out* ..... 外向きのパケットを対象にする  
 ○ *filter\_list* ..... フィルタ番号
- [説明] インタフェースで送受信する RIPng パケットに対して適用するフィルタを設定する。
- [初期値] フィルタは設定されていない

### 17.5.7 回線接続時の PP 側の RIPng の動作の設定

- [書式] **ipv6 pp rip connect send action**  
**no ipv6 pp rip connect send**
- [設定値] ○ *action*  
   • *interval* ..... **ipv6 pp rip connect interval** コマンドで設定された時間間隔で RIPng を送出する  
   • *update* ..... 経路情報が変わった時にのみ RIPng を送出する  
   • *none* ..... RIPng を送信しない
- [説明] 選択されている相手について回線接続時に RIP を送出する条件を設定する。

- [ 初期値 ]        update
- [ 設定例 ]        # ipv6 pp rip connect interval 60  
# ipv6 pp rip connect send interval

### 17.5.8 回線接続時の PP 側の RIPng 送出の時間間隔の設定

---

- [ 書式 ]            **ipv6 pp rip connect interval time**  
**no ipv6 pp rip connect interval**
- [ 設定値 ]        ◦ *time*..... 秒数 (30..21474836)
- [ 説明 ]            選択されている相手について回線接続時に RIP を送出する時間間隔を設定する。
- [ 初期値 ]        30
- [ 設定例 ]        # ipv6 pp rip connect interval 60  
# ipv6 pp rip connect send interval

### 17.5.9 回線切断時の PP 側の RIPng の動作の設定

---

- [ 書式 ]            **ipv6 pp rip disconnect send action**  
**no ipv6 pp rip disconnect send**
- [ 設定値 ]        ◦ *action*
- none..... RIPng を送信しない
  - interval ..... **ipv6 pp rip disconnect interval** コマンドで設定された時間間隔で RIPng を送出する
  - update..... 経路情報が変わった時にのみ RIPng を送信する
- [ 説明 ]            選択されている相手について回線切断時に RIP を送出する条件を設定する。
- [ 初期値 ]        none
- [ 設定例 ]        # ipv6 pp rip disconnect interval 1800  
# ipv6 pp rip disconnect send interval

### 17.5.10 回線切断時の PP 側の RIPng 送出の時間間隔の設定

---

- [ 書式 ]            **ipv6 pp rip disconnect interval time**  
**no ipv6 pp rip disconnect interval**
- [ 設定値 ]        ◦ *time*..... 秒数 (30..21474836)
- [ 説明 ]            選択されている相手について回線切断時に RIP を送出する時間間隔を設定する。
- [ 初期値 ]        3600
- [ 設定例 ]        # ipv6 pp rip disconnect interval 1800  
# ipv6 pp rip disconnect send interval

### 17.5.11 RIPng による経路を回線切断時に保持するか否かの設定

---

- [ 書式 ]            **ipv6 pp rip hold routing hold**  
**no ipv6 pp rip hold routing**
- [ 設定値 ]        ◦ *hold*
- on..... 保持する
  - off ..... 保持しない
- [ 説明 ]            PP インタフェースから RIPng で得られた経路を、回線が切断されたときに保持するか否かを設定する。
- [ 初期値 ]        off

## 17.6 フィルタの設定

### 17.6.1 IPv6 フィルタの定義

- [書式] **ipv6 filter** *filter\_num* *pass\_reject* *src\_address*[/*prefix\_len*] [*dst\_address*[/*prefix\_len*]] [*protocol* [*src\_port\_list* [*dst\_port\_list*]]]
- no ipv6 filter** *filter\_num*
- [設定値]
- *filter\_num* ..... 静的フィルタ番号 (1..21474836)
  - *pass\_reject* ..... フィルタのタイプ (**ip filter** コマンドに準ずる)
  - *src\_address*
    - 始点 IPv6 アドレス
    - *prefix\_type@prefix\_interface:interface\_id*
      - *prefix\_type*
        - *ra-prefix* ..... RA で取得したプレフィックスを使用する
        - *dhcp-prefix* ..... DHCPv6-PD で取得したプレフィックスを使用する
        - *dtcp-prefix* ..... DTCP で取得したプレフィックスを使用する
      - *prefix\_interface* ..... プレフィックスを取得するインターフェース
      - *interface\_id* ..... インタフェース識別子
  - *prefix\_len* ..... プレフィックス長
  - *dst\_address*
    - 終点 IPv6 アドレス
    - *prefix\_type@prefix\_interface:interface\_id* (*src\_address* と同じ形式)
    - 省略時は 1 個の \* と同じ。
  - *protocol*
    - フィルタリングするパケットの種類 (**ip filter** コマンドに準ずる)
    - *icmp-nd* ..... 近隣探索に関するパケットの指定を示すキーワード
  - *src\_port\_list* ..... UDP、TCP のソースポート番号 (**ip filter** コマンドに準ずる)
  - *dst\_port\_list* ..... UDP、TCP のデスティネーションポート番号

[説明] IPv6 のフィルタを定義する。

*prefix\_type@prefix\_interface:interface\_id* が指定された場合には、取得したプレフィックスとインタフェース識別子により、IPv6 アドレスが決定される。

[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。

- neighbor advertisement
- neighbor solicitation
- router advertisement
- router solicitation

### 17.6.2 IPv6 フィルタの適用

- [書式] **ipv6 interface secure filter** *direction* *filter\_list* [*filter\_list...*]
- ipv6 pp secure filter** *direction* *filter\_list* [*filter\_list...*]
- ipv6 tunnel secure filter** *direction* *filter\_list* [*filter\_list...*]
- no ipv6 interface secure filter** *direction*
- no ipv6 pp secure filter** *direction*
- no ipv6 tunnel secure filter** *direction*

- [設定値]
- *interface* ..... LAN インタフェース名
  - *direction*
    - *in* ..... 内向きのパケットを対象にする
    - *out* ..... 外向きのパケットを対象にする
  - *filter\_list* ..... 静的フィルタ番号

[説明] IPv6 フィルタをインタフェースに適用する。

## 17.6.3 IPv6 動的フィルタの定義

- [書式] **ipv6 filter dynamic** *dyn\_filter\_num srcaddr dstaddr protocol* [*option ...*]  
**ipv6 filter dynamic** *dyn\_filter\_num srcaddr dstaddr filter filter\_list* [*in filter\_list*] [*out filter\_list*] [*option ...*]  
**no ipv6 filter dynamic** *dyn\_filter\_num* [*dyn\_filter\_num...*]
- [設定値]
- *dyn\_filter\_num* ..... 動的フィルタ番号 (1..21474836)
  - *src\_address*
    - 始点 IPv6 アドレス
    - *prefix\_type@prefix\_interface:interface\_id*
      - *prefix\_type*
        - *ra-prefix*..... RA で取得したプレフィックスを使用する
        - *dhcp-prefix*..... DHCPv6-PD で取得したプレフィックスを使用する
        - *dtcp-prefix*..... DTCP で取得したプレフィックスを使用する
      - *prefix\_interface*..... プレフィックスを取得するインターフェース
      - *interface\_id*..... インタフェース識別子
  - *prefix\_len*..... プレフィックス長
  - *dst\_address*
    - 終点 IPv6 アドレス
    - *prefix\_type@prefix\_interface:interface\_id* (*src\_address* と同じ形式)
    - 省略時は 1 個の \* と同じ
  - *protocol* ..... プロトコル
    - tcp
    - udp
    - ftp
    - tftp
    - domain
    - www
    - smtp
    - pop3
    - telnet
  - *filter\_list*..... **ipv6 filter** コマンドで登録されたフィルタ番号のリスト
  - *option*
    - *syslog=switch*
      - *on*..... コネクションの通信履歴を syslog に残す
      - *off*..... コネクションの通信履歴を syslog に残さない
    - *timeout=time*
      - *time*..... データが流れなくなったときにコネクション情報を解放するまでの秒数
- [説明] IPv6 の動的フィルタを定義する。第 1 書式では、あらかじめルータ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に扱いは容易である。*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。
- prefix\_type@prefix\_interface:interface\_id* が指定された場合には、取得したプレフィックスとインタフェース識別子により、IPv6 アドレスが決定される。
- [初期値] *syslog* = on  
*timeout* = 60

## 17.7 IPv6 マルチキャストパケットの転送の設定

MLDv1、MLDv2、MLD プロキシの機能を提供します。MLDv1 と MLDv2 については、ホスト側とルータ側の双方に対応し、インタフェースごとにホストとルータの機能を使い分けすることができます。MLDv1 は RFC2710、MLDv2 は draft-vida-ml-d-v2-07.txt に対応します。MLD プロキシは、下流のインタフェースに存在するリスナーの情報を、上流のインタフェースに中継する機能であり、draft-ietf-magma-igmp-proxy-04.txt に基づいて実装しています。

マルチキャストは、マルチキャストのルーティングに対応した特別な網で実現されます。マルチキャスト網を構成するルータは、特定の端末が送信するマルチキャストパケットを複製して、複数の端末に配送します。マルチキャストパケットを送信する端末をソース (source) と呼び、それを受信する端末をリスナー (listener) と呼びます。以下の説明では、マルチキャストパケットを単にパケットと書きます。

ソースが送信するパケットは原則としてすべてのリスナーに届きます。しかし、リスナーによって受信するパケットを変えたいければ、リスナーをグループに分けることができます。同じグループに属する端末は同じパケットを受信し、異なるグループに属する端末は異なるパケットを受信します。それぞれのグループには識別子としてマルチキャストアドレスが割り当てられます。

パケットの IP ヘッダの終点アドレスには、グループに対応するマルチキャストアドレスが格納されます。網内のルータは、このマルチキャストアドレスを見て、パケットの転送先のグループを確認します。網内のルータはグループごとに編成された経路表を持っているので、その経路表にしたがってパケットを配布します。経路表は、通常、PIM-SM、PIM-DM、DVMRP などのルーティングプロトコルによって自動的に生成されます。

MLD (Multicast Listener Discovery) の目的は、端末がマルチキャスト網に対して、端末が参加するグループを通知することです。

網内のルータは端末に対してクエリー (Query) というメッセージを送信します。クエリーを受信した端末は、ルータに対してレポート (Report) というメッセージを返信します。レポートの中には、端末が参加するグループのマルチキャストアドレスを格納します。レポートを受信したルータはその情報をルーティングに反映します。

MLDv2 では、受信するパケットのソースを制限することができますが、この機能を実現するためにフィルタモード (Filter Mode) とソースリスト (Source List) を使用します。フィルタモードには INCLUDE と EXCLUDE があり、INCLUDE では許可するソースを列挙し、EXCLUDE では許可しないソースを列挙します。

例えば、次の場合には、2001:x:x::1 と 2001:x:x::2 をソースとするパケットだけが転送の対象になります。

- フィルタモード: INCLUDE
- ソースリスト: { 2001:x:x::1, 2001:x:x::2 }

MLD のメッセージは原則としてルータを超えることができません。そこで、端末とマルチキャスト網の間にルータが介入する場合には、ルータが MLD プロキシの機能を持つ必要があります。MLD プロキシの機能を持つルータは、LAN 側に対してクエリーを送信し、LAN 側からレポートを受信します。また、そのレポートに含まれる情報を WAN 側に転送します。

### 17.7.1 MLD の動作の設定

[ 書式 ]

```

ipv6 interface mld type [option ...]
ipv6 pp mld type [option ...]
ipv6 tunnel mld type [option ...]
no ipv6 interface mld [type [option ...]]
no ipv6 pp mld [type [option ...]]
no ipv6 tunnel mld [type [option ...]]

```

[ 設定値 ]

- *interface* ..... LAN インタフェース名
- *type* ..... MLD の動作方式
  - *off* ..... MLD は動作しない
  - *router* ..... MLD ルータとして動作する
  - *host* ..... MLD ホストとして動作する
- *option* ..... オプション
  - *version=version* ... MLD のバージョン
    - 1 ..... MLDv1
    - 2 ..... MLDv2
    - 1,2 ..... MLDv1 と MLDv2 の両方に対応する。(MLDv1 互換モード)
  - *syslog=switch* ..... 詳細な情報を syslog に出力するか否か
    - *on* ..... 表示する
    - *off* ..... 表示しない
  - *robust-variable=VALUE* (1 .. 10)
    - MLD で規定される Robust Variable の値を設定する。

[ 説明 ] インタフェースの MLD の動作を設定する。

[ 初期値 ]

```

type=off
version=1,2
syslog=off
robust-variable=2

```

## 17.7.2 MLD の静的な設定を登録するコマンド

- [書式] **ipv6 interface mld static** *group* [*filter\_mode* *source* ...]  
**ipv6 pp mld static** *group* [*filter\_mode* *source* ...]  
**ipv6 tunnel mld static** *group* [*filter\_mode* *source* ...]  
**no ipv6 interface mld static** [*group* [*filter\_mode* *source* ...]]  
**no ipv6 pp mld static** [*group* [*filter\_mode* *source* ...]]  
**no ipv6 tunnel mld static** [*group* [*filter\_mode* *source* ...]]
- [設定値]
- *interface* ..... LAN インタフェース名
  - *group* ..... グループのマルチキャストアドレス
  - *filter\_mode* ..... フィルタモード
    - *include*..... MLD の "INCLUDE" モード
    - *exclude*..... MLD の "EXCLUDE" モード
  - *source* ..... マルチキャストパケットの送信元のアドレス
- [説明] 指定したグループについて、常にリスナーが存在するものとみなす。  
このコマンドは、MLD をサポートするリスナーがないときに設定する。  
*filter\_mode* と *source* は、マルチキャストパケットの送信元を限定するものである。*filter\_mode* として *include* を指定したときには、*source* として受信したい送信元を列挙する。*filter\_mode* として *exclude* を指定したときには、*source* として受信したくない送信元を列挙する。
- [ノート] このコマンドで設定されたリスナーは、**ipv6 interface mld** コマンドで *host* を設定したインタフェースで通知される。もし、このインタフェースが MLDv1 を使う場合には、*filter\_mode* や *source* の値は無視される。



## 18. アナログ通信機能の設定

本製品のアナログ通信機能の設定は、TEL ポートに接続した PB 電話機のキー操作でも可能ですが、ここではコンソールからのコマンドについてだけ述べます。キー操作による設定手順は活用マニュアルを参照してください。キー操作とコンソールコマンドの対応表は本ページに示します。

TEL ポートには、**識別着信リスト**と呼ぶリストがあり、このリストに一致した着信だけを許可したり拒否したりすることができます。識別着信リストへの登録は **analog arrive restrict list** コマンド、削除は **no analog arrive restrict list** コマンドで行ないます。実際の許可拒否動作はポート毎に行なうことができ、**analog arrive restrict** コマンドにより動作を指定します。

本製品の TEL ポートの電気的入出力レベルは調節することができます。受話器からの音声が大きくて耳障りな音になったり、モデムや FAX の通信がうまくいかない場合には、**analog pad send**、**analog pad receive** コマンドで送話と受話レベルを調節し、最適な状態にします。

アナログ通信機器の発着信回数は **show account analog** コマンドで知ることができます。

### 18.1 キー操作とコンソールコマンドの対応

#### TEL ポート ( 機器 ) 側の設定

| 機能                          | 機能番号 | 対応するコンソールコマンド                                               |
|-----------------------------|------|-------------------------------------------------------------|
| TEL ポートのダイヤル番号設定            | 11   | <b>analog local address</b>                                 |
| TEL ポートのサブアドレス設定            | 12   | <b>analog local address</b>                                 |
| 通信機器の種類設定                   | 13   | <b>analog device type</b>                                   |
| TEL ポート使用制限の設定              | 14   | <b>analog use</b>                                           |
| 発信者番号通知                     | 21   | <b>analog local address notice</b>                          |
| 即時発信                        | 22   | <b>analog rapid call</b>                                    |
| ボースを判定する時間                  | 23   | <b>analog pause timer</b>                                   |
| グローバル着信                     | 31   | <b>analog arrive global permit</b>                          |
| 識別着信                        | 32   | <b>analog arrive restrict</b>                               |
| 識別着信の番号登録                   | 33   | <b>analog arrive restrict list</b>                          |
| サブアドレスなしの着信                 | 34   | <b>analog arrive without-subaddress permit</b>              |
| 通信機器種別指定の着信                 | 35   | <b>analog arrive another-device permit</b>                  |
| 話中着信                        | 36   | <b>analog arrive ring-while-talking permit</b>              |
| 優先着信ポート                     | 37   | <b>analog arrive priority</b>                               |
| 着信ベル設定                      | 38   | <b>analog arrive ringer-type list</b>                       |
| ナンバー・ディスプレイ機能               | 39   | <b>analog arrive number display</b>                         |
| ダイヤル桁の間隔設定 ( 秒 )            | 41   | <b>analog wait dial timer</b>                               |
| フッキング判定時間 ( 1/10 秒 )        | 42   | <b>analog hooking timer</b>                                 |
| フッキング後の操作有効時間 ( 秒 )         | 43   | <b>analog hooking wait timer</b>                            |
| フッキング、オンフック無効時間 ( 秒 )       | 44   | <b>analog hooking inhibit timer</b>                         |
| 擬似切断信号の設定                   | 45   | <b>analog disc-signal</b>                                   |
| INS キャッチホン機能 ( コールウェイトニング ) | 52   | <b>analog supplementary-service</b>                         |
| 通信中転送機能                     | 53   | <b>analog supplementary-service</b>                         |
| 三者通話機能                      | 54   | <b>analog supplementary-service</b>                         |
| 着信転送機能                      | 55   | <b>analog supplementary-service</b>                         |
| 着信転送先番号登録                   | 56   | <b>analog supplementary-service call-deflection address</b> |
| 着信転送トーク設定                   | 57   | <b>analog supplementary-service call-deflection talkie</b>  |
| 着信転送起動タイミング設定               | 58   | <b>analog supplementary-service call-deflection ringer</b>  |
| 着信転送失敗時の動作設定                | 59   | <b>analog supplementary-service call-deflection reject</b>  |
| 送話 PAD の音量設定                | 61   | <b>analog pad send</b>                                      |
| 受話 PAD の音量設定                | 62   | <b>analog pad receive</b>                                   |
| DTMF 検出レベルの設定               | 63   | <b>analog dtmf level</b>                                    |
| LAN ポートの IP アドレスとネットマスク設定   | 71   | <b>ip interface address</b>                                 |
| BOD の設定                     | 73   | <b>analog mp prior</b>                                      |
| i・ナンバーの設定                   | 81   | <b>analog arrive inumber-port</b>                           |
| 着信時サービス設定                   | 82   | <b>analog arrive incoming-signal</b>                        |

| 機能                | 機能番号   | 対応するコンソールコマンド                                   |
|-------------------|--------|-------------------------------------------------|
| 発番号無し着信設定         | 83     | <b>analog arrive without-calling-number</b>     |
| ダイヤル完了ボタンの設定      | 84     | <b>analog end-of-dialing-code</b>               |
| TEL ポートの再呼出時間設定   | 85     | <b>analog re-ringing-timer</b>                  |
| TEL ポート設定の消去      | 91     | -                                               |
| 識別着信の番号削除         | 92     | <b>no analog arrive restrict list</b>           |
| 着信ベルの番号削除         | 93     | <b>no analog arrive ringer-type list</b>        |
| 料金情報の消去           | 94     | <b>clear account analog</b>                     |
| TEL ポート設定の全消去     | 99     | -                                               |
| パスワードの設定          | 00     | <b>login password AA administrator password</b> |
| 電話機からのリビジョンアップの実行 | 020901 | <b>http revision-up go</b>                      |

### LINE ポート (回線) 側の設定

| 機能                 | 機能番号 | 対応するコンソールコマンド                     |
|--------------------|------|-----------------------------------|
| ダイヤルの種別選択          | 201  | <b>pstn dial type</b>             |
| ナンバー・ディスプレイ着信識別    | 203  | <b>pstn number display</b>        |
| 付加サービス機能設定         | 204  | <b>pstn supplementary-service</b> |
| 回線側のポーズ時間設定 (秒)    | 205  | <b>pstn pause timer</b>           |
| フッキング時間設定 (1/10 秒) | 206  | <b>pstn hooking timer</b>         |
| 送話 PAD の音量設定       | 207  | <b>pstn pad send</b>              |
| 受話 PAD の音量設定       | 208  | <b>pstn pad receive</b>           |
| LINE ポート使用制限の設定    | 209  | <b>pstn use</b>                   |

## 18.2 TEL ポートごとの設定

### 18.2.1 TEL ポートを使うか否かの設定

[書式] **analog use port use**  
**no analog use port**

[設定値] ○ *port*

- 1..... TEL1 ポート
- 2..... TEL2 ポート

○ *use*

- on..... 発着信可能として使用する
- off..... 使用しない
- call-only..... 発信専用として使用
- arrive-only..... 着信専用として使用

[説明] TEL ポートを公衆回線および内線の発着信に使用するか否かを設定する。

[初期値] on

### 18.2.2 TEL ポートのダイヤルイン番号の設定

[書式] **analog local address port dialin\_num [/sub\_address] [dialin\_num\_list]**  
**no analog local address port**

[設定値] ○ *port*

- 1..... TEL1 ポート
- 2..... TEL2 ポート

○ *dialin\_num*..... ダイヤルイン番号

○ *sub\_adres*..... サブアドレス (0x21 から 0x7e の ASCII 文字列)

○ *dialin\_num\_list*..... *dialin\_num* [/sub\_address] を空白で区切った並び (最大 4 つ)

[説明] TEL ポートのダイヤルイン番号を設定する。最大 5 つまで設定できる。

[ノート] サブアドレスの指定は、ISDN 回線を使用する場合にのみ有効である。

### 18.2.3 TEL ポートに接続する機器の設定

- [ 書式 ]            **analog device type** *port type*  
                  **no analog device type** *port*
- [ 設定値 ]            ◦ *port*
- 1..... TEL1 ポート
  - 2..... TEL2 ポート
- *type*
- any ..... 通信機器の設定なし
  - tel ..... 電話
  - fax ..... G2/G3 FAX
- [ 説明 ]            TEL ポートに接続する機器を指定する。  
これを設定すると、*type* パラメータが any の場合には HLC をつけずに、それ以外では指定した HLC をつけて発信する。また **analog arrive another-device permit** コマンドとの組み合わせにより、着信時に *port* パラメータで指定したポートへは、*type* パラメータで指定した以外の着信にตอบสนองしなくなる。
- [ ノート ]            このコマンドは、ISDN 回線を使用する場合にのみ有効である。
- [ 初期値 ]            *type* = any

### 18.2.4 TEL ポートの発信者番号を通知するか否かの設定

- [ 書式 ]            **analog local address notice** *port notice*  
                  **no analog local address notice** *port*
- [ 設定値 ]            ◦ *port*
- 1..... TEL1 ポート
  - 2..... TEL2 ポート
- *notice*
- on ..... 通知する
  - off ..... 通知しない
- [ 説明 ]            TEL ポートに設定した発信者番号を相手に通知するか否かを設定する。  
相手に通知される番号は **analog local address** コマンドで設定されたものである。  
**analog local address** コマンドで複数の番号が設定されている場合は最初に設定した番号が通知される。
- [ ノート ]            契約時に発信者番号通知サービスを選択しない場合には、常に通知されなくなる。  
このコマンドは、ISDN 回線を使用する場合にのみ有効である。
- [ 初期値 ]            on

### 18.2.5 相手先番号による即時発信を許可するか否かの設定

- [ 書式 ]            **analog rapid call** *port rapid*  
                  **no analog rapid call** *port*
- [ 設定値 ]            ◦ *port*
- 1..... TEL1 ポート
  - 2..... TEL2 ポート
- *rapid*
- on ..... 許可する
  - off ..... 拒否する
- [ 説明 ]            相手先番号による即時発信を許可するか否かを設定する。  
ダイヤル終了後、'#' ボタンを押さなくても、一定時間の経過を待たずに発信を開始することを即時発信と呼ぶ。  
過去に、発信により通話状態となった相手先が即時発信の対象となる。
- [ ノート ]            アナログ回線に接続して使用する場合、アナログ回線への発信には即時発信機能は動作しない。
- [ 初期値 ]            on

### 18.2.6 ダイアル完了ボタンの設定

- [書式]           **analog end-of-dialing-code** *port switch*  
**no analog end-of-dialing-code** *port*
- [設定値]        ◦ *port*
- 1..... TEL1 ポート
  - 2..... TEL2 ポート
- *switch*
- on..... '#' ボタンをダイアル完了ボタンとして使用する
  - off..... '#' ボタンをダイアル完了ボタンとして使用しない
- [説明]           '#' ボタンをダイアル完了ボタンとして使用するかどうかを選択する。  
offを指定している場合には、'#' ボタンは回線番号として網に通知される。  
ダイアルの先頭が'#' の場合、最初の '#' ボタンは、本コマンドの設定にかかわらず回線番号として網に通知される。  
(#ダイアル(短縮ダイアルサービス)のようにダイアルの先頭が'#' の場合)
- [初期値]        on

### 18.2.7 グローバル着信を許可するか否かの設定

- [書式]           **analog arrive global permit** *port permit*  
**no analog arrive global permit** *port*
- [設定値]        ◦ *port*
- 1..... TEL1 ポート
  - 2..... TEL2 ポート
- *permit*
- on..... 許可する
  - off..... 拒否する
- [説明]           グローバル着信を許可するか否かを設定する。  
グローバル着信の場合、着信時に着番号情報要素が付かない。グローバル着信を使用するためには、ダイヤルイン契約の際に利用指定が必要。
- [ノート]         このコマンドは、ISDN 回線を使用する場合にのみ有効である。
- [初期値]        on

### 18.2.8 TEL ポートでの識別着信をするか否かの設定

- [書式]           **analog arrive restrict** *port restrict*  
**no analog arrive restrict** *port*
- [設定値]        ◦ *port*
- 1..... TEL1 ポート
  - 2..... TEL2 ポート
- *restrict*
- permit..... 着信許可
  - reject..... 着信拒否
  - none..... 識別着信しない
- [説明]           TEL ポートで識別着信をするか否かを設定する。  
**analog arrive restrict list** コマンドで登録された識別着信リストに対しての着信動作を決定する。  
permit の場合には、発番号が登録リストに含まれれば着信許可となり、それ以外は着信拒否となる。  
reject の場合には、発番号が登録リストに含まれれば着信拒否となり、それ以外は着信許可となる。none  
の場合には、すべての発番号に対して着信許可となる。
- [ノート]         ナンバー・ディスプレイサービスの契約が必要。  
アナログ回線を使用している場合は、着信拒否に設定しても発信側には話中音は流れず、呼出状態となる。
- [初期値]        reject

**18.2.9 識別着信リストの登録**

[書式] **analog arrive restrict list** *port number dial\_num [/sub\_address]*  
**no analog arrive restrict list** *port number*

[設定値] ○ *port*

- 1..... TEL1 ポート
- 2..... TEL2 ポート

○ *number*..... リスト番号

○ *dial\_num*..... 電話番号

○ *sub\_addres*..... サブアドレス (0x21 から 0x7e の ASCII 文字列)

[説明] 識別着信用の電話番号を識別着信リストへ登録する。  
 リスト番号とは、識別着信リストの中で管理される通し番号である。また、識別着信リストは TEL ポート毎に管理される個別のリストである。

[ノート] サブアドレスの指定は、ISDN 回線を使用する場合にのみ有効である。

**18.2.10 サブアドレス無し着信を許可するか否かの設定**

[書式] **analog arrive without-subaddress permit** *port permit*  
**no analog arrive without-subaddress permit** *port*

[設定値] ○ *port*

- 1..... TEL1 ポート
- 2..... TEL2 ポート

○ *permit*

- on..... 許可する
- off..... 拒否する

[説明] サブアドレス情報要素の無い着信を許可するか否かを設定する。  
**analog local address** コマンドを使用してポート毎に異なるサブアドレスを設定しておくこと、ポートを区別して着信させることが可能になる。  
 ISDN 回線以外からの着信にはサブアドレス情報要素が付いてこない。

[ノート] このコマンドは、ISDN 回線を使用する場合にのみ有効である。

[初期値] on

**18.2.11 異なる種類の通信機器からの着信を許可するか否かの設定**

[書式] **analog arrive another-device permit** *port permit*  
**no analog arrive another-device permit** *port*

[設定値] ○ *port*

- 1..... TEL1 ポート
- 2..... TEL2 ポート

○ *permit*

- on..... 許可する
- off..... 許可しない

[説明] 異なる種類の通信機器からの着信を許可するか否かを設定する。

[ノート] 着信時の HLC 情報要素と **analog device type** コマンドにより設定された機器を比較して、着信整合性を調べる。  
 このコマンドは、ISDN 回線を使用する場合にのみ有効である。

[初期値] on

**18.2.12 話中着信を許可するか否かの設定**

[書式] **analog arrive ring-while-talking permit** *port permit*  
**no analog arrive ring-while-talking permit** *port*

- [ 設定値 ]
- *port*
    - 1..... TEL1 ポート
    - 2..... TEL2 ポート
  - *permit*
    - on..... 許可する
    - off..... 許可しない
- [ 説明 ]            話中着信を許可するか否かを設定する。
- [ ノート ]
- ・ ISDN 回線を使用している場合  
*permit* が on になっていないと、フレックスホンの INS キャッチホン (コールウェイティング) も擬似キャッチホン (擬似コールウェイティング) も使用できない。
  - ・ アナログ回線を使用している場合  
*permit* を on にすると、通話中にアナログ回線への着信があった場合、着信音によって着信が確認できる。なお、フッキングによる通話の切り替えを行なうことはできない。  
網の付加サービスによる話中着信はこの設定に関わらず動作する。  
また、**pstn supplementary-service** が on に設定されている場合は、話中着信はこの設定に関わらず動作しない。
- [ 初期値 ]            off

### 18.2.13 着信ベルリストの登録

---

- [ 書式 ]            **analog arrive ringer-type list** *port type number dial\_num* [*sub\_address*]  
**no analog arrive ringer-type list** *port type number*
- [ 設定値 ]
- *port*
    - 1..... TEL1 ポート
    - 2..... TEL2 ポート
  - *type*..... 着信時のベル音の種類 (1,2)
  - *number*..... リスト番号
  - *dial\_num*..... 相手発信者の電話番号
  - *sub\_addres*..... サブアドレス (0x21 から 0x7e の ASCII 文字列)
- [ 説明 ]            着信ベルリストを登録する。
- [ ノート ]
- type* パラメータで指定される着信ベル音の種類と、通常の着信時のベル音及び内線着信ベル音は異なる。サブアドレスの指定は、ISDN 回線を使用する場合にのみ有効である。  
ナンバー・ディスプレイサービスの契約が必要。

### 18.2.14 ナンバー・ディスプレイの設定

---

- [ 書式 ]            **analog arrive number display** *port mode*  
**no analog arrive number display** *port*
- [ 設定値 ]
- *port*
    - 1..... TEL1 ポート
    - 2..... TEL2 ポート
  - *mode*
    - off..... ナンバー・ディスプレイを使用しない
    - on..... ナンバー・ディスプレイを使用する
    - name-display..... ネーム・ディスプレイを使用する
- [ 説明 ]            指定した TEL ポートでナンバー・ディスプレイを使用可能にする。  
name-display に設定すると、ネーム・ディスプレイが使用可能になる。
- [ ノート ]
- ナンバー・ディスプレイサービスの契約が必要。  
ネーム・ディスプレイを使用する場合は、ネーム・ディスプレイサービスの契約も必要。
- ・ アナログ回線を使用時のみ  
キャッチホン・ディスプレイサービスを契約されているアナログ回線を使用した通話中は、設定に関係なく通話中の電話機がキャッチホン・ディスプレイに対応していればキャッチホン・ディスプレイサービスが利用可能。

[ 初期値 ]      off

### 18.2.15 指定した TEL ポートの優先着信順位を設定

---

[ 書式 ]            **analog arrive priority** *port priority*  
                  **no analog arrive priority** *port*

[ 設定値 ]        ◦ *port*  
                  • 1..... TEL1 ポート  
                  • 2..... TEL2 ポート  
                  ◦ *priority*..... 優先順位 (1..3)

[ 説明 ]            指定した TEL ポートの優先着信順位を設定する。  
*priority* は、1 (優先度高) - 3 (優先度低) である。

[ 初期値 ]        2

### 18.2.16 ダイヤル桁間タイマの設定

---

[ 書式 ]            **analog wait dial timer** *port time*  
                  **no analog wait dial timer** *port*

[ 設定値 ]        ◦ *port*  
                  • 1..... TEL1 ポート  
                  • 2..... TEL2 ポート  
                  ◦ *time*..... 秒数 (1..59)

[ 説明 ]            ダイヤル桁間タイマ値を設定する。  
ダイヤル中に本タイマ値を越えてキー操作が無いと発信動作を開始する。秒数は 1 秒単位で設定できる。

[ 初期値 ]        4

### 18.2.17 フッキングを判定する時間の設定

---

[ 書式 ]            **analog hooking timer** *port time*  
                  **no analog hooking timer** *port*

[ 設定値 ]        ◦ *port*  
                  • 1..... TEL1 ポート  
                  • 2..... TEL2 ポート  
                  ◦ *time*..... 秒数 (0.5..2)

[ 説明 ]            フッキングとして判断する最大の時間を設定する。  
この時間を越えて TEL ポートに接続された通信機器のフックスイッチを押し続けた場合はオンフックとみなして切断処理される。秒数は 0.1 秒単位で設定できる。

[ 初期値 ]        1

### 18.2.18 フッキング後にキー操作を受け入れる時間の設定

---

[ 書式 ]            **analog hooking wait timer** *port time*  
                  **no analog hooking wait timer** *port*

[ 設定値 ]        ◦ *port*  
                  • 1..... TEL1 ポート  
                  • 2..... TEL2 ポート  
                  ◦ *time*..... 秒数 (1..9)

[ 説明 ]            フッキング後にキー操作を受け入れる時間を設定する。  
フレックスホン機能を利用するためのフック操作を行った後、次のフッキングまたはオンフック操作を受け入れる時間である。秒数は 1 秒単位で設定できる。

[ 初期値 ]        4

**18.2.19** フッキング及びオンフック検出を無効と判断する時間の設定

[書式] **analog hooking inhibit timer** *port time*  
**no analog hooking inhibit timer** *port*

[設定値] ○ *port*

- 1..... TEL1 ポート
- 2..... TEL2 ポート

○ *time*

- 秒数 (1..3)
- off ..... 0 秒

[説明] オフフック後から、フッキング及びオンフック検出を無効と判断する時間を設定する。秒数は 1 秒単位で設定できる。

[ノート] オフフック後の数秒間、直流ループ断が発生するようなホームテレホン等を接続した場合に有効。通常は off でよい。

[初期値] off

**18.2.20** 保留音の種類の設定

[書式] **audio hold-tone type** *type*

[設定値] ○ *type*

- melody..... 保留音としてメロディーを流す
- beep..... 保留音としてビーブ音(「ブッブ」)を流す

[説明] 保留音としてメロディーを流すかビーブ音を流すかを設定する。

[ノート] beep に設定すると、従来の保留音「ブッブ」が流れる。

[初期値] melody

**18.2.21** TEL ポートの再呼出時間設定

[書式] **analog re-ringing-timer** *port time*  
**no analog re-ringing-timer** *port*

[設定値] ○ *port*

- 1..... TEL1 ポート
- 2..... TEL2 ポート

○ *time*..... 再呼出時間の秒数 (10..180)

[説明] 指定した TEL ポートの再呼出時間を設定する。  
 再呼出時間とは、以下の時間を示す。

- 相手呼出状態で内線転送を行った場合の呼出時間
- 呼び返し(保留呼があることを通知するための呼出)の呼出時間

[初期値] 30

**18.2.22** フレックスホン機能の使用パターンの設定

[書式] **analog supplementary-service** [*network*] *func* [*func...*]  
**analog supplementary-service** *pseudo func* [*func...*]  
**no analog supplementary-service**

[設定値] ○ *network* ..... 網提供のフレックスホンを示すキーワード

○ *func*

- call-waiting ..... INS キャッチホン(コールウェイティング)機能使用を示すキーワード
- call-transfer ..... 通信中転送機能使用を示すキーワード
- add-on ..... 三者通話機能使用を示すキーワード
- call-deflection 1 ..... TEL1 ポートでの着信転送機能使用を示すキーワード
- call-deflection 2 ..... TEL2 ポートでの着信転送機能使用を示すキーワード

○ *pseudo* ..... 擬似機能使用を示すキーワード



- [説明] フレックスホン機能の使用パターンを設定する。
- [ノート] 着信転送機能を実際に動作させるためには、着信転送先アドレスの設定 (**analog supplementary-service call-deflection address** コマンド) が必要。  
このコマンドは、ISDN 回線を使用する場合にのみ有効である。
- [初期値] フレックスホン機能を使用しない

### 18.2.23 着信転送先アドレスの設定

- [書式] **analog supplementary-service call-deflection address** *port dial\_num*[/*sub\_address*]  
**no analog supplementary-service call-deflection address** *port*
- [設定値]
- *port*
    - 1..... TEL1 ポート
    - 2..... TEL2 ポート
  - *dial\_num*..... 電話番号
  - *sub\_address*..... サブアドレス (0x21 から 0x7e の ASCII 文字)
- [説明] 着信転送先アドレスを登録する。
- [ノート] 網提供のフレックスホンによる着信転送では、サブアドレスの指定は無効となる。  
このコマンドは、ISDN 回線を使用する場合にのみ有効である。

### 18.2.24 着信転送を起動するタイミングの設定

- [書式] **analog supplementary-service call-deflection ringer** *port count*  
**no analog supplementary-service call-deflection ringer** *port*
- [設定値]
- *port*
    - 1..... TEL1 ポート
    - 2..... TEL2 ポート
  - *count*
    - 回数 (1..10) ..... 指定回数着信ベルを鳴らした後に起動する
    - off ..... 着信ベルを鳴らさずにすぐに起動開始する
- [説明] 着信転送を起動するタイミングを設定する。  
タイミングは 3 秒周期のリズムを 1 回とカウントする。
- [ノート] このコマンドは、ISDN 回線を使用する場合にのみ有効である。
- [初期値] off

### 18.2.25 着信転送トーキの設定

- [書式] **analog supplementary-service call-deflection talkie** *port transfer originator*  
**no analog supplementary-service call-deflection talkie** *port*
- [設定値]
- *port*
    - 1..... TEL1 ポート
    - 2..... TEL2 ポート
  - *transfer* ..... 転送トーキ
    - on..... あり
    - off..... なし
  - *originator* ..... 転送元トーキ
    - on..... あり
    - off..... なし
- [説明] 着信転送におけるトーキのありなしを設定する。

- [ノート] 転送トークは、網提供の着信転送使用時に、発信側で聞こえる音声ガイドであり、転送元トークは、転送先の相手に聞こえる音声ガイドのこと。  
 なお、擬似機能による着信転送使用時には転送トークは無い。  
 フレックスホンの着信転送機能の契約が必要。  
 このコマンドは、ISDN 回線を使用する場合にのみ有効である。
- [初期値] *transfer = off*  
*originator = off*

### 18.2.26 着信転送が拒否された時の動作の設定

- [書式] **analog supplementary-service call-deflection reject port action**  
**no analog supplementary-service call-deflection reject port**
- [設定値] ◦ *port*
- 1..... TEL1 ポート
  - 2..... TEL2 ポート
- *action*
- *busy* ..... 着信に対し、ビジートーン（話中）を返す
  - *alert* ..... 着信に対して応答する
- [説明] 着信転送を行なう際、網からそれを拒否された場合の動作を設定する。*busy* の場合には、着信に対しビジー（話中）を返すので、電話をかけてきた方にはビジートーンが返り、通話はできない。*alert* の場合には、呼出を返すと同時に手元の電話機のベルを鳴らすので、ここで受話器をとれば通話できる。
- [ノート] このコマンドは、ISDN 回線を使用する場合にのみ有効である。
- [初期値] *alert*

### 18.2.27 送話 PAD の設定

- [書式] **analog pad send port pad**  
**no analog pad send port**
- [設定値] ◦ *port*
- 1..... TEL1 ポート
  - 2..... TEL2 ポート
- *pad*
- -3dB..... -3dB PAD 挿入
  - -6dB..... -6dB PAD 挿入
  - -9dB..... -9dB PAD 挿入
  - -12dB..... -12dB PAD 挿入
  - -15dB..... -15dB PAD 挿入
  - -18dB..... -18dB PAD 挿入
  - -21dB..... -21dB PAD 挿入
  - *off* ..... PAD なし
- [説明] 送話 PAD を設定する。
- [初期値] *off*

### 18.2.28 受話 PAD の設定

- [書式] **analog pad receive port pad**  
**no analog pad receive port**
- [設定値] ◦ *port*
- 1..... TEL1 ポート
  - 2..... TEL2 ポート
- *pad*
- -3dB..... -3dB PAD 挿入
  - -6dB..... -6dB PAD 挿入
  - -9dB..... -9dB PAD 挿入
  - -12dB..... -12dB PAD 挿入
  - -15dB..... -15dB PAD 挿入
  - -18dB..... -18dB PAD 挿入

- -21dB..... -21dB PAD 挿入
- off ..... PAD なし

[ 説明 ] 受話 PAD を設定する。

[ 初期値 ] off

### 18.2.29 MP 時に電話発着信のために 1B チャンネルに落とすか否かの設定

[ 書式 ] **analog mp prior port down**  
**no analog mp prior port**

[ 設定値 ]

- *port*
  - 1..... TEL1 ポート
  - 2..... TEL2 ポート
- *down*
  - on..... 落とす
  - off ..... 落とさない

[ 説明 ] MP 時に 2B チャンネルでデータ通信中、電話の発着信を行なうためにデータ通信のチャンネル数を 1B に落とすか否かを設定する。

[ ノート ] このコマンドは、ISDN 回線を使用する場合にのみ有効である。

[ 初期値 ] on

### 18.2.30 TEL ポートへの切断信号の送出の設定

[ 書式 ] **analog disc-signal port use**  
**no analog disc-signal port**

[ 設定値 ]

- *port*
  - 1..... TEL1 ポート
  - 2..... TEL2 ポート
- *use*
  - on..... 使用する
  - off ..... 使用しない

[ 説明 ] 指定した TEL ポートへの切断信号を送出するか否かを設定する。  
on に設定すると、着信による通話時、発信側が先に通信を切断した場合に、極性反転して擬似的な切断信号をその TEL ポートへ送出する。

[ 初期値 ] on

### 18.2.31 DTMF 検出レベルの設定

[ 書式 ] **analog dtmf level port level**  
**no analog dtmf level port**

[ 設定値 ]

- *port*
  - 1..... TEL1 ポート
  - 2..... TEL2 ポート
- *level*
  - off ..... off
  - -3dB..... -3dB
  - -6dB..... -6dB
  - -9dB..... -9dB
  - -12dB..... -12dB
  - -15dB..... -15dB
  - -18dB..... -18dB
  - -21dB..... -21dB
  - -24dB..... -24dB
  - -27dB..... -27dB
  - -30dB..... -30dB

[ 説明 ] TEL ポートの DTMF 信号検出レベルを設定する。

[ 初期値 ]           off

### 18.2.32     アザーダイヤルトーンを出すか否かの設定

[ 書式 ]           **analog extension other-dial-tone switch**  
**no analog extension other-dial-tone**

[ 設定値 ]       ○ *switch*

- on.....アザーダイヤルトーンを出す
- off.....アザーダイヤルトーンを出さない

[ 説明 ]       一般回線から発呼できない場合のダイヤルトーン (アザーダイヤルトーン) を区別するか否かを設定する。offとした場合、内線を含めて発信が可能な場合は通常のダイヤルトーンが鳴る。

[ 初期値 ]       on

### 18.2.33     着信時の着信ベル鳴動モードの設定

[ 書式 ]           **analog extension incoming ringer mode**  
**no analog extension incoming ringer**

[ 設定値 ]       ○ *mode*

- all.....着信可能な全 TEL ポートを鳴動させる
- one-by-one.....着信可能な TEL ポートのうちの 1 つだけを鳴動させる

[ 説明 ]       着信時、着信可能なすべての TEL ポートを鳴動させるか、そのうちの 1 つだけを鳴動させるかを設定する。

[ ノート ]       TEL ポートに PBX 等を接続し、複数のポートを同時に鳴動させたくない場合、one-by-one に設定する。

優先度が同じ場合には、TEL1 → TEL2 の順番で検索した最初の空きポートに着信する。

[ 初期値 ]       all

### 18.2.34     i・ナンバーサービスのポート番号の設定

[ 書式 ]           **analog arrive innumber-port port inum\_port [inum\_port...]**  
**no analog arrive innumber-port port**

[ 設定値 ]       ○ *port*

- 1.....TEL1 ポート
- 2.....TEL2 ポート

○ *inum\_port*

- 1.....ポート番号 1 で着信する
- 2.....ポート番号 2 で着信する
- 3.....ポート番号 3 で着信する
- all.....すべてのポート番号で着信する
- none.....着信しない

[ 説明 ]       i・ナンバーサービスで網から送られるポート番号を TEL ポートに対応させる。対応させたポート番号が送られてきたら、その TEL ポートが着信を受ける。

all を設定したときには、どのポート番号が送られてきても着信を受ける。

none を設定したときにはどのポート番号が送られてきても着信を受けない。

[ ノート ]       このコマンドは、ISDN 回線を使用する場合にのみ有効である。

[ 初期値 ]       i・ナンバーサービスのポート番号と同じ番号の TEL ポートが着信を受ける

### 18.2.35     アナログダイヤルインと無鳴動着信機能の設定

[ 書式 ]           **analog arrive incoming-signal port number address type signal dial\_in-num**  
**no analog arrive incoming-signal port number**

## [ 設定値 ]

- *port*
  - 1..... TEL1 ポート
  - 2..... TEL2 ポート
- *number*..... 登録番号 (1..65535)
- *address*
  - *global*..... グローバル着信を登録
  - *local1*..... 1 番目のローカルアドレスを登録
  - *local2*..... 2 番目のローカルアドレスを登録
  - *local3*..... 3 番目のローカルアドレスを登録
  - *local4*..... 4 番目のローカルアドレスを登録
  - *local5*..... 5 番目のローカルアドレスを登録
  - *inumber1*..... i・ナンバーのポート番号 1 を登録
  - *inumber2*..... i・ナンバーのポート番号 2 を登録
  - *inumber3*..... i・ナンバーのポート番号 3 を登録
- *type*
  - *tel*..... HLC が電話
  - *fax*..... HLC が FAX
  - *none*..... HLC がない
  - *all*..... すべて
- *signal*
  - *modem*..... モデムダイヤルイン
  - *pb*..... PB ダイヤルイン
  - *no-ringing-fax*..... 無鳴動着信
- *dial\_in-num*..... アナログ機器に送出するダイヤルイン番号  
(*signal* で *modem* と *pb* を指定したときのみ有効)

## [ 説明 ]

指定した *port* に対して、*address* の一致する着信があったときに、*signal* に相当した着信処理を行なう。アナログダイヤルインのときには、*dial\_in-num* で設定されたダイヤルイン信号を出す。*dial\_in-num* は *signal* が *modem* の場合には 20 桁以内、*pb* の場合には 4 桁以内で設定できる。

## [ ノート ]

ダイヤルインサービスの契約が必要。

・ ISDN 回線を使用している場合

*address* にグローバル着信を指定する場合は、ダイヤルイン契約時にグローバル着信ありを指定した場合のみ有効。

*address* に i・ナンバーのポート番号を指定する場合は、i・ナンバーの契約が必要。  
*type* に HLC を指定した場合は、発信側が ISDN 回線ではないときは無効となる。

・ アナログ回線を使用している場合

*address* にグローバル着信、i・ナンバーのポート番号を指定しても無効である。  
*type* に *all* 以外を指定しても無効である。

### 18.2.36 PB ダイヤルインの一次応答検出タイミングの設定

## [ 書式 ]

**analog arrive incoming-signal timing pb *port mode***  
**no analog arrive incoming-signal timing pb *port***

## [ 設定値 ]

- *port*
  - 1..... TEL1 ポート
  - 2..... TEL2 ポート
- *mode*
  - 1..... 呼出信号送出前の極性反転のタイミングにおける直流ループ閉成を一次応答信号とみなさない
  - 2..... 呼出信号送出前の極性反転のタイミングにおける直流ループ閉成を一次応答信号とみなす

## [ 説明 ]

指定した PORT に対して、PB ダイヤルインの動作を行なう場合において、呼出信号送出前の極性反転のタイミングにおける直流ループ閉成に対する動作を選択する。

## [ 初期値 ]

*mode* = 1

### 18.2.37 発番号情報なし着信機能の設定

## [ 書式 ]

**analog arrive without-calling-number *port type* [*option1* [*option2* [*option3*]]]**  
**no analog arrive without-calling-number *port***

- [ 設定値 ]
- *port*
    - 1..... TEL1 ポート
    - 2..... TEL2 ポート
  - *type*
    - *permit*..... 発番号情報なし着信を許可する
    - *reject*..... 発番号情報なし着信を拒否する
  - *option1, option2, option3*
    - *all* ..... すべての着信を対象にする
    - *public-telephone*..... 本設定を公衆電話からの着信に限定する
    - *rejected-by-user*..... 本設定をユーザによる通知拒否の着信に限定する
    - *service-unavailable*..... 本設定を表示圏外からの着信に限定する
    - 省略時は *all* と同じ
- [ 説明 ] 指定した TEL ポートの発番号情報なしの着信を、指定した非通知理由により許可するか否かを選択する。
- [ ノート ] ナンバー・ディスプレイサービスの契約が必要。
- [ 初期値 ] *type* = *permit*  
*option* = *all*

### 18.2.38 ポーズを判定する時間の設定

- [ 書式 ] **analog pause timer** *port time*
- [ 設定値 ]
- *port*
    - 1..... TEL1 ポート
    - 2..... TEL2 ポート
  - *time*..... 秒数 (1 .. 10)
- [ 説明 ] ポーズとして判断する最小の時間を設置する。
- [ ノート ] このコマンドは、アナログ回線を使用する場合にのみ有効である。
- [ 初期値 ] 2

### 18.2.39 TEL ポートに対する電力供給の設定

- [ 書式 ] **analog power** *port sw*  
**no analog power** *port*
- [ 設定値 ]
- *port*
    - 1..... TEL1 ポート
    - 2..... TEL2 ポート
  - *sw*
    - *on*..... TEL ポートに電力を供給し、使用可能にする
    - *off*..... 電力供給を行わず、使用不可能にする
- [ 説明 ] TEL ポートに対して電力を供給するか否かを設定する。  
電力供給を行わない場合、その TEL ポートは機能しなくなる。  
再起動によって設定変更が有効となる。
- [ 初期値 ] *on*

## 18.3 アナログ回線の設定

本節のコマンドはアナログ回線を使用する場合にのみ有効である。

### 18.3.1 ダイヤルの種別を選択

- [ 書式 ] **pstn dial type** *type*
- [ 設定値 ]
- *type*
    - 10pps..... パルス (10pps)
    - 20pps..... パルス (20pps)
    - pb ..... PB

- [ 説明 ]           アナログ回線に対するダイヤルの種別を選択する。
- [ 初期値 ]        20pps

### 18.3.2       フッキング時間の設定

---

- [ 書式 ]           **pstn hooking timer *time***  
**no pstn hooking timer**
- [ 設定値 ]        ◦ *time*..... 秒数 (0.3..1)
- [ 説明 ]           アナログ回線に対してフッキング操作を行なう場合のフッキング時間を設定する。
- [ 初期値 ]        0.5

### 18.3.3       アナログ回線のモデム信号を検出するまでの時間を設定する

---

- [ 書式 ]           **pstn modem signal timer *time***  
**no pstn modem signal timer**
- [ 設定値 ]        ◦ *time* ..... 0.1-3.0[ 秒 ]
- [ 説明 ]           アナログ回線のモデム信号を検出するまでの時間を設定する。  
 ナンバー・ディスプレイが表示されない場合や、モデム・ダイヤルインが正しく動作しない場合は、この  
 コマンドを調整する必要がある。  
 秒数は 0.1 秒単位で設定できる。
- [ 初期値 ]        1

### 18.3.4       ナンバーディスプレイ (ダイヤルイン) の着信の識別設定

---

- [ 書式 ]           **pstn number display *sw***  
**no pstn number display**
- [ 設定値 ]        ◦ *sw*  
                   • auto..... ナンバーディスプレイ (ダイヤルイン) の着信を自動判別する  
                   • off ..... ナンバーディスプレイ (ダイヤルイン) の着信を判別しない
- [ 説明 ]           アナログ回線に対するナンバーディスプレイ (ダイヤルイン) の着信に対する動作を設定する。
- [ ノート ]        auto に設定すると、ナンバーディスプレイの他、ダイヤルインに対する着信を自動的に判別する。  
 off に設定すると、上記の着信においても、通常の着信と同様な動作を行なう。
- [ 初期値 ]        auto

### 18.3.5       アナログ回線に対する受話 PAD の設定

---

- [ 書式 ]           **pstn pad receive *pad***  
**no pstn pad receive**
- [ 設定値 ]        ◦ *pad*  
                   • -3dB ..... -3dB PAD 挿入  
                   • -6dB ..... -6dB PAD 挿入  
                   • -9dB ..... -9dB PAD 挿入  
                   • -12dB..... -12dB PAD 挿入  
                   • -15dB..... -15dB PAD 挿入  
                   • -18dB..... -18dB PAD 挿入  
                   • -21dB..... -21dB PAD 挿入  
                   • off ..... PAD なし
- [ 説明 ]           アナログ回線に対する受話 PAD を設定する。
- [ 初期値 ]        off

**18.3.6 アナログ回線に対する送話 PAD の設定**

---

- [ 書式 ]            **pstn pad send *pad***  
                      **no pstn pad send**
- [ 設定値 ]            ◦ *pad*
- -3dB ..... -3dB PAD 挿入
  - -6dB ..... -6dB PAD 挿入
  - -9dB ..... -9dB PAD 挿入
  - -12dB ..... -12dB PAD 挿入
  - -15dB ..... -15dB PAD 挿入
  - -18dB ..... -18dB PAD 挿入
  - -21dB ..... -21dB PAD 挿入
  - off ..... PAD なし
- [ 説明 ]            アナログ回線に対する送話 PAD を設定する。
- [ 初期値 ]            off

**18.3.7 アナログ回線に対するポーズ時間の設定**

---

- [ 書式 ]            **pstn pause timer *time***  
                      **no pstn pause timer**
- [ 設定値 ]            ◦ *time* ..... 秒数 (1 .. 10)
- [ 説明 ]            アナログ回線に対してポーズ操作を行なう場合のポーズ時間を設定する。
- [ 初期値 ]            2

**18.3.8 付加サービス機能の設定**

---

- [ 書式 ]            **pstn supplementary-service *sw***  
                      **no pstn supplementary-service**
- [ 設定値 ]            ◦ *sw*
- on ..... 付加サービスを契約している回線
  - off ..... 付加サービスを契約していない回線
- [ 説明 ]            アナログ回線に対して付加サービス (キャッチホン / ボイスワープ / トリオホン) を契約しているかどうかを設定する。
- [ 初期値 ]            off

**18.3.9 アナログ回線を使用するか否かの設定**

---

- [ 書式 ]            **pstn use *sw***  
                      **no pstn use**
- [ 設定値 ]            ◦ *sw*
- on ..... アナログ回線を使用する
  - off ..... アナログ回線を使用しない
- [ 説明 ]            アナログ回線を使用するか否かを設定する。
- [ 初期値 ]            on



## 19. メール着信確認、メール転送、メール通知機能の設定

メール着信確認機能は、プロバイダに新しいメールがあるかどうかを本製品が確認して、その結果をブラウザで確かめたりする機能です。

メール転送機能は、指定したメールサーバーのメールを別のメールサーバーに転送する機能です。

メール通知機能は、接続情報または不正アクセス検知情報を指定した宛先にメールで通知する機能です。

### 19.1 メール着信確認機能

#### 19.1.1 メールサーバーの設定

[書式] **mail-check server** *server\_num destination protocol userid password [name]*  
**no mail-check server** *server\_num*

- [設定値]
- *server\_num* ..... サーバー番号 (1..5)
  - *destination*
    - メールサーバーの IP アドレス
    - ホスト名
  - *protocol*
    - *pop3* ..... メール通信プロトコルとして POP3 を使用
    - *apop* ..... メール通信プロトコルとして APOP を使用
  - *userid* ..... ユーザ ID (64 文字以内)
  - *password* ..... パスワード (64 文字以内)
  - *name* ..... 識別名 (64 文字以内)

[説明] メールサーバーの IP アドレス等の情報を設定する。

#### 19.1.2 メールチェックの実行

[書式] **mail-check go** *server\_num*

- [設定値] ○ *server\_num* ..... サーバー番号 (1..5)

[説明] メールチェックを実行する。  
かんたん設定ページから実行した場合は、実行後 10 分経過しないと再実行できない。

[ノート] 既に接続中のプロバイダにないメールサーバーに対して本コマンドを実行すると、パスワード情報などが暗号化されずにインターネット上に流れるので注意が必要。

#### 19.1.3 メールチェックの実行を許可するか否かの設定

[書式] **mail-check prohibit** *server\_num prohibit*

- [設定値]
- *server\_num* ..... サーバー番号 (1..5)
  - *prohibit*
    - *on* ..... 実行禁止
    - *off* ..... 実行許可

[説明] メール着信確認の実行を許可するか否かを設定する。

[初期値] off

#### 19.1.4 メールチェックタイムアウトの設定

[書式] **mail-check timeout** *server\_num time*  
**no mail-check timeout** *server\_num*

- [設定値]
- *server\_num* ..... サーバー番号 (1..5)
  - *time* ..... メール到着チェック時にタイムアウトするまでの秒数 (1..180)

[説明] メールチェックでのタイムアウトするまでの時間を設定する。メールサーバーに対するアクセスに時間がかかる場合はこの値を大きくする。

[初期値] 30

## 19.2 メール転送機能

### 19.2.1 送信メールサーバーの設定

---

[書式] **mail-transfer server** *server\_num destination protocol from to [name]*  
**no mail-transfer server** *server\_num*

[設定値] ○ *server\_num* ..... サーバー番号 (1..5)  
 ○ *destination* ..... 送信メールサーバーの IP アドレスまたはホスト名  
 ○ *protocol*  
   • *smtp* ..... SMTP  
 ○ *from* ..... 転送元ユーザのメールアドレス (255 文字以内)  
 ○ *to* ..... 転送先ユーザのメールアドレス (255 文字以内)  
 ○ *name* ..... 識別名 (64 文字以内)

[説明] 送信メールサーバーの IP アドレス等の情報を設定する。

[初期値] なし

### 19.2.2 送信先サーバーの設定

---

[書式] **mail-transfer send to** *server\_num*  
**no mail-transfer send to**

[設定値] ○ *server\_num* ..... メッセージを転送するサーバー番号 (1..5、複数設定可)

[説明] **mail-transfer server** コマンドで設定された送信用メールサーバーをメール転送用に設定する。

[初期値] なし

### 19.2.3 受信メッセージサーバーの設定

---

[書式] **mail-transfer receive from** *server\_num*  
**no mail-transfer receive from**

[設定値] ○ *server\_num* ..... メッセージを受信するサーバー番号の並び (1..5)

[説明] **mail-check server** コマンドで設定された受信用メールサーバーをメール転送用に設定する。

[初期値] なし

### 19.2.4 受信メッセージの最大長の設定

---

[書式] **mail-transfer receive maxlength** *max\_length*  
**no mail-transfer receive maxlength**

[設定値] ○ *max\_length* ..... 取り込み可能なメッセージ長 (1..100:1024 バイト単位)

[説明] 受信するメッセージの最大長を設定する。  
 かんたん設定ページからの設定では 10240 バイトに制限される。設定した最大長を超えるメールは受信しない。

[初期値] 10

### 19.2.5 メール転送タイムアウトの設定

- [書式]        **mail-transfer timeout** *server\_num time*  
**no mail-transfer timeout** *server\_num*
- [設定値]     ◦ *server\_num* ..... サーバー番号 (1..5)  
               ◦ *time*..... メール転送時にタイムアウトするまでの秒数 (1..180)
- [説明]        メール転送でのタイムアウトするまでの時間を設定する。
- [ノート]      ここで指定するタイムアウトの時間はメール転送機能全体に要する時間ではなく、あるサーバーへの転送時の SMTP コネクションの時間。
- [初期値]     120

### 19.2.6 転送メッセージの最大長の設定

- [書式]        **mail-transfer send maxlength** *server\_num len*  
**no mail-transfer send maxlength**
- [設定値]     ◦ *server\_num* ..... サーバー番号 (1..5)  
               ◦ *len*  
               • メッセージが *len* の長さを超えたら超過部分を削除する (0..4096)  
               • *infinity* ..... **mail-transfer receive maxlength** コマンドで設定された長さまでを転送する
- [説明]        転送するメッセージの最大長を設定する。
- [初期値]     *infinity*

### 19.2.7 メール転送の実行

- [書式]        **mail-transfer go** [*from pop\_servers*] [*to smtp\_servers*]
- [設定値]     ◦ *pop\_servers* ..... メッセージを受信するサーバー番号の並び (1..5)  
               ◦ *smtp\_servers* ..... メッセージを転送するサーバー番号の並び (1..5)
- [説明]        メール転送を実行する。
- [ノート]      *pop\_servers* には、**mail-check server** コマンドで設定された受信用メールサーバーをメール転送用に指定する。  
*smtp\_servers* のサーバー番号指定には、**mail-transfer server** コマンドで設定された送信用メールサーバーをメール転送用に指定する。  
*pop\_servers* を省略した場合、**mail-transfer receive from** コマンドで登録された番号の受信サーバーから受信する。  
*smtp\_servers* を省略した場合、**mail-transfer send to** コマンドで登録された番号の送信サーバーへ送信する。  
本コマンドで *pop\_servers* や *smtp\_servers* を指定して実行した場合、**mail-transfer receive from** コマンドや **mail-transfer send to** コマンドの設定に関係なく、メール転送が実行可能になる。  
メッセージの取り込みは、指定されたサーバーに対して未読分のみ行なう。取り込んだメッセージは、設定された転送先に応じて設定されたフィルタに従って転送の拒否が決定され、必要なメッセージのみが転送される。

### 19.2.8 受信メッセージサーバー制限の設定

- [書式]        **mail-transfer receive restrict** *server\_num from pop\_server* [*pop\_server..*]
- [設定値]     ◦ *server\_num* ..... サーバー番号 (1..5)  
               ◦ *pop\_server* ..... メッセージを受信するサーバー (複数設定可)
- [説明]        指定したサーバーに転送するメッセージを受信するサーバーを制限する。

[ 初期値 ]      mail-transfer receive restrict 1 from 1 2 3 4  
 mail-transfer receive restrict 2 from 1 2 3 4  
 mail-transfer receive restrict 3 from 1 2 3 4  
 mail-transfer receive restrict 4 from 1 2 3 4

### 19.2.9 転送メッセージのフィルタ設定

---

[ 書式 ]            **mail-transfer filter** *server\_num condition*  
**no mail-transfer filter** *server\_num*

[ 設定値 ]        ◦ *server\_num* ..... サーバー番号 (1..5)  
 ◦ *condition* ..... フィルタ条件

- *from string* ..... From フィールドに *string* が含まれるメッセージ
- *to string* ..... To フィールドに *string* が含まれるメッセージ
- *subject string* ..... Subject フィールドに *string* が含まれるメッセージ
- *length<=N* ..... 長さが *N* オクテット以下のメッセージ
- *and* ..... 上記 2 つの条件の AND
- *or* ..... 上記 2 つの条件の OR
- *not* ..... 上記 1 つの条件の NOT

[ 説明 ]            メール転送フィルタを定義する。  
 フィルタを指定する文字列全体の大きさに制限はない。

[ 初期値 ]        なし

### 19.2.10 メッセージ転送を禁止するか否かの設定

---

[ 書式 ]            **mail-transfer prohibit** *server\_num prohibit*  
**no mail-transfer prohibit** *server\_num*

[ 設定値 ]        ◦ *server\_num* ..... サーバー番号 (1..5)  
 ◦ *prohibit*

- *on* ..... 禁止する
- *off* ..... 禁止しない

[ 説明 ]            メール着信確認の実行を許可するか否かを設定する。  
 メッセージの取り込みが行われた後に転送が行われない動作となる。

[ 初期値 ]        off

## 19.3 メール通知機能

### 19.3.1 送信情報の文字コードの設定

---

[ 書式 ]            **mail-notify charset** *server\_num charset*  
**no mail-notify charset** *server\_num*

[ 設定値 ]        ◦ *server\_num* ..... サーバー番号 (1..5)  
 ◦ *charset* ..... 文字コード

- *us-ascii*
- *iso-2022-jp*

[ 説明 ]            メール通知機能で使用する文字コードを指定する。

[ 初期値 ]        iso-2022-jp

### 19.3.2 メール送信時のサブジェクトの指定

---

[ 書式 ]            **mail-notify subject** *server\_num subject*

[ 設定値 ]        ◦ *server\_num* ..... サーバー番号 (1..5)  
 ◦ *subject* ..... メールのサブジェクトの文字列 (64 文字以内)

[ 説明 ]            メール通知機能で送信するメールのサブジェクトを指定する。

[初期値] 空文字列

### 19.3.3 メール送信の実行

---

[書式] **mail-notify go** *server\_num*

[設定値] ◦ *server\_num* ..... サーバー番号 (1..5)

[説明] 接続情報をメールで送信する。

[ノート] サーバー番号には、**mail-transfer server** コマンドで設定された送信用メールサーバーをメール通知先として指定して実行する。

### 19.3.4 不正アクセス検知時のメール通知設定

---

[書式] **mail-notify intrusion** *server\_num* *notify* [*count*]  
**no mail-notify intrusion** *server\_num*

[設定値] ◦ *server\_num* ..... サーバー番号 (1..5)

◦ *notify*

- *auto* ..... 自動通知する
- *manual* ..... 手動通知する
- *off* ..... 通知しない

◦ *count* ..... 不正アクセス検知回数 (1..50)

[説明] 不正アクセスを検知した場合にメールで通知するか否かを設定する。  
*count* パラメータで設定した回数の不正アクセスを検知した場合にメール通知をする。  
*notify* パラメータを *auto* に設定している場合には、*count* パラメータの設定が有効となる。  
*count* パラメータが設定されていない場合には、1 に設定される。

[初期値] *notify* = off

*count* = 1

### 19.3.5 不正アクセス検知時に通知されるメールのサブジェクト設定

---

[書式] **mail-notify intrusion subject** *server\_num* *subject*  
**no mail-notify intrusion subject** *server\_num*

[設定値] ◦ *server\_num* ..... サーバー番号 (1..5)

◦ *subject* ..... サブジェクト

[説明] 不正アクセスを検知した場合に通知するメールのサブジェクトを設定する。

[初期値] 空文字列

### 19.3.6 不正アクセス検知情報をメールで通知する

---

[書式] **mail-notify intrusion go** *server\_num*

[設定値] ◦ *server\_num* ..... サーバー番号 (1..5)

[説明] 不正アクセス検知情報をメールで送信する。

[ノート] サーバー番号には、**mail-transfer server** コマンドで設定された送信用メールサーバーをメール通知先として指定して実行する。

## 20. HTTP サーバー機能 (かんたん設定 / プロバイダ設定) の設定

本章のコマンドは、本製品のかんたん設定ページでプロバイダ接続を登録する際に使用され、「設定の確定」ボタンをクリックすることで自動的に設定されるものです。本章のコマンドを手動で設定することは、かんたん設定ページで登録した内容を変更することになるため、各コマンドの機能や動作を十分に理解した上で行ってください。

かんたん設定ページからはプロバイダの情報は最大 10 個まで登録でき、既に設定されている相手先情報番号のいずれかに **provider set** コマンドを使用して対応させます。解除する場合には **no provider set** コマンドを使用します。

設定されたプロバイダを選択するには、**provider select** コマンドを使用します。本コマンドによりプロバイダを変更すると、プロバイダごとに異なる DNS やデフォルトルートの設定など、そのプロバイダに接続するために必要な事項を自動的に設定変更します。プロバイダ設定の状況はかんたん設定ページで調べるか、**show config** コマンドで調べます。

### 20.1 プロバイダ接続タイプの設定

|         |                                                                                                                                                                                                                                                                                                                                          |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ 書式 ]  | <b>provider type</b> <i>provider_type</i><br><b>no provider type</b>                                                                                                                                                                                                                                                                     |
| [ 設定値 ] | <ul style="list-style-type: none"> <li>○ <i>provider_type</i> <ul style="list-style-type: none"> <li>• isdn-terminal ..... ISDN/PPPoE 型の端末接続</li> <li>• isdn-network ..... ISDN/PPPoE 型のネットワーク接続</li> <li>• leased-network ..... 専用線のネットワーク接続</li> <li>• leased-wan ..... 専用線の LAN 間接続</li> <li>• none ..... 設定なし</li> </ul> </li> </ul> |
| [ 説明 ]  | プロバイダの接続タイプを設定する。                                                                                                                                                                                                                                                                                                                        |
| [ 初期値 ] | none                                                                                                                                                                                                                                                                                                                                     |

### 20.2 プロバイダ名称の設定

|         |                                                                                                                                                                                                                                                                            |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ 書式 ]  | <b>pp name</b> <i>type:name</i><br><b>no pp name</b>                                                                                                                                                                                                                       |
| [ 設定値 ] | <ul style="list-style-type: none"> <li>○ <i>type</i> <ul style="list-style-type: none"> <li>• PRV/1..10 ..... プロバイダ型の識別 (1..10)</li> <li>• RAS ..... リモートアクセスサーバー型の識別</li> <li>• WAN ..... LAN 間接続の識別</li> </ul> </li> <li>○ <i>name</i> ..... ユーザが設定したプロバイダの名称</li> </ul> |
| [ 説明 ]  | かんたん設定用の識別コマンド。かんたん設定で、プロバイダ名称等で入力した名称がここに設定される。                                                                                                                                                                                                                           |
| [ 初期値 ] | なし                                                                                                                                                                                                                                                                         |

### 20.3 トンネル接続の名称の設定

|         |                                                         |
|---------|---------------------------------------------------------|
| [ 書式 ]  | <b>tunnel name</b> <i>name</i><br><b>no tunnel name</b> |
| [ 設定値 ] | ○ <i>name</i> ..... ユーザが設定したトンネル接続の名称                   |
| [ 説明 ]  | かんたん設定用の識別コマンド。<br>かんたん設定でトンネル接続の名称等で入力した名前がここに設定される。   |
| [ 初期値 ] | なし                                                      |

### 20.4 プロバイダ情報の PP との関連付けと名前設定

|        |                                                                                               |
|--------|-----------------------------------------------------------------------------------------------|
| [ 書式 ] | <b>provider set</b> <i>peer_num</i> [ <i>name</i> ]<br><b>no provider set</b> <i>peer_num</i> |
|--------|-----------------------------------------------------------------------------------------------|

- [設定値]    ◦ *peer\_num* ..... 相手先情報番号  
                   ◦ *name* ..... 名前 (32 文字以内)
- [説明]        プロバイダ切り替えを利用するために設定する。  
                   結び付けられた相手先情報番号はプロバイダとして扱われる。何も設定されていない相手先情報番号に対しては無効である。

## 20.5 プロバイダの接続設定

---

- [書式]        **provider select** *peer\_num*  
**no provider select**
- [設定値]    ◦ *peer\_num* ..... 相手先情報番号
- [説明]        接続するプロバイダ情報を選択し、利用可能にセットアップする。  
                   本コマンドが実行されると、各種プロバイダ設定コマンドに記録された情報に基づき、デフォルトルート、DNS サーバー、スケジュール等の変更が行われる。  
                   また、かんたん設定のプロバイダ接続設定において、接続先の変更や手動接続を行った場合にも、本コマンドが実行され接続先が切り換えられる。
- 本コマンドの上書き対象コマンドは以下のとおり。  
                   すべてのプロバイダ情報 : **pp disable**  
                   選択されたプロバイダ情報 : **pp enable**、**ip route**、**dns server** 及び **schedule at**。
- [ノート]     **provider set** コマンドに設定されていない相手先情報番号に対しては無効。  
                   かんたん設定のプロバイダに接続設定において、「複数のプロバイダに同時接続する」を選択している場合は、本コマンドを実行してはいけない。

## 20.6 プロバイダの DNS サーバーのアドレス設定

---

- [書式]        **provider dns server** *peer\_num ip\_address [ip\_address]*  
**no provider dns server** *peer\_num*
- [設定値]    ◦ *peer\_num* ..... 相手先情報番号  
                   ◦ *ip\_address* ..... DNS サーバーの IP アドレス (最大 4 つ)
- [説明]        プロバイダ毎の情報として DNS サーバーのアドレスを設定する。  
                   プロバイダが選択された場合にこのアドレスが **dns server** コマンドに上書きされる。
- [ノート]     **provider set** コマンドが実行されていない相手先情報番号に対しては無効。  
                   削除時、**dns server** コマンドの内容はクリアされない。クリアされるのは **provider dns server** コマンドで設定された内容だけである。

## 20.7 LAN インタフェースの DNS サーバーのアドレスの設定

---

- [書式]        **provider interface dns server** *ip\_address [ip\_address]*  
**no provider interface dns server**
- [設定値]    ◦ *interface* ..... LAN インタフェース名  
                   ◦ *ip\_address* ..... DNS サーバーの IP アドレス (最大 2 つ)
- [説明]        かんたん設定ページでプロバイダ情報として LAN インタフェース側 DNS サーバーの IP アドレスを設定する。
- [初期値]     なし

## 20.8 DNS サーバーを通知してくれる相手の相手先情報番号の設定

---

- [書式]        **provider dns server pp** *peer\_num dns\_peer\_num*  
**no provider dns server pp** *peer\_num*

- [設定値]     ◦ *peer\_num* ..... 相手先情報番号 (1..30)  
               ◦ *dns\_peer\_num* ..... DNS 通知相手先情報番号 (1..30)
- [説明]       プロバイダ情報として DNS サーバーを通知してくれる相手先情報番号を設定する。

## 20.9 フィルタ型ルーティングの形式の設定

- [書式]       **provider filter routing type**  
               **no provider filter routing**
- [設定値]     ◦ *type* ..... フィルタ型ルーティングの形式  
               • *off* ..... かんたん設定で手動接続をした場合に、自動接続先が自動的に切り変わる  
               • *connection* ..... かんたん設定で手動接続をした場合に、手動接続している間だけ有効なデフォルト経路が選択される。手動接続先が切断されると自動接続先に接続される  
               • *mail* ..... メールとそれ以外のプロトコルの種類を区別し、プロバイダを切り換える  
               • *host* ..... ホスト (IP アドレス) を区別してプロバイダを切り換える。  
                   最大同時に 2 つのホストに接続。
- [説明]       かんたん設定専用の識別コマンド。かんたん設定ページで選択中のフィルタ型ルーティングの形式を設定する。
- [ノート]      コンソールなどから設定した場合の動作は保証されない。
- [初期値]     *off*

## 20.10 LAN 側のプロバイダ名称の設定

- [書式]       **provider interface name type:name**  
               **no provider interface name**
- [設定値]     ◦ *interface* ..... LAN インタフェース名  
               ◦ *type* ..... プロバイダ情報の識別情報 ("PRV" など)  
               ◦ *name* ..... ユーザが設定したプロバイダの名称など
- [説明]       かんたん設定専用の識別コマンド。かんたん設定ページでプロバイダ名称等を入力した名称が設定される。
- [ノート]      コンソールなどから手動設定した場合の動作は保証されない。
- [初期値]     なし

## 20.11 プロバイダに対する昼間課金単位時間の設定

- [書式]       **provider isdn disconnect daytime peer\_num unit**  
               **no provider isdn disconnect daytime peer\_num**
- [設定値]     ◦ *peer\_num* ..... 相手先情報番号  
               ◦ *unit* ..... 昼間料金適用時の課金単位時間  
                   • 秒数 (1..21474836)  
                   • *off* ..... 設定しない
- [説明]       選択したプロバイダとの接続で、昼間料金適用時の課金単位時間を設定する。*unit* パラメータは 0.1 秒単位で設定できる。  
               選択したプロバイダとの接続で、**isdn disconnect policy 1** の場合の切断に関するタイマ値を設定する。夜間料金適用をスケジュールで切り替える場合、**isdn disconnect time** コマンドで設定された単位時間は無視される。
- [ノート]      **provider set** コマンドが実行されていない相手先情報番号に対しては無効。
- [初期値]     *unit* = 60



## 20.12 プロバイダに対する昼間課金単位時間方式での単位時間と監視時間の設定

- [書式] **provider isdn disconnect interval daytime** *peer\_num unit watch spare*  
**no provider isdn disconnect interval daytime** *peer\_num*
- [設定値]
- *peer\_num* ..... 相手先情報番号
  - *unit* ..... 課金単位秒数 (1..21474836)
  - *watch* ..... 監視秒数 (1..21474836)
  - *spare* ..... 切断余裕秒数 (1..21474836)
- [説明] 選択したプロバイダとの接続で、**isdn disconnect policy 2** の場合の切断に関するタイマ値を設定する。夜間料金時間帯での値は、**provider isdn disconnect interval nighttime** コマンドで設定する。
- [ノート] **provider set** コマンドが実行されていない相手先情報番号に対しては無効。
- [初期値] *unit* = 180  
*watch* = 6  
*spare* = 2

## 20.13 プロバイダに対する夜間課金単位時間の設定

- [書式] **provider isdn disconnect nighttime** *peer\_num unit*  
**no provider isdn disconnect nighttime** *peer\_num*
- [設定値]
- *peer\_num* ..... 相手先情報番号
  - *unit* ..... 昼間料金適用時の課金単位時間
    - 秒数 (1..21474836)
    - off ..... 設定しない
- [説明] 選択したプロバイダとの接続で、夜間料金適用時の課金単位時間を設定する。  
*unit* パラメータは 0.1 秒単位で設定できる。  
 選択したプロバイダとの接続で、**isdn disconnect policy 1** の場合の切断に関するタイマ値を設定する。昼間料金適用時の課金単位時間の設定値と異なる場合に、**provider isdn account nighttime** の設定値とともに、プロバイダが選択された場合にスケジュールに組み込まれる。この場合、**isdn disconnect time** で設定された単位時間は無視される。
- [ノート] **provider set** コマンドが実行されていない相手先情報番号に対しては無効。
- [初期値] *unit* = 60

## 20.14 プロバイダに対する夜間課金単位時間方式での単位時間と監視時間の設定

- [書式] **provider isdn disconnect interval nighttime** *peer\_num unit watch spare*  
**no provider isdn disconnect interval nighttime** *peer\_num*
- [設定値]
- *peer\_num* ..... 相手先情報番号
  - *unit* ..... 課金単位秒数 (1..21474836)
  - *watch* ..... 監視秒数 (1..21474836)
  - *spare* ..... 切断余裕秒数 (1..21474836)
- [説明] 選択したプロバイダとの接続で、**isdn disconnect policy 2** に設定した場合の夜間料金時間帯での切断に関するタイマ値を設定する。昼間のタイマ値は、**provider isdn disconnect interval daytime** コマンドで設定する。
- [ノート] **provider set** コマンドが実行されていない相手先情報番号に対しては無効。
- [初期値] *unit* = 180  
*watch* = 6  
*spare* = 2

## 20.15 NTP サーバーの設定

---

- [書式]           **provider ntpdate** *server\_name*  
**no provider ntpdate**
- [設定値]        ◦ *server\_name* ..... NTP サーバー名 (IP アドレスまたは FQDN)
- [説明]           かんたん設定専用のコマンド。  
NTP サーバーを 1 箇所設定する。**provider ntp server** コマンドでは接続先毎の IP アドレス情報を設定し、本コマンドでは 1 箇所の IP アドレスまたは FQDN を設定する。
- [ノート]         コンソールなどから手動設定した場合の動作は保証されない。

## 20.16 プロバイダに対する自動切断タイマ無効時間の設定

---

- [書式]           **provider isdn auto disconnect off** *peer\_num from to*  
**no provider isdn auto disconnect off** *peer\_num*
- [設定値]        ◦ *peer\_num* ..... 相手先情報番号  
◦ *from* ..... 時 : 分 開始時刻 (0:0..23:59)  
◦ *to* ..... 時 : 分 終了時刻 (0:0..23:59)
- [説明]           選択したプロバイダとの接続時、自動切断タイマを無効にする時間を設定する。  
相手先情報番号の設定で **isdn disconnect policy** が課金単位時間方式である場合に有効。プロバイダが選択された場合にスケジュールに組み込まれる。
- [ノート]         **provider set** コマンドが実行されていない相手先情報番号に対しては無効。

## 20.17 プロバイダに対する夜間料金時間の設定

---

- [書式]           **provider isdn account nighttime** *peer\_num from to*  
**no provider isdn account nighttime** *peer\_num*
- [設定値]        ◦ *peer\_num* ..... 相手先情報番号  
◦ *from* ..... 時 : 分 開始時刻 (0:0..23:59)  
◦ *to* ..... 時 : 分 終了時刻 (0:0..23:59)
- [説明]           選択したプロバイダとの接続で、夜間料金が適用される時間を設定する。  
**provider isdn disconnect nighttime** コマンドで設定された夜間課金単位時間と、**provider isdn disconnect daytime** コマンドで設定された課金単位時間が異なる場合に有効。プロバイダが選択された場合にスケジュールに組み込まれる。
- [ノート]         **provider set** コマンドが実行されていない相手先情報番号に対しては無効。

## 20.18 プロバイダの NTP サーバーのアドレス設定

---

- [書式]           **provider ntp server** *peer\_num ip\_address*  
**no provider ntp server** *peer\_num*
- [設定値]        ◦ *peer\_num* ..... 相手先情報番号  
◦ *ip\_address* ..... NTP サーバーの IP アドレス
- [説明]           プロバイダ毎の情報として NTP サーバーのアドレスを設定する。  
本コマンドで IP アドレスが設定されていると、プロバイダが選択されている場合に、定期的に時刻を問い合わせる。プロバイダが選択された場合にスケジュールに組み込まれる。
- [ノート]         **provider set** コマンドが実行されていない相手先情報番号に対しては無効。

## 20.19 MP 使用時間帯の設定

- [書式]           **provider ppp mp use on** *peer\_num from to*  
**no provider ppp mp use on** *peer\_num*
- [設定値]           ◦ *peer\_num* ..... 相手先情報番号  
◦ *from* ..... 時 : 分 開始時刻 (0:0..23:59)  
◦ *to* ..... 時 : 分 終了時刻 (0:0..23:59)
- [説明]            選択したプロバイダとの接続で、MP を使用する時間を設定する。プロバイダが選択された場合にスケジュールに組み込まれる。
- [ノート]           **provider set** コマンドが実行されていない相手先情報番号に対しては無効。

## 20.20 かんたん設定ページの切断ボタンを押した後に自動接続するか否かの設定

- [書式]           **provider auto connect forced disable** *switch*  
**no provider auto connect forced disable** [*switch*]
- [設定値]           ◦ *switch*  
                  • on ..... 自動接続する  
                  • off ..... 自動接続しない
- [説明]            かんたん設定ページの切断ボタンを押した後、自動接続を禁止するか否かを設定する。
- [ノート]           on に設定してある場合、かんたん設定ページの手動切断ボタンを押した後に **pp disable** コマンド、接続ボタンを押した時に **pp enable** コマンドを自動設定する。そのため、切断ボタンを押した後は、自動接続をしなくなる。また、**connect** コマンドからは接続できなくなる。接続するには、手動接続ボタンを押すか、ルータを再起動する必要がある。
- [初期値]           off

## 20.21 かんたん設定ページで IPv6 接続を行なうか否かの設定

- [書式]           **provider ipv6 connect pp** *peer\_num connect*  
**no provider ipv6 connect pp** *peer\_num*
- [設定値]           ◦ *peer\_num* ..... 相手先情報番号  
◦ *connect*  
                  • off ..... 接続する  
                  • on ..... 接続しない
- [説明]            かんたん設定ページでプロバイダ情報として IPv6 接続を有効にするか否かを設定する。
- [ノート]           かんたん設定ページで IPv6 接続設定をした時に自動的に on になる。
- [初期値]           off

## 20.22 プロバイダ情報とトンネルとの関連付け

- [書式]           **provider pp bind** *pp\_num\_tunnel\_num...*  
**no provider pp bind** *pp\_num [tunnel\_num...]*
- [設定値]           ◦ *pp\_num* ..... 相手先情報番号  
◦ *tunnel\_num* ..... トンネルインタフェース番号
- [説明]            プロバイダ情報とトンネルとの関連付けを設定します。

## 20.23 LAN インタフェースのプロバイダ情報とトンネルとの関連付け

- [書式]           **provider interface bind** *tunnel\_num...*  
**no provider interface bind** [*tunnel\_num...*]

- [設定値]     ◦ *interface* ..... LAN インタフェース名  
               ◦ *tunnel\_num* ..... トンネルインタフェース番号
- [説明]       LAN インタフェースのプロバイダ情報とトンネルとの関連付けを設定します。

## 20.24 HTTP サーバー機能の有無の設定

---

- [書式]       **httpd service *switch***  
               **no httpd service**
- [設定値]     ◦ *switch*  
               • *on* ..... HTTP サーバー機能を有効にする  
               • *off* ..... HTTP サーバー機能を無効にする
- [説明]       HTTP サーバーを有効にするか否かを選択する。
- [初期値]     *on*

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

---

- [書式]       **httpd host *host***  
               **no httpd host**
- [設定値]     ◦ *host*  
               • *any* ..... すべてのホストからのアクセスを許可する  
               • *lan* ..... LAN ポート (LAN1) 側ネットワーク内、あるいは、WAN ポート (LAN2) 側ネットワーク内ならば許可する  
               • *lan1* ..... LAN ポート (LAN1) 側ネットワーク内ならば許可する  
               • *lan2* ..... WAN ポート (LAN2) 側ネットワーク内ならば許可する  
               • *none* ..... すべてのホストからのアクセスを禁止する  
               • HTTP サーバーへアクセスを許可するホストの IP アドレス  
               • HTTP サーバーへアクセスを許可するホストの IP アドレス範囲 (*ip\_address-ip\_address*)
- [説明]       HTTP サーバーへのアクセスを許可するホストを設定します。
- [ノート]     *lan* の場合、*primary* および *secondary* が *clear* ではなく、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ホストアドレスからのリクエストを許可する。
- [初期値]     *lan*

## 20.26 HTTP サーバーのセッションタイムアウト時間の設定

---

- [書式]       **httpd timeout *time***  
               **no httpd timeout [*time*]**
- [設定値]     ◦ *time* ..... 秒数 (1..180)
- [説明]       HTTP サーバーのタイムアウト時間を設定する。
- [ノート]     インターネット経由で本製品のかんたん設定ページへアクセスする等の状況で、通信タイムアウトが発生して本製品のかんたん設定ページへ正常にアクセスできない場合には、タイムアウト時間に大きな値を設定する。
- [初期値]     5

## 20.27 HTTP サーバー機能の listen ポートの設定

---

- [書式]       **httpd listen *port***  
               **no httpd listen**
- [設定値]     ◦ *port* ..... ポート番号 (1..65535)
- [説明]       HTTP サーバーの待ち受けるポートを設定する。
- [初期値]     80

## 21. UPnP の設定

### 21.1 UPnP を使用するか否かの設定

|         |                                                                                                       |
|---------|-------------------------------------------------------------------------------------------------------|
| [ 書式 ]  | <b>upnp use</b> <i>use</i><br><b>no upnp use</b>                                                      |
| [ 設定値 ] | ◦ <i>use</i> <ul style="list-style-type: none"> <li>• on.....使用する</li> <li>• off.....使用しない</li> </ul> |
| [ 説明 ]  | UPnP 機能を使用するか否かを設定する。                                                                                 |
| [ 初期値 ] | on                                                                                                    |

### 21.2 UPnP に使用する IP アドレスを取得するインタフェースの設定

|         |                                                                                                                                                                                                                                                                                          |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ 書式 ]  | <b>upnp external address refer</b> <i>interface</i><br><b>upnp external address refer pp</b> <i>peer_num</i><br><b>upnp external address refer</b> default<br><b>no upnp external address refer</b> [ <i>interface</i> ]<br><b>no upnp external address refer pp</b> [ <i>peer_num</i> ] |
| [ 設定値 ] | ◦ <i>interface</i> ..... LAN インタフェース名<br>◦ default ..... デフォルトルートのインタフェース<br>◦ <i>peer_num</i> <ul style="list-style-type: none"> <li>• 相手先情報番号</li> <li>• anonymous</li> </ul>                                                                                                          |
| [ 説明 ]  | UPnP に使用する IP アドレスを取得するインタフェースを設定する。                                                                                                                                                                                                                                                     |
| [ 初期値 ] | default                                                                                                                                                                                                                                                                                  |

### 21.3 UPnP のポートマッピング用消去タイマのタイプの設定

|         |                                                                                                                                                               |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ 書式 ]  | <b>upnp port mapping timer type</b> <i>type</i><br><b>no upnp port mapping timer type</b>                                                                     |
| [ 設定値 ] | ◦ <i>type</i> <ul style="list-style-type: none"> <li>• normal ..... ARP 情報を参照しない</li> <li>• arp ..... ARP 情報を参照する</li> </ul>                                  |
| [ 説明 ]  | UPnP のポートマッピングを消去するためのタイマのタイプを設定する。<br>このコマンドで変更を行なうと arp の場合の消去タイマ値は 3600 秒、normal の場合は 172800 秒にセットされる。消去タイマの秒数は <b>upnp port mapping timer</b> コマンドで変更できる。 |
| [ 初期値 ] | arp                                                                                                                                                           |

### 21.4 UPnP のポートマッピングの消去タイマの設定

|         |                                                                                                                 |
|---------|-----------------------------------------------------------------------------------------------------------------|
| [ 書式 ]  | <b>upnp port mapping timer</b> <i>time</i><br><b>no upnp port mapping timer</b>                                 |
| [ 設定値 ] | ◦ <i>time</i> <ul style="list-style-type: none"> <li>• 秒数 (600..21474836)</li> <li>• off ..... 消去しない</li> </ul> |
| [ 説明 ]  | UPnP によって生成されたポートマッピングを消去するまでの時間を設定する。                                                                          |
| [ ノート ] | <b>upnp port mapping timer type</b> コマンドで設定を行った後、このコマンドの設定を変更する。                                                |
| [ 初期値 ] | 172800                                                                                                          |

## 21.5 UPnP の syslog を出力するか否かの設定

---

- [書式]           **upnp syslog** *syslog*  
                  **no upnp syslog**
- [設定値]        ◦ *syslog*
- on.....UPnP の syslog を出力する
  - off .....UPnP の syslog を出力しない
- [説明]           UPnP の syslog を出力するか否かを設定する。デバッグレベルで出力される。
- [初期値]        off

## 22. USB の設定

### 22.1 USB ホスト機能を使うか否かの設定

|         |                                                                                                                                                          |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ 書式 ]  | <b>usbhost use</b> <i>switch</i><br><b>no usbhost use</b> [ <i>switch</i> ]                                                                              |
| [ 設定値 ] | ○ <i>switch</i> <ul style="list-style-type: none"> <li>• on..... USB ホスト機能を使用する</li> <li>• off..... USB ホスト機能を使用しない</li> </ul>                           |
| [ 説明 ]  | USB ホスト機能を使用するか否かを設定する。<br>このコマンドが off に設定されているときは USB メモリをルータに接続しても認識されない。<br>また、過電流により USB ホスト機能に障害が発生した場合、USB メモリが接続されていない状態で本コマンドを再設定すると復旧させることができる。 |
| [ 初期値 ] | on                                                                                                                                                       |

### 22.2 USB メモリに保存する SYSLOG ファイル名の指定

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [ 書式 ]  | <b>usbhost syslog filename</b> <i>name</i><br><b>no usbhost syslog filename</b> [ <i>name</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| [ 設定値 ] | ○ <i>name</i> .....SYSLOG ファイル名 <ul style="list-style-type: none"> <li>• <i>usb1:filename</i> ..... USB メモリ内のファイル (<i>filename</i> は 64 文字以内。ただし、.bak 拡張子を含む名前は指定できない)</li> </ul>                                                                                                                                                                                                                                                                                                                                                               |
| [ 説明 ]  | USB メモリ内に保存する SYSLOG ファイル名を指定する。<br>このコマンドを設定することで USB メモリへの SYSLOG の記録を開始する。<br>このコマンドを消去することで USB メモリへの SYSLOG の記録が停止する。<br>ファイルに書き込むことのできるサイズの上限は、USB メモリへの書き込み開始時の空き容量から自動計算される。また、USB メモリ内には本コマンドで設定したファイルの他、必要に応じてバックアップファイルが作成される。これは SYSLOG ファイルが上限サイズに達した場合の退避先ファイルであり、ファイル名は以下の規則に従って決定される。<br><i>filename</i> に拡張子が含まれている場合 ..... 拡張子を .bak に置き換える<br><i>filename</i> に拡張子が含まれていない場合 ..... <i>filename</i> .bak とする<br>バックアップファイルとの名前重複を避けるため、 <i>filename</i> に .bak 拡張子を含むファイル名は指定できない。このコマンドが設定されていないときは SYSLOG を USB メモリに書き込まない。 |
| [ 初期値 ] | 設定されていない                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

### 22.3 USB ボタンと DOWNLOAD ボタン同時押下による設定ファイル、ファームウェアファイルのコピー操作を許可するか否かの設定

|         |                                                                                                                 |
|---------|-----------------------------------------------------------------------------------------------------------------|
| [ 書式 ]  | <b>operation usb-download permit</b> <i>switch</i><br><b>no operation usb-download permit</b> [ <i>switch</i> ] |
| [ 設定値 ] | ○ <i>switch</i> <ul style="list-style-type: none"> <li>• on..... 許可する</li> <li>• off..... 許可しない</li> </ul>      |
| [ 説明 ]  | USB ボタンと DOWNLOAD ボタンの同時押下により、設定ファイル、およびファームウェアファイルを内蔵フラッシュ ROM へコピーするか否かを設定する。                                 |
| [ 初期値 ] | on                                                                                                              |

### 22.4 USB ボタンと DOWNLOAD ボタン同時押下によりコピーする設定ファイル名の指定

|        |                                                                                    |
|--------|------------------------------------------------------------------------------------|
| [ 書式 ] | <b>usbhost config filename</b> <i>from to</i><br><b>no usbhost config filename</b> |
|--------|------------------------------------------------------------------------------------|

- [ 設定値 ]      ◦ *from*
- `usb1:filename` ..... USB メモリ内の設定ファイル名 (*filename* は 64 文字以内)
- *to*
- 内蔵フラッシュ ROM の設定ファイル番号
- [ 説明 ]            USB ボタンと DOWNLOAD ボタンの同時押下により内蔵フラッシュ ROM へコピーする設定ファイル名を指定する。  
指定可能な内蔵フラッシュ ROM の設定ファイル番号は、0。
- [ 初期値 ]        `usb1:config.txt` 0

## 22.5 USB ボタンと DOWNLOAD ボタン同時押下によりコピーするファームウェアファイル名の指定

---

- [ 書式 ]            **usbhost exec filename** *from to*  
**no usbhost exec filename** [*from to*]
- [ 設定値 ]        ◦ *from*
- `usb1:filename` ..... USB メモリ内の実行形式ファームウェアファイル名 (*filename* は 64 文字以内)
- *to*
- 内蔵フラッシュ ROM の実行形式ファームウェアファイル番号
- [ 説明 ]            USB ボタンと DOWNLOAD ボタンの同時押下により内蔵フラッシュ ROM へコピーする実行形式ファームウェアファイル名を指定する。  
指定可能な内蔵フラッシュ ROM の実行形式ファームウェアファイル番号は、0。
- [ 初期値 ]        `usb1:n58i.bin` 0



## 23. スケジュール

### 23.1 スケジュールの設定

[書式] **schedule at** *id* [*date*] *time* \* *command*...  
**schedule at** *id* [*date*] *time* *pp peer\_num* *command*...  
**schedule at** *id* [*date*] *time* *tunnel tunnel\_num* *command*...  
**no scudule at** *id* [[*date*]...]

[設定値] ○ *id*..... スケジュール番号  
 ○ *date*..... 日付 (省略可)  
 ● 月 / 日  
 ● 省略時は \*/\* とみなす

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

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

○ *time*..... 時刻  
 ● 時 (0..23 または \*): 分 (0..59 または \*)  
 ● startup ..... 起動時  
 ○ *peer\_num*  
 ● 相手先情報番号  
 ● anonymous  
 ○ *tunnel\_num* ..... トンネルインタフェース番号  
 ○ *command*..... 実行するコマンド (制限あり)

[説明] *time* で指定した時刻に *command* で指定されたコマンドを実行する。  
 第2、第3書式で指定された場合には、それぞれあらかじめ指定された相手先情報番号 / トンネル番号での、**pp select** / **tunnel select** コマンドが発行済みであるように動作する。  
**schedule at** コマンドは複数指定でき、同じ時刻に指定されたものは *id* の小さな順に実行される。  
 以下のコマンドは指定できない。  
**administrator**, **administrator password**, **cold start**, **console info** と **console prompt** を除く **console** で始まるコマンド、**date**, **exit**, **help**, **http revision-up go**, **interface reset**, **less** で始まるコマンド、**login password**, **login timer**, **ping**, **ping6**, **pp select**, **provider interface dns server**, **provider interface name**, **quit**, **remote setup**, **save**, **schedule at**, **show** で始まるコマンド、**telnet**, **time**, **timezone**, **traceroute**, **traceroute6**, **tunnel select**

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

## 【設定例】

- ウィークデイの 8:00 ~ 17:00 だけ接続を許可する
  - # schedule at 1 \*/mon-fri 8:00 pp 1 isdn auto connect on
  - # schedule at 2 \*/mon-fri 17:00 pp 1 isdn auto connect off
  - # schedule at 3 \*/mon-fri 17:05 \* disconnect 1
  
- 毎時 0 分から 15 分間だけ接続を許可する
  - # schedule at 1 \*:00 pp 1 isdn auto connect on
  - # schedule at 2 \*:15 pp 1 isdn auto connect off
  - # schedule at 3 \*:15 \* disconnect 1

今度の元旦にルーティングを切替える

```
schedule at 1 1/1 0:0 * ip route NETWORK gateway pp 2
```

## 24. 操作

### 24.1 相手先情報番号の選択

---

- [書式]            **pp select** *peer\_num*  
**no pp select**
- [設定値]        ◦ *peer\_num*
- 相手先情報番号
  - none..... 相手を選択しない
  - anonymous
- [説明]            設定や表示の対象となる相手先情報番号を選択する。以降プロンプトには、**console prompt** コマンドで設定した文字列と相手先情報番号が続けて表示される。  
none を指定すると、プロンプトに相手先情報番号を表示しない。
- [ノート]         この操作コマンドは一般ユーザでも実行できる。  
**no pp select** コマンドは **pp select none** コマンドと同じ動作をする。

### 24.2 トンネルインタフェース番号の選択

---

- [書式]            **tunnel select** *tunnel\_num*  
**no tunnel select**
- [設定値]        ◦ *tunnel\_num*
- トンネルインタフェース番号
  - none..... トンネルインタフェースを選択しない
- [説明]            トンネルモードの設定や表示の対象となるトンネルインタフェース番号を選択する。
- [ノート]         本コマンドの操作は、一般ユーザでも実行できる。  
プロンプトが tunnel の場合は、pp 関係のコマンドは入力できない。  
**no tunnel select** コマンドは **tunnel select none** コマンドと同じ動作をする。

### 24.3 設定に関する操作

#### 24.3.1 管理ユーザへの移行

---

- [書式]            **administrator**
- [設定値]        なし
- [説明]            このコマンドを発行してからでないと、ルータ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。  
コマンド入力後、管理パスワードを入力しなければならない。

#### 24.3.2 終了

---

- [書式]            **quit**  
**quit save**  
**exit**  
**exit save**
- [設定値]        ◦ save ..... 管理ユーザから抜ける際に指定すると、設定内容を不揮発性メモリに保存して終了
- [説明]            ルータへのログインを終了、または管理ユーザから抜ける。  
設定を変更して保存せずに管理ユーザから抜けようとする、新しい設定内容を保存するか否かを問い合わせる。

### 24.3.3 設定内容の保存

---

[書式]           **save**  
**save** *filename* [*comment*]

[設定値]       ○ *filename*..... 設定を保存するファイル名  
                   • 0..... 内蔵 Flash ROM の設定ファイル  
                   ○ *comment* ..... 設定ファイルのコメント

[説明]           現在の設定内容を不揮発性メモリに保存する。

ファイルを指定することができる。ファイルの指定を省略すると、起動時に使用した設定ファイルに保存する。*filename* として 0 のみ指定可能。

### 24.3.4 設定ファイルの複製

---

[書式]           **copy config from to**

[設定値]       ○ *from, to*..... 設定ファイル名  
                   • 内蔵フラッシュ ROM の設定ファイル番号  
                   • *usb1:filename* ..... USB メモリ内の設定ファイル名 (*filename* は 64 文字以内)

[説明]           保存されている設定ファイル FROM を TO へ複製する。  
 FROM、TO の両方に USB メモリ内のファイルを指定することはできない。  
 指定可能な内蔵フラッシュ ROM の設定ファイル番号は 0。

cold start 直後は内蔵フラッシュ ROM から USB 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を再起動する必要がある。

### 24.3.5 ファームウェアファイルを内蔵フラッシュ ROM にコピー

---

[書式]           **copy exec from to**

[設定値]       ○ *from*  
                   • *usb1:filename*..... USB メモリ内の実行形式ファームウェアファイル名 (*filename* は 64 文字以内)  
                   ○ *to*  
                   • 内蔵フラッシュ ROM の実行形式ファームウェアファイル番号

[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。  
 指定可能な内蔵フラッシュ ROM の実行形式ファームウェアファイル番号は 0。

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を再起動する必要がある。

### 24.3.6 設定ファイルの削除

---

[書式]           **delete config filename**

[設定値]       ○ *filename*..... 削除するファイル名  
                   • 0..... 内蔵 Flash ROM の設定ファイル

[説明]           保存されている設定ファイルを削除する。  
*filename* として 0 のみ指定可能。

### 24.3.7 設定ファイルの一覧

---

[書式]           **show config list**  
**less config list**

- [設定値] なし
- [説明] 内蔵 Flash ROM に保存されている設定ファイルの一覧を表示する。

### 24.3.8 設定の初期化

---

- [書式] **cold start**
- [設定値] なし
- [説明] 工場出荷時の設定に戻し、再起動する。  
コマンド実行時に管理パスワードを入力する必要がある。
- [ノート] 内蔵 Flash ROM の設定ファイルがすべて削除されることに注意。

### 24.3.9 遠隔地のルータの設定

---

- [書式] **remote setup interface [isdn\_num[/sub\_address]]**
- [設定値]
  - *interface* ..... BRI インタフェース名
  - *isdn\_num* ..... ISDN 番号
  - *sub\_address* ..... ISDN サブアドレス (0x21 から 0x7e の ASCII 文字列)
- [説明] 指定したインタフェースを利用して、遠隔地のルータの設定をする。  
インタフェースは、ISDN、専用線いずれの場合でも設定できる。
- [ノート] 専用線の場合は、*isdn\_num*、*sub\_address* パラメータは不要。

### 24.3.10 遠隔地のルータからの設定に対する制限

---

- [書式] **remote setup accept isdn\_num[/sub\_address] [isdn\_num\_list]**  
**remote setup accept any**  
**remote setup accept none**  
**no remote setup accept**
- [設定値]
  - *isdn\_num* ..... ISDN 番号
  - *sub\_address* ..... ISDN サブアドレス (0x21 から 0x7e の ASCII 文字列)
  - *isdn\_num\_list* ..... ISDN 番号だけまたは ISDN 番号とサブアドレスを空白で区切った並び
  - *any* ..... すべての遠隔地のルータからの設定を許可することを示すキーワード
  - *none* ..... すべての遠隔地のルータからの設定を拒否することを示すキーワード
- [説明] 自分のルータの設定を許可する相手先を設定する。
- [初期値] any

## 24.4 動的情報のクリア操作

### 24.4.1 ARP テーブルのクリア

---

- [書式] **clear arp**
- [設定値] なし
- [説明] ARP テーブルをクリアする。

### 24.4.2 IP の動的経路情報のクリア

---

- [書式] **clear ip dynamic routing**
- [設定値] なし

[説明] 動的に設定された IP の経路情報をクリアする。

### 24.4.3 ログのクリア

---

[書式] **clear log**

[設定値] なし

[説明] ログをクリアする。

### 24.4.4 アカウントのクリア

---

[書式] **clear account**  
**clear account interface**  
**clear account pp** [*peer\_num*]  
**clear account pstn**

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

◦ *peer\_num*

- 相手先情報番号
- anonymous
- 省略時は現在選択している相手先

[説明] 指定したインタフェース (第 1 書式ではすべて) に関するアカウント情報および通信履歴をクリアする。

[ノート] 通信履歴とは **show history** コマンドで表示される内容を指す。  
**clear account** を実行すると、**show account analog** コマンドで表示されるような通話のアカウント情報および通信履歴についてもクリアされる。

### 24.4.5 TEL ポートに関するアカウントのクリア

---

[書式] **clear account analog** [*port*]  
**clear account analog total**

[設定値] ◦ *port*

- 1..... TEL 1 ポート
  - 2..... TEL 2 ポート
  - 省略時はすべての TEL ポートについてクリアする
- *total*..... 電話回線を示すキーワード

[説明] TEL ポートに関するアカウントをクリアする。  
*port* パラメータを省略した場合には、すべての TEL ポートのアカウントがクリアされる。

### 24.4.6 DNS キャッシュのクリア

---

[書式] **clear dns cache**

[設定値] なし

[説明] DNS リカーシブサーバーで持っているキャッシュをクリアする。

### 24.4.7 NAT アドレステーブルのクリア

---

[書式] **clear nat descriptor dynamic** *nat\_descriptor*

[設定値] ◦ *nat\_descriptor*

- NAT ディスクリプタ番号 (1..21474836)
- all..... すべての NAT ディスクリプタ番号

[説明] NAT アドレステーブルをクリアする。

[ノート] 通信中にアドレス管理テーブルをクリアした場合、通信が一時的に不安定になる可能性がある。

### 24.4.8 インタフェースの NAT アドレステーブルのクリア

---

- [書式]        **clear nat descriptor interface dynamic** *interface*  
**clear nat descriptor interface dynamic pp** *peer\_num*  
**clear nat descriptor interface dynamic tunnel** *tunnel\_num*
- [設定値]     ◦ *interface* ..... LAN インタフェース名  
◦ *peer\_num* ..... 相手先情報番号  
◦ *tunnel\_num* ..... トンネルインタフェース番号
- [説明]        インタフェースに適用されている NAT アドレステーブルをクリアする。

### 24.4.9 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。

### 24.4.10 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。

## 24.5 その他の操作

### 24.5.1 相手先の使用許可の設定

---

- [書式]        **pp enable** *peer\_num*  
**no pp enable** *peer\_num*
- [設定値]     ◦ *peer\_num*  
• 相手先情報番号  
• anonymous  
• all ..... すべての相手先情報番号
- [説明]        相手先を使用できる状態にする。  
工場出荷時、すべての相手先は disable 状態なので、使用する場合は必ずこのコマンドで enable 状態にしなければならない。

### 24.5.2 相手先の使用不許可の設定

---

- [書式]        **pp disable** *peer\_num*
- [設定値]     ◦ *peer\_num*  
• 相手先情報番号  
• anonymous  
• all ..... すべての相手先情報番号
- [説明]        相手先を使用できない状態にする。  
相手先の設定を行なう場合は disable 状態であることが望ましい。

### 24.5.3 再起動

---

- [書式]        **restart**
- [設定値]     なし
- [説明]        ルータを再起動する。

#### 24.5.4 インタフェースの再起動

---

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

[設定値] ◦ *interface*

- LAN インタフェース名
- BRI インタフェース名

[説明] 指定したインタフェースを再起動する。  
LAN インタフェースでは、オートネゴシエーションする設定になっていればオートネゴシエーション手順が起動される。  
BRI インタフェースでは、回線種別を **line type** コマンドで変更した場合には、本コマンドでインタフェースを再起動する必要がある。  
なお、MP を使用しているインタフェースに対しては、**interface reset pp** コマンドを使用する。

[ノート] **line type** コマンド、**pp bind** コマンド、経路情報などすべての設定を整えた後に実行する。対象とするインタフェースがバインドされているすべての pp の通信を停止した状態で、また回線種別を変更する場合には回線を抜いた状態で実行すること。

#### 24.5.5 PP インタフェースの再起動

---

[書式] **interface reset pp** [*peer\_num*]

[設定値] ◦ *peer\_num*

- 相手先情報番号
- anonymous

[説明] 選択した相手先番号にバインドされているインタフェースをリセットする。MP を使用しているインタフェースに対して使用する。

#### 24.5.6 発信

---

[書式] **connect peer\_num**

[設定値] ◦ *peer\_num* ..... 発信相手の相手先情報番号

[説明] 手動で発信する。

#### 24.5.7 切断

---

[書式] **disconnect peer\_num**

[設定値] ◦ *peer\_num*

- 相手先情報番号
- all ..... すべての相手先情報番号
- anonymous ..... anonymous のすべて
- 指定した anonymous(anonymous1..)

[説明] 手動で切断する。

#### 24.5.8 DTCP セッションの手動接続

---

[書式] **tunnel dtcp connect**

[説明] DTCP の認証を開始する。

[ノート] DTCP 接続の設定が存在する場合には、起動時に自動的に認証が開始される。  
認証失敗が再接続回数の上限を超えて再接続を行わなくなった場合、あるいは、**tunnel dtcp disconnect** コマンドで強制的に切断した場合には、本コマンドを利用して接続動作を開始することができる。



### 24.5.9 DTCP セッションの手動切断

- [書式]           **tunnel dtcp disconnect**
- [説明]           DTCP の接続を強制的に切断する。

### 24.5.10 ping の実行

- [書式]           **ping** [-s *datalen*] [-c *count*] [-sa *ip\_address*] [-w *wait*] *host*
- [設定値]
  - *datalen* ..... データ長 (64..65535)
  - *count* ..... 実行回数 (1..21474836)
  - *ip\_address* ..... 始点 IP アドレス (*xxx.xxx.xxx.xxx* (*xxx* は十進数))
  - *wait* ..... パケット送信間隔秒数 (0.1..99.9)
  - *host*
    - ping をかけるホストの IP アドレス (*xxx.xxx.xxx.xxx* (*xxx* は十進数))
    - ping をかけるホストの名称
- [説明]           ICMP Echo を指定したホストに送出し、ICMP Echo Reply が送られてくるのを待つ。送られてきたら、その旨を表示する。コマンドが終了すると簡単な統計情報を表示する。  
*count* パラメータを省略すると、Ctrl+c キーを入力するまで実行を継続する。  
 -w オプションを指定した時には、次のパケットを送信するまでの間に相手からの返事を確認できなかった時にはその旨のメッセージを表示する。-w オプションを指定していない時には、パケットが受信できなくても何もメッセージを表示しない。
- [ノート]        一般ユーザモードでも実行することが可能。
- [初期値]        データ長: 64 バイト  
 送信回数: Ctrl+c キーが入力されるまで無限に繰り返す  
 始点 IP アドレス: ルータ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  
 送信間隔: 1 秒

### 24.5.11 ping6 の実行

- [書式]           **ping6** *destination* [*count*]  
**ping6** *destination*%*scope\_id* [*count*]  
**ping6** *destination* *interface* [*count*]  
**ping6** *destination* pp *peer\_num* [*count*]  
**ping6** *destination* tunnel *tunnel\_num* [*count*]
- [設定値]
  - *destination* ..... 送信する宛先の IPv6 アドレス、または名前
  - *scope\_id* ..... スコープ識別子
  - *interface* ..... LAN インタフェース名
  - *peer\_num* ..... 相手先情報番号
  - *tunnel\_num* ..... トンネルインタフェース番号
  - *count* ..... 送信回数 (1..21474836)
- [説明]           指定した宛先に対して ICMPv6 Echo Request を送信する。  
 スコープ識別子は、**show ipv6 address** コマンドで表示できる。
- [ノート]        一般ユーザモードでも実行することが可能。

### 24.5.12 traceroute の実行

- [書式]           **traceroute** *host* [noresolv]
- [設定値]
  - *host*
    - traceroute をかけるホストの IP アドレス (*xxx.xxx.xxx.xxx* (*xxx* は十進数))
    - traceroute をかけるホストの名称
  - noresolv ..... DNS による解決を行なわないことを示すキーワード
- [説明]           指定したホストまでの経路を調べて表示する。

[ノート] 一般ユーザモードでも実行することが可能。

### 24.5.13 traceroute6 の実行

---

[書式] **traceroute6 destination**

[設定値] ◦ *destination*..... 送信する宛先の IPv6 アドレス、または名前

[説明] 指定した宛先までの経路を調べて表示する。

[ノート] 一般ユーザモードでも実行することが可能。

### 24.5.14 nslookup

---

[書式] **nslookup host**

[設定値] ◦ *host*

- IP アドレス (xxx.xxx.xxx.xxx(xxx は十進数))
- ホスト名

[説明] DNS による名前解決を行なう。

### 24.5.15 メールチェックの結果の消去

---

[書式] **clear mail-check info [server\_num]**

[設定値] ◦ *server\_num*

- サーバー番号 (1..5)
- 省略時はすべてのサーバー番号

[説明] メール着信情報をクリアする。

### 24.5.16 TELNET クライアント

---

[書式] **telnet host [port [mode [negotiation [abort]]]]**

[設定値] ◦ *host*..... TELNET をかける相手のホスト名、もしくは IP アドレス

◦ *port*..... 使用するポート番号

- 十進数
- ポート番号の二一モニク
- 省略時は 23 (TELNET)

◦ *mode*..... TELNET 通信 (送信) の動作モード

- *character*..... 文字単位で通信する
- *line*..... 行単位で通信する
- *auto*..... *port* パラメータの設定値により *character/line* を選択
- 省略時は *auto*

◦ *negotiation*..... TELNET オプションのネゴシエーションの選択

- *on*..... ネゴシエーションする
- *off*..... ネゴシエーションしない
- *auto*..... *port* パラメータの設定値により *on/off* を選択
- 省略時は *auto*

◦ *abort*..... TELNET クライアントを強制的に終了させるためのアボートキー

- 十進数の ASCII コード
- 省略時は 29(^)

[説明] TELNET クライアントを実行する。

[ノート] *character* モードは、通常の TELNET サーバーなどへの接続のための透過的な通信を行なう。  
*line* モードは、入力行を編集して行単位の通信を行なう。行編集の終了は、改行コード (CR:0x0d または LF:0x0a) の入力で判断する。

ポート番号による機能自動選択について

1. TELNET 通信の動作モードの自動選択

*port* 番号が 23 の場合は文字単位モードとなり、そうでない場合は行単位モードとなる。

2. TELNET オプションのネゴシエーションの自動選択

*port* 番号が 23 の場合はネゴシエーションし、そうでない場合はネゴシエーションしない。

[ 初期値 ]  
 port = 23  
 mode = auto  
 negotiation = auto  
 abort = 29

#### 24.5.17 IPv4 動的フィルタのコネクション管理情報の削除

[ 書式 ]            **disconnect ip connection** *session\_id* [*channel\_id*]

[ 設定値 ]        ◦ *session\_id* ..... セッションの識別子  
 ◦ *channel\_id* ..... チャンネルの識別子

[ 説明 ]           指定したセッションに属する特定のチャンネルを削除する。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。

#### 24.5.18 IPv6 動的フィルタのコネクション管理情報の削除

[ 書式 ]            **disconnect ipv6 connection** *session\_id* [*channel\_id*]

[ 設定値 ]        ◦ *session\_id* ..... セッションの識別子  
 ◦ *channel\_id* ..... チャンネルの識別子

[ 説明 ]           指定したセッションに属する特定のチャンネルを削除する。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。

#### 24.5.19 ファームウェアのチェックおよびリビジョンアップ

[ 書式 ]            **http revision-up go** [no-confirm]

[ 設定値 ]        ◦ no-confirm ..... 書き換え可能なリビジョンのファームウェアが存在するときに、ファームウェアの更新を行なうかどうかを確認しない

[ 説明 ]           WEB サーバーに置いてあるファームウェアと現在のファームウェアのリビジョンをチェックして、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なう。  
 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リビジョンアップを行なう。

**http revision-up permit** コマンドで HTTP リビジョンアップを許可していない場合には、ファームウェアのリビジョンアップは行なわない。

**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には、WEB サーバーに置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なう。

なお、WEB サーバーに置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なわない。

#### 24.5.20 Magic Packet の送信

[ 書式 ]            **wol send** [*i interval*] [-c *count*] *interface mac\_address* [*ip\_address* [*udp port*]]  
**wol send** [*i interval*] [-c *count*] *interface mac\_address* ethernet type

- [設定値]
- *interval* ..... パケットの送信間隔 (秒)
  - *count* ..... パケットの送信回数
  - *interface* ..... LAN インタフェース名
  - *mac\_address* ..... MAC アドレス
  - *ip\_address* ..... IPv4 アドレス
  - *port* ..... UDP ポート番号
  - *type* ..... イーサネットタイプフィールドの値 (1501..65535)

[説明] 指定した LAN インタフェースに Magic Packet を送信する。

第 1 書式では、IPv4 UDP パケットとして UDP ペイロードに Magic Packet データシーケンスを格納したパケットを送信する。終点 IP アドレスと、終点 UDP ポート番号を指定できるが、省略した場合には、終点 IP アドレスとしてはインタフェースのディレクティッドブロードキャストアドレスが、終点ポート番号には 9(discard) が使われる。

また、終点 IP アドレスを指定した場合にはユニキャストでパケットを送信する。その場合、通常のルーティングや ARP の手順は踏まず、終点 MAC アドレスはコマンドで指定したものになる。終点 IP アドレスを省略した場合にはブロードキャストでパケットを送信する。

第 2 書式では、Ethernet ヘッダの直後から Magic Packet のデータシーケンスが始まるパケットを送信する。

どちらの形式でも、-i、-c オプションで Magic Packet の送信間隔および回数を指定できる。パケットの送信中でも、^C キーでコマンドを中断できる。

[ノート] 本製品が直結している LAN インタフェース以外には Magic Packet を送信できない。

[初期値] *interval* = 1  
*count* = 4



## 25.6 ファイル情報の一覧の表示

---

- [書式]            **show file list** *location*  
                  **less file list** *location*
- [設定値]        ◦ *location* ..... 表示するファイルのある位置  
                  • *internal* ..... 内蔵フラッシュ ROM
- [説明]            指定した場所に格納されているファイルの情報を表示する。

## 25.7 インタフェースに付与されている IPv6 アドレスの表示

---

- [書式]            **show ipv6 address**
- [設定値]        なし
- [説明]            すべてのインタフェースについて、付与されている IPv6 アドレスを表示する。

## 25.8 SSH サーバー 公開鍵の表示

---

- [書式]            **show sshd public key**
- [説明]            SSH サーバーの公開鍵を表示する。



## 26.5 侵入情報の履歴の表示

---

- [書式]           **show ip intrusion detection**  
                  **show ip intrusion detection interface** [direction]  
                  **show ip intrusion detection pp** [peer\_num] [direction]  
                  **show ip intrusion detection tunnel** [tunnel\_num] [direction]
- [設定値]           ○ *interface* ..... LAN インタフェース名  
                  ○ *peer\_num* ..... 相手先情報番号  
                  ○ *tunnel\_num* ..... トンネルインタフェース番号  
                  ○ *direction*  
                  • *in* ..... 入力方向  
                  • *out* ..... 出力方向
- [説明]            最近の侵入情報を表示する。各インタフェースの各方向ごとに最大 50 件まで表示できる。

## 26.6 IPv6 の経路情報の表示

---

- [書式]           **show ipv6 route**  
                  **show ipv6 route detail**  
                  **show ipv6 route summary**
- [設定値]           ○ *detail* ..... 現在有効な IPv6 経路に加えて隠されている IPv6 経路も表示する  
                  ○ *summary* ..... IPv6 の経路数をプロトコル毎に合計して表示する
- [説明]            IPv6 の経路情報を表示する。  
  
                  *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。

## 26.7 近隣キャッシュの表示

---

- [書式]           **show ipv6 neighbor cache**
- [設定値]           なし
- [説明]            近隣キャッシュの状態を表示する。

## 26.8 IPv6 の RIP テーブルの表示

---

- [書式]           **show ipv6 rip table**
- [設定値]           なし
- [説明]            IPv6 の RIP テーブルを表示する。



## 26.9 IPv6 の動的フィルタによって管理されているコネクションの表示

---

- [書式]           **show ipv6 connection**  
                  **show ipv6 connection interface** [*direction*]  
                  **show ipv6 connection pp** [*peer\_num* [*direction*]]  
                  **show ipv6 connection tunnel** [*tunnel\_num* [*direction*]]  
                  **show ipv6 connection summary**
- [設定値]        ◦ *interface* ..... LAN インタフェース名  
                  ◦ *peer\_num* ..... 相手先情報番号  
                  ◦ *tunnel\_num* ..... トンネルインタフェース番号  
                  ◦ *direction*  
                    • *in* ..... 入力方向  
                    • *out* ..... 出力方向  
                  ◦ *summary* ..... インタフェース / 方向単位の管理コネクション数、および全体の合計を表示する
- [説明]           指定したインタフェースについて、動的なフィルタによって管理されているコネクションを表示する。インタフェースを指定しないときには、すべてのインタフェースの情報を表示する。

## 26.10 ネットワーク監視機能の状態の表示

---

- [書式]           **show status ip keepalive**
- [設定値]        なし
- [説明]           ネットワーク監視機能の状態を表示する。

## 26.11 相手先ごとの接続時間情報の表示

---

- [書式]           **show pp connect time** [*peer\_num*]
- [設定値]        ◦ *peer\_num*  
                  • 相手先情報番号  
                  • *anonymous*  
                  • 省略時、選択されている相手について表示する
- [説明]           選択されている相手の接続時間情報を表示する。

## 26.12 動的 NAT ディスクリプタのアドレスマップの表示

---

- [書式]           **show nat descriptor address** [*nat\_descriptor*]
- [設定値]        ◦ *nat\_descriptor*  
                  • NAT ディスクリプタ番号 (1..21474836)  
                  • *all* ..... すべての NAT ディスクリプタ番号
- [説明]           *nat\_descriptor* を省略した場合にはすべての NAT ディスクリプタ番号について表示する。動的な NAT ディスクリプタのアドレスマップを表示する。

## 26.13 動作中の NAT ディスクリプタの適用リストの表示

---

- [書式]           **show nat descriptor interface bind interface**  
                  **show nat descriptor interface bind pp**  
                  **show nat descriptor interface bind tunnel**
- [設定値]        ◦ *interface* ..... LAN インタフェース名
- [説明]           NAT ディスクリプタと適用インタフェースのリストを表示する。

## 26.14 LAN インタフェースのNAT ディスクリプタのアドレスマップの表示

---

- [書式]           **show nat descriptor interface address** *interface*  
**show nat descriptor interface address pp** *peer\_num*  
**show nat descriptor interface address tunnel** *tunnel\_num*
- [設定値]       ○ *interface* ..... LAN インタフェース名  
○ *peer\_num* ..... 相手先情報番号  
○ *tunnel\_num* ..... トンネルインタフェース番号
- [説明]           インタフェースに適用されている NAT ディスクリプタのアドレスマップを表示する。

## 26.15 起動時の情報の表示

---

- [書式]           **show status boot**
- [設定値]       なし
- [説明]           起動の理由等の情報を表示します。

## 26.16 インタフェースの状態の表示

---

- [書式]           **show status interface**
- [設定値]       ○ *interface*  
                  • BRI インタフェース名  
                  • LAN インタフェース名
- [説明]           インタフェースの状態を表示する。  
BRI インタフェースを指定した場合は、接続状況とエラー情報（障害情報）を表示する。

## 26.17 各相手先の状態の表示

---

- [書式]           **show status pp** [*peer\_num*]
- [設定値]       ○ *peer\_num*  
                  • 相手先情報番号  
                  • anonymous  
                  • 省略時、選択されている相手について表示する
- [説明]           各相手先の接続中または最後に接続された場合の状態を表示する。  
                  • 現在接続されているか否か  
                  • 直前の呼の状態  
                  • 接続（切断）した日時  
                  • 回線の種類  
                  • 通信時間  
                  • 切断理由  
                  • 通信料金  
                  • 相手とこちらの PP 側 IP アドレス  
                  • 正常に送信したパケットの数  
                  • 送信エラーの数と内分け  
                  • 正常に受信したパケットの数  
                  • 受信エラーの数と内分け  
                  • PPP の状態  
                  • CCP の状態  
                  • その他

## 26.18 トンネルインタフェース情報の表示

---

- [書式]           **show status tunnel** *tunnel\_num*
- [設定値]       ○ *tunnel\_num* ..... トンネルインタフェース番号 (1..30)
- [説明]           トンネルインタフェースの情報を表示する。

## 26.19 DTCP セッション情報の表示

---

[書式] **show status dtcp**

[説明] DTCP を設定したトンネルインタフェースごとに以下の情報を表示する。

- *Status*..... 現在の状態
- *Timer* ..... 現在の状態を維持する最大残り時間
- *Server Name* ..... 接続する DTCP サーバーのアドレスまたはドメイン名
- *User Name* ..... 認証用のユーザ名
- *Local Endpoint* ..... IPv6 over IPv4 トンネルに使用する自分側の端点の IP アドレス
- *Remote Endpoint* .. IPv6 over IPv4IP トンネルに使用する相手側の端点の IP アドレス
- *Prefix* ..... DTCP 認証時に割り当てられた IPv6 のプレフィックス
- *Retry Count* ..... 再接続の残り回数  
無制限の場合は *infinity* と表示される

## 26.20 DHCP サーバーの状態の表示

---

[書式] **show status dhcp**

[設定値] なし

[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 スコープの全アドレス数
- 除外アドレス数
- 割り当て中アドレス数
- 利用可能アドレス数 (うち予約済 IP アドレス数)

## 26.21 DHCP クライアントの状態の表示

---

[書式] **show status dhcpc**

[設定値] なし

[説明] DHCP クライアントの状態を表示する。

- クライアントの状態
  - インタフェース
  - IP アドレス (取得できないときはその状態)
  - DHCP サーバー
  - リース残時間
  - クライアント ID
  - ホスト名 (設定時)
- 共通情報
  - DNS サーバー
  - ゲートウェイ

## 26.22 DHCPv6 の状態の表示

---

[書式] **show status ipv6 dhcp**

[設定値] なし

[説明] DHCPv6 に関する状態を表示する。

## 26.23 MLD の状態の表示

---

[書式] **show status ipv6 mld**

- [ 説明 ] MLD で管理されている情報を一覧表示する。  
MLD プロキシが動作している場合は、このコマンドで転送先を確認することができる。

---

### 26.24 PPTP の状態の表示

- [ 書式 ] **show status pptp**
- [ 設定値 ] なし
- [ 説明 ] PPTP の状態や GRE の統計情報などを表示する。

---

### 26.25 アナログ関係の状態の表示

- [ 書式 ] **show status analog [port]**
- [ 設定値 ] ◦ *port*
- 1..... TEL1 ポート
  - 2..... TEL2 ポート
  - 省略時はすべての TEL ポートを表示する
- [ 説明 ] アナログ関係の状態を表示する。

---

### 26.26 音声通話の接続状態の表示

- [ 書式 ] **show status voice call**
- [ 設定値 ] なし
- [ 説明 ] すべての音声通話の接続状態を表示する。

---

### 26.27 メールチェックの状態表示

- [ 書式 ] **show status mail-check [server\_num]**
- [ 設定値 ] ◦ *server\_num*
- サーバー番号 (1..5)
  - 省略時はすべてのサーバー番号
- [ 説明 ] 先のメールチェックの実行結果を表示する。  
サーバー情報、未読メール数、チェックした時刻を一覧表示する。

---

### 26.28 UPnP に関するステータス情報の表示

- [ 書式 ] **show status upnp**
- [ 設定値 ] なし
- [ 説明 ] UPnP に関するステータス情報を表示する。

---

### 26.29 パケットバッファの状態を表示する

- [ 書式 ] **show status packet-buffer [group]**
- [ 設定値 ] ◦ *group* ..... 表示するパケットバッファのグループを指定する。グループ名: small, middle, large, huge パラメータを省略すると、すべてのグループを表示する。

[ 説明 ]           パケットバッファの状態を表示する。表示する項目は以下の通り：

- グループ名
- 格納できるパケットサイズ
- 管理パラメータ
- 現在、割り当て中のパケットバッファ数
- 現在、フリーリストにつながれているパケットバッファ数
- 現在、確保しているチャンク数
- パケットバッファの割り当て要求を受けた回数
- パケットバッファの割り当てに成功した回数
- パケットバッファの割り当てに失敗した回数
- パケットバッファが解放された回数
- チャンクを確保した回数
- チャンクを確保しようとして失敗した回数
- チャンクを解放した回数

[ 実行例 ]           # show status packet-buffer large  
 large group: 2048 bytes length  
 parameters: max-buffer=20000 max-free=562 min-free=12  
                   buffers-in-chunk=125 initial-chunk=4  
 340 buffers in free list  
 160 buffers are allocated, req/succ/fail/rel = 266/266/0/106  
 4 chunks are allocated, req/succ/fail/rel = 4/4/0/0

## 26.30 QoS ステータスの表示

[ 書式 ]           **show status qos info** [*interface* [*class*]]

[ 設定値 ]           ○ *info*..... 表示する情報の種類

- *bandwidth* ..... 使用帯域
- *length* ..... キューイングしているパケット数
- *all* ..... 使用帯域とキューイングしているパケット数

○ *interface* ..... LAN インタフェース名  
                   省略時、すべての LAN インタフェースについて表示する

○ *class* ..... クラス (1..100)

[ 説明 ]           インタフェースに対して、QoS の設定情報や各クラスの使用状況を表示する。

- LAN インタフェース名
- キューイングアルゴリズム
- インタフェース速度
- クラス数
- 各クラスの設定帯域、使用帯域、使用帯域のピーク値と記録日時
- 設定帯域の合計
- 各クラスのエンキュー成功回数 / 失敗回数、デキュー回数、保持しているパケット数、パケット数のピーク値と記録日時

## 26.31 連携動作の状態の表示

[ 書式 ]           **show status cooperation type** [*id*]

[ 設定値 ]           ○ *type* ..... 連携動作タイプ

- *bandwidth-measuring* ..... 回線帯域検出
- *load-watch* ..... 負荷監視通知

○ *id* ..... 相手先 ID 番号 (1-100)

[説明] 連携動作の情報を表示する。

回線帯域検出の場合、以下の項目が表示される。

- 相手先情報
- 状態表示
  - 回数
  - 測定時刻
  - 測定結果 (クライアント動作のみ)
  - 現状 (クライアント動作のみ)
  - 設定変更履歴 (クライアント動作のみ)
  - 次の測定までの残り時間 (クライアント動作のみ)

負荷監視通知の場合、以下の項目が表示される。

- 相手先情報
- 状態表示
  - 抑制要請回数
  - 抑制解除回数
  - 履歴

### 26.32 ルータにログインしているユーザの情報を表示する

---

[書式] **show status user**

[説明] ルータにログインしているユーザの情報を表示する。以下の内容が表示される。

- ユーザ名
- 接続種別
- 接続した時間
- アイドル時間
- 接続相手の IP アドレス
- 管理ユーザか否か

自分自身のユーザ情報には、先頭にアスタリスク (\*) が付く。

管理者モードになっているユーザは、ユーザ名の前にプラス (+) が付く。

### 26.33 USB ホスト機能の動作状態を表示

---

[書式] **show status usbhost**

[設定値] なし

[説明] USB ホスト機能の動作状態を表示する。

## 27. ロギング

### 27.1 ログの表示

---

- [書式]           **show log** [reverse]  
                  **less log** [reverse]
- [設定値]        ◦ reverse ..... ログを逆順に表示する
- [説明]           ルータの動作状況を記録したログを表示する。

ログは最大 500 件保持することができる。最大数を越えた場合には、発生時刻の古いものから消去されていく。最大数以上のログを保存する場合には、**syslog host** コマンドでログを SYSLOG サーバーに転送して、そちらで保存する必要がある。

このコマンドでは、通常は発生時刻の古いものからログを順に表示するが、'reverse' を指定することで新しいものから表示させることができる。

ログは、ルータの電源を切ると消去される。

- [ノート]        電源を切らない限りはログは保存される。

### 27.2 アカウントの表示

---

- [書式]           **show account**  
                  **show account interface**  
                  **show account pp** [peer\_num]
- [設定値]        ◦ *interface*  
                  • BRI インタフェース名
- *peer\_num*  
                  • 相手先情報番号  
                  • anonymous  
                  • 省略時、選択されている相手について表示する
- [説明]           以下の項目を表示  
                  • 発信回数  
                  • 着信回数  
                  • ISDN 料金の総計
- [ノート]        課金額は通信の切断時に ISDN 回線を通じて通知される料金情報を集計しているため、割引サービスなどを利用している場合には、最終的に請求される料金とは異なる場合がある。また、弊社以外の通信事業者を利用して通信した場合には料金情報は通知されないため、アカウントとしても集計されない。

### 27.3 アナログ関係のアカウントの表示

---

- [書式]           **show account analog** [port]  
                  **show account analog total**
- [設定値]        ◦ *port*  
                  • 1 ..... TEL1 ポート  
                  • 2 ..... TEL2 ポート  
                  • 省略時は TEL ポートの合計を表示する
- total ..... 電話回線を示すキーワード
- [説明]           TEL ポートの発着信回数と課金合計を表示する。

- [ノート]
- ・ ISDN 回線を使用している場合  
課金額は通信の切断時に ISDN 回線を通じて通知される料金情報を集計しているため、割引サービスなどを利用している場合には、最終的に請求される料金とは異なる場合がある。また、弊社以外の通信事業者を利用して通信した場合には料金情報は通知されないため、アカウントとしても集計されない。
  - ・ アナログ回線を使用している場合  
アナログ回線では料金情報は通知されないため、アカウントとしても集計されない。

#### 27.4 アナログ回線のアカウントの表示

---

- [書式]            **show account pstn**
- [設定値]        なし
- [説明]            アナログ回線の発着信回数を表示する。

#### 27.5 通信履歴の表示

---

- [書式]            **show history**
- [設定値]        なし
- [説明]            通信履歴を表示する。



当社ホームページでは、各種商品の最新の情報などを提供しています。  
本商品を最適にご利用いただくために、定期的にご覧いただくことを  
お勧めします。

当社ホームページ

<http://web116.jp/ced/>

<http://www.ntt-west.co.jp/kiki/>

使い方等で不明の点がございましたら、NTT通信機器お取扱相談センタへお気軽  
にご相談ください。

### NTT通信機器お取扱相談センタ

- NTT東日本エリア(北海道、東北、関東、甲信越地区)でご利用のお客様

お問い合わせ先:  **0120-970413**

※携帯電話・PHS・050IP電話からのご利用は  
03-5667-7100(通話料金がかかります)

受付時間 9:00~21:00

※年末年始12月29日~1月3日は休業とさせていただきます。

- NTT西日本エリア(東海、北陸、近畿、中国、四国、九州地区)でご利用のお客様

本商品の取り扱いおよび故障に関するお問い合わせ

お問い合わせ先:  **0120-248995**

(携帯電話・PHSからもご利用可能です)

### 受付時間

- 本商品のお取扱いに関するお問い合わせ:

9:00~21:00(年末年始12月29日~1月3日を除く)

- 故障に関するお問合わせ:24時間(年中無休)※

※故障修理対応時間は9:00~17:00です。

電話番号をお間違えにならないように、ご注意願います。