

YAMAHA *Broadband & Remote ROUTER*

コマンドリファレンス

Rev.6.03.11

Rev.7.00.01



- 本書の記載内容の一部または全部を無断で転載することを禁じます。
 - 本書の記載内容は将来予告なく変更されることがあります。
 - 本製品を使用した結果発生した情報の消失等の損失については、当社では責任を負いかねます。保証は本製品物損の範囲に限ります。予めご了承ください。
 - 本書の内容については万全を期して作成致しておりますが、記載漏れやご不審な点がございましたらご一報くださいますようお願い致します。
-
- ※ イーサネットは富士ゼロックス社の登録商標です。
 - ※ Windows は米国 Microsoft 社の登録商標です。
 - ※ NetWare は米国 Novell,Inc. の登録商標です。
 - ※ INS ネット 64、INS ネット 1500 は日本電信電話株式会社の登録商標です。
 - ※ 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	19
1.1 対応するプログラムのリビジョン	19
1.2 コマンドリファレンスの見方	19
1.3 インタフェース名について	19
1.4 no で始まるコマンドの入力形式について	20
1.5 相手先情報番号のモデルによる違いについて	20
1.6 コマンドの仕様変更について	20
2. ヘルプ	21
2.1 コンソールに対する簡易説明の表示	21
2.2 コマンド一覧の表示	21
3. 機器の設定	22
3.1 ログインパスワードの設定	22
3.2 管理パスワードの設定	22
3.3 セキュリティクラスの設定	22
3.4 ログインタイマの設定	23
3.5 タイムゾーンの設定	23
3.6 現在の日付けの設定	23
3.7 現在の時刻の設定	23
3.8 リモートホストによる時計の設定	24
3.9 NTP による時計の設定	24
3.10 コンソールの言語とコードの設定	24
3.11 コンソールの表示文字数の設定	25
3.12 コンソールの表示行数の設定	25
3.13 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	25
3.14 コンソールのプロンプト表示の設定	25
3.15 SYSLOG を受けるホストの IP アドレスの設定	26
3.16 SYSLOG ファシリティの設定	26
3.17 NOTICE タイプの SYSLOG を出力するか否かの設定	26
3.18 INFO タイプの SYSLOG を出力するか否かの設定	26
3.19 DEBUG タイプの SYSLOG を出力するか否かの設定	27
3.20 TFTP によりアクセスできるホストの IP アドレスの設定	27
3.21 SYSLOG パケットの始点ポート番号の設定	27
3.22 マスタクロック用インタフェースの設定	28
3.23 電源の設定	28
3.24 温度監視の閾値の設定	29
3.25 LAN インタフェースの動作タイプの設定	30
4. ISDN 関連の設定	31
4.1 自分側の設定	31
4.1.1 BRI 回線の種類の指定	31
4.1.2 自分の ISDN 番号の設定	31
4.1.3 課金額による発信制限の設定	32
4.1.4 PIAFS の発信方式の設定	32
4.1.5 PIAFS の着信を許可するか否かの設定	33
4.1.6 PIAFS 接続時の起動側の指定	33
4.1.7 専用線がダウンした時にバックアップする相手先情報番号の設定	33
4.1.8 常時接続の設定	34
4.1.9 終端抵抗の設定	34
4.1.10 PP で使用するインタフェースの設定	34
4.2 相手側の設定	35
4.2.1 相手 ISDN 番号の設定	35
4.2.2 相手への発信順序の設定	35
4.2.3 自動接続の設定	35
4.2.4 自動切断の設定	36
4.2.5 着信許可の設定	36
4.2.6 発信許可の設定	36
4.2.7 再発信抑制タイマの設定	37

4.2.8	エラー切断後の再発信禁止タイマの設定	37
4.2.9	相手にコールバック要求を行うか否かの設定	37
4.2.10	コールバック要求タイプの設定	37
4.2.11	相手からのコールバック要求に応じるか否かの設定	38
4.2.12	コールバック受け入れタイプの設定	38
4.2.13	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	38
4.2.14	コールバックタイマの設定	38
4.2.15	コールバック待機タイマの設定	39
4.2.16	ISDN 回線を切断するタイマ方式の指定	39
4.2.17	切断タイマの設定 (ノーマル)	39
4.2.18	入力切断タイマの設定 (ノーマル)	40
4.2.19	出力切断タイマの設定 (ノーマル)	40
4.2.20	課金単位時間方式での課金単位時間と監視時間の設定	41
4.2.21	切断タイマの設定 (ファスト)	41
4.2.22	切断タイマの設定 (強制)	42
5.	IP の設定	43
5.1	インタフェース共通の設定	43
5.1.1	IP パケットを扱うか否かの設定	43
5.1.2	IP アドレスの設定	43
5.1.3	セカンダリ IP アドレスの設定	44
5.1.4	IP の静的経路情報の設定	45
5.1.5	IP パケットのフィルタの設定	46
5.1.6	フィルタセットの定義	47
5.1.7	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	47
5.1.8	Directed-Broadcast パケットをフィルタアウトするか否かの設定	48
5.1.9	動的フィルタの定義	48
5.1.10	動的フィルタのタイムアウトの設定	49
5.1.11	侵入検知機能の動作の設定	49
5.1.12	フィルタリングによるセキュリティの設定	50
5.1.13	IP パケットの TOS フィールドの書き換えの設定	51
5.1.14	インタフェースの MTU の設定	51
5.1.15	echo, discard, time サービスを動作させるか否かの設定	51
5.2	代理 ARP の設定	52
5.3	PP 側の設定	52
5.3.1	PP 側 IP アドレスの設定	52
5.3.2	リモート IP アドレスプールの設定	53
5.4	RIP の設定	53
5.4.1	RIP を使用するか否かの設定	53
5.4.2	RIP による経路の優先度の設定	53
5.4.3	RIP パケットの送信に関する設定	54
5.4.4	RIP パケットの受信に関する設定	54
5.4.5	RIP に関して信用できるゲートウェイの設定	55
5.4.6	RIP のフィルタリングの設定	55
5.4.7	RIP で加算するホップ数の設定	55
5.4.8	RIP2 での認証の設定	56
5.4.9	RIP2 での認証キーの設定	56
5.4.10	回線切断時の経路保持の設定	56
5.4.11	回線接続時の PP 側の RIP の動作の設定	57
5.4.12	回線接続時の PP 側の RIP 送出の時間間隔の設定	57
5.4.13	回線切断時の PP 側の RIP の動作の設定	57
5.4.14	回線切断時の PP 側の RIP 送出の時間間隔の設定	58
5.4.15	バックアップ時に RIP の送信元インタフェースを切り替えるか否かを設定する	58
5.5	VRRP の設定	59
5.5.1	インタフェース毎の VRRP の設定	59
5.5.2	シャットダウントリガの設定	60
5.6	バックアップの設定	60
5.6.1	プロバイダ接続がダウンした時にバックアップする接続先の指定	60
5.6.2	バックアップからの復帰待ち時間の設定	61
5.6.3	PP 経由のキープアライブを使用するか否かの設定	61
5.6.4	PP 経由のキープアライブのログをとるか否かの設定	62

5.6.5	PP 経由のキープアライブの時間間隔の設定	62
5.6.6	専用線ダウン検出時の動作の設定	62
5.6.7	LAN 経由でのプロバイダ接続がダウンした時にバックアップする接続先の指定	63
5.6.8	LAN 経由のキープアライブを使用するか否かの設定	63
5.6.9	LAN 経由のキープアライブの時間間隔の設定	64
5.6.10	バックアップからの復帰待ち時間の設定	64
5.6.11	LAN 経由のキープアライブのログをとるか否かの設定	64
6.	IPX の設定	65
6.1	インタフェース共通の設定	65
6.1.1	IPX パケットを扱うか否かの設定	65
6.1.2	IPX パケットのフィルタの設定	66
6.1.3	静的な SAP テーブルの設定	67
6.1.4	IPX SAP Get Nearest Server Request に応答するか否かの設定	67
6.2	LAN 側の設定	68
6.2.1	イーサネットフレームタイプの設定	68
6.2.2	LAN 側の IPX ネットワーク番号の設定	68
6.2.3	経路情報の追加	68
6.2.4	LAN 側の RIP/SAP フロードキャストの設定	69
6.2.5	LAN 側でのフィルタリングによるセキュリティの設定	69
6.3	PP 側相手毎の IPX の設定	69
6.3.1	IPX ルーティング許可の設定	69
6.3.2	PP 側 IPX ネットワーク番号の設定	70
6.3.3	経路情報の追加	70
6.3.4	回線接続時の PP 側の RIP/SAP の動作の設定	70
6.3.5	回線接続時の PP 側の RIP/SAP 送出の時間間隔の設定	71
6.3.6	回線切断時の PP 側の RIP/SAP の動作の設定	71
6.3.7	回線切断時の PP 側の RIP/SAP 送出の時間間隔の設定	71
6.3.8	回線切断時に RIP/SAP 情報を保持するか否かの設定	72
6.3.9	IPXWAN 使用の設定	72
6.3.10	Timer/Information Request の再送間隔と最大再送回数の設定	72
6.3.11	IPXWAN プライマリネットワーク番号の設定	72
6.3.12	Watchdog パケットに対する代理応答の設定	73
6.3.13	Watchdog 代理応答の時間間隔の設定	73
6.3.14	SPX キープアライブ代理応答を行うか否かの設定	73
6.3.15	SPX キープアライブ代理応答のタイマの設定	74
6.3.16	IPX シリアライゼーションパケットをフィルタアウトするか否かの設定	74
6.3.17	PP 側でのフィルタリングによるセキュリティの設定	74
7.	ブリッジの設定	75
7.1	インタフェース共通の設定	75
7.1.1	ブリッジ使用許可の設定	75
7.1.2	ブリッジするインタフェースの設定	75
7.1.3	ブリッジのフィルタの設定	76
7.1.4	MAC アドレスのラーニングを行うか否かの設定	76
7.1.5	ラーニング情報消去タイマの設定	76
7.2	LAN 側の設定	77
7.2.1	ラーニング情報の設定	77
7.2.2	LAN 側でのブリッジのフィルタリングの設定	77
7.3	PP 側相手毎のブリッジの設定	77
7.3.1	ラーニング情報の設定	77
7.3.2	PP 側でのブリッジのフィルタリングの設定	78
8.	PPP の設定	79
8.1	相手の名前とパスワードの設定	79
8.2	要求する認証タイプの設定	80
8.3	受け入れる認証タイプの設定	80
8.4	自分の名前とパスワードの設定	80
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	81

8.6	LCP 関連の設定	81
8.6.1	Address and Control Field Compression オプション使用の設定	81
8.6.2	Magic Number オプション使用の設定	81
8.6.3	Maximum Receive Unit オプション使用の設定	82
8.6.4	Protocol Field Compression オプション使用の設定	82
8.6.5	lcp-restart パラメータの設定	82
8.6.6	lcp-max-terminate パラメータの設定	83
8.6.7	lcp-max-configure パラメータの設定	83
8.6.8	lcp-max-failure パラメータの設定	83
8.6.9	Configure-Request をすぐに送信するか否かの設定	83
8.7	PAP 関連の設定	84
8.7.1	pap-restart パラメータの設定	84
8.7.2	pap-max-authreq パラメータの設定	84
8.8	CHAP 関連の設定	84
8.8.1	chap-restart パラメータの設定	84
8.8.2	chap-max-challenge パラメータの設定	84
8.9	IPCP 関連の設定	85
8.9.1	Van Jacobson Compressed TCP/IP 使用の設定	85
8.9.2	PP 側 IP アドレスのネゴシエーションの設定	85
8.9.3	ipcp-restart パラメータの設定	85
8.9.4	ipcp-max-terminate パラメータの設定	85
8.9.5	ipcp-max-configure パラメータの設定	86
8.9.6	ipcp-max-failure パラメータの設定	86
8.9.7	IPCP の MS 拡張オプションを使うか否かの設定	86
8.9.8	WINS サーバの IP アドレスの設定	86
8.10	IPXCP 関連の設定	87
8.10.1	ipxcp-restart パラメータの設定	87
8.10.2	ipxcp-max-terminate パラメータの設定	87
8.10.3	ipxcp-max-configure パラメータの設定	87
8.10.4	ipxcp-max-failure パラメータの設定	87
8.11	BCP 関連の設定	88
8.11.1	LAN Identification 使用の設定	88
8.11.2	Tinygram compression 使用の設定	88
8.11.3	bcp-restart パラメータの設定	88
8.11.4	bcp-max-terminate パラメータの設定	88
8.11.5	bcp-max-configure パラメータの設定	89
8.11.6	bcp-max-failure パラメータの設定	89
8.12	MSCBCP 関連の設定	89
8.12.1	mscbcp-restart パラメータの設定	89
8.12.2	mscbcp-maxretry パラメータの設定	89
8.13	CCP 関連の設定	90
8.13.1	全パケットの圧縮タイプの設定	90
8.13.2	ccp-restart パラメータの設定	90
8.13.3	ccp-max-terminate パラメータの設定	90
8.13.4	ccp-max-configure パラメータの設定	91
8.13.5	ccp-max-failure パラメータの設定	91
8.14	IPV6CP 関連の設定	91
8.14.1	IPV6CP を使用するか否かの設定	91
8.15	MP 関連の設定	91
8.15.1	MP を使用するか否かの設定	91
8.15.2	MP の制御方法の設定	92
8.15.3	MP のための負荷閾値の設定	92
8.15.4	MP の最大リンク数の設定	92
8.15.5	MP の最小リンク数の設定	93
8.15.6	MP のための負荷計測間隔の設定	93
8.15.7	MP のパケットを分割するか否かの設定	93
8.16	BACP 関連の設定	93
8.16.1	bacp-restart パラメータ の設定	93
8.16.2	bacp-max-terminate パラメータ の設定	94
8.16.3	bacp-max-configure パラメータ の設定	94
8.16.4	bacp-max-failure パラメータ の設定	94

8.17	BAP 関連の設定	94
8.17.1	bap-restart パラメータの設定	94
8.17.2	bap-max-retry パラメータの設定	95
8.18	PPPoE 関連の設定	95
8.18.1	PPPoE で使用する LAN インタフェースの指定	95
8.18.2	アクセスコンセントレータ名の設定	95
8.18.3	セッションの自動接続の設定	95
8.18.4	セッションの自動切断の設定	96
8.18.5	PADI パケットの最大再送回数の設定	96
8.18.6	PADI パケットの再送時間の設定	96
8.18.7	PADR パケットの最大再送回数の設定	96
8.18.8	PADR パケットの再送時間の設定	97
8.18.9	PPPoE セッションの切断タイムの設定	97
8.18.10	TCP パケットの MSS の制限の有無とサイズの指定	97
8.18.11	サービス名の指定	97
9.	DHCP の設定	98
9.1	DHCP サーバ・リレーエージェント機能	98
9.1.1	DHCP の動作の設定	98
9.1.2	RFC2131 対応動作の設定	99
9.1.3	DHCP スコープの定義	100
9.1.4	DHCP 予約アドレスの設定	101
9.1.5	DHCP オプションの設定	102
9.1.6	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	103
9.1.7	DHCP サーバの指定の設定	103
9.1.8	DHCP サーバの選択方法の設定	103
9.1.9	DHCP BOOTREQUEST パケットの中継基準の設定	104
9.2	DHCP クライアント機能	104
9.2.1	要求する IP アドレスリース期間の設定	104
9.2.2	IP アドレス取得要求の再送回数と間隔の設定	104
9.2.3	DHCP クライアント ID オプションの設定	105
9.2.4	DHCP クライアントのホスト名の設定	105
9.2.5	DNS サーバアドレスを取得する LAN インタフェースの設定	106
10.	ICMP の設定	107
10.1	IPv4 の設定	107
10.1.1	ICMP Echo Reply を送信するか否かの設定	107
10.1.2	ICMP Mask Reply を送信するか否かの設定	107
10.1.3	ICMP Parameter Problem を送信するか否かの設定	107
10.1.4	ICMP Redirect を送信するか否かの設定	108
10.1.5	ICMP Redirect 受信時の処理の設定	108
10.1.6	ICMP Time Exceeded を送信するか否かの設定	108
10.1.7	ICMP Timestamp Reply を送信するか否かの設定	108
10.1.8	ICMP Destination Unreachable を送信するか否かの設定	109
10.1.9	受信した ICMP のログを記録するか否かの設定	109
10.1.10	ステルス機能の設定	109
10.2	IPv6 の設定	110
10.2.1	ICMP Echo Reply を送信するか否かの設定	110
10.2.2	ICMP Parameter Problem を送信するか否かの設定	110
10.2.3	ICMP Redirect を送信するか否かの設定	110
10.2.4	ICMP Redirect 受信時の処理の設定	110
10.2.5	ICMP Time Exceeded を送信するか否かの設定	111
10.2.6	ICMP Destination Unreachable を送信するか否かの設定	111
10.2.7	受信した ICMP のログを記録するか否かの設定	111
10.2.8	ICMP Packet-Too-Big を送信するか否かの設定	111
10.2.9	ステルス機能の設定	112
11.	フレームリレー関連の設定	113
11.1	カプセル化の種類の設定	113
11.2	DLCI の設定	114
11.3	PVC 状態確認手順の設定	114

11.4	InARP 使用の設定	114
11.5	フレームリレーダウン時にバックアップする相手先情報番号の設定	115
11.6	FR 圧縮機能の設定	115
11.7	DLCI ごとのパラメータの設定	115
11.8	輻輳制御をするか否かの設定	116
11.9	回線に対する送信順序方式の設定	116
11.10	指定パケットに DE ビットを立てるか否かの設定	116
12.	PRI 関連の設定	117
12.1	PRI 回線の種類の設定	118
12.2	情報チャンネルとタイムスロットの設定	118
12.3	PP で使用するインタフェースの設定	119
13.	IPsec の設定	120
13.1	事前共有鍵の登録	121
13.2	相手側セキュリティ・ゲートウェイの IP アドレスの設定	121
13.3	相手側のセキュリティ・ゲートウェイの名前の設定	121
13.4	自分側セキュリティ・ゲートウェイの IP アドレスの設定	122
13.5	自分側のセキュリティ・ゲートウェイの名前の設定	122
13.6	鍵交換の再送回数と間隔の設定	122
13.7	IKE が用いる暗号アルゴリズムの設定	123
13.8	IKE が用いるグループの設定	123
13.9	IKE が用いるハッシュアルゴリズムの設定	123
13.10	自分側の ID の設定	124
13.11	IKE のログの種類の設定	124
13.12	IKE ペイロードのタイプの設定	124
13.13	PFS を用いるか否かの設定	125
13.14	相手側の ID の設定	125
13.15	IKE の情報ペイロードを送信するか否かの設定	125
13.16	IKE キープアライブ機能の設定	126
13.17	IKE キープアライブに関する SYSLOG を出力するか否かの設定	126
13.18	ESP を UDP でカプセル化して送受信するか否かの設定	126
13.19	IKE の鍵交換に失敗したときに鍵交換を休止せずに継続するか否かの設定	127
13.20	SA 関連の設定	127
13.20.1	SA のポリシーの定義	127
13.20.2	SA の寿命の設定	127
13.20.3	SA の削除	128
13.20.4	SA の手動更新	128
13.20.5	SA を自動更新するか否かの設定	128
13.21	トンネルインタフェース関連の設定	128
13.21.1	使用する SA のポリシーの設定	128
13.21.2	IPComp によるデータ圧縮の設定	129
13.21.3	トンネルインタフェースの使用許可の設定	129
13.21.4	トンネルインタフェースの使用不許可の設定	129
13.21.5	トンネルインタフェース番号の選択	130
13.21.6	トンネルバックアップの設定	130
13.22	トランスポートモード関連の設定	130
13.22.1	トランスポートモードの定義	130
14.	PPTP 機能の設定	131
14.1	共通の設定	131
14.1.1	PPTP サーバを動作させるか否かの設定	131
14.1.2	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	131
14.1.3	PPTP の動作タイプの設定	131
14.1.4	PPTP ホスト名の設定	132
14.1.5	PPTP パケットのウィンドウサイズの設定	132
14.1.6	PPTP の動作モードの設定	132
14.1.7	PPTP 暗号鍵生成のための認証方式の設定	132
14.1.8	PPTP 暗号鍵生成のための認証方式の設定	133
14.2	リモートアクセス VPN 機能	133
14.2.1	PPTP トンネルの切断タイムの設定	133
14.2.2	PPTP トンネルの端点の名前の設定	133
14.2.3	PPTP キープアライブの設定	134

14.2.4	PPTP キープアライブのログ設定	134
14.2.5	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	134
14.2.6	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	135
15.	SNMP の設定	136
15.1	読み出し専用のコミュニティ名の設定	136
15.2	読み書き可能なコミュニティ名の設定	136
15.3	認証失敗時 (authenticationFailure) にトラップを送信するか否かの設定	136
15.4	SNMP によるアクセスを許可するホストの設定	137
15.5	sysContact の設定	137
15.6	sysLocation の設定	137
15.7	sysName の設定	138
15.8	SNMP トラップのコミュニティ名の設定	138
15.9	SNMP トラップの送信先の設定	138
15.10	PP インタフェースの情報を MIB2 の範囲で表示するか否かの設定	138
15.11	PP インタフェースのアドレスの強制表示の設定	139
15.12	SNMP 送信パケットの始点アドレスの設定	139
16.	RADIUS の設定	140
16.1	RADIUS による認証を使用するか否かの設定	140
16.2	RADIUS によるアカウントを使用するか否かの設定	140
16.3	RADIUS サーバの指定	140
16.4	RADIUS 認証サーバの指定	141
16.5	RADIUS アカウントサーバの指定	141
16.6	RADIUS 認証サーバの UDP ポートの設定	141
16.7	RADIUS アカウントサーバの UDP ポートの設定	141
16.8	RADIUS シークレットの設定	142
16.9	RADIUS 再送信パラメータの設定	142
17.	NAT 機能	143
17.1	インタフェースへの NAT ディスクリプタ適用の設定	143
17.2	NAT ディスクリプタの動作タイプの設定	143
17.3	NAT 処理の外側 IP アドレスの設定	144
17.4	NAT 処理の内側 IP アドレスの設定	144
17.5	静的 NAT エントリの設定	144
17.6	IP マスカレード使用時に rlogin,rcp と ssh を使用するかどうかの設定	145
17.7	静的 IP マスカレードエントリの設定	145
17.8	NAT の IP アドレスマップの消去タイマの設定	145
17.9	IP マスカレードテーブルの TTL 処理方式の設定	146
17.10	外側から受信したパケットに該当する変換テーブルが存在しないときの動作の設定	146
17.11	NAT のアドレス割当をログに記録するか否かの設定	146
17.12	IP マスカレードで利用するポートの範囲の設定	147
17.13	FTP として認識するポート番号の設定	147
17.14	IP マスカレードで変換しないポート番号の範囲の設定	147
18.	DNS の設定	148
18.1	DNS を利用するか否かの設定	148
18.2	DNS サーバの IP アドレスの設定	148
18.3	DNS サーバを通知してもらおう相手先情報番号の設定	149
18.4	DNS 問い合わせの内容に応じた DNS サーバの選択	150
18.5	DNS ドメイン名の設定	150
18.6	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	151
18.7	DHCP/IPCP MS 拡張で DNS サーバを通知する順序の設定	151
18.8	SYSLOG 表示で DNS により名前解決するか否かの設定	151
18.9	静的 DNS レコードの登録	152
19.	優先制御／帯域制御	153
19.1	インタフェース速度の設定	153
19.2	クラス分けのためのフィルタ設定	153
19.3	キューイングアルゴリズムタイプの選択	155
19.4	デフォルトクラスの設定	156
19.5	クラス分けフィルタの適用	156
19.6	クラスの属性の設定	157

19.7	クラス毎のキュー長の設定	157
19.8	MP インタリーブの設定	158
20.	OSPF	159
20.1	OSPF の有効設定	159
20.2	OSPF の使用設定	159
20.3	OSPF による経路の優先度設定	159
20.4	OSPF のルータ ID 設定	159
20.5	外部プロトコルによる経路導入	160
20.6	外部経路導入に適用するフィルタ定義	161
20.7	OSPF エリア設定	161
20.8	エリアへの経路広告	162
20.9	スタブ的接続の広告	162
20.10	仮想リンク設定	163
20.11	指定インタフェースの OSPF エリア設定	164
20.12	非ブロードキャスト型ネットワークに接続されている OSPF ルータの指定	166
21.	BGP	167
21.1	経路の集約の設定	167
21.2	経路を集約するためのフィルタの設定	167
21.3	AS 番号の設定	167
21.4	BGP の設定の有効化	168
21.5	BGP で受信した経路に対するフィルタの適用	168
21.6	BGP で受信する経路に適用するフィルタの設定	168
21.7	BGP に導入する経路に対するフィルタの適用	169
21.8	BGP に導入する経路に適用するフィルタの設定	169
21.9	BGP による接続先の設定	170
21.10	BGP による経路の優先度の設定	170
21.11	ルータ ID の設定	170
21.12	BGP の起動の設定	171
22.	IPv6	172
22.1	共通の設定	172
22.1.1	IPv6 パケットを扱うか否かの設定	172
22.1.2	IPv6 インタフェースのリンク MTU の設定	172
22.2	IPv6 アドレスの管理	172
22.2.1	インタフェースの IPv6 アドレスの設定	172
22.2.2	インタフェースに付与されている IPv6 アドレスの表示	172
22.3	近隣探索	173
22.3.1	ルータ広告で配布するプレフィックスの定義	173
22.3.2	ルータ広告の送信の制御	174
22.4	経路制御	174
22.4.1	IPv6 の経路情報の追加	174
22.5	RIPng	175
22.5.1	RIPng の使用の設定	175
22.5.2	インタフェースにおける RIPng の送信ポリシーの設定	175
22.5.3	インタフェースにおける RIPng の受信ポリシーの設定	175
22.5.4	インタフェースにおける信頼できる RIPng ゲートウェイの設定	176
22.5.5	RIPng の加算ホップ数の設定	176
22.5.6	RIPng で送受信する経路に対するフィルタリングの設定	176
22.5.7	回線接続時の PP 側の RIPng の動作の設定	177
22.5.8	回線接続時の PP 側の RIPng 送出の時間間隔の設定	177
22.5.9	回線切断時の PP 側の RIPng の動作の設定	177
22.5.10	回線切断時の PP 側の RIPng 送出の時間間隔の設定	178
22.5.11	RIPng による経路を回線切断時に保持するか否かの設定	178
22.6	フィルタの設定	178
22.6.1	IPv6 フィルタの定義	178
22.6.2	IPv6 フィルタの適用	179
22.6.3	IPv6 動的フィルタの定義	179
22.7	トンネリング	180
22.7.1	トンネルインタフェースの種別の設定	180
22.7.2	トンネルインタフェースの端点 IP アドレスの設定	180

22.8	管理ツール	180
22.8.1	ping の実行	180
22.8.2	traceroute の実行	181
23.	スケジュール	182
23.1	スケジュールの設定	182
24.	操作	183
24.1	相手先情報番号の選択	183
24.2	設定に関する操作	183
24.2.1	管理ユーザへの移行	183
24.2.2	終了	183
24.2.3	設定内容の保存	183
24.2.4	設定ファイルの削除	184
24.2.5	実行形式ファームウェアファイルの削除	184
24.2.6	設定ファイルの一覧	184
24.2.7	設定の初期化	184
24.2.8	遠隔地のルータの設定	185
24.2.9	遠隔地のルータからの設定に対する制限	185
24.3	動的情報のクリア操作	185
24.3.1	ARP テーブルのクリア	185
24.3.2	IP の動的経路情報のクリア	185
24.3.3	IPX の動的経路情報のクリア	186
24.3.4	IPX の動的 SAP 情報のクリア	186
24.3.5	ブリッジのラーニング情報のクリア	186
24.3.6	ログのクリア	186
24.3.7	アカウントのクリア	186
24.3.8	InARP のクリア	187
24.3.9	DNS キャッシュのクリア	187
24.3.10	PRI のステータス情報のクリア	187
24.3.11	NAT アドレステーブルのクリア	187
24.3.12	インタフェースの NAT アドレステーブルのクリア	187
24.3.13	IPv6 の動的経路情報の消去	188
24.3.14	近隣キャッシュの消去	188
24.4	その他の操作	188
24.4.1	相手先の使用許可の設定	188
24.4.2	相手先の使用不許可の設定	188
24.4.3	再起動	189
24.4.4	インタフェースの再起動	189
24.4.5	PP インタフェースの再起動	189
24.4.6	発信	189
24.4.7	切断	190
24.4.8	ping	190
24.4.9	traceroute	190
24.4.10	telnet	191
24.4.11	telnet サーバ機能の ON/OFF の設定	191
24.4.12	telnet サーバ機能の listen ポートの設定	192
24.4.13	telnet サーバへアクセスできるホストの IP アドレスの設定	192
24.4.14	PRI のループバックの実行	193
24.4.15	PRI のループバック待ち受けの設定	194
24.4.16	ファームウェアファイルを内蔵フラッシュ ROM にコピー	194
24.4.17	IPv4 動的フィルタのコネクション管理情報の削除	194
24.4.18	IPv6 動的フィルタのコネクション管理情報の削除	195
25.	設定の表示	196
25.1	機器設定の表示	196
25.2	すべての設定内容の表示	196
25.3	指定した PP の設定内容の表示	196
25.4	ファイル情報の一覧の表示	196
25.5	マスタクロックを得ている回線の表示	197
26.	状態の表示	198

26.1	ARP テーブルの表示	198
26.2	インタフェースの状態の表示	198
26.3	各相手先の状態の表示	198
26.4	DHCP サーバの状態の表示	199
26.5	IP の経路情報テーブルの表示	199
26.6	IPX の経路情報テーブルの表示	199
26.7	IPv6 の経路情報の表示	199
26.8	近隣キャッシュの表示	200
26.9	SAP テーブルの表示	200
26.10	IPXWAN の状態の表示	200
26.11	ブリッジのラーニング情報の表示	200
26.12	RIP で得られた経路情報の表示	200
26.13	IPsec の SA の表示	201
26.14	VRRP の情報の表示	201
26.15	動的 NAT ディスクリプタのアドレスマップの表示	201
26.16	動作中の NAT ディスクリプタの適用リストの表示	201
26.17	LAN インタフェースの NAT ディスクリプタのアドレスマップの表示	202
26.18	OSPF 情報の表示	202
26.19	DHCP クライアントの状態の表示	202
26.20	BGP の状態の表示	202
26.21	動的フィルタによって管理されている接続の表示	203
26.22	IPv6 の RIP テーブルの表示	203
26.23	IPv6 の動的フィルタによって管理されている接続の表示	203
27.	ロギング	204
27.1	ログの表示	204
27.2	アカウントの表示	204

コマンド索引

A

account threshold	32
account threshold pp	32
administrator	183
administrator password	22

B

bgp aggregate	167
bgp aggregate filter	167
bgp autonomous-system	167
bgp configure refresh	168
bgp export	168
bgp export filter	168
bgp import	169
bgp import filter	169
bgp neighbor	170
bgp preference	170
bgp router id	170
bgp use	171
bridge filter	76
bridge group	75
bridge interface filter	77
bridge interface learning	77
bridge learning	76
bridge learning expire	76
bridge pp filter	78
bridge pp learning	77
bridge use	75

C

clear account	186
clear account pp	186
clear arp	185
clear bridge learning	186
clear dns cache	187
clear inarp	187
clear ip dynamic routing	185
clear ipv6 dynamic routing	188
clear ipv6 neighbor cache	188
clear ipx dynamic routing	186
clear ipx dynamic sap	186
clear log	186
clear nat descriptor dynamic	187
clear nat descriptor interface dynamic	187
clear nat descriptor interface dynamic pp	187
clear nat descriptor interface dynamic tunnel	187
clear pri status	187
cold start	184
connect	189
console character	24
console columns	25
console info	25
console lines	25
console prompt	25
copy exec	194

D

date	23
delete config	184
delete exec	184
dhcp client client-identifier	105

dhcp client hostname	105
dhcp duplicate check	103
dhcp relay select	103
dhcp relay server	103
dhcp relay threshold	104
dhcp scope	100
dhcp scope bind	101
dhcp scope option	102
dhcp server rfc2131 compliant	99
dhcp service	98
disconnect	190
disconnect ip connection	194
disconnect ipv6 connection	195
dns domain	150
dns notice order	151
dns private address spoof	151
dns server dhcp	106
dns server ip_address	148
dns server pp	149
dns server select	150
dns static	152
dns syslog resolv	151

E

exit	183
------	-----

F

fr backup	115
fr cir	115
fr compression use	115
fr congestion control	116
fr de	116
fr dlci	114
fr inarp	114
fr lmi	114
fr pp dequeue type	116

H

help	21
------	----

I

interface reset	189
interface reset pp	189
ip filter	46
ip filter directed-broadcast	48
ip filter dynamic	48
ip filter dynamic timer	49
ip filter set	47
ip filter source-route	47
ip host	152
ip icmp echo-reply send	107
ip icmp log	109
ip icmp mask-reply send	107
ip icmp parameter-problem send	20, 107
ip icmp redirect receive	108
ip icmp redirect send	108
ip icmp time-exceeded send	108
ip icmp timestamp-reply send	108
ip icmp unreachable send	109
ip interface address	43
ip interface dhcp lease time	104

ip interface dhcp retry	104	ipsec ike local address	122
ip interface intrusion detection	49	ipsec ike local id	124
ip interface mtu	51	ipsec ike local name	122
ip interface nat descriptor	143	ipsec ike log	124
ip interface ospf area	164	ipsec ike payload type	124
ip interface ospf neighbor	166	ipsec ike pfs	125
ip interface proxyarp	52	ipsec ike pre-shared-key	121
ip interface rip auth key	56	ipsec ike remote address	121
ip interface rip auth text	56	ipsec ike remote id	125
ip interface rip auth type	56	ipsec ike remote name	121
ip interface rip filter	55	ipsec ike retry	122
ip interface rip hop	55	ipsec ike send info	125
ip interface rip receive	54	ipsec ipcomp type	129
ip interface rip send	54	ipsec refresh sa	128
ip interface rip trust gateway	55	ipsec sa delete	128
ip interface secondary address	44	ipsec sa policy	127
ip interface secure filter	50	ipsec transport	130
ip interface vrrp	59	ipsec tunnel	128
ip interface vrrp shutdown trigger	60	ipv6 filter	178
ip pp address	43	ipv6 filter dynamic	179
ip pp intrusion detection	49	ipv6 icmp echo-reply send	110
ip pp nat descriptor	143	ipv6 icmp log	111
ip pp ospf area	164	ipv6 icmp packet-too-big send	111
ip pp remote address	52	ipv6 icmp parameter-problem send	110
ip pp remote address pool	53	ipv6 icmp redirect receive	110
ip pp rip auth key	56	ipv6 icmp redirect send	110
ip pp rip auth text	56	ipv6 icmp time-exceeded send	111
ip pp rip auth type	56	ipv6 icmp unreachable send	111
ip pp rip backup interface	58	ipv6 interface address	172
ip pp rip connect interval	57	ipv6 interface mtu	172
ip pp rip connect send	57	ipv6 interface rip filter	176
ip pp rip disconnect interval	58	ipv6 interface rip receive	175
ip pp rip disconnect send	57	ipv6 interface rip send	175
ip pp rip filter	55	ipv6 interface rip trust gateway	176
ip pp rip hold routing	56	ipv6 interface rtadv send	174
ip pp rip hop	55	ipv6 interface secure filter	179
ip pp rip receive	54	ipv6 pp address	172
ip pp rip send	54	ipv6 pp rip connect interval	177
ip pp rip trust gateway	55	ipv6 pp rip connect send	177
ip pp secure filter	50	ipv6 pp rip disconnect interval	178
ip route	45	ipv6 pp rip disconnect send	177
ip routing	43	ipv6 pp rip filter	176
ip simple-service	51	ipv6 pp rip hold routing	178
ip stealth	109	ipv6 pp rip hop	176
ip tos supersede	51	ipv6 pp rip receive	175
ip tunnel intrusion detection	49	ipv6 pp rip send	175
ip tunnel nat descriptor	143	ipv6 pp rip trust gateway	176
ip tunnel ospf area	164	ipv6 pp rtadv send	174
ip tunnel rip auth key	56	ipv6 pp secure filter	179
ip tunnel rip auth text	56	ipv6 prefix	173
ip tunnel rip auth type	56	ipv6 rip use	175
ip tunnel rip filter	55	ipv6 route	174
ip tunnel rip hop	55	ipv6 routing	172
ip tunnel rip receive	54	ipv6 stealth	112
ip tunnel rip send	54	ipv6 tunnel address	172
ip tunnel rip trust gateway	55	ipx filter	66
ip tunnel secure filter	50	ipx interface frame type	68
ipsec auto refresh	128	ipx interface network	68
ipsec ike always-on	127	ipx interface ripsap broadcast	69
ipsec ike duration ipsec-sa	127	ipx interface route	68
ipsec ike encryption	123	ipx interface secure filter	69
ipsec ike esp-encapsulation	126	ipx pp ipxwan primnet	72
ipsec ike group	123	ipx pp ipxwan retry	72
ipsec ike hash	123	ipx pp ipxwan use	72
ipsec ike keepalive log	126	ipx pp network	70
ipsec ike keepalive use	126	ipx pp ripsap connect interval	71

ipx pp ripsap connect send	70
ipx pp ripsap disconnect interval	71
ipx pp ripsap disconnect send	71
ipx pp ripsap hold	72
ipx pp route	70
ipx pp routing	69
ipx pp secure filter	74
ipx pp serialization filter	74
ipx pp spx keepalive proxy	73
ipx pp spx keepalive timer	74
ipx pp watchdog interval	73
ipx pp watchdog proxy	73
ipx routing	65
ipx sap	67
ipx sap response	67
isdn arrive permit	36
isdn auto connect	35
isdn auto disconnect	36
isdn call block time	37
isdn call permit	36
isdn call prohibit time	37
isdn callback msccbp user-specify	38
isdn callback permit	38
isdn callback permit type	38
isdn callback request	37
isdn callback request type	37
isdn callback response time	38
isdn callback wait time	39
isdn disconnect input time	40
isdn disconnect interval time	41
isdn disconnect output time	40
isdn disconnect policy	39
isdn disconnect time	39
isdn fast disconnect time	41
isdn forced disconnect time	42
isdn local address	31
isdn piafs arrive	33
isdn piafs call	32
isdn piafs control	33
isdn remote address	35
isdn remote call order	35
isdn terminator	34
L	
lan backup	63
lan backup recovery time	64
lan keepalive interval	64
lan keepalive log	64
lan keepalive use	63
lan type	30
leased backup	33
leased keepalive down	62
less config	196
less config list	184
less config pp	196
less file list	196
less log	204
line masterclock	28
line type	31, 118
login password	22
login timer	23
N	
nat descriptor address inner	144
nat descriptor address outer	144
nat descriptor ftp port	147
nat descriptor log	146
nat descriptor masquerade incoming	146
nat descriptor masquerade port range	147
nat descriptor masquerade rlogin	145
nat descriptor masquerade static	145
nat descriptor masquerade ttl hold	146
nat descriptor masquerade unconvertible port	147
nat descriptor static	144
nat descriptor timer	145
nat descriptor type	143
ntpdate	24
O	
ospf area	161
ospf area network	162
ospf area stubhost	162
ospf configure refresh	159
ospf import filter	161
ospf import from	160
ospf preference	159
ospf router id	159
ospf use	159
ospf virtual-link	163
P	
ping	190
ping6	180
pp	132
pp always-on	34
pp auth accept	80, 133
pp auth multi connect prohibit	81
pp auth myname	20, 80
pp auth request	80, 132
pp auth username	20, 79
pp backup	60
pp backup recovery time	20, 61
pp bind	34, 119, 131
pp disable	188
pp enable	188
pp encapsulation	113
pp keepalive interval	20, 62
pp keepalive log	20, 62
pp keepalive use	20, 61
pp select	183
ppp bacp maxconfigure	94
ppp bacp maxfailure	94
ppp bacp maxterminate	94
ppp bacp restart	93
ppp bap maxretry	95
ppp bap restart	94
ppp bcp lanid	88
ppp bcp maxconfigure	89
ppp bcp maxfailure	89
ppp bcp maxterminate	88
ppp bcp restart	88
ppp bcp tinycomp	88
ppp ccp maxconfigure	91
ppp ccp maxfailure	91
ppp ccp maxterminate	90
ppp ccp no-encryption	135
ppp ccp restart	90
ppp ccp type	90, 131
ppp chap maxchallenge	84
ppp chap restart	84

ppp ipcp ipaddress	85	queue pp class property	157
ppp ipcp maxconfigure	86	queue pp type	155
ppp ipcp maxfailure	86	quit	183
ppp ipcp maxterminate	85		
ppp ipcp msex	86	R	
ppp ipcp restart	85	radius account	140
ppp ipcp vjc	85	radius account port	141
ppp ipv6cp use	91	radius account server	141
ppp ipxcp maxconfigure	87	radius auth	140
ppp ipxcp maxfailure	87	radius auth port	141
ppp ipxcp maxterminate	87	radius auth server	141
ppp ipxcp restart	87	radius retry	142
ppp lcp acfc	81	radius secret	142
ppp lcp magicnumber	81	radius server	140
ppp lcp maxconfigure	83	rdate	24
ppp lcp maxfailure	83	remote setup accept	185
ppp lcp maxterminate	83	remote setup interface	185
ppp lcp mru	82	restart	189
ppp lcp pfc	82	rip preference	53
ppp lcp restart	82	rip use	53
ppp lcp silent	83		
ppp mp control	92	S	
ppp mp divide	93	save	183
ppp mp interleave	158	schedule at	182
ppp mp load threshold	92	security class	22
ppp mp maxlink	92	show account	204
ppp mp minlink	93	show account pp	204
ppp mp timer	93	show arp	198
ppp mp use	91	show bridge learning	200
ppp msbcpc maxretry	89	show command	21
ppp msbcpc restart	89	show config	196
ppp pap maxauthreq	84	show config list	184
ppp pap restart	84	show config pp	196
pppoe	97	show environment	196
pppoe access concentrator	95	show file list	196
pppoe auto connect	95	show ip connection	203
pppoe auto disconnect	96	show ip rip table	200
pppoe disconnect time	97	show ip route	199
pppoe padi maxretry	96	show ipsec sa	201
pppoe padi restart	96	show ipsec sa gateway	201
pppoe padr maxretry	96	show ipv6 address	172
pppoe padr restart	97	show ipv6 connection	203
pppoe service-name	97	show ipv6 neighbor cache	200
pppoe tcp mss limit	97	show ipv6 rip table	203
pppoe use	95	show ipv6 route	199
pptp call-id mode	132	show ipx wan	200
pptp hostname	132	show ipx route	199
pptp keepalive interval	134	show ipx sap	200
pptp keepalive log	134	show line masterclock	197
pptp keepalive use	134	show log	204
pptp service	131	show nat descriptor address	201
pptp service type	131	show nat descriptor interface address	202
pptp tunnel disconnect time	133	show nat descriptor interface bind	201
pptp window size	132	show status	198
pri leased channel	118	show status bgp	202
pri loopback active	193	show status dhcp	199
pri loopback passive	194	show status dhcpc	202
pri loopback passive off	194	show status ospf	202
		show status pp	198
		show status vrrp	201
		snmp community read-only	136
		snmp community read-write	136
		snmp display ipcp force	139
		snmp enableauthentraps	136
		snmp host	137
Q			
queue class filter	153		
queue interface class filter list	156		
queue interface class property	157		
queue interface default	156		
queue interface length	157		
queue interface type	155		

snmp local address	.139
snmp syscontact	.137
snmp syslocation	.137
snmp sysname	.138
snmp trap community	.138
snmp trap host	.138
snmp yrifppdisplayatmib2	.138
speed interface	.153
speed pp	.153
syslog debug	.27
syslog facility	.26
syslog host	.26
syslog info	.26
syslog notice	.26
syslog srcport	.27
system power 2 use	.28
system temperature threshold	.29

T

telnet	.191
telnetd host	.192
telnetd listen	.192
telnetd service	.191
tftp host	.27
time	.23
timezone	.23
traceroute	.190
traceroute6	.181
tunnel backup	.130
tunnel disable	.129
tunnel enable	.129
tunnel encapsulation	.20, 131, 180
tunnel endpoint address	.20, 131, 180
tunnel endpoint name	.133
tunnel select	.130

W

wins server	.86
-------------	-----

1. コマンドリファレンスの見方

1.1 対応するプログラムのリビジョン

このコマンドリファレンスは、YAMAHA ルータのファームウェア、**Rev.6.03.11** と **Rev.7.00.01** に対応しています。
このコマンドリファレンスの印刷より後にリリースされた最新のファームウェアや、マニュアル類および差分については以下に示す URL の WWW サーバにある情報を参照してください。

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

1.2 コマンドリファレンスの見方

このコマンドリファレンスは、ルータ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。

- 【入力形式】 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。
- 【パラメータ】 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。
- 【デフォルト値】 コマンドのデフォルト値を示します。
- 【設定例】 コマンドの具体例を示します。
- 【適用モデル】 コマンドが適用できるモデル名称を示します。網がけのかかったモデルはこのコマンドが使用できません。

1.3 インタフェース名について

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

また、YAMAHA リモートルータ RT300i の BRI 拡張モジュールのように、1 つのモジュールに複数のインタフェースがある場合には、インタフェース番号はモジュールに振られた番号とモジュール内の番号をピリオド (.) でつなげた形式となります。

例：

メインモジュール上の LAN	lan1
RTX2000 本体上の LAN	lan1.1, lan1.2, ..., lan1.8
メインモジュール上の BRI	bri1
1 つ目の LAN モジュール	lan2
1 つ目の 8BRI モジュール	bri2.1, bri2.2, ..., bri2.8
2 つ目の 8BRI モジュール	bri3.1, bri3.2, ..., bri3.8
1 つ目の PRI モジュール	pri1

20 1. コマンドリファレンスの見方

1.4 no で始まるコマンドの入力形式について

コマンドの入力形式に **no** で始まる形のもが並記されているコマンドが多数あります。**no** で始まる形式を使うと、特別な記述がない限り、そのコマンドの設定を削除し、デフォルト値に戻します。

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、たとえデフォルト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ら影響を与えません。

1.5 相手先情報番号のモデルによる違いについて

相手先情報番号はモデルによって使用できる数値の範囲が異なります。

モデル名称	相手先情報番号の範囲
RTX2000	1 - 100
RTX1000	1 - 30
RT300i	1 - 100
RT140p	1 - 100
RT140f	1 - 100
RT140i	1 - 100
RT140e	1 - 100
RT105p	1 - 30
RT105i	1 - 30
RT105e	1 - 30

1.6 コマンドの仕様変更について

プログラムの古いリビジョンから Rev.6.02.16 以降へ変更する場合には以下の注意が必要となります

- **ip icmp parameter-problem send** コマンドのデフォルト値が on から off に変更。
- **ip tunnel local address** コマンドを廃止し、**tunnel endpoint address** コマンドに統合。
- **ip tunnel remote address** コマンドを廃止し、**tunnel endpoint address** コマンドに統合。
- **ipv6 tunnel local address** コマンドを廃止し、**tunnel endpoint address** コマンドに統合。
- **ipv6 tunnel remote address** コマンドを廃止し、**tunnel endpoint address** コマンドに統合。
- **tunnel encapsulation** コマンドのパラメータ `6over4`, `4over6` キーワードを廃止し、**ipip** キーワードに統合。
- **pp auth username** と **pp auth myname** コマンドの名前とパスワードの文字数が最大 64 文字以内に変更。
- **leased backup recovery time** コマンドを廃止し、**pp backup recovery time** に統合。
- **leased keepalive use** コマンドを廃止し、**pp keepalive use** に統合。
- **leased keepalive interval** コマンドを廃止し、**pp keepalive interval** に統合。
- **leased keepalive log** コマンドを廃止し、**pp keepalive log** に統合、デフォルト値は off。

プログラムの古いリビジョンから Rev.6.02.19 以降へ変更する場合には以下の注意が必要となります

- **pppoe access concentrator** と **pppoe service-name** コマンドの入力可能文字数が最大 255 文字以内に変更。
- **ipsec ike encryption** と **ipsec sa policy** コマンドのアルゴリズムとして AES-CBC が指定可能。

プログラムの古いリビジョンから Rev.6.03.04 以降へ変更する場合には以下の注意が必要となります

- **nat descriptor timer** コマンドの入力形式を拡張。プロトコルが指定可能。
- **lan keepalive use** コマンドのパラメータを拡張して、ダウン検出とアップ検出をそれぞれ指定可能。
- **pp keepalive use** コマンドのパラメータを拡張して、ダウン検出とアップ検出をそれぞれ指定可能。

2. ヘルプ

2.1 コンソールに対する簡易説明の表示

【入力形式】 **help**

【パラメータ】 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。

【適用モデル】

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

2.2 コマンド一覧の表示

【入力形式】 **show command**

【パラメータ】 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。

【適用モデル】

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

3. 機器の設定

3.1 ログインパスワードの設定

[入力形式] **login password**

[パラメータ] 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。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

3.2 管理パスワードの設定

[入力形式] **administrator password**

[パラメータ] 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。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

3.3 セキュリティクラスの設定

[入力形式] **security class level forget telnet**
no security class [*level forget telnet*]

[パラメータ] ◦ *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、エー) でもログインでき、設定の変更も可能になる。ただしシリアルのみ
- off パスワードを入力しないとログインできない

◦ *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機種だけが持つ機能である。

[デフォルト値] *level* = 1
forget = on
telnet = off

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

3.8 リモートホストによる時計の設定

[入力形式] **rdate** *host* [syslog]

[パラメータ] ◦ *host*

- リモートホストの IP アドレス (xxx.xxx.xxx.xxx (xxx は 10 進数))
- ホストの名称

◦ *syslog*.....出力結果を SYSLOG へ出力することを表すキーワード

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

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

3.9 NTP による時計の設定

[入力形式] **ntpdate** *ntp_server* [syslog]

[パラメータ] ◦ *ntp_server*

- NTP サーバの IP アドレス (xxx.xxx.xxx.xxx (xxx は 10 進数))
- NTP サーバの名称

◦ *syslog*.....出力結果を SYSLOG へ出力することを表すキーワード

[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 サーバはできるだけ近くのを指定した方がよい。利用可能な NTP サーバについてはプロバイダに問い合わせること。
YAMAHA ルータ自身は NTP サーバになれない。
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。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

3.10 コンソールの言語とコードの設定

[入力形式] **console character** *code*
no console character [*code*]

[パラメータ] ◦ *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。

[デフォルト値] *sjis*

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

3.11 コンソールの表示文字数の設定

[入力形式]	console columns <i>col</i> no console columns [<i>col</i>]														
[パラメータ]	○ <i>col</i> 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。														
[デフォルト値]	80														
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

3.12 コンソールの表示行数の設定

[入力形式]	console lines <i>lines</i> no console lines [<i>lines</i>]														
[パラメータ]	○ <i>lines</i> <ul style="list-style-type: none"> • 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。														
[デフォルト値]	24														
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

3.13 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

[入力形式]	console info <i>info</i> no console info <i>info</i>														
[パラメータ]	○ <i>info</i> <ul style="list-style-type: none"> • 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。														
[デフォルト値]	off														
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

3.14 コンソールのプロンプト表示の設定

[入力形式]	console prompt <i>prompt</i> no console prompt [<i>prompt</i>]														
[パラメータ]	○ <i>prompt</i> 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。														
[デフォルト値]	空文字列														
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

3.15 SYSLOG を受けるホストの IP アドレスの設定

- [入力形式] **syslog host *host***
no syslog host [*host*]
- [パラメータ] ◦ *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。
- [デフォルト値] SYSLOG ホストは設定されない
- [適用モデル]
- | | | | | | | |
|---------|---------|--------|--------|--------|--------|--------|
| RTX2000 | RTX1000 | RT300i | RT140p | RT140f | RT140i | RT140e |
| RT105p | RT105i | RT105e | | | | |

3.16 SYSLOG ファシリティの設定

- [入力形式] **syslog facility *facility***
no syslog facility [*facility*]
- [パラメータ] ◦ *facility*
 • 0..23
 • user..... 1
 • local0..local7..... 16..27
- [説明] SYSLOG のファシリティを設定する。
- [デフォルト値] user
- [適用モデル]
- | | | | | | | |
|---------|---------|--------|--------|--------|--------|--------|
| RTX2000 | RTX1000 | RT300i | RT140p | RT140f | RT140i | RT140e |
| RT105p | RT105i | RT105e | | | | |

3.17 NOTICE タイプの SYSLOG を出力するか否かの設定

- [入力形式] **syslog notice *notice***
no syslog notice [*notice*]
- [パラメータ] ◦ *notice*
 • on..... 出力する
 • off..... 出力しない
- [説明] IP フィルタ、IPX フィルタ、ブリッジ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。
- [デフォルト値] off
- [適用モデル]
- | | | | | | | |
|---------|---------|--------|--------|--------|--------|--------|
| RTX2000 | RTX1000 | RT300i | RT140p | RT140f | RT140i | RT140e |
| RT105p | RT105i | RT105e | | | | |

3.18 INFO タイプの SYSLOG を出力するか否かの設定

- [入力形式] **syslog info *info***
no syslog info [*info*]
- [パラメータ] ◦ *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。
- [デフォルト値] on
- [適用モデル]
- | | | | | | | |
|---------|---------|--------|--------|--------|--------|--------|
| RTX2000 | RTX1000 | RT300i | RT140p | RT140f | RT140i | RT140e |
| RT105p | RT105i | RT105e | | | | |

3.19 DEBUG タイプの SYSLOG を出力するか否かの設定

[入力形式]	syslog debug <i>debug</i> no syslog debug [<i>debug</i>]														
[パラメータ]	○ <i>debug</i> <ul style="list-style-type: none"> • 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]	<i>debug</i> 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。														
[デフォルト値]	off														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

3.20 TFTP によりアクセスできるホストの IP アドレスの設定

[入力形式]	tftp host <i>host</i> no tftp host [<i>host</i>]														
[パラメータ]	○ <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。														
[デフォルト値]	none														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

3.21 SYSLOG パケットの始点ポート番号の設定

[入力形式]	syslog srcport <i>port</i> no syslog srcport [<i>port</i>]														
[パラメータ]	○ <i>port</i> ポート番号 (1..65535)														
[説明]	本機が送信する SYSLOG パケットの始点ポート番号を設定する。														
[デフォルト値]	514														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

3.22 マスタクロック用インタフェースの設定

[入力形式]	line masterclock interface no line masterclock														
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>interface</i> <ul style="list-style-type: none"> • インタフェース名 • auto自動選択 														
[説明]	<p>RT300iでは、装備されているすべての BRI/PRI インタフェースは 1 つのマスタクロックに同期している必要がある。マスタクロックは通常、BRI/PRI インタフェースに接続された WAN 回線から供給される。このコマンドでは、どのインタフェースからマスタクロックを得るかを指定することができる。</p> <p>auto を設定した場合は、実際に回線が接続されている BRI/PRI インタフェースの中からマスタクロックを供給するインタフェースを自動的に選択する。選択基準は、BRI よりも PRI を優先し、同じ回線種別の中ではより若番のポート番号を持つインタフェースを優先する。マスタとなるインタフェースの回線がダウンしてクロックを得られなくなった場合には、同じモジュール内のインタフェースを優先して、次のマスタクロック供給インタフェースを選択する。すべての回線がダウンしている場合には内部クロックを用いたフリーラン状態となる。</p> <p>インタフェースを指定している場合には、そのインタフェースからマスタクロックを得る。そのインタフェースに接続されている回線がダウンした場合には、常に <code>bri 1</code> をマスタとする。<code>bri 1</code> もダウンした場合には内部クロックを用いたフリーラン状態となる。</p>														
[ノート]	<p>すべての BRI/PRI はマスタクロックに同期するので、それらに接続されている回線もお互いに同期している必要がある。日本国内の通信事業者が提供する実回線は、すべて NTT を基準として同期しているはずなので、その点では問題はない。一部の BRI/PRI に、構内網など独自に構築した回線や、疑似交換機などを接続する場合には、マスタクロックと同期していない回線ではクロックシフトによるビットエラーが発生する可能性があることに注意しなくてはならない。</p>														
[デフォルト値]	auto														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 14.28%;">RTX2000</td> <td style="width: 14.28%;">RTX1000</td> <td style="width: 14.28%;">RT300i</td> <td style="width: 14.28%;">RT140p</td> <td style="width: 14.28%;">RT140f</td> <td style="width: 14.28%;">RT140i</td> <td style="width: 14.28%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

3.23 電源の設定

[入力形式]	system power module use sw no system power module use [sw]														
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>module</i>モジュール番号 (1,2) ◦ <i>sw</i> <ul style="list-style-type: none"> • onモジュールを装着している • offモジュールを装着していない 														
[説明]	<p>電源モジュールの装着状態を設定する。電源モジュールからの電源供給自体は、実際に装着すればこのコマンドに関係なく機能するが、このコマンドを設定することで電源モジュールの監視機能が正しく働くようになる。</p>														
[ノート]	<p>電源モジュールを装着していないにも関わらず、<i>sw</i> を <code>on</code> に設定すると、監視機能が働き電源モジュールの異常を報告する。</p>														
[デフォルト値]	<p>モジュール 1 = off モジュール 2 = on</p>														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 14.28%;">RTX2000</td> <td style="width: 14.28%;">RTX1000</td> <td style="width: 14.28%;">RT300i</td> <td style="width: 14.28%;">RT140p</td> <td style="width: 14.28%;">RT140f</td> <td style="width: 14.28%;">RT140i</td> <td style="width: 14.28%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

3.24 温度監視の閾値の設定

[入力形式]	system temperature threshold <i>t1 t2</i> no system temperature threshold <i>t1 t2</i>														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>t1</i> 警告を発する温度 (°C) ○ <i>t2</i> 警告を解除する温度 (°C) 														
[説明]	本体内部の温度を監視して、 <i>t1</i> 以上の温度になると SYSLOG や ALM ランプで警告を発する。一度、警告が発せられると、温度が <i>t2</i> を下回らない限り、ALM ランプは消えない。														
[デフォルト値]	<i>t1</i> = 80 <i>t2</i> = 75														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center;">RTX2000</td> <td style="text-align: center;">RTX1000</td> <td style="text-align: center;">RT300i</td> <td style="text-align: center;">RT140p</td> <td style="text-align: center;">RT140f</td> <td style="text-align: center;">RT140i</td> <td style="text-align: center;">RT140e</td> </tr> <tr> <td style="text-align: center;">RT105p</td> <td style="text-align: center;">RT105i</td> <td style="text-align: center;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

3.25 LAN インタフェースの動作タイプの設定

[入力形式] **lan type interface speed_type [port ...] [speed_type ...] [port-based-ks8995e group_type port [port ...] [ip-routing=routing] [group_type ...]] [auto-crossover=sw]**
lan type interface port-based-ks8995e group_type port [port ...] [ip-routing=routing] [group_type ...] [auto-crossover=sw]
lan type interface auto-crossover=sw
no lan type interface

- [パラメータ]
- *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*..... 10MHz 半二重
 - *10-fdx*..... 10MHz 全二重
 - *100-hdx*..... 100MHz 半二重
 - *100-fdx*..... 100MHz 全二重
 - 省略時は *auto*
 - *port* (スイッチングハブ内蔵機種のみ)
 - スwitchingハブのポート番号 (1 .. 4)
 - 省略時は全ポート
 - *group_type*..... ポートの属するネットワークあるいは無効化の指定
 - *primary* 指定ポートはプライマリアドレスネットワークに属する
 - *secondary*..... 指定ポートはセカンダリアドレスネットワークに属する
 - *disable* 指定ポートは使用しない
 - *routing*IP ルーティング接続
 - *on* 指定ポートをルーティング機能と接続する
 - *off*..... 指定ポートをルーティング機能と接続しない
 - 省略時は *on*
 - *sw* クロスストレート自動判別機能を使用するか否か (スイッチングハブインタフェースのみ)
 - *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。
 キーワード **port-based-ks8995e** を指定するとネットワークに属するポートを限定し、ネットワーク間での IP 通信を制限することができる。

[ノート] 本コマンドの実行後、LAN インタフェースのリセットが自動で行われ、その終了後に設定が有効となる。
port-based-ks8995e と **auto-crossover** キーワードが使用できるのは RT105p と RT105eのみである。
port-based-ks8995e を指定した場合、**primary** 指定しかなされておらずかつ指定されていないポートがある場合には、残りのポートはセカンダリアドレスネットワークに属する。**primary** 指定と **secondary** 指定がなされ、かつどちらにも指定されていないポートがある場合には、そのポートは **disable** 指定されたものとみなされ、他との通信は一切遮断される。
ip-routing=off を指定されたネットワークのポートに接続されたホストは、それらのポートに接続されたホスト以外との通信は一切遮断される。YAMAHA ルータ自身との通信も遮断される。
 YAMAHA ルータ自身からのブロードキャストパケットは、**ip-routing=off** の指定がされていない限り、どちらのネットワークにも送出される。動的経路制御の使用は制限される。

[デフォルト値] **speed_type = auto**
port-based-ks8995e 指定なし
auto-crossover = on

[設定例]

例 1)

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

 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。

例 2)

```
# lan type lan1 100-fdx 1 port-based-ks8995e primary 1 2
```

 ポート 1 は 100BASE-TX 全二重、その他のポートはオートネゴシエーションで接続する。ポート 1,2 は LAN1 プライマリアドレスネットワークに、その他のポートは LAN1 セカンダリアドレスネットワークに属するものとされる。両ネットワーク間でブロードキャストドメインが分離され、IP 通信が制限される。

例 3)

```
# lan type lan1 port-based-ks8995e primary 1 2 secondary 3
```

 全ポートはオートネゴシエーションで接続する。ポート 1,2 は LAN1 プライマリアドレスネットワーク、ポート 3 は LAN1 セカンダリアドレスネットワークに属するものとされる。残りのポートは **disable** 指定されたものとみなされ、他のポートとの通信はできない。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

4. ISDN 関連の設定

4.1 自分側の設定

4.1.1 BRI 回線の種類の指定

[入力形式]	line type interface line [channels] no line type interface line [channels]														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>interface</i> BRI インタフェース名 ○ <i>line</i> <ul style="list-style-type: none"> • <i>isdn, isdn-ntt</i>..... ISDN 回線交換 • <i>164</i>..... デジタル専用線、64kbit/s • <i>1128</i>..... デジタル専用線、128kbit/s ○ <i>channels</i> <i>line</i> パラメータが <i>isdn</i>、<i>isdn-ntt</i> の場合のみ指定可 <ul style="list-style-type: none"> • <i>1b</i>..... B チャンネルは 1 チャンネルだけ使用 • <i>2b</i>..... 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 <i>channels</i> パラメータを <i>1b</i> に設定する。														
[デフォルト値]	<i>line</i> = <i>isdn</i> <i>channels</i> = <i>2b</i>														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

4.1.2 自分の ISDN 番号の設定

[入力形式]	isdn local address interface isdn_num[/sub_address] isdn local address interface /sub_address no isdn local address interface														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>interface</i> BRI/PRI インタフェース名 ○ <i>isdn_num</i> ISDN 番号 ○ <i>sub_address</i> 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。														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

4.1.3 課金額による発信制限の設定

- [入力形式] **account threshold** [interface] yen
account threshold pp yen
no account threshold interface [yen]
no account threshold [yen]
no account threshold pp [yen]
- [パラメータ] ◦ interfaceBRI/PRI 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う。
 課金が網から通知されるのは通信切断時なので、長時間の接続の途中切断することはできず、この場合は制限はできない。この場合に対処するには、**isdn forced disconnect time** コマンドで通信中でも時間を監視して強制的に回線を切るような設定にしておく方法がある。また、課金合計は **clear account** コマンドで 0 にリセットでき、**schedule at** コマンドで定期的に **clear account** を実行するようしておく、毎月一定額以内に課金を抑えるといったことが自動で可能になる。
- [ノート] 電源 OFF や再起動により、それまでの課金情報がクリアされることに注意。課金額は通信の切断時に NTT から ISDN で通知される料金情報に基づくため、割引サービスなどを利用している場合には、最終的に NTT から請求される料金とは異なる場合がある。また、NTT 以外の通信事業者を利用して通信した場合には料金情報は通知されない。
- [デフォルト値] off

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

4.1.4 PIAFS の発信方式の設定

- [入力形式] **isdn piafs call speed** [64kmode]
no isdn piafs call [speed [64kmode]]
- [パラメータ] ◦ 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
 • guaranteePIAFS 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。
- [デフォルト値] off

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

4.1.5 PIAFS の着信を許可するか否かの設定

[入力形式]	isdn piafs arrive arrive no isdn piafs arrive [arrive]														
[パラメータ]	○ arrive <ul style="list-style-type: none"> • 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。														
[デフォルト値]	on														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

4.1.6 PIAFS 接続時の起動側の指定

[入力形式]	isdn piafs control switch														
[パラメータ]	○ switch <ul style="list-style-type: none"> • 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。														
	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr> <th style="text-align: left;">switch パラメータの設定</th> <th>call</th> <th>both</th> <th>arrive</th> </tr> </thead> <tbody> <tr> <td>発信時</td> <td>起動時</td> <td>起動側</td> <td>被起動側</td> </tr> <tr> <td>着信時</td> <td>被起動側</td> <td>起動側</td> <td>起動側</td> </tr> </tbody> </table>	switch パラメータの設定	call	both	arrive	発信時	起動時	起動側	被起動側	着信時	被起動側	起動側	起動側		
switch パラメータの設定	call	both	arrive												
発信時	起動時	起動側	被起動側												
着信時	被起動側	起動側	起動側												
[デフォルト値]	call														
[設定例]	<pre># pp select 2 # isdn piafs control call # pp enable 2</pre>														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

4.1.7 専用線がダウンした時にバックアップする相手先情報番号の設定

[入力形式]	leased backup peer_num no leased backup [peer_num]														
[パラメータ]	○ peer_num <ul style="list-style-type: none"> • バックアップする相手先情報番号 • none ISDN でバックアップをしない 														
[説明]	BRI インタフェースを複数持つ機種で有効なコマンド。 選択した相手先に対する専用線がダウンした場合に ISDN でバックアップする、バックアップ用の相手先情報番号を設定する。														
[デフォルト値]	none														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

4.1.8 常時接続の設定

[入力形式] **pp always-on sw** [*time*]

- [パラメータ]
- *sw*
 - 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時間間隔 (60-21474836 秒)

[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。*sw* 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。

[デフォルト値] off

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

4.1.9 終端抵抗の設定

[入力形式] **isdn terminator interface terminator**
no isdn terminator interface [*terminator*]

- [パラメータ]
- *interface*BRI インタフェース名
 - *terminator*
 - on..... 終端抵抗を ON にする
 - off..... 終端抵抗を OFF にする

[説明] 指定した BRI インタフェースの終端抵抗を ON または OFF にする。

[ノート] DSU に直結する場合には必ず on にする。
 バス配線されている場合、バスの終端でなければ off にする。

[デフォルト値] off

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

4.1.10 PP で使用するインタフェースの設定

[入力形式] **pp bind interface** [*interface*]
no pp bind [*interface*]

- [パラメータ] ◦ *interface*BRI/PRI 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。

[デフォルト値] どのインタフェースともバインドされていない

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

4.2 相手側の設定

4.2.1 相手 ISDN 番号の設定

[入力形式] **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]

[パラメータ] ○ *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。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

4.2.2 相手への発信順序の設定

[入力形式] **isdn remote call order order**
no isdn remote call order [order]

[パラメータ] ○ *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、どことも接続されていない状態や相手先とすべてのチャンネルで切断された後では、最初に設定された ISDN 番号から発信に使用される。

[ノート] MP を使用する場合は、*round* にした方が効率がよい。

[デフォルト値] *serial*

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

4.2.3 自動接続の設定

[入力形式] **isdn auto connect auto**
no isdn auto connect [auto]

[パラメータ] ○ *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。

[デフォルト値] *on*

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

4.2.4 自動切断の設定

- [入力形式] **isdn auto disconnect auto**
 no isdn auto disconnect [auto]
- [パラメータ] ◦ *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。
- [デフォルト値] on

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

4.2.5 着信許可の設定

- [入力形式] **isdn arrive permit arrive**
 no isdn arrive permit [arrive]
- [パラメータ] ◦ *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 を設定した場合は通信できない。
- [デフォルト値] on

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

4.2.6 発信許可の設定

- [入力形式] **isdn call permit permit**
 no isdn call permit [permit]
- [パラメータ] ◦ *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。
- [デフォルト値] on

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

4.2.7 再発信抑制タイマの設定

[入力形式]	isdn call block time <i>time</i> no isdn call block time [<i>time</i>]														
[パラメータ]	○ <i>time</i> 秒数 (0..15)														
[説明]	<p>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。</p> <p>isdn call prohibit time コマンドによるタイマはエラーで切断された場合だけに適用されるが、このコマンドによるタイマは正常切断でも適用される点異なる。</p>														
[ノート]	<p>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。</p> <p>isdn forced disconnect time コマンドと併用するとよい。</p>														
[デフォルト値]	0														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT140p</td> <td style="padding: 2px;">RT140f</td> <td style="padding: 2px;">RT140i</td> <td style="padding: 2px;">RT140e</td> </tr> <tr> <td style="padding: 2px;">RT105p</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

4.2.8 エラー切断後の再発信禁止タイマの設定

[入力形式]	isdn call prohibit time <i>time</i> no isdn call prohibit time [<i>time</i>]														
[パラメータ]	○ <i>time</i> 秒数 (60..21474836)														
[説明]	<p>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。</p> <p>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。</p>														
[デフォルト値]	60														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT140p</td> <td style="padding: 2px;">RT140f</td> <td style="padding: 2px;">RT140i</td> <td style="padding: 2px;">RT140e</td> </tr> <tr> <td style="padding: 2px;">RT105p</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

4.2.9 相手にコールバック要求を行うか否かの設定

[入力形式]	isdn callback request <i>callback_request</i> no isdn callback request [<i>callback_request</i>]														
[パラメータ]	○ <i>callback_request</i> <ul style="list-style-type: none"> • 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うか否かを設定する。														
[デフォルト値]	off														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT140p</td> <td style="padding: 2px;">RT140f</td> <td style="padding: 2px;">RT140i</td> <td style="padding: 2px;">RT140e</td> </tr> <tr> <td style="padding: 2px;">RT105p</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

4.2.10 コールバック要求タイプの設定

[入力形式]	isdn callback request type <i>type</i> no isdn callback request type [<i>type</i>]														
[パラメータ]	○ <i>type</i> <ul style="list-style-type: none"> • 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。														
[デフォルト値]	yamaha														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT140p</td> <td style="padding: 2px;">RT140f</td> <td style="padding: 2px;">RT140i</td> <td style="padding: 2px;">RT140e</td> </tr> <tr> <td style="padding: 2px;">RT105p</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

4.2.11 相手からのコールバック要求に応じるか否かの設定

[入力形式] **isdn callback permit** *callback_permit*
no isdn callback permit [*callback_permit*]

[パラメータ] ◦ *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。

[デフォルト値] off

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

4.2.12 コールバック受け入れタイプの設定

[入力形式] **isdn callback permit type** *type1* [*type2*]
no isdn callback permit type [*type1* [*type2*]]

[パラメータ] ◦ *type1, type2*
 • yamahaヤマハ方式
 • mschbcipMS 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。

[デフォルト値] *type1* = yamaha
type2 = mschbcip

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

4.2.13 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

[入力形式] **isdn callback mschbcip user-specify** *specify*
no isdn callback mschbcip user-specify [*specify*]

[パラメータ] ◦ *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。

[デフォルト値] off

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

4.2.14 コールバックタイムの設定

[入力形式] **isdn callback response time** *type time*

[パラメータ] ◦ *type*
 • 1b.....1B でコールバックする
 ◦ *time*秒数 (0..15)

[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。

[デフォルト値] *time* = 0

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

4.2.15 コールバック待機タイマの設定

[入力形式]	isdn callback wait time <i>time</i> no isdn callback wait time [<i>time</i>]														
[パラメータ]	○ <i>time</i> 秒数 (1..60)														
[説明]	選択されている相手にコールバックを要求し、それが受け入れられていったん回線が切断されてから、このタイマがタイムアウトするまで相手からのコールバックによる着信を受け取れなかった場合には接続失敗とする。秒数は 0.1 秒単位で設定できる。														
[デフォルト値]	60														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT140p</td> <td style="padding: 2px;">RT140f</td> <td style="padding: 2px;">RT140i</td> <td style="padding: 2px;">RT140e</td> </tr> <tr> <td style="padding: 2px;">RT105p</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

4.2.16 ISDN 回線を切断するタイマ方式の指定

[入力形式]	isdn disconnect policy <i>type</i> no isdn disconnect policy [<i>type</i>]														
[パラメータ]	○ <i>type</i> <ul style="list-style-type: none"> • 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 つのタイマコマンドでトラフィックを監視し、一定時間パケットが流れなくなった時点で回線を切断する。 課金単位時間方式では、課金単位時間と監視時間を isdn disconnect interval time コマンドで設定し、監視時間中にパケットが流れなければ課金単位時間の倍数の時間で回線を切断する。通信料金を減らす効果が期待できる。														
[デフォルト値]	1														
[設定例]	# isdn disconnect policy 2 # isdn disconnect interval time 240 6 2														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT140p</td> <td style="padding: 2px;">RT140f</td> <td style="padding: 2px;">RT140i</td> <td style="padding: 2px;">RT140e</td> </tr> <tr> <td style="padding: 2px;">RT105p</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

4.2.17 切断タイマの設定 (ノーマル)

[入力形式]	isdn disconnect time <i>time</i> no isdn disconnect time [<i>time</i>]														
[パラメータ]	○ <i>time</i> <ul style="list-style-type: none"> • 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。														
[デフォルト値]	60														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT140p</td> <td style="padding: 2px;">RT140f</td> <td style="padding: 2px;">RT140i</td> <td style="padding: 2px;">RT140e</td> </tr> <tr> <td style="padding: 2px;">RT105p</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

4.2.18 入力切断タイマの設定 (ノーマル)

[入力形式] **isdn disconnect input time time**
no isdn disconnect input time [time]

[パラメータ] ◦ *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。
 4.2.17 切断タイマの設定 (ノーマル) のノート参照。

[デフォルト値] 120

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

4.2.19 出力切断タイマの設定 (ノーマル)

[入力形式] **isdn disconnect output time time**
no isdn disconnect output time [time]

[パラメータ] ◦ *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、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。
 4.2.17 切断タイマの設定 (ノーマル) のノート参照。

[デフォルト値] 120

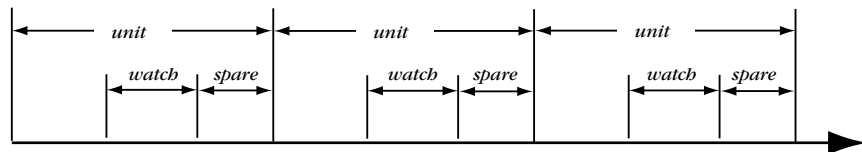
[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

4.2.20 課金単位時間方式での課金単位時間と監視時間の設定

[入力形式] **isdn disconnect interval time** *unit watch spare*
no isdn disconnect interval time [*unit watch spare*]

- [パラメータ]
- *unit* 課金単位時間
 - 秒数 (1..21474836)
 - off
 - *watch* 監視時間
 - 秒数 (1..21474836)
 - off
 - *spare* 切断余裕時間
 - 秒数 (1..21474836)
 - 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。

[デフォルト値] *unit* = 180
watch = 6
spare = 2

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

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

4.2.21 切断タイマの設定 (ファスト)

[入力形式] **isdn fast disconnect time** *time*
no isdn fast disconnect time [*time*]

- [パラメータ]
- *time*
 - 秒数 (1..21474836)
 - 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。

[デフォルト値] 20

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

4.2.22 切断タイマの設定 (強制)

[入力形式] **isdn forced disconnect time** *time*
no isdn forced disconnect time [*time*]

[パラメータ] ◦ *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。

[デフォルト値] off

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

5. IP の設定

5.1 インタフェース共通の設定

5.1.1 IP パケットを扱うか否かの設定

[入力形式] **ip routing** *routing*
no ip routing [*routing*]

[パラメータ] ◦ *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。

[デフォルト値] on

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

5.1.2 IP アドレスの設定

[入力形式] **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*]

[パラメータ] ◦ *interface* LAN インタフェース名
 ◦ *ip_adddes* IP アドレス xxx.xxx.xxx.xxx (xxx は 10 進数)
 ◦ dhcp DHCP クライアントとして IP アドレスを取得する
 ◦ *mask*
 • xxx.xxx.xxx.xxx (xxx は 10 進数)
 • 0x に続く 16 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

[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。

[デフォルト値] 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

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

5.1.3 セカンダリ IP アドレスの設定

[入力形式] **ip interface secondary address ip_address[/mask]**
ip interface secondary address dhcp
no ip interface secondary address [ip_address/mask]

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

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

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

5.1.4 IP の静的経路情報の設定

[入力形式]	ip route network gateway gateway [parameter] [gateway gateway [parameter]] no ip route network [gateway..]														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>network</i> <ul style="list-style-type: none"> • <i>default</i> 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) ○ <i>gateway</i> <ul style="list-style-type: none"> • IP アドレス..... xxx.xxx.xxx.xxx (xxx は 10 進数) • pp <i>pp_num</i> [<i>dldci=dldci</i>] PP インタフェースへの経路 "dldci=dldci" が指定された場合は、フレームリレーの DLCI への経路 <ul style="list-style-type: none"> ■ <i>pp_num</i> <ul style="list-style-type: none"> □ 相手先情報番号 □ <i>anonymous</i> • pp <i>anonymous name=name</i> <ul style="list-style-type: none"> ■ <i>name</i> PAP/CHAP による名前 • <i>dhcp interface</i> <ul style="list-style-type: none"> ■ <i>interface</i> DHCP にて与えられるデフォルトゲートウェイを使う場合の、DHCP クライアントとして動作する LAN インタフェース名 (送り先が Default の時のみ有効) • <i>tunnel tunnel_num</i> Tunnel インタフェースへの経路 ○ <i>parameter</i> 以下のパラメータを空白で区切り複数設定可能 <ul style="list-style-type: none"> • <i>filter number [number..]</i> ... フィルタ型経路の指定 <ul style="list-style-type: none"> ■ <i>number</i>..... フィルタの番号 (1..21474836) (空白で区切り複数設定可能) • <i>metric metric</i>..... メトリックの指定 <ul style="list-style-type: none"> ■ <i>metric</i> メトリック値 (1..15) (省略時は 1) • <i>hide</i> 出力インタフェースが PP インタフェースまたは 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 • <i>weight weight</i> 異なる経路間の比率を表す値 <ul style="list-style-type: none"> ■ <i>weight</i> 経路への重み (1..2147483647、省略時は 1) 														
[説明]	<p>IP の静的経路を設定する。</p> <p><i>gateway</i> 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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p><i>filter</i> 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。<i>weight</i> 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 <i>weight</i> 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。</p> <p>いずれの場合でも、<i>hide</i> 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。</p>														
[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]	<ul style="list-style-type: none"> ○ デフォルトゲートウェイを 192.168.0.1 とする # ip route default gateway 192.168.0.1 ○ PP1 で接続している相手のネットワークは 192.168.1.0/24 である # ip route 192.168.1.0/24 gateway pp 1 ○ マルチホーミングによる負荷分散を行う。デフォルトゲートウェイとして 2 経路持ち、PP1 には専用線 128k で、PP2 には専用線 64k で接続しており、かつ各専用線ダウン時の経路を無効としてパケットロスを防ぐ。 ※ NAT 機能と専用線キーブアライブの併用が必要となる。 # ip route default gateway pp 1 weight 2 hide gateway pp 2 weight 1 hide 														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

5.1.5 IP パケットのフィルタの設定

[入力形式] **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*]

- [パラメータ]
- *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 は
 - 10 進数
 - * (ネットマスクの対応するビットが 8 ビットとも 0 と同じ)
 - 間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。
 - * (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 0xffffffff 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 10 進数)
 - 0x に続く 16 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 10 進数 (0..255)
 - プロトコルを表すニーモニック

ニーモニック	10 進数	説明
icmp	1	icmp パケット
icmp-error	-	特定の TYPE コードの icmp パケット
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
	-	ACK フラグの立っている tcp パケット
established	-	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 10 進数
- ポート番号を表す二進モニック (一部)

二進モニック	ポート番号	二進モニック	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、そのために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

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

5.1.6 フィルタセットの定義

[入力形式] **ip filter set name direction filter_list [filter_list ...]**
no ip filter set name [direction ...]

[パラメータ] ○ *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* 100 個以内の、空白で区切られたフィルタ番号の並び

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

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

5.1.7 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

[入力形式] **ip filter source-route filter_out**
no ip filter source-route [filter_out]

[パラメータ] ○ *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。

[デフォルト値] on

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

5.1.8 Directed-Broadcast パケットをフィルタアウトするか否かの設定

[入力形式] **ip filter directed-broadcast** *filter_out*
no ip filter directed-broadcast [*filter_out*]

[パラメータ] ◦ *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] 終点 IP アドレスが Directed-Broadcast アドレス宛になっている IP パケットをルータが接続されているネットワークにブロードキャストするか否かを設定する。

[ノート] いわゆる smurf 攻撃を防止するためには on にしておく。

[デフォルト値] on

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

5.1.9 動的フィルタの定義

[入力形式] **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...*]

[パラメータ] ◦ *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。

[デフォルト値] *syslog=on*
timeout=60

[設定例] # ip filter 10 * * udp * snmp
ip filter dynamic 1 * * filter 10

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

5.1.10 動的フィルタのタイムアウトの設定

[入力形式]	ip filter dynamic timer [<i>option=timeout</i> [<i>option...</i>]] no ip filter dynamic timer														
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>option</i> オプション名 <ul style="list-style-type: none"> • <i>tcp-syn-timeout</i> 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 • <i>tcp-fin-timeout</i> 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 • <i>tcp-idle-time</i> 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 • <i>udp-idle-time</i> 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 • <i>dns-timeout</i> 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 ◦ <i>timeout</i> 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。														
[デフォルト値]	<pre>tcp-syn-timeout=30 tcp-fin-timeout=5 tcp-idle-time=3600 udp-idle-time=30 dns-timeout=5</pre>														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

5.1.11 侵入検知機能の動作の設定

[入力形式]	ip interface intrusion detection <i>direction switch</i> [<i>option</i>] ip pp intrusion detection <i>direction switch</i> [<i>option</i>] ip tunnel intrusion detection <i>direction switch</i> [<i>option</i>] no ip interface intrusion detection no ip pp intrusion detection no ip tunnel intrusion detection														
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>interface</i> LAN インタフェース名 ◦ <i>direction</i> 観察するパケットの方向 <ul style="list-style-type: none"> • <i>in</i> インタフェース側から内側へ • <i>out</i> インタフェース側から外側へ ◦ <i>switch</i> 動作 <ul style="list-style-type: none"> • <i>on</i> 実行する • <i>off</i> 実行しない ◦ <i>option</i> オプション <ul style="list-style-type: none"> • <i>reject=rjt</i> <ul style="list-style-type: none"> ▪ <i>on</i> 不正なパケットを破棄する ▪ <i>off</i> 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。														
[デフォルト値]	<pre>switch = off reject = off</pre>														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

5.1.12 フィルタリングによるセキュリティの設定

[入力形式] **ip interface secure filter direction** [*filter_list...*] [*dynamic filter_list...*]
ip pp secure filter direction [*filter_list...*] [*dynamic filter_list...*]
ip tunnel secure filter direction [*filter_list...*] [*dynamic filter_list...*]
ip interface secure filter name *set_name*
ip pp secure filter name *set_name*
ip tunnel secure filter name *set_name*
no ip interface secure filter direction [*filter_list*]
no ip pp secure filter direction [*filter_list*]
no ip tunnel secure filter direction [*filter_list*]
no ip interface secure filter [name [*set_name*]]
no ip pp secure filter [name [*set_name*]]
no ip tunnel secure filter [name [*set_name*]]

[パラメータ] ○ *interface*LAN インタフェース名
 ○ *direction*
 • *in*受信したパケットのフィルタリング
 • *out*送信するパケットのフィルタリング
 ○ *filter_list* 100 個以内の、空白で区切られたフィルタ番号の並び
 ○ *set_name* フィルタセットの名前を表す文字列
 ○ *dynamic*キーワード後に動的フィルタの番号を記述する

[説明] **ip filter** コマンドによるパケットのフィルタを組み合わせ、インタフェースで送受信するパケットの種類を制限する。
 方向を指定する書式では、それぞれの方向に対して適用するフィルタ列をフィルタ番号で指定する。指定された番号のフィルタが順番に適用され、パケットにマッチするフィルタが見つければそのフィルタにより通過 / 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。
 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 での検査は行われない。そのため、フィルタ 2 は何も意味を持たない。
 フィルタリストを操作した結果、どのフィルタにも一致しないパケットは破棄される。

PP Anonymous で認証に RADIUS を利用する場合で、RADIUS サーバから送られた Access-Response にアトリビュート 'Filter-Id' がついていた場合には、その値に指定されたフィルタセットを適用し、**ip pp secure filter** コマンドの設定は無視される。
 ただしアトリビュート "Filter-Id" が存在しない場合には、**ip pp secure filter** コマンドの設定がフィルタとして利用される。

[デフォルト値] フィルタは設定されていない

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

5.1.13 IP パケットの TOS フィールドの書き換えの設定

[入力形式]	ip tos supersede <i>id tos</i> [<i>precedence=precedence</i>] <i>filter_num</i> [<i>filter_num_list</i>] no ip tos supersede <i>id</i> [<i>tos</i>]														
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>id</i> 識別番号 (1..65535) ◦ <i>tos</i> 書き換える TOS 値 (0..15) 以下のニーモニックが利用できる <table border="1" style="margin-left: 20px; border-collapse: collapse;"> <tr><td style="padding: 2px;">normal</td><td style="padding: 2px;">0</td></tr> <tr><td style="padding: 2px;">min-monetary-cost</td><td style="padding: 2px;">1</td></tr> <tr><td style="padding: 2px;">max-reliability</td><td style="padding: 2px;">2</td></tr> <tr><td style="padding: 2px;">max-throughput</td><td style="padding: 2px;">4</td></tr> <tr><td style="padding: 2px;">min-delay</td><td style="padding: 2px;">8</td></tr> </table> <ul style="list-style-type: none"> ◦ <i>precedence</i> <ul style="list-style-type: none"> • PRECEDENCE 値 (0..7) • <i>precedence</i> を省略した場合、PRECEDENCE 値は変更しない ◦ <i>filter_num</i> , <i>filter_num_list</i> 静的フィルタの番号 (1..100) 	normal	0	min-monetary-cost	1	max-reliability	2	max-throughput	4	min-delay	8				
normal	0														
min-monetary-cost	1														
max-reliability	2														
max-throughput	4														
min-delay	8														
[説明]	<p>IP パケットを中継する場合に TOS フィールドを指定した値に書き換える。識別番号順にリストをチェックし、<i>filter_num</i> リストのフィルタを順次適用していく。そして、最初にマッチした IP フィルタが <i>pass</i>、<i>pass-log</i>、<i>pass-nolog</i>、<i>restrict</i>、<i>restrict-log</i>、<i>restrict-nolog</i> のいずれかであれば TOS フィールドが書き換えられる。</p> <p><i>reject</i>、<i>reject-log</i> または <i>reject-nolog</i> である場合は書き換えずに処理を終わる。</p>														
[適用モデル]	<table border="1" style="border-collapse: collapse; text-align: center;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT140p</td> <td style="padding: 2px;">RT140f</td> <td style="padding: 2px;">RT140i</td> <td style="padding: 2px;">RT140e</td> </tr> <tr> <td style="padding: 2px;">RT105p</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

5.1.14 インタフェースの MTU の設定

[入力形式]	ip interface mtu <i>mtu</i> ip pp mtu <i>mtu</i> no ip interface mtu [<i>mtu</i>] no ip pp mtu [<i>mtu</i>]														
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>interface</i> LAN インタフェース名 ◦ <i>mtu</i> 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、それらではデフォルトのまま 1500 の MTU となる。														
[デフォルト値]	1500														
[適用モデル]	<table border="1" style="border-collapse: collapse; text-align: center;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT140p</td> <td style="padding: 2px;">RT140f</td> <td style="padding: 2px;">RT140i</td> <td style="padding: 2px;">RT140e</td> </tr> <tr> <td style="padding: 2px;">RT105p</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

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

[入力形式]	ip simple-service <i>service</i> no ip simple-service [<i>service</i>]														
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>service</i> <ul style="list-style-type: none"> • <i>on</i> TCP/UDP の各種サービスを動作させる • <i>off</i> サービスを停止させる 														
[説明]	TCP/UDP の <i>echo</i> (7)、 <i>discard</i> (9)、 <i>time</i> (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。														
[デフォルト値]	on														
[適用モデル]	<table border="1" style="border-collapse: collapse; text-align: center;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT140p</td> <td style="padding: 2px;">RT140f</td> <td style="padding: 2px;">RT140i</td> <td style="padding: 2px;">RT140e</td> </tr> <tr> <td style="padding: 2px;">RT105p</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

5.2 代理 ARP の設定

- [入力形式] **ip interface proxyarp proxyarp**
no ip interface proxyarp [proxyarp]
- [パラメータ] ◦ *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。
- [デフォルト値] off

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

5.3 PP 側の設定

5.3.1 PP 側 IP アドレスの設定

- [入力形式] **ip pp remote address ip_address**
ip pp remote address dhcpc [interface]
no ip pp remote address [ip_address]
- [パラメータ] ◦ *ip_address*
 • IP アドレス xxx.xxx.xxx.xxx (xxx は 10 進数)
 • *dhcp*自分自身の DHCP サーバ機能より IP アドレスを割り当てる
 ◦ *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] 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 サーバとして動作している必要がある。自分で管理している DHCP スコープの中から、IP アドレスを割り当てる。
 装着されている BRI/PPRI インタフェースで利用できる ISDN Bch の数まで設定できる。
 PP として *anonymous* が選択された場合のみ有効である。
dhcpc を設定した場合は、*interface* で指定した LAN インタフェースが DHCP クライアントとして IP アドレスを取得し、そのアドレスを PP 側に割り当てる。取得できなかった場合は、0.0.0.0 を割り当てる。
- [ノート] 実際に設定される IP アドレスは **ppp ipcp ipaddress** コマンドと相手の設定により決まる。自分側で設定した IP アドレスを xxx.xxx.xxx.xxx、相手先が要求してくる IP アドレスを yyy.yyy.yyy.yyy とすると実際に設定される IP アドレスは次のようになる。
- [デフォルト値] 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 の PP 側の IP アドレスは "yyy.yyy.yyy.yyy" になることを意味する。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

5.3.2 リモート IP アドレスプールの設定

[入力形式]	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 dhcp [interface] no ip pp remote address pool														
[パラメータ]	<ul style="list-style-type: none"> ○ 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]	<p>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。</p> <p>dhcp を設定した場合は、自分自身が DHCP サーバ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。</p> <p>dhcpc を設定した場合は、interface で指定した LAN インタフェースが DHCP クライアントとして IP アドレスを取得し、そのアドレスを割り当てる。取得できなかった場合は、0.0.0.0 を割り当てる。</p> <p>RT300i では装着されている BRI/PRI インタフェースで利用できる ISDN Bch の数まで設定および DHCP クライアントで取得できる。RT140p では 8 個まで、RT140f、RT140i、RT140e では 4 個まで、それ以外は 2 個までとなる。PP として anonymous が選択された場合のみ有効である。</p>														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%;"> <tr> <td style="text-align: center;">RTX2000</td> <td style="text-align: center;">RTX1000</td> <td style="text-align: center;">RT300i</td> <td style="text-align: center;">RT140p</td> <td style="text-align: center;">RT140f</td> <td style="text-align: center;">RT140i</td> <td style="text-align: center;">RT140e</td> </tr> <tr> <td style="text-align: center;">RT105p</td> <td style="text-align: center;">RT105i</td> <td style="text-align: center;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

5.4 RIP の設定

5.4.1 RIP を使用するか否かの設定

[入力形式]	rip use rip_use no rip use rip_use														
[パラメータ]	<ul style="list-style-type: none"> ○ rip_use <ul style="list-style-type: none"> ● on RIP を使用する ● off RIP を使用しない 														
[説明]	<p>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。</p>														
[デフォルト値]	off														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%;"> <tr> <td style="text-align: center;">RTX2000</td> <td style="text-align: center;">RTX1000</td> <td style="text-align: center;">RT300i</td> <td style="text-align: center;">RT140p</td> <td style="text-align: center;">RT140f</td> <td style="text-align: center;">RT140i</td> <td style="text-align: center;">RT140e</td> </tr> <tr> <td style="text-align: center;">RT105p</td> <td style="text-align: center;">RT105i</td> <td style="text-align: center;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

5.4.2 RIP による経路の優先度の設定

[入力形式]	rip preference rip_preference no rip preference rip_preference														
[パラメータ]	<ul style="list-style-type: none"> ○ rip_preference 1 以上の数値 														
[説明]	<p>RIP により得られた経路の優先度を設定する。経路の優先度は 1 以上の数値で表され、数字が大きい程優先度が高い。スタティックと RIP など複数のプロトコルで得られた経路が食い違う場合には、優先度が高い方が採用される。優先度が同じ場合には時間的に先に採用された経路が有効となる。</p>														
[ノート]	スタティック経路の優先度は 10000 で固定である。														
[デフォルト値]	1000														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%;"> <tr> <td style="text-align: center;">RTX2000</td> <td style="text-align: center;">RTX1000</td> <td style="text-align: center;">RT300i</td> <td style="text-align: center;">RT140p</td> <td style="text-align: center;">RT140f</td> <td style="text-align: center;">RT140i</td> <td style="text-align: center;">RT140e</td> </tr> <tr> <td style="text-align: center;">RT105p</td> <td style="text-align: center;">RT105i</td> <td style="text-align: center;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

5.4.3 RIP パケットの送信に関する設定

[入力形式] **ip interface rip send rip_send** [version version [broadcast]]
ip pp rip send rip_send [version version [broadcast]]
ip tunnel rip send rip_send [version version [broadcast]]
no ip interface rip send [rip_send...]
no ip pp rip send [rip_send...]
no ip tunnel rip send [rip_send...]

[パラメータ] ○ interfaceLAN 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 broadcast address

[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。

[デフォルト値] on version 1

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

5.4.4 RIP パケットの受信に関する設定

[入力形式] **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...]

[パラメータ] ○ interfaceLAN インタフェース
○ 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、RIP 1/2 ともに受信する。

[デフォルト値] rip_receive = on
version = 1 2

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

5.4.5 RIP に関して信用できるゲートウェイの設定

[入力形式]	ip interface rip trust gateway [except] <i>gateway_list</i> ip pp rip trust gateway [except] <i>gateway_list</i> ip tunnel rip trust gateway [except] <i>gateway_list</i> no ip interface rip trust gateway [[except] <i>gateway_list</i>] no ip pp rip trust gateway [[except] <i>gateway_list</i>] no ip tunnel rip trust gateway [[except] <i>gateway_list</i>]														
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>interface</i> LAN インタフェース名 ◦ <i>gateway_list</i> 10 個以内の IP アドレスの並び 														
[説明]	RIP に関して信用できる、あるいは信用できないゲートウェイを設定する。 except キーワードを指定していない場合には、列挙したゲートウェイを信用できるゲートウェイとし、それらからの RIP だけを受信する。 except キーワードを指定した場合は、列挙したゲートウェイを信用できないゲートウェイとし、それらを除いた他のゲートウェイからの RIP だけを受信する。														
[デフォルト値]	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														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

5.4.6 RIP のフィルタリングの設定

[入力形式]	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														
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>interface</i> LAN インタフェース名 ◦ <i>direction</i> <ul style="list-style-type: none"> • <i>in</i> 受信した RIP のフィルタリング • <i>out</i> 送信する RIP のフィルタリング ◦ <i>filter_list</i> 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 <i>pass</i> であればそれを処理し、 <i>reject</i> であればその経路情報だけを破棄する。														
[デフォルト値]	フィルタは設定されていない														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

5.4.7 RIP で加算するホップ数の設定

[入力形式]	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														
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>interface</i> LAN インタフェース名 ◦ <i>direction</i> <ul style="list-style-type: none"> • <i>in</i> 受信した RIP に加算する • <i>out</i> 送信する RIP に加算する ◦ <i>hop</i> 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。														
[デフォルト値]	0														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

5.4.8 RIP2 での認証の設定

- [入力形式] **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]
- [パラメータ] ◦ interfaceLAN 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う。
- [デフォルト値] none

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

5.4.9 RIP2 での認証キーの設定

- [入力形式] **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 text text_key
ip pp rip auth text text_key
ip tunnel rip auth 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 text
no ip pp rip auth text
no ip tunnel rip auth text
- [パラメータ] ◦ interfaceLAN インタフェース名
 ◦ hex_key 16 進数の列で表現された認証キー
 ◦ 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

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

5.4.10 回線切断時の経路保持の設定

- [入力形式] **ip pp rip hold routing rip_bold**
no ip pp rip hold routing [rip_bold]
- [パラメータ] ◦ 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。
- [デフォルト値] off

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

5.4.11 回線接続時の PP 側の RIP の動作の設定

- [入力形式] **ip pp rip connect send rip_action**
no ip pp rip connect send [rip_action]
- [パラメータ] ○ *rip_action*
- 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。
- [デフォルト値] update
- [設定例] # ip pp rip connect interval 60
ip pp rip connect send interval

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

5.4.12 回線接続時の PP 側の RIP 送出の時間間隔の設定

- [入力形式] **ip pp rip connect interval time**
no ip pp rip connect interval [time]
- [パラメータ] ○ *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。
- [デフォルト値] 30
- [設定例] # ip pp rip connect interval 60
ip pp rip connect send interval

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

5.4.13 回線切断時の PP 側の RIP の動作の設定

- [入力形式] **ip pp rip disconnect send rip_action**
no ip pp rip disconnect send [rip_action]
- [パラメータ] ○ *rip_action*
- none 回線切断時に RIP を送出しない
 - interval **ip pp rip disconnect interval** コマンドで設定された時間間隔で RIP を送出する
 - update 経路情報が変わった時にのみ RIP を送出する
- [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。
- [デフォルト値] none
- [設定例] # ip pp rip disconnect interval 1800
ip pp rip disconnect send interval

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

5.4.14 回線切断時の PP 側の RIP 送出の時間間隔の設定

[入力形式] **ip pp rip disconnect interval time**
no ip pp rip disconnect interval [time]

[パラメータ] ◦ *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。

[デフォルト値] 3600

[設定例] # ip pp rip disconnect interval 1800
 # ip pp rip disconnect send interval

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

5.4.15 バックアップ時に RIP の送信元インタフェースを切り替えるか否かを設定する

[入力形式] **ip pp rip backup interface switch**

[パラメータ] ◦ *switch*
 • on.....切り替える
 • off.....切り替えない

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

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

[デフォルト値] off

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

5.5 VRRP の設定

5.5.1 インタフェース毎の VRRP の設定

[入力形式] **ip interface vrrp vrid ip_address** [priority=*priority*] [preempt=*preempt*] [auth=*auth*]
no ip interface vrrp vrid [*vrid*...]

[パラメータ]

- *interface* LAN インタフェース名
- *vrid* VRRP グループ ID (1..255)
- *ip_address* 仮想ルータの IP アドレス
- *priority* 優先度 (1..254)
- *preempt* プリエンプトモード
 - on
 - off
- *auth* 8 文字以内のテキスト認証文字列

[説明] 指定した VRRP グループを利用することを設定する。
 同じ VRRP グループに所属するルータの間では、VRID 及び仮想ルータの IP アドレスを一致させておかななくては
 いけない。これらが食い違った場合の動作は予測できない。
auth パラメータを指定しない場合には、認証なしとして動作する。

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

[デフォルト値] *priority*=100
preempt=on
auth= 認証なし

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

5.5.2 シャットダウントリガの設定

[入力形式] **ip interface vrrp shutdown trigger vrid interface**
ip interface vrrp shutdown trigger vrid pp pp-num [dcli=dcli]
ip interface vrrp shutdown trigger vrid route network [nexthop]
no ip interface vrrp shutdown trigger vrid interface
no ip interface vrrp shutdown trigger vrid pp pp-num [...]
no ip interface vrrp shutdown trigger vrid route network

[パラメータ] ○ *interface*LAN インタフェース名
 ○ *vrid*VRRP グループ ID (1..255)
 ○ *pp-num*PP 番号
 ○ *dcli*DLCI 番号
 ○ *network*
 • ネットワークアドレス
 • IP アドレス / マスク長
 • default
 ○ *nexthop*
 • インタフェース名
 • IP アドレス

[説明] 設定した VRRP グループでマスタールータとして動作している場合に、指定した条件によってシャットダウンすることを設定する。
 • LAN インタフェース形式 指定した LAN インタフェースのリンクが落ちるとシャットダウンする。
 • pp 形式 指定した PP 番号に該当する回線で通信できなくなった場合にシャットダウンする。通信できなくなるとは、ケーブルが抜けるなどレイヤ 1 が落ちた場合と、以下の場合である。
 □ 回線が ISDN 回線である時は、呼が接続されていない場合
 □ 回線が専用線である時には、LCP キープアライブによって通信相手が落ちたと判断した場合
 □ 回線がフレームリレーであって "dcli=dcli" を指定している場合には、PVC 状態確認手順によって指定した DLCI 番号が通信できないと判断した場合
 □ **pp keepalive use** 設定によりダウンが検出された場合
 • route 形式 指定した経路が経路テーブルに存在しないか、*nexthop* で指定したインタフェースもしくは IP アドレスで指定するゲートウェイに向いていない場合に、シャットダウンする。
nexthop を省略した場合には、経路がどのような先を向いていても存在する限りはシャットダウンしない。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

5.6 バックアップの設定

5.6.1 プロバイダ接続がダウンした時にバックアップする接続先の指定

[入力形式] **pp backup peer_num**
pp backup backup_interface gateway
no pp backup

[パラメータ] ○ *peer_num*バックアップとして pp を使用する相手の相手先情報番号
 ○ *backup_interface*バックアップとして使用する LAN インタフェース
 ○ *gateway*ゲートウェイの IP アドレス

[説明] 選択した相手先に対するプロバイダ接続がダウンした場合にバックアップするインタフェース情報を設定する。

[ノート] PP 毎のコマンドである。

接続のダウンを検知するキープアライブ動作が必要なため、専用線の場合は **pp keepalive use lcp-echo** の設定が、それ以外の場合には **pp always-on on** が同時に必要になる。

プロバイダ接続のバックアップなど、バックアップ接続先にバックアップであることを通知する必要のない場合に使用する。拠点間接続のバックアップでは、専用線接続による **leased backup** を使用することもできる。**leased backup** では相手先にバックアップ接続であることが通知されるので、経路が双方で切り換えられる。

[デフォルト値] none

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

5.6.2 バックアップからの復帰待ち時間の設定

[入力形式]	pp backup recovery time <i>time</i> no pp backup recovery time [<i>time</i>]														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>time</i> <ul style="list-style-type: none"> • 秒数 (1..21474836) • off..... すぐに復帰 														
[説明]	バックアップから復帰する場合には、すぐに復帰させるか、設定された時間だけ待ってから復帰するかを設定する。														
[ノート]	この設定は、すべての PP で共通に用いられる。また専用線バックアップでも FR バックアップでもこの設定が共通に用いられる。														
[デフォルト値]	off														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 14.28%;">RTX2000</td> <td style="width: 14.28%;">RTX1000</td> <td style="width: 14.28%;">RT300i</td> <td style="width: 14.28%;">RT140p</td> <td style="width: 14.28%;">RT140f</td> <td style="width: 14.28%;">RT140i</td> <td style="width: 14.28%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

5.6.3 PP 経由のキープアライブを使用するか否かの設定

[入力形式]	pp keepalive use lcp-echo pp keepalive use icmp-echo <i>dest_ip</i> [downwait= <i>downwait</i>] [upwait= <i>upwait</i>] [disconnect= <i>disc</i>][<i>dest_ip</i> ...] pp keepalive use lcp-echo icmp-echo <i>dest_ip</i> [downwait= <i>downwait</i>] [upwait= <i>upwait</i>] [disconnect= <i>disc</i>][<i>dest_ip</i> ...] pp keepalive use off no pp keepalive use														
[パラメータ]	<ul style="list-style-type: none"> ○ lcp-echo LCP Echo Request/Reply を用いる ○ icmp-echo ICMP Echo Request/Reply を用いる ○ <i>dest_ip</i> キープアライブ確認先の IP アドレス ○ <i>downwait</i> icmp-echo を使用する場合のダウン検知のための許容応答時間 (ミリ秒)(1..1000) ○ <i>upwait</i> icmp-echo を使用する場合のアップ検知のための許容応答時間 (ミリ秒)(1..1000) ○ <i>disc</i> icmp-echo を使用する場合の無応答切断時間 (秒)(1.. 21474836) ○ off..... キープアライブを使用しない 														
[説明]	<p>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。</p> <p>lcp-echo 指定で LCP Echo Request/Reply を用い、icmp-echo も指定すれば ICMP Echo Request/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。</p>														
[ノート]	<p>off を指定した場合でも、pp always-on on と設定されていれば LCP Echo によるキープアライブが実行される。</p> <p>icmp-echo での確認先 IP アドレスへの経路情報は、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。</p> <p><i>downwait</i> パラメータの設定で応答時間を制限する場合でも、pp keepalive interval の設定値のほうが小さい場合には、pp keepalive interval の設定値が優先される。</p> <p><i>downwait</i>、<i>upwait</i> パラメータのうち一方しか設定していない場合には、他方も同じ値が設定されたものとして動作する。</p> <p>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は、disconnect 指定が有効である。設定時間内に icmp-echo の応答がない場合、PPPoE レベルで一度切断操作を行うため、pp always-on on との併用により再接続動作を行うことができる。デフォルトでは <i>disc</i>=70 程度に設定しておけば、ダウン検出後の切断動作が期待できる。</p>														
[デフォルト値]	off														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 14.28%;">RTX2000</td> <td style="width: 14.28%;">RTX1000</td> <td style="width: 14.28%;">RT300i</td> <td style="width: 14.28%;">RT140p</td> <td style="width: 14.28%;">RT140f</td> <td style="width: 14.28%;">RT140i</td> <td style="width: 14.28%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

5.6.4 PP 経由のキープアライブのログをとるか否かの設定

- [入力形式] **pp keepalive log log**
no pp keepalive log [log]
- [パラメータ] ◦ *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。
- [デフォルト値] off

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

5.6.5 PP 経由のキープアライブの時間間隔の設定

- [入力形式] **pp keepalive interval interval [count]**
no pp keepalive interval [interval [count]]
- [パラメータ] ◦ *interval*キープアライブパケットを送出する時間間隔 [秒](1..65535)
◦ *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)
- [説明] キープアライブパケットを送出する時間間隔とダウン検出を判定する回数を設定する。
- [ノート] PP 毎のコマンドである。
一度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。
- [デフォルト値] *interval* = 30
count = 6

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

5.6.6 専用線ダウン検出時の動作の設定

- [入力形式] **leased keepalive down action**
no leased keepalive down [action]
- [パラメータ] ◦ *action*
 - silent.....何もしない
 - resetルータを再起動する
- [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。
- [デフォルト値] silent

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

5.6.7 LAN 経由でのプロバイダ接続がダウンした時にバックアップする接続先の指定

[入力形式]	lan backup interface peer_num lan backup interface backup_interface gateway no lan backup interface														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>interface</i> バックアップ対象の LAN インタフェース名 ○ <i>peer_num</i> バックアップとして pp を使用する場合の相手先情報番号 ○ <i>backup_interface</i> バックアップとして使用する LAN インタフェース ○ <i>gateway</i> ゲートウェイの IP アドレス 														
[説明]	指定する LAN インタフェースに対して、LAN 経由でのプロバイダ接続がダウンした場合にバックアップするインタフェース情報を設定する。														
[ノート]	バックアップ動作のためには、LAN 経由での接続のダウンを検知するために lan keepalive use コマンドでの設定が併せて必要である。プロバイダ接続のバックアップなど、バックアップ接続先にバックアップ情報を通知する必要のない場合に使用する。														
[デフォルト値]	none														
[適用モデル]	<table border="1" style="border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

5.6.8 LAN 経由のキープアライブを使用するか否かの設定

[入力形式]	lan keepalive use interface icmp-echo dest_ip [downwait=downwait] [upwait=upwait] [dest_ip...] lan keepalive use interface arp dest_ip [dest_ip...] lan keepalive use interface icmp-echo dest_ip [downwait=wait] [upwait=wait] [dest_ip...] arp dest_ip [dest_ip...] lan keepalive use off no pp keepalive use interface														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>interface</i> バックアップ対象の LAN インタフェース名 ○ <i>dest_ip</i> キープアライブ確認先の IP アドレス ○ <i>downwait</i> icmp-echo を使用する場合のダウン検知のための許容応答時間 (ミリ秒)(1..1000) ○ <i>upwait</i> icmp-echo を使用する場合のアップ検知のための許容応答時間 (ミリ秒)(1..1000) ○ <i>off</i> キープアライブを使用しない 														
[説明]	指定する LAN インタフェースに対して、キープアライブ動作を行うか否かを設定する。icmp-echo を指定すれば ICMP Echo Request/Reply を用い、arp を指定すれば ARP Request/Reply を用いる。併記することで併用も可能である。														
[ノート]	icmp-echo で確認する IP アドレスに対する経路は、バックアップをする LAN インタフェースに向くこと。downwait パラメータで応答時間を制限する場合でも、lan keepalive interval の設定値のほうが小さい場合には、lan keepalive interval の設定値が優先される。downwait、upwait パラメータのうち一方しか設定していない場合には、他方も同じ値が設定されたものとして動作する。														
[デフォルト値]	キープアライブは使用しない														
[適用モデル]	<table border="1" style="border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

5.6.9 LAN 経由のキープアライブの時間間隔の設定

- [入力形式] **lan keepalive interval interface interval [count]**
- [パラメータ] ◦ *interface*バックアップ対象の LAN インタフェース名
 ◦ *interval*キープアライブパケットを送出する時間間隔 (1.. 65535)
 ◦ *count* ダウン検出を判定する回数 (3 ..100)
- [説明] 指定する LAN インタフェースに対して、キープアライブパケットの送出間隔とダウン検出を判定する回数を設定する。*count* に設定した回数だけ連続して応答パケットを検出できない場合に、ダウンと判定する。
- 一度応答が返ってこないのを検出したら、その後のキープアライブパケットの送出間隔は 1 秒に短縮される。そのため、デフォルトの設定値の場合でもダウン検出に要する時間は 35 秒程度である。
- [デフォルト値] *interval* = 30
 count = 6

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

5.6.10 バックアップからの復帰待ち時間の設定

- [入力形式] **lan backup recovery time interface [time]**
 no lan backup recovery time
- [パラメータ] ◦ *interface*バックアップ対象の LAN インタフェース名
 ◦ *time*
 • 秒数 (1.. 21474836)
 • off
- [説明] 指定する LAN インタフェースに対して、バックアップから復帰する場合に、すぐに復帰させるか、設定された時間だけ待ってから復帰するかを設定する。
- [デフォルト値] off

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

5.6.11 LAN 経由のキープアライブのログをとるか否かの設定

- [入力形式] **lan keepalive log interface log**
 no lan keepalive log interface
- [パラメータ] ◦ *interface*バックアップ対象の LAN インタフェース名
 ◦ *log*
 • on ログをとる
 • off ログをとらない
- [説明] キープアライブパケットのログをとるか否かを設定する。
- [デフォルト値] off

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

6. IPX の設定

6.1 インタフェース共通の設定

6.1.1 IPX パケットを扱うか否かの設定

[入力形式] **ipx routing** *routing*
 no ipx routing [*routing*]

[パラメータ] ◦ *routing*
 • on IPX パケットを処理対象として扱う
 • off IPX パケットを処理対象として扱わない

[説明] IPX パケットをルーティングするかどうかを設定する。このスイッチを **on** にしないと IPX 関連は一切動作しない。

[デフォルト値] off

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

6.1.2 IPX パケットのフィルタの設定

[入力形式] **ipx filter filter_num pass_reject src_net [src_node [dst_net [dst_node [type [src_socket [dst_socket]]]]]]**
no ipx filter filter_num [pass_reject]

- [パラメータ]
- *filter_num*静的フィルタの番号 (1..100)
 - *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_net* 始点 IPX ネットワーク番号
 - 0:0:0:1FF:FF:FF:FE (2 桁以内の 16 進数以外に '*' も指定可)
 - * (すべての IPX ネットワーク番号)
 - *src_node*始点 IPX ノード番号
 - 0:0:0:0:1FF:FF:FF:FF:FE (2 桁以内の 16 進数以外に '*' も指定可)
 - * (すべての IPX ノード番号)
 - 省略時は一個の * と同じ
 - *dst_net* 終点 IPX ネットワーク番号 *src_net* と同じ形式。
 - *dst_node*終点 IPX ノード番号 *src_node* と同じ形式。
 - *type*IPX パケットタイプ

unknown	0
rip	1
sap	4
spx	5
ncp	17
netbios	20

 - 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 (5 個以内)
 - * (すべての IPX パケットタイプ)
 - 省略時は一個の * と同じ
 - *src_socket*始点ソケット番号

ncp	0x0451
sap	0x0452
rip	0x0453
netbios	0x0455
diag	0x0456
serialization	0x0457

 - 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 (5 個以内)
 - * (すべてのソケット番号)
 - 省略時は一個の * と同じ
 - *dst_socket*終点ソケット番号 *src_socket* と同じ形式。

[説明] IPX パケットに対するフィルタを設定する。
 このコマンドで設定されたフィルタは、**ipx interface secure filter** コマンド、**ipx pp secure filter** コマンドで
 用いられる。

[ノート] IPX パケットタイプでは、"-xxx" は "0-xxx" の意味に、また "yyy-" は "yyy-255" の意味に取る。
 ソケット番号では、"yyy" は "yyy-65535" の意味に取る。
restrict-log および **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、そのために回
 線に発信するまでもないようなパケットに対して有効である。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

6.1.3 静的な SAP テーブルの設定

- [入力形式] **ipx sap service_type server_name network node_num socket bop**
no ipx sap service_type server_name [network node_num socket bop]
- [パラメータ] ○ *service_type*..... サービスタイプ
- 10 進数 (0..65535)
 - 0x に続く 4 桁以内の 16 進数
 - *file*..... 0x0004 の二一モニック
 - *printer* 0x0007 の二一モニック
- *server_name*..... サーバ名
- 'A' ~ 'Z', '0' ~ '9', '-', '@' で構成された 47 文字以内の文字列
- *network* サーバの IPX ネットワーク番号 (0:0:0:1 .. FF:FF:FF:FE)
- *node_num*..... サーバの IPX ノード番号 (0:0:0:0:0:1 .. FF:FF:FF:FF:FE)
- *socket*..... ソケット番号
- 10 進数 (0..65535)
 - 0x に続く 4 桁以内の 16 進数
 - プロトコルを表す二一モニック
- | | |
|----------------------|--------|
| <i>ncp</i> | 0x0451 |
| <i>sap</i> | 0x0452 |
| <i>rip</i> | 0x0453 |
| <i>netbios</i> | 0x0455 |
| <i>diag</i> | 0x0456 |
| <i>serialization</i> | 0x0457 |
- *bop*..... ホップカウント (1..14)
- [説明] SAP テーブルを設定する。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

6.1.4 IPX SAP Get Nearest Server Request に応答するか否かの設定

- [入力形式] **ipx sap response response**
no ipx sap response [response]
- [パラメータ] ○ *response*
- *on*..... 応答する
 - *off*..... 応答しない
- [説明] IPX SAP Get Nearest Server Request に応答するか否かを設定する。
- [デフォルト値] on

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

6.2 LAN 側の設定

6.2.1 イーサネットフレームタイプの設定

- [入力形式] **ipx interface frame type type**
no ipx interface frame type [type]
- [パラメータ] ○ interfaceLAN インタフェース名
 ○ type
 • 0IEEE 802.3 Raw
 • 1Ethernet II、イーサネットタイプは 0x8137
 • 2IEEE 802.3 + IEEE 802.2 SAP は 0xE0
 • 3IEEE 802.3 + IEEE 802.2 SNAP、プロトコル ID は 0x0000008137
- [説明] IPX が用いるイーサネットでのフレームタイプを設定する。
 同じイーサネット上にある NetWare サーバや NetWare ワークステーションの設定と一致させる必要がある。

type	NetWare での表現
0	ETHERNET 802.3
1	ETHERNET II
2	ETHERNET 802.2
3	ETHERNET SNAP

[デフォルト値] 0

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

6.2.2 LAN 側の IPX ネットワーク番号の設定

- [入力形式] **ipx interface network network**
no ipx interface network [network]
- [パラメータ] ○ interfaceLAN インタフェース名
 ○ networkIPX ネットワーク番号 (0:0:0:1 ..FF:FF:FF:FE)
- [説明] LAN インタフェースに割り当てる IPX ネットワーク番号を設定する。
- [デフォルト値] IPX ネットワーク番号は設定されていない

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

6.2.3 経路情報の追加

- [入力形式] **ipx interface route network gateway hop [ticks]**
no ipx interface route network [gateway hop [ticks]]
- [パラメータ] ○ interfaceLAN インタフェース名
 ○ network終点 IPX ネットワーク番号 (0:0:0:1 .. FF:FF:FF:FE)
 ○ gatewayゲートウェイの IPX ノード番号 (0:0:0:0:1 .. FF:FF:FF:FF:FE)
 ○ hopホップカウント (1..14)
 ○ ticksティック (1..65535)
- [説明] IPX の経路情報テーブルに LAN 側の経路情報を追加する。
- [ノート] ティックを省略した場合はホップカウントと同じになる。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

6.2.4 LAN 側の RIP/SAP ブロードキャストの設定

- [入力形式] **ipx interface ripsap broadcast broadcast**
no ipx interface ripsap broadcast [broadcast]
- [パラメータ] ◦ *interface* LAN インタフェース名
 ◦ *broadcast*
 • 秒数 (60..21474836)
 • off RIP/SAP をブロードキャストしない
- [説明] LAN に対して RIP/SAP をブロードキャストする間隔を設定する。
 off を設定すると、ブロードキャストしなくなる。
- [ノート] この設定にかかわらず、RIP/SAP Request に対しては常に Response を返す。
- [デフォルト値] 60

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

6.2.5 LAN 側でのフィルタリングによるセキュリティの設定

- [入力形式] **ipx interface secure filter direction filter_list**
no ipx interface secure filter direction [filter_list]
- [パラメータ] ◦ *interface* LAN インタフェース名
 ◦ *direction*
 • in LAN 側から入ってくる方向でフィルタを適用
 • out LAN 側へ出ていく方向でフィルタを適用
 ◦ *filter_list* 100 個以内の空白で区切られたフィルタ番号の並び
- [説明] LAN 側に対して適用する IPX フィルタを設定する。
- [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。
 ipx filter 1 pass 0:0:1:*
 ipx filter 2 reject 0:0:1:1
 ipx lan secure filter in 1 2
 では、最初のフィルタリスト 1 で通過が決定した後でフィルタリスト 2 の破棄を判断することになるのでフィルタリスト 2 は無効である。
 どのフィルタにも一致しない場合は破棄になる。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

6.3 PP 側相手毎の IPX の設定

6.3.1 IPX ルーティング許可の設定

- [入力形式] **ipx pp routing routing**
no ipx pp routing [routing]
- [パラメータ] ◦ *routing*
 • on PP 側に IPX パケットをルーティングする
 • off PP 側に IPX パケットをルーティングしない
- [説明] 選択されている相手について IPX パケットを PP 側にルーティングするかどうかを設定する。
- [デフォルト値] off

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

6.3.2 PP 側 IPX ネットワーク番号の設定

[入力形式] **ipx pp network network [node_num]**
no ipx pp network [network [node_num]]

[パラメータ] ○ *network*IPX ネットワーク番号 (0:0:0:1..FF:FF:FF:FE)
 ○ *node_num*IPX ノード番号 (0:0:0:0:1..FF:FF:FF:FF:FF:FE)

[説明] PP インタフェースに割り当てる IPX ネットワーク番号を設定する。

[ノート] IPX ノード番号は通常デフォルトのままとする。

[デフォルト値] IPX ネットワーク番号は設定されていない
 IPX ノード番号は MAC アドレス

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

6.3.3 経路情報の追加

[入力形式] **ipx pp route network [name] hop [tick]**
ipx pp route network [dlsi=dlsi_num] hop [tick]
no ipx pp route network [network...]

[パラメータ] ○ *network*終点 IPX ネットワーク番号 (0:0:0:1..FF:FF:FF:FE)
 ○ *name*名前 (16 文字以内)
 ○ *hop*ホップカウント (1..14)
 ○ *tick*ティック (1..65535)
 ○ *dlsi_num*ゲートウェイの DLCI

[説明] 選択されている相手について経路情報テーブルに PP 側の IPX の経路情報を追加する。フレームリレーの場合は、ゲートウェイを指定するために DLCI を書くことができる。

[ノート] 通常 PP 側に関してのみ設定する。ティックを省略した場合はホップカウントの 55 倍になる。*name* パラメータは、anonymous が選択された場合のみ有効である。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

6.3.4 回線接続時の PP 側の RIP/SAP の動作の設定

[入力形式] **ipx pp ripsap connect send send**
no ipx pp ripsap connect send [send]

[パラメータ] ○ *send*
 ● none回線接続時に RIP/SAP を送出しない
 ● interval **ipx pp ripsap connect interval** コマンドで設定された時間間隔で RIP/SAP を送出する
 ● updateRIP/SAP テーブルに変更があった場合だけ送出する

[説明] 選択されている相手について回線接続時に RIP/SAP を送出する条件を選択する。

[ノート] この設定にかかわらず、RIP/SAP Request に対しては Response を返す。

[デフォルト値] update

[設定例] # ipx pp ripsap connect interval 120
 # ipx pp ripsap connect send interval

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

6.3.5 回線接続時の PP 側の RIP/SAP 送出の時間間隔の設定

- [入力形式] **ipx pp ripsap connect interval *time***
no ipx pp ripsap connect interval [*time*]
- [パラメータ] ○ *time*..... 秒数 (60..21474836)
- [説明] 選択されている相手について回線接続時に PP 側に RIP/SAP を送出する時間間隔を設定する。
- [デフォルト値] 60
- [設定例] # ipx pp ripsap connect interval 120
ipx pp ripsap connect send interval

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

6.3.6 回線切断時の PP 側の RIP/SAP の動作の設定

- [入力形式] **ipx pp ripsap disconnect send *send***
no ipx pp ripsap disconnect send [*send*]
- [パラメータ] ○ *send*
 - none 回線切断時に RIP/SAP を送出しない
 - interval **ipx pp ripsap disconnect interval** コマンドで設定された時間間隔で RIP/SAP を送出する
 - update RIP/SAP テーブルに変更があった時だけ送出する
- [説明] 選択されている相手について回線切断時に RIP/SAP を送出する条件を選択する。
- [デフォルト値] none
- [設定例] # ipx pp ripsap disconnect interval 120
ipx pp ripsap disconnect send interval

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

6.3.7 回線切断時の PP 側の RIP/SAP 送出の時間間隔の設定

- [入力形式] **ipx pp ripsap disconnect interval *interval***
no ipx pp ripsap disconnect interval [*interval*]
- [パラメータ] ○ *interval*..... 秒数 (60..21474836)
- [説明] 選択されている相手について回線切断時に RIP/SAP を送出する時間間隔を設定する。
- [デフォルト値] 60
- [設定例] # ipx pp ripsap disconnect interval 120
ipx pp ripsap disconnect send interval

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

6.3.8 回線切断時に RIP/SAP 情報を保持するか否かの設定

[入力形式] **ipx pp ripsap hold *bold***
no ipx pp ripsap hold [*bold*]

[パラメータ] ◦ *bold*
 • on.....保持する
 • off.....保持しない

[説明] 選択されている相手について回線接続中に取得した動的 RIP/SAP 情報を回線切断後も保持するか否かを設定する。

[デフォルト値] on

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

6.3.9 IPXWAN 使用の設定

[入力形式] **ipx pp ipxwan use *use***
no ipx pp ipxwan use [*use*]

[パラメータ] ◦ *use*
 • on.....接続時に IPXWAN を用いてパラメータのネゴシエーションを行う
 • off.....パラメータのネゴシエーションは IPXCP で行い、IPXWAN は用いない

[説明] 回線接続時のパラメータネゴシエーションの手順として IPXWAN を用いるかどうかを設定する。

[デフォルト値] on

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

6.3.10 Timer/Information Request の再送間隔と最大再送回数の設定

[入力形式] **ipx pp ipxwan retry *interval max***
no ipx pp ipxwan retry [*interval max*]

[パラメータ] ◦ *interval*秒数 (10..21474836)
 ◦ *max*最大再送回数 (0..10)

[説明] IPXWAN の Timer/Information Request の再送間隔と最大再送回数を設定する。

[デフォルト値] *interval* = 20
max = 3

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

6.3.11 IPXWAN プライマリネットワーク番号の設定

[入力形式] **ipx pp ipxwan primnet *network***
no ipx pp ipxwan primnet [*network*]

[パラメータ] ◦ *network*IPXWAN プライマリネットワーク番号 (0:0:0:1 .. FF:FF:FF:FE)

[説明] IPXWAN で用いるプライマリネットワーク番号を設定する。

[デフォルト値] PP 側インタフェースの MAC アドレスの下位 32 ビット

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

6.3.12 Watchdog パケットに対する代理応答の設定

[入力形式]	ipx pp watchdog proxy <i>proxy</i> no ipx pp watchdog proxy [<i>proxy</i>]														
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>proxy</i> • on 代理応答する • off 代理応答しない 														
[説明]	回線切断時に、PPの向こう側のワークステーションに対してサーバから出された NCP Watchdog Request パケットに対して代理応答するか否かを設定する。														
[デフォルト値]	on														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT140p</td> <td style="padding: 2px;">RT140f</td> <td style="padding: 2px;">RT140i</td> <td style="padding: 2px;">RT140e</td> </tr> <tr> <td style="padding: 2px;">RT105p</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

6.3.13 Watchdog 代理応答の時間間隔の設定

[入力形式]	ipx pp watchdog interval <i>interval</i> no ipx pp watchdog interval [<i>interval</i>]														
[パラメータ]	◦ <i>interval</i> 秒数 (1..21474836)														
[説明]	PPの向こう側のワークステーションが動作しているかどうかを確認する時間間隔を設定する。														
[デフォルト値]	3600														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT140p</td> <td style="padding: 2px;">RT140f</td> <td style="padding: 2px;">RT140i</td> <td style="padding: 2px;">RT140e</td> </tr> <tr> <td style="padding: 2px;">RT105p</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

6.3.14 SPX キープアライブ代理応答を行うか否かの設定

[入力形式]	ipx pp spx keepalive proxy <i>proxy</i> no ipx pp spx keepalive proxy [<i>proxy</i>]														
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>proxy</i> • on 代理応答を行う • off 代理応答を行わない 														
[説明]	SPX キープアライブ代理応答を行うか否かを設定する。														
[デフォルト値]	on														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT140p</td> <td style="padding: 2px;">RT140f</td> <td style="padding: 2px;">RT140i</td> <td style="padding: 2px;">RT140e</td> </tr> <tr> <td style="padding: 2px;">RT105p</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

6.3.15 SPX キープアライブ代理応答のタイマの設定

[入力形式] **ipx pp spx keepalive timer** *t1* [*t2* [*t3*]]
no ipx pp spx keepalive timer *t1* [*t2* [*t3*]]

[パラメータ] ○ *t1*秒数 (30..21474836)
 ○ *t2*秒数 (30..65535)
 ○ *t3*秒数 (1..65535)

[説明] SPX キープアライブ代理応答のためのタイマ値を設定する。それぞれのタイマ値の意味は次の通り。
 ○ *t1*代理応答を行っていてもこの時間毎に相手に接続し、正常に動作しているかどうか確認する。
 ○ *t2*この時間以内に、ローカルに接続しているサーバ/クライアントから SPX パケットを受信できなかったら正常でないものと判断する。
 ○ *t3*この時間間隔でローカルに接続しているサーバ/クライアントに対してリモートにある筈のマシンの代理で本機が SPX キープアライブパケットを送信する。

[デフォルト値] *t1* = 7200
t2 = 60
t3 = 10

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

6.3.16 IPX シリアライゼーションパケットをフィルタアウトするか否かの設定

[入力形式] **ipx pp serialization filter** *filter*
no ipx pp serialization filter [*filter*]

[パラメータ] ○ *filter*
 • on.....フィルタアウトする
 • off.....フィルタアウトしない

[説明] 選択されている相手について IPX シリアライゼーションパケットをフィルタアウトするか否かを設定する。

[デフォルト値] on

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

6.3.17 PP 側でのフィルタリングによるセキュリティの設定

[入力形式] **ipx pp secure filter** *direction filter_list*
no ipx pp secure filter *direction* [*filter_list*]

[パラメータ] ○ *direction*
 • in.....PP 側から入って来る方向でフィルタを適用
 • out.....PP 側へ出て行く方向でフィルタを適用
 ○ *filter_list*30 個以内の空白で区切られたフィルタ番号の並び

[説明] PP 側に対し適用するフィルタを設定する。

[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。

```
ipx filter 1 pass 0:0:1:*
ipx filter 2 reject 0:0:1:1
ipx pp secure filter in 1 2
```

では、最初のフィルタリスト 1 で通過が決定した後でフィルタリスト 2 の破棄を判断することになるのでフィルタリスト 2 は無効である。
 どのフィルタにも一致しない場合は破棄になる。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

7. ブリッジの設定

7.1 インタフェース共通の設定

7.1.1 ブリッジ使用許可の設定

[入力形式] **bridge use** *use*
 no bridge use [*use*]

[パラメータ] ◦ *use*

- on ブリッジする
- off ブリッジしない
- multicast マルチキャストのみブリッジする

[説明] ブリッジを行うかどうかを設定する。

[ノート] このスイッチが on でも、ip routing on であれば、IP パケットはブリッジング対象外となる。
 同様に ipx routing on であれば、IPX パケットはブリッジング対象外となる。

[デフォルト値] off

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

7.1.2 ブリッジするインタフェースの設定

[入力形式] **bridge group** *interface_list*
 no bridge group [*interface_list*]

[パラメータ] ◦ *interface_list*

- 相手先情報番号
- anonymous
- LAN インタフェース名

[説明] ブリッジをする相手先を設定する。
 PP の相手先は、WAN 回線数の 2 倍まで設定できる。
 LAN の相手先は、LAN インタフェース数まで設定できる。

[ノート] anonymous を含める場合には、相手先情報番号を同時に指定することはできない。

[デフォルト値] インタフェースは設定されていない

[設定例] ◦ LAN1 ポートと LAN2 ポート間でブリッジする
 # bridge group lan1 lan2

 ◦ LAN2 ポートと相手先情報番号 3 の間でブリッジする
 # bridge group lan2 3

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

7.1.3 ブリッジのフィルタの設定

[入力形式]	bridge filter <i>filter_num</i> <i>pass_reject</i> <i>src_mac</i> [<i>dst_mac</i> [<i>offset</i> <i>byte_list</i>]] bridge filter <i>filter_num</i> [<i>pass_reject</i> <i>src_mac</i> [<i>dst_mac</i> [<i>offset</i> <i>byte_list</i>]]]														
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>filter_num</i> 静的フィルタの番号 (1..100) ◦ <i>pass_reject</i> <ul style="list-style-type: none"> • <i>pass-log</i> 一致すれば通す (ログに記録する) • <i>pass-nolog</i> 一致すれば通す (ログに記録しない) • <i>reject-log</i> 一致すれば破棄する (ログに記録する) • <i>reject-nolog</i> 一致すれば破棄する (ログに記録しない) • <i>restrict-log</i> 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) • <i>restrict-nolog</i> 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) ◦ <i>src_mac</i> 始点 MAC アドレス <ul style="list-style-type: none"> • <i>xx:xx:xx:xx:xx:xx</i>, <i>xx</i> は 16 進数、または * • * (すべての MAC アドレスに対応) ◦ <i>dst_mac</i> 終点 MAC アドレス <i>src_mac</i> と同じ形式。省略時は一つの * と同じ ◦ <i>offset</i> オフセットを表す 10 進数 (イーサネットフレームの始点 MAC アドレスの直後を 0 とするバイト数) ◦ <i>byte_list</i> <ul style="list-style-type: none"> • バイト列 <ul style="list-style-type: none"> ▪ <i>xx(xx)</i> は 2 桁の 16 進数) ▪ 上項目のカンマで区切った並び (16 個以内) • * (すべてのバイト表現) 														
[説明]	ブリッジのフィルタを設定する。このコマンドで設定されたフィルタは bridge lan filter コマンド、 bridge pp filter コマンドで用いられる。														
[ノート]	<i>restrict-log</i> および <i>restrict-nolog</i> 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、そのために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である。														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

7.1.4 MAC アドレスのラーニングを行うか否かの設定

[入力形式]	bridge learning <i>learning</i> no bridge learning [<i>learning</i>]														
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>learning</i> <ul style="list-style-type: none"> • <i>on</i> 行う • <i>off</i> 行わない 														
[説明]	ラーニングとは、インタフェースから受け取った始点 MAC アドレスを覚えておき、別のインタフェースから受け取ったパケットをブリッジする場合に終点 MAC アドレスが覚えていた MAC アドレスに一致したならばそのインタフェースにのみパケットを送り出すことを言う。このコマンドではインタフェースから受け取った始点 MAC アドレスを覚えておくかどうかを設定する。														
[デフォルト値]	on														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

7.1.5 ラーニング情報消去タイマの設定

[入力形式]	bridge learning expire <i>time</i> no bridge learning expire [<i>time</i>]														
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>time</i> <ul style="list-style-type: none"> • 秒数 (1..21474836) • <i>off</i> タイマを設定しない 														
[説明]	このコマンドで設定した時間中に、ある始点 MAC アドレスのパケットを受け取らなかった場合には、その MAC アドレスに関するラーニング情報を消去する。 <i>off</i> を指定するとラーニング情報は自動的に消去されなくなる。														
[パラメータ]	off														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

7.2 LAN 側の設定

7.2.1 ラーニング情報の設定

[入力形式]	bridge interface learning mac_address no bridge interface learning mac_address														
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>interface</i> LAN インタフェース名 ◦ <i>mac_address</i> xx:xx:xx:xx:xx:xx (xx は 16 進数) 														
[説明]	LAN 側インタフェースに対して MAC アドレスのラーニング情報を設定する。														
[ノート]	ラーニング情報は全体で 30 個まで設定できる。														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

7.2.2 LAN 側でのブリッジのフィルタリングの設定

[入力形式]	bridge interface filter direction filter_list no bridge interface filter direction [filter_list]														
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>interface</i> LAN インタフェース名 ◦ <i>direction</i> <ul style="list-style-type: none"> • <i>in</i> LAN 側から入ってくるパケットのフィルタリング • <i>out</i> LAN 側に出ていくパケットのフィルタリング ◦ <i>filter_list</i> 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 bridge filter コマンドによるパケットのフィルタを組み合わせ、ブリッジするパケットの種類を制限を設定する。														
[デフォルト値]	フィルタは設定されていない														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

7.3 PP 側相手毎のブリッジの設定

7.3.1 ラーニング情報の設定

[入力形式]	bridge pp learning mac_address [dlci=dlci_num] no bridge pp learning mac_address [dlci=dlci_num]														
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>mac_address</i>xx:xx:xx:xx:xx:xx (xx は 16 進数) ◦ <i>dlci_num</i> DLCI 番号 														
[説明]	PP 側インタフェースに対して MAC アドレスのラーニング情報を設定する。フレームリレーの場合は、DLCI 番号を指定することが可能である。														
[ノート]	ラーニング情報は全体で 30 個まで設定できる。														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

7.3.2 PP側でのブリッジのフィルタリングの設定

- [入力形式] **bridge pp filter** *direction filter_list*
 no bridge pp filter *direction [filter_list]*
- [パラメータ] ◦ *direction*
- *in*.....PP側から入ってくるパケットのフィルタリング
 - *out*.....PP側に出っていくパケットのフィルタリング
- *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] PP側を通るパケットについて **bridge filter** コマンドによるパケットのフィルタを組み合わせ、ブリッジするパケットの種類を制限を設定する。
- [デフォルト値] フィルタは設定されていない

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

8. PPPの設定

8.1 相手の名前とパスワードの設定

【入力形式】 **pp auth username** *username password* [*myname myname mypass*] [*isdn1*] [*clid* [*isdn2*]] [*mscbc*p] [*ip_address*]
pp auth username *username password* [*myname myname mypass*] [*ip_address*]
no pp auth username *username* [*password...*]

【パラメータ】

- *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ためのキーワード
- *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
- *mscbc*p 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】 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。

RTX2000 と RT105e では第 2 書式を用いる。

双方向で認証を行う場合には、相手のユーザ名が確定してから自分を相手に認証させるプロセスが動き始める。これらのパラメータが設定されていない場合には、**pp auth myname** コマンドの設定が参照される。オプションで ISDN 番号が設定でき、名前と結びついたルーティングやリモート IP アドレスに対しての発信を可能にする。*isdn1* は発信用の ISDN アドレスである。*isdn1* を省略すると、この相手には発信しなくなる。名前に '*' を与えた場合にはワイルドカードとして扱い、他の名前とマッチしなかった相手に対してその設定を使用する。

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

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

【適用モデル】

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

8.2 要求する認証タイプの設定

[入力形式] **pp auth request *auth* [arrive-only]**
no pp auth request [*auth* [arrive-only]]

[パラメータ] ○ *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

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

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

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

PP 毎のコマンドである。

[デフォルト値] none

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.3 受け入れる認証タイプの設定

[入力形式] **pp auth accept *accept* [*accept*]**
no pp auth accept [*accept*]

[パラメータ] ○ *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 による認証を要求する
- mschap-v2 MSCHAP Version2 による認証を要求する

[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。

[デフォルト値] 認証を受け入れない

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.4 自分の名前とパスワードの設定

[入力形式] **pp auth myname *myname password***
no pp auth myname [*myname password*]

[パラメータ] ○ *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。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

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

[入力形式]	pp auth multi connect prohibit prohibit no pp auth multi connect prohibit [<i>prohibit</i>]														
[パラメータ]	○ <i>prohibit</i> <ul style="list-style-type: none"> • on 禁止する • off 禁止しない 														
[説明]	pp auth username で登録した同一 <i>username</i> を持つ相手からの二重接続を禁止するか否かを設定する。														
[ノート]	定額制プロバイダを営む場合に便利である。ユーザ管理を RADIUS で行う場合には、二重接続の禁止は RADIUS サーバの方で対処する必要がある。 anonymous が選択された場合のみ有効である。														
[デフォルト値]	off														
[適用モデル]	<table border="1" style="border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

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

[入力形式]	ppp lcp acfc acfc no ppp lcp acfc [<i>acfc</i>]														
[パラメータ]	○ <i>acfc</i> <ul style="list-style-type: none"> • 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。														
[デフォルト値]	off														
[適用モデル]	<table border="1" style="border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

8.6.2 Magic Number オプション使用の設定

[入力形式]	ppp lcp magicnumber magicnumber no ppp lcp magicnumber [<i>magicnumber</i>]														
[パラメータ]	○ <i>magicnumber</i> <ul style="list-style-type: none"> • 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。														
[デフォルト値]	on														
[適用モデル]	<table border="1" style="border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

8.6.3 Maximum Receive Unit オプション使用の設定

- [入力形式] **ppp lcp mru *mru* [*length*]**
no ppp lcp mru [*mru* [*length*]]
- [パラメータ] ◦ *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。
- [デフォルト値] *mru* = on
 length = 1792

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

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

- [入力形式] **ppp lcp pfc *pfc***
no ppp lcp pfc [*pfc*]
- [パラメータ] ◦ *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。
- [デフォルト値] off

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.6.5 lcp-restart パラメータの設定

- [入力形式] **ppp lcp restart *time***
no ppp lcp restart [*time*]
- [パラメータ] ◦ *time* ミリ秒 (20..10000)
- [説明] 選択されている相手について [PPP,LCP] の configure-request、terminate-request の再送時間を設定する。
- [デフォルト値] 3000

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.6.6 lcp-max-terminate パラメータの設定

[入力形式]	ppp lcp maxterminate count no ppp lcp maxterminate [count]														
[パラメータ]	○ <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 terminate-request の送信回数を設定する。														
[デフォルト値]	2														
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

8.6.7 lcp-max-configure パラメータの設定

[入力形式]	ppp lcp maxconfigure count no ppp lcp maxconfigure [count]														
[パラメータ]	○ <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 configure-request の送信回数を設定する。														
[デフォルト値]	10														
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

8.6.8 lcp-max-failure パラメータの設定

[入力形式]	ppp lcp maxfailure count no ppp lcp maxfailure [count]														
[パラメータ]	○ <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 configure-nak の送信回数を設定する。														
[デフォルト値]	10														
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

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

[入力形式]	ppp lcp silent sw														
[パラメータ]	○ <i>sw</i> <ul style="list-style-type: none"> • on PPP/LCP で、回線接続直後の Configure-Request の送信を、相手から Configure-Request を受信するまで遅らせる • off PPP/LCP で、回線接続直後に Configure-Request を送信する 														
[説明]	PPP/LCP で、回線接続後 Configure-Request をすぐに送信するか、あるいは相手から Configure-Request を受信するまで遅らせるかを設定する。通常は回線接続直後に Configure-Request を送信して構わないが、接続相手によってはこれを遅らせた方がよいものがある。														
[デフォルト値]	off														
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

84 8.PPPの設定

8.7 PAP関連の設定

8.7.1 pap-restart パラメータの設定

[入力形式] **ppp pap restart time**
no ppp pap restart [time]

[パラメータ] ◦ *time* 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。

[デフォルト値] 3000

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

8.7.2 pap-max-authreq パラメータの設定

[入力形式] **ppp pap maxauthreq count**
no ppp pap maxauthreq [count]

[パラメータ] ◦ *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。

[デフォルト値] 10

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

8.8 CHAP関連の設定

8.8.1 chap-restart パラメータの設定

[入力形式] **ppp chap restart time**
no ppp chap restart [time]

[パラメータ] ◦ *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。

[デフォルト値] 3000

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

8.8.2 chap-max-challenge パラメータの設定

[入力形式] **ppp chap maxchallenge count**
no ppp chap maxchallenge [count]

[パラメータ] ◦ *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。

[デフォルト値] 10

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

8.9 IPCP 関連の設定

8.9.1 Van Jacobson Compressed TCP/IP 使用の設定

[入力形式]	ppp ipcp vjc <i>compression</i> no ppp ipcp vjc [<i>compression</i>]														
[パラメータ]	○ <i>compression</i> <ul style="list-style-type: none"> • 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。														
[デフォルト値]	off														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT140p</td> <td style="padding: 2px;">RT140f</td> <td style="padding: 2px;">RT140i</td> <td style="padding: 2px;">RT140e</td> </tr> <tr> <td style="padding: 2px;">RT105p</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

8.9.2 PP 側 IP アドレスのネゴシエーションの設定

[入力形式]	ppp ipcp ipaddress <i>negotiation</i> no ppp ipcp ipaddress [<i>negotiation</i>]														
[パラメータ]	○ <i>negotiation</i> <ul style="list-style-type: none"> • 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。														
[デフォルト値]	off														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT140p</td> <td style="padding: 2px;">RT140f</td> <td style="padding: 2px;">RT140i</td> <td style="padding: 2px;">RT140e</td> </tr> <tr> <td style="padding: 2px;">RT105p</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

8.9.3 ipcp-restart パラメータの設定

[入力形式]	ppp ipcp restart <i>time</i> no ppp ipcp restart [<i>time</i>]														
[パラメータ]	○ <i>time</i> 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。														
[デフォルト値]	3000														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT140p</td> <td style="padding: 2px;">RT140f</td> <td style="padding: 2px;">RT140i</td> <td style="padding: 2px;">RT140e</td> </tr> <tr> <td style="padding: 2px;">RT105p</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

8.9.4 ipcp-max-terminate パラメータの設定

[入力形式]	ppp ipcp maxterminate <i>count</i> no ppp ipcp maxterminate [<i>count</i>]														
[パラメータ]	○ <i>count</i> 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。														
[デフォルト値]	2														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT140p</td> <td style="padding: 2px;">RT140f</td> <td style="padding: 2px;">RT140i</td> <td style="padding: 2px;">RT140e</td> </tr> <tr> <td style="padding: 2px;">RT105p</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

8.9.5 ipcp-max-configure パラメータの設定

[入力形式] **ppp ipcp maxconfigure count**
no ppp ipcp maxconfigure [count]

[パラメータ] ◦ *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。

[デフォルト値] 10

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.9.6 ipcp-max-failure パラメータの設定

[入力形式] **ppp ipcp maxfailure count**
no ppp ipcp maxfailure [count]

[パラメータ] ◦ *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。

[デフォルト値] 10

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.9.7 IPCP の MS 拡張オプションを使うか否かの設定

[入力形式] **ppp ipcp msex** *msex*
no ppp ipcp msex [*msex*]

[パラメータ] ◦ *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。IPCP の Microsoft 拡張オプションを使うように設定すると、DNS サーバの IP アドレスと WINS (Windows Internet Name Service) サーバの 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 サーバや WINS サーバの 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。

[デフォルト値] off

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.9.8 WINS サーバの IP アドレスの設定

[入力形式] **wins server server1** [*server2*]
no wins server [*server1* [*server2*]]

[パラメータ] ◦ *server; server*.....IP アドレス (xxx.xxx.xxx.xxx (xxx は 10 進数))

[説明] WINS (Windows Internet Name Service) サーバの 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 サーバの IP アドレスを設定する。ルータはこのサーバに対し WINS クライアントとしての動作は一切行わない。

[デフォルト値] WINS サーバは設定されていない

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.10 IPXCP 関連の設定

8.10.1 ipxcp-restart パラメータの設定

[入力形式]	ppp ipxcp restart time no ppp ipxcp restart [time]														
[パラメータ]	○ <i>time</i> ミリ秒 (20..10000)														
[説明]	選択されている相手について [PPP、IPXCP] の configure-request、terminate-request の再送時間を設定する。														
[デフォルト値]	3000														
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

8.10.2 ipxcp-max-terminate パラメータの設定

[入力形式]	ppp ipxcp maxterminate count no ppp ipxcp maxterminate [count]														
[パラメータ]	○ <i>count</i> 回数 (1..10)														
[説明]	選択されている相手について [PPP、IPXCP] の terminate-request の送信回数を設定する。														
[デフォルト値]	2														
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

8.10.3 ipxcp-max-configure パラメータの設定

[入力形式]	ppp ipxcp maxconfigure count no ppp ipxcp maxconfigure [count]														
[パラメータ]	○ <i>count</i> 回数 (1..10)														
[説明]	選択されている相手について [PPP、IPXCP] の configure-request の送信回数を設定する。														
[デフォルト値]	10														
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

8.10.4 ipxcp-max-failure パラメータの設定

[入力形式]	ppp ipxcp maxfailure count no ppp ipxcp maxfailure [count]														
[パラメータ]	○ <i>count</i> 回数 (1..10)														
[説明]	選択されている相手について [PPP、IPXCP] の configure-nak の送信回数を設定する。														
[デフォルト値]	10														
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

8.11 BCP 関連の設定

8.11.1 LAN Identification 使用の設定

[入力形式] **ppp bcp lanid** *lan_id*
no ppp bcp lanid [*lan_id*]

[パラメータ] ○ *lan_id*
 ● 十六進数 (0x1 .. 0xfffffe)
 ● off.....LAN-Identification を使用しない

[説明] LAN-Identification の値を設定する。

[デフォルト値] off

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.11.2 Tinygram compression 使用の設定

[入力形式] **ppp bcp tinycomp** *compression*
no ppp bcp tinycomp [*compression*]

[パラメータ] ○ *compression*
 ● on.....使用する
 ● off.....使用しない

[説明] Tinygram compression を使用するか否かを設定する。

[デフォルト値] on

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.11.3 bcp-restart パラメータの設定

[入力形式] **ppp bcp restart** *time*
no ppp bcp restart [*time*]

[パラメータ] ○ *time*..... ミリ秒 (20..10000)

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

[デフォルト値] 3000

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.11.4 bcp-max-terminate パラメータの設定

[入力形式] **ppp bcp maxterminate** *count*
no ppp bcp maxterminate [*count*]

[パラメータ] ○ *count*..... 回数 (1..10)

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

[デフォルト値] 2

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.11.5 bcp-max-configure パラメータの設定

[入力形式] **ppp bcp maxconfigure count**
 no ppp bcp maxconfigure [count]

[パラメータ] ◦ *count* 回数 (1..10)

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

[デフォルト値] 10

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.11.6 bcp-max-failure パラメータの設定

[入力形式] **ppp bcp maxfailure count**
 no ppp bcp maxfailure [count]

[パラメータ] ◦ *count* 回数 (1..10)

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

[デフォルト値] 10

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.12 MSCBCP 関連の設定**8.12.1 mscbcpr-restart パラメータの設定**

[入力形式] **ppp mscbcpr restart time**
 no ppp mscbcpr restart [time]

[パラメータ] ◦ *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。

[デフォルト値] 1000

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.12.2 mscbcpr-maxretry パラメータの設定

[入力形式] **ppp mscbcpr maxretry count**
 no ppp mscbcpr maxretry [count]

[パラメータ] ◦ *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。

[デフォルト値] 30

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.13 CCP 関連の設定

8.13.1 全パケットの圧縮タイプの設定

[入力形式] **ppp ccp type type**
no ppp ccp type [type]

- [パラメータ] ◦ *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。
 パケットの取りこぼしで頻繁に CCP リセットが発生する環境では、設定を *stac0* にして、パケット毎に圧縮するようにすれば良い。ただし接続先も *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。また、接続相手が Cisco ルータの場合に *stac* を適用するとデータ転送中に頻繁に CCP のリセットが発生して、データ転送速度が遅くなることもある。そのような場合には、設定を *cstac* に変更すると状況が改善することがある。

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。

[デフォルト値] *stac*

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

8.13.2 ccp-restart パラメータの設定

[入力形式] **ppp ccp restart time**
no ppp ccp restart [time]

[パラメータ] ◦ *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。

[デフォルト値] 3000

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

8.13.3 ccp-max-terminate パラメータの設定

[入力形式] **ppp ccp maxterminate count**
no ppp ccp maxterminate [count]

[パラメータ] ◦ *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。

[デフォルト値] 2

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

8.13.4 ccp-max-configure パラメータの設定

[入力形式] **ppp ccp maxconfigure count**
no ppp ccp maxconfigure [count]

[パラメータ] ○ *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。

[デフォルト値] 10

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.13.5 ccp-max-failure パラメータの設定

[入力形式] **ppp ccp maxfailure count**
no ppp ccp maxfailure [count]

[パラメータ] ○ *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。

[デフォルト値] 10

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.14 IPV6CP 関連の設定**8.14.1** IPV6CP を使用するか否かの設定

[入力形式] **ppp ipv6cp use use**
no ppp ipv6cp use [use]

[パラメータ] ○ *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。

[デフォルト値] on

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.15 MP 関連の設定**8.15.1** MP を使用するか否かの設定

[入力形式] **ppp mp use use**
no ppp mp use [use]

[パラメータ] ○ *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。

[デフォルト値] off

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.15.2 MP の制御方法の設定

[入力形式] **ppp mp control** *type*
no ppp mp control [*type*]

[パラメータ] ◦ *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 / 切断を行う場合を設定する。通常は default 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。

[デフォルト値] call

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.15.3 MP のための負荷閾値の設定

[入力形式] **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*]

[パラメータ] ◦ *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。

[デフォルト値] *call_load* = 70
call_count = 1
disc_load = 30
disc_count = 2

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.15.4 MP の最大リンク数の設定

[入力形式] **ppp mp maxlink** *number*
no ppp mp maxlink [*number*]

[パラメータ] ◦ *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。

[デフォルト値] 2

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.15.5 MP の最小リンク数の設定

[入力形式] **ppp mp minlink number**
no ppp mp minlink [number]

[パラメータ] ◦ *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。

[デフォルト値] 1

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.15.6 MP のための負荷計測間隔の設定

[入力形式] **ppp mp timer time**
no ppp mp timer [time]

[パラメータ] ◦ *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。

[デフォルト値] 10

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.15.7 MP のパケットを分割するか否かの設定

[入力形式] **ppp mp divide divide**
no ppp mp divide [divide]

[パラメータ] ◦ *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否かを設定する。
 分割するとうまく接続できない相手に対してだけ off にする。
 分割しないように設定した場合、特に TCP の転送効率に悪影響が出る可能性がある。
 64 バイト以下のパケットは本コマンドの設定に関わらず分割されない。

[デフォルト値] on

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.16 BACP 関連の設定**8.16.1 bacp-restart パラメータ の設定**

[入力形式] **ppp bacp restart time**
no ppp bacp restart [time]

[パラメータ] ◦ *time*..... ミリ秒 (20..10000)

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

[デフォルト値] 3000

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.16.2 bacp-max-terminate パラメータ の設定

[入力形式] **ppp bacp maxterminate count**
no ppp bacp maxterminate [count]

[パラメータ] ◦ *count*.....回数 (1..10)

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

[デフォルト値] 2

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

8.16.3 bacp-max-configure パラメータ の設定

[入力形式] **ppp bacp maxconfigure count**
no ppp bacp maxconfigure [count]

[パラメータ] ◦ *count*.....回数 (1..10)

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

[デフォルト値] 10

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

8.16.4 bacp-max-failure パラメータ の設定

[入力形式] **ppp bacp maxfailure count**
no ppp bacp maxfailure [count]

[パラメータ] ◦ *count*.....回数 (1..10)

[説明] 選択されている相手について [PPP, BACP] の configure-nak を送る回数を設定する。

[デフォルト値] 10

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

8.17 BAP 関連の設定

8.17.1 bap-restart パラメータの設定

[入力形式] **ppp bap restart time**
no ppp bap restart [time]

[パラメータ] ◦ *time*ミリ秒 (20..10000)

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

[デフォルト値] 1000

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

8.17.2 bap-max-retry パラメータの設定

- [入力形式] **ppp bap maxretry count**
no ppp bap maxretry [count]
- [パラメータ] ◦ *count* 再送回数 (1..30)
- [説明] 選択されている相手について [PPP, BAP] の最大再送回数を設定する。
- [デフォルト値] 30

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.18 PPPoE 関連の設定**8.18.1** PPPoE で使用する LAN インタフェースの指定

- [入力形式] **pppoe use interface**
no pppoe use
- [パラメータ] ◦ *interface* LAN インタフェース名
◦ *off* 指定しない
- [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。
- [デフォルト値] off

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.18.2 アクセスコンセントレータ名の設定

- [入力形式] **pppoe access concentrator name**
no pppoe access concentrator
- [パラメータ] ◦ *name* アクセスコンセントレータの名前を表す文字列 (7bit US-ASCII)
- [説明] 選択されている相手について PPPoE で接続するアクセスコンセントレータの名前を設定する。接続できるアクセスコンセントレータが複数ある場合に、どのアクセスコンセントレータに接続するのかを指定するために使用する。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.18.3 セッションの自動接続の設定

- [入力形式] **pppoe auto connect switch**
no pppoe auto connect
- [パラメータ] ◦ *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否かを設定する。
- [デフォルト値] on

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.18.4 セッションの自動切断の設定

[入力形式] **pppoe auto disconnect switch**
no pppoe auto disconnect

[パラメータ] ◦ *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否かを設定する。

[デフォルト値] on

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

8.18.5 PADIパケットの最大再送回数の設定

[入力形式] **pppoe padi maxretry times**
no pppoe padi maxretry

[パラメータ] ◦ *times*.....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。

[デフォルト値] 5

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

8.18.6 PADIパケットの再送時間の設定

[入力形式] **pppoe padi restart time**
no pppoe padi restart

[パラメータ] ◦ *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。

[デフォルト値] 3000

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

8.18.7 PADRパケットの最大再送回数の設定

[入力形式] **pppoe padr maxretry times**
no pppoe padr maxretry

[パラメータ] ◦ *times*.....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。

[デフォルト値] 5

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

8.18.8 PADR パケットの再送時間の設定

- [入力形式] **pppoe padr restart time**
no pppoe padr restart
- [パラメータ] ○ *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。
- [デフォルト値] 3000

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.18.9 PPPoE セッションの切断タイマの設定

- [入力形式] **pppoe disconnect time time**
no pppoe disconnect time
- [パラメータ] ○ *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。
- [デフォルト値] off

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.18.10 TCP パケットの MSS の制限の有無とサイズの指定

- [入力形式] **pppoe tcp mss limit length**
pppoe tcp mss limit
- [パラメータ] ○ *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。
- [デフォルト値] auto

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

8.18.11 サービス名の指定

- [入力形式] **pppoe service-name name**
- [パラメータ] ○ *name* サービス名を表す文字列 (7bit US-ASCII、255 文字以内)
- [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。
- [デフォルト値] 指定なし

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

9. DHCP の設定

本機は DHCP¹ 機能として、DHCP サーバ機能、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 95, 98 や Windows NT 等で実装されており、これらと本機の DHCP サーバ機能、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 **dhcp scope unbind** コマンドで行います。IP アドレスのリース期間には時間指定と無期限の両方が可能であり、これは **dhcp scope** コマンドの **expire** 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 サーバへ転送します。リモートセグメントの DHCP サーバは **dhcp relay server** コマンドで設定します。DHCP サーバ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・リレーエージェント機能

9.1.1 DHCP の動作の設定

[入力形式] **dhcp service type**
no dhcp service [type]

[パラメータ] ○ *type*

- **server**DHCP サーバとして機能させる
- **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。

[デフォルト値] DHCP サービスは機能しない

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

1. Dynamic Host Configuration Protocol; RFC1541, RFC2131
URL 参照: <http://rfc.rtpro.yamaha.co.jp/rfc/rfc1541.txt> (rfc2131.txt)

9.1.2 RFC2131 対応動作の設定

[入力形式] **dhcp server rfc2131 compliant comp**
dhcp server rfc2131 compliant [except] *function* [*function..*]
no dhcp server rfc2131 compliant

- *comp*
 - on RFC2131 準拠
 - off RFC1541 準拠
- *except*..... 指定した機能以外が RFC2131 対応となるキーワード
- *function*
 - 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 サーバの動作を指定する。on の場合には RFC2131 準拠となる。off の場合には、RFC1541 準拠の動作となる。

また RFC1541 をベースとして RFC2131 記述の個別機能のみを対応させる場合には以下のパラメータで指定する。これらのパラメータはスペースで区切り複数指定できる。except キーワードを指示すると、指定したパラメータ以外の機能が RFC2131 対応となる。

- broadcast-nak 同じサブネット上のクライアントに対しては DHCPNAK はブロードキャストで送る。DHCPREQUEST をクライアントが INIT-REBOOT state で送られてきたものに対しては、giaddr 宛であれば Bbit を立てる。
- none-domain-null... 本ドメイン名の最後に NULL 文字を付加しない。RFC1541 ではドメイン名の最後に NULL 文字を付加するかどうかは明確ではなかったが、RFC2131 では禁止された。一方、Windows NT/2000 の DHCP サーバは 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。

[デフォルト値] on

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

9.1.3 DHCP スコープの定義

[入力形式] **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*]]

- [パラメータ]
- *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 10 進数)
 - 0x に続く 16 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 (空白で区切って複数指定可能)
 - *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*時間
 - 分 (1..21474836)
 - 時間: 分
 - infinity.....無期限リース

[説明] DHCP サーバとして割り当てる IP アドレスのスコープを設定する。
 除外 IP アドレスは複数指定できる。リース期間としては無期限を指定できるほか、DHCP クライアントから要求があった場合の許容最大リース期間を指定できる。

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

[デフォルト値] expire *time* = 72:00
 maxexpire *time* = 72:00

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

9.1.4 DHCP 予約アドレスの設定

[入力形式] **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

[パラメータ]

- *scope_num* スコープ番号 (1..65535)
- *ip_address* 予約する 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 *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 16 進数の列で先頭は *type* フィールド
 - *mac_address* xx:xx:xx:xx:xx:xx (xx は 16 進数) 予約 DHCP クライアントの MAC アドレス
- *ipcp* IPCP でリモート側に与えることを示す

[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。

[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 **dhcp delete scope** コマンドを実行した場合、関連する予約はすべて消去される。*ipcp* の指定は、同時に接続できる B チャンネルの数に限られる。また、*ipcp* で与えるアドレスは LAN 側のスコープから選択される。

コマンドの第 1 の書式を使う場合は、あらかじめ **dhcp server rfc2131 compliant on** あるいは *use-clientid* 機能を使用するよう設定されていないなければならない。また **dhcp server rfc2131 compliant off** あるいは *use-clientid* 機能が使用されないよう設定された時点で、コマンドの第 2 の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 の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 の書式による MAC アドレスでの予約は、クライアントの識別に DHCP パケットの *chaddr* フィールドを用いる。この形の予約機能は、RT の設定が **dhcp server rfc2131 compliant off** あるいは *use-clientid* 機能を使用しない設定になっているか、もしくは DHCP クライアントが DHCP パケット中に Client-Identifier オプションを付けてこない場合でないかと動作しない。

クライアントが Client-Identifier オプションを使う場合、コマンドの第 2 の書式での予約は、**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	<i>chaddr</i> (※ 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、16 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 16 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作用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、YAMAHA ルータ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。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

9.1.5 DHCP オプションの設定

[入力形式] **dhcp scope option scope_num option=value**
no dhcp scope option scope_num [option=value]

[パラメータ] ○ 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 16 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。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

9.1.6 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

[入力形式]	dhcp duplicate check <i>check1 check2</i> no dhcp duplicate check														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>check1</i>..... LAN 内を対象とするチェックの確認用待ち時間 <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わない 														
[説明]	DHCP サーバ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。														
[デフォルト値]	<i>check1</i> = 100 <i>check2</i> = 500														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

9.1.7 DHCP サーバの指定の設定

[入力形式]	dhcp relay server <i>host [host...]</i> no dhcp relay server [<i>host [host...]</i>]														
[パラメータ]	○ <i>host1..host4</i> DHCP サーバの IP アドレス														
[説明]	DHCP BOOTREQUEST パケットを中継するサーバを最大 4 つまで設定する。 サーバ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に中継するか、あるいは 1 つだけサーバを選択して中継するかは dhcp relay select コマンドの設定で決定される。														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

9.1.8 DHCP サーバの選択方法の設定

[入力形式]	dhcp relay select <i>type</i> no dhcp relay select [<i>type</i>]														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>type</i> <ul style="list-style-type: none"> • hash Hash 関数を利用して一つだけサーバを選択する • all..... すべてのサーバを選択する 														
[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 <i>chaddr</i> 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に対し複製中継される。														
[デフォルト値]	hash														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

9.1.9 DHCP BOOTREQUEST パケットの中継基準の設定

[入力形式] **dhcp relay threshold time**
no dhcp relay threshold [time]

[パラメータ] ◦ *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 サーバがあるにも関わらず遠隔地の DHCP サーバにパケットを中継してしまうのを避けることができる。

[デフォルト値] 0

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

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

[入力形式] **ip interface dhcp lease time time**
no ip interface dhcp lease time [time]

[パラメータ] ◦ *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 サーバからのリース期間を利用する。

[デフォルト値] リース期間を要求しない

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

9.2.2 IP アドレス取得要求の再送回数と間隔の設定

[入力形式] **ip interface dhcp retry retry interval**
no ip interface dhcp retry [retry interval]

[パラメータ] ◦ *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。

[デフォルト値] *retry* = infinity
interfal = 5

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

9.2.3 DHCP クライアント ID オプションの設定

[入力形式]	dhcp client client-identifier <i>interface</i> primary [type type] <i>id</i> dhcp client client-identifier <i>interface</i> secondary [type type] <i>id</i> dhcp client client-identifier pp <i>peer_num</i> [type type] <i>id</i> dhcp client client-identifier pool <i>pool_num</i> [type type] <i>id</i> no dhcp client client-identifier <i>interface</i> primary no dhcp client client-identifier <i>interface</i> secondary no dhcp client client-identifier pp <i>peer_num</i> no dhcp client client-identifier pool <i>pool_num</i>														
[デフォルト値]	<ul style="list-style-type: none"> ○ <i>interface</i>.....LAN インタフェース名 ○ <i>type</i>.....ID オプションの <i>type</i> フィールドの値を設定することを示すキーワード ○ <i>type</i>.....ID オプションの <i>type</i> フィールドの値 ○ <i>id</i> <ul style="list-style-type: none"> ● ASCII 文字列で表した ID ● 2 桁の 16 進数列で表した ID ○ <i>peer_num</i>..... 相手先情報番号 <ul style="list-style-type: none"> ● <i>anonymous</i>..... 匿名 ● <i>leased</i>..... 専用線 ○ <i>pool_num</i>.....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、<i>pool_num</i> 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 <i>type</i> フィールドと ID を設定する。														
[デフォルト値]	<i>type</i> = 0														
[適用モデル]	<table border="1" style="border-collapse: collapse; text-align: center;"> <tr> <td style="padding: 2px 10px;">RTX2000</td> <td style="padding: 2px 10px;">RTX1000</td> <td style="padding: 2px 10px;">RT300i</td> <td style="padding: 2px 10px;">RT140p</td> <td style="padding: 2px 10px;">RT140f</td> <td style="padding: 2px 10px;">RT140i</td> <td style="padding: 2px 10px;">RT140e</td> </tr> <tr> <td style="padding: 2px 10px;">RT105p</td> <td style="padding: 2px 10px;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

9.2.4 DHCP クライアントのホスト名の設定

[入力形式]	dhcp client hostname <i>interface</i> primary <i>host</i> dhcp client hostname <i>interface</i> secondary <i>host</i> dhcp client hostname pp <i>peer_num</i> <i>host</i> dhcp client hostname pool <i>pool_num</i> <i>host</i> no dhcp client hostname <i>interface</i> primary [<i>host</i>] no dhcp client hostname <i>interface</i> secondary [<i>host</i>] no dhcp client hostname pp <i>peer_num</i> [<i>host</i>] no dhcp client hostname pool <i>pool_num</i> [<i>host</i>]														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>interface</i>.....LAN インタフェース名 ○ <i>peer_num</i>..... 相手先情報番号 <ul style="list-style-type: none"> ● <i>anonymous</i>..... 匿名 ○ <i>pool_num</i>.....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、<i>pool_num</i> 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) ○ <i>host</i>.....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。														
[デフォルト値]	DHCP クライアントのホスト名は設定されていない														
[適用モデル]	<table border="1" style="border-collapse: collapse; text-align: center;"> <tr> <td style="padding: 2px 10px;">RTX2000</td> <td style="padding: 2px 10px;">RTX1000</td> <td style="padding: 2px 10px;">RT300i</td> <td style="padding: 2px 10px;">RT140p</td> <td style="padding: 2px 10px;">RT140f</td> <td style="padding: 2px 10px;">RT140i</td> <td style="padding: 2px 10px;">RT140e</td> </tr> <tr> <td style="padding: 2px 10px;">RT105p</td> <td style="padding: 2px 10px;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

9.2.5 DNS サーバアドレスを取得する LAN インタフェースの設定

[入力形式] **dns server dhcp interface**
no dns server dhcp

[パラメータ] ◦ *interface*.....LAN インタフェース名

[説明] DNS サーバ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 で名前解決を行うときに、指定した LAN インタフェースで DHCP サーバから取得した DNS サーバアドレスに対して問い合わせを行う。DHCP サーバから DNS サーバアドレスを取得できなかった場合は名前解決を行わない。
dns server コマンドで DNS サーバ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 インターフェースが DHCP クライアントとして動作していなければならない。

[デフォルト値] LAN インタフェースは設定されていない

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

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

[入力形式] **ip icmp echo-reply send send**
no ip icmp echo-reply send [send]

[パラメータ] ◦ *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。

[デフォルト値] on

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

10.1.2 ICMP Mask Reply を送信するか否かの設定

[入力形式] **ip icmp mask-reply send send**
no ip icmp mask-reply send [send]

[パラメータ] ◦ *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。

[デフォルト値] on

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

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

[入力形式] **ip icmp parameter-problem send send**
no ip icmp parameter-problem send [send]

[パラメータ] ◦ *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。

[デフォルト値] off

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

10.1.4 ICMP Redirect を送信するか否かの設定

[入力形式] **ip icmp redirect send send**
no ip icmp redirect send [send]

[パラメータ] ◦ *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。

[デフォルト値] on

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

10.1.5 ICMP Redirect 受信時の処理の設定

[入力形式] **ip icmp redirect receive action**
no ip icmp redirect receive [action]

[パラメータ] ◦ *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。

[デフォルト値] off

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

10.1.6 ICMP Time Exceeded を送信するか否かの設定

[入力形式] **ip icmp time-exceeded send send**
no ip icmp time-exceeded send [send]

[パラメータ] ◦ *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。

[デフォルト値] on

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

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

[入力形式] **ip icmp timestamp-reply send send**
no ip icmp timestamp-reply send [send]

[パラメータ] ◦ *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。

[デフォルト値] on

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

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

[入力形式]	ip icmp unreachable send send no ip icmp unreachable send [send]														
[パラメータ]	<ul style="list-style-type: none"> ○ send <ul style="list-style-type: none"> • 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 を送信するか否かを設定する。														
[デフォルト値]	on														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT140p</td> <td style="padding: 2px;">RT140f</td> <td style="padding: 2px;">RT140i</td> <td style="padding: 2px;">RT140e</td> </tr> <tr> <td style="padding: 2px;">RT105p</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

10.1.9 受信した ICMP のログを記録するか否かの設定

[入力形式]	ip icmp log log no ip icmp log [log]														
[パラメータ]	<ul style="list-style-type: none"> ○ log <ul style="list-style-type: none"> • 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。														
[デフォルト値]	off														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT140p</td> <td style="padding: 2px;">RT140f</td> <td style="padding: 2px;">RT140i</td> <td style="padding: 2px;">RT140e</td> </tr> <tr> <td style="padding: 2px;">RT105p</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

10.1.10 ステルス機能の設定

[入力形式]	ip stealth all ip stealth interface [interface...] no ip stealth [...]														
[パラメータ]	<ul style="list-style-type: none"> ○ all すべての論理インタフェースからのパケットに対してステルス動作を行う ○ 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う 														
[説明]	<p>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。</p> <p>自分がサポートしていないプロトコルや IPv6 ヘッダ、あるいはオープンしていない TCP/UDP ポートに対して指定されたインタフェースからパケットを受信した時に、通常であれば ICMP unreachable や TCP リセットを返送する。しかし、このコマンドを設定しておくそれを禁止することができ、ポートスキャナーなどによる攻撃を受けた時にルータの存在を隠すことができる。</p>														
[ノート]	<p>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。</p> <p>自分宛ではないパケットが原因で発生する ICMP はこのコマンドでは制御できない。それらを送信しないようにするには、ip icmp コマンドを用いる必要がある。</p>														
[デフォルト値]	ステルス動作を行わない														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT140p</td> <td style="padding: 2px;">RT140f</td> <td style="padding: 2px;">RT140i</td> <td style="padding: 2px;">RT140e</td> </tr> <tr> <td style="padding: 2px;">RT105p</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

110 10.ICMP の設定

10.2 IPv6 の設定

10.2.1 ICMP Echo Reply を送信するか否かの設定

[入力形式] **ipv6 icmp echo-reply send** *send*
 no ipv6 icmp echo-reply send [*send*]

[パラメータ] ◦ *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。

[デフォルト値] on

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

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

[入力形式] **ipv6 icmp parameter-problem send** *send*
 no ipv6 icmp parameter-problem send [*send*]

[パラメータ] ◦ *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。

[デフォルト値] off

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

10.2.3 ICMP Redirect を送信するか否かの設定

[入力形式] **ipv6 icmp redirect send** *send*
 no ipv6 icmp redirect send [*send*]

[パラメータ] ◦ *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。

[デフォルト値] on

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

10.2.4 ICMP Redirect 受信時の処理の設定

[入力形式] **ipv6 icmp redirect receive** *action*
 no ipv6 icmp redirect receive [*action*]

[パラメータ] ◦ *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。

[デフォルト値] off

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

10.2.5 ICMP Time Exceeded を送信するか否かの設定

[入力形式] **ipv6 icmp time-exceeded send send**
no ipv6 icmp time-exceeded send [send]

[パラメータ] ○ *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。

[デフォルト値] on

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

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

[入力形式] **ipv6 icmp unreachable send send**
no ipv6 icmp unreachable send [send]

[パラメータ] ○ *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。

[デフォルト値] on

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

10.2.7 受信した ICMP のログを記録するか否かの設定

[入力形式] **ipv6 icmp log log**
no ipv6 icmp log [log]

[パラメータ] ○ *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。

[デフォルト値] off

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

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

[入力形式] **ipv6 icmp packet-too-big send send**
no ipv6 icmp packet-too-big send [send]

[パラメータ] ○ *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。

[デフォルト値] on

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

10.2.9 ステルス機能の設定

[入力形式] **ipv6 stealth all**
 ipv6 stealth interface [interface...]
 no ipv6 stealth [...]

[パラメータ] ○ allすべての論理インタフェースからのパケットに対してステルス動作を行う
 ○ 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、**ip icmp** コマンドを用いる必要がある。

[デフォルト値] ステルス動作を行わない

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

11. フレームリレー関連の設定

BRI/PRI インタフェースを持つ機種ではアクセス回線としてフレームリレーに対応しています。

PPP によるダイヤルアップ接続と専用線接続、フレームリレー接続では同じ HDLC¹ フレームを使用して通信しますが、PPP とフレームリレーでは HDLC フレーム内のフォーマットが異なるため、フレームリレーで運用を開始する前にはカプセル化プロトコルを指定する必要があります。カプセル化の指定は **pp encapsulation** コマンドで設定します。

DLCI² はフレームリレーで相手先を指定するための識別子です。1 本の回線で複数の DLCI を利用することができ、回線を論理多重化してそれぞれが仮想的な専用線のようにネットワークを構築することができます。具体的な DLCI の値はフレームリレーネットワーク提供者との契約時に決まります。

DLCI をルータに設定する方法は、ルータによる自動取得と管理者による手動設定の 2 種類があります。手動設定は **fr dlcI** コマンドで行います。

自動取得の場合には PVC³ 状態確認手順の LMI⁴ により行われます。本機は JT-Q933 と ANSI の 2 種類の LMI をサポートしており、**fr lmi** コマンドを使用していずれかを指定します。手動設定の場合、DLCI は最大 96 個まで設定できます。自動取得の場合には、制限はありません。DLCI は **show dlcI** コマンドで確認することができます。

一般に、フレームリレーでのルーティングは 1 つの相手先情報番号に複数の相手先 (DLCI) が接続するために PP 側は numbered となります。相手の PP 側の IP アドレスと DLCI の対応を解決するプロトコルが InARP⁵ です。InARP を使用するかどうかは **fr inarp** コマンドで設定します。

本機の特徴として、直接 DLCI を指定してルーティングすることが可能です。この場合は PP 側の IP アドレス (**ip pp address** コマンド) を設定せず、PP 側 unnumbered のスタティックルーティングとなり InARP も使用されません。

YAMAHA リモートルータ同士であれば、unnumbered でダイナミックルーティングが可能です。

データ圧縮機能によってフレームリレー回線上での通信負荷を最大 2/5 程度まで軽減することが可能です。

本機能の実装は Frame Relay Forum の FRF.9 に基づいており、特に、FRF.9 のモード 1 に対応しています。データの圧縮と伸長アルゴリズムは Stac LZS を使用します。

このデータ圧縮機能を使用するかは **fr compression use** コマンドで設定します。

なお、このデータ圧縮機能が適用できる対地の最大数は、本機では 50 であり、これを超える数の対地に対して本機能を適用することはできません。

同じフレームリレー回線に PP インタフェースを複数バインドする場合、最も若い PP インタフェースが代表となります。

pp encapsulation fr の設定は、関係するすべてのインタフェースに対して設定する必要があります。一方、**fr lmi**、**fr inarp**、**fr congestion control**、そして、**fr pp dequeue type** の各コマンドは代表のインタフェースにのみ設定します。

データリンクの DLCI 値が **fr dlcI** コマンドで明示的に設定されている場合には、その設定のあるインタフェースにデータリンクが収容されます。その DLCI 値が複数のインタフェースで設定されている場合には、まず代表のインタフェースが優先され、その後の優先順位は番号の若い順となります。

データリンクの DLCI 値が、**fr dlcI** コマンドで明示的に設定されていない場合には、**fr dlcI auto** が設定されているインタフェースにデータリンクが収容されます。**fr dlcI auto** の設定されたインタフェースがない場合にはどのインタフェースにも収容されません。**fr dlcI auto** の設定されたインタフェースが複数ある場合は、まず代表のインタフェースが優先され、その後の優先順位は番号の若い順となります。

11.1 カプセル化の種類の設定

【入力形式】 **pp encapsulation type**
no pp encapsulation [type]

【パラメータ】 ◦ *type*

- **ppp** PPP でカプセル化する
- **fr** フレームリレーでカプセル化する

【説明】 選択されている相手のカプセル化の種類を設定する。

【ノート】 フレームリレーでは IPXWAN の設定は無効 (常に OFF)

【デフォルト値】 **ppp**

【適用モデル】	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

1. High level Data Link Control procedure
 2. Data Link Connection Identifier
 3. Permanent Virtual Circuit
 4. Local Management Interface
 5. Inverse Address Resolution Protocol; RFC1293

11.4 11. フレームリレー関連の設定

11.2 DLCI の設定

- [入力形式] **fr dlc** *dlci_num*
no fr dlc [*dlci_num*]
- [パラメータ] ○ *dlci_num*
- autoDLCI を自動取得する
 - DLCI 値 (16..991) を空白で区切って並べたもの (96 個以内)
- [説明] 選択されている相手で使用する DLCI を自動設定するか、または手動設定する。
auto に設定した場合は PVC 状態確認手順により DLCI を自動取得する。
- [ノート] `fr lmi off` に設定されていない場合、このコマンドで DLCI を手動設定した場合には、網から通知された DLCI の中で手動設定されているものだけが有効となる。
- [デフォルト値] auto
- [設定例] # fr dlc 16 17 18

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

11.3 PVC 状態確認手順の設定

- [入力形式] **fr lmi** *lmi*
no fr lmi [*lmi*]
- [パラメータ] ○ *lmi*
- q933TTC 標準 JT-Q933 付属資料 A に基づいて状態確認を行う
 - ansiANSI T1.617 AnnexD に基づいて状態確認を行う
 - offPVC 状態確認手順は行わない
- [説明] 選択されている相手に対するフレームリレーでの PVC 状態確認手順を設定する。
- [ノート] 網との契約で LMI が無い場合、`fr lmi off` に設定しておかなければ、回線ダウンとみなされるので注意。
- [デフォルト値] q933

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

11.4 InARP 使用の設定

- [入力形式] **fr inarp** *inarp*
no fr inarp [*inarp*]
- [パラメータ] ○ *inarp*
- 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、InARP (Inverse Address Resolution Protocol) を使用して、相手の IP アドレスを自動取得するかどうかを設定する。この設定が on の場合でも、自分の PP 側のローカル IP アドレスが設定されていない場合 (unnumbered) は InARP は使用しない。
また、自分の PP 側ローカル IP アドレスが設定されていれば、相手から InARP のリクエストが来た場合、この設定に関わらず常にレスポンスを返す。
- [ノート] **ip pp address** コマンドを参照
- [デフォルト値] on

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

11.5 フレームリレーダウン時にバックアップする相手先情報番号の設定

[入力形式]	fr backup dlci= <i>dlci_num</i> peer_num no fr backup dlci= <i>dlci_num</i> [<i>peer_num</i>]														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>dlci_num</i> <ul style="list-style-type: none"> • DLCI 値 (16..991) ○ <i>peer_num</i> バックアップする相手先情報番号 														
[説明]	指定した DLCI がダウンした場合にバックアップする相手先情報番号を設定する。														
[ノート]	同じ相手先情報番号に、専用線バックアップ (leased backup コマンド) とフレームリレーバックアップの両方を設定することはできない。														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

11.6 FR 圧縮機能の設定

[入力形式]	fr compression use dlci= <i>dlci_num</i> type no fr compression use dlci= <i>dlci_num</i> [<i>type</i>]														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>dlci_num</i> <ul style="list-style-type: none"> • DLCI 値 (16..991) • * (すべてのデータリンク) ○ <i>type</i> <ul style="list-style-type: none"> • stac Stac LZS 方式を用いてデータを圧縮する • cstac cstac 方式を用いてデータを圧縮する • none データを圧縮しない 														
[説明]	FR のデータ圧縮機能の方式を設定する。 <i>dlci_num</i> パラメータには、対象となるリンクに付された自分側の DLCI 値を指定する。なお、このコマンドを設定している場合でも、交渉に失敗した場合には圧縮機能は働かない。														
[デフォルト値]	<i>type</i> = none														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

11.7 DLCI ごとのパラメータの設定

[入力形式]	fr cir dlci= <i>dlci_num</i> cir [slowstart-idle= <i>idle</i>] [bc= <i>bc_size</i>] [be= <i>be_size</i>] [s= <i>step_count</i>] no fr cir dlci= <i>dlci_num</i> [<i>cir</i> []]														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>dlci_num</i> DLCI 値 (16..991) ○ <i>cir</i> CIR 値 (bit/s 単位) ○ <i>idle</i> スロースタート状態に戻るまでのアイドル時間 <ul style="list-style-type: none"> • 秒数 (1..21474836) • 0 スロースタート動作を行わない ○ <i>bc_size</i> 認定バーストサイズ (ビット) ○ <i>be_size</i> 超過バーストサイズ (ビット) ○ <i>step_count</i> ステップカウント 														
[説明]	DLCI 毎のパラメータを設定する。PP 毎に設定し、その PP に所属する DLCI 値に対して設定が有効となる。														
[デフォルト値]	<i>idle</i> = 20 <i>bc=be</i> = 7000 <i>s=cir/bc_size/be_size</i> から計算される値														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

116 11. フレームリレー関連の設定

11.8 輻輳制御をするか否かの設定

[入力形式]	fr congestion control control no fr congestion control [control]														
[パラメータ]	◦ control <ul style="list-style-type: none">• on.....輻輳制御を行う• off.....輻輳制御を行わない														
[説明]	フレームリレーの輻輳制御を行うかどうかを設定する。CIR が設定されていない DLCI に対しては、回線速度の半分の CIR が設定されているものとして動作する。														
[ノート]	輻輳制御は、BECN および CLLM の通知に基づいて行う。暗黙的輻輳検出および FECN による明示的輻輳通知は扱わない。														
[デフォルト値]	off														
[適用モデル]	<table border="1"><tr><td>RTX2000</td><td>RTX1000</td><td>RT300i</td><td>RT140p</td><td>RT140f</td><td>RT140i</td><td>RT140e</td></tr><tr><td>RT105p</td><td>RT105i</td><td>RT105e</td><td></td><td></td><td></td><td></td></tr></table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

11.9 回線に対する送信順序方式の設定

[入力形式]	fr pp dequeue type type no fr pp dequeue type [type]														
[パラメータ]	◦ type <ul style="list-style-type: none">• serial.....順次サーチ方式• round-robin.....ラウンドロビン方式														
[説明]	同じフレームリレー回線に複数の PP インタフェースがバインドされている場合の送信順序方式を設定する。serial の場合には、同じフレームリレー回線にバインドされた PP インタフェースに対して順位を与え、順位の高い PP インタフェースから優先してパケットを送信する。round-robin の場合には、優先順位を設定せずすべての PP インタフェースから均等にパケットを送信する。														
[ノート]	相手先情報番号の若い PP インタフェースがより高い順位を持つものと定義する。														
[デフォルト値]	round-robin														
[適用モデル]	<table border="1"><tr><td>RTX2000</td><td>RTX1000</td><td>RT300i</td><td>RT140p</td><td>RT140f</td><td>RT140i</td><td>RT140e</td></tr><tr><td>RT105p</td><td>RT105i</td><td>RT105e</td><td></td><td></td><td></td><td></td></tr></table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

11.10 指定パケットに DE ビットを立てるか否かの設定

[入力形式]	fr de protocol filter dlcid=dlci_num filter_num_list no fr de protocol filter dlcid=dlci_num [filter_num_list]														
[パラメータ]	◦ protocol <ul style="list-style-type: none">• ip.....IP パケット• ipx.....IPX パケット• bridge.....ブリッジするパケット ◦ filter.....固定のキーワード														
	◦ dlci_num <ul style="list-style-type: none">• DLCI 値 (16..991)• * (すべてのデータリンク)														
	◦ filter_num_list.....静的フィルタ番号 (1..100) の並び														
[説明]	指定パケットに DE ビットを立てるか否かを設定する。 filter_num_list で指定したフィルタを順番にパケットに対して適用し、マッチしたところでそのフィルタが pass、pass-log、pass-nolog、restrict、restrict-log、restrict-nolog のいずれかであれば DE ビットを立てる。reject、reject-log または reject-nolog である場合は DE ビットを立てない。フィルタ列の最後までマッチしなかった場合には DE ビットを立てない。														
[デフォルト値]	DE ビットは立てない														
[適用モデル]	<table border="1"><tr><td>RTX2000</td><td>RTX1000</td><td>RT300i</td><td>RT140p</td><td>RT140f</td><td>RT140i</td><td>RT140e</td></tr><tr><td>RT105p</td><td>RT105i</td><td>RT105e</td><td></td><td></td><td></td><td></td></tr></table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

12. PRI 関連の設定

RT300i は、オプションの PRI 拡張モジュールを装着することにより一次群速度インタフェース (PRI:Primary Rate Interface) に対応します。多重化非対応の PRI 拡張モジュール (製品番号: YBA-1PRI-N) は、192kbit/s ~ 1.5Mbit/s のスーパーリレー FR や DA1500 などの高速デジタル専用線に最適です。多重化対応の PRI 拡張モジュール (製品番号: YBA-1PRI-M) を利用すると、それに加えて最大 24 対地までの HSD の多重アクセスサービスや INS ネット 1500 を利用することができます。

RT105p は標準で一次群速度インタフェースに対応しており、192kbit/s ~ 1.5Mbit/s のスーパーリレー FR や DA1500 などの高速デジタル専用線に最適です。HSD の多重アクセスサービスや INS ネット 1500 には対応しません。

RT140p は標準で RT105p 同等の機能を持っており、オプションの多重化ソフトウェア (YMS15P) を追加することにより、最大 24 対地までの HSD の多重アクセスサービスや INS ネット 1500 を利用することができます。

機種によってはサービスを利用するために、オプションモジュール、ソフトウェアを購入していただく必要があります。また、DSU はどの機種にも内蔵しておりませんので別途用意してください。

機種	192kbit/s ~ 1.5Mbit/s 専用線 (A)	192kbit/s ~ 1.5Mbit/s 専用線多重 (B)	回線交換 (C)
RT300i	YBA-1PRI-N YBA-1PRI-M	YBA-1PRI-M	YBA-1PRI-M
RT140p	標準	YMS15P	YMS15P
RT105p	標準	未対応	未対応

(A): HSD, DA1500, スーパーリレー FR

(B): HSD の多重アクセスサービス

(C): INS ネット 1500

YBA-1PRI-N: 多重化非対応 PRI 拡張モジュール

YBA-1PRI-M: 多重化、回線交換対応 PRI 拡張モジュール

YMS15P: 多重化、回線交換対応オプションソフトウェア

専用線を利用するためには、PRI ネットワーク提供者との契約で指定されたタイムスロットに関する値を **pri leased channel** コマンドで設定します。PRI を経由してパケットをやり取りするためには、**pp bind** コマンドで相手先情報番号 (pp) と PRI インタフェース名、情報チャンネル番号 (pri1/1) を関連づけます。専用線に関する設定は次のようになります。

```
pri leased channel 1/1 1 24
pp select 1
pp bind pri1/1
pp enable 1
```

また、回線交換を利用するためには、通信回線種別を line type コマンドで isdn に設定します。PRI を経由してパケットをやり取りするためには、pp bind コマンドで相手先情報番号 (pp) と PRI インタフェース名 (pri1) を関連づけます。選択されている相手の発着信用の ISDN 番号を **isdn remote address** コマンドで設定します。回線交換に関する設定は次のようになります。

```
line type pri1 isdn
pp select 1
pp bind pri1
isdn remote address call ISDN 番号
pp enable 1
```

これにルーティングに関する設定を追加すると PRI を経由してパケットをやり取りすることができます。

実際に、別途用意していただいた DSU とルータ間を付属のコネクタケーブルで繋いで、**show status pri1** コマンドで表示されるレイヤ 1 情報、回線交換ではレイヤ 2 まで、物理的配線が適切であるか確認することができます。

専用線に対しては、接続環境が適切であるかどうか確認するためのループバック試験を行うことができます。ループバック試験は、指定したデータを指定したループバックポイントまたは対抗ルータで折り返して、送信データと折り返しデータを比較して正常性の検証を行います。ループバックには、検証を行う Active 側と単に受け取ったデータを折り返す Passive 側があり、ルータはどちらか一方で動作します。Active 側にはハードウェアの正常性を確認するためのループバック A と回線上にデータを流して、対向ルータからの折り返しデータを比較検証するタイムスロットループバックがあります。Passive 側のループバックポイントは機種により若干異なります。ハードウェアの制限により、RT105p ではタイムスロットポイントでの折り返しは出来ず、他の機種のタイムスロットポイントで折り返したデータも受けることは出来ませんので注意が必要です。

118 12.PRI 関連の設定

ループバックは、コンソールコマンドから実行します。結果は Active 側のコンソールにだけ表示します。ループバック試験を行う前に、通常の通信を **pp disable** コマンドで停止させてから行ってください。Active 側のタイムスロットループバックでは、相手側のルータは **pri loopback passive** コマンドで待ち受け状態にしておく必要があります。ループバック A はコネクタケーブルを抜いた状態でないと実行できません。

12.1 PRI 回線の種類の設定

[入力形式]	line type interface line no line type interface line														
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>interface</i>PRI インタフェース名 ◦ <i>line</i> <ul style="list-style-type: none"> • <i>isdn ,isdn-ntt</i>ISDN 回線交換 • <i>leased</i>デジタル専用線 														
[説明]	PRI 回線の種類を指定する。設定の変更は、再起動か、あるいは該当インタフェースに対する interface reset コマンドの発行により反映される。														
[デフォルト値]	leased														
[適用モデル]	<table border="1" style="border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

12.2 情報チャンネルとタイムスロットの設定

[入力形式]	pri leased channel pri/info timeslot_bead timeslot_num no pri leased channel pri/info [timeslot_bead timeslot_num]																
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>pri</i>PRI インタフェース名 ◦ <i>info</i>情報チャンネル番号 (1..24) ◦ <i>timeslot_bead</i>先頭タイムスロット番号 (1..24) ◦ <i>timeslot_num</i>タイムスロット数 (1..24) <p style="margin-left: 20px;">以下の二ーモニックが使用可能</p> <table border="1" style="border-collapse: collapse; margin-left: 20px; text-align: center;"> <thead> <tr> <th>二ーモニック速度 (bit/s)</th> <th>タイムスロット数</th> </tr> </thead> <tbody> <tr><td>192k</td><td>3</td></tr> <tr><td>256k</td><td>4</td></tr> <tr><td>384k</td><td>6</td></tr> <tr><td>512k</td><td>8</td></tr> <tr><td>768k</td><td>12</td></tr> <tr><td>1024k</td><td>16</td></tr> <tr><td>1536k</td><td>24</td></tr> </tbody> </table>	二ーモニック速度 (bit/s)	タイムスロット数	192k	3	256k	4	384k	6	512k	8	768k	12	1024k	16	1536k	24
二ーモニック速度 (bit/s)	タイムスロット数																
192k	3																
256k	4																
384k	6																
512k	8																
768k	12																
1024k	16																
1536k	24																
[説明]	指定した PRI 回線内の情報チャンネルを、先頭タイムスロット番号とタイムスロット数 (通信速度) で設定する。																
[ノート]	設定変更時には再起動か、対象の PRI インタフェースに対する interface reset コマンドが必要である。RT300iの多重化非対応の PRI 拡張モジュール (YBA-1PRI-N)、RT105p、RT140p(YMS15Pなし) では、2 つ以上の情報チャンネルは設定できない。																
[適用モデル]	<table border="1" style="border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e						
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e											
RT105p	RT105i	RT105e															

12.3 PP で使用するインタフェースの設定

- 【入力形式】 **pp bind** *interface/pri_num* [*interface/info*]
no pp bind [*interface/info*]
- 【パラメータ】
- *interface* PRI インタフェース名
 - *pri_num* インタフェース番号
 - *info* 情報チャンネル番号
- 【説明】 選択されている相手先に対して実際に使用するインタフェースを設定する。
- 【ノート】 PRI 回線を専用線として使用する場合、**pri leased channel** コマンドで設定した情報チャンネル番号を、インタフェース名に付加する必要がある。
 例えば、**pri leased channel 1/1 1 24** の場合は、**pp bind pri1/1** となる。
- 【デフォルト値】 どのインタフェースともバインドされていない

【適用モデル】

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

13. IPsec の設定

本機は、暗号化により IP 通信に対するセキュリティを保証する IPsec 機能を実装しています。IPsec では、鍵交換プロトコル IKE (Internet Key Exchange) を使用します。必要な鍵は IKE により自動的に生成されますが、鍵の種となる事前共有鍵は **ipsec ike pre-shared-key** コマンドで事前に登録しておく必要があります。この鍵はセキュリティ・ゲートウェイごとに設定できます。また、鍵交換の要求に応じるかどうかは、**ipsec ike remote address** コマンドで設定します。

鍵や鍵の寿命、暗号や認証のアルゴリズムなどを登録した管理情報は、SA (Security Association) で管理します。SA を区別する ID は自動的に付与されます。SA の ID や状態は **show ipsec sa** コマンドで確認することができます。SA には、鍵の寿命に合わせた寿命があります。SA の属性のうちユーザが指定可能なパラメータをポリシーと呼びます。またその番号はポリシー ID と呼び、**ipsec sa policy** コマンドで定義し、**ipsec ike duration ipsec-sa**、**ipsec ike duration isakmp-sa** コマンドで寿命を設定します。

SA の削除は **ipsec sa delete** コマンドで、SA の初期化は **ipsec refresh sa** コマンドで行います。**ipsec auto refresh** コマンドにより、SA を自動更新させることも可能です。

IPsec による通信には、大きく分けてトンネルモードとトランスポートモードの 2 種類があります。

トンネルモードは IPsec による VPN (Virtual Private Network) を利用するためのモードです。ルータがセキュリティ・ゲートウェイとなり、LAN 上に流れる IP パケットデータを暗号化して対向のセキュリティ・ゲートウェイとの間でやりとりします。ルータが IPsec に必要な処理をすべて行うので、LAN 上の始点や終点となるホストには特別な設定を必要としません。

トンネルモードを用いる場合は、トンネルインタフェースという仮想的なインタフェースを定義し、処理すべき IP パケットがトンネルインタフェースに流れるように経路を設定します。個々のトンネルインタフェースはトンネルインタフェース番号で管理されます。設定のためにトンネル番号を切替えるには **tunnel select** コマンドを使用します。トンネルインタフェースを使用するか使用しないかは、それぞれ **tunnel enable**、**tunnel disable** コマンドを使用します。

相手先情報番号による設定		トンネルインタフェース番号による設定
pp enable	⇔	tunnel enable
pp disable		tunnel disable
pp select		tunnel select

トランスポートモードは特殊なモードであり、ルータ自身が始点または終点になる通信に対してセキュリティを保証するモードです。ルータからリモートのルータへ telnet で入るなどの特殊な場合に利用できます。トランスポートモードを使用するには **ipsec transport** コマンドで定義を行い、使用をやめるには **no ipsec transport** コマンドで定義を削除します。

トンネルモードとトランスポートモードは併用が可能ですが、それぞれを二重に適用することはできません。

IPsec による通信では、セキュリティ・ゲートウェイとなる本機のプログラムのリビジョンに注意してください。これらはリビジョンにより以下のように区別されます。IPsec リリース 2 と IPsec リリース 3 は相互接続性がありますが、後者の設定を前者に適合させる必要があります。

リビジョン系列	IPsec リリース 1	IPsec リリース 2	IPsec リリース 3
3.00	3.00.09 ~ 3.00.11	—	—
3.01	3.01.07	3.01.11 ~	
4.02	—	4.00.02 ~ 4.00.14	4.02.04 ~
6.00	—	—	6.00.01 ~

セキュリティ・ゲートウェイの識別子とトンネルインタフェース番号はモデルにより異なり、以下の表のようになります。

モデル	セキュリティ・ゲートウェイの識別子	トンネルインタフェース番号
RTX2000 + YBB-VPN-A	1 - 500	1 - 500
RTX1000	1 - 30	1 - 30
RT300i + YBA-VPN	1 - 500	1 - 500
RT300i	1 - 100	1 - 100
RT140p	1 - 20	1 - 20
RT140f	1 - 20	1 - 20
RT140i	1 - 20	1 - 20
RT140e	1 - 20	1 - 20
RT105p	1 - 20	1 - 20
RT105i	1 - 20	1 - 20
RT105e	1 - 30	1 - 30

13.1 事前共有鍵の登録

- [入力形式] **ipsec ike pre-shared-key gateway_id key**
ipsec ike pre-shared-key gateway_id text text
no ipsec ike pre-shared-key gateway_id [...]
- [パラメータ] ◦ gateway_id..... セキュリティ・ゲートウェイの識別子
 ◦ key 鍵となる 0x ではじまる 16 進数列 (最大 32 バイト)
 ◦ text ASCII 文字列で表した鍵 (最大 32 文字)
- [説明] 鍵交換に必要な事前共有鍵を登録する。設定されていない場合には、鍵交換は行われない。
 鍵交換を行う相手ルータには同じ事前共有鍵が設定されている必要がある。
- [デフォルト値] 事前共有鍵は設定されていない
- [設定例] ipsec ike pre-shared-key 1 text himitsu
 ipsec ike pre-shared-key 8 0xCDEEEDCOCD EDCD

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

13.2 相手側セキュリティ・ゲートウェイの IP アドレスの設定

- [入力形式] **ipsec ike remote address gateway_id ip_address**
no ipsec ike remote address gateway_id [ip_address]
- [パラメータ] ◦ gateway_id..... セキュリティ・ゲートウェイの識別子
 ◦ ip_address
 • 相手側セキュリティ・ゲートウェイの IP アドレス
 • any..... 自動選択
- [説明] 相手側セキュリティ・ゲートウェイの IP アドレスを設定する。相手側セキュリティ・ゲートウェイ 1 つに対して
 1 つ設定可能である。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

13.3 相手側のセキュリティ・ゲートウェイの名前の設定

- [入力形式] **ipsec ike remote name gateway name**
no ipsec ike remote name gateway [name]
- [パラメータ] ◦ gateway セキュリティ・ゲートウェイの識別子
 ◦ name 名前 (最大 32 文字)
- [説明] 相手側のセキュリティ・ゲートウェイの名前を設定する。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

13.4 自分側セキュリティ・ゲートウェイの IP アドレスの設定

[入力形式] **ipsec ike local address gateway_id ip_address**
ipsec ike local address gateway_id vrrp interface vrid
no ipsec ike local address gateway_id [ip_address]

[パラメータ] ◦ gateway_idセキュリティ・ゲートウェイの識別子
 ◦ ip_address
 • 自分側セキュリティ・ゲートウェイの IP アドレス
 • any.....自動選択
 ◦ interfaceLAN インタフェース名
 ◦ vrid.....VRRP グループ ID (1..255)

[説明] 自分側セキュリティ・ゲートウェイの IP アドレスを設定する。
 vrrp タイプの指定方式では、VRRP マスターとして動作している場合のみ、指定した LAN インタフェース / VRRP グループ ID の仮想 IP アドレスを自分側 セキュリティ・ゲートウェイアドレスとして利用する。VRRP マスターでない場合には鍵交換は行わない。

[ノート] 本コマンドが設定されていない場合には、相手側のセキュリティ・ゲートウェイに近いインタフェースの IP アドレスを用いて IKE を起動する。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

13.5 自分側のセキュリティ・ゲートウェイの名前の設定

[入力形式] **ipsec ike local name gateway_id name [type]**
no ipsec ike local name gateway_id [name]

[パラメータ] ◦ gateway_idセキュリティ・ゲートウェイの識別子
 ◦ name名前 (最大 32 文字)
 ◦ typeID の種類
 • fqdn.....ID_FQDN
 • use-fqdnID_USER_FQDN
 • key-id.....ID_KEY_ID

[説明] 自分側のセキュリティゲートウェイの名前と ID の種類を設定する。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

13.6 鍵交換の再送回数と間隔の設定

[入力形式] **ipsec ike retry count interval**
no ipsec ike retry [count interval]

[パラメータ] ◦ count再送回数 (1..50)
 ◦ interval再送間隔の秒数 (1..100)

[説明] 鍵交換が失敗した場合に鍵交換を繰り返す回数とその時間間隔を設定する。

[デフォルト値] count = 10
 interval = 5

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

13.7 IKE が用いる暗号アルゴリズムの設定

[入力形式]	ipsec ike encryption gateway_id algorithm no ipsec ike encryption gateway_id [algorithm]														
[パラメータ]	<ul style="list-style-type: none"> ○ gateway_id セキュリティ・ゲートウェイの識別子 ○ algorithm 暗号アルゴリズム <ul style="list-style-type: none"> • 3des-cbc 3DES-CBC • des-cbc DES-CBC • aes-cbc AES-CBC 														
[説明]	IKE が用いる暗号アルゴリズムを設定する。														
[ノート]	IKE で始動側として働く場合には、このコマンドで設定されたアルゴリズムを提案する。応答側として働く場合はこのコマンドの設定に関係なく、3DES-CBC と DES-CBC、AES-CBC を用いることができる。														
[デフォルト値]	des-cbc														
[設定例]	# ipsec ike encryption 1 aes-cbc														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

13.8 IKE が用いるグループの設定

[入力形式]	ipsec ike group gateway_id group [group] no ipsec ike group gateway_id [group [group]]														
[パラメータ]	<ul style="list-style-type: none"> ○ gateway_id セキュリティ・ゲートウェイの識別子 ○ group グループ識別子 <ul style="list-style-type: none"> • modp768 • modp1024 														
[説明]	IKE で用いるグループを設定する。														
[ノート]	IKE で始動側として働く場合には、このコマンドで設定されたグループを提案する。応答側として働く場合には、このコマンドの設定に関係なく、MODP768 と MODP1024 を用いることができる。2 種類のグループを設定した場合には、1 つ目がフェーズ 1 で、2 つ目がフェーズ 2 で提案される。グループを 1 種類しか設定しない場合は、フェーズ 1 とフェーズ 2 の両方で、設定したグループが提案される。														
[デフォルト値]	modp768														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

13.9 IKE が用いるハッシュアルゴリズムの設定

[入力形式]	ipsec ike hash gateway_id algorithm no ipsec ike hash gateway_id [algorithm]														
[パラメータ]	<ul style="list-style-type: none"> ○ gateway_id セキュリティ・ゲートウェイの識別子 ○ algorithm ハッシュアルゴリズム <ul style="list-style-type: none"> • md5 MD5 • sha SHA-1 														
[説明]	IKE が用いるハッシュアルゴリズムを設定する。														
[ノート]	IKE で始動側として働く場合には、このコマンドで設定されたアルゴリズムを提案する。応答側として働く場合はこのコマンドの設定に関係なく、MD5 と SHA-1 を用いることができる。														
[デフォルト値]	md5														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

124 13.IPsec の設定

13.10 自分側の ID の設定

[入力形式]	ipsec ike local id gateway_id ip_address[/mask] no ipsec ike local id gateway_id [ip_address[/mask]]														
[パラメータ]	○ gateway_id セキュリティ・ゲートウェイの識別子 ○ ip_address IP アドレス ○ mask ネットマスク														
[説明]	IKEのフェーズ2 で用いる自分側の ID を設定する。														
[ノート]	このコマンドが設定されていない場合には、ID を送信しない。mask パラメータを省略した場合は、タイプ 1 の ID が送信される。また、mask パラメータを指定した場合は、タイプ 4 の ID が送信される。														
[適用モデル]	<table border="1"><tr><td>RTX2000</td><td>RTX1000</td><td>RT300i</td><td>RT140p</td><td>RT140f</td><td>RT140i</td><td>RT140e</td></tr><tr><td>RT105p</td><td>RT105i</td><td>RT105e</td><td></td><td></td><td></td><td></td></tr></table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

13.11 IKE のログの種類の設定

[入力形式]	ipsec ike log gateway_id type [type] no ipsec ike log gateway_id [type]														
[パラメータ]	○ gateway_id セキュリティ・ゲートウェイの識別子 ○ type 出力するログの種類 <ul style="list-style-type: none">• message-info IKE メッセージの内容• payload-info ペイロードの処理内容• key-info 鍵計算の処理内容														
[説明]	出力するログの種類を設定する。ログはすべて、debug レベルの SYSLOG で出力される。														
[ノート]	このコマンドが設定されていない場合には、最小限のログしか出力しない。複数の type パラメータを設定することもできる。														
[適用モデル]	<table border="1"><tr><td>RTX2000</td><td>RTX1000</td><td>RT300i</td><td>RT140p</td><td>RT140f</td><td>RT140i</td><td>RT140e</td></tr><tr><td>RT105p</td><td>RT105i</td><td>RT105e</td><td></td><td></td><td></td><td></td></tr></table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

13.12 IKE ペイロードのタイプの設定

[入力形式]	ipsec ike payload type gateway_id type no ipsec ike payload type gateway_id [type]														
[パラメータ]	○ gateway_id セキュリティ・ゲートウェイの識別子 ○ type ペイロードのタイプ <ul style="list-style-type: none">• 1 IPsec リリース 2 以前• 2 IPsec リリース 3														
[説明]	IKE ペイロードのタイプを設定する。YAMAHA リモートルータの古いリビジョンと接続する場合には、タイプを 1 に設定する必要がある。														
[デフォルト値]	2														
[適用モデル]	<table border="1"><tr><td>RTX2000</td><td>RTX1000</td><td>RT300i</td><td>RT140p</td><td>RT140f</td><td>RT140i</td><td>RT140e</td></tr><tr><td>RT105p</td><td>RT105i</td><td>RT105e</td><td></td><td></td><td></td><td></td></tr></table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

13.13 PFS を用いるか否かの設定

[入力形式]	ipsec ike pfs gateway_id pfs no ipsec ike pfs gateway_id [pfs]														
[パラメータ]	<ul style="list-style-type: none"> ◦ gateway_id..... セキュリティ・ゲートウェイの識別子 ◦ pfs <ul style="list-style-type: none"> • on..... 用いる • off..... 用いない 														
[説明]	IKE で PFS(Perfect Forward Secrecy) を用いるか否かを設定する。														
[ノート]	相手側のセキュリティ・ゲートウェイと同じように設定する必要がある。														
[デフォルト値]	off														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

13.14 相手側の ID の設定

[入力形式]	ipsec ike remote id gateway_id ip_address[/mask] no ipsec ike remote id gateway_id [ip_address/mask]														
[パラメータ]	<ul style="list-style-type: none"> ◦ gateway_id..... セキュリティ・ゲートウェイの識別子 ◦ ip_address..... IP アドレス ◦ mask..... ネットマスク 														
[説明]	IKE のフェーズ 2 で用いる相手側の ID を設定する。														
[ノート]	このコマンドが設定されていない場合には ID を送信しない。 mask パラメータを省略した場合は、タイプ 1 の ID が送信される。また、mask パラメータを指定した場合は、タイプ 4 の ID が送信される。														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

13.15 IKE の情報ペイロードを送信するか否かの設定

[入力形式]	ipsec ike send info gateway_id info no ipsec ike send info gateway_id [info]														
[パラメータ]	<ul style="list-style-type: none"> ◦ gateway_id..... セキュリティ・ゲートウェイの識別子 ◦ info <ul style="list-style-type: none"> • on..... 送信する • off..... 送信しない 														
[説明]	IKE の情報ペイロードを送信するか否かを設定する。受信に関しては、この設定に関わらず、すべての情報ペイロードを解釈する。														
[ノート]	このコマンドは、接続性の検証などの特別な目的で使用される。定常の運用時は on に設定する必要がある。														
[デフォルト値]	on														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

13.16 IKE キープアライブ機能の設定

[入力形式] **ipsec ike keepalive use** *gateway_id switch [type [ip_address][internal][count]]*
no ipsec ike keepalive use [*gateway_id switch [type [ip_address][internal][count]]*]

[パラメータ] ◦ *gateway_id* セキュリティ・ゲートウェイの識別子
 ◦ *switch*
 • *on* キープアライブする
 • *off* キープアライブしない
 • *auto* 対向のルータからキープアライブを受信したときに限って送信する
 ◦ *type* キープアライブの方法
 • *heartbeat* IKE heartbeat (従来の方法)
 • *icmp-echo* ping
 ◦ *ip_address* pingを送信する宛先の IP アドレス (IPv4/IPv6) (このパラメータは *type* として *icmp-echo* を指定したときのみ設定できる)
 ◦ *internal* キープアライブパケットの送信間隔
 ◦ *count* キープアライブパケットが届かないときに障害とみなすまでの試行回数

[説明] IKE キープアライブの動作を設定する。
 このコマンドの設定は、双方のルータで一致させる必要がある。

[デフォルト値] *switch* = *auto*
 type = *heartbeat*
 internal = 10
 count = 6

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

13.17 IKE キープアライブに関する SYSLOG を出力するか否かの設定

[入力形式] **ipsec ike keepalive log** *gateway_id log*
no ipsec ike keepalive log *gateway_id [log]*

[パラメータ] ◦ *gateway_id* セキュリティ・ゲートウェイの識別子
 ◦ *log*
 • *on* 出力する
 • *off* 出力しない

[説明] IKE キープアライブに関する SYSLOG を出力するか否かを設定する。この SYSLOG は DEBEG レベルの出力である。

[デフォルト値] *on*

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

13.18 ESP を UDP でカプセル化して送受信するか否かの設定

[入力形式] **ipsec ike esp-encapsulation** *gateway_id encap*

[パラメータ] ◦ *gateway_id* セキュリティ・ゲートウェイの識別子
 ◦ *encap*
 • *on* ESP を UDP でカプセル化して送信する
 • *off* ESP を UDP でカプセル化しないで送信する

[説明] NAT などの影響で ESP が通過できない環境で IPsec の通信を確立するために、ESP を UDP でカプセル化して送受信できるようにする。このコマンドの設定は双方のルータで一致させる必要がある。

[デフォルト値] *off*

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

13.19 IKE の鍵交換に失敗したときに鍵交換を休止せずに継続するか否かの設定

[入力形式]	ipsec ike always-on gateway_id sw						
[パラメータ]	<ul style="list-style-type: none"> ○ gateway_id..... セキュリティ・ゲートウェイの識別子 ○ sw <ul style="list-style-type: none"> • on 鍵交換を継続する • off 鍵交換を休止する 						
[説明]	IKE の鍵交換に失敗したときに鍵交換を休止せずに継続できるようにする。IKE キープアライブを用いるときには、このコマンドを設定しなくても、常に鍵交換を継続する。						
[デフォルト値]	off						
[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

13.20 SA 関連の設定

再起動されるとすべての SA がクリアされることに注意しなくてはならない。

13.20.1 SA のポリシーの定義

[入力形式]	ipsec sa policy policy_id gateway_id ah ah_algorithm ipsec sa policy policy_id gateway_id esp esp_algorithm [ah_algorithm] no ipsec sa policy policy_id [gateway_id]						
[パラメータ]	<ul style="list-style-type: none"> ○ policy_id ポリシー ID (1..255) ○ gateway_id..... セキュリティ・ゲートウェイの識別子 ○ ah 認証ヘッダ (Authentication Header) を示すキーワード ○ esp..... 暗号ペイロード (Encapsulating Security Payload) を示すキーワード ○ ah_algorithm <ul style="list-style-type: none"> • md5-hmac..... HMAC-MD5 • sha-hmac HMAC-SHA ○ esp_algorithm <ul style="list-style-type: none"> • 3des-cbc 3DES-CBC • des-cbc DES-CBC • aes-cbc AES-CBC 						
[説明]	SA のポリシーを定義する。この定義はトンネルモードおよびトランスポートモードの設定に必要である。この定義は複数のトンネルモードおよびトランスポートモードで使用できる。						
[設定例]	# ipsec sa policy 101 1 esp aes-cbc sha-hmac						
[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

13.20.2 SA の寿命の設定

[入力形式]	ipsec ike duration sa gateway_id second [kbytes] no ipsec ike duration sa gateway_id [second [kbytes]]						
[パラメータ]	<ul style="list-style-type: none"> ○ sa <ul style="list-style-type: none"> • ipsec-sa IPsec SA • isakmp-sa ISAKMP SA ○ gateway_id..... セキュリティ・ゲートウェイの識別子 ○ second 秒数 (300..691200) ○ kbytes キロ単位のバイト数 (100..100000) 						
[説明]	IKE で提案する IPsec SA または ISAKMP SA の寿命を設定する。 kbytes パラメータを指定した場合には、second パラメータで指定した時間を経過するか指定したバイト数のデータが処理された後に SA は消滅する。						
[デフォルト値]	28800 秒						
[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

13.20.3 SA の削除

[入力形式] **ipsec sa delete id**

[パラメータ] ◦ *id*
 • SA の ID
 • all..... すべての SA

[説明] 指定した SA を削除する。
 SA の ID は自動的に付与され、**show ipsec sa** コマンドで確認することができる。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

13.20.4 SA の手動更新

[入力形式] **ipsec refresh sa**

[パラメータ] なし

[説明] SA を手動で更新する。

[ノート] 管理されている SA をすべて削除して、IKE の状態を初期化する。
 このコマンドでは、SA の削除を相手に通知しないので、通常の運用では **ipsec sa delete all** コマンドの方が望ましい。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

13.20.5 SA を自動更新するか否かの設定

[入力形式] **ipsec auto refresh refresh**
no ipsec auto refresh [refresh]

[パラメータ] ◦ *refresh*
 • on..... 自動更新する
 • off..... 自動更新しない

[説明] SA を自動更新するか否かを設定する。

[ノート] 古い SA を削除せずに新しい SA を生成する。

[デフォルト値] off

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

13.21 トンネルインタフェース関連の設定

13.21.1 使用する SA のポリシーの設定

[入力形式] **ipsec tunnel policy_id**
no ipsec tunnel [policy_id]

[パラメータ] ◦ *policy_id* 整数 (1..255)

[説明] 選択されているトンネルインタフェースで使用する SA のポリシーを設定する。

[デフォルト値] SA のポリシーは設定されていない

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

13.21.2 IPComp によるデータ圧縮の設定

[入力形式]	ipsec ipcomp type type no ipsec ipcomp type [type]														
[パラメータ]	<ul style="list-style-type: none"> ○ type <ul style="list-style-type: none"> • deflate..... deflate 圧縮でデータを圧縮する • none データ圧縮を行わない 														
[説明]	<p>IPComp でデータ圧縮を行うかどうかを設定する。サポートしているアルゴリズムは deflate のみである。受信した IPComp パケットを展開するためには、特別な設定を必要としない。すなわち、サポートしているアルゴリズムで圧縮された IPComp パケットを受信した場合には、設定に関係なく展開する。必ずしもセキュリティ・ゲートウェイの両方にこのコマンドを設定する必要はない。片側のみ設定した場合には、そのセキュリティ・ゲートウェイから送信される IP パケットのみが圧縮される。トランスポートモードのみを使用する場合には、IPComp を使用することはできない。</p>														
[ノート]	<p>データ圧縮には、PPP で使われる CCP や、フレームリレーで使われる FRF.9 もある。圧縮アルゴリズムとして、IPComp で使われる deflate と、CCP/FRF.9 で使われる Stac-LZS との間に基本的な違いはない。しかし、CCP/FRF.9 でのデータ圧縮は IPsec による暗号化の後に行われる。このため、暗号化でランダムになったデータを圧縮しようとする事になり、ほとんど効果がない。一方、IPComp は IPsec による暗号化の前にデータ圧縮が行われるため、一定の効果を得られる。また、CCP/FRF.9 とは異なり、対向のセキュリティ・ゲートウェイまでの全経路で圧縮されたままのデータが流れるため、例えば本機の出カインタフェースが LAN であってもデータ圧縮効果を期待できる。</p>														
[デフォルト値]	none														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

13.21.3 トンネルインタフェースの使用許可の設定

[入力形式]	tunnel enable tunnel_num no tunnel enable														
[パラメータ]	<ul style="list-style-type: none"> ○ tunnel_num <ul style="list-style-type: none"> • 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]	<p>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。</p>														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

13.21.4 トンネルインタフェースの使用不許可の設定

[入力形式]	tunnel disable tunnel_num														
[パラメータ]	<ul style="list-style-type: none"> ○ tunnel_num <ul style="list-style-type: none"> • 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]	<p>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う場合は、disable 状態で行うのが望ましい。</p>														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

130 13.IPsec の設定

13.21.5 トンネルインタフェース番号の選択

[入力形式] **tunnel select** *tunnel_num*

[パラメータ] ◦ *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。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

13.21.6 トンネルバックアップの設定

[入力形式] **tunnel backup** *peer_num*
no tunnel backup

[パラメータ] ◦ *peer_num* バックアップ先の相手先情報番号

[説明] トンネルインタフェースが down したときに、バックアップとして使用する PP インタフェースを設定する。

[デフォルト値] none

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

13.22 トランスポートモード関連の設定

13.22.1 トランスポートモードの定義

[入力形式] **ipsec transport** *id* *policy_id* [*proto* [*src_port_list* [*dst_port_list*]]]
no ipsec transport *id* [*policy_id* [*proto* [*src_port_list* [*dst_port_list*]]]]

[パラメータ] ◦ *id* トランスポート ID (1..255)
◦ *policy_id* ポリシー ID (1..255)
◦ *proto* プロトコル
◦ *src_port_list* UDP、TCP のソースポート番号列

- ポート番号を表す 10 進数
- ポート番号を表す二進モニク
- * (すべてのポート)

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

- ポート番号を表す 10 進数
- ポート番号を表す二進モニク
- * (すべてのポート)

[説明] トランスポートモードを定義する。
定義後、*proto*、*src_port_list*、*dst_port_list* パラメータに合致する IP パケットに対してトランスポートモードでの通信を開始する。

[設定例] ◦ 192.168.112.25 のルータへの telnet のデータをトランスポートモードで通信

```
# ipsec sa policy 102 192.168.112.25 esp des-cbc sha-hmac
# ipsec transport 1 102 tcp * telnet
```

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

14. 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 Windows95 や Windows98 などの「Microsoft(R) VPN Adaptor/マイクロソフト (R) 仮想プライベートネットワーク」が必要となります。

14.1 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。

14.1.1 PPTP サーバを動作させるか否かの設定

[入力形式]	pptp service <i>service</i> no pptp service [<i>service</i>]														
[パラメータ]	○ <i>service</i> <ul style="list-style-type: none"> • on PPTP サーバとして動作する • off PPTP サーバとして動作しない 														
[説明]	PPTP サーバ機能を動作させるか否かを設定する。														
[ノート]	PPTP サーバで使う TCP のポート番号 1723 を閉じます。デフォルト off なので、PPTP サーバを起動する場合には、 pptp service on を設定する。														
[デフォルト値]	off														
[適用モデル]	<table border="1" style="border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

14.1.2 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

[入力形式]	pp bind <i>tunnel_num</i> no pp bind [<i>tunnel_num</i>]														
[パラメータ]	○ <i>tunnel_num</i> トンネルインタフェースの番号 (tunnel1 .. tunnel20)														
[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。														
[ノート]	PPTP は PP 毎に設定します。 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。														
[デフォルト値]	設定されていない														
[適用モデル]	<table border="1" style="border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

14.1.3 PPTP の動作タイプの設定

[入力形式]	pptp service type <i>type</i> no pptp service type [<i>type</i>]														
[パラメータ]	○ <i>type</i> <ul style="list-style-type: none"> • server サーバとして動作 • client クライアントとして動作 														
[説明]	PPTP サーバとして動作するか、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、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で、もう一方がクライアントである必要がある。														
[デフォルト値]	server														
[適用モデル]	<table border="1" style="border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

14.1.4 PPTP ホスト名の設定

- [入力形式] **pptp hostname** *name*
no ptp hostname [*name*]
- [パラメータ] ◦ *name*.....ホスト名 (64byte 以下)
- [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 ptp** コマンドの '接続相手先:' で表示される。
- [デフォルト値] 機種名

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

14.1.5 PPTP パケットのウィンドウサイズの設定

- [入力形式] **pptp window size** *size*
no ptp window size [*size*]
- [パラメータ] ◦ *size*.....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。
- [デフォルト値] 32

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

14.1.6 PPTP の動作モードの設定

- [入力形式] **pptp call-id mode** *mode*
no ptp call-id mode [*mode*]
- [パラメータ] ◦ *mode*
 • normal 通常モード
 • backward-compatibility Rev.4.06.16 互換モード
- [説明] PPTP の動作モードを設定する。
 接続相手が Rev.4.06.16 の場合にのみ、動作モードを backward-compatibility にする。
- [デフォルト値] normal

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

14.1.7 PPTP 暗号鍵生成のための認証方式の設定

- [入力形式] **pp auth request** *auth* [arrive-only]
no pp auth request [*auth*]
- [パラメータ] ◦ *auth*
 • pap PAP
 • chap CHAP
 • mschap MSCHAP
 • mschap-v2 MSCHAP-Version2
 • chap-pap CHAP と PAP 両方
- [説明] 要求する認証方式を設定します
- [ノート] PPTP 暗号鍵生成のために認証プロトコルの MS-CHAP または MS-CHAPv2 を設定する。通常サーバ側で設定する。
- [デフォルト値] 設定されない

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

14.1.8 PPTP 暗号鍵生成のための認証方式の設定

[入力形式]	pp auth accept auth [<i>auth</i>] no pp auth accept [<i>auth auth</i>]														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>auth</i> • 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します														
[ノート]	PPTP 暗号鍵生成のために認証プロトコルの MS-CHAP または MS-CHAPv2 を設定する。通常クライアント側で設定する。														
[デフォルト値]	設定されない														
[適用モデル]	<table border="1" style="border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

14.2 リモートアクセス VPN 機能

14.2.1 PPTP トンネルの切断タイマの設定

[入力形式]	pptp tunnel disconnect time <i>time</i> no pptp tunnel disconnect time [<i>time</i>]														
[パラメータ]	○ <i>time</i> 切断タイマの秒数 (1..21474836)														
[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。														
[デフォルト値]	60														
[適用モデル]	<table border="1" style="border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

14.2.2 PPTP トンネルの端点の名前の設定

[入力形式]	tunnel endpoint name [<i>local_name</i>] <i>remote_name</i> no tunnel endpoint name [<i>local_name remote_name</i>]														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>local_name</i> 自分側端点 ○ <i>remote_name</i>..... 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。														
[適用モデル]	<table border="1" style="border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

14.2.3 PPTP キープアライブの設定

[入力形式] **pptp keepalive use** *use*
no pptp keepalive use [*use*]

[パラメータ] ○ *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う。

[デフォルト値] on

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

14.2.4 PPTP キープアライブのログ設定

[入力形式] **pptp keepalive log** *log*
no pptp keepalive log [*log*]

[パラメータ] ○ *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どうかを選択する。

[デフォルト値] off

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

14.2.5 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

[入力形式] **pptp keepalive interval** *interval* [*count*]
no pptp keepalive interval [*interval count*]

[パラメータ] ○ *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、その後の監視タイムは 1 秒に短縮される。

[デフォルト値] 30 6

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

14.2.6 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

【入力形式】 **ppp ccp no-encryption mode**
no ppp ccp no-encryption [mode]

【パラメータ】 ○ 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。

【デフォルト値】 accept

【適用モデル】	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

15. SNMP の設定

15.1 読み出し専用のコミュニティ名の設定

[入力形式]	snmp community read-only name no snmp community read-only [name]														
[パラメータ]	◦ <i>name</i>SNMP によるアクセスモードが読み出し専用であるコミュニティ名														
[説明]	SNMP によるアクセスモードが読み出し専用であるコミュニティ名を設定する。名称は 1 文字以上 16 文字以内。														
[デフォルト値]	public														
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

15.2 読み書き可能なコミュニティ名の設定

[入力形式]	snmp community read-write name no snmp community read-write [name]														
[パラメータ]	◦ <i>name</i>SNMP によるアクセスモードが読み書き可能であるコミュニティ名														
[説明]	SNMP によるアクセスモードが読み書き可能であるコミュニティ名を設定する。名称は 1 文字以上 16 文字以内。														
[デフォルト値]	空文字列														
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

15.3 認証失敗時 (authenticationFailure) にトラップを送信するか否かの設定

[入力形式]	snmp enableauthentraps send no snmp enableauthentraps [send]														
[パラメータ]	◦ <i>send</i> <ul style="list-style-type: none"> • on.....送信する • off.....送信しない 														
[説明]	MIB 変数 snmpEnableAuthenTraps を設定する。 これを off にすると、誤ったコミュニティ名を持つパケットを受信した場合にトラップを送信しない。SNMP トラップは snmp trap host コマンドで指定されたホストに対して送信される。														
[デフォルト値]	on														
[設定例]	# snmp trap host 192.168.0.2 # snmp enableauthentraps on														
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

15.4 SNMPによるアクセスを許可するホストの設定

[入力形式] **snmp host *bost***
no snmp host [*bost*]

[パラメータ] ○ *bost*

- none すべてのホストから SNMP によりアクセスできない
- any すべてのホストから SNMP によりアクセスできる
- IP アドレス SNMP によるアクセスを許可するホストの IP アドレス

[説明] SNMP によるアクセスを許可するホストを設定する。

[デフォルト値] none

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

15.5 sysContact の設定

[入力形式] **snmp syscontact *name***
no snmp syscontact [*name*]

[パラメータ] ○ *name* sysContact として登録する名称

[説明] MIB 変数 sysContact を設定する。255 文字以内の文字列が設定できる。空白を含ませるためには、パラメータ全体をダブルクォート (")、もしくはシングルクォート (') で囲む。
sysContact は一般的に、管理者の名前や連絡先を記入しておく変数である。

[デフォルト値] sysContact は設定されていない

[設定例] # snmp syscontact "RT administrator"

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

15.6 sysLocation の設定

[入力形式] **snmp syslocation *name***
no snmp syslocation [*name*]

[パラメータ] ○ *name* sysLocation として登録する名称

[説明] MIB 変数 sysLocation を設定する。255 文字以内の文字列が設定できる。空白を含ませるためには、パラメータ全体をダブルクォート (")、もしくはシングルクォート (') で囲む。
sysLocation は一般的に、機器の設置場所を記入しておく変数である。

[デフォルト値] sysLocation は設定されていない

[設定例] # snmp syslocation "RT room"

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

15.7 sysName の設定

- [入力形式] **snmp sysname name**
 no snmp sysname [name]
- [パラメータ] ◦ *name*.....sysNameとして登録する名称
- [説明] MIB 変数 sysName を設定する。255 文字以内の文字列が設定できる。空白を含ませるためには、パラメータ全体をダブルクォート("), もしくはシングルクォート(')で囲む。
 sysName は一般的に、機器の名称を記入しておく変数である。
- [デフォルト値] sysName は設定されていない
- [設定例] # snmp sysname "RT300i with VPN module"

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

15.8 SNMP トラップのコミュニティ名の設定

- [入力形式] **snmp trap community name**
 no snmp trap community [name]
- [パラメータ] ◦ *name*.....送信トラップのコミュニティ名
- [説明] トラップを送信する際のコミュニティ名を設定する。名称は 1 文字以上 16 文字以内。
- [デフォルト値] public

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

15.9 SNMP トラップの送信先の設定

- [入力形式] **snmp trap host host**
 no snmp trap host [host]
- [パラメータ] ◦ *host*
 • IP アドレス.....SNMP トラップを送信する先のホストの IP アドレス
- [説明] SNMP トラップを送信する先のホストを設定する。
- [デフォルト値] SNMP トラップを送信しない

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

15.10 PP インタフェースの情報を MIB2 の範囲で表示するか否かの設定

- [入力形式] **snmp yrifppdisplayatmib2 switch**
 no snmp yrifppdisplayatmib2
- [パラメータ] ◦ *sw*
 • on.....MIB 変数 yrIfPpDisplayAtMib2 を "enabled(1)" とする
 • off.....MIB 変数 yrIfPpDisplayAtMib2 を "disabled(2)" とする
- [説明] MIB 変数 yrIfPpDisplayAtMib2 の値をセットする。この MIB 変数は、PP インタフェースを MIB2 の範囲で表示するかどうかを決定する。Rev.4 以前と同じ表示にする場合には、MIB 変数を "enabled(1)" に、つまり、このコマンドで on を設定する。
- [デフォルト値] off

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

15.11 PP インタフェースのアドレスの強制表示の設定

[入力形式]	snmp display ipcp force <i>sw</i> no snmp display ipcp force														
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>sw</i> • on IPCP により付与された IP アドレスを PP インタフェースのアドレスとして必ず表示する • off IPCP により付与された IP アドレスは PP インタフェースのアドレスとして必ずしも表示されない 														
[説明]	<p>NAT を使用しない場合や、NAT の外側アドレスとして固定の IP アドレスが指定されている場合には、IPCP で得られた IP アドレスはそのまま PP インタフェースのアドレスとして使われる。この場合、SNMP では通常のインタフェースの IP アドレスを調べる手順で IPCP としてどのようなアドレスが得られたのか調べることができる。</p> <p>しかし、NAT の外側アドレスとして 'ipcp' と指定している場合には、IPCP で得られた IP アドレスは NAT の外側アドレスとして使用され、インタフェースには付与されない。そのため、SNMP でインタフェースの IP アドレスを調べても、IPCP でどのようなアドレスが得られたのかを知ることができない。</p> <p>本コマンドを on に設定しておく、IPCP で得られた IP アドレスが NAT の外側アドレスとして使用される場合でも、SNMP ではそのアドレスをインタフェースのアドレスとして表示する。アドレスが実際にインタフェースに付与されるわけではないので、始点 IP アドレスとして、その IP アドレスが利用されることはない。</p>														
[デフォルト値]	off														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

15.12 SNMP 送信パケットの始点アドレスの設定

[入力形式]	snmp local address <i>ip_address</i> no snmp local address [<i>ip_address</i>]														
[パラメータ]	◦ <i>ip_address</i> IP アドレス														
[説明]	SNMP 送信パケットの始点 IP アドレスを設定する。														
[デフォルト値]	インタフェースに設定されているアドレスから自動選択														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

16. RADIUS の設定

16.1 RADIUS による認証を使用するか否かの設定

[入力形式]	radius auth auth no radius auth [auth]														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>auth</i> <ul style="list-style-type: none"> • on.....使用する • off.....使用しない 														
[説明]	anonymous に対して何らかの認証を要求する設定の場合に、相手から受け取ったユーザネーム (PAP であれば UserID、CHAP であれば NAME) が、自分で持つユーザネーム (pp auth username コマンドで指定) の中に含まれていない場合には RADIUS サーバに問い合わせるか否かを設定する。														
[ノート]	RADIUS による認証と RADIUS によるアカウントは独立して使用できる。サポートしているアトリビュートについては、WWW サイトのドキュメント < http://www.rtpro.yamaha.co.jp/ > を参照すること。														
[デフォルト値]	off														
[適用モデル]	<table border="1" style="border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

16.2 RADIUS によるアカウントを使用するか否かの設定

[入力形式]	radius account account no radius account [account]														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>account</i> <ul style="list-style-type: none"> • on.....使用する • off.....使用しない 														
[説明]	RADIUS によるアカウントを使用するか否かを設定する。														
[ノート]	RADIUS による認証と RADIUS によるアカウントは独立して使用できる。サポートしているアトリビュートについては、WWW サイトのドキュメント < http://www.rtpro.yamaha.co.jp/ > を参照すること。														
[デフォルト値]	off														
[適用モデル]	<table border="1" style="border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

16.3 RADIUS サーバの指定

[入力形式]	radius server ip1 [ip2] no radius server [ip1 [ip2]]														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>ip1</i>RADIUS サーバ (正) の IP アドレス (IPv6 アドレス可) ○ <i>ip2</i>RADIUS サーバ (副) の IP アドレス (IPv6 アドレス可) 														
[説明]	<p>RADIUS サーバを設定する。2 つまで指定でき、最初のサーバから返事をもらえない場合は、2 番目のサーバに問い合わせを行う。</p> <p>RADIUS には認証とアカウントの 2 つの機能があり、それぞれのサーバは radius auth server / radius account server コマンドで個別に設定できる。radius server コマンドでの設定は、これら個別の設定が行われていない場合に有効となり、認証、アカウントいずれでも用いられる。</p>														
[適用モデル]	<table border="1" style="border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

16.4 RADIUS 認証サーバの指定

[入力形式]	radius auth server <i>ip1</i> [<i>ip2</i>] no radius auth server [<i>ip1</i> [<i>ip2</i>]]														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>ip1</i>..... RADIUS 認証サーバ (正) の IP アドレス (IPv6 アドレス可) ○ <i>ip2</i>..... RADIUS 認証サーバ (副) の IP アドレス (IPv6 アドレス可) 														
[説明]	RADIUS 認証サーバを設定する。2 つまで指定でき、最初のサーバから返事をもらえない場合は、2 番目のサーバに問い合わせを行う。														
[ノート]	このコマンドで RADIUS 認証サーバの IP アドレスが指定されていない場合は、 radius server コマンドで指定した IP アドレスを認証サーバとして用いる。														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center;">RTX2000</td> <td style="text-align: center;">RTX1000</td> <td style="text-align: center;">RT300i</td> <td style="text-align: center;">RT140p</td> <td style="text-align: center;">RT140f</td> <td style="text-align: center;">RT140i</td> <td style="text-align: center;">RT140e</td> </tr> <tr> <td style="text-align: center;">RT105p</td> <td style="text-align: center;">RT105i</td> <td style="text-align: center;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

16.5 RADIUS アカウントサーバの指定

[入力形式]	radius account server <i>ip1</i> [<i>ip2</i>] no radius account server [<i>ip1</i> [<i>ip2</i>]]														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>ip1</i>..... RADIUS アカウントサーバ (正) の IP アドレス (IPv6 アドレス可) ○ <i>ip2</i>..... RADIUS アカウントサーバ (副) の IP アドレス (IPv6 アドレス可) 														
[説明]	RADIUS アカウントサーバを設定する。2 つまで指定でき、最初のサーバから返事をもらえない場合は、2 番目のサーバに問い合わせを行う。														
[ノート]	このコマンドで RADIUS アカウントサーバの IP アドレスが指定されていない場合は、 radius server コマンドで指定した IP アドレスを認証サーバとして用いる。														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center;">RTX2000</td> <td style="text-align: center;">RTX1000</td> <td style="text-align: center;">RT300i</td> <td style="text-align: center;">RT140p</td> <td style="text-align: center;">RT140f</td> <td style="text-align: center;">RT140i</td> <td style="text-align: center;">RT140e</td> </tr> <tr> <td style="text-align: center;">RT105p</td> <td style="text-align: center;">RT105i</td> <td style="text-align: center;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

16.6 RADIUS 認証サーバの UDP ポートの設定

[入力形式]	radius auth port <i>port_num</i> no radius auth port [<i>port_num</i>]														
[パラメータ]	○ <i>port_num</i> UDP ポート番号														
[説明]	RADIUS 認証サーバの UDP ポート番号を設定する。														
[ノート]	RFC2138 ではポート番号として 1812 を使うことになっている。														
[デフォルト値]	1645														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center;">RTX2000</td> <td style="text-align: center;">RTX1000</td> <td style="text-align: center;">RT300i</td> <td style="text-align: center;">RT140p</td> <td style="text-align: center;">RT140f</td> <td style="text-align: center;">RT140i</td> <td style="text-align: center;">RT140e</td> </tr> <tr> <td style="text-align: center;">RT105p</td> <td style="text-align: center;">RT105i</td> <td style="text-align: center;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

16.7 RADIUS アカウントサーバの UDP ポートの設定

[入力形式]	radius account port <i>port_num</i> no radius account port [<i>port_num</i>]														
[パラメータ]	○ <i>port_num</i> UDP ポート番号														
[説明]	RADIUS アカウントサーバの UDP ポート番号を設定する。														
[ノート]	RFC2138 ではポート番号として 1813 を使うことになっている。														
[デフォルト値]	1646														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center;">RTX2000</td> <td style="text-align: center;">RTX1000</td> <td style="text-align: center;">RT300i</td> <td style="text-align: center;">RT140p</td> <td style="text-align: center;">RT140f</td> <td style="text-align: center;">RT140i</td> <td style="text-align: center;">RT140e</td> </tr> <tr> <td style="text-align: center;">RT105p</td> <td style="text-align: center;">RT105i</td> <td style="text-align: center;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

16.8 RADIUS シークレットの設定

- [入力形式] **radius secret secret**
 no radius secret [secret]
- [パラメータ] ○ *secret* シークレット文字列
- [説明] RADIUS シークレットを設定する。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

16.9 RADIUS 再送信パラメータの設定

- [入力形式] **radius retry count time**
 no radius retry [count time]
- [パラメータ] ○ *count* 再送回数 (1..10)
 ○ *time* ミリ秒 (20..10000)
- [説明] RADIUS パケットの再送回数とその時間間隔を設定する。
- [デフォルト値] *count* = 4
 time = 3000

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

17. 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。

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

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

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

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

17.1 インタフェースへの NAT ディスクリプタ適用の設定

[入力形式]	<pre>ip interface nat descriptor nat_descriptor_list ip pp nat descriptor nat_descriptor_list ip tunnel nat descriptor nat_descriptor_list no ip interface nat descriptor [nat_descriptor_list] no ip pp nat descriptor [nat_descriptor_list] no ip tunnel nat descriptor [nat_descriptor_list]</pre>														
[パラメータ]	<ul style="list-style-type: none"> ○ 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。														
[ノート]	インタフェースが LAN である場合、NAT ディスクリプタの OUTER アドレスに関しては、同一 LAN の ARP 要求に対して ARP 応答する。														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

17.2 NAT ディスクリプタの動作タイプの設定

[入力形式]	<pre>nat descriptor type nat_descriptor type no nat descriptor type [nat_descriptor type]</pre>														
[パラメータ]	<ul style="list-style-type: none"> ○ nat_descriptor NAT ディスクリプタ番号 (1..21474836) ○ type NAT ディスクリプタの動作タイプ <ul style="list-style-type: none"> • 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 個利用可能な場合は先勝ちで 15 個 NAT 変換され、残りは IP マスカレード変換される。														
[デフォルト値]	none														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

17.3 NAT 処理の外側 IP アドレスの設定

- [入力形式] **nat descriptor address outer nat_descriptor outer_ipaddress_list**
no nat descriptor address outer nat_descriptor [outer_ipaddress_list]
- [パラメータ]
- *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
ipcp	×	○	×
primary	○	×	×
secondary	○	×	×
IP アドレス	○	○	○

[デフォルト値] ipcp

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

17.4 NAT 処理の内側 IP アドレスの設定

- [入力形式] **nat descriptor address inner nat_descriptor inner_ipaddress_list**
no nat descriptor address inner nat_descriptor [inner_ipaddress_list]
- [パラメータ]
- *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。
- [デフォルト値] auto

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

17.5 静的 NAT エントリの設定

- [入力形式] **nat descriptor static nat_descriptor id outer_ip=inner_ip [count]**
no nat descriptor static nat_descriptor id [outer_ip=inner_ip [count]]
- [パラメータ]
- *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。デフォルト値がそれぞれ ipcp と auto であるので、例えば何らかの IP アドレスをダミーで設定しておくことで動的動作しないようにする。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

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

[入力形式]	nat descriptor masquerade rlogin <i>nat_descriptor use</i> no nat descriptor masquerade rlogin <i>nat_descriptor [use]</i>														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>nat_descriptor</i>..... NAT ディスクリプタ番号 (1..21474836) ○ <i>use</i> <ul style="list-style-type: none"> • <i>on</i>..... 使用する • <i>off</i>..... 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]	<i>on</i> 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 <i>on</i> の場合に rsh は使用できない。														
[デフォルト値]	off														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

17.7 静的 IP マスカレードエントリの設定

[入力形式]	nat descriptor masquerade static <i>nat_descriptor id inner_ip protocol port</i> no nat descriptor masquerade static <i>nat_descriptor id [inner_ip protocol port]</i>														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>nat_descriptor</i>..... NAT ディスクリプタ番号 (1..21474836) ○ <i>id</i>..... 静的 IP マスカレードエントリの識別情報 (1 以上の数値) ○ <i>inner_ip</i>..... 内側 IP アドレス (1 個) ○ <i>protocol</i> 対象プロトコル <ul style="list-style-type: none"> • <i>tcp</i> TCP プロトコル • <i>udp</i> UDP プロトコル • <i>icmp</i> 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 ○ <i>port</i>..... 固定するポート番号 (ニーモニック)、または、ポート番号の範囲指定 														
[説明]	IP マスカレードによる通信でポート番号変換を行わないようにポートを固定する。														
[設定例]	NetMeeting する NAT の内側の端末の IP アドレスが 192.168.0.2 の場合 # nat descriptor masquerade static 1 1 192.168.0.2 tcp 1720 # nat descriptor masquerade static 1 2 192.168.0.2 tcp 1503														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

17.8 NAT の IP アドレスマップの消去タイマの設定

[入力形式]	nat descriptor timer <i>nat_descriptor time</i> nat descriptor timer <i>nat_descriptor protocol=protocol [port=port_range] time</i> no nat descriptor timer <i>nat_descriptor [time]</i> no nat descriptor timer <i>nat_descriptor protocol=protocol [port=port_range] [...]</i>														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>nat_descriptor</i>..... NAT ディスクリプタ番号 (1..21474836) ○ <i>time</i>..... 消去タイマの秒数 (30..21474836) ○ <i>protocol</i> プロトコル ○ <i>port_range</i>..... 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。														
[デフォルト値]	900 プロトコル毎の設定はなし														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

17.9 IP マスカレードテーブルの TTL 処理方式の設定

- [入力形式] **nat descriptor masquerade ttl hold type**
no nat descriptor masquerade ttl hold
- [パラメータ]
 - *type*.....TTL を同期させる方法
 - *all*.....すべてのコネクションを対象とする
 - *ftp*.....FTP の制御チャンネルのみを対象とする
- [説明] 本コマンドによって IP マスカレードテーブルの TTL の扱いを制御することができる。通常、テーブルの TTL は単調に減少するが、FTP のように制御チャンネルとデータチャンネルからなるアプリケーションでは、制御チャンネルに対応するテーブルをデータ転送中に削除するべきではないため、制御チャンネルとデータチャンネルの両テーブルの TTL を同期させている。
- ただし、現時点では制御チャンネルとデータチャンネルの対応を把握することが難しいため、同じホスト間の通信について、すべてのコネクションを関係づけ TTL を同期させている。しかし、このような動作では、多くのテーブルの TTL が同期し多くのテーブルが長く残留するという現象が起きる。
- さらに、状況によっては、ルータのメモリが枯渇する可能性もあるため、この処理を FTP の制御チャンネルに限定し、メモリの枯渇を予防する選択肢を設ける。TTL の同期を FTP の制御チャンネルに限定する場合には、パラメータに *ftp* を設定する。FTP に限定せず、従来と同じように動作させるためには、パラメータに *all* を設定する。
- [デフォルト値] *all*

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

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

- [入力形式] **nat descriptor masquerade incoming nat_descriptor action [ip_address]**
- [パラメータ]
 - *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。
- [デフォルト値] *reject*
- [適用モデル]

	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

17.11 NAT のアドレス割当をログに記録するか否かの設定

- [入力形式] **nat descriptor log switch**
- [パラメータ]
 - *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。
- [デフォルト値] *off*
- [適用モデル]

	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

17.12 IP マスカレードで利用するポートの範囲の設定

[入力形式] **nat descriptor masquerade port range** *nat_descriptor* *start* [*port_num*]
no nat descriptor masquerade port range *nat_descriptor* [*start* [*port_num*]]

[パラメータ] ◦ *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*
 • ポート数 (1024..65534)
 • 省略時は 4096

[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。

[デフォルト値] 60000 4096

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

17.13 FTP として認識するポート番号の設定

[入力形式] **nat descriptor ftp port** *nat_descriptor* *port* [*port...*]
no nat descriptor ftp port *nat_descriptor* [*port...*]

[パラメータ] ◦ *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だとみなして処理をする。

[デフォルト値] 21

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

17.14 IP マスカレードで変換しないポート番号の範囲の設定

[入力形式] **nat descriptor masquerade unconvertible port** *nat_descriptor* *if-possible* [*clear*]
nat descriptor masquerade unconvertible port *nat_descriptor* *protocol* *clear*
nat descriptor masquerade unconvertible port *nat_descriptor* *protocol* *port*
no nat descriptor masquerade unconvertible port *nat_descriptor* *protocol* [*port*]

[パラメータ] ◦ *nat_descriptor*..... NAT ディスクリプタの識別番号 (1..21474836)
 ◦ *protocol* プロトコル
 • *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。

[デフォルト値] *clear*

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

18. DNS の設定

本機は、DNS(Domain Name Service) 機能として名前解決、リカーシブサーバ機能、上位 DNS サーバの選択機能、簡易 DNS サーバ機能 (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 **tracroute**、**rdate**、**ntpd**、**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。

リカーシブサーバ機能は、DNS サーバとクライアントの間に入って、DNS パケットの中継を行います。本機宛にクライアントから届いた DNS 問い合わせパケットを **dns server** コマンドで設定された DNS サーバに中継します。DNS サーバからの回答は本機宛に届くので、それをクライアントに転送します。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 サーバからデータを得た場合にデータに記されていた時間だけ保持されます。

DNS の機能を使用するためには、**dns server** 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。

18.1 DNS を利用するか否かの設定

[入力形式]	dns service service no dns service [service]														
[パラメータ]	○ <i>service</i> <ul style="list-style-type: none"> • recursiveDNS リカーシブサーバとして動作する • off..... サービスを停止させる 														
[説明]	DNS リカーシブサーバ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。														
[デフォルト値]	recursive														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

18.2 DNS サーバの IP アドレスの設定

[入力形式]	dns server ip_address [ip_address ...] no dns server [ip_address ...]														
[パラメータ]	○ <i>ip_address</i>DNS サーバの 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。														
[デフォルト値]	DNS サーバは設定されていない														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

18.3 DNS サーバを通知してもらう相手先情報番号の設定

- [入力形式] **dns server pp** *peer_num*
no dns server pp [*peer_num*]
- [パラメータ] ◦ *peer_num* DNS サーバを通知してもらう相手先情報番号
- [説明] DNS サーバを通知してもらう相手先情報番号を設定する。このコマンドで相手先情報番号が設定されていると、DNS での名前解決を行う場合に、まずこの相手先に発信して、そこで PPP の IPCP MS 拡張機能で通知された DNS サーバに対して問い合わせを行う。
相手先に接続できなかつたり、接続できても DNS サーバ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から返事がない場合には、相手先への接続と DNS サーバ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 msex** on の設定が必要である。
- [デフォルト値] DNS サーバ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 msex on
pp2# dns server pp 2

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

18.4 DNS 問い合わせの内容に応じた DNS サーバの選択

- [入力形式] **dns server select** *id server [type] query [original-sender][restrict pp connection-pp]*
dns server select *id pp pp_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*
- [パラメータ]
 - *id*DNS サーバ選択テーブルの番号
 - *server* DNS サーバの 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
 - *ns*.....ネームサーバ
 - *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、"**yamaha.co.jp**"であれば、**comm.yamaha.co.jp**、**rtpro.yamaha.co.jp** などにマッチする。"."を指定すると全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。"."を指定すると全ての IP アドレスにマッチする。
 - *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
 - *pp_num*IPCP により接続相手から通知される DNS サーバを使う場合の接続相手先情報番号
 - *interface*DHCP サーバより取得する DNS サーバを使う場合の LAN インタフェース名
 - *default-server**pp_num* パラメータで指定した接続相手から DNS サーバを獲得できなかったときに使う DNS サーバの 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アップしているかどうかサーバの選択条件に追加される。相手先がアップしていないとサーバは選択されない。相手先がアップしていて、かつ、他の条件もマッチしている場合に指定したサーバが選択される。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

18.5 DNS ドメイン名の設定

- [入力形式] **dns domain** *domain_name*
no dns domain [*domain_name*]
- [パラメータ]
 - *domain_name*.....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。
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。
空文字列を設定する場合には、**dns domain** とだけ入力する。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

18.6 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

[入力形式]	dns private address spoof spoof no dns private address spoof [spoof]														
[パラメータ]	<ul style="list-style-type: none"> ○ spoof <ul style="list-style-type: none"> • 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。														
[デフォルト値]	off														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

18.7 DHCP/IPCP MS 拡張で DNS サーバを通知する順序の設定

[入力形式]	dns notice order protocol server [server] no dns notice order protocol [server [server]]														
[パラメータ]	<ul style="list-style-type: none"> ○ protocol <ul style="list-style-type: none"> • dhcp DHCP による通知 • msex IPCP MS 拡張による通知 ○ server <ul style="list-style-type: none"> • none 一切通知しない • me 本機自身 • server dns server コマンドに設定したサーバ群 														
[説明]	DHCP や IPCP MS 拡張では DNS サーバ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 サーバの通知を行わなくなる。me は本機自身の DNS リカーシブサーバ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の数が最大 2 に限定されているので、後ろに me が続く場合は先頭の 1 つだけと本機自身を、server 単独で設定されている場合には先頭の 2 つだけを通知する。														
[デフォルト値]	dhcp me server msex me server														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

18.8 SYSLOG 表示で DNS により名前解決するか否かの設定

[入力形式]	dns syslog resolv resolv no dns syslog resolv [resolv]														
[パラメータ]	<ul style="list-style-type: none"> ○ resolv <ul style="list-style-type: none"> • 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。														
[デフォルト値]	off														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

18.9 静的 DNS レコードの登録

[入力形式] **ip host fqdn value**
dns static type name value
no ip host fqdn [value]
no dns static type name [value]

- [パラメータ]
- *type*.....名前タイプ
 - *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
 - *ns*.....ネームサーバ
 - *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>
<i>a</i>	FQDN	IP アドレス
<i>ptr</i>	IP アドレス	FQDN
<i>mx</i>	FQDN	FQDN
<i>ns</i>	FQDN	FQDN
<i>cname</i>	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.rtpro.yamaha.co.jp 133.176.200.1
# dns static ptr 133.176.200.2 pc2.yamaha.co.jp
# dns static cname mail.yamaha.co.jp mail2.yamaha.co.jp
```

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

19. 優先制御／帯域制御

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

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

帯域制御は、クラス分けしたキューをラウンドロビン方式で監視しますが、監視頻度に差を与えてキューごとに利用できる帯域に差をつけます。

クラスは、**queue class filter** コマンドにより、パケットのフィルタリングと同様な定義でパケットを分類します。クラスは 1 から 16 までの番号で識別します。優先制御では 1 から 4 までのクラスが、帯域制御では 1 から 16 までのクラスが使用できます。クラスは番号が大きいほど優先順位が高くなります。

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

19.1 インタフェース速度の設定

【入力形式】	speed interface speed speed pp speed no speed interface speed no speed pp [speed]														
【パラメータ】	<ul style="list-style-type: none"> ○ <i>interface</i> LAN インタフェース名 ○ <i>speed</i> インタフェース速度 (bit/s) 														
【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。帯域制御のためのパラメータ計算に用いられるもので、実際の速度を設定できるわけではない。物理的な速度と一致しているのが望ましい。MP により動的に回線速度が変動する場合などは、最低限の速度に設定しておく。														
【ノート】	<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。														
【デフォルト値】	0														
【適用モデル】	<table border="1" style="border-collapse: collapse; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

19.2 クラス分けのためのフィルタ設定

【入力形式】	queue class filter num class ip src_addr [dest_addr [proto [src_port [dest_port]]]] queue class filter num class ipx src_net [src_node [dst_net [dst_node [type [src_socket [dst_socket]]]]]] queue class filter num class bridge src_mac [dst_mac [offset byte_list]] no queue class filter num class [protocol ...]						
【パラメータ】	<ul style="list-style-type: none"> ○ <i>num</i> クラスフィルタの識別番号 (1..100) ○ <i>class</i> クラス (1..16) <p>IP フィルタ</p> <ul style="list-style-type: none"> ○ <i>src_addr</i> IP パケットの始点 IP アドレス <ul style="list-style-type: none"> • xxx.xxx.xxx.xxx xxx <ul style="list-style-type: none"> ▪ 10 進数 ▪ * (ネットマスクの対応するビットが 8 ビットとも 0 と同じ) • * (すべての IP アドレスに対応) ○ <i>dest_addr</i> IP パケットの終点 IP アドレス (<i>src_addr</i> と同じ形式)。省略した場合は一つの * と同じ。 ○ <i>proto</i> フィルタリングするパケットの種類 <ul style="list-style-type: none"> • プロトコルを表す 10 進数 • プロトコルを表すニーモニック <table border="1" style="border-collapse: collapse; text-align: center; margin: 10px 0;"> <tr><td>icmp</td><td>1</td></tr> <tr><td>tcp</td><td>6</td></tr> <tr><td>udp</td><td>17</td></tr> </table> <ul style="list-style-type: none"> • 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 <p>省略時は * と同じ。</p>	icmp	1	tcp	6	udp	17
icmp	1						
tcp	6						
udp	17						

○ *src_port*UDP、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

IPX フィルタ

○ *src_net* 始点 IPX ネットワーク番号

- 0:0:0:1FF:FF:FF:FE (2 桁以内の 16 進数以外に * も指定可)
- * (すべての IPX ネットワーク番号)

○ *src_node* 始点 IPX ノード番号

- 0:0:0:0:0:1FF:FF:FF:FF:FF:FE (2 桁以内の 16 進数以外に * も指定可)
- * (すべての IPX ノード番号)
- 省略時は一個の * と同じ

○ *dst_net* 終点 IPX ネットワーク番号 *src_net* と同じ形式

○ *dst_node* 終点 IPX ノード番号 *src_node* と同じ形式

○ *type* IPX パケットタイプ

- 10 進数 (0..255)
- 16 進数 (0x0..0xFF)
- ニーモニック文字列

unknown	0
rip	1
sap	4
spx	5
ncp	17
netbios	20

- 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 (5 個以内)
- * (すべての IPX パケットタイプ)
- 省略時は一個の * と同じ

○ *src_socket* 始点ソケット番号

- 10 進数 (0..65535)
- 0x を先頭に持つ 4 桁以内の 16 進数
- プロトコルを表すニーモニック

ncp	0x0451
sap	0x0452
rip	0x0453
netbios	0x0455
diag	0x0456
serialization	0x0457

- 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 (5 個以内)
- * (すべてのソケット番号)
- 省略時は一個の * と同じ

○ *dst_socket* 終点ソケット番号 *src_socket* と同じ形式。

ブリッジフィルタ

- *src_mac* 始点 MAC アドレス
 - *x:xx:xx:xx:xx:xx*
 - 16 進数
 - *
 - * (すべての MAC アドレスに対応)
- *dst_mac* 終点 MAC アドレス *src_mac* と同じ形式。省略時は一つの * と同じ
- *offset* オフセットを表す 10 進数 (イーサネットフレームの始点 MAC アドレスの直後を 0 とするバイト数)
- *byte_list*
 - バイト列
 - *xx* (*xx* は 2 桁の 16 進数)
 - 上項目のカンマで区切った並び (16 個以内)
 - * (すべてのバイト表現)

【説明】 クラス分けのためのフィルタを設定する。

RTX1000 では第 2、第 3 書式は使用できない。

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。

【適用モデル】

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

19.3 キューイングアルゴリズムタイプの選択

【入力形式】 **queue interface type type**
queue pp type type
no queue interface type type
no queue pp type [type]

【パラメータ】 ◦ *interface* LAN インタフェース名
 ◦ *type*
 • *fifo* First In, First Out 形式のキューイング
 • *priority* 優先制御キューイング
 • *cbq* 帯域制御キューイング
 • *wfq* Weighted Fair Queue 形式のキューイング

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

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

wfq は、送信待ちのパケットを始点・終点 IP アドレスやプロトコル、ポート番号でフローとしてグループ分けして、それぞれのフローで使用する帯域のバランスが取れるようにするキューイングアルゴリズムである。*wfq* を使用すると、TELNET のような、帯域はあまり必要としないが速い応答時間を必要とするプロトコルと、FTP のような応答時間よりも広い帯域を必要とするプロトコルを同時に利用した場合に、TELNET の応答時間の落ち込みを *fifo* に比べて軽減することができる。

wfq のもう一つの特徴は、設定がいらぬということである。設定するところがないため、優先制御や帯域制御に比べて細かい調整はできないが、簡単にフロー間での帯域のバランスを図ることができる。

priority は優先制御を行う。**queue class filter** コマンドおよび **queue interface class filter list** コマンドでパケットをクラス分けし、送信待ちのパケットの中から最も優先順位の高いクラスのパケットを送信する。

cbq は帯域制御を行う。**queue interface class property** コマンドで各クラスに割り振る帯域をあらかじめ設定しておき、**queue class filter** コマンドおよび **queue interface class filter list** コマンドでクラス分けされたパケットが指定の帯域になるように送信する。

【デフォルト値】 *fifo*

【適用モデル】

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

19.4 デフォルトクラスの設定

- [入力形式] **queue interface default class class**
 queue pp default class class
 no queue interface default class class
 no queue pp default class [class]
- [パラメータ] ◦ *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。
- [デフォルト値] 2

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

19.5 クラス分けフィルタの適用

- [入力形式] **queue interface class filter list filter_list**
 no queue interface class filter list [filter_list]
- [パラメータ] ◦ *interface*LAN インタフェース名、もしくは pp
 ◦ *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。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

19.6 クラスの属性の設定

[入力形式]	<pre> queue interface class property class bandwidth=<i>bandwidth</i> [<i>parent=parent</i>] [<i>borrow=borrow</i>] [<i>maxburst=maxburst</i>] [<i>minburst=minburst</i>] [<i>packetsize=packetsize</i>] queue pp class property class bandwidth=<i>bandwidth</i> [<i>parent=parent</i>] [<i>borrow=borrow</i>] [<i>maxburst=maxburst</i>] [<i>minburst=minburst</i>] [<i>packetsize=packetsize</i>] no queue interface class property class [<i>bandwidth=bandwidth ...</i>] no queue pp class property class [<i>bandwidth=bandwidth ...</i>] </pre>														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>interface</i> LAN インタフェース名 ○ <i>class</i> クラス (1..16) ○ <i>bandwidth</i> クラスに割り当てる帯域 (bit/s) 数値の後ろに 'k'、'M' をつけるとそれぞれ kbit/s、Mbit/s として扱われる。また、数値の後ろに '%' をつけると、回線全体の帯域に帯するパーセンテージとなる。 ○ <i>parent</i> 親クラスの番号 (0..16) ○ <i>borrow</i> 帯域が足りなくなった場合に親クラスから帯域を借りるか否かの設定 <ul style="list-style-type: none"> • <i>on</i> 借りる • <i>off</i> 借りない ○ <i>maxburst</i> 連続送信できる最大パケット数 (1..10000) ○ <i>minburst</i> 安定送信中に連続送信できる最大パケット数 (1..10000) ○ <i>packetsize</i> クラスで流れるパケットの平均パケット長 (1..10000) 														
[説明]	指定したクラスの属性を設定する。														
[ノート]	<p>パラメータを指定する場合には、各キーワードを明記すること。</p> <p><i>bandwidth</i> 属性は必ず指定されなければならない。回線全体の帯域は、speed コマンドで設定される。クラスに割り当てる帯域は、親クラス以下の値でなければいけない。</p> <p>クラス番号 0 はルートクラスを表す。ルートクラスは仮想的なクラスで、常に 100% の帯域を持ち、デフォルトでは他のクラスの親クラスになっている。ルートクラスに直接パケットを割り振ることはできず、その帯域は他のクラスに貸し出すためにだけ割り当てられている。</p> <p>帯域が足りなくなった場合に、親クラスから帯域を借りてくる (<i>borrow=on</i>) と設定すると、このクラスの最大速度は親クラスの最大速度まで増えることができる。通常は 100% の帯域を持つルートクラスを親クラスとするので、クラスの帯域は回線速度一杯に広がることができる。この場合、<i>bandwidth</i> の設定は、回線が混雑している場合に他のクラスとどの程度の割合で帯域をわけかの目安として使われる。</p> <p>帯域を借りてこない設定 (<i>borrow=off</i>) だと、このクラスの最大速度は <i>bandwidth</i> の値になり、それ以上の帯域を使わなくなる。特定のトラフィックの帯域を制限したい場合に有効である。</p> <p>このコマンドが設定されていないクラスには、100% の帯域が割り振られている。そのため、優先制御の設定をする場合には最低限でも対象としているクラスと、デフォルトクラスの 2 つに関してこのコマンドを設定しなくてはならない。デフォルトクラスの設定を忘れると、デフォルトクラスに 100% の帯域が割り振られるため、対象とするクラスは常にデフォルトクラスより狭い帯域を割り当てられることになる。</p>														
[デフォルト値]	<pre> <i>parent</i> = 0 <i>borrow</i> = on <i>maxburst</i> = 20 <i>minburst</i> = <i>maxburst</i> / 10 <i>packetsize</i> = 512 </pre>														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

19.7 クラス毎のキュー長の設定

[入力形式]	<pre> queue interface length len1 [<i>len2...len16</i>] no queue interface length [<i>len1</i> [<i>len2...len16</i>]] </pre>														
[パラメータ]	○ <i>len1..len16</i> クラス 1 からクラス 16 のキュー長														
[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で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。														
[デフォルト値]	200 (LAN、RT300i 以外の機種は 40) 20 (PP、全機種共通)														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

19.8 MP インタリーブの設定

- [入力形式] **ppp mp interleave** [*delay*] *switch*
no ppp mp interleave [[*delay*] *switch*]
- [パラメータ] ○ *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
- [デフォルト値] *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 bri2.1
 # 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
- [適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

20. OSPF

OSPF はインテリアゲートウェイプロトコルの一種で、グラフ理論をベースとしたリンク状態型の動的ルーティングプロトコルである。

20.1 OSPF の有効設定

【入力形式】	ospf configure refresh						
【パラメータ】	なし						
【説明】	OSPF 関係の設定を有効にする。OSPF 関係の設定を変更したら、ルータを再起動するか、あるいはこのコマンドを実行しなくてはならない。						
【適用モデル】	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

20.2 OSPF の使用設定

【入力形式】	ospf use switch no ospf use [switch]						
【パラメータ】	<ul style="list-style-type: none"> ○ <i>switch</i> <ul style="list-style-type: none"> • on OSPF を使用する • off OSPF を使用しない 						
【説明】	OSPF を使用するか否かを設定する。						
【デフォルト値】	off						
【適用モデル】	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

20.3 OSPF による経路の優先度設定

【入力形式】	ospf preference preference no ospf preference [preference]						
【パラメータ】	○ <i>preference</i> OSPF による経路の優先度を表す 1 以上の数値						
【説明】	OSPF による経路の優先度を設定する。優先度は 1 以上の数値で表され、数字が大きい程優先度が高い。OSPF と RIP など複数のプロトコルで得られた経路が食い違う場合には、優先度が高い方が採用される。優先度が同じ場合には時間的に先に採用された経路が有効となる。						
【ノート】	静的経路の優先度は 10000 で固定である。						
【デフォルト値】	2000						
【適用モデル】	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

20.4 OSPF のルータ ID 設定

【入力形式】	ospf router id router-id no ospf router id [router-id]						
【パラメータ】	○ <i>router_id</i> IP アドレス						
【説明】	OSPF のルータ ID を指定する。						
【デフォルト値】	LAN インタフェースの中でインタフェースの若いものから順にサーチして、プライマリ IP アドレスがついているインタフェースの IP アドレスをルータ ID とする						
【適用モデル】	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

20.5 外部プロトコルによる経路導入

[入力形式] **ospf import from** *protocol* [*filter filter_num...*]
 no ospf import from [*protocol* [*filter filter_num...*]]

[パラメータ] ◦ *protocol* OSPFの経路テーブルに導入する外部プロトコル

- *static* 静的経路
- *rip* RIP
- *bgp* BGP

◦ *filter_num* フィルタ番号

[説明] OSPFの経路テーブルに外部プロトコルによる経路を導入するかどうかを設定する。導入された経路は外部経路として他の OSPF ルータに広告される。

filter_num は **ospf import filter** コマンドで定義したフィルタ番号を指定する。外部プロトコルから導入されようとする経路は指定したフィルタにより検査され、フィルタに該当すればその経路は OSPF に導入される。該当するフィルタがない経路は導入されない。また、**filter** キーワード以降を省略した場合には、すべての経路が OSPF に導入される。

経路を広告する場合のパラメータであるメトリック値、メトリックタイプ、タグは、フィルタの検査で該当した **ospf import filter** コマンドで指定されたものを使う。**filter** キーワード以降を省略した場合には、以下のパラメータを使用する。

- *metric* = 1
- *type* = 2
- *tag* = 1

[デフォルト値] 外部経路は導入しない

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

20.6 外部経路導入に適用するフィルタ定義

[入力形式]	<pre>ospf import filter filter_num [not] kind ip_address/mask...[parameter...] no ospf import filter filter_num [[not] kind ip_address/mask...[parameter...]]</pre>														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>filter_num</i> フィルタ番号 ○ <i>kind</i> フィルタ種別 <ul style="list-style-type: none"> ● <i>include</i> 指定したネットワークアドレスに含まれる経路 (ネットワークアドレス自身を含む) ● <i>refines</i> 指定したネットワークアドレスに含まれる経路 (ネットワークアドレス自身は含まない) ● <i>equal</i> 指定したネットワークアドレスに一致する経路 ○ <i>ip_address/mask</i> ネットワークアドレスをあらわす IP アドレスとマスク長 ○ <i>parameter</i> 外部経路を広告する場合のパラメータで以下の種類がある <ul style="list-style-type: none"> ● <i>metric</i> メトリック値 (0..16777215) ● <i>type</i> メトリックタイプ (1..2) ● <i>tag</i> タグの値 (0..4294967295) 														
[説明]	<p>OSPF の経路テーブルに外部経路を導入する際に適用するフィルタを定義する。このコマンドで定義したフィルタは、ospf import from コマンドの <i>filter</i> 項で指定されてはじめて効果を持つ。</p> <p><i>ip_address/mask</i> では、ネットワークアドレスを設定する。これは、複数設定でき、経路の検査時にはそれぞれのネットワークアドレスに対して検査を行い、1 つでも該当するものがあればそれが適用される。</p> <p><i>kind</i> では、経路の検査方法を設定する。</p> <ul style="list-style-type: none"> ● <i>include</i> ネットワークアドレスと一致する経路および、ネットワークアドレスに含まれる経路が該当となる ● <i>refines</i> ネットワークアドレスに含まれる経路が該当となるが、ネットワークアドレスと一致する経路が含まれない ● <i>equal</i> ネットワークアドレスに一致する経路だけが該当となる <p><i>kind</i> の前に not キーワードを置くと、該当 / 非該当の判断が反転する。例えば、not equal では、ネットワークアドレスに一致しない経路が該当となる。</p> <p><i>parameter</i> では、該当した経路を OSPF の外部経路として広告する場合のパラメータとして、メトリック値、メトリックタイプ、タグがそれぞれ <i>metric</i>、<i>type</i>、<i>tag</i> により指定できる。これらを省略した場合場合には、以下の値が採用される。</p> <ul style="list-style-type: none"> ● <i>metric</i> = 1 ● <i>type</i> = 2 ● <i>tag</i> = 1 														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

20.7 OSPF エリア設定

[入力形式]	<pre>ospf area area [auth=auth] [stub [cost=cost]] no ospf area area [auth=auth] [stub [cost=cost]]</pre>														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>area</i> <ul style="list-style-type: none"> ● <i>backbone</i> バックボーンエリア ● 1 以上の数値 非バックボーンエリア ● IP アドレス表記 (0.0.0.0 は不可) 非バックボーンエリア ○ <i>auth</i> 認証を行う <ul style="list-style-type: none"> ● <i>text</i> プレーンテキスト認証 ● <i>md5</i> MD5 認証 ○ <i>cost</i> 0 以上の数値 														
[説明]	<p>OSPF エリアを設定する。</p> <ul style="list-style-type: none"> ● <i>stub [cost=cost]</i> スタブエリアであることを指定する。<i>cost</i> は 0 以上の数値で、エリアボーダルータがエリア内に広告するデフォルト経路のコストとして使われる。<i>cost</i> を指定しないとデフォルト経路の広告は行われない。 														
[デフォルト値]	<p>認証は行わない スタブエリアではない</p>														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

20.8 エリアへの経路広告

[入力形式] **ospf area network** *area network/mask* [restrict]
no ospf area network *area network/mask* [restrict]

[パラメータ] ◦ *area*

- backboneバックボーンエリア
- 1 以上の数値非バックボーンエリア
- IP アドレス表記 (0.0.0.0 は不可) 非バックボーンエリア

◦ *network*IP アドレス

◦ *mask* ネットマスク長

[説明] エリア境界ルータが他のエリアに経路を広告する場合に、このコマンドで指定したネットワークの範囲内の経路は単一のネットワーク経路として広告する。restrict キーワードが指定された場合には、範囲内の経路は要約した経路も広告しない。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

20.9 スタブ的接続の広告

[入力形式] **ospf area stubhost** *area host* [cost *cost*]
no ospf area stubhost *area host*

[パラメータ] ◦ *area*

- backboneバックボーンエリア
- 1 以上の数値非バックボーンエリア
- IP アドレス表記 (0.0.0.0 は不可) 非バックボーンエリア

◦ *host*IP アドレス

◦ *cost* 1 以上の数値

[説明] 指定したホストが指定したコストでスタブ的に接続されていることを エリア内に広告する。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

20.10 仮想リンク設定

- [入力形式] **ospf virtual-link** *router_id* *area* [*parameters...*]
no ospf virtual-link *router_id* [*router_id* [*parameters...*]]
- [パラメータ] ○ *router_id* 仮想リンクの相手のルータ ID
 ○ *area*
 • backbone..... バックボーンエリア
 • 1 以上の数値 非バックボーンエリア
 • IP アドレス表記 (0.0.0.0 は不可) 非バックボーンエリア
 ○ *parameters*..... *name=value* の列
- [説明] 仮想リンクを設定する。仮想リンクは *router_id* で指定したルータに対して、*area* で指定したエリアを経由して設定される。*parameters* では、仮想リンクのパラメータが設定できる。パラメータは *name=value* の形で指定され、以下の種類がある。

<i>name</i>	<i>value</i>	説明
retransmit-interval	秒数	LSA を連続して送る場合の再送間隔を秒単位で設定する。
transmit-delay	秒数	リンクの状態が変わってから LSA を送信するまでの時間を秒単位で設定する。
hello-interval	秒数	HELLO パケットの送信間隔を秒単位で設定する。
dead-interval	秒数	相手から HELLO を受け取れない場合に、相手がダウンしたと判断するまでの時間を秒単位で設定する。
authkey	文字列	プレーンテキスト認証の認証鍵を表す文字列を設定する。 KEY は文字列で、8 文字以内。
md5key	ID, 文字列	MD5 認証の認証鍵を表す ID と鍵文字列を設定する。ID は 10 進数で 0 ~ 255、KEY は文字列で 16 文字以内。MD5 認証鍵は 2 つまで設定できる。複数の MD5 認証鍵が設定されている場合には、送信パケットは同じ内容のパケットを複数個、それぞれの鍵による認証データを付加して送信する。受信時には鍵 ID が一致する鍵が比較対象となる。

- [ノート] ○ hello-interval/dead-interval について
 hello-interval/dead-interval の値は、そのインタフェースから直接通信できるすべての近隣ルータとの間で同じ値でなくてはならない。これらのパラメータの値が設定値とは異なっている OSPF HELLO パケットを受信した場合には、それは無視される。
- MD5 認証鍵について
 MD5 認証鍵を複数設定できる機能は、MD5 認証鍵を円滑に変更するためである。通常の運用では、MD5 認証鍵は 1 つだけ設定しておく。MD5 認証鍵を変更する場合は、まず 1 つのルータで新旧の MD5 認証鍵を 2 つ設定し、その後、近隣ルータで MD5 認証鍵を新しいものに変更していく。そして、最後に 2 つの鍵を設定したルータで古い鍵を削除すれば良い。

- [デフォルト値] *router_id*, *area* = なし
 retransmit-interval = 5 秒
 transmit-delay = 1 秒
 hello-interval = 10 秒
 dead-interval = 40 秒
 authkey = なし
 md5key = なし

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

20.11 指定インタフェースの OSPF エリア設定

[入力形式] **ip interface ospf area area [parameters...]**
ip pp ospf area area [parameters...]
ip tunnel ospf area area [parameters...]
no ip interface ospf area area [parameters...]
no ip pp ospf area [area [parameters...]]
no ip pp ospf area [area [parameters...]]

[パラメータ]

- *interface*LAN インタフェース
- *area*
 - backboneバックボーンエリア
 - 1 以上の数値非バックボーンエリア
 - IP アドレス表記 (0.0.0.0 は不可) 非バックボーンエリア
- *parameters*name=value の列

[説明] 指定したインタフェースの属する OSPF エリアを設定する。
name パラメータの *type* はインタフェースのネットワークがどのようなタイプであるかを設定する。
parameters では、リンクパラメータを設定する。パラメータは *name=value* の形で指定され、以下の種類がある。

<i>name</i>	<i>value</i>	説明
<i>type</i>	broadcast	ブロードキャスト
	point-to-point	ポイント・ポイント
	point-to-multipoint	ポイント・マルチポイント
	non-broadcast	NBMA
	passive	インタフェースに対して、OSPF パケットを送信しない。該当インタフェースに他の OSPF ルータがない場合に設定する。インタフェースのコストを設定する。デフォルト値は、インタフェースの種類と回線速度によって決定される。LAN インタフェースの場合は 1、PP インタフェースの場合は、バインドされている回線の回線速度を S[kbit/s] とすると、以下の計算式で決定される。例えば、64kbit/s の場合は 1562、1.536Mbit/s の場合には 65 となる。 $\cdot \text{COST} = 100000 / S$
<i>cost</i>	コスト	指定ルータの選択の際の優先度を設定する。PRIORITY 値が大きいルータが指定ルータに選ばれる。0 を設定すると、指定ルータに選ばれなくなる。
<i>priority</i>	優先度	LSA を連続して送る場合の再送間隔を秒単位で設定する。リンクの状態が変わってから LSA を送信するまでの時間を秒単位で設定する。
<i>retransmit-interval</i>	秒数	HELLO パケットの送信間隔を秒単位で設定する。
<i>transmit-delay</i>	秒数	近隣ルータから HELLO を受け取れない場合に、近隣ルータがダウンしたと判断するまでの時間を秒単位で設定する。
<i>hello-interval</i>	秒数	非ブロードキャストリンクでのみ有効なパラメータで、近隣ルータがダウンしている場合の HELLO パケットの送信間隔を秒単位で設定する。
<i>dead-interval</i>	秒数	プレーンテキスト認証の認証鍵を表す文字列を設定する。文字列で、8 文字以内。
<i>poll-interval</i>	秒数	MD5 認証の認証鍵を表す ID と鍵文字列を設定する。ID は 10 進数で 0 ~ 255、文字列は 16 文字以内。MD5 認証鍵は 2 つまで設定できる。複数の MD5 認証鍵が設定されている場合には、送信パケットは同じ内容のパケットを複数個、それぞれの鍵による認証データを付加して送信する。受信時には鍵 ID が一致する鍵が比較対象となる。
<i>authkey</i>	文字列	
<i>md5key</i>	ID, 文字列	

[ノート] ◦ *name* パラメータの *type* について
name パラメータの *type* として、LAN インタフェースは broadcast のみが許される。PP インタフェースは、PPP を利用する場合は point-to-point、フレームリレーを利用する場合は point-to-multipoint と non-broadcast のいずれかが設定できる。
フレームリレーで non-broadcast (NBMA) を利用する場合には、フレームリレーの各拠点間のすべての間で PVC が設定されており、FR に接続された各ルータは他のルータと直接通信できるような状態、すなわちフルメッシュになっていなくてはならない。また、non-broadcast では近隣ルータを自動的に認識することができないため、すべての近隣ルータを **ip pp ospf neighbor** コマンドで設定する必要がある。

point-to-multipoint を利用する場合には、フレームリレーの PVC はフルメッシュである必要はなく、一部が欠けたパッチメッシュでも利用できる。近隣ルータは InArp を利用して自動的に認識するため、InArp が必須となる。RT では InArp を使うかどうかは **fr inarp** コマンドで制御できるが、デフォルトでは InArp を使用する設定になっているので、**ip pp address** コマンドでインタフェースに適切な IP アドレスを与えるだけでよい。

point-to-multipoint と設定されたインタフェースでは、**ip pp ospf neighbor** コマンドの設定は無視される。

point-to-multipoint の方が non-broadcast よりもネットワークの制約が少なく、また設定も簡単だが、その代わりに

回線を流れるトラフィックは大きくなる。**non-broadcast** では、**broadcast** と同じように指定ルータが選定され、HELLO などの OSPF トラフィックは各ルータと指定ルータの間だけに限定されるが、**point-to-multipoint** ではすべての通信可能なルータペアの間に **point-to-point** リンクがあるという考え方なので、OSPF トラフィックもすべての通信可能なルータペアの間でやりとりされる。

○ **passive** について

passive は、インタフェースが接続しているネットワークに他の OSPF ルータが存在しない場合に指定する。**passive** を指定しておく、インタフェースから OSPF パケットを送信しなくなるので、無駄なトラフィックを抑制したり、受信側で誤動作の原因になるのを防ぐことができる。

LAN インタフェース (**type=broadcast** であるインタフェース) の場合には、インタフェースが接続しているネットワークへの経路は、**ip interface ospf area** コマンドを設定していないと他の OSPF ルータに広告されない。そのため、OSPF を利用しないネットワークに接続する LAN インタフェースに対しては、**passive** を付けた **ip interface ospf area** コマンドを設定しておくことでそのネットワークでは OSPF を利用しないまま、そこへの経路を他の OSPF ルータに広告することができる。

PP インタフェースに対して **ip interface ospf area** コマンドを設定していない場合は、インタフェースが接続するネットワークへの経路は外部経路として扱われる。外部経路なので、他の OSPF ルータに広告するには **ospf import** コマンドの設定が必要である。

○ **hello-interval/dead-interval** について

hello-interval/dead-interval の値は、そのインタフェースから直接通信できるすべての近隣ルータとの間で同じ値でなくてはならない。これらのパラメータの値が設定値とは異なっている OSPF HELLO パケットを受信した場合には、それは無視される。

○ MD5 認証鍵について

MD5 認証鍵を複数設定できる機能は、MD5 認証鍵を円滑に変更するためである。

通常の運用では、MD5 認証鍵は 1 つだけ設定しておく。MD5 認証鍵を変更する場合は、まず 1 つのルータで新旧の MD5 認証鍵を 2 つ設定し、その後、近隣ルータで MD5 認証鍵を新しいものに変更していく。そして、最後に 2 つの鍵を設定したルータで古い鍵を削除すれば良い。

[デフォルト値] **area** = インタフェースは OSPF エリアに属していない
type = **broadcast** (LAN インタフェース設定時)
 = **point-to-point** (PP インタフェース設定時)
passive = インタフェースは **passive** ではない
cost = 1 (lan 設定時)、pp は回線速度に依存
priority = 1
retransmit-interval = 5 秒
transmit-delay = 1 秒
hello-interval = 10 秒 (**type = broadcast** 設定時)
 = 10 秒 (**point-to-point** 設定時)
 = 30 秒 (**non-broadcast** 設定時)
 = 30 秒 (**point-to-multipoint** 設定時)
dead-interval = **hello-interval** の 4 倍
poll-interval = 120 秒
authkey = なし
md5key = なし

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

20.12 非ブロードキャスト型ネットワークに接続されている OSPF ルータの指定

[入力形式] **ip interface ospf neighbor ip_address** [eligible]
 no ip interface ospf neighbor ip_address [eligible]

[パラメータ] ○ *interface* インタフェース名
 ○ *ip_address* 近隣ルータの IP アドレス

[説明] 非ブロードキャスト型のネットワークに接続されている OSPF ルータを指定する。
 eligible キーワードが指定されたルータは指定ルータとして適格であることを表す。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

21. BGP

21.1 経路の集約の設定

[入力形式]	bgp aggregate remote_as filter filter_num ... no bgp aggregate remote_as [filter filter_num ...]														
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>remote_as</i> 相手の AS 番号 (1..65535) ◦ <i>filter_num</i> フィルタ番号 (1 .. 21474836) 														
[説明]	BGP で広告する集約経路を設定する。フィルタの番号には、 bgp aggregate filter コマンドで定義した番号を指定する。														
[デフォルト値]	デフォルトでは経路は集約されない。														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

21.2 経路を集約するためのフィルタの設定

[入力形式]	bgp aggregate filter filter_num [reject] kind ip_address/mask ... no bgp aggregate filter filter_num [[reject] kind ip_address/mask ...]														
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>filter_num</i> フィルタ番号 (1 .. 21474836) ◦ <i>kind</i> フィルタの種類 <ul style="list-style-type: none"> • <i>include</i> 指定したネットワークに含まれる経路 (ネットワークアドレス自身を含む) • <i>refines</i> 指定したネットワークに含まれる経路 (ネットワークアドレス自身を含まない) • <i>equal</i> 指定したネットワークに一致する経路 ◦ <i>ip_address/mask</i> <ul style="list-style-type: none"> • IP アドレス / ネットマスク • <i>all</i> すべてのネットワーク 														
[説明]	<p>BGP で広告する経路を集約するためのフィルタを定義する。このコマンドで定義したフィルタは、bgp aggregate コマンドの <i>filter</i> 節で指定されてはじめて効果を持つ。</p> <p><i>ip_address/mask</i> では、ネットワークアドレスを設定する。これは複数設定でき、そのうち、一致するネットワーク長が長い設定が採用される。</p> <p><i>kind</i> の前に <i>reject</i> キーワードを置くと、その経路は集約されない。</p>														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

21.3 AS 番号の設定

[入力形式]	bgp autonomous-system as no bgp autonomous-system [as]														
[パラメータ]	◦ <i>as</i> AS 番号 (1..65535)														
[説明]	ルータの AS 番号を設定する。														
[ノート]	AS 番号を設定するまで BGP は動作しない。														
[デフォルト値]	AS 番号は設定されない。														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

21.4 BGP の設定の有効化

- [入力形式] **bgp configure refresh**
- [パラメータ] なし
- [説明] BGP の設定を有効にする。BGP の設定を変更したら、ルータを再起動するか、このコマンドを実行する必要がある。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

21.5 BGP で受信した経路に対するフィルタの適用

- [入力形式] **bgp export remote_as filter filter_num ...**
no bgp export remote_as [filter filter_num ...]
- [パラメータ]
 ◦ *remote_as*相手の AS 番号 (1..65535)
 ◦ *filter_num* フィルタ番号 (1 .. 21474836)
- [説明] BGP で受けた経路に対して適用するフィルタを設定する。フィルタに該当しない経路は、実際のルーティングには適用されず、RIP や OSPF のような他のプロトコルに通知されることもない。フィルタの番号には、**bgp export filter** コマンドで定義した番号を指定する。
- [デフォルト値] このコマンドが設定されていないときには、BGP が受信したすべての経路が破棄される。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

21.6 BGP で受信する経路に適用するフィルタの設定

- [入力形式] **bgp export filter filter_num [reject] kind ip_address/mask ... [parameter]**
no bgp export filter filter_num [[reject] kind ip_address/mask ... [parameter]]
- [パラメータ]
 ◦ *filter_num* フィルタ番号 (1 .. 21474836)
 ◦ *kind* フィルタの種類
 • **include** 指定したネットワークに含まれる経路 (ネットワークアドレス自身を含む)
 • **refines** 指定したネットワークに含まれる経路 (ネットワークアドレス自身を含まない)
 • **equal** 指定したネットワークに一致する経路
 ◦ *ip_address/mask*
 • IP アドレス / ネットマスク
 • **all** すべてのネットワーク
 ◦ *parameter* TYPE=VALUE の組

TYPE	VALUE	説明
preference	0..255	同じ経路を複数の相手から受信したときに、一方を選択するための優先度

- [説明] BGP で受信する経路に適用するフィルタを定義する。このコマンドで定義したフィルタは、**bgp export** コマンドの filter 節で指定されてはじめて効果を持つ。
ip_address/mask では、ネットワークアドレスを設定する。複数の設定があるときには、プレフィックスが最も長く一致する設定が採用される。
kind の前に reject キーワードを置くと、その経路が拒否される。
- [ノート] preference の設定は BGP 経路の間で優先順位をつけるために使用される。BGP 経路の全体の優先度は、**bgp preference** コマンドで設定する。
- [デフォルト値] 指定のないパラメータのデフォルト値は以下のとおり。
 preference ...0
- [設定例] # bgp export filter 1 include 10.0.0.0/16 172.16.0.0/16
 # bgp export filter 2 not equal 192.168.0.0/24

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

21.7 BGPに導入する経路に対するフィルタの適用

[入力形式]	bgp import remote_as protocol [from_as] [filter filter_num ...] no bgp import remote_as protocol [from_as] [filter filter_num ...]														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>remote_as</i> 相手の AS 番号 (1..65535) ○ <i>protocol</i> 経路制御プロトコル <ul style="list-style-type: none"> • <i>static</i> 静的経路 • <i>rip</i> RIP • <i>ospf</i> OSPF • <i>bgp</i> BGP • <i>aggregate</i> 集約経路 ○ <i>from_as</i> 導入する経路を受信した AS (<i>protocol</i> で <i>bgp</i> を指定したときのみ) (1..65535) ○ <i>filter_num</i> フィルタ番号 (1 .. 21474836) 														
[説明]	RIP や OSPF のような BGP 以外の経路を導入するときに適用する フィルタを設定する。フィルタに該当しない経路は導入されない。フィルタの番号には、bgp filter コマンドで定義した番号を指定する。BGP の経路を導入するときには、その経路を受信した AS 番号を指定する 必要がある。														
[デフォルト値]	このコマンドが設定されていないときには、外部経路は導入されない。														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

21.8 BGPに導入する経路に適用するフィルタの設定

[入力形式]	bgp import filter filter_num [reject] kind ip_address/mask ... [parameter] no bgp import filter filter_num [[reject] kind ip_address/mask ... [parameter]]														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>filter_num</i> フィルタ番号 (1 .. 21474836) ○ <i>kind</i> フィルタの種別 <ul style="list-style-type: none"> • <i>include</i> 指定したネットワークに含まれる経路 (ネットワークアドレス自身を含む) • <i>refines</i> 指定したネットワークに含まれる経路 (ネットワークアドレス自身を含まない) • <i>equal</i> 指定したネットワークに一致する経路 ○ <i>ip_address/mask</i> <ul style="list-style-type: none"> • IP アドレス / ネットマスク • <i>all</i> すべてのネットワーク ○ <i>parameter</i> TYPE=VALUE の組 <table border="1" style="width: 100%; border-collapse: collapse; text-align: center; margin-top: 10px;"> <thead> <tr> <th style="width: 15%;">TYPE</th> <th style="width: 15%;">VALUE</th> <th style="width: 70%;">説明</th> </tr> </thead> <tbody> <tr> <td><i>metric</i></td> <td>1..16777215</td> <td>MED(Multi-Exit Discriminator) で通知するメトリック値 (指定しないときは MED を送信しない)</td> </tr> </tbody> </table>	TYPE	VALUE	説明	<i>metric</i>	1..16777215	MED(Multi-Exit Discriminator) で通知するメトリック値 (指定しないときは MED を送信しない)								
TYPE	VALUE	説明													
<i>metric</i>	1..16777215	MED(Multi-Exit Discriminator) で通知するメトリック値 (指定しないときは MED を送信しない)													
[説明]	<p>BGP に導入する経路に適用するフィルタを定義する。このコマンドで定義したフィルタは、bgp import コマンドの filter 節で指定されてはじめて効果を持つ。</p> <p><i>ip_address/mask</i> では、ネットワークアドレスを設定する。複数の設定があるときには、プレフィックスが最も長く一致する設定が採用される。</p> <p><i>kind</i> の前に <i>reject</i> キーワードを置くと、その経路が拒否される。</p>														
[デフォルト値]	指定のないパラメータのデフォルト値は以下のとおり。 <i>metric</i> ...1														
[設定例]	<pre># bgp import filter 1 include 10.0.0.0/16 172.16.0.0/16 # bgp import filter 2 reject equal 192.168.0.0/24</pre>														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

21.9 BGP による接続先の設定

[入力形式] **bgp neighbor neighbor_id remote_as remote_address [parameter ...]**
no bgp neighbor neighbor_id [remote_as remote_address [parameter ...]]

- [パラメータ] ○ neighbor_id 近隣ルータの番号 (1 .. 21474836)
- remote_as 相手の AS 番号 (1..65535)
- remote_address 相手の IP アドレス
- parameter TYPE=VALUE の組

TYPE	VALUE	説明
hold-time	off もしくは 3 以上の整数 [秒]	キープアライブの送信間隔
metric	1 .. 21474836	MED (Multi-Exit Discriminator) で通知するメトリック値
passive	on または off	能動的な BGP コネクションの接続を抑制するか否か

[説明] BGP コネクションを接続する近隣ルータを定義する。

[ノート] metric パラメータはすべての MED のデフォルト値として働くので、**bgp import** コマンドで MED を設定したときにはそれが優先される。

[デフォルト値] 指定のないパラメータのデフォルト値は以下のとおり。

hold-time ...180
 metric ...MED は送信されない
 passive ...off

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

21.10 BGP による経路の優先度の設定

[入力形式] **bgp preference preference**
no bgp preference [preference]

- [パラメータ] ○ preference 優先度 (1 .. 21474836)

[説明] BGP による経路の優先度を設定する。優先度は 1 以上の整数で示され、数字が大きいくほど優先度が高い。BGP とその他のプロトコルで得られた経路が食い違う場合には、優先度の高い経路が採用される。優先度が同じ場合には、先に採用された経路が有効になる。

[ノート] 各プロトコルに与えられた優先度のデフォルト値は次のとおり。

- スタティック 10000
- RIP 1000
- OSPF 2000
- BGP 500

[デフォルト値] 500

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

21.11 ルータ ID の設定

[入力形式] **bgp router id ip_address**
no bgp router id [ip_address]

- [パラメータ] ○ ip_address IP アドレス

[説明] ルータ ID を設定する。

[ノート] 通常はこのコマンドを設定する必要はない。

[デフォルト値] インタフェースに付与されているプライマリアドレスから自動的に選択する。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

21.12 BGPの起動の設定

【入力形式】 **bgp use use**
no bgp use [use]

【パラメータ】 ○ *use*

- on BGP を起動する
- off BGP を起動しない

【説明】 BGP を起動するかどうかを設定する。

【デフォルト値】 off

【適用モデル】	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

22. IPv6

22.1 共通の設定

22.1.1 IPv6 パケットを扱うか否かの設定

- [入力形式] **ipv6 routing routing**
no ipv6 routing [routing]
- [パラメータ] ◦ *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。
- [デフォルト値] on

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

22.1.2 IPv6 インタフェースのリンク MTU の設定

- [入力形式] **ipv6 interface mtu mtu**
- [パラメータ] ◦ *interface*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。
- [デフォルト値] 1500

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

22.2 IPv6 アドレスの管理

22.2.1 インタフェースの IPv6 アドレスの設定

- [入力形式] **ipv6 interface address ipv6_address/prefix_len**
ipv6 pp address ipv6_address/prefix_len
ipv6 tunnel address ipv6_address/prefix_len
no ipv6 interface address ipv6_address/prefix_len
no ipv6 pp address ipv6_address/prefix_len
no ipv6 tunnel address ipv6_address/prefix_len
- [パラメータ] ◦ *interface*LAN インタフェース
 ◦ *ipv6_address*.....IPv6 アドレス
 ◦ *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。
- [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。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

22.2.2 インタフェースに付与されている IPv6 アドレスの表示

- [入力形式] **show ipv6 address**
- [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。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

22.3 近隣探索

22.3.1 ルータ広告で配布するプレフィックスの定義

[入力形式] **ipv6 prefix** *prefix_id prefix/prefix_len* [*valid_lifetime=time*] [*preferred_lifetime=time*] [*l_flag=sw*] [*a_flag=sw*]
no ipv6 prefix *prefix_id*

[パラメータ]

- *prefix_id* プレフィックス番号
- *prefix* プレフィックス
- *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,bb:mm[:ss]*
 - *YYYY* 年 (1980..2079)
 - *MM* 月 (01..12)
 - *DD* 日 (01..31)
 - *bb* 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
- *sw*
 - 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 1 5552000 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。最終有効期間とはアドレスが無効になるまでの時間であり、推奨有効期間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。

[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。

[デフォルト値] *valid_lifetime* = 2592000
preferred_lifetime = 604800
l_flag = on
a_flag = on

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

22.3.2 ルータ広告の送信の制御

[入力形式] **ipv6 interface rtadv send prefix_id [prefix_id...] [m_flag=sw] [o_flag=sw]**
ipv6 pp rtadv send prefix_id [prefix_id...] [m_flag=sw] [o_flag=sw]
no ipv6 interface rtadv send
no ipv6 pp rtadv send

- [パラメータ]
- interfaceLAN インタフェース
 - prefix_idプレフィックス番号
 - m_flagmanaged address configuration フラグ
 - o_flagother stateful configuration フラグ
 - switch
 - on
 - off

[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。managed address configuration フラグを **off** とすることで、ネットワークに接続されているホストのステートレス自動設定が許され、ホスト自身でアドレス設定がなされる。また other stateful configuration フラグを **off** とすることで、ホストはオプションとして格納されているプレフィックスリストを調べることになる。

[デフォルト値] m_flag = off
o_flag = off

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

22.4 経路制御

22.4.1 IPv6 の経路情報の追加

[入力形式] **ipv6 route network gateway gateway [parameter] [gateway gateway [parameter]]**
no ipv6 route network

- [パラメータ]
- network
 - IP アドレス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 pp_num [dlsi=dlsi] PP インタフェースへの経路
 "dlsi=dlsi" が指定された場合は、フレームリレーの DLCI への経路
 - pp_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。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

22.5 RIPng

22.5.1 RIPng の使用の設定

[入力形式] **ipv6 rip use use**
 no ipv6 rip use

[パラメータ] ○ *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。

[デフォルト値] off

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

22.5.2 インタフェースにおける RIPng の送信ポリシーの設定

[入力形式] **ipv6 interface rip send send**
 ipv6 pp rip send send
 no ipv6 interface rip send
 no ipv6 pp rip send

[パラメータ] ○ *interface* LAN インタフェース
 ○ *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。

[デフォルト値] on

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

22.5.3 インタフェースにおける RIPng の受信ポリシーの設定

[入力形式] **ipv6 interface rip receive sw**
 ipv6 pp rip receive sw
 no ipv6 interface rip receive
 no ipv6 pp rip receive

[パラメータ] ○ *interface* LAN インタフェース
 ○ *sw* スイッチ
 • 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。

[デフォルト値] on

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

22.5.4 インタフェースにおける信頼できる RIPng ゲートウェイの設定

- [入力形式] **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
- [パラメータ] ◦ *interface*LAN インタフェース
 ◦ *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。
- [適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

22.5.5 RIPng の加算ホップ数の設定

- [入力形式] **ipv6 pp rip hop direction bop**
no ipv6 pp rip hop
- [パラメータ] ◦ *direction*方向
 • *in*受信時に加算する
 • *out*送信時に加算する
 ◦ *bop*加算ホップ数 (0..15)
- [説明] PP インタフェースで送受信する RIPng のメトリックに対して加算するホップ数を設定する。
- [デフォルト値] 0
- [適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

22.5.6 RIPng で送受信する経路に対するフィルタリングの設定

- [入力形式] **ipv6 interface rip filter direction filter_list** [filter_list...]
ipv6 pp rip filter direction filter_list [filter_list...]
no ipv6 interface rip filter
no ipv6 pp rip filter
- [パラメータ] ◦ *interface*LAN インタフェース
 ◦ *direction*方向
 • *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] PP 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。
- [デフォルト値] フィルタは設定されていない
- [適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

22.5.7 回線接続時の PP 側の RIPng の動作の設定

[入力形式]	ipv6 pp rip connect send action no ipv6 pp rip connect send														
[パラメータ]	○ <i>action</i> <ul style="list-style-type: none"> • 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 														
[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。														
[デフォルト値]	update														
[設定例]	# ipv6 pp rip connect interval 60 # ipv6 pp rip connect send interval														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

22.5.8 回線接続時の PP 側の RIPng 送出の時間間隔の設定

[入力形式]	ipv6 pp rip connect interval time no ipv6 pp rip connect interval														
[パラメータ]	○ <i>time</i> 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。														
[デフォルト値]	30														
[設定例]	# ipv6 pp rip connect interval 60 # ipv6 pp rip connect send interval														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

22.5.9 回線切断時の PP 側の RIPng の動作の設定

[入力形式]	ipv6 pp rip disconnect send action no ipv6 pp rip disconnect send														
[パラメータ]	○ <i>action</i> <ul style="list-style-type: none"> • 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接続時に RIP を送出する条件を設定する。														
[デフォルト値]	none														
[設定例]	# ipv6 pp rip disconnect interval 1800 # ipv6 pp rip disconnect send interval														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

22.5.10 回線切断時の PP 側の RIPng 送出の時間間隔の設定

- [入力形式] **ipv6 pp rip disconnect interval time**
 no ipv6 pp rip disconnect interval
- [パラメータ] ◦ *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。
- [デフォルト値] 3600
- [設定例] # ipv6 pp rip disconnect interval 1800
 # ipv6 pp rip disconnect send interval

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

22.5.11 RIPng による経路を回線切断時に保持するか否かの設定

- [入力形式] **ipv6 pp rip hold routing bold**
 no ipv6 pp rip hold routing
- [パラメータ] ◦ *bold*
 • 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。
- [デフォルト値] off

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

22.6 フィルタの設定

22.6.1 IPv6 フィルタの定義

- [入力形式] **ipv6 filter filter_num pass_reject src_address[/prefix_len] [dst_address[/prefix_len]]**
 [protocol [src_port_list [dst_port_list]]]
- [パラメータ] ◦ *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*IP パケットの始点 IP アドレス
- *prefix_len*プレフィックス長
- *dst_address*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。
- *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。
- [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

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

22.6.2 IPv6 フィルタの適用

[入力形式] **ipv6 interface secure filter direction filter_list [filter_list...]**
ipv6 pp secure filter direction filter_list [filter_list...]
no ipv6 interface secure filter direction
no ipv6 pp secure filter direction

[パラメータ] ○ *interface* LAN インタフェース
 ○ *direction* 方向
 • *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。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

22.6.3 IPv6 動的フィルタの定義

[入力形式] **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...]

[パラメータ] ○ *dyn_filter_num* 動的フィルタ番号 (1..21474836)
 ○ *srcaddr* 始点 IPv6 アドレス
 ○ *dstaddr* 終点 IPv6 アドレス
 ○ *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時間 (秒)

[説明] IPv6 の動的フィルタを定義する。1 つ目の書式では、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。2 つ目の書式では、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。

[デフォルト値] *syslog* = on
timeout = 60

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

22.7 トンネリング

22.7.1 トンネルインタフェースの種別の設定

[入力形式] **tunnel encapsulation type**
no tunnel encapsulation

[パラメータ] ○ *type*..... トンネルインタフェースの種別
 • *ipsec*.....IPsec tunnel mode
 • *ipip*.....IPv6 over IPv4 tunnel または IPv4 over IPv6 tunnel
 • *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。

[デフォルト値] ipsec

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

22.7.2 トンネルインタフェースの端点 IP アドレスの設定

[入力形式] **tunnel endpoint address [local] remote**
no tunnel endpoint address [[local] remote]

[パラメータ] ○ *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 の種別が揃ってはいない。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 IPv4 トンネルが利用できる。

local を省略した場合は、適当なインタフェースの IP アドレスが利用される。

[ノート] このコマンドにより設定した IP アドレスが利用されるのは、**tunnel encapsulation** コマンドの設定値が *ipip* の場合だけである。IPsec トンネルでは、トンネル端点は **ipsec ike local address** 及び **ipsec ike remote address** コマンドにより設定される。PPTP サーバの Anonymous で受ける場合には設定する必要はない。

[デフォルト値] IP アドレスは設定されていない

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

22.8 管理ツール

22.8.1 ping の実行

[入力形式] **ping6 destination [count]**
ping6 destination scope_id [count]
ping6 destination interface [count]
ping6 destination pp pp_num [count]

[パラメータ] ○ *destination*.....送信する宛先の IPv6 アドレス、または名前
 ○ *scope_id*スコープ ID
 ○ *interface*LAN インタフェース
 ○ *pp_num*PP 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 ID は、**show ipv6 address** コマンドで表示できる。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

22.8.2 traceroute の実行

【入力形式】 **traceroute6** *destination*

【パラメータ】 ◦ *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。

【適用モデル】

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

23. スケジュール

23.1 スケジュールの設定

[入力形式] **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*]...]

[パラメータ] ○ *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	日の設定例	設定内容
1,2	1月と2月	1	1日のみ
2-	2月から12月まで	1,2	1日と2日
2-7	2月から7月まで	2-	2日から月末まで
-7	1月から7月まで	2-7	2日から7日まで
*	毎月	-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の番号
 ○ *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。
 2、3 番目の形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** で始まるコマンド、
date、**help**、**login password**、**login timer**、**ping**、**line type**、**quit**、**remote setup**、**save**、**show** で始まるコマンド、**time**、**timezone**、**traceroute**

[ノート] 入力時、*command* パラメータに対して TAB キーによるコマンド補完は行わぬが、シンタックスエラーなどは実行時まで検出されない。**schedule at** コマンドにより指定されたコマンドを実行する場合には、何を実行しようとしたかを INFO タイプの SYSLOG に出力する。
date に数字と曜日を混在させて指定はできない。
startup を指定したスケジュールはルータ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

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

24. 操作

24.1 相手先情報番号の選択

[入力形式] **pp select peer_num**

[パラメータ] ○ *peer_num*

- 相手先情報番号
- none 相手を選択しない
- anonymous..... ISDN 番号が不明である相手の設定

[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。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

24.2 設定に関する操作

24.2.1 管理ユーザへの移行

[入力形式] **administrator**

[パラメータ] 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。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

24.2.2 終了

[入力形式] **quit**
quit save
exit
exit save

[パラメータ] ○ 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。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

24.2.3 設定内容の保存

[入力形式] **save**
save [filename [comment]]

[パラメータ] ○ *filename* 設定を保存するファイル名

- 0..9..... 内蔵 Flash ROM の設定ファイル (0..9)
- ext0:*filename*..... PCMCIA Flash ATA カードの設定ファイル

○ *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。
第 2 書式は、RTX1000、RTX2000 と RT300i 用のコマンドで、設定を保存する
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。
RTX2000 では *filename* として 0..9 のみ指定可能。RTX1000 では *filename* として 0 のみ指定可能。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

24.2.4 設定ファイルの削除

[入力形式] **delete config file**

[パラメータ] ◦ *file*削除するファイル名
 • 内蔵フラッシュ ROM の設定ファイル (0..9)
 • *ext0:name* PCMCIA Flash ATA カードの設定ファイル

[説明] 保存されている設定ファイルを削除する。
 RTX2000 では *filename* として 0..9 のみ指定可能。RTX1000 では *filename* として 0 のみ指定可能。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

24.2.5 実行形式ファームウェアファイルの削除

[入力形式] **delete exec file**

[パラメータ] ◦ *file*削除するファイル名
 • *ext0:name* PCMCIA Flash ATA カードの設定ファイル

[説明] PCMCIA Flash ATA カードに保存されている実行形式ファームウェアファイルを削除する。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

24.2.6 設定ファイルの一覧

[入力形式] **show config list**
less config list

[パラメータ] 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。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

24.2.7 設定の初期化

[入力形式] **cold start**

[パラメータ] 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。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

24.2.8 遠隔地のルータの設定

[入力形式]	remote setup interface [isdn_num[/sub_address]] remote setup interface dlcid=dlci														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>interface</i> BRI、PRI インタフェース名 ○ <i>isdn_num</i> ISDN 番号 ○ <i>sub_address</i> ISDN サブアドレス (0x21 から 0x7e の ASCII 文字列) ○ <i>dlci</i> フレームリレーの DLCI 番号 														
[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。 インタフェースには BRI、PRI とともに利用でき、また、ISDN、専用線、フレームリレーいずれの場合でも設定できる。														
[ノート]	専用線の場合は、 <i>isdn_num</i> 、 <i>sub_address</i> パラメータは不要。														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

24.2.9 遠隔地のルータからの設定に対する制限

[入力形式]	remote setup accept isdn_num [/sub_address] [isdn_num_list] remote setup accept any remote setup accept none														
[パラメータ]	<ul style="list-style-type: none"> ○ <i>isdn_num</i> ISDN 番号 ○ <i>sub_address</i> ISDN サブアドレス (0x21 から 0x7e の ASCII 文字列) ○ <i>isdn_num_list</i> 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 ○ <i>any</i> すべての遠隔地のルータからの設定を許可する ○ <i>none</i> すべての遠隔地のルータからの設定を拒否する 														
[説明]	自分のルータの設定を許可する相手先を設定する。														
[デフォルト値]	any														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

24.3 動的情報のクリア操作

24.3.1 ARP テーブルのクリア

[入力形式]	clear arp														
[パラメータ]	なし														
[説明]	ARP テーブルをクリアする。														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

24.3.2 IP の動的経路情報のクリア

[入力形式]	clear ip dynamic routing														
[パラメータ]	なし														
[説明]	動的に設定された IP の経路情報をクリアする。														
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 12.5%;">RTX2000</td> <td style="width: 12.5%;">RTX1000</td> <td style="width: 12.5%;">RT300i</td> <td style="width: 12.5%;">RT140p</td> <td style="width: 12.5%;">RT140f</td> <td style="width: 12.5%;">RT140i</td> <td style="width: 12.5%;">RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

24.3.3 IPX の動的経路情報のクリア

- [入力形式] **clear ipx dynamic routing**
- [パラメータ] なし
- [説明] 動的に設定された IPX の経路情報をクリアする。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

24.3.4 IPX の動的 SAP 情報のクリア

- [入力形式] **clear ipx dynamic sap**
- [パラメータ] なし
- [説明] IPX SAP テーブル中、動的に得られた SAP 情報をクリアする。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

24.3.5 ブリッジのラーニング情報のクリア

- [入力形式] **clear bridge learning**
- [パラメータ] なし
- [説明] 動的に受け取ったブリッジのラーニング情報をすべて消去する。
- [ノート] **bridge interface learning add** コマンドで設定したものは消去されない。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

24.3.6 ログのクリア

- [入力形式] **clear log**
- [パラメータ] なし
- [説明] ログをクリアする。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

24.3.7 アカウントのクリア

- [入力形式] **clear account**
clear account interface
clear account pp [peer_num]
- [パラメータ] ◦ *interface*BRI、PRI インタフェース名
 ◦ *peer_num*.....相手先情報番号、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 (1 番目の入力形式では、すべての合計) に関するアカウントをクリアする。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

24.3.8 InARP のクリア

- [入力形式] **clear inarp** [*peer_num*]
- [パラメータ] ◦ *peer_num* 相手先情報番号、省略時は現在選択している相手先
- [説明] InARP で得られた相手 IP アドレスをクリアし、InARP が on なら再度 InARP を開始する。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

24.3.9 DNS キャッシュのクリア

- [入力形式] **clear dns cache**
- [パラメータ] なし
- [説明] DNS リカーシブサーバで持っているキャッシュをクリアする。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

24.3.10 PRI のステータス情報のクリア

- [入力形式] **clear pri status** *pri*
- [パラメータ] ◦ *pri* PRI 番号 (1..4)
- [説明] PRI のステータス情報をクリアする。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

24.3.11 NAT アドレステーブルのクリア

- [入力形式] **clear nat descriptor dynamic** *nat_descriptor*
- [パラメータ] ◦ *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。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

24.3.12 インタフェースの NAT アドレステーブルのクリア

- [入力形式] **clear nat descriptor interface dynamic** *interface*
clear nat descriptor interface dynamic pp *peer_num*
clear nat descriptor interface dynamic tunnel *tunnel_num*
- [パラメータ] ◦ *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。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

24.3.13 IPv6 の動的経路情報の消去[入力形式] **clear ipv6 dynamic routing**

[説明] 経路制御プロトコルが得た IPv6 の経路情報を消去する。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

24.3.14 近隣キャッシュの消去[入力形式] **clear ipv6 neighbor cache**

[説明] 近隣キャッシュを消去する。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

24.4 その他の操作**24.4.1 相手先の使用許可の設定**[入力形式] **pp enable peer_num**
no pp enable[パラメータ] ◦ *peer_num*

- 相手先情報番号
- anonymous
- all

[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。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

24.4.2 相手先の使用不許可の設定[入力形式] **pp disable peer_num**[パラメータ] ◦ *peer_num*

- 相手先情報番号
- anonymous
- all

[説明] 相手先を使用できない状態にする。
相手先の設定を行う場合は disable 状態であることが望ましい。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

24.4.3 再起動

[入力形式]	restart restart [<i>binary</i>][<i>file</i>]														
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>binary</i>..... PCMCIA Flash ATA カードの実行形式ファイル名 ◦ <i>file</i>..... 起動時の設定ファイル名 <ul style="list-style-type: none"> • 内蔵フラッシュ ROM の設定ファイル (0..9) • PCMCIA Flash ATA カードの設定ファイル名 														
[説明]	第 2 書式は RT300i 専用のコマンド。ルータを再起動する。第 2 の書式では起動時の設定ファイルを指定できる。														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td style="padding: 2px 10px;">RTX2000</td> <td style="padding: 2px 10px;">RTX1000</td> <td style="padding: 2px 10px;">RT300i</td> <td style="padding: 2px 10px;">RT140p</td> <td style="padding: 2px 10px;">RT140f</td> <td style="padding: 2px 10px;">RT140i</td> <td style="padding: 2px 10px;">RT140e</td> </tr> <tr> <td style="padding: 2px 10px;">RT105p</td> <td style="padding: 2px 10px;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

24.4.4 インタフェースの再起動

[入力形式]	interface reset <i>interface</i> [<i>interface</i> ...]														
[パラメータ]	◦ <i>interface</i> インタフェース名														
[説明]	<p>指定したインタフェースを再起動する。</p> <p>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。</p> <p>BRI、PRI 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。</p> <p>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。</p>														
[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 bind 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。														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td style="padding: 2px 10px;">RTX2000</td> <td style="padding: 2px 10px;">RTX1000</td> <td style="padding: 2px 10px;">RT300i</td> <td style="padding: 2px 10px;">RT140p</td> <td style="padding: 2px 10px;">RT140f</td> <td style="padding: 2px 10px;">RT140i</td> <td style="padding: 2px 10px;">RT140e</td> </tr> <tr> <td style="padding: 2px 10px;">RT105p</td> <td style="padding: 2px 10px;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

24.4.5 PP インタフェースの再起動

[入力形式]	interface reset pp [<i>pp_num</i>]														
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>pp_num</i> <ul style="list-style-type: none"> • 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。														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td style="padding: 2px 10px;">RTX2000</td> <td style="padding: 2px 10px;">RTX1000</td> <td style="padding: 2px 10px;">RT300i</td> <td style="padding: 2px 10px;">RT140p</td> <td style="padding: 2px 10px;">RT140f</td> <td style="padding: 2px 10px;">RT140i</td> <td style="padding: 2px 10px;">RT140e</td> </tr> <tr> <td style="padding: 2px 10px;">RT105p</td> <td style="padding: 2px 10px;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

24.4.6 発信

[入力形式]	connect <i>peer_num</i>														
[パラメータ]	◦ <i>peer_num</i> 発信相手の相手先情報番号														
[説明]	手動で発信する。														
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td style="padding: 2px 10px;">RTX2000</td> <td style="padding: 2px 10px;">RTX1000</td> <td style="padding: 2px 10px;">RT300i</td> <td style="padding: 2px 10px;">RT140p</td> <td style="padding: 2px 10px;">RT140f</td> <td style="padding: 2px 10px;">RT140i</td> <td style="padding: 2px 10px;">RT140e</td> </tr> <tr> <td style="padding: 2px 10px;">RT105p</td> <td style="padding: 2px 10px;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

24.4.7 切断

[入力形式] **disconnect** *peer_num*

- [パラメータ]
- *peer_num*
 - 切断する相手先情報番号
 - all.....すべて
 - anonymous.....anonymous のすべて
 - anonymous1..anonymous16.....指定した anonymous

[説明] 手動で切断する。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

24.4.8 ping

[入力形式] **ping** [-s *datalen*] [-c *count*] *host*

- [パラメータ]
- *datalen*データ長 (64 .. 65535)
 - *count*
 - 実行回数 (1..21474836)
 - *host*
 - ping をかけるホストの IP アドレス (xxx.xxx.xxx.xxx (xxx は 10 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、相手からの応答があったかどうかだけを表示する。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

24.4.9 traceroute

[入力形式] **traceroute** *host* [noresolv]

- [パラメータ]
- *host*
 - traceroute をかけるホストの IP アドレス (xxx.xxx.xxx.xxx (xxx は 10 進数))
 - traceroute をかけるホストの名称
 - noresolvDNS による解決を行わないためのキーワード

[説明] 指定したホストまでの経路を調べて表示する。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

24.4.10 telnet

- [入力形式] **telnet** *host* [*port* [*mode* [*negotiation* [*abort*]]]]
- [パラメータ]
- *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
 - 10 進数
 - ポート番号の二一モニック
 - 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
 - 10 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 サーバなどへの接続のための透過的な通信を行う。
line モードは、入力行を編集して行単位の通信を行う。行編集の終了は、改行コード (CR:0x0d または LF:0x0a) の入力で判断する。

ポート番号による機能自動選択について

1. telnet 通信の動作モードの自動選択
 port 番号が 23 の場合は文字単位モードとなり、そうでない場合は行単位モードとなる。
2. telnet オプションのネゴシエーションの自動選択
 port 番号が 23 の場合はネゴシエーションし、そうでない場合はネゴシエーションしない。

[デフォルト値] *port* = 23
mode = *auto*
negotiation = *auto*
abort = 29

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

24.4.11 telnet サーバ機能の ON/OFF の設定

- [入力形式] **telnetd** *service* *service*
- [パラメータ]
- *service*
 - *on* telnet サーバ機能を有効にする
 - *off* telnet サーバ機能を停止させる

[説明] telnet サーバ機能の利用を選択する。

[ノート] telnet サーバが停止している場合、telnet サーバはアクセス要求に一切応答しない。

[デフォルト値] *on*

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

24.4.12 telnet サーバ機能の listen ポートの設定[入力形式] **telnetd listen port**[パラメータ] ◦ *port*.....telnet サーバ機能の待ち受け (listen) ポート番号 (1..65535)

[説明] telnet サーバ機能の 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。

[デフォルト値] 23

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

24.4.13 telnet サーバへアクセスできるホストの IP アドレスの設定[入力形式] **telnetd host ip_range [ip_range...]**[パラメータ] ◦ *ip_range*

- telnet サーバ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
- lan全ポートに属するネットワーク内ならば許可する
- interfaceLAN インタフェース名、指定 LAN インタフェースに属する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

[説明] telnet サーバ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。
lan の場合、primary および secondary が clear では無く、ネットワークアドレスと directed broadcast address を除くホストアドレスからのリクエストを許可する。
設定後の新しい telnet 接続から適用される。

[デフォルト値] any

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

24.4.14 PRI のループバックの実行

【入力形式】 **pri loopback active pri a data**
pri loopback active pri timeslot bead num data

- 【パラメータ】
- *pri* PRI 番号 (1..4)
 - *a* ループバック A を示すキーワード
 - *timeslot* タイムスロットループバックを示すキーワード
 - *data* 送信データパターン (1..4)

<i>data</i>	擬似ランダムパターン
1	$2^6 - 1$
2	$2^7 - 1$
3	$2^9 - 1$
4	$2^{11} - 1$

- *bead* 先頭タイムスロット番号 (1..24)
- *number* タイムスロット数 (1..24)

【説明】 指定したデータパターンを送信して、ループバックテストを行う。コマンドを実行する場合に、管理パスワードを入力する必要がある。a キーワードの場合は、24B すべてのタイムスロットがループバックする。ループバックするポイントはルータの PRI コネクタの直前であり、PRI コネクタにケーブルを接続しているとその先の機器を破壊する可能性があるため、必ずケーブルを抜いてからテストを行わなければならない。timeslot キーワードの場合には、指定したタイムスロットに対してだけループバックテストを行う。データがループバックするのは、接続相手のルータなので、あらかじめ相手のルータをループバックを待ち受けるモードに設定しておく必要がある。ループバックテストが終了すると、自動的に通信モードに復帰する。

【ノート】 ループバック A の場合は、PRI コネクタを外した状態で行う必要がある。タイムスロットループバックを実行する前に、相手ルータはループバック待ち受け状態になっている必要がある。save コマンドを実行しても不揮発性メモリには保存されない。専用回線に対してのみ実行可能。RT105p ではタイムスロットキーワードの指定はできない。

【適用モデル】

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

24.4.15 PRI のループバック待ち受けの設定

[入力形式] **pri loopback passive pri remote**
pri loopback passive pri payload
pri loopback passive pri timeslot bead number
pri loopback passive pri off

[パラメータ] ◦ *pri*PRI 番号 (1..4)
◦ *remote*ループバックポイントが PRI コネクタであることを示すキーワード
◦ *payload*ループバックポイントがペイロードであることを示すキーワード
◦ *timeslot*タイムスロットループバックを示すキーワード
◦ *bead*先頭タイムスロット番号 (1..24)
◦ *number*タイムスロット数 (1..24)

[説明] 相手からのタイムスロットループバックテストに対して待ち受けモードに入る。コマンドを実行する場合に、管理パスワードを入力する必要がある。また、このコマンド実行後には、通常の通信は行なえなくなる。*remote* および *payload* キーワードの場合は、24B すべてのタイムスロットがループバックされる。*timeslot* キーワードの場合には、指定したタイムスロットに対してだけループバックテストされる。**pri loopback passive off** コマンドを実行すると、ループバックテストを終了して待ち受けモードから通常の通信モードへ復帰する。

[ノート] ループバックテストの結果は、実行側にしか表示されない。RT140p ではディップスイッチを変更して再起動することによってもこのコマンドと同様のモードにすることが可能。ただし、ループバックテスト終了後に再びディップスイッチの変更と再起動が必要。**save** コマンドを実行しても不揮発性メモリには保存されない。専用回線に対してのみ実行可能。
RT105p ではタイムスロットキーワードの指定はできない。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

24.4.16 ファームウェアファイルを内蔵フラッシュ ROM にコピー

[入力形式] **copy exec file internal**

[パラメータ] ◦ *file*コピー元のファイル名
 • *ext0:name* PCMCIA Flash ATA カードの実行形式ファイル名
◦ *internal*保存先を示すキーワード

[説明] Flash ATA カード上の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。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

24.4.17 IPv4 動的フィルタの接続管理情報の削除

[入力形式] **disconnect ip connection session_id [channel_id]**

[パラメータ] ◦ *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。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

24.4.18 IPv6 動的フィルタのコネクション管理情報の削除

【入力形式】 **disconnect ipv6 connection** *session_id* [*channel_id*]

【パラメータ】

- *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。

【適用モデル】	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

25. 設定の表示

25.1 機器設定の表示

[入力形式] **show environment**

[パラメータ] なし

[説明] 以下の項目が表示される。

- システムのリビジョン
- CPU、メモリの使用量 (%)
- 動作しているファームウェアファイルと起動時に使用した設定ファイルの名前
- 起動時刻、現在時刻、起動してから現在までの経過時間
- セキュリティクラス
- 電源、ファン、内部温度の状態 (RT300i のみ)

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

25.2 すべての設定内容の表示

[入力形式] **show config**
less config

[パラメータ] なし

[説明] 設定されたすべての設定内容を表示する。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

25.3 指定した PP の設定内容の表示

[入力形式] **show config pp** [peer_num]
less config pp [peer_num]

[パラメータ] ◦ peer_num

- 相手先情報番号
- anonymous
- peer_num 省略時、選択されている相手について表示する

[説明] **show config**、**less config** コマンドの表示の中から、指定した相手先情報番号に関するものだけを表示する。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

25.4 ファイル情報の一覧の表示

[入力形式] **show file list** location
less file list location

[パラメータ] ◦ location表示するファイルのある位置

- internal.....内蔵フラッシュ ROM
- ext0外付け Flash ATA カード

[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。
RTX2000 と RTX1000 では location として internal のみ指定可能。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

25.5 マスタクロックを得ている回線の表示

【入力形式】 **show line masterclock**

【パラメータ】 なし

【説明】 通信に使用しているクロックを得ている回線を表示する。フリーラン状態の場合はその旨を表示する。

【適用モデル】

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

26. 状態の表示

26.1 ARP テーブルの表示

[入力形式] **show arp**

[パラメータ] なし

[説明] ARP テーブルを表示する。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

26.2 インタフェースの状態の表示

[入力形式] **show status interface**

[パラメータ] ◦ *interface*LAN、BRI、PRI のインタフェース名

[説明] インタフェースの状態を表示する。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

26.3 各相手先の状態の表示

[入力形式] **show status pp [peer_num]**

[パラメータ] ◦ *peer_num*

- 相手先情報番号
- anonymous
- *peer_num* 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

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

26.4 DHCP サーバの状態の表示

- [入力形式] **show status dhcp**
- [パラメータ] 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 IP アドレス数
 - 除外 IP アドレス数
 - 割り当て中 IP アドレス数
 - 利用可能アドレス数 (うち予約済 IP アドレス数)

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

26.5 IP の経路情報テーブルの表示

- [入力形式] **show ip route [destination]**
- [パラメータ] ◦ *destination*..... 相手先 IP アドレス
省略時、経路情報テーブル全体を表示する。
- [説明] IP の経路情報テーブルまたは相手先 IP アドレスへのゲートウェイを表示する。
ネットマスクは設定時の表現に関わらず連続するビット数で表現される。
フレームリレーの場合は DLCI の値が表示される。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

26.6 IPX の経路情報テーブルの表示

- [入力形式] **show ipx route**
- [パラメータ] なし
- [説明] IPX の経路情報テーブルを表示する。
フレームリレーの場合は DLCI の値が表示される。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

26.7 IPv6 の経路情報の表示

- [入力形式] **show ipv6 route**
- [説明] IPv6 の経路情報を表示する。

[適用モデル]	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
	RT105p	RT105i	RT105e				

200 26. 状態の表示

26.8 近隣キャッシュの表示

- [入力形式] **show ipv6 neighbor cache**
- [パラメータ] なし
- [説明] 近隣キャッシュの状態を表示する。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

26.9 SAP テーブルの表示

- [入力形式] **show ipx sap**
- [パラメータ] なし
- [説明] IPX SAP テーブルを表示する。
非 ASCII 文字は 8 進数で表示される。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

26.10 IPXWAN の状態の表示

- [入力形式] **show ipx ipxwan** [*peer_num*]
- [パラメータ] ◦ *peer_num*
- 相手先情報番号
 - anonymous
 - *peer_num* 省略時、選択されている相手先について表示する。
- [説明] IPXWAN の状態を表示する。
- [ノート] 複数 WAN ポートモデルでは *leased* を指定することはできない。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

26.11 ブリッジのラーニング情報の表示

- [入力形式] **show bridge learning**
- [パラメータ] なし
- [説明] ブリッジの MAC アドレスのラーニング情報を表示する。
フレームリレーの場合は DLCI の値が表示される。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

26.12 RIP で得られた経路情報の表示

- [入力形式] **show ip rip table**
- [パラメータ] なし
- [説明] RIP で得られた経路情報を表示する。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

26.13 IPsec の SA の表示

【入力形式】	show ipsec sa [<i>id</i>] show ipsec sa gateway [<i>gateway_id</i>] [detail]														
【パラメータ】	<ul style="list-style-type: none"> ○ <i>id</i> <ul style="list-style-type: none"> • SA の識別子 • 省略時はすべての SA について表示する ○ <i>gateway_id</i> <ul style="list-style-type: none"> • 指定されたセキュリティ・ゲートウェイの SA のサマリを表示する。 • 省略時はすべてのセキュリティ・ゲートウェイの SA のサマリを表示する。 ○ detail SA の詳細な情報を表示する。 														
【説明】	IPsec の SA の状態を表示する。 <i>id</i> で与えられた識別子を持つ SA の情報を表示する。														
【適用モデル】	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

26.14 VRRP の情報の表示

【入力形式】	show status vrrp [<i>interface</i> [<i>vrid</i>]]														
【パラメータ】	<ul style="list-style-type: none"> ○ <i>interface</i> LAN インタフェース名 ○ <i>vrid</i> VRRP グループ ID (1..255) 														
【説明】	VRRP の情報を表示する。														
【適用モデル】	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

26.15 動的 NAT ディスクリプタのアドレスマップの表示

【入力形式】	show nat descriptor address [<i>nat_descriptor</i>]														
【パラメータ】	<ul style="list-style-type: none"> ○ <i>nat_descriptor</i> <ul style="list-style-type: none"> • 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】	<i>nat_descriptor</i> を省略した場合はすべての NAT ディスクリプタ番号について表示する。 動的な NAT ディスクリプタのアドレスマップを表示する。														
【適用モデル】	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

26.16 動作中の NAT ディスクリプタの適用リストの表示

【入力形式】	show nat descriptor interface bind <i>interface</i> show nat descriptor interface bind pp show nat descriptor interface bind tunnel														
【パラメータ】	○ <i>interface</i> 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。														
【適用モデル】	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT140p</td> <td>RT140f</td> <td>RT140i</td> <td>RT140e</td> </tr> <tr> <td>RT105p</td> <td>RT105i</td> <td>RT105e</td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e	RT105p	RT105i	RT105e				
RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e									
RT105p	RT105i	RT105e													

26.17 LAN インタフェースの NAT ディスクリプタのアドレスマップの表示

[入力形式] **show nat descriptor interface address** *interface*
show nat descriptor interface address pp *peer_num*
show nat descriptor interface address tunnel *tunnel_num*

[パラメータ] ◦ *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。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

26.18 OSPF 情報の表示

[入力形式] **show status ospf** *info*

[パラメータ] ◦ *info*表示する情報の種類
 • *database*OSPF のデータベース
 • *neighbor*近隣ルータ
 • *interface*各インタフェースの状態
 • *virtual-link*バーチャルリンクの状態

[説明] OSPF の各種情報を表示する。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

26.19 DHCP クライアントの状態の表示

[入力形式] **show status dhcp**

[パラメータ] 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
 - 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
 - ゲートウェイ

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

26.20 BGP の状態の表示

[入力形式] **show status bgp** *info*

[パラメータ] ◦ *info*表示する情報の種類
 • *neighbor*近隣ルータの情報

[説明] BGP の各種の状態を表示する。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

26.21 動的フィルタによって管理されている接続の表示

【入力形式】 **show ip connection** [*interface* [*interface_num*] [*direction*]]

- 【パラメータ】
- *interface*
 - lan/lan1/lan2
 - pp
 - tunnel
 - *interface_num* PP/TUNNEL インタフェースの番号
 - *direction* 方向
 - in
 - out

【説明】 指定したインタフェースについて、動的なフィルタによって管理されている接続を表示する。インタフェースを指定しないときには、すべてのインタフェースの情報を表示する。

【適用モデル】

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

26.22 IPv6 の RIP テーブルの表示

【入力形式】 **show ipv6 rip table**

【パラメータ】 なし

【説明】 IPv6 の RIP テーブルを表示する。

【適用モデル】

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

26.23 IPv6 の動的フィルタによって管理されている接続の表示

【入力形式】 **show ipv6 connection** [*interface* [*interface_number*] [*direction*]]

- 【パラメータ】
- *interface* インタフェース
 - LAN インタフェース名
 - pp
 - tunnel
 - *interface_number* PP/TUNNEL インタフェースの番号
 - *direction*
 - in 入力方向
 - out 出力方向

【説明】 指定したインタフェースについて、動的なフィルタによって管理されている接続を表示する。インタフェースを指定しないときには、すべてのインタフェースの情報を表示する。

【適用モデル】

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

27. ログイン

27.1 ログの表示

- [入力形式] **show log**
less log
- [パラメータ] なし
- [説明] パワーオンからのログを表示する。
- パワーオンの日時
 - 不揮発性メモリに設定を保存した日時
 - 設定のためのログインの記録
 - 接続した日時、発着
 - 回線の種類
 - 接続失敗の原因
 - 切断した日時、接続時間、ISDN 料金

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				

27.2 アカウントの表示

- [入力形式] **show account**
show account interface
show account pp [peer_num]
- [パラメータ] ◦ *interface*BRI、PRI インタフェース名
◦ *peer_num*
 - 相手先情報番号
 - *anonymous*
 - *peer_num* 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] 電源 OFF や再起動により、それまでの課金情報がクリアされる。
課金額は通信の切断時に NTT から ISDN で通知される料金情報を集計しているため、割引サービスなどを利用している場合には、最終的に NTT から請求される料金とは異なる場合がある。また、NTT 以外の通信事業者を利用して通信した場合には料金情報は通知されないため、アカウントとしても集計されない。

[適用モデル]

RTX2000	RTX1000	RT300i	RT140p	RT140f	RT140i	RT140e
RT105p	RT105i	RT105e				