

YAMAHA *Broadband & Remote ROUTER*

コマンドリファレンス

Rev.6.03.28

Rev.7.00.26

Rev.7.01.17



- 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。
 - ※ Stac LZS は米国 Hi/fn 社の登録商標です。

目次

1. コマンドリファレンスの見方	21
1.1 対応するプログラムのリビジョン	21
1.2 コマンドリファレンスの見方	21
1.3 インタフェース名について	21
1.4 no で始まるコマンドの入力形式について	21
1.5 コマンドの入力文字数とエスケープシーケンスについて	22
1.6 相手先情報番号のモデルによる違いについて	22
1.7 コマンドの仕様変更について	22
2. コマンドの使い方	24
2.1 コンソールについて	24
2.1.1 コンソールによる設定手順	25
2.1.2 CONSOLE または SERIAL ポートからの設定	26
2.1.3 TELNET による設定	28
2.1.4 リモートセットアップ	29
2.2 TFTP について	29
2.2.1 TFTP による設定手順	30
2.2.2 設定ファイルの読み出し	30
2.2.3 設定ファイルの書き込み	31
3. ヘルプ	32
3.1 コンソールに対する簡易説明の表示	32
3.2 コマンド一覧の表示	32
4. 機器の設定	33
4.1 ログインパスワードの設定	33
4.2 管理パスワードの設定	33
4.3 セキュリティクラスの設定	33
4.4 現在の日付けの設定	33
4.5 現在の時刻の設定	34
4.6 タイムゾーンの設定	34
4.7 リモートホストによる時計の設定	34
4.8 NTP による時計の設定	34
4.9 コンソールのプロンプト表示の設定	35
4.10 コンソールの言語とコードの設定	35
4.11 コンソールの表示文字数の設定	35
4.12 コンソールの表示行数の設定	35
4.13 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	36
4.14 SYSLOG を受けるホストの IP アドレスの設定	36
4.15 SYSLOG ファシリティの設定	36
4.16 NOTICE タイプの SYSLOG を出力するか否かの設定	36
4.17 INFO タイプの SYSLOG を出力するか否かの設定	37
4.18 DEBUG タイプの SYSLOG を出力するか否かの設定	37
4.19 SYSLOG パケットの始点ポート番号の設定	37
4.20 電源の設定	37
4.21 マスタクロック用インタフェースの設定	38
4.22 温度監視の閾値の設定	38
4.23 ファストバス機能の設定	38
4.24 LAN インタフェースの動作タイプの設定	39
4.25 ログインタイマの設定	40
4.26 TFTP によりアクセスできるホストの IP アドレスの設定	40
5. ISDN 関連の設定	41
5.1 共通の設定	41
5.1.1 BRI 回線の種類の指定	41
5.1.2 自分の ISDN 番号の設定	41
5.1.3 PP で使用するインタフェースの設定	41
5.1.4 課金額による発信制限の設定	42
5.1.5 PIAFS の発信方式の設定	42
5.1.6 PIAFS の着信を許可するか否かの設定	43

5.1.7	PIAFS 接続時の起動側の指定	43
5.1.8	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	43
5.1.9	常時接続の設定	44
5.1.10	終端抵抗の設定	44
5.2	相手側の設定	44
5.2.1	相手 ISDN 番号の設定	44
5.2.2	相手への発信順序の設定	45
5.2.3	自動接続の設定	45
5.2.4	着信許可の設定	45
5.2.5	発信許可の設定	46
5.2.6	再発信抑制タイマの設定	46
5.2.7	エラー切断後の再発信禁止タイマの設定	46
5.2.8	相手にコールバック要求を行うか否かの設定	46
5.2.9	相手からのコールバック要求に応じるか否かの設定	47
5.2.10	コールバック要求タイプの設定	47
5.2.11	コールバック受け入れタイプの設定	47
5.2.12	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	47
5.2.13	コールバックタイマの設定	48
5.2.14	コールバック待機タイマの設定	48
5.2.15	ISDN 回線を切断するタイマ方式の指定	48
5.2.16	切断タイマの設定 (ノーマル)	49
5.2.17	切断タイマの設定 (ファスト)	49
5.2.18	切断タイマの設定 (強制)	49
5.2.19	入力切断タイマの設定 (ノーマル)	50
5.2.20	出力切断タイマの設定 (ノーマル)	50
5.2.21	課金単位時間方式での課金単位時間と監視時間の設定	51
6.	フレームリレー関連の設定	52
6.1	カプセル化の種類の設定	52
6.2	DLCI の設定	53
6.3	DLCI ごとのパラメータの設定	53
6.4	PVC 状態確認手順の設定	53
6.5	InARP 使用の設定	54
6.6	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	54
6.7	FR 圧縮機能の設定	54
6.8	輻輳制御をするか否かの設定	55
6.9	回線に対する送信順序方式の設定	55
6.10	指定パケットに DE ビットを立てるか否かの設定	55
7.	PRI 関連の設定	56
7.1	PRI 回線の種類の設定	57
7.2	情報チャンネルとタイムスロットの設定	57
7.3	PP で使用するインタフェースの設定	57
8.	IP の設定	58
8.1	インタフェース共通の設定	58
8.1.1	IP パケットを扱うか否かの設定	58
8.1.2	IP アドレスの設定	58
8.1.3	セカンダリ IP アドレスの設定	59
8.1.4	インタフェースの MTU の設定	59
8.1.5	echo, discard, time サービスを動作させるか否かの設定	59
8.1.6	IP の静的経路情報の設定	60
8.1.7	IP パケットのフィルタの設定	61
8.1.8	フィルタセットの定義	62
8.1.9	Source-route オプション付き IP パケットをフィルタアウトするか否かの設定	62
8.1.10	ディレクテッドブロードキャストパケットをフィルタアウトするか否かの設定	62
8.1.11	動的フィルタの定義	63
8.1.12	動的フィルタのタイムアウトの設定	63
8.1.13	侵入検知機能の動作の設定	64
8.1.14	TCP セッションの MSS 制限の設定	64
8.1.15	フィルタリングによるセキュリティの設定	65
8.1.16	フィルタに一致する IP パケットの DF ビットを 0 に書き換えるか否かの設定	65

8.1.17	IP パケットの TOS フィールドの書き換えの設定	66
8.2	代理 ARP の設定	66
8.3	PP 側の設定	67
8.3.1	PP 側 IP アドレスの設定	67
8.3.2	リモート IP アドレスプールの設定	67
8.4	RIP の設定	68
8.4.1	RIP を使用するか否かの設定	68
8.4.2	RIP による経路の優先度の設定	68
8.4.3	RIP パケットの送信に関する設定	68
8.4.4	RIP パケットの受信に関する設定	69
8.4.5	RIP に関して信用できるゲートウェイの設定	69
8.4.6	RIP のフィルタリングの設定	69
8.4.7	RIP で加算するホップ数の設定	70
8.4.8	RIP2 での認証の設定	70
8.4.9	RIP2 での認証キーの設定	70
8.4.10	回線切断時の経路保持の設定	71
8.4.11	回線接続時の PP 側の RIP の動作の設定	71
8.4.12	回線接続時の PP 側の RIP 送出の時間間隔の設定	71
8.4.13	回線切断時の PP 側の RIP の動作の設定	71
8.4.14	回線切断時の PP 側の RIP 送出の時間間隔の設定	72
8.4.15	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	72
8.5	VRRP の設定	72
8.5.1	インタフェース毎の VRRP の設定	72
8.5.2	シャットダウントリガの設定	73
8.6	バックアップの設定	73
8.6.1	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	73
8.6.2	バックアップからの復帰待ち時間の設定	74
8.6.3	PP 経由のキープアライブを使用するか否かの設定	74
8.6.4	PP 経由のキープアライブのログをとるか否かの設定	75
8.6.5	PP 経由のキープアライブの時間間隔の設定	75
8.6.6	専用線ダウン検出時の動作の設定	75
8.6.7	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	76
8.6.8	バックアップからの復帰待ち時間の設定	76
8.6.9	LAN 経由のキープアライブを使用するか否かの設定	76
8.6.10	LAN 経由のキープアライブの時間間隔の設定	77
8.6.11	LAN 経由のキープアライブのログをとるか否かの設定	77
8.6.12	ネットワーク監視機能の設定	77
9.	IPX の設定	78
9.1	インタフェース共通の設定	78
9.1.1	IPX パケットを扱うか否かの設定	78
9.1.2	静的な SAP テーブルの設定	78
9.1.3	IPX SAP Get Nearest Server Request に応答するか否かの設定	78
9.1.4	IPX パケットのフィルタの設定	79
9.2	LAN 側の設定	80
9.2.1	イーサネットフレームタイプの設定	80
9.2.2	LAN 側の IPX ネットワーク番号の設定	80
9.2.3	LAN 側の RIP/SAP ブロードキャストの設定	80
9.2.4	経路情報の追加	81
9.2.5	LAN 側でのフィルタリングによるセキュリティの設定	81
9.3	PP 側相手毎の IPX の設定	81
9.3.1	IPX ルーティング許可の設定	81
9.3.2	PP 側 IPX ネットワーク番号の設定	82
9.3.3	経路情報の追加	82
9.3.4	IPXWAN 使用の設定	82
9.3.5	IPXWAN プライマリネットワーク番号の設定	82
9.3.6	回線接続時の PP 側の RIP/SAP の動作の設定	83
9.3.7	回線接続時の PP 側の RIP/SAP 送出の時間間隔の設定	83
9.3.8	回線切断時の PP 側の RIP/SAP の動作の設定	83

9.3.9	回線切断時のPP側のRIP/SAP送出の時間間隔の設定	83
9.3.10	回線切断時にRIP/SAP情報を保持するか否かの設定	84
9.3.11	Timer/Information Requestの再送間隔と最大再送回数の設定	84
9.3.12	Watchdogパケットに対する代理応答の設定	84
9.3.13	Watchdog代理応答の時間間隔の設定	84
9.3.14	SPXキーブアライブ代理応答を行うか否かの設定	85
9.3.15	SPXキーブアライブ代理応答のタイマの設定	85
9.3.16	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	85
9.3.17	PP側でのフィルタリングによるセキュリティの設定	86
10.	ブリッジの設定	87
10.1	インタフェース共通の設定	87
10.1.1	ブリッジ使用許可の設定	87
10.1.2	ブリッジするインタフェースの設定	87
10.1.3	MACアドレスのラーニングを行うか否かの設定	87
10.1.4	ラーニング情報消去タイマの設定	88
10.1.5	ブリッジのフィルタの設定	88
10.2	LAN側の設定	88
10.2.1	ラーニング情報の設定	88
10.2.2	LAN側でのブリッジのフィルタリングの設定	89
10.3	PP側相手毎のブリッジの設定	89
10.3.1	ラーニング情報の設定	89
10.3.2	PP側でのブリッジのフィルタリングの設定	89
11.	PPPの設定	90
11.1	相手の名前とパスワードの設定	90
11.2	要求する認証タイプの設定	90
11.3	受け入れる認証タイプの設定	91
11.4	自分の名前とパスワードの設定	91
11.5	同一usernameを持つ相手からの二重接続を禁止するか否かの設定	91
11.6	LCP関連の設定	92
11.6.1	Address and Control Field Compressionオプション使用の設定	92
11.6.2	Magic Numberオプション使用の設定	92
11.6.3	Maximum Receive Unitオプション使用の設定	92
11.6.4	Protocol Field Compressionオプション使用の設定	93
11.6.5	lcp-restartパラメータの設定	93
11.6.6	lcp-max-terminateパラメータの設定	93
11.6.7	lcp-max-configureパラメータの設定	93
11.6.8	lcp-max-failureパラメータの設定	93
11.6.9	Configure-Requestをすぐに送信するか否かの設定	94
11.7	PAP関連の設定	94
11.7.1	pap-restartパラメータの設定	94
11.7.2	pap-max-authreqパラメータの設定	94
11.8	CHAP関連の設定	94
11.8.1	chap-restartパラメータの設定	94
11.8.2	chap-max-challengeパラメータの設定	95
11.9	IPCP関連の設定	95
11.9.1	Van Jacobson Compressed TCP/IP使用の設定	95
11.9.2	PP側IPアドレスのネゴシエーションの設定	95
11.9.3	ipcp-restartパラメータの設定	95
11.9.4	ipcp-max-terminateパラメータの設定	95
11.9.5	ipcp-max-configureパラメータの設定	96
11.9.6	ipcp-max-failureパラメータの設定	96
11.9.7	WINSサーバのIPアドレスの設定	96
11.9.8	IPCPのMS拡張オプションを使うか否かの設定	96
11.10	IPXCP関連の設定	97
11.10.1	ipxcp-restartパラメータの設定	97
11.10.2	ipxcp-max-terminateパラメータの設定	97
11.10.3	ipxcp-max-configureパラメータの設定	97
11.10.4	ipxcp-max-failureパラメータの設定	97
11.11	BCP関連の設定	97
11.11.1	LAN Identification使用の設定	97

11.11.2	Tinygram compression 使用の設定	98
11.11.3	bcp-restart パラメータの設定	98
11.11.4	bcp-max-terminate パラメータの設定	98
11.11.5	bcp-max-configure パラメータの設定	98
11.11.6	bcp-max-failure パラメータの設定	98
11.12	MSCBCP 関連の設定	99
11.12.1	mscbcp-restart パラメータの設定	99
11.12.2	mscbcp-maxretry パラメータの設定	99
11.13	CCP 関連の設定	99
11.13.1	全パケットの圧縮タイプの設定	99
11.13.2	ccp-restart パラメータの設定	100
11.13.3	ccp-max-terminate パラメータの設定	100
11.13.4	ccp-max-configure パラメータの設定	100
11.13.5	ccp-max-failure パラメータの設定	100
11.14	IPV6CP 関連の設定	100
11.14.1	IPV6CP を使用するか否かの設定	100
11.15	MP 関連の設定	101
11.15.1	MP を使用するか否かの設定	101
11.15.2	MP の制御方法の設定	101
11.15.3	MP のための負荷閾値の設定	101
11.15.4	MP の最大リンク数の設定	101
11.15.5	MP の最小リンク数の設定	102
11.15.6	MP のための負荷計測間隔の設定	102
11.15.7	MP のパケットを分割するか否かの設定	102
11.16	BACP 関連の設定	102
11.16.1	bacp-restart パラメータ の設定	102
11.16.2	bacp-max-terminate パラメータ の設定	103
11.16.3	bacp-max-configure パラメータ の設定	103
11.16.4	bacp-max-failure パラメータ の設定	103
11.17	BAP 関連の設定	103
11.17.1	bap-restart パラメータの設定	103
11.17.2	bap-max-retry パラメータの設定	103
11.18	PPPoE 関連の設定	104
11.18.1	PPPoE で使用する LAN インタフェースの指定	104
11.18.2	アクセスコンセントレータ名の設定	104
11.18.3	セッションの自動接続の設定	104
11.18.4	セッションの自動切断の設定	104
11.18.5	PADI パケットの最大再送回数の設定	104
11.18.6	PADI パケットの再送時間の設定	105
11.18.7	PADR パケットの最大再送回数の設定	105
11.18.8	PADR パケットの再送時間の設定	105
11.18.9	PPPoE セッションの切断タイマの設定	105
11.18.10	サービス名の指定	105
11.18.11	TCP パケットの MSS の制限の有無とサイズの指定	106
12.	DHCP の設定	107
12.1	DHCP サーバ・リレーエージェント機能	107
12.1.1	DHCP の動作の設定	107
12.1.2	RFC2131 対応動作の設定	108
12.1.3	リースする IP アドレスの重複をチェックするか否かの設定	108
12.1.4	DHCP スコープの定義	109
12.1.5	DHCP 予約アドレスの設定	109
12.1.6	DHCP オプションの設定	111
12.1.7	DHCP サーバの指定の設定	111
12.1.8	DHCP サーバの選択方法の設定	111
12.1.9	DHCP BOOTREQUEST パケットの中継基準の設定	112
12.2	DHCP クライアント機能	112
12.2.1	DHCP クライアントのホスト名の設定	112
12.2.2	DNS サーバアドレスを取得する LAN インタフェースの設定	112
12.2.3	要求する IP アドレスリース期間の設定	113
12.2.4	IP アドレス取得要求の再送回数と間隔の設定	113

12.2.5	DHCP クライアント ID オプションの設定	113
13.	ICMP の設定	114
13.1	IPv4 の設定	114
13.1.1	ICMP Echo Reply を送信するか否かの設定	114
13.1.2	ICMP Mask Reply を送信するか否かの設定	114
13.1.3	ICMP Parameter Problem を送信するか否かの設定	114
13.1.4	ICMP Redirect を送信するか否かの設定	114
13.1.5	ICMP Redirect 受信時の処理の設定	115
13.1.6	ICMP Time Exceeded を送信するか否かの設定	115
13.1.7	ICMP Timestamp Reply を送信するか否かの設定	115
13.1.8	ICMP Destination Unreachable を送信するか否かの設定	115
13.1.9	受信した ICMP のログを記録するか否かの設定	116
13.1.10	ステルス機能の設定	116
13.2	IPv6 の設定	116
13.2.1	ICMP Echo Reply を送信するか否かの設定	116
13.2.2	ICMP Parameter Problem を送信するか否かの設定	116
13.2.3	ICMP Redirect を送信するか否かの設定	117
13.2.4	ICMP Redirect 受信時の処理の設定	117
13.2.5	ICMP Time Exceeded を送信するか否かの設定	117
13.2.6	ICMP Destination Unreachable を送信するか否かの設定	117
13.2.7	受信した ICMP のログを記録するか否かの設定	118
13.2.8	ICMP Packet-Too-Big を送信するか否かの設定	118
13.2.9	ステルス機能の設定	118
14.	トンネリング	119
14.1	トンネルインタフェースの使用許可の設定	119
14.2	トンネルインタフェースの使用不許可の設定	119
14.3	トンネルインタフェースの種別の設定	119
14.4	トンネルインタフェースの端点 IP アドレスの設定	120
15.	IPsec の設定	121
15.1	IPsec の動作の設定	122
15.2	事前共有鍵の登録	122
15.3	設定が異なる場合に鍵交換を拒否するか否かの設定	122
15.4	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	123
15.5	鍵交換の再送回数と間隔の設定	123
15.6	IKE の鍵交換を始動するか否かの設定	123
15.7	相手側のセキュリティ・ゲートウェイの名前の設定	123
15.8	相手側セキュリティ・ゲートウェイの IP アドレスの設定	124
15.9	相手側の ID の設定	124
15.10	自分側のセキュリティ・ゲートウェイの名前の設定	124
15.11	自分側セキュリティ・ゲートウェイの IP アドレスの設定	125
15.12	自分側の ID の設定	125
15.13	IKE キープアライブ機能の設定	125
15.14	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
15.15	IKE が用いる暗号アルゴリズムの設定	126
15.16	受信した IKE パケットを蓄積するキューの長さの設定	126
15.17	IKE が用いるグループの設定	127
15.18	IKE が用いるハッシュアルゴリズムの設定	127
15.19	受信したパケットの SPI 値が無効な値の場合にログに出力するか否かの設定	127
15.20	IKE ペイロードのタイプの設定	128
15.21	IKE の情報ペイロードを送信するか否かの設定	128
15.22	PFS を用いるか否かの設定	128
15.23	XAUTH の設定	128
15.24	IKE のログの種類の設定	129
15.25	ESP を UDP でカプセル化して送受信するか否かの設定	129
15.26	SA 関連の設定	129
15.26.1	SA のポリシーの定義	129
15.26.2	SA の寿命の設定	130
15.26.3	ダンangling SA の動作の設定	130
15.26.4	SA の削除	131
15.26.5	SA の手動更新	131

15.27	トンネルインタフェース関連の設定	131
15.27.1	使用する SA のポリシーの設定	131
15.27.2	IPComp によるデータ圧縮の設定	131
15.27.3	トンネルバックアップの設定	132
15.28	トランスポートモード関連の設定	132
15.28.1	トランスポートモードの定義	132
16.	PPTP 機能の設定	133
16.1	共通の設定	133
16.1.1	PPTP サーバを動作させるか否かの設定	133
16.1.2	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	133
16.1.3	PPTP の動作タイプの設定	133
16.1.4	PPTP ホスト名の設定	134
16.1.5	PPTP パケットのウィンドウサイズの設定	134
16.1.6	PPTP の動作モードの設定	134
16.1.7	PPTP 暗号鍵生成のための要求する認証方式の設定	134
16.1.8	PPTP 暗号鍵生成のための受け入れ可能な認証方式の設定	135
16.1.9	PPTP のコネクション制御の syslog を出力するか否かの設定	135
16.2	リモートアクセス VPN 機能	135
16.2.1	PPTP トンネルの切断タイマの設定	135
16.2.2	PPTP トンネルの端点の名前の設定	135
16.2.3	PPTP キープアライブの設定	136
16.2.4	PPTP キープアライブのログ設定	136
16.2.5	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	136
16.2.6	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	136
17.	SNMP の設定	137
17.1	SNMP によるアクセスを許可するホストの設定	137
17.2	SNMP 送信パケットの始点アドレスの設定	137
17.3	読み出し専用のコミュニティ名の設定	138
17.4	読み書き可能なコミュニティ名の設定	138
17.5	sysContact の設定	138
17.6	sysLocation の設定	138
17.7	sysName の設定	139
17.8	SNMP トラップを送信するか否かの設定	139
17.9	SNMP の LinkDown トラップの送信制御の設定	139
17.10	SNMP トラップのコミュニティ名の設定	140
17.11	SNMP トラップの送信先の設定	140
17.12	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	140
17.13	トンネルインタフェースの情報を MIB2 の範囲で表示するか否かの設定	140
17.14	PP インタフェースのアドレスの強制表示の設定	141
18.	RADIUS の設定	142
18.1	RADIUS による認証を使用するか否かの設定	142
18.2	RADIUS によるアカウントを使用するか否かの設定	142
18.3	RADIUS サーバの指定	142
18.4	RADIUS 認証サーバの指定	143
18.5	RADIUS アカウントサーバの指定	143
18.6	RADIUS 認証サーバの UDP ポートの設定	143
18.7	RADIUS アカウントサーバの UDP ポートの設定	143
18.8	RADIUS シークレットの設定	144
18.9	RADIUS 再送信パラメータの設定	144
19.	NAT 機能	145
19.1	インタフェースへの NAT ディスクリプタ適用の設定	145
19.2	NAT ディスクリプタの動作タイプの設定	145
19.3	NAT 処理の外側 IP アドレスの設定	146
19.4	NAT 処理の内側 IP アドレスの設定	146
19.5	静的 NAT エントリの設定	146
19.6	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	147
19.7	静的 IP マスカレードエントリの設定	147
19.8	NAT の IP アドレスマップの消去タイマの設定	147

19.9	IP マスカレードテーブルの TTL 処理方式の設定	148
19.10	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	148
19.11	IP マスカレードで利用するポートの範囲の設定	148
19.12	FTP として認識するポート番号の設定	149
19.13	IP マスカレードで変換しないポート番号の範囲の設定	149
19.14	NAT のアドレス割当をログに記録するか否かの設定	149
20.	DNS の設定	150
20.1	DNS を利用するか否かの設定	150
20.2	DNS サーバの IP アドレスの設定	150
20.3	DNS ドメイン名の設定	150
20.4	DNS サーバを通知してもらう相手先情報番号の設定	151
20.5	DHCP/IPCP MS 拡張で DNS サーバを通知する順序の設定	151
20.6	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
20.7	SYSLOG 表示で DNS により名前解決するか否かの設定	152
20.8	DNS 問い合わせの内容に応じた DNS サーバの選択	152
20.9	静的 DNS レコードの登録	153
21.	優先制御／帯域制御	154
21.1	インタフェース速度の設定	154
21.2	クラス分けのためのフィルタ設定	154
21.3	キューイングアルゴリズムタイプの選択	156
21.4	MP インタリーブの設定	157
21.5	クラス分けフィルタの適用	157
21.6	クラス毎のキュー長の設定	157
21.7	クラスの属性の設定	158
21.8	デフォルトクラスの設定	158
22.	OSPF	159
22.1	OSPF の有効設定	159
22.2	OSPF の使用設定	159
22.3	OSPF による経路の優先度設定	159
22.4	OSPF のルータ ID 設定	159
22.5	外部プロトコルによる経路導入	160
22.6	外部経路導入に適用するフィルタ定義	160
22.7	OSPF エリア設定	161
22.8	エリアへの経路広告	161
22.9	スタブ的接続の広告	161
22.10	仮想リンク設定	162
22.11	指定インタフェースの OSPF エリア設定	163
22.12	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	164
23.	BGP	165
23.1	BGP の起動の設定	165
23.2	経路の集約の設定	165
23.3	経路を集約するためのフィルタの設定	165
23.4	AS 番号の設定	166
23.5	ルータ ID の設定	166
23.6	BGP による経路の優先度の設定	166
23.7	BGP で受信した経路に対するフィルタの適用	166
23.8	BGP で受信する経路に適用するフィルタの設定	167
23.9	BGP に導入する経路に対するフィルタの適用	167
23.10	BGP の設定の有効化	167
23.11	BGP に導入する経路に適用するフィルタの設定	168
23.12	BGP による接続先の設定	168
24.	IPv6	169
24.1	共通の設定	169
24.1.1	IPv6 パケットを扱うか否かの設定	169
24.1.2	IPv6 インタフェースのリンク MTU の設定	169
24.1.3	TCP セッションの MSS 制限の設定	169
24.2	IPv6 アドレスの管理	170
24.2.1	インタフェースの IPv6 アドレスの設定	170

24.2.2	インタフェースのプレフィックスに基づく IPv6 アドレスの設定	170
24.3	近隣探索	171
24.3.1	ルータ広告で配布するプレフィックスの定義	171
24.3.2	ルータ広告の送信の制御	172
24.4	経路制御	172
24.4.1	IPv6 の経路情報の追加	172
24.5	RIPng	173
24.5.1	RIPng の使用の設定	173
24.5.2	インタフェースにおける RIPng の送信ポリシーの設定	173
24.5.3	インタフェースにおける RIPng の受信ポリシーの設定	173
24.5.4	RIPng の加算ホップ数の設定	174
24.5.5	インタフェースにおける信頼できる RIPng ゲートウェイの設定	174
24.5.6	RIPng で送受信する経路に対するフィルタリングの設定	174
24.5.7	回線接続時の PP 側の RIPng の動作の設定	175
24.5.8	回線接続時の PP 側の RIPng 送出の時間間隔の設定	175
24.5.9	回線切断時の PP 側の RIPng の動作の設定	175
24.5.10	回線切断時の PP 側の RIPng 送出の時間間隔の設定	175
24.5.11	RIPng による経路を回線切断時に保持するか否かの設定	176
24.6	フィルタの設定	176
24.6.1	IPv6 フィルタの定義	176
24.6.2	IPv6 フィルタの適用	176
24.6.3	IPv6 動的フィルタの定義	177
25.	ネットボランチ DNS サービスの設定	178
25.1	ネットボランチ DNS サービスの使用の可否	178
25.2	ネットボランチ DNS サーバに手動で更新する	178
25.3	ネットボランチ DNS サーバから削除する	178
25.4	ネットボランチ DNS サービスで使用するポート番号の設定	179
25.5	ネットボランチ DNS サーバに登録済みのホスト名一覧を取得	179
25.6	ホスト名の登録	179
25.7	通信タイムアウトの設定	179
25.8	ホスト名を自動生成するか否かの設定	180
25.9	ネットボランチ DNS サーバの設定	180
26.	スケジュール	181
26.1	スケジュールの設定	181
27.	操作	182
27.1	相手先情報番号の選択	182
27.2	トンネルインタフェース番号の選択	182
27.3	設定に関する操作	182
27.3.1	管理ユーザへの移行	182
27.3.2	終了	182
27.3.3	設定内容の保存	183
27.3.4	設定ファイルの削除	183
27.3.5	実行形式ファームウェアファイルの削除	183
27.3.6	設定ファイルの一覧	183
27.3.7	設定の初期化	183
27.3.8	遠隔地のルータの設定	184
27.3.9	遠隔地のルータからの設定に対する制限	184
27.4	動的情報のクリア操作	184
27.4.1	アカウントのクリア	184
27.4.2	ARP テーブルのクリア	184
27.4.3	IP の動的経路情報のクリア	185
27.4.4	IPX の動的経路情報のクリア	185
27.4.5	IPX の動的 SAP 情報のクリア	185
27.4.6	ブリッジのラーニング情報のクリア	185
27.4.7	ログのクリア	185
27.4.8	InARP のクリア	185
27.4.9	DNS キャッシュのクリア	186
27.4.10	PRI のステータス情報のクリア	186
27.4.11	NAT アドレステーブルのクリア	186

27.4.12	インタフェースのNAT アドレステーブルのクリア	186
27.4.13	IPv6 の動的経路情報の消去	186
27.4.14	近隣キャッシュの消去	186
27.5	その他の操作	187
27.5.1	相手先の使用許可の設定	187
27.5.2	相手先の使用不許可の設定	187
27.5.3	再起動	187
27.5.4	インタフェースの再起動	187
27.5.5	PP インタフェースの再起動	188
27.5.6	発信	188
27.5.7	切断	188
27.5.8	traceroute	188
27.5.9	traceroute6 の実行	188
27.5.10	ping	189
27.5.11	ping6 の実行	189
27.5.12	TELNET サーバ機能の ON/OFF の設定	189
27.5.13	TELNET サーバ機能の listen ポートの設定	189
27.5.14	TELNET サーバへアクセスできるホストの IP アドレスの設定	190
27.5.15	TELNET クライアント	190
27.5.16	ファームウェアファイルを内蔵フラッシュ ROM にコピー	190
27.5.17	IPv4 動的フィルタのコネクション管理情報の削除	191
27.5.18	IPv6 動的フィルタのコネクション管理情報の削除	191
27.5.19	PRI のループバックの実行	191
27.5.20	PRI のループバック待ち受けの設定	192
28.	設定の表示	193
28.1	機器設定の表示	193
28.2	すべての設定内容の表示	193
28.3	指定した PP の設定内容の表示	193
28.4	ファイル情報の一覧の表示	193
28.5	インタフェースに付与されている IPv6 アドレスの表示	193
28.6	マスタクロックを得ている回線の表示	194
29.	状態の表示	195
29.1	ARP テーブルの表示	195
29.2	インタフェースの状態の表示	195
29.3	各相手先の状態の表示	195
29.4	IP の経路情報テーブルの表示	195
29.5	RIP で得られた経路情報の表示	196
29.6	IPv6 の経路情報の表示	196
29.7	IPv6 の RIP テーブルの表示	196
29.8	近隣キャッシュの表示	196
29.9	IPXWAN の状態の表示	196
29.10	SAP テーブルの表示	196
29.11	IPX の経路情報テーブルの表示	197
29.12	ブリッジのラーニング情報の表示	197
29.13	IPsec の SA の表示	197
29.14	VRRP の情報の表示	197
29.15	動的 NAT ディスクリプタのアドレスマップの表示	197
29.16	動作中の NAT ディスクリプタの適用リストの表示	198
29.17	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	198
29.18	PPTP の状態の表示	198
29.19	OSPF 情報の表示	198
29.20	BGP の状態の表示	198
29.21	DHCP サーバの状態の表示	199
29.22	DHCP クライアントの状態の表示	199
29.23	バックアップ状態の表示	199
29.24	動的フィルタによって管理されているコネクションの表示	199
29.25	IPv6 の動的フィルタによって管理されているコネクションの表示	200
29.26	ネットワーク監視機能の状態の表示	200
29.27	侵入情報の履歴の表示	200
29.28	相手先ごとの接続時間情報の表示	200

- 29.29 ネットボランチ DNS サービスに関する設定の表示 201
- 30. ログイン202**
- 30.1 ログの表示 202
- 30.2 アカウントの表示 202
- 30.3 通信履歴の表示 202

コマンド索引

A

account threshold	42
account threshold pp	42
administrator	25, 182
administrator password	33

B

bgp aggregate	165
bgp aggregate filter	165
bgp autonomous-system	166
bgp configure refresh	167
bgp export	166
bgp export filter	167
bgp import	167
bgp import filter	168
bgp neighbor	168
bgp preference	166
bgp router id	166
bgp use	165
bridge filter	88
bridge group	87
bridge interface filter	89
bridge interface learning	88
bridge learning	87
bridge learning expire	88
bridge pp filter	89
bridge pp learning	89
bridge use	87

C

clear account	184
clear account pp	184
clear arp	184
clear bridge learning	185
clear dns cache	186
clear inarp	185
clear ip dynamic routing	185
clear ipv6 dynamic routing	186
clear ipv6 neighbor cache	186
clear ipx dynamic routing	185
clear ipx dynamic sap	185
clear log	185
clear nat descriptor dynamic	186
clear nat descriptor interface dynamic	186
clear nat descriptor interface dynamic pp	186
clear nat descriptor interface dynamic tunnel	186
clear pri status	186
cold start	183
connect	188
console character	25, 35
console columns	35
console info	36
console lines	35
console prompt	35
copy exec	190

D

date	33
delete config	183
delete exec	183
dhcp client client-identifier	113

dhcp client client-identifier pool	113
dhcp client client-identifier pp	113
dhcp client hostname	112
dhcp duplicate check	108
dhcp relay select	111
dhcp relay server	111
dhcp relay threshold	112
dhcp scope	109
dhcp scope bind	109
dhcp scope option	111
dhcp server rfc2131 compliant	108
dhcp service	107
disconnect	25, 188
disconnect ip connection	191
disconnect ipv6 connection	191
dns domain	150
dns notice order	151
dns private address spoof	151
dns server dhcp	112
dns server ip_address	150
dns server pp	151
dns server select	152
dns static	153
dns syslog resolv	152

E

exit	182
------	-----

F

fr backup	54
fr cir	53
fr compression use	54
fr congestion control	55
fr de	55
fr dlci	53
fr inarp	54
fr lmi	53
fr pp dequeue type	55

H

help	32
------	----

I

interface reset	187
interface reset pp	188
ip filter	61
ip filter directed-broadcast	62
ip filter dynamic	63
ip filter dynamic timer	63
ip filter set	62
ip filter source-route	62
ip fragment remove df-bit filter	65
ip host	153
ip icmp echo-reply send	114
ip icmp log	116
ip icmp mask-reply send	114
ip icmp parameter-problem send	22, 114
ip icmp redirect receive	115
ip icmp redirect send	114
ip icmp time-exceeded send	115
ip icmp timestamp-reply send	115

ip icmp unreachable send	115	ipsec ike always-on	123
ip interface address	58	ipsec ike duration	130
ip interface dhcp lease time	113	ipsec ike encryption	126
ip interface dhcp retry	113	ipsec ike esp-encapsulation	129
ip interface intrusion detection	64	ipsec ike group	127
ip interface mtu	59	ipsec ike hash	127
ip interface nat descriptor	145	ipsec ike keepalive log	126
ip interface ospf area	163	ipsec ike keepalive use	125
ip interface ospf neighbor	164	ipsec ike local address	125
ip interface proxyarp	66	ipsec ike local id	125
ip interface rip auth key	70	ipsec ike local name	124
ip interface rip auth text	70	ipsec ike log	129
ip interface rip auth type	70	ipsec ike negotiate-strictly	122
ip interface rip filter	69	ipsec ike payload type	128
ip interface rip hop	70	ipsec ike pfs	128
ip interface rip receive	69	ipsec ike pre-shared-key	122
ip interface rip send	68	ipsec ike queue length	126
ip interface rip trust gateway	69	ipsec ike remote address	124
ip interface secondary address	59	ipsec ike remote id	124
ip interface secure filter	65	ipsec ike remote name	123
ip interface tcp mss limit	64	ipsec ike restrict-dangling-sa	130
ip interface vrrp	72	ipsec ike retry	123
ip interface vrrp shutdown trigger	73	ipsec ike send info	128
ip keepalive	77	ipsec ike xauth myname	128
ip pp address	58	ipsec ipcomp type	131
ip pp intrusion detection	64	ipsec log illegal-spi	127
ip pp nat descriptor	145	ipsec refresh sa	131
ip pp ospf area	163	ipsec sa delete	131
ip pp remote address	67	ipsec sa policy	129
ip pp remote address pool	67	ipsec transport	132
ip pp rip auth key	70	ipsec tunnel	131
ip pp rip auth text	70	ipsec use	122
ip pp rip auth type	70	ipv6 filter	176
ip pp rip backup interface	72	ipv6 filter dynamic	177
ip pp rip connect interval	71	ipv6 icmp echo-reply send	116
ip pp rip connect send	71	ipv6 icmp log	118
ip pp rip disconnect interval	72	ipv6 icmp packet-too-big send	118
ip pp rip disconnect send	71	ipv6 icmp parameter-problem send	116
ip pp rip filter	69	ipv6 icmp redirect receive	117
ip pp rip hold routing	71	ipv6 icmp redirect send	117
ip pp rip hop	70	ipv6 icmp time-exceeded send	117
ip pp rip receive	69	ipv6 icmp unreachable send	117
ip pp rip send	68	ipv6 interface address	170
ip pp rip trust gateway	69	ipv6 interface mtu	169
ip pp secure filter	65	ipv6 interface prefix	170
ip pp tcp mss limit	64	ipv6 interface rip filter	174
ip route	60	ipv6 interface rip hop	174
ip routing	58	ipv6 interface rip receive	173
ip routing process	38	ipv6 interface rip send	173
ip simple-service	59	ipv6 interface rip trust gateway	174
ip stealth	116	ipv6 interface rtadv send	172
ip tos supersede	66	ipv6 interface secure filter	176
ip tunnel intrusion detection	64	ipv6 interface tcp mss limit	169
ip tunnel nat descriptor	145	ipv6 pp address	170
ip tunnel ospf area	163	ipv6 pp mtu	169
ip tunnel rip auth key	70	ipv6 pp prefix	170
ip tunnel rip auth text	70	ipv6 pp rip connect interval	175
ip tunnel rip auth type	70	ipv6 pp rip connect send	175
ip tunnel rip filter	69	ipv6 pp rip disconnect interval	175
ip tunnel rip hop	70	ipv6 pp rip disconnect send	175
ip tunnel rip receive	69	ipv6 pp rip filter	174
ip tunnel rip send	68	ipv6 pp rip hold routing	176
ip tunnel rip trust gateway	69	ipv6 pp rip hop	174
ip tunnel secure filter	65	ipv6 pp rip receive	173
ip tunnel tcp mss limit	64	ipv6 pp rip send	173
ipsec auto refresh	123	ipv6 pp rip trust gateway	174

ipv6 pp rtadv send	172
ipv6 pp secure filter	176
ipv6 pp tcp mss limit	169
ipv6 prefix	171
ipv6 rip use	173
ipv6 route	172
ipv6 routing	169
ipv6 stealth	118
ipv6 tunnel address	170
ipv6 tunnel prefix	170
ipv6 tunnel rip filter	174
ipv6 tunnel rip receive	173
ipv6 tunnel rip send	173
ipv6 tunnel secure filter	176
ipv6 tunnel tcp mss limit	169
ipx filter	79
ipx interface frame type	80
ipx interface network	80
ipx interface ripsap broadcast	80
ipx interface route	81
ipx interface secure filter	81
ipx pp ipxwan primnet	82
ipx pp ipxwan retry	84
ipx pp ipxwan use	82
ipx pp network	82
ipx pp ripsap connect interval	83
ipx pp ripsap connect send	83
ipx pp ripsap disconnect interval	83
ipx pp ripsap disconnect send	83
ipx pp ripsap hold	84
ipx pp route	82
ipx pp routing	81
ipx pp secure filter	86
ipx pp serialization filter	85
ipx pp spx keepalive proxy	85
ipx pp spx keepalive timer	85
ipx pp watchdog interval	84
ipx pp watchdog proxy	84
ipx routing	78
ipx sap	78
ipx sap response	78
isdn arrive permit	45
isdn auto connect	45
isdn call block time	46
isdn call permit	46
isdn call prohibit time	46
isdn callback mscbcu user-specify	47
isdn callback permit	47
isdn callback permit type	47
isdn callback request	46
isdn callback request type	47
isdn callback response time	48
isdn callback wait time	48
isdn disconnect input time	50
isdn disconnect interval time	51
isdn disconnect output time	50
isdn disconnect policy	48
isdn disconnect time	49
isdn fast disconnect time	49
isdn forced disconnect time	49
isdn local address	41
isdn piafs arrive	43
isdn piafs call	42
isdn piafs control	43
isdn remote address	44
isdn remote call order	45

isdn terminator	44
-----------------	----

L

lan backup	76
lan backup recovery time	76
lan keepalive interval	77
lan keepalive log	77
lan keepalive use	76
lan type	39
leased backup	43
leased keepalive down	75
less config	193
less config list	183
less config pp	193
less file list	193
less log	202
line masterclock	38
line type	30, 41, 57
login password	33
login timer	25, 40

N

nat descriptor address inner	146
nat descriptor address outer	146
nat descriptor ftp port	149
nat descriptor log	149
nat descriptor masquerade incoming	148
nat descriptor masquerade port range	148
nat descriptor masquerade rlogin	147
nat descriptor masquerade static	147
nat descriptor masquerade ttl hold	148
nat descriptor masquerade unconvertible port	149
nat descriptor static	146
nat descriptor timer	147
nat descriptor type	145
netvolante-dns auto hostname	180
netvolante-dns auto hostname pp	180
netvolante-dns delete go	178
netvolante-dns delete go pp	178
netvolante-dns get hostname list	179
netvolante-dns get hostname list pp	179
netvolante-dns go	178
netvolante-dns go pp	178
netvolante-dns hostname host	179
netvolante-dns hostname host pp	179
netvolante-dns port	179
netvolante-dns server	180
netvolante-dns timeout	179
netvolante-dns timeout pp	179
netvolante-dns use	178
netvolante-dns use pp	178
ntpdate	34

O

ospf area	161
ospf area network	161
ospf area stubhost	161
ospf configure refresh	159
ospf import filter	160
ospf import from	160
ospf preference	159
ospf router id	159
ospf use	159
ospf virtual-link	162

P	
ping	189
ping6	189
pp always-on	44
pp auth accept	91, 135
pp auth multi connect prohibit	91
pp auth myname	22, 91
pp auth request	90, 134
pp auth username	22, 90
pp backup	73
pp backup recovery time	22, 74
pp bind	41, 57, 133
pp disable	25, 187
pp enable	25, 187
pp encapsulation	52
pp keepalive interval	22, 75
pp keepalive log	22, 75
pp keepalive use	22, 74
pp select	182
ppp bacp maxconfigure	103
ppp bacp maxfailure	103
ppp bacp maxterminate	103
ppp bacp restart	102
ppp bap maxretry	103
ppp bap restart	103
ppp bcp lanid	97
ppp bcp maxconfigure	98
ppp bcp maxfailure	98
ppp bcp maxterminate	98
ppp bcp restart	98
ppp bcp tinycomp	98
ppp ccp maxconfigure	100
ppp ccp maxfailure	100
ppp ccp maxterminate	100
ppp ccp no-encryption	136
ppp ccp restart	100
ppp ccp type	99, 133
ppp chap maxchallenge	95
ppp chap restart	94
ppp ipcp ipaddress	95
ppp ipcp maxconfigure	96
ppp ipcp maxfailure	96
ppp ipcp maxterminate	95
ppp ipcp msex	96
ppp ipcp restart	95
ppp ipcp vjc	95
ppp ipv6cp use	100
ppp ipxcp maxconfigure	97
ppp ipxcp maxfailure	97
ppp ipxcp maxterminate	97
ppp ipxcp restart	97
ppp lcp acfc	92
ppp lcp magicnumber	92
ppp lcp maxconfigure	93
ppp lcp maxfailure	93
ppp lcp maxterminate	93
ppp lcp mru	92
ppp lcp pfc	93
ppp lcp restart	93
ppp lcp silent	94
ppp mp control	101
ppp mp divide	102
ppp mp interleave	157
ppp mp load threshold	101
ppp mp maxlink	101
ppp mp minlink	102
ppp mp timer	102
ppp mp use	101
ppp mscbcp maxretry	99
ppp mscbcp restart	99
ppp pap maxauthreq	94
ppp pap restart	94
pppoe	105
pppoe access concentrator	104
pppoe auto connect	104
pppoe auto disconnect	104
pppoe disconnect time	105
pppoe padi maxretry	104
pppoe padi restart	105
pppoe padr maxretry	105
pppoe padr restart	105
pppoe service-name	105
pppoe tcp mss limit	106
pppoe use	104
pptp call-id mode	134
pptp hostname	134
pptp keepalive interval	136
pptp keepalive log	136
pptp keepalive use	136
pptp service	133
pptp service type	133
pptp syslog	135
pptp tunnel disconnect time	135
pptp window size	134
pri leased channel	57
pri loopback active	191
pri loopback passive	192
pri loopback passive off	192
Q	
queue class filter	154
queue interface class filter list	157
queue interface class property	158
queue interface default	158
queue interface length	157
queue interface type	156
queue pp class filter list	157
queue pp class property	158
queue pp length	157
queue pp type	156
quit	182
R	
radius account	142
radius account port	143
radius account server	143
radius auth	142
radius auth port	143
radius auth server	143
radius retry	144
radius secret	144
radius server	142
rdate	34
remote setup	184
remote setup accept	184
restart	30, 187
rip preference	68
rip use	68
S	
save	25, 183

schedule at	181	snmp yrifunneldisplayatmib2	140
security class	33	speed	154
show account	202	speed pp	154
show account pp	202	syslog debug	37
show arp	195	syslog facility	36
show bridge learning	197	syslog host	36
show command	32	syslog info	37
show config	193	syslog notice	36
show config list	183	syslog srcport	37
show config pp	193	system power module use	37
show environment	193	system temperature threshold	38
show file list	193		
show history	202	T	
show ip connection	199	telnet	190
show ip connection pp	199	telnetd host	190
show ip connection tunnel	199	telnetd listen	189
show ip intrusion detection	200	telnetd service	189
show ip intrusion detection pp	200	tftp host	30, 40
show ip intrusion detection tunnel	200	time	34
show ip rip table	196	timezone	34
show ip route	195	traceroute	188
show ipsec sa	197	traceroute6	188
show ipsec sa gateway	197	tunnel backup	132
show ipv6 address	193	tunnel disable	119
show ipv6 connection	200	tunnel enable	119
show ipv6 connection pp	200	tunnel encapsulation	22, 119, 133
show ipv6 connection tunnel	200	tunnel endpoint address	22, 120, 133
show ipv6 neighbor cache	196	tunnel endpoint name	135
show ipv6 rip table	196	tunnel select	182
show ipv6 route	196		
show ipx ipxwan	196	W	
show ipx route	197	wins server	96
show ipx sap	196		
show line masterclock	194		
show log	202		
show nat descriptor address	197		
show nat descriptor interface address	198		
show nat descriptor interface bind	198		
show pp connect time	200		
show status	195		
show status backup	199		
show status bgp	198		
show status dhcp	199		
show status dhcpc	199		
show status ip keepalive	200		
show status netvolante-dns	201		
show status netvolante-dns pp	201		
show status ospf	198		
show status pp	195		
show status pptp	198		
show status vrrp	197		
snmp community read-only	138		
snmp community read-write	138		
snmp display ipcp force	141		
snmp host	137		
snmp local address	137		
snmp syscontact	138		
snmp syslocation	138		
snmp sysname	139		
snmp trap community	140		
snmp trap enable snmp	139		
snmp trap host	140		
snmp trap send linkdown	139		
snmp trap send linkdown pp	139		
snmp trap send linkdown tunnel	139		
snmp yrifppdisplayatmib2	140		

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.6.03.28](#)、[Rev.7.00.26](#)、[Rev.7.01.17](#) 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

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んら影響を与えません。

1.5 コマンドの入力文字数とエスケープシーケンスについて

1つのコマンドとして入力できる文字数は、コマンド本体とパラメータ部分を含めて最大 4095 文字以内です。
また、コマンドのパラメータ部分に以下の特殊文字を入力する場合には表に示す方法で入力してください。

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

1.6 相手先情報番号のモデルによる違いについて

相手先情報番号はモデルによって使用できる数値の範囲が異なります。

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

1.7 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。

プログラムの古いリビジョンから Rev.6.03.11 以降へ変更する場合には以下の注意が必要となります

- **pptp keepalive use** コマンドのデフォルト値が off から on に変更。
- **nat descriptor masquerade static** コマンドの入力形式を拡張。

プログラムの古いリビジョンから Rev.6.03.15 以降へ変更する場合には以下の注意が必要となります

- **pp bind** コマンドの入力形式を拡張。複数のトンネルインタフェース番号が指定可能。
- **dhcp client client-identifier** コマンドのデフォルト値を *type=1* に変更。

プログラムの古いリビジョンから Rev.6.03.25 以降へ変更する場合には以下の注意が必要となります

- **dns server select** コマンドを拡張。セカンダリ DNS サーバが設定可能。

プログラムの古いリビジョンから Rev.7.00.14 以降へ変更する場合には以下の注意が必要となります

- **lan backup** コマンドの入力形式を拡張。バックアップにトンネルインタフェースが指定可能。
- **pp backup** コマンドの入力形式を拡張。バックアップにトンネルインタフェースが指定可能。
- **tunnel backup** コマンドの入力形式を拡張。バックアップにトンネルインタフェースが指定可能。
- **pppoe disconnect time** コマンド廃止 (RTX2000 に対してのみ)。

プログラムの古いリビジョンから Rev.7.01.15 以降へ変更する場合には以下の注意が必要となります

- **snmp host** コマンドの入力形式を拡張。パラメータにコミュニティ文字列が指定可能。
- **ipsec ike xauth myname** コマンドで、ユーザ名やパスワードの最大文字数を 31 から 32 に変更。
- **snmp trap host** コマンドで、複数のホストをトラップ送信先が設定可能。また、ホスト毎にコミュニティ文字列を変更できる。
- **ipsec ike payload type** コマンドを拡張。メッセージフォーマット 3 が指定可能。

プログラムの古いリビジョンから Rev.7.01.17 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 interface ospf area** コマンドの入力形式を拡張。パラメータに md5-sequence-mode が指定可能。
- **ospf virtual-link** コマンドの入力形式を拡張。パラメータに md5-sequence-mode が指定可能。

2. コマンドの使い方

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

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

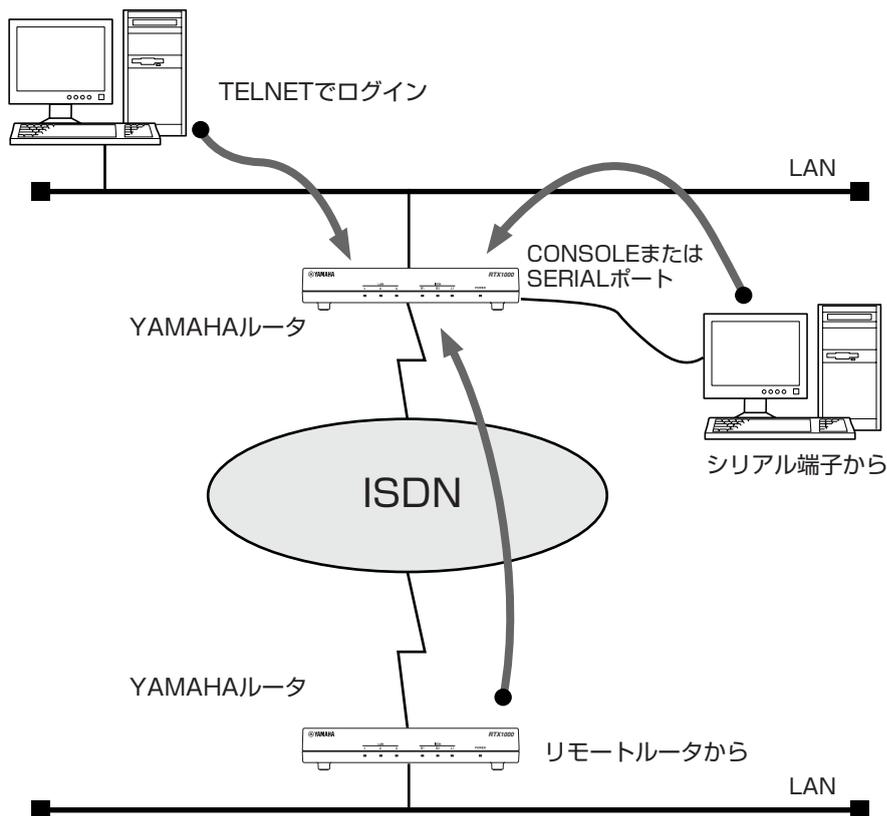
2.1 コンソールについて

各種の設定を行うためには、YAMAHA ルータの CONSOLE ポートにシリアル端末を接続する方法と、LAN 上のホストから TELNET でログインする方法、ISDN 回線や専用線を介して別の YAMAHA ルータからログインする方法の3つがあります。

YAMAHA ルータへのアクセス方法

- CONSOLE または SERIAL ポートに接続した端末からアクセス
- LAN 上のホストから TELNET でログイン
- ISDN 回線や専用線を介して別の YAMAHA ルータからログイン

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



2.1.1 コンソールによる設定手順

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

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

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

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

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

設定手順のおおまかな流れは次のようになります。

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

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

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

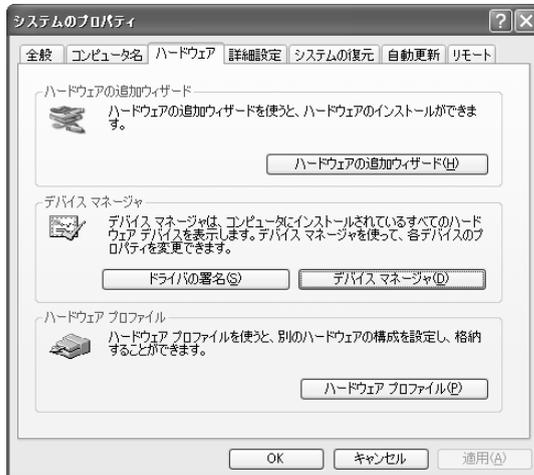
新たに管理ユーザになって設定コマンドを実行すると、その内容はすぐに動作に反映されますが、**save** コマンドを実行しないと不揮発性メモリに書き込まれません。

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

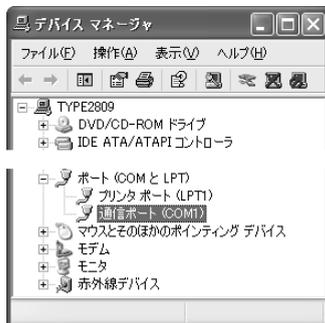
2.1.2 CONSOLE または SERIAL ポートからの設定

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

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



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



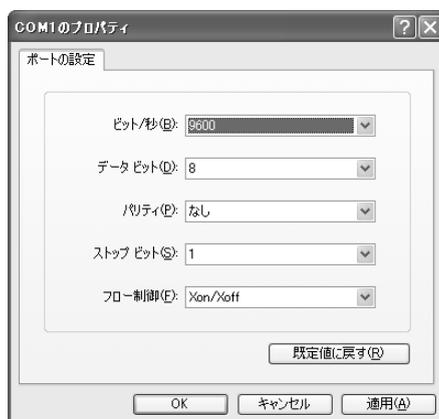
3. 「デバイス マネージャ」ウィンドウを閉じます。
4. [スタート] メニューから [すべてのプログラム] - [アクセサリ] - [通信] - [ハイパーターミナル] を選びます。「接続の設定」ウィンドウが開いたら、名前欄に適切な名前を入力して [OK] をクリックします。



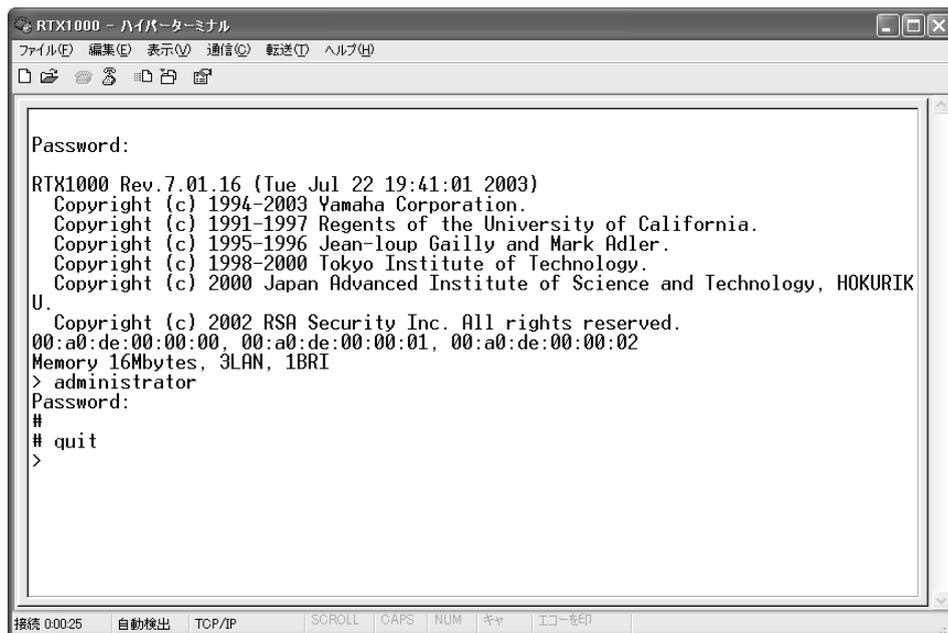
5. 「接続方法」欄から、手順2で調べたCOMポートを選択して [OK] をクリックします。



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



7. 「Password:」と表示されたら、ログインパスワードを入力してから Enter キーを押します。何も表示されないときは、1度 Enter キーを押します。「>」が表示されると、コンソールコマンドを入力できるようになります。以下の例は、RTX1000 にログインした場合の表示です。



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

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

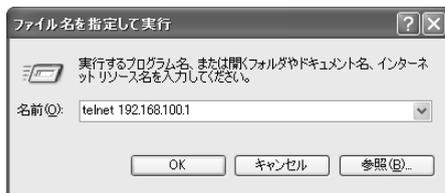
2.1.3 TELNET による設定

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

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



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



3. 「Password:」と表示されたら、ログインパスワードを入力してから Enter キーを押します。
何も表示されないときは、1 度 Enter キーを押します。
> が表示されると、コンソールコマンドを入力できるようになります。

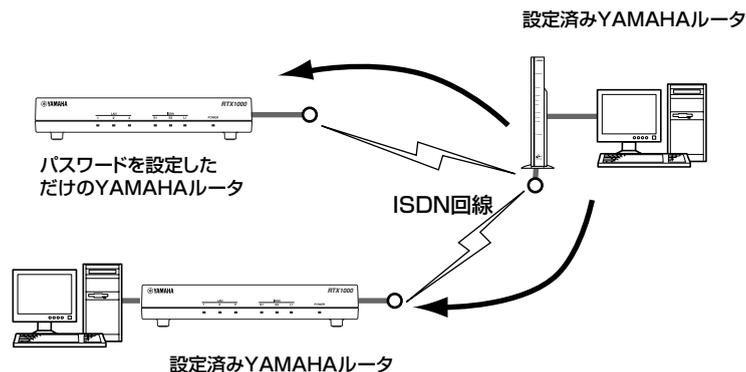


- 【ノート】
- ・「**help**」と入力してから Enter キーを押すと、キー操作の説明が表示されます。
 - ・「**show command**」と入力してから Enter キーを押すと、コマンド一覧が表示されます。

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

2.1.4 リモートセットアップ

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



リモートセットアップで設定される側は、パスワードが設定されている必要があります。パスワードを知らないと設定することはできません。また、リモートセットアップを拒否するようにも設定できるため、拒否に設定しておけば、不特定の相手からの侵入を防げます。

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

相手の YAMAHA ルータへのログインが完了すると、設定したいルータをコンソールコマンドで設定できるようになります。

- 【ご注意】
- ・ YAMAHA ルータ以外のルータからリモートセットアップすることはできません。
 - ・ FTTH や CATV、ADSL などの WAN ポート経由で、リモートセットアップすることはできません。

2.2 TFTP について

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

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

30 2. コマンドの使い方

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

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

2.2.1 TFTP による設定手順

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



```
Telnet 192.168.100.1
> administrator
Password:
# tftp host 192.168.100.25
# save
セーブ中... CONFIG0 終了
# quit
>
```

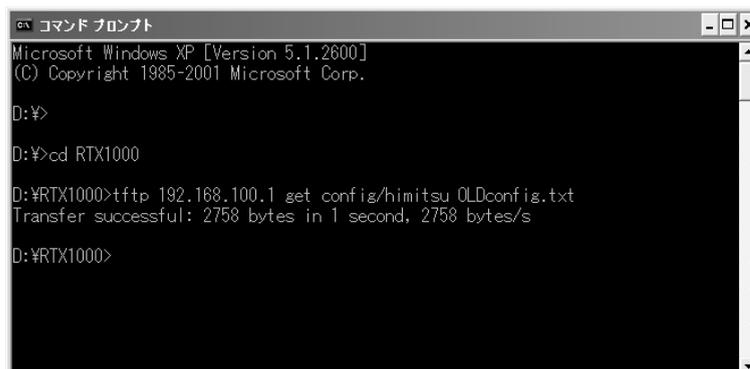
次に、LAN 上のホストから TFTP コマンドを実行します。使用するコマンドの形式は、そのホストの OS に依存します。次の点に注意して実行してください。

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

2.2.2 設定ファイルの読み出し

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

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



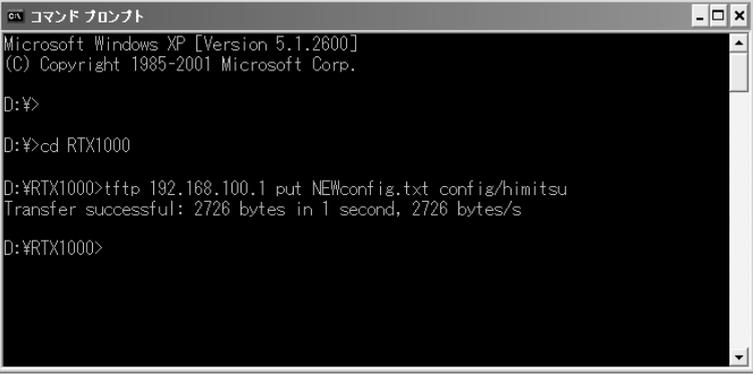
```
コマンドプロンプト
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:¥>
D:¥>cd RTX1000
D:¥RTX1000>tftp 192.168.100.1 get config/himitsu OLDconfig.txt
Transfer successful: 2758 bytes in 1 second, 2758 bytes/s
D:¥RTX1000>
```

2.2.3 設定ファイルの書き込み

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

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



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

D:\>
D:\>cd RTX1000
D:\RTX1000>tftp 192.168.100.1 put NEWconfig.txt config/himitsu
Transfer successful: 2726 bytes in 1 second, 2726 bytes/s
D:\RTX1000>
```

3. ヘルプ

3.1 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	RT105i	RT105e
---------	---------	--------	--------	--------

3.2 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	RT105i	RT105e
---------	---------	--------	--------	--------

4. 機器の設定

4.1 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】	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

4.2 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】	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

4.3 セキュリティクラスの設定

【入力形式】	security class <i>level forget telnet</i> no security class [<i>level forget telnet</i>]					
【パラメータ】	<ul style="list-style-type: none"> ○ <i>level</i> <ul style="list-style-type: none"> ● 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 ○ <i>forget</i> <ul style="list-style-type: none"> ● 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 ○ <i>telnet</i> <ul style="list-style-type: none"> ● 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】	<i>level</i> = 1 <i>forget</i> = on <i>telnet</i> = off					
【適用モデル】	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

4.4 現在の日付けの設定

【入力形式】	date <i>date</i>					
【パラメータ】	○ <i>date</i>yyyy-mm-dd または yyyy/mm/dd					
【説明】	現在の日付けを設定する。					
【適用モデル】	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

4.5 現在の時刻の設定

[入力形式] **time** *time*

[パラメータ] ◦ *time*..... hh:mm:ss

[説明] 現在の時刻を設定する。

[適用モデル]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

4.6 タイムゾーンの設定

[入力形式] **timezone** *timezone*
no timezone [*timezone*]

[パラメータ] ◦ *timezone* その地域と世界標準時との差

- *jst*..... 日本標準時 (+09:00)
- *utc*..... 世界標準時 (+00:00)
- 時刻 : 分 (-12:00 .. +11:59)

[説明] タイムゾーンを設定する。

[デフォルト値] *jst*

[適用モデル]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

4.7 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 は十進数))
- ホストの名称

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

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

[ノート] 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	RT105i	RT105e
---------	---------	--------	--------	--------

4.8 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 は十進数))
- NTP サーバの名称

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

[説明] NTP を利用してルータの時計を設定する。このコマンドが実行されるとホストの UDP の 123 番ポートに接続する。

[ノート] インターネットに接続している場合には、**rdate** コマンドを使用した場合よりも精密な計合わせが可能になる。
NTP サーバはできるだけ近くのを指定した方が良い。利用可能な NTP サーバ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	RT105i	RT105e
---------	---------	--------	--------	--------

4.9 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>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

4.10 コンソールの言語とコードの設定

[入力形式]	console character <i>code</i> no console character [<i>code</i>]					
[パラメータ]	◦ <i>code</i> <ul style="list-style-type: none"> • <i>ascii</i>..... 英語で表示する、文字コードは ASCII • <i>sjis</i>..... 日本語で表示する、文字コードはシフト JIS • <i>euc</i>..... 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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

4.11 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>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

4.12 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) • <i>infinity</i> 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>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

4.13 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" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

4.14 SYSLOG を受けるホストの IP アドレスの設定

[入力形式]	syslog host <i>host</i> no syslog host [<i>host</i>]					
[パラメータ]	◦ <i>host</i>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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

4.15 SYSLOG ファシリティの設定

[入力形式]	syslog facility <i>facility</i> no syslog facility [<i>facility</i>]					
[パラメータ]	◦ <i>facility</i> <ul style="list-style-type: none"> • 0..23 • user 1 • local0..local7..... 16..23 					
[説明]	SYSLOG のファシリティを設定する。					
[ノート]	ファシリティ番号の意味づけは、各 SYSLOG サーバで独自に行なう。					
[デフォルト値]	user					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

4.16 NOTICE タイプの SYSLOG を出力するか否かの設定

[入力形式]	syslog notice <i>notice</i> no syslog notice [<i>notice</i>]					
[パラメータ]	◦ <i>notice</i> <ul style="list-style-type: none"> • 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

4.17 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]	<ul style="list-style-type: none"> ◦ <i>info</i> <ul style="list-style-type: none"> • 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

4.18 DEBUG タイプのSYSLOG を出力するか否かの設定

[入力形式]	syslog debug debug no syslog debug [debug]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <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="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

4.19 SYSLOG パケットの始点ポート番号の設定

[入力形式]	syslog srcport port no syslog srcport [port]					
[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="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

4.20 電源の設定

[入力形式]	system power module use switch no system power module use [switch]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>module</i> モジュール番号 (1,2) ◦ <i>switch</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]	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。					
[ノート]	電源モジュールを装着していないにも関わらず、 <i>switch</i> を on 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。					
[デフォルト値]	モジュール 1 = on モジュール 2 = off					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

4.21 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"> ◦ interface <ul style="list-style-type: none"> • BRI インタフェース名 • PRI 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 よりは 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 bri1 をマスタとする。bri1 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ておくべき。</p>					
[デフォルト値]	auto					
[適用モデル]	<table border="1" style="display: inline-table; 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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

4.22 温度監視の閾値の設定

[入力形式]	system temperature threshold t1 t2 no system temperature threshold t1 t2					
[パラメータ]	<ul style="list-style-type: none"> ◦ t1警告を発する温度 (°C) ◦ t2警告を解除する温度 (°C) 					
[説明]	<p>本体内部の温度を監視して、t1 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 t2 を下回らない限り、ALM ランプは消えない。</p>					
[デフォルト値]	t1 = 80 t2 = 75					
[適用モデル]	<table border="1" style="display: inline-table; 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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

4.23 ファストパス機能の設定

[入力形式]	ip routing process process no ip routing process					
[パラメータ]	<ul style="list-style-type: none"> ◦ process <ul style="list-style-type: none"> • fast.....ファストパス機能を利用する • normal.....ファストパス機能を利用せず、すべてのパケットをスローパスで処理する 					
[説明]	<p>パケット転送をファストパス機能で処理するか、スローパス機能で処理するかを設定する。</p>					
[ノート]	<p>ファストパスでは使用できる機能に制限は無いが、取り扱うパケットの種類によってはファストパスで処理されずスローパスで処理されることもある。</p> <p>ファームウェアが Rev.7.01 以降でのみ有効。</p>					
[デフォルト値]	fast					
[適用モデル]	<table border="1" style="display: inline-table; 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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

4.2.4 LAN インタフェースの動作タイプの設定

[入力形式]	<pre>lan type interface speed_type [port ...] [speed_type ...] [port-based-ks8995e group_type port [port ...] [ip-routing=routing] [group_type ...]] [auto-crossover=switch] lan type interface port-based-ks8995e group_type port [port ...] [ip-routing=routing] [group_type ...] [auto-crossover=switch] lan type interface auto-crossover=switch no lan type interface</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>speed_type</i> LAN 動作タイプ <ul style="list-style-type: none"> ● <i>auto</i> 自動判別 ● <i>10-hdx</i> 10BASE-T 半二重 ● <i>10-fdx</i> 10BASE-T 全二重 ● <i>100-hdx</i> 100BASE-TX 半二重 ● <i>100-fdx</i> 100BASE-TX 全二重 ● 省略時は <i>auto</i> ○ <i>port</i> (スイッチングハブ内蔵機種のみ) <ul style="list-style-type: none"> ● スイッチングハブのポート番号 (1..4) ● 省略時は全ポート ○ <i>group_type</i> ポートの属するネットワークあるいは無効化の指定 <ul style="list-style-type: none"> ● <i>primary</i> 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 ● <i>secondary</i> 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 ● <i>disable</i> 指定ポートは使用しない ○ <i>routing</i> IP ルーティング接続 <ul style="list-style-type: none"> ● <i>on</i> 指定ポートをルーティング機能と接続する ● <i>off</i> 指定ポートをルーティング機能と接続しない ● 省略時は <i>on</i> ○ <i>switch</i> クロスストレート自動判別機能を使用するか否か (RT105p と RT105e スイッチングハブインタフェースのみ) <ul style="list-style-type: none"> ● <i>on</i> クロスストレート自動判別機能を使用する ● <i>off</i> クロスストレート自動判別機能を使用しない 					
[説明]	<p>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。 RT105e ではキーワード <i>port-based-ks8995e</i> 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。</p>					
[ノート]	<p>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。 <i>port-based-ks8995e</i> と <i>auto-crossover</i> キーワードが使用できるのは RT105p と RT105e のみである。 また <i>auto-crossover</i> キーワードは RTX2000/RT300i/RT140 シリーズ及び RT105i は使用できない。</p> <p><i>port-based-ks8995e</i> を指定した場合、<i>primary</i> 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。<i>primary</i> 指定と <i>secondary</i> 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 <i>disable</i> 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。</p> <p><i>ip-routing=off</i> 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。</p> <p>YAMAHA ルータ自身からのブロードキャストパケットは、<i>ip-routing=off</i> 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。</p>					
[デフォルト値]	<pre>speed_type = auto port-based-ks8995e 指定なし auto-crossover = on</pre>					
[設定例]	<p>例 1) ポート 1,2 は 100BASE-TX 全二重、その他のポートはオートネゴシエーションで接続する。 # lan type lan1 100-fdx 1 2</p> <p>例 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。 # lan type lan1 100-fdx 1 port-based-ks8995e primary 1 2</p> <p>例 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 <i>disable</i> 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。 # lan type lan1 port-based-ks8995e primary 1 2 secondary 3</p>					
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 25%;">RTX2000</td> <td style="width: 25%;">RTX1000</td> <td style="width: 25%;">RT300i</td> <td style="width: 25%;">RT105i</td> <td style="width: 25%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

4.25 ログインタイマの設定

- [入力形式] **login timer** *time*
 no login timer [*time*]
- [パラメータ] ◦ *time*
- 秒数 キー入力がない場合に自動的にログアウトするまでの秒数 (30.. 21474836)
 - clear ログインタイマを設定しない
- [説明] キー入力がない場合に自動的にログアウトするまでの時間を設定する。
- [ノート] TELNET でログインした場合、clear が設定されていてもタイマ値は 300 秒として扱う。
- [デフォルト値] 300
- [適用モデル]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

4.26 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** *host*
 no tftp host [*host*]
- [パラメータ] ◦ *host*
- 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 IPv4 または IPv6 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]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

5. ISDN 関連の設定

5.1 共通の設定

5.1.1 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="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

5.1.2 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> <ul style="list-style-type: none"> • BRI インタフェース名 • 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ならないことがある。					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

5.1.3 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]	○ <i>interface</i> BRI インタフェース名と BRI インタフェース名の並び					
[説明]	選択されている相手先に対して実際に使用するインタフェースを設定する。					
[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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

5.1.4 課金額による発信制限の設定

[入力形式]	account threshold [<i>interface</i>] <i>yen</i> account threshold pp <i>yen</i> no account threshold <i>interface</i> [<i>yen</i>] no account threshold [<i>yen</i>] no account threshold pp [<i>yen</i>]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>interface</i> <ul style="list-style-type: none"> • BRI インタフェース名 • PRI インタフェース名 ◦ <i>yen</i> <ul style="list-style-type: none"> • 課金額円 (10..21474836) • off..... 発信制限機能を使わない 					
[説明]	<p>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。</p> <p>account threshold コマンドではルータ全体の合計金額を設定し、<i>interface</i> 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。</p> <p>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。</p>					
[ノート]	<p>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。</p>					
[デフォルト値]	off					
[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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

5.1.5 PIAFS の発信方式の設定

[入力形式]	isdn piafs call speed [<i>64kmode</i>] no isdn piafs call [<i>speed</i> [<i>64kmode</i>]]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>speed</i> <ul style="list-style-type: none"> • 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 ◦ <i>64kmode</i> <ul style="list-style-type: none"> • guarantee PIAFS 64k の発信ではギャランティー方式を使用する • best-effort..... PIAFS 64k の発信ではベストエフォート方式を使用する 					
[説明]	<p>PIAFS モードの発信を可能にするか否かを設定する。</p> <p>また、PIAFS モードの速度を選択する。</p> <p><i>speed</i> 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。</p> <p><i>speed</i> が 64k に設定されている場合には、<i>64kmode</i> の設定が有効になる。</p> <p><i>64kmode</i> が設定されていない、または <i>guarantee</i> 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。</p> <p><i>64kmode</i> が <i>best-effort</i> 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。</p>					
[ノート]	<p>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。</p>					
[デフォルト値]	off					
[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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

5.1.6 PIAFS の着信を許可するか否かの設定

[入力形式]	isdn piafs arrive <i>arrive</i> no isdn piafs arrive [<i>arrive</i>]					
[パラメータ]	○ <i>arrive</i> <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="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

5.1.7 PIAFS 接続時の起動側の指定

[入力形式]	isdn piafs control <i>switch</i> no isdn piafs control												
[パラメータ]	○ <i>switch</i> <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 自分が発着信いずれの場合でも PIAFS の起動側となる • arrive 自分が着信側の場合に PIAFS の起動側となる 												
[説明]	PIAFS を制御する側を選択する。												
[ノート]	本コマンドの設定と、発信 / 着信の組み合わせにより、起動側となるか被起動側となるかが以下のように決定される。												
	<table border="1" style="margin-left: auto; margin-right: auto; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;"><i>switch</i> パラメータの設定</th> <th style="text-align: center;">call</th> <th style="text-align: center;">both</th> <th style="text-align: center;">arrive</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">発信時</td> <td style="text-align: center;">起動時</td> <td style="text-align: center;">起動側</td> <td style="text-align: center;">被起動側</td> </tr> <tr> <td style="text-align: center;">着信時</td> <td style="text-align: center;">被起動側</td> <td style="text-align: center;">起動側</td> <td style="text-align: center;">起動側</td> </tr> </tbody> </table>	<i>switch</i> 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
<i>switch</i> 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="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e							
RTX2000	RTX1000	RT300i	RT105i	RT105e									

5.1.8 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 <i>peer_num</i> no leased backup [<i>peer_num</i>]					
[パラメータ]	○ <i>peer_num</i> <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="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

5.1.9 常時接続の設定

[入力形式]	pp always-on switch [<i>time</i>] no pp always-on					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>switch</i> <ul style="list-style-type: none"> • on.....常時接続する • off.....常時接続しない ◦ <i>time</i>.....再接続を要求するまでの秒数 (60 .. 21474836) 					
[説明]	<p>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。</p> <p>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 <i>time</i> 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。<i>sw</i> が on に設定されている場合には、<i>time</i> の設定が有効となる。<i>time</i> が設定されていない場合には <i>time</i> は 60 になる。</p>					
[ノート]	<p>PP 毎のコマンドである。</p> <p>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。</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 style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

5.1.10 終端抵抗の設定

[入力形式]	isdn terminator interface terminator no isdn terminator interface [<i>terminator</i>]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>interface</i>.....BRI インタフェース名 ◦ <i>terminator</i> <ul style="list-style-type: none"> • 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]	<p>DSU に直結する場合には必ず on にする。</p> <p>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。</p>					
[デフォルト値]	on					
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

5.2 相手側の設定

5.2.1 相手 ISDN 番号の設定

[入力形式]	isdn remote address call_arrive isdn_num [/sub_address][<i>isdn_num_list</i>] isdn remote address call_arrive isdn_num [<i>isdn_num_list</i>] no isdn remote address call_arrive [<i>isdn_num</i> /sub_address][<i>isdn_num_list</i>]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>call_arrive</i> <ul style="list-style-type: none"> • call.....発着信用 • arrive.....着信専用 ◦ <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) ◦ <i>isdn_num_list</i>.....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]	<p>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。</p> <p>選択されている相手が anonymous の場合は無意味である。</p> <p>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。</p> <p>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。</p>					
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

5.2.2 相手への発信順序の設定

[入力形式]	isdn remote call order <i>order</i> no isdn remote call order [<i>order</i>]					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>order</i> <ul style="list-style-type: none"> • round..... ラウンドロビン方式 • serial..... 順次サーチ方式 					
[説明]	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>					
[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]	<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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

5.2.3 自動接続の設定

[入力形式]	isdn auto connect <i>auto</i> no isdn auto connect [<i>auto</i>]					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>auto</i> <ul style="list-style-type: none"> • 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]	<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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

5.2.4 着信許可の設定

[入力形式]	isdn arrive permit <i>arrive</i> [<i>vrrp interface vrid</i> [<i>slave</i>]] no isdn arrive permit [<i>arrive</i>]					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>arrive</i> <ul style="list-style-type: none"> • on..... 許可する • off..... 許可しない ○ <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]	<p>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。</p> <p>on に設定しかつ VRRP グループを指定することで、VRRP の状態によって着信を許可するか否かの動作を動的に変えることが可能である。</p> <p>この時、slave パラメータを省略した場合には指定した VRRP グループでマスターとして動作している場合にのみ着信が許可される。slave パラメータを設定した場合には、指定した VRRP グループで非マスターである場合にのみ着信が許可される。</p>					
[ノート]	isdn arrive permit 、 isdn call permit コマンドとも off を設定した場合は ISDN 回線経由での通信できない。					
[デフォルト値]	on					
[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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

5.2.5 発信許可の設定

[入力形式]	isdn call permit <i>permit</i> no isdn call permit [<i>permit</i>]					
[パラメータ]	◦ <i>permit</i> <ul style="list-style-type: none"> • 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]	<table border="1" style="width: 100%; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

5.2.6 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="width: 100%; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

5.2.7 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="width: 100%; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

5.2.8 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="width: 100%; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

5.2.9 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 <i>callback_permit</i> no isdn callback permit [<i>callback_permit</i>]					
[パラメータ]	○ <i>callback_permit</i> <ul style="list-style-type: none"> • 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

5.2.10 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 • mscbcp 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="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

5.2.11 コールバック受け入れタイプの設定

[入力形式]	isdn callback permit type <i>type1</i> [<i>type2</i>] no isdn callback permit type [<i>type1</i> [<i>type2</i>]]					
[パラメータ]	○ <i>type1, type2</i> <ul style="list-style-type: none"> • yamaha ヤマハ方式 • mscbcp MS コールバック 					
[説明]	受け入れることのできるコールバック方式を設定する。					
[デフォルト値]	<i>type1</i> = yamaha <i>type2</i> = mscbcp					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

5.2.12 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 mscbcp user-specify <i>specify</i> no isdn callback mscbcp user-specify [<i>specify</i>]					
[パラメータ]	○ <i>specify</i> <ul style="list-style-type: none"> • 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

5.2.13 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	RT105i	RT105e
---------	---------	--------	--------	--------

5.2.14 コールバック待機タイムの設定

[入力形式] **isdn callback wait time** *time*
no isdn callback wait time [*time*]

[パラメータ] ◦ *time* 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]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

5.2.15 ISDN 回線を切断するタイム方式の指定

[入力形式] **isdn disconnect policy** *type*
no isdn disconnect policy [*type*]

[パラメータ] ◦ *type*

- 1 単純トラフィック監視方式
- 2 課金単位時間方式

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

[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]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

5.2.16 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]	<ul style="list-style-type: none"> ○ <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="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

5.2.17 切断タイマの設定 (ファスト)

[入力形式]	isdn fast disconnect time <i>time</i> no isdn fast disconnect 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..... 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

5.2.18 切断タイマの設定 (強制)

[入力形式]	isdn forced disconnect time <i>time</i> no isdn forced disconnect 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..... 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

5.2.19 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。
 5.2.16 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	RT105i	RT105e
---------	---------	--------	--------	--------

5.2.20 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。
 5.2.16 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]

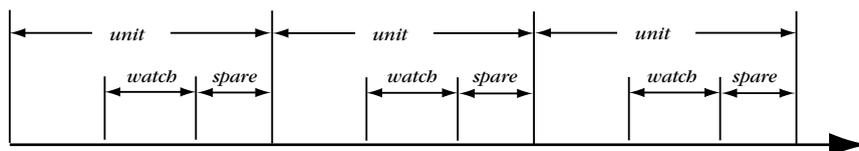
RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

5.2.21 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	RT105i	RT105e
---------	---------	--------	--------	--------

6. フレームリレー関連の設定

BRI インタフェースまたは 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 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否かは **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。

6.1 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 <ul style="list-style-type: none"> • 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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	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

6.2 DLCI の設定

[入力形式]	fr dlc <i>dlci_num</i> no fr dlc [<i>dlci_num</i>]					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>dlci_num</i> <ul style="list-style-type: none"> • auto DLCI 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]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

6.3 DLCI ごとのパラメータの設定

[入力形式]	fr cir <i>dlci=dlci_num cir</i> [slowstart-idle= <i>idle</i>] [bc= <i>bc_size</i>] [be= <i>be_size</i>] [s= <i>step_count</i>] no fr cir <i>dlci=dlci_num</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: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

6.4 PVC 状態確認手順の設定

[入力形式]	fr lmi <i>lmi</i> no fr lmi [<i>lmi</i>]					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>lmi</i> <ul style="list-style-type: none"> • q933 TTC 標準 JT-Q933 付属資料 A に基づいて状態確認を行う • ansi ANSI T1.617 AnnexD に基づいて状態確認を行う • off PVC 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]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

6.5 InARP 使用の設定

[入力形式]	fr inarp inarp no fr inarp [inarp]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>inarp</i> <ul style="list-style-type: none"> • on.....使用する • off.....使用しない 					
[説明]	<p>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。</p> <p>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。</p>					
[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]	<table border="1" style="width: 100%; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

6.6 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=dlci_num peer_num no fr backup dlci=dlci_num [peer_num]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>dlci_num</i>..... 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%; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

6.7 FR 圧縮機能の設定

[入力形式]	fr compression use dlci=dlci_num type no fr compression use dlci=dlci_num [type]					
[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%; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

6.8 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]	<ul style="list-style-type: none"> ○ 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" style="display: inline-table; 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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

6.9 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]	<ul style="list-style-type: none"> ○ 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にすべての 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" style="display: inline-table; 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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

6.10 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 dlci=dlci_num filter_num_list no fr de protocol filter dlci=dlci_num [filter_num_list]					
[パラメータ]	<ul style="list-style-type: none"> ○ 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。 <i>filter_num_list</i> 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" style="display: inline-table; 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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

7. 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。

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 はどのオプションモジュール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

(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

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を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、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。

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。

7.1 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="display: inline-table; 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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

7.2 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: 40px;">以下のニーモニックが使用可能</p> <table border="1" style="margin-left: 40px; border-collapse: collapse; text-align: center;"> <thead> <tr> <th style="padding: 2px 10px;">ニーモニック速度 (bit/s)</th> <th style="padding: 2px 10px;">タイムスロット数</th> </tr> </thead> <tbody> <tr><td style="padding: 2px 10px;">192k</td><td style="padding: 2px 10px;">3</td></tr> <tr><td style="padding: 2px 10px;">256k</td><td style="padding: 2px 10px;">4</td></tr> <tr><td style="padding: 2px 10px;">384k</td><td style="padding: 2px 10px;">6</td></tr> <tr><td style="padding: 2px 10px;">512k</td><td style="padding: 2px 10px;">8</td></tr> <tr><td style="padding: 2px 10px;">768k</td><td style="padding: 2px 10px;">12</td></tr> <tr><td style="padding: 2px 10px;">1024k</td><td style="padding: 2px 10px;">16</td></tr> <tr><td style="padding: 2px 10px;">1536k</td><td style="padding: 2px 10px;">24</td></tr> </tbody> </table>	ニーモニック速度 (bit/s)	タイムスロット数	192k	3	256k	4	384k	6	512k	8	768k	12	1024k	16	1536k	24
ニーモニック速度 (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-1 PRI-N) 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="display: inline-table; 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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e											
RTX2000	RTX1000	RT300i	RT105i	RT105e													

7.3 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]	<ul style="list-style-type: none"> ○ <i>interface</i> PRI インタフェース名 ○ <i>pri_num</i> インタフェース番号 ○ <i>info</i> 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]	<table border="1" style="display: inline-table; 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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8. IPの設定

8.1 インタフェース共通の設定

8.1.1 IP パケットを扱うか否かの設定

[入力形式]	ip routing <i>routing</i> no ip routing [<i>routing</i>]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>routing</i> <ul style="list-style-type: none"> • 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]	<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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.1.2 IP アドレスの設定

[入力形式]	ip interface address <i>ip_address/mask</i> [<i>broadcast broadcast_ip</i>] ip interface address <i>dhcp</i> ip pp address <i>ip_address/mask</i> [<i>broadcast broadcast_ip</i>] no ip interface address [<i>ip_address/mask</i>] no ip pp address [<i>ip_address/mask</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>ip_adress</i>IP アドレス xxx.xxx.xxx.xxx (xxx は十進数) ◦ <i>dhcp</i>DHCP クライアントとして IP アドレスを取得することを示すキーワード ◦ <i>mask</i> <ul style="list-style-type: none"> • xxx.xxx.xxx.xxx (xxx は十進数) • 0x に続く十六進数 • マスクビット数 ◦ <i>broadcast_ip</i>.....ブロードキャスト IP アドレス 					
[説明]	<p>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。“<i>broadcast broadcast_ip</i>” 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。</p> <p><i>dhcp</i> を指定すると、設定直後に DHCP クライアントとして IP アドレスを取得する。また <i>dhcp</i> を指定している場合に no ip interface address を入力すると、取得していた IP アドレスの開放メッセージを DHCP サーバに送る。</p>					
[ノート]	<p>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。</p> <p>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。</p> <p>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。</p>					
[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]	<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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.1.3 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]	<ul style="list-style-type: none"> ◦ <i>interface</i> LAN インタフェース名 ◦ <i>ip_address</i> セカンダリ IP アドレス xxx.xxx.xxx.xxx (xxx は十進数) ◦ <i>dhcp</i> DHCP クライアントとして IP アドレスを取得することを示すキーワード ◦ <i>mask</i> <ul style="list-style-type: none"> • xxx.xxx.xxx.xxx (xxx は十進数) • 0x に続く十六進数 • マスクビット数 					
[説明]	LAN 側のセカンダリ IP アドレスとネットマスクを設定する。 dhcp を指定すると、設定直後に DHCP クライアントとして IP アドレスを取得する。					
[ノート]	セカンダリのネットワークでのブロードキャストアドレスは必ずディレクティッドブロードキャストアドレスが使われる。					
[適用モデル]	<table border="1" style="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.1.4 インタフェースの MTU の設定

[入力形式]	ip interface mtu mtu ip pp mtu mtu no ip interface mtu [mtu] no ip pp mtu [mtu]					
[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="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.1.5 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 service no ip simple-service [service]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>service</i> <ul style="list-style-type: none"> • on TCP/UDP の各種サービスを動作させる • off サービスを停止させる 					
[説明]	TCP/UDP の echo(7)、discard(9)、time(37) の各種サービスを動作させるか否かを設定する。サービスを停止すると該当のポートも閉じる。					
[デフォルト値]	on					
[適用モデル]	<table border="1" style="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.1.6 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]
- network
 - default デフォルト経路
 - IP アドレス 送り先のホスト / マスクビット数
 - 省略時は 32
 - gateway
 - IP アドレス xxx.xxx.xxx.xxx (xxx は十進数)
 - pp peer_num [dci=dci] ... PP インタフェースへの経路
 "dci=dci" が指定された場合は、フレームリレーの DLCI への経路
 - peer_num
 - 相手先情報番号
 - anonymous
 - pp anonymous name=name
 - name PAP/CHAP による名前
 - dhcp interface
 - interface DHCP にて与えられるデフォルトゲートウェイを使う場合の、DHCP クライアントとして動作する LAN インタフェース名 (送り先が Default の時のみ有効)
 - tunnel tunnel_num トンネルインタフェースへの経路
 - parameter 以下のパラメータを空白で区切り複数設定可能
 - filter number [number...] ... フィルタ型経路の指定
 - number フィルタの番号 (1..21474836) (空白で区切り複数設定可能)
 - metric metric メトリックの指定
 - metric
 - メトリック値 (1..15)
 - 省略時は 1
 - hide 出カインタフェースが PP インタフェースまたは TUNNEL インタフェースの場合のみ有効なオプションで、回線が接続されている場合だけ経路が有効になることを意味する
 - weight weight 異なる経路間の比率を表す値
 - weight
 - 経路への重み (1..2147483647)
 - 省略時は 1
- [説明] IPの静的経路を設定する。
gatewayのパラメータとしてフィルタ型経路を指定した場合には、記述されている順にフィルタを適用していき、適合したゲートウェイが選択される。
適合するゲートウェイが存在しない場合や、フィルタ型経路が指定されているゲートウェイが一つも記述されていない場合には、フィルタ型経路が指定されていないゲートウェイが選択される。
フィルタ型経路が指定されていないゲートウェイも存在しない場合には、その経路は存在しないものとして処理が継続される。
フィルタ型経路が指定されていないゲートウェイが複数記述された場合の経路の選択は、それらの経路を使用する時点でラウンドロビンにより決定される。
- filterが指定されていないゲートウェイが複数記述されている場合で、それらの経路を使うべき時にどちらを使うかは、始点 / 終点 IP アドレス、プロトコル、始点 / 終点ポート番号により識別されるストリームにより決定される。同じストリームのパケットは必ず同じゲートウェイに送出される。weightで値(例えば回線速度の比率)が指定されている場合には、その値の他のゲートウェイのweight値に対する比率に比例して、その経路に送出されるストリームの比率が上がる。
- いずれの場合でも、hide キーワードが指定されているゲートウェイは、回線が接続している場合のみ有効で、回線が接続していない場合には評価されない。
- [ノート] 既に存在する経路を上書きすることができる。
RTX2000では、複数のgatewayパラメータを指定できない。
- [設定例]
- デフォルトゲートウェイを 192.168.0.1 とする

```
# ip route default gateway 192.168.0.1
```
 - PP1 で接続している相手のネットワークは 192.168.1.0/24 である

```
# ip route 192.168.1.0/24 gateway pp 1
```
 - マルチホーミングによる負荷分散を行う。デフォルトゲートウェイとして2経路持ち、PP1には専用線128kで、PP2には専用線64kで接続しており、かつ各専用線ダウン時の経路を無効としてパケットロスを防ぐ。
 ※ NAT機能と専用線キー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]
- | | | | | |
|---------|---------|--------|--------|--------|
| RTX2000 | RTX1000 | RT300i | RT105i | RT105e |
|---------|---------|--------|--------|--------|

8.1.7 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 xxx (xxx は十進数)
 - * (ネットマスクの対応するビットが 8 ビットとも 0 と同じ。すべての IP アドレスに対応)
 - 間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。
 - *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 (*src_addr* 及び *dest_addr* がネットワークアドレスの場合のみ指定可)
 - xxx.xxx.xxx.xxx (xxx は十進数)
 - 0x に続く十六進数
 - マスクビット数
 - 省略時は 0xffffffff と同じ
 - *protocol* フィルタリングするパケットの種類
 - プロトコルを表す十進数 (0..255)
 - プロトコルを表すニーモニック

ニーモニック	十進数	説明
icmp	1	icmp パケット
icmp-error	-	特定の TYPE コードの icmp パケット
icmp-info	-	特定の TYPE コードの icmp パケット
tcp	6	tcp パケット
tcpfin	-	FIN フラグの立っている tcp パケット
tcprst	-	RST フラグの立っている tcp パケット
		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
 - ポート番号を表す十進数
 - ポート番号を表すニーモニック (一部)

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

- 間に - を挟んだ 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。

62 8.IPの設定

[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	RT105i	RT105e
---------	---------	--------	--------	--------

8.1.8 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 空白で区切られたフィルタ番号の並び (100 個以内)

[説明] フィルタセットを定義する。フィルタセットは、in/out のフィルタをそれぞれ定義し、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	RT105i	RT105e
---------	---------	--------	--------	--------

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

[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	RT105i	RT105e
---------	---------	--------	--------	--------

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

[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 アドレスがディレクテッドブロードキャストアドレス宛になっている IP パケットをルータ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	RT105i	RT105e
---------	---------	--------	--------	--------

8.1.11 動的フィルタの定義

[入力形式]	<pre>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...]</pre>					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>dyn_filter_num</i> 動的フィルタ番号 (1...21474836) ○ <i>srcaddr</i> 始点 IP アドレス ○ <i>dstaddr</i> 終点 IP アドレス ○ <i>protocol</i> プロトコルの二モニック <ul style="list-style-type: none"> • tcp • udp • ftp • tftp • domain • www • smtp • pop3 • telnet • netmeeting ○ <i>filter_list</i> ip filter コマンドで登録されたフィルタ番号のリスト ○ <i>option</i> <ul style="list-style-type: none"> • <i>syslog=switch</i> <ul style="list-style-type: none"> ■ <i>on</i> コネクションの通信履歴を SYSLOG に残す ■ <i>off</i> コネクションの通信履歴を SYSLOG に残さない • <i>timeout=time</i> <ul style="list-style-type: none"> ■ <i>time</i> 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]	<p>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。</p> <p>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 の回数も同様に無視される。</p> <p>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。</p>					
[デフォルト値]	<pre>syslog=on timeout=60</pre>					
[設定例]	<pre># ip filter 10 ** udp * snmp # ip filter dynamic 1 ** filter 10</pre>					
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.1.12 動的フィルタのタイムアウトの設定

[入力形式]	<pre>ip filter dynamic timer [option=timeout [option...]] no ip filter dynamic timer</pre>					
[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="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.1.13 侵入検知機能の動作の設定

[入力形式]	ip interface intrusion detection direction switch [option] ip pp intrusion detection direction switch [option] ip tunnel intrusion detection direction switch [option] no ip interface intrusion detection no ip pp intrusion detection no ip tunnel intrusion detection					
[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> <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]	<i>switch</i> = off <i>reject</i> = off					
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.1.14 TCPセッションのMSS制限の設定

[入力形式]	ip interface tcp mss limit mss ip pp tcp mss limit mss ip tunnel tcp mss limit mss no ip interface tcp mss limit [mss] no ip pp tcp mss limit [mss] no ip tunnel tcp mss limit [mss]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>mss</i> <ul style="list-style-type: none"> • MSS の最大長 (536 .. 1460) • <i>auto</i> 自動設定 • <i>off</i> 設定しない 					
[説明]	インタフェースを通過する TCPセッションのMSS を制限する。インタフェースを通過する TCP パケットを監視し、MSS オプションの値が設定値を越えている場合には、設定値に書き換える。キーワード auto を指定した場合には、インタフェースの MTU、もしくは PP インタフェースの場合で相手の MRU 値が分かる場合にはその MRU 値から計算した値に書き換える。					
[ノート]	PPPoE用の PP インタフェースに対しては、 pppoe tcp mss limit コマンドでも TCPセッションのMSS を制限することができる。このコマンドと pppoe tcp mss limit コマンドの両方が有効な場合は、MSS はどちらかより小さな方の値に制限される。					
[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: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.1.15 フィルタリングによるセキュリティの設定

[入力形式]	<pre> 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]] </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>direction</i> <ul style="list-style-type: none"> • <i>in</i> 受信したパケットのフィルタリング • <i>out</i> 送信するパケットのフィルタリング ◦ <i>filter_list</i> 空白で区切られたフィルタ番号の並び (100 個以内) ◦ <i>set_name</i> フィルタセットの名前を表す文字列 ◦ <i>dynamic</i> キーワード後に動的フィルタの番号を記述する 					
[説明]	<p>ip filter コマンドによるパケットのフィルタを組み合わせて、インタフェースで送受信するパケットの種類を制限する。</p> <p>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。</p>					
[ノート]	<p>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。</p> <pre> # ip filter 1 pass 192.168.0.0/24 * # ip filter 2 reject 192.168.0.1 # ip lan1 secure filter in 1 2 </pre> <p>この設定では、始点 IP アドレスが 192.168.0.1 であるパケットは、最初のフィルタ 1 で通過が決定してしまうため、フィルタ 2 での検査は行われず、そのため、フィルタ 2 は何も意味を持たない。フィルタリストを操作した結果、どのフィルタにも一致しないパケットは破棄される。</p> <p>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。</p>					
[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="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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

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

[入力形式]	<pre> ip fragment remove df-bit filter filter_num ... no ip fragment remove df-bit filter [filter_num ...] </pre>					
[パラメータ]	◦ <i>filter_num</i> ip filter コマンドで登録されたフィルタ番号					
[説明]	フォワーディングする IP パケットの内、フィルタに一致するものは DF ビットを 0 に書き換える。					
[ノート]	<p>DF ビットは経路 MTU 探索アルゴリズムで利用されるが、経路の途中に ICMP パケットをフィルタするファイアウォールなどがあるとアルゴリズムがうまく動作せず、特定の通信相手とだけは通信ができないなどの現象になることがある。このような現象は、「経路 MTU 探索ブラックホール (Path MTU Discovery Blackhole)」と呼ばれている。この経路 MTU 探索ブラックホールがある場合には、このコマンドでそのような相手との通信に関して DF ビットを 0 に書き換えてしまえば、経路 MTU 探索は正しく動作しなくなるものの、通信できなくなるということはない。</p>					
[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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.1.17 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 id tos** [precedence=*precedence*] *filter_num* [*filter_num_list*]
no ip tos supersede id [*tos*]

[パラメータ] ◦ *id* 識別番号 (1..65535)
 ◦ *tos* 書き換える TOS 値 (0..15)
 以下の二ーモニックが利用できる

normal	0
min-monetary-cost	1
max-reliability	2
max-throughput	4
min-delay	8

- *precedence*
 - PRECEDENCE 値 (0..7)
 - *precedence* を省略した場合、PRECEDENCE 値は変更しない
- *filter_num* 静的フィルタの番号 (1..100)
- *filter_num_list* 静的フィルタの番号 (1..100) の並び

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

[適用モデル]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

8.2 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	RT105i	RT105e
---------	---------	--------	--------	--------

8.3 PP 側の設定

8.3.1 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]	<ul style="list-style-type: none"> ○ ip_address <ul style="list-style-type: none"> • IP アドレス xxx.xxx.xxx.xxx (xxx は十進数) • 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 <ul style="list-style-type: none"> • 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>選択されている相手の PP 側の IP アドレスを設定する。</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copeの中から、IP アドレスを割り当てる。</p> <p>装着されている BRI/PRI インタフェースで利用できる ISDN Bch の数まで設定できる。</p> <p>PP として anonymous が選択された場合のみ有効である。</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 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。</p>					
[ノート]	<p>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。</p>					
[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]	<p>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。</p>					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.3.2 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 dhcpc [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 <ul style="list-style-type: none"> • 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。PP として anonymous が選択された場合のみ有効である。</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cope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 アドレス情報のみを取得し、そのアドレスを割り当てる。取得できなかった場合は、0.0.0.0 を割り当てる。</p> <p>RT300i では装着されている BRI インタフェースまたは 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。RTX1000、RT300i (モジュール無し)、RT105i は 2 個までとなる。</p>					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.4 RIPの設定

8.4.1 RIPを使用するか否かの設定

[入力形式]	rip use use no rip use use					
[パラメータ]	<ul style="list-style-type: none"> ○ use <ul style="list-style-type: none"> • on.....RIP を使用する • off.....RIP を使用しない 					
[説明]	RIPを使用するか否かを設定する。この機能を OFF にすると、すべてのインタフェースに対して RIP パケットを送信することはなくなり、受信した RIP パケットは無視される。					
[デフォルト値]	off					
[適用モデル]	<table border="1" style="width: 100%;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.4.2 RIPによる経路の優先度の設定

[入力形式]	rip preference preference no rip preference preference					
[パラメータ]	○ preference..... 1 以上の数値					
[説明]	RIPにより得られた経路の優先度を設定する。経路の優先度は 1 以上の数値で表され、数字が大きい程優先度が高い。スタティックと RIP など複数のプロトコルで得られた経路が食い違う場合には、優先度が高い方が採用される。優先度が同じ場合には時間的に先に採用された経路が有効となる。					
[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="width: 100%;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.4.3 RIPパケットの送信に関する設定

[入力形式]	ip interface rip send send [version version [broadcast]] ip pp rip send send [version version [broadcast]] ip tunnel rip send send [version version [broadcast]] no ip interface rip send [send...] no ip pp rip send [send...] no ip tunnel rip send [send...]					
[パラメータ]	<ul style="list-style-type: none"> ○ interfaceLAN インタフェース名 ○ send <ul style="list-style-type: none"> • on.....RIP パケットを送信する • off.....RIP パケットを送信しない ○ version送信する RIP のバージョン (1,2) ○ broadcast ip interface address コマンドで指定したブロードキャスト IP アドレス 					
[説明]	指定したインタフェースに対し、RIP パケットを送信するか否かを設定する。 "version version" で送信する RIP のバージョンを指定できる。					
[デフォルト値]	off (トンネルインタフェースの場合) on version 1 (その他のインタフェースの場合)					
[適用モデル]	<table border="1" style="width: 100%;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.4.4 RIP パケットの受信に関する設定

[入力形式]	ip interface rip receive receive [version <i>version</i> [<i>version</i>]] ip pp rip receive receive [version <i>version</i> [<i>version</i>]] ip tunnel rip receive receive [version <i>version</i> [<i>version</i>]] no ip interface rip receive [<i>receive</i> ...] no ip pp rip receive [<i>receive</i> ...] no ip tunnel rip receive [<i>receive</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>receive</i> <ul style="list-style-type: none"> • on RIP パケットを受信する • off RIP パケットを受信しない ○ <i>version</i> 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 <i>version</i> " 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]	off (トンネルインタフェースの場合) on version 1 (その他のインタフェースの場合)					
[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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.4.5 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> IP アドレスの並び (10 個以内) 					
[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="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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.4.6 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"> • in 受信した RIP のフィルタリング • out 送信する RIP のフィルタリング ○ <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 pass であればそれを処理し、reject であればその経路情報だけを破棄する。					
[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="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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.4.7 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] ◦ *interface*LAN インタフェース名
 ◦ *direction*
 • *in*受信した RIP に加算する
 • *out*送信する RIP に加算する
 ◦ *hop*加算する値 (0..15)

[説明] インタフェースで送受信する RIP に加算するホップ数を設定する。

[デフォルト値] 0

[適用モデル]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

8.4.8 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] ◦ *interface*LAN インタフェース名
 ◦ *type*
 • *none*認証しない
 • *text*テキスト型の認証を行う

[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	RT105i	RT105e
---------	---------	--------	--------	--------

8.4.9 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] ◦ *interface*LAN インタフェース名
 ◦ *hex_key*十六進数の列で表現された認証キー
 ◦ *text_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	RT105i	RT105e
---------	---------	--------	--------	--------

8.4.10 回線切断時の経路保持の設定

[入力形式]	ip pp rip hold routing rip_hold no ip pp rip hold routing [rip_hold]					
[パラメータ]	<ul style="list-style-type: none"> ○ rip_hold <ul style="list-style-type: none"> • 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]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.4.11 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]	<ul style="list-style-type: none"> ○ rip_action <ul style="list-style-type: none"> • interval ip pp rip connect interval コマンドで設定された時間間隔で RIP を送出する • update 経路情報が変わった場合にのみ RIP を送出する • none RIP を送出しない 					
[説明]	選択されている相手について回線接続時に RIP を送出する条件を設定する。					
[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]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.4.12 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]	<p>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。</p> <p>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。</p>					
[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]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.4.13 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]	<ul style="list-style-type: none"> ○ rip_action <ul style="list-style-type: none"> • none 回線切断時に RIP を送出しない • interval ip pp rip disconnect interval コマンドで設定された時間間隔で RIP を送出する • 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]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.4.14 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]	◦ <i>time</i>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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.4.15 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 no ip pp rip backup interface					
[パラメータ]	◦ <i>switch</i> <ul style="list-style-type: none"> • 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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.5 VRRP の設定

8.5.1 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]	◦ <i>interface</i>LAN インタフェース名 ◦ <i>vrid</i>VRRP グループ ID (1..255) ◦ <i>ip_address</i>仮想ルータの IP アドレス ◦ <i>priority</i>優先度 (1..254) ◦ <i>preempt</i>プリエンプトモード <ul style="list-style-type: none"> • on • off ◦ <i>auth</i>テキスト認証文字列 (8 文字以内)					
[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ならない。これらが食い違った場合の動作は予測できない。 <i>auth</i> 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]	<i>priority</i> および <i>preempt</i> 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]	<i>priority</i> =100 <i>preempt</i> =on <i>auth</i> = 認証なし					
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.5.2 シャットダウントリガの設定

[入力形式]	<pre> ip interface vrrp shutdown trigger vrid interface ip interface vrrp shutdown trigger vrid pp peer_num [dcli=dcli] ip interface vrrp shutdown trigger vrid route network [nextbop] no ip interface vrrp shutdown trigger vrid interface no ip interface vrrp shutdown trigger vrid pp peer_num [...] no ip interface vrrp shutdown trigger vrid route network </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>vrid</i> VRRP グループ ID (1..255) ○ <i>peer_num</i> 相手先情報番号 ○ <i>dcli</i> DLCI 番号 ○ <i>network</i> <ul style="list-style-type: none"> • ネットワークアドレス • IP アドレス / マスク長 • default ○ <i>nextbop</i> <ul style="list-style-type: none"> • インタフェース名 • IP アドレス 					
[説明]	<p>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。</p> <ul style="list-style-type: none"> • 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..... 指定した相手先情報番号に該当する回線で通信できなくなった場合にシャットダウンする。通信できなくなるとは、ケーブルが抜けるなどレイヤ 1 が落ちた場合と、以下の場合である。 <ul style="list-style-type: none"> □ 回線が 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、<i>nextbop</i> で指定したインタフェースもしくは IP アドレスで指定するゲートウェイに向いていない場合に、シャットダウンする。<i>nextbop</i> 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]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.6 バックアップの設定

8.6.1 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]	<pre> pp backup none pp backup pp peer_num pp backup interface ip_address pp backup tunnel tunnel_num no pp backup </pre>					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>none</i> バックアップ動作しない ○ <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>interface</i> バックアップとして使用する LAN インタフェース ○ <i>ip_address</i> ゲートウェイの IP アドレス ○ <i>tunnel_num</i> トンネルインタフェース番号 					
[説明]	<p>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。</p>					
[ノート]	<p>PP 毎のコマンドである。</p> <p>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 pp always-on on が同時に必要である。専用線の場合は pp always-on コマンドの代わりに pp keepalive use lcp-echo コマンドを使用する。</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: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.6.2 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="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.6.3 PP経路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..10000) ○ <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..10000) ○ <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。 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="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.6.4 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]	<ul style="list-style-type: none"> ○ log <ul style="list-style-type: none"> • 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.6.5 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 [retry-interval=retry-interval] [count=count][time=time] no pp keepalive interval [interval [count]]					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>interval</i> キープアライブパケットを送出する時間間隔 [秒](1..65535) ○ <i>retry-interval</i> キープアライブパケットの確認に一度失敗した後の送信間隔。単位は秒。キープアライブパケットが確認できれば、送信間隔はまた <i>interval</i> に戻る。 ○ <i>count</i> 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) ○ <i>time</i> キープアライブパケットの確認に失敗するようになってから回線断と判断するまでの時間。単位は秒。<i>count</i> パラメータとは同時には指定できない。 					
[説明]	<p>PP インタフェースでのキープアライブパケットの送信間隔と、回線断と判定するまでの再送回数および時間を設定する。</p> <p>送信したキープアライブパケットに対して返事が返って来ている間は <i>interval</i> で指定した間隔でキープアライブパケットを送信する。一度、返事が確認できなかった時には送信間隔が <i>retry-interval</i> パラメータの値に変更される。<i>count</i> パラメータに示された回数だけ連続して返事が確認できなかった時には回線断と判定する。</p> <p>回線断判定までの時間を <i>time</i> パラメータで指定した場合には、少なくとも指定した時間の間、キープアライブパケットの返事が連続して確認できない時に回線断と判定する。</p>					
[ノート]	<i>time</i> パラメータを指定した場合には、その値はキープアライブの間隔と再送回数によって再計算されるため、設定値とは異なる値が show config で表示されることがある。					
[デフォルト値]	<i>interval</i> = 30 <i>retry-interval</i> = 1 <i>count</i> = 6					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.6.6 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]	<ul style="list-style-type: none"> ○ <i>action</i> <ul style="list-style-type: none"> • 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.6.7 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 none lan backup interface pp peer_num lan backup interface backup_interface ip_address lan backup interface tunnel tunnel_num no lan backup interface					
[パラメータ]	<ul style="list-style-type: none"> ○ none.....バックアップ動作しない ○ interfaceバックアップ対象の LAN インタフェース名 ○ peer_num.....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 ○ backup_interfaceバックアップとして使用する LAN インタフェース ○ ip_addressゲートウェイの IP アドレス ○ tunnel_num.....トンネルインタフェース番号 					
[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。					
[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: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.6.8 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]	<ul style="list-style-type: none"> ○ interfaceバックアップ対象の LAN インタフェース名 ○ time <ul style="list-style-type: none"> • 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]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.6.9 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 lan keepalive use interface					
[パラメータ]	<ul style="list-style-type: none"> ○ interfaceバックアップ対象の LAN インタフェース名 ○ dest_ipキープアライブ確認先の IP アドレス ○ downwait.....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) ○ upwait..... 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) ○ off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="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.6.10 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] no lan keepalive interval 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>interval</i> キープアライブパケットを送出する時間間隔 (1.. 65535) ○ <i>count</i> ダウン検出を判定する回数 (3 ..100) 					
[説明]	<p>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。<i>count</i> 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。</p> <p>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。</p>					
[デフォルト値]	<i>interval</i> = 30 <i>count</i> = 6					
[適用モデル]	<table border="1" style="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.6.11 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]	<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>log</i> <ul style="list-style-type: none"> • 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]	<table border="1" style="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

8.6.12 ネットワーク監視機能の設定

[入力形式]	ip keepalive num kind interval count ip_address [ip_address ...][option=value ...] no ip keepalive num															
[パラメータ]	<ul style="list-style-type: none"> ○ <i>num</i> このコマンドの識別番号 (1..100) ○ <i>kind</i> 監視方式 <ul style="list-style-type: none"> • icmp-echo ICMP Echo を使用する ○ <i>interval</i> キープアライブの送信間隔秒数 (1..65535) ○ <i>count</i> 到達性がないと判断するまでに送信する回数 (3..100) ○ <i>ip_address</i> 送信先の IP アドレス ○ OPTION = VALUE 列 <table border="1" style="margin-left: 40px; border-collapse: collapse; width: 60%;"> <thead> <tr> <th style="text-align: left;">OPTION</th> <th style="text-align: left;">VALUE</th> <th style="text-align: left;">説明</th> </tr> </thead> <tbody> <tr> <td>log</td> <td>on</td> <td>SYSLD を出力する</td> </tr> <tr> <td></td> <td>off</td> <td>SYSLD を出力しない</td> </tr> <tr> <td>upwait</td> <td>秒数</td> <td>到達性があると判断するまでの待機時間 (1..1000000)</td> </tr> <tr> <td>downwait</td> <td>秒数</td> <td>到達性がないと判断するまでの待機秒数 (1..1000000)</td> </tr> </tbody> </table>	OPTION	VALUE	説明	log	on	SYSLD を出力する		off	SYSLD を出力しない	upwait	秒数	到達性があると判断するまでの待機時間 (1..1000000)	downwait	秒数	到達性がないと判断するまでの待機秒数 (1..1000000)
OPTION	VALUE	説明														
log	on	SYSLD を出力する														
	off	SYSLD を出力しない														
upwait	秒数	到達性があると判断するまでの待機時間 (1..1000000)														
downwait	秒数	到達性がないと判断するまでの待機秒数 (1..1000000)														
[説明]	指定した IP アドレスに対して ICMP Echo を送信し、その返事を受信できるかどうかを判定する。															
[ノート]	Rev.7.01 以上で実行可能															
[デフォルト値]	log = off upwait = 5 downwait = 5															
[適用モデル]	<table border="1" style="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e										
RTX2000	RTX1000	RT300i	RT105i	RT105e												

9. IPX の設定

9.1 インタフェース共通の設定

9.1.1 IPX パケットを扱うか否かの設定

[入力形式]	ipx routing <i>routing</i> no ipx routing [<i>routing</i>]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>routing</i> <ul style="list-style-type: none"> • 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]	<table border="1" style="display: inline-table;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

9.1.2 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 [<i>network node_num socket bop</i>]												
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>service_type</i> サービスタイプ <ul style="list-style-type: none"> • 十進数 (0..65535) • 0x に続く 4 桁以内の十六進数 • file 0x0004 の二モニック • printer 0x0007 の二モニック ◦ <i>server_name</i> サーバ名 <ul style="list-style-type: none"> • 'A' ~ 'Z','0' ~ '9','-',':','@' で構成された文字列 (47 文字以内) ◦ <i>network</i> サーバの IPX ネットワーク番号 (0:0:0:1 .. FF:FF:FF:FE) ◦ <i>node_num</i> サーバの IPX ノード番号 (0:0:0:0:1 .. FF:FF:FF:FF:FE) ◦ <i>socket</i> ソケット番号 <ul style="list-style-type: none"> • 十進数 (0..65535) • 0x に続く 4 桁以内の十六進数 • プロトコルを表す二モニック <table border="1" style="margin-left: 20px;"> <tr><td>ncp</td><td>0x0451</td></tr> <tr><td>sap</td><td>0x0452</td></tr> <tr><td>rip</td><td>0x0453</td></tr> <tr><td>netbios</td><td>0x0455</td></tr> <tr><td>diag</td><td>0x0456</td></tr> <tr><td>serialization</td><td>0x0457</td></tr> </table> ◦ <i>bop</i> ホップカウント (1..14) 	ncp	0x0451	sap	0x0452	rip	0x0453	netbios	0x0455	diag	0x0456	serialization	0x0457
ncp	0x0451												
sap	0x0452												
rip	0x0453												
netbios	0x0455												
diag	0x0456												
serialization	0x0457												
[説明]	SAP テーブルを設定する。												
[適用モデル]	<table border="1" style="display: inline-table;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e							
RTX2000	RTX1000	RT300i	RT105i	RT105e									

9.1.3 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 [<i>response</i>]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>response</i> <ul style="list-style-type: none"> • 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]	<table border="1" style="display: inline-table;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

9.1.4 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

- 0:0:0:1 FF:FF:FF:FE (2 桁以内の十六進数以外に '*' 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

- 0:0:0:0:0:1 FF:FF:FF:FF:FF:FE (2 桁以内の十六進数以外に '*' も指定可)
- * (すべての IPX ノード番号)
- 省略時は一つの * 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

- 十進数 (0..255)
- 十六進数 (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)
- 省略時は一つの * と同じ

○ *src_socket* 始点ソケット番号

- 十進数 (0..65535)
- 0x を先頭に持つ 4 桁以内の十六進数
- 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)
- 省略時は一つの * 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	RT105i	RT105e
---------	---------	--------	--------	--------

9.2 LAN 側の設定

9.2.1 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] ○ *interface*LAN 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。

<i>type</i>	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	RT105i	RT105e
---------	---------	--------	--------	--------

9.2.2 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] ○ *interface*LAN インタフェース名
 ○ *network*IPX 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	RT105i	RT105e
---------	---------	--------	--------	--------

9.2.3 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	RT105i	RT105e
---------	---------	--------	--------	--------

9.2.4 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]	<ul style="list-style-type: none"> ◦ <i>interface</i> LAN インタフェース名 ◦ <i>network</i> 終点 IPX ネットワーク番号 (0:0:0:1 .. FF:FF:FF:FE) ◦ <i>gateway</i> ゲートウェイの IPX ノード番号 (0:0:0:0:1 .. FF:FF:FF:FF:FE) ◦ <i>hop</i> ホップカウント (1..14) ◦ <i>ticks</i> 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]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

9.2.5 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]	<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 側から入ってくる方向でフィルタを適用 • <i>out</i> LAN 側へ出ていく方向でフィルタを適用 ◦ <i>filter_list</i> フィルタ番号の並び (100 個以内) 					
[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]	<p>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。</p> <pre>ipx filter 1 pass 0:0:1:* ipx filter 2 reject 0:0:1:1 ipx lan secure filter in 1 2</pre> <p>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。</p> <p>どのフィルタにも一致しない場合は破棄になる。</p>					
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

9.3 PP 側相手毎の IPX の設定

9.3.1 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]	<ul style="list-style-type: none"> ◦ <i>routing</i> <ul style="list-style-type: none"> • <i>on</i> PP 側に IPX パケットをルーティングする • <i>off</i> 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]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

9.3.2 PP 側 IPX ネットワーク番号の設定

[入力形式]	ipx pp network <i>network</i> [<i>node_num</i>] no ipx pp network [<i>network</i> [<i>node_num</i>]]					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>network</i>IPX ネットワーク番号 (0:0:0:1..FF:FF:FF:FE) ○ <i>node_num</i>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]	<table border="1" style="width: 100%; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

9.3.3 経路情報の追加

[入力形式]	ipx pp route <i>network</i> [<i>name</i>] <i>bop</i> [<i>tick</i>] ipx pp route <i>network</i> [<i>dldci=dldci_num</i>] <i>bop</i> [<i>tick</i>] no ipx pp route <i>network</i> [<i>network</i> ...]					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>network</i>終点 IPX ネットワーク番号 (0:0:0:1..FF:FF:FF:FE) ○ <i>name</i>名前 (16 文字以内) ○ <i>bop</i>ホップカウント (1..14) ○ <i>tick</i>ティック (1..65535) ○ <i>dldci_num</i>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。 <i>name</i> 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]	<table border="1" style="width: 100%; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

9.3.4 IPXWAN 使用の設定

[入力形式]	ipx pp ipxwan use <i>use</i> no ipx pp ipxwan use [<i>use</i>]					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>use</i> <ul style="list-style-type: none"> ● 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]	<table border="1" style="width: 100%; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

9.3.5 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 <i>network</i> no ipx pp ipxwan primnet [<i>network</i>]					
[パラメータ]	○ <i>network</i>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]	<table border="1" style="width: 100%; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

9.3.6 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]	<ul style="list-style-type: none"> ○ send <ul style="list-style-type: none"> • 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 • update RIP/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]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

9.3.7 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]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

9.3.8 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]	<ul style="list-style-type: none"> ○ send <ul style="list-style-type: none"> • 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]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

9.3.9 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]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

9.3.10 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 <i>bold</i> no ipx pp ripsap hold [<i>bold</i>]					
[パラメータ]	◦ <i>bold</i> <ul style="list-style-type: none"> • 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]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

9.3.11 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 <i>interval max</i> no ipx pp ipxwan retry [<i>interval max</i>]					
[パラメータ]	◦ <i>interval</i>秒数 (10..21474836) ◦ <i>max</i>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]	<i>interval</i> = 20 <i>max</i> = 3					
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

9.3.12 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]	◦ <i>proxy</i> <ul style="list-style-type: none"> • 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="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

9.3.13 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="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

9.3.14 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> <ul style="list-style-type: none"> • 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="text-align: center;">RTX2000</td> <td style="text-align: center;">RTX1000</td> <td style="text-align: center;">RT300i</td> <td style="text-align: center;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

9.3.15 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 <i>t1</i> [<i>t2</i> [<i>t3</i>]] no ipx pp spx keepalive timer <i>t1</i> [<i>t2</i> [<i>t3</i>]]					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>t1</i> 秒数 (30..21474836) ○ <i>t2</i> 秒数 (30..65535) ○ <i>t3</i> 秒数 (1..65535) 					
[説明]	<p>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。</p> <ul style="list-style-type: none"> ○ <i>t1</i> 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を確認する。 ○ <i>t2</i> 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。 ○ <i>t3</i> 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]	<i>t1</i> = 7200 <i>t2</i> = 60 <i>t3</i> = 10					
[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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

9.3.16 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 <i>filter</i> no ipx pp serialization filter [<i>filter</i>]					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>filter</i> <ul style="list-style-type: none"> • 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]	<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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

9.3.17 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*空白で区切られたフィルタ番号の並び (30 個以内)

[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	RT105i	RT105e
---------	---------	--------	--------	--------

10. ブリッジの設定

10.1 インタフェース共通の設定

10.1.1 ブリッジ使用許可の設定

【入力形式】	bridge use <i>use</i> no bridge use [<i>use</i>]					
【パラメータ】	<ul style="list-style-type: none"> ◦ <i>use</i> <ul style="list-style-type: none"> • 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。同様に ipv6 routing on であれば、IPv6 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】	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

10.1.2 ブリッジするインタフェースの設定

【入力形式】	bridge group <i>interface_list</i> no bridge group [<i>interface_list</i>]					
【パラメータ】	<ul style="list-style-type: none"> ◦ <i>interface_list</i> <ul style="list-style-type: none"> • 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】	<ul style="list-style-type: none"> ◦ 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】	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

10.1.3 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"> • on 行う • off 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="display: inline-table; border-collapse: collapse;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

10.1.4 ラーニング情報消去タイマの設定

[入力形式]	bridge learning expire time no bridge learning expire [time]					
[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..... 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。 off 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%; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

10.1.5 ブリッジのフィルタの設定

[入力形式]	bridge filter filter_num pass_reject src_mac[dst_mac[offset byte_list]] bridge filter filter_num [pass_reject src_mac[dst_mac[offset byte_list]]]					
[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"> • xx:xx:xx:xx:xx:xx (xx は十六進数、または *) • * (すべての MAC アドレスに対応) ◦ <i>dst_mac</i> <ul style="list-style-type: none"> • 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> オフセットを表す十進数 (イーサネットフレームの始点 MAC アドレスの直後を 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"> ▪ xx(xx は 2 桁の十六進数) ▪ 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]	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]	<table border="1" style="width: 100%; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

10.2 LAN 側の設定

10.2.1 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 は十六進数) 					
[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%; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

10.2.2 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: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

10.3 PP 側相手毎のブリッジの設定

10.3.1 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 は十六進数) ◦ <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: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

10.3.2 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]	<ul style="list-style-type: none"> ◦ <i>direction</i> <ul style="list-style-type: none"> • <i>in</i> PP 側から入ってくるパケットのフィルタリング • <i>out</i> PP 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]	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]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11. PPP の設定

11.1 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]] [mscbcp] [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
 - *mscbcp*.....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。

mscbcp 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	RT105i	RT105e
---------	---------	--------	--------	--------

11.2 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ことを示すキーワード

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

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

arrive-only キーワードが指定された場合には、着信時にのみ 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。

[デフォルト値] none

[適用モデル]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

11.3 受け入れる認証タイプの設定

[入力形式]	pp auth accept <i>accept</i> [<i>accept</i>] no pp auth accept [<i>accept</i>]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>accept</i> • <i>pap</i> PAP による認証を受け入れる • <i>chap</i> CHAP による認証を受け入れる • <i>mschap</i> MSCHAP による認証を要求する • <i>mschap-v2</i> MSCHAP Version2 による認証を要求する 					
[説明]	<p>相手からの PPP 認証要求を受け入れるかどうか設定する。発信時には常に適用される。anonymous でない着信の場合には発番号により PP が選択されてから適用される。anonymous での着信時には、発番号による PP の選択が失敗した場合に適用される。</p> <p>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。</p>					
[デフォルト値]	認証を受け入れない					
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.4 自分の名前とパスワードの設定

[入力形式]	pp auth myname <i>myname password</i> no pp auth myname [<i>myname password</i>]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>myname</i> 名前 (64 文字以内) ◦ <i>password</i> 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]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

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

[入力形式]	pp auth multi connect prohibit <i>prohibit</i> no pp auth multi connect prohibit [<i>prohibit</i>]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>prohibit</i> • <i>on</i> 禁止する • <i>off</i> 禁止しない 					
[説明]	pp auth username コマンドで登録した同一 <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="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.6 LCP 関連の設定

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

[入力形式]	ppp lcp acfc acfc no ppp lcp acfc [<i>acfc</i>]					
[パラメータ]	<ul style="list-style-type: none"> ○ <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="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.6.2 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]	<ul style="list-style-type: none"> ○ <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="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.6.3 Maximum Receive Unit オプション使用の設定

[入力形式]	ppp lcp mru mru [<i>length</i>] no ppp lcp mru [<i>mru</i> [<i>length</i>]]					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>mru</i> <ul style="list-style-type: none"> • on.....用いる • off.....用いない ○ <i>length</i>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、 <i>length</i> 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]	<i>mru</i> = on <i>length</i> = 1792					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.6.4 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]	○ <i>pfc</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 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.6.5 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]	○ <i>time</i> ミリ秒 (20..10000)					
[説明]	選択されている相手について [PPP,LCP] の 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="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.6.6 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" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.6.7 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" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.6.8 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" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

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

[入力形式]	ppp lcp silent <i>switch</i> no ppp lcp silent					
[パラメータ]	◦ <i>switch</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" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.7 PAP 関連の設定

11.7.1 pap-restart パラメータの設定

[入力形式]	ppp pap restart <i>time</i> no ppp pap 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,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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.7.2 pap-max-authreq パラメータの設定

[入力形式]	ppp pap maxauthreq <i>count</i> no ppp pap maxauthreq [<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,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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.8 CHAP 関連の設定

11.8.1 chap-restart パラメータの設定

[入力形式]	ppp chap restart <i>time</i> no ppp chap 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,CHAP] challenge 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="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.8.2 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]	○ <i>count</i> 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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.9 IPCP 関連の設定

11.9.1 Van Jacobson Compressed TCP/IP 使用の設定

[入力形式]	ppp ipcp vjc compression no ppp ipcp vjc [compression]					
[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"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.9.2 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 negotiation no ppp ipcp ipaddress [negotiation]					
[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"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.9.3 ipcp-restart パラメータの設定

[入力形式]	ppp ipcp restart time no ppp ipcp 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,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"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.9.4 ipcp-max-terminate パラメータの設定

[入力形式]	ppp ipcp maxterminate count no ppp ipcp 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,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"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.9.5 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	RT105i	RT105e
---------	---------	--------	--------	--------

11.9.6 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	RT105i	RT105e
---------	---------	--------	--------	--------

11.9.7 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] ◦ *server1, server2*IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))
- [説明] WINS (Windows Internet Name Service) サーバの 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	RT105i	RT105e
---------	---------	--------	--------	--------

11.9.8 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 msextn msextn**
no ppp ipcp msextn [msextn]
- [パラメータ] ◦ *msextn*
 • 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	RT105i	RT105e
---------	---------	--------	--------	--------

11.10 IPXCP 関連の設定

11.10.1 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>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.10.2 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>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.10.3 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>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.10.4 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>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.11 BCP 関連の設定

11.11.1 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]	◦ <i>lan_id</i> <ul style="list-style-type: none"> • 十六進数 (0x1 .. 0xffffffffe) • off..... LAN-identification を使用しない 					
[説明]	選択されている相手について LAN-identification の値を設定する。					
[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>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.11.2 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] 選択されている相手について 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	RT105i	RT105e
---------	---------	--------	--------	--------

11.11.3 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	RT105i	RT105e
---------	---------	--------	--------	--------

11.11.4 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	RT105i	RT105e
---------	---------	--------	--------	--------

11.11.5 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	RT105i	RT105e
---------	---------	--------	--------	--------

11.11.6 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	RT105i	RT105e
---------	---------	--------	--------	--------

11.12 MSCBCP 関連の設定

11.12.1 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]	○ <i>time</i> 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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.12.2 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]	○ <i>count</i> 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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.13 CCP 関連の設定

11.13.1 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]	○ <i>type</i> <ul style="list-style-type: none"> • <i>stac0</i> Stac LZS で圧縮する • <i>stac</i> Stac LZS で圧縮する • <i>costac</i> Stac LZS で圧縮する (接続相手が Cisco ルータの場合) • <i>mppe-40</i> 40bit MPPE で暗号化する • <i>mppe-128</i> 128bit MPPE で暗号化する • <i>mppe-any</i> 40bit, 128bit MPPE いずれかの暗号化を行う • <i>none</i> 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]	<p>Van Jacobson Compressed TCP/IP との併用も可能である。</p> <p><i>type</i> に <i>stac</i> を指定した時、回線状態が悪い場合や、高負荷で、パケットロスが頻繁に起きると、通信が正常に行えなくなることがある。このような場合、自動的に「圧縮なし」になる。その後、リスタートまで「圧縮なし」のままである。このような状況が改善できない時は、<i>stac0</i> を指定すればよい。ただしその時は接続先も <i>stac0</i> に対応していなければならない。<i>stac0</i> は <i>stac</i> よりも圧縮効率は落ちる。</p> <p>接続相手が Cisco ルータの場合に <i>stac</i> を適用する通信できないことがある。そのような場合には、設定を <i>costac</i> に変更すると通信が可能になることがある。</p> <p><i>mppe-40</i>, <i>mppe-128</i>, <i>mppe-any</i> 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。</p>					
[デフォルト値]	<i>stac</i>					
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.13.2 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	RT105i	RT105e
---------	---------	--------	--------	--------

11.13.3 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	RT105i	RT105e
---------	---------	--------	--------	--------

11.13.4 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	RT105i	RT105e
---------	---------	--------	--------	--------

11.13.5 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	RT105i	RT105e
---------	---------	--------	--------	--------

11.14 IPV6CP 関連の設定

11.14.1 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	RT105i	RT105e
---------	---------	--------	--------	--------

11.15 MP 関連の設定

11.15.1 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]	<ul style="list-style-type: none"> ○ use <ul style="list-style-type: none"> • on 使用する • off 使用しない 					
[説明]	<p>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。</p> <p>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。</p>					
[デフォルト値]	off					
[適用モデル]	<table border="1" style="width: 100%; text-align: center;"> <tr> <td style="background-color: #cccccc;">RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.15.2 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]	<ul style="list-style-type: none"> ○ type <ul style="list-style-type: none"> • 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]	<p>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。通常はデフォルト値のように自分が 1B 目の発信側の場合だけ制御するようにしておく。</p>					
[デフォルト値]	call					
[適用モデル]	<table border="1" style="width: 100%; text-align: center;"> <tr> <td style="background-color: #cccccc;">RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.15.3 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]	<ul style="list-style-type: none"> ○ 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]	<p>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。</p> <p>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。</p>					
[デフォルト値]	<pre>call_load = 70 call_count = 1 disc_load = 30 disc_count = 2</pre>					
[適用モデル]	<table border="1" style="width: 100%; text-align: center;"> <tr> <td style="background-color: #cccccc;">RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.15.4 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]	<ul style="list-style-type: none"> ○ number リンク数 					
[説明]	<p>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。</p>					
[デフォルト値]	2					
[適用モデル]	<table border="1" style="width: 100%; text-align: center;"> <tr> <td style="background-color: #cccccc;">RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.15.5 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	RT105i	RT105e
---------	---------	--------	--------	--------

11.15.6 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	RT105i	RT105e
---------	---------	--------	--------	--------

11.15.7 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	RT105i	RT105e
---------	---------	--------	--------	--------

11.16 BACP 関連の設定

11.16.1 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	RT105i	RT105e
---------	---------	--------	--------	--------

11.16.2 bacp-max-terminate パラメータの設定

[入力形式]	ppp bacp maxterminate <i>count</i> no ppp bacp 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, 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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.16.3 bacp-max-configure パラメータの設定

[入力形式]	ppp bacp maxconfigure <i>count</i> no ppp bacp maxconfigure [<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, 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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.16.4 bacp-max-failure パラメータの設定

[入力形式]	ppp bacp maxfailure <i>count</i> no ppp bacp maxfailure [<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, 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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.17 BAP関連の設定

11.17.1 bap-restart パラメータの設定

[入力形式]	ppp bap restart <i>time</i> no ppp bap 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, 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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.17.2 bap-max-retry パラメータの設定

[入力形式]	ppp bap maxretry <i>count</i> no ppp bap maxretry [<i>count</i>]					
[パラメータ]	○ <i>count</i> 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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.18 PPPoE 関連の設定

11.18.1 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	RT105i	RT105e
---------	---------	--------	--------	--------

11.18.2 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	RT105i	RT105e
---------	---------	--------	--------	--------

11.18.3 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	RT105i	RT105e
---------	---------	--------	--------	--------

11.18.4 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	RT105i	RT105e
---------	---------	--------	--------	--------

11.18.5 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	RT105i	RT105e
---------	---------	--------	--------	--------

11.18.6 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]	◦ <i>time</i> 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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.18.7 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]	◦ <i>times</i> 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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.18.8 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]	◦ <i>time</i> 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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.18.9 PPPoE セッションの切断タイムの設定

[入力形式]	pppoe disconnect time time no pppoe disconnect time					
[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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.18.10 サービス名の指定

[入力形式]	pppoe service-name name no pppoe service-name					
[パラメータ]	◦ <i>name</i> 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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

11.18.11 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)
- autoMSS を MTU の値に応じて制限する
- offMSS 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) を制限するか否かを設定する。

[ノート] このコマンドと **ip interface tcp mss limit** コマンドの両方が有効な場合は、MSS はどちらかより小さな方の値に制限される。

[デフォルト値] auto

[適用モデル]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

12. 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、ネットワークマスク、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。

12.1 DHCP サーバ・リレーエージェント機能

12.1.1 DHCP の動作の設定

【入力形式】	dhcp service <i>type</i> no dhcp service [<i>type</i>]					
【パラメータ】	○ <i>type</i> <ul style="list-style-type: none"> • 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】	<table border="1" style="display: inline-table;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

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

12.1.2 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	RT105i	RT105e
--	---------	---------	--------	--------	--------

12.1.3 リースする IP アドレスの重複をチェックするか否かの設定

[入力形式] **dhcp duplicate check check1 check2**
no dhcp duplicate check

[パラメータ]

- *check1*.....LAN 内を対象とするチェックの確認用待ち時間
 - ミリ秒 (1..1000)
 - off.....LAN 内を対象とするチェックを行わない
- *check2*.....LAN 外 (DHCP リレーエージェント経由) を対象とするチェックの確認用待ち時間
 - 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] *check1* = 100
check2 = 500

[適用モデル]

	RTX2000	RTX1000	RT300i	RT105i	RT105e
--	---------	---------	--------	--------	--------

12.1.4 DHCP スコープの定義

[入力形式]	dhcp scope <i>scope_num ip_address-ip_address/netmask</i> [except <i>ex_ip</i> ...] [<i>gateway gw_ip</i>] [<i>expire time</i>] [<i>maxexpire time</i>] no dhcp scope <i>scope_num</i> [<i>ip_address-ip_address/netmask</i> [except <i>ex_ip</i> ...] [<i>gateway gw_ip</i>] [<i>expire time</i>] [<i>maxexpire time</i>]]					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>scope_num</i> スコープ番号 (1..65535) ○ <i>ip_address-ip_address</i> .. 対象となるサブネットで割り当てる IP アドレスの範囲 ○ <i>netmask</i> <ul style="list-style-type: none"> • xxx.xxx.xxx.xxx (xxx は十進数) • 0xに続く十六進数 • マスクビット数 ○ <i>ex_ip</i> 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) ○ <i>gw_ip</i> 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 ○ <i>time</i> 時間 <ul style="list-style-type: none"> • 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 アドレスの範囲を設定する。 除外 IP アドレスは複数指定できる。リース期間としては無期限を指定できるほか、DHCP クライアントから要求があった場合の許容最大リース期間を指定できる。					
[ノート]	ひとつのネットワークについて複数の DHCP スコープを設定することはできない。複数の DHCP スコープで同一の IP アドレスを含めることはできない。IP アドレス範囲にネットワークアドレス、ブロードキャストアドレスを含む場合、割り当て可能アドレスから除外される。 DHCP リレーエージェントを経由しない DHCP クライアントに対して gateway キーワードによる設定パラメータが省略されている場合にはルータ自身の 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]	<i>expire time</i> = 72:00 <i>maxexpire time</i> = 72:00					
[適用モデル]	<table border="1" style="width: 100%; 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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

12.1.5 DHCP 予約アドレスの設定

[入力形式]	dhcp scope bind <i>scope_num ip_address</i> [<i>type</i>] <i>id</i> dhcp scope bind <i>scope_num ip_address mac_address</i> dhcp scope bind <i>scope_num ip_address</i> <i>ipcp</i> no dhcp scope bind <i>scope_num ip_address</i>
[パラメータ]	<ul style="list-style-type: none"> ○ <i>scope_num</i> スコープ番号 (1..65535) ○ <i>ip_address</i> 予約する IP アドレス ○ <i>type</i> Client-Identifier オプションの <i>type</i> フィールドを決定する <ul style="list-style-type: none"> ■ <i>text</i> 0x00 ■ <i>ethernet</i> 0x01 ○ <i>id</i> <ul style="list-style-type: none"> • <i>type</i> が <i>ethernet</i> の場合 MAC アドレス • <i>type</i> が <i>text</i> の場合 文字列 • <i>type</i> が省略された場合 2 桁十六進数の列で先頭は <i>type</i> フィールド • <i>mac_address</i> xx:xx:xx:xx:xx:xx (xx は十六進数) 予約 DHCP クライアントの MAC アドレス ○ <i>ipcp</i> 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、 <i>scope_num</i> 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。 <i>ipcp</i> 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、 <i>ipcp</i> で与えるアドレスは LAN 側のスコープから選択される。 コマンドの第 1 書式を使う場合は、あらかじめ dhcp server rfc2131 compliant on あるいは use-clientid 機能を使用するよう設定されていないといけない。また dhcp server rfc2131 compliant off あるいは use-clientid 機能が使用されないよう設定された時点で、コマンドの第 2 書式によるもの以外の予約は消去される。

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

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

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

[設定例]

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

1. **dhcp server rfc2131 compliant** on あるいは use-clientid 機能ありの場合

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

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

dhcp server rfc2131 compliant on あるいは use-clientid 機能ありでアドレスをリースする場合、DHCP サーバは 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、ここで表示される十六進文字列あるいは文字列を使用する。

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

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

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

なお、クライアントとの相互動作に関して下記の留意点がある。

- 個々の機能を単独で用いるとクライアント側の思わぬ動作を招く可能性があるため、**dhcp server rfc2131 compliant** on あるいは **dhcp server rfc2131 compliant** off で使用することを推奨する。
- ルータの再起動、スコープの再設定などでリース情報が消去されている場合、アドレス延長要求時、あるいはリース期間内のクライアントの再起動時、クライアントの使用する IP アドレスが変わることがある。
 - これを防ぐために **dhcp server rfc2131 compliant** on (あるいは remain-silent 機能) が有効である場合がある。この設定では、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	RT105i	RT105e
---------	---------	--------	--------	--------

12.1.6 DHCP オプションの設定

[入力形式]	dhcp scope option <i>scope_num option=value</i> no dhcp scope option <i>scope_num [option=value]</i>																												
[パラメータ]	<ul style="list-style-type: none"> ○ <i>scope_num</i> スコープ番号 (1..65535) ○ <i>option</i> オプション番号 (1..49,64..76,128..254) またはニーモニック <ul style="list-style-type: none"> • 主なニーモニック <table border="1" style="margin-left: 40px; border-collapse: collapse;"> <tr><td>router</td><td>3</td></tr> <tr><td>dns</td><td>6</td></tr> <tr><td>hostname</td><td>12</td></tr> <tr><td>domain</td><td>15</td></tr> <tr><td>wins_server</td><td>44</td></tr> </table> ○ <i>value</i> オプション値 <ul style="list-style-type: none"> • 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。 <table border="1" style="margin-left: 40px; border-collapse: collapse;"> <tr><td>1 オクテット整数</td><td>0..255</td></tr> <tr><td>2 オクテット整数</td><td>0..65535</td></tr> <tr><td>2 オクテット数の配列</td><td>2 オクテット整数をコンマ (,) で並べたもの</td></tr> <tr><td>4 オクテット整数</td><td>0..4294967295</td></tr> <tr><td>IP アドレス</td><td>IP アドレス</td></tr> <tr><td>IP アドレスの配列</td><td>IP アドレスをコンマ (,) で並べたもの</td></tr> <tr><td>文字列</td><td>文字列</td></tr> <tr><td>スイッチ</td><td>"on", "off", "1", "0" のいずれか</td></tr> <tr><td>バイナリ</td><td>2 桁十六進数をコンマ (,) で並べたもの</td></tr> </table> 	router	3	dns	6	hostname	12	domain	15	wins_server	44	1 オクテット整数	0..255	2 オクテット整数	0..65535	2 オクテット数の配列	2 オクテット整数をコンマ (,) で並べたもの	4 オクテット整数	0..4294967295	IP アドレス	IP アドレス	IP アドレスの配列	IP アドレスをコンマ (,) で並べたもの	文字列	文字列	スイッチ	"on", "off", "1", "0" のいずれか	バイナリ	2 桁十六進数をコンマ (,) で並べたもの
router	3																												
dns	6																												
hostname	12																												
domain	15																												
wins_server	44																												
1 オクテット整数	0..255																												
2 オクテット整数	0..65535																												
2 オクテット数の配列	2 オクテット整数をコンマ (,) で並べたもの																												
4 オクテット整数	0..4294967295																												
IP アドレス	IP アドレス																												
IP アドレスの配列	IP アドレスをコンマ (,) で並べたもの																												
文字列	文字列																												
スイッチ	"on", "off", "1", "0" のいずれか																												
バイナリ	2 桁十六進数をコンマ (,) で並べたもの																												
[説明]	スコープに対して送信する DHCP オプションを設定する。 dns server コマンドや wins server コマンドなどでも暗黙のうちに DHCP オプションを送信していたが、それを明示的に指定できる。また、暗黙の DHCP オプションではスコープでオプションの値を変更することはできないが、このコマンドを使えばそれも可能になる。																												
[ノート]	no dhcp scope コマンドでスコープが削除されるとオプションの設定もすべて消える。																												
[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>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e																							
RTX2000	RTX1000	RT300i	RT105i	RT105e																									

12.1.7 DHCP サーバの指定の設定

[入力形式]	dhcp relay server <i>host1 [host2 [host3 [host4]]]</i> no dhcp relay server					
[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; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

12.1.8 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; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

12.1.9 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]	◦ <i>time</i>秒数 (0..65535)					
[説明]	DHCP BOOTREQUEST パケットの <i>secs</i> 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 <i>secs</i> 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

12.2 DHCP クライアント機能

12.2.1 DHCP クライアントのホスト名の設定

[入力形式]	dhcp client hostname interface primary bost dhcp client hostname interface secondary bost dhcp client hostname pp peer_num bost dhcp client hostname pool pool_num bost no dhcp client hostname interface primary [bost] no dhcp client hostname interface secondary [bost] no dhcp client hostname pp peer_num [bost] no dhcp client hostname pool pool_num [bost]					
[パラメータ]	◦ <i>interface</i>LAN インタフェース名 ◦ <i>peer_num</i> • 相手先情報番号 • anonymous. ◦ <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>bost</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="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

12.2.2 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]	◦ <i>interface</i>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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

12.2.3 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]	<ul style="list-style-type: none"> ◦ <i>interface</i> LAN インタフェース名 ◦ <i>time</i> <ul style="list-style-type: none"> • 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

12.2.4 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]	<ul style="list-style-type: none"> ◦ <i>interface</i> LAN インタフェース名 ◦ <i>retry</i> <ul style="list-style-type: none"> • 回数 (1..100) • infinity 無制限 ◦ <i>interval</i> 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]	<i>retry</i> = infinity <i>interfal</i> = 5					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

12.2.5 DHCP クライアント ID オプションの設定

[入力形式]	dhcp client client-identifier interface primary [type type] id dhcp client client-identifier interface secondary [type type] id dhcp client client-identifier pp peer_num [type type] id dhcp client client-identifier pool pool_num [type type] id no dhcp client client-identifier interface primary no dhcp client client-identifier interface secondary no dhcp client client-identifier pp peer_num no dhcp client client-identifier pool pool_num					
[パラメータ]	<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 type 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 type 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 桁の十六進数列で表した ID ◦ <i>peer_num</i> <ul style="list-style-type: none"> • 相手先情報番号 • anonymous. ◦ <i>pool_num</i> ip pp remote address pool dhcp コマンドで取得する IP アドレスの番号。例えば、ip pp remote address pool dhcp コマンドで IP アドレスを 2 個取得できる機種で、<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 dhcp コマンドで取得できる IP アドレスの最大数) 					
[説明]	DHCP クライアント ID オプションの type フィールドと ID を設定する。					
[デフォルト値]	<i>type</i> = 1					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

13. ICMP の設定

13.1 IPv4 の設定

13.1.1 ICMP Echo Reply を送信するか否かの設定

[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	RT105i	RT105e
---------	---------	--------	--------	--------

13.1.2 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	RT105i	RT105e
---------	---------	--------	--------	--------

13.1.3 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	RT105i	RT105e
---------	---------	--------	--------	--------

13.1.4 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	RT105i	RT105e
---------	---------	--------	--------	--------

13.1.5 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]	<ul style="list-style-type: none"> ◦ action <ul style="list-style-type: none"> • 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]	<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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

13.1.6 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]	<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]	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]	<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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

13.1.7 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]	<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]	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]	<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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

13.1.8 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="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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

13.1.9 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 <i>log</i> no ip icmp log [<i>log</i>]					
[パラメータ]	◦ <i>log</i> <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="display: inline-table; border-collapse: collapse;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

13.1.10 ステルス機能の設定

[入力形式]	ip stealth all ip stealth <i>interface</i> [<i>interface...</i>] no ip 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 ◦ <i>interface</i>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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

13.2 IPv6 の設定

13.2.1 ICMP Echo Reply を送信するか否かの設定

[入力形式]	ipv6 icmp echo-reply send <i>send</i> no ipv6 icmp echo-reply send [<i>send</i>]					
[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]	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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

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

[入力形式]	ipv6 icmp parameter-problem send <i>send</i> no ipv6 icmp parameter-problem send [<i>send</i>]					
[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]	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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="padding: 2px;">RTX2000</td> <td style="padding: 2px;">RTX1000</td> <td style="padding: 2px;">RT300i</td> <td style="padding: 2px;">RT105i</td> <td style="padding: 2px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

13.2.3 ICMP Redirect を送信するか否かの設定

[入力形式]	ipv6 icmp redirect send <i>send</i> no ipv6 icmp redirect send [<i>send</i>]					
[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]	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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

13.2.4 ICMP Redirect 受信時の処理の設定

[入力形式]	ipv6 icmp redirect receive <i>action</i> no ipv6 icmp redirect receive [<i>action</i>]					
[パラメータ]	○ <i>action</i> <ul style="list-style-type: none"> • 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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

13.2.5 ICMP Time Exceeded を送信するか否かの設定

[入力形式]	ipv6 icmp time-exceeded send <i>send</i> no ipv6 icmp time-exceeded send [<i>send</i>]					
[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]	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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

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

[入力形式]	ipv6 icmp unreachable send <i>send</i> no ipv6 icmp unreachable send [<i>send</i>]					
[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]	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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

13.2.7 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 <i>log</i> no ipv6 icmp log [<i>log</i>]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>log</i> • 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="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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

13.2.8 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 <i>send</i> no ipv6 icmp packet-too-big send [<i>send</i>]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>send</i> • 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]	<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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

13.2.9 ステルス機能の設定

[入力形式]	ipv6 stealth all ipv6 stealth <i>interface</i> [<i>interface...</i>] no ipv6 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 ◦ <i>interface</i>.....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。</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="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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

14. トンネリング

14.1 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 <i>tunnel_num</i> no tunnel enable					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>tunnel_num</i> <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]	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 <code>disable</code> 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。					
[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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

14.2 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 <i>tunnel_num</i>					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>tunnel_num</i> <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]	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、 <code>disable</code> 状態で行うのが望ましい。					
[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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

14.3 トンネルインタフェースの種別の設定

[入力形式]	tunnel encapsulation <i>type</i> no tunnel encapsulation					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>type</i> <ul style="list-style-type: none"> • ipsec IPsec トンネル • ipip IPv6 over IPv4 トンネルまたは IPv4 over IPv6 トンネル • pptp PPTP トンネル 					
[説明]	トンネルインタフェースの種別を設定する。					
[ノート]	トンネリングと NAT を併用する場合には tunnel endpoint address コマンドにより始点 IP アドレスを設定することが望ましい。					
[デフォルト値]	ipsec					
[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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

14.4 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 [<i>local</i>] <i>remote</i> no tunnel endpoint address [[<i>local</i>] <i>remote</i>]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>local</i> 自分側のトンネルインタフェース端点の IP アドレス ◦ <i>remote</i>..... 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]	<p>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 IPv6 トンネルが利用できる。</p> <p><i>local</i> 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。</p>					
[ノート]	<p>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。</p> <p>PPTP サーバの Anonymous で受ける場合には設定する必要はない。</p>					
[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]	<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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15. 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 に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 ~
7.00	—	—	7.00.01 ~
7.01	—	—	7.01.01 ~

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
RT105i	1 - 20	1 - 20
RT105e	1 - 30	1 - 30

本機はメインモード (main mode) とアグレッシブモード (aggressive mode) に対応しています。VPN を構成する両方のルータが固定のグローバルアドレスを持つときにはメインモードを使用し、一方のルータしか固定のグローバルアドレスを持たないときにはアグレッシブモードを使用します。

メインモードを使用するためには、**ipsec ike remote address** コマンドで対向のルータの IP アドレスを設定する必要があります。アグレッシブモードを使用するときには、固定のグローバルアドレスを持つかどうかによって設定が異なります。固定のグローバルアドレスを持つルータには、**ipsec ike remote name** コマンドを設定し、**ipsec ike remote address** コマンドで any を設定します。固定のグローバルアドレスを持たないルータでは、**ipsec ike local name** コマンドを設定し、**ipsec ike remote address** コマンドで IP アドレスを設定します。

122 15.IPsec の設定

メインモードでは、**ipsec ike local name** コマンドや **ipsec ike remote name** コマンドを設定することはできません。また、アップグレードモードでは、**ipsec ike local name** コマンドと **ipsec ike remote name** コマンドの両方を同時に設定することはできません。このように設定した場合には、正しく動作しない可能性があります。

15.1 IPsec の動作の設定

[入力形式]	ipsec use use no ipsec use [use]					
[パラメータ]	<ul style="list-style-type: none"> ◦ use <ul style="list-style-type: none"> • on.....動作させる • off.....動作させない 					
[説明]	IPsec を動作させ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="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15.2 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]	<ul style="list-style-type: none"> ◦ gateway_idセキュリティ・ゲートウェイの識別子 ◦ key鍵となる 0x で始まる十六進数列 (32 バイト以内) ◦ text ASCII 文字列で表した鍵 (32 文字以内) 					
[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 0xCDEEEDC0CEDCD					
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15.3 設定が異なる場合に鍵交換を拒否するか否かの設定

[書式]	ipsec ike negotiate-strictly gateway_id switch no ipsec ike negotiate-strictly gateway_id												
[設定値]	<ul style="list-style-type: none"> ◦ gateway_idセキュリティ・ゲートウェイの識別子 ◦ switch <ul style="list-style-type: none"> • on.....鍵交換を拒否する • off.....鍵交換を受理する 												
[説明]	設定が異なる場合に鍵交換を拒否するか否かを設定する。 このコマンドの設定が off のときには、従来のファームウェアと同様に動作する。すなわち、相手の提案するパラメータが自分の設定と異なる場合でも、そのパラメータをサポートしていれば、それを受理する。このコマンドの設定が on のときには、同様の状況で相手の提案を拒否する。このコマンドが適用されるパラメータと対応するコマンドは以下の通りである。												
	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">パラメータ</th> <th style="text-align: left;">対応するコマンド</th> </tr> </thead> <tbody> <tr> <td>暗号アルゴリズム</td> <td>ipsec ike encryption</td> </tr> <tr> <td>グループ</td> <td>ipsec ike group</td> </tr> <tr> <td>ハッシュアルゴリズム</td> <td>ipsec ike hash</td> </tr> <tr> <td>PFS</td> <td>ipsec ike pfs</td> </tr> <tr> <td>フェーズ 1 のモード</td> <td>ipsec ike local name など</td> </tr> </tbody> </table>	パラメータ	対応するコマンド	暗号アルゴリズム	ipsec ike encryption	グループ	ipsec ike group	ハッシュアルゴリズム	ipsec ike hash	PFS	ipsec ike pfs	フェーズ 1 のモード	ipsec ike local name など
パラメータ	対応するコマンド												
暗号アルゴリズム	ipsec ike encryption												
グループ	ipsec ike group												
ハッシュアルゴリズム	ipsec ike hash												
PFS	ipsec ike pfs												
フェーズ 1 のモード	ipsec ike local name など												
[初期値]	off												
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e							
RTX2000	RTX1000	RT300i	RT105i	RT105e									

15.4 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 switch no ipsec ike always-on					
[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 ○ switch <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 キーブ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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15.5 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]	<ul style="list-style-type: none"> ○ 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15.6 IKE の鍵交換を始動するか否かの設定

[入力形式]	ipsec auto refresh [gateway_id] switch no ipsec auto refresh [gateway_id]					
[設定値]	<ul style="list-style-type: none"> ○ gateway_id セキュリティ・ゲートウェイの識別番号 ○ switch <ul style="list-style-type: none"> • on 鍵交換を始動する • off 鍵交換を始動しない 					
[説明]	IKE の鍵交換を始動するかどうかを設定する。このコマンドの設定が on の場合には、IPsec の通信に必要な鍵を作るために、必要に応じて鍵交換を始動する。このコマンドの設定が off の場合には、鍵交換を始動することはない。なお、このコマンドの設定に関係なく、他のルータが始動した鍵交換については、常に受け付ける。					
[ノート]	Rev.7.01.15 から仕様変更された。					
[デフォルト値]	ipsec auto refresh off ipsec auto refresh gateway_id on					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15.7 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]	<ul style="list-style-type: none"> ○ gateway セキュリティ・ゲートウェイの識別子 ○ name 名前 (32 文字以内) 					
[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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15.8 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]	<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 <ul style="list-style-type: none"> • 相手側セキュリティ・ゲートウェイの IP アドレス、またはホスト名 • any 自動選択 					
[説明]	<p>相手側セキュリティ・ゲートウェイの IP アドレスまたはホスト名を設定する。ホスト名で設定した場合には、鍵交換の始動時にホスト名から IP アドレスを DNS により検索する。そのため、dns server コマンドなどで必ず DNS サーバが設定されていないといけない。</p> <p>any が設定された場合には、相手側セキュリティ・ゲートウェイとして任意のホストからのアクセスを受け付ける。その代わりに、自分から鍵交換を始動することはできない。any はアグレッシブモードで固定のグローバルアドレスを持つ側の場合に利用する。</p>					
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15.9 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。 <i>mask</i> 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、 <i>mask</i> 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="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15.10 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]	<ul style="list-style-type: none"> ○ gateway_id セキュリティ・ゲートウェイの識別子 ○ name 名前 (32 文字以内) ○ type ID の種類 <ul style="list-style-type: none"> • fqdn ID_FQDN • use-fqdn ID_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]	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15.11 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]	<ul style="list-style-type: none"> ◦ <i>gateway_id</i> セキュリティ・ゲートウェイの識別子 ◦ <i>ip_address</i> 自分側セキュリティ・ゲートウェイの IP アドレス ◦ <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]	自分側セキュリティ・ゲートウェイの IP アドレスを設定する。 vrrp キーワードを指定する第 2 書式では、VRRP マスターとして動作している場合のみ、指定した LAN インタフェース / VRRP グループ ID の仮想 IP アドレスを自分側セキュリティ・ゲートウェイアドレスとして利用する。 VRRP マスターでない場合には鍵交換は行わない。					
[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]	<table border="1" style="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15.12 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]	<ul style="list-style-type: none"> ◦ <i>gateway_id</i> セキュリティ・ゲートウェイの識別子 ◦ <i>ip_address</i> IP アドレス ◦ <i>mask</i> 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。 <i>mask</i> 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、 <i>mask</i> 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="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15.13 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]][interval][count] no ipsec ike keepalive use [gateway_id switch [type [ip_address]][interval][count]]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>gateway_id</i> セキュリティ・ゲートウェイの識別子 ◦ <i>switch</i> <ul style="list-style-type: none"> • 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 ◦ <i>type</i> キープアライブの方法 <ul style="list-style-type: none"> • heartbeat IKE heartbeat (従来の方法) • icmp-echo ping ◦ <i>ip_address</i> ping を送信する宛先の IP アドレス (IPv4/IPv6) (このパラメータは <i>type</i> として icmp-echo を指定したときのみ設定できる) ◦ <i>interval</i> キープアライブパケットの送信間隔 ◦ <i>count</i> 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]	<i>switch</i> = auto <i>type</i> = heartbeat <i>interval</i> = 10 <i>count</i> = 6					
[適用モデル]	<table border="1" style="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15.14 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15.15 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]	○ gateway_id セキュリティ・ゲートウェイの識別子 ○ algorithm • 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="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15.16 受信した IKE パケットを蓄積するキューの長さの設定

[書式]	ipsec ike queue length length no ipsec ike queue length [length]					
[設定値]	○ length キュー長 (8..64)					
[説明]	受信した IKE パケットを蓄積するキューの長さを設定する。 この設定は、短時間に集中して IKE パケットを受信した際のルータの振る舞いを決定する。設定した値が大きいほど、IKE パケットが集中したときにより多くのパケットを取りこぼさないで処理することができるが、逆に IKE パケットがルータに滞留する時間が長くなるためキープアライブの応答が遅れ、トンネルの障害を間違えて検出する可能性が増える。 通常の運用では、この設定を変更する必要はないが、多数のトンネルを構成しており、多数の SA を同時に消す状況があるならば値を大きめに設定するとよい。					
[ノート]	Rev.7.01.15 以前のファームウェアでは、このキューの長さは 8 で固定されていた。 キューの長さを長くすると、一度に受信して処理できる IKE パケットの数を増やすことができる。しかし、あまり大きくすると、ルータ内部にたまった IKE パケットの処理が遅れ、対向のルータでタイムアウトと検知されてしまう可能性が増える。そのため、このコマンドの設定を変更する時には、慎重に行なう必要がある。 通常の運用では、この設定を変更する必要はない。					
[初期値]	8					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15.17 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="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15.18 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 <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="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15.19 受信したパケットの SPI 値が無効な値の場合にログに出力するか否かの設定

[入力形式]	ipsec log illegal-spi switch no ipsec log illegal-spi					
[パラメータ]	<ul style="list-style-type: none"> ◦ switch <ul style="list-style-type: none"> • on ログに出力する • off ログに出力しない 					
[説明]	IPsec で、受信したパケットの SPI 値が無効な値の場合に、その旨をログに出力するか否かを設定する。SPI 値と相手の IP アドレスがログに出力される。 無効な SPI 値を含むパケットを大量に送り付けられることによる DoS の可能性を減らすため、ログは 1 秒あたり最大 10 種類のパケットだけを記録する。実際に受信したパケットの数を知ることはできない。					
[ノート]	鍵交換時には、鍵の生成速度の差により一方が新しい鍵を使い始めても他方ではまだその鍵が使用できない状態になっているためにこのログが一時的に出力されてしまうことがある。					
[デフォルト値]	off					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15.20 IKE ペイロードのタイプの設定

[入力形式]	ipsec ike payload type <i>gateway_id type</i> no ipsec ike payload type <i>gateway_id [type]</i>					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>gateway_id</i> セキュリティ・ゲートウェイの識別子 ○ <i>type</i> メッセージのフォーマット <ul style="list-style-type: none"> ● 1 ヤマハルータのリリース 2 との互換性を保持する ● 2 ヤマハルータのリリース 3 に合わせる ● 3 初期ベクトル (IV) の生成方法を一部の実装に合わせる 					
[説明]	IKE ペイロードのタイプを設定する。YAMAHA 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" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15.21 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 <i>gateway_id info</i> no ipsec ike send info <i>gateway_id [info]</i>					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>gateway_id</i> セキュリティ・ゲートウェイの識別子 ○ <i>info</i> <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="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15.22 PFS を用いるか否かの設定

[入力形式]	ipsec ike pfs <i>gateway_id pfs</i> no ipsec ike pfs <i>gateway_id [pfs]</i>					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>gateway_id</i> セキュリティ・ゲートウェイの識別子 ○ <i>pfs</i> <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="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15.23 XAUTH の設定

[入力形式]	ipsec ike xauth myname <i>gateway_id name password</i> no ipsec ike xauth myname					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>gateway_id</i> セキュリティ・ゲートウェイの識別子 ○ <i>name</i> XAUTH で通知する名前 (32 文字以内) ○ <i>password</i> XAUTH で通知するパスワード (32 文字以内) 					
[説明]	XAUTH の認証を要求されたときに通知する名前とパスワードを設定する。					
[デフォルト値]	なし					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15.24 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]	<ul style="list-style-type: none"> ◦ gateway_id..... セキュリティ・ゲートウェイの識別子 ◦ type <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 <i>type</i> パラメータを設定することもできる。					
[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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15.25 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 no ipsec ike esp-encapsulation gateway_id					
[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 ◦ encap <ul style="list-style-type: none"> • 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]	<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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15.26 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。

15.26.1 SA のポリシーの定義

[入力形式]	ipsec sa policy policy_id gateway_id ah ab_algorithm ipsec sa policy policy_id gateway_id esp esp_algorithm [ab_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..21474836) ◦ 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 ◦ ab_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]	<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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15.26.2 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]	<p>IKE で提案する IPsec SA または ISAKMP SA の寿命を設定する。</p> <p><i>kbytes</i> パラメータを指定した場合には、<i>second</i> 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。なお、<i>kbytes</i> パラメータは <i>sa</i> が ipsec-sa の場合のみ有効。</p>					
[デフォルト値]	28800 秒					
[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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

15.26.3 ダングリング SA の動作の設定

[書式]	ipsec ike restrict-dangling-sa gateway_id action no ipsec ike restrict-dangling-sa gateway_id [action]															
[設定値]	<ul style="list-style-type: none"> ○ gateway_id セキュリティ・ゲートウェイの識別子 ○ action <ul style="list-style-type: none"> • auto アグレッシブモードの始動側でのみ IKE SA と IPsec SA を同期させる • off IKE SA と IPsec SA を同期させない。 															
[説明]	<p>このコマンドはダングリング SA の動作に制限を設ける。</p> <p>ダングリング SA とは、IKE SA を削除するときに対応する IPsec SA を削除せずに残したときの状態を指す。RT シリーズでは基本的にはダングリング SA を許す方針で実装しており、IKE SA と IPsec SA を独立のタイミングで削除する。</p> <p><i>auto</i> を設定したときには、アグレッシブモードの始動側でダングリング SA を排除し、IKE SA と IPsec SA を同期して削除する。この動作は IKE keepalive が正常に動作するために必要な処置である。</p> <p><i>off</i> を設定したときには、常にダングリング SA を許す動作となり、IKE SA と IPsec SA を独立なタイミングで削除する。</p> <p>ダイヤルアップ VPN のクライアント側ではない場合には、このコマンドの設定に関わらず常に IKE SA と IPsec SA は独立に管理され、削除のタイミングは必ずしも同期しない。</p>															
[ノート]	<p>ダングリング SA の強制削除が行なわれても、通常は新しい IKE SA に基づいた新しい IPsec SA が存在するので通信に支障が出ることはない。</p> <p>ダイヤルアップ VPN のクライアント側でダングリング SA を許さないのは、IKE キープアライブを正しく機能させるために必要なことである。</p> <p>IKE キープアライブでは、IKE SA に基づいてキープアライブを行なう。ダングリング SA が発生した場合には、その SA についてはキープアライブを行なう IKE SA が存在せず、キープアライブ動作が行なえない。そのため、IKE キープアライブを有効に動作させるにはダングリング SA が発生したら強制的に削除して、通信は対応する IKE SA が存在する IPsec SA で行なわれるようにしなくてはならない。</p> <p>ダングリング SA の扱いについては、動作モードとリビジョンによって動作が異なる。</p>															
	<table border="1" style="border-collapse: collapse; text-align: center; width: 100%;"> <thead> <tr> <th style="padding: 5px;">リビジョン</th> <th style="padding: 5px;">7.01.05 以前</th> <th style="padding: 5px;">7.01.08</th> <th style="padding: 5px;">7.01.15</th> <th style="padding: 5px;">7.01.16 以降</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;">ダイヤルアップ VPN のクライアント側</td> <td style="padding: 5px;">(A)</td> <td colspan="2" style="padding: 5px;">(B)</td> <td style="padding: 5px;">(C)</td> </tr> <tr> <td style="padding: 5px;">それ以外</td> <td style="padding: 5px;">(A)</td> <td style="padding: 5px;">(B)</td> <td colspan="2" style="padding: 5px;">(A)</td> </tr> </tbody> </table>	リビジョン	7.01.05 以前	7.01.08	7.01.15	7.01.16 以降	ダイヤルアップ VPN のクライアント側	(A)	(B)		(C)	それ以外	(A)	(B)	(A)	
リビジョン	7.01.05 以前	7.01.08	7.01.15	7.01.16 以降												
ダイヤルアップ VPN のクライアント側	(A)	(B)		(C)												
それ以外	(A)	(B)	(A)													
	<p>(A) ダングリング SA が発生しても何もせず通信を続ける</p> <p>(B) ダングリング SA が発生した時にはそれを消去し、必要であれば新しい SA を作成して通信を行なう</p> <p>(C) このコマンドにより動作を変更できる</p>															
[初期値]	auto															
[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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e										
RTX2000	RTX1000	RT300i	RT105i	RT105e												

15.26.4 SA の削除

【入力形式】	ipsec sa delete id				
【パラメータ】	<ul style="list-style-type: none"> ◦ id <ul style="list-style-type: none"> • 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	RT105i	RT105e

15.26.5 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	RT105i	RT105e

15.27 トンネルインタフェース関連の設定

15.27.1 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】	◦ <i>policy_id</i> 整数 (1..2147483647)				
【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	RT105i	RT105e

15.27.2 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"> ◦ <i>type</i> <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】	IPComp でデータ圧縮を行うかどうかを設定する。サポートしているアルゴリズムは deflate のみである。 受信した IPComp パケットを展開するためには、特別な設定を必要としない。すなわち、サポートしているアルゴリズムで圧縮された IPComp パケットを受信した場合には、設定に関係なく展開する。 必ずしもセキュリティ・ゲートウェイの両方にこのコマンドを設定する必要はない。片側にのみ設定した場合には、そのセキュリティ・ゲートウェイから送信される IP パケットのみが圧縮される。 トランスポートモードのみを使用する場合には、IPComp を使用することはできない。				
【ノート】	データ圧縮には、PPP で使われる CCP 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ることになり、ほとんど効果がない。一方、IPComp は IPsec による暗号化の前にデータ圧縮が行われるため、一定の効果を得られる。また、CCP/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。				
【デフォルト値】	none				
【適用モデル】	RTX2000	RTX1000	RT300i	RT105i	RT105e

15.27.3 トンネルバックアップの設定

[入力形式] **tunnel backup** none
tunnel backup interface ip_address
tunnel backup pp peer_num [switch-router=switch1]
tunnel backup tunnel tunnel_num [switch-interface=switch2]
no tunnel backup

[パラメータ] ○ interfaceLAN インタフェース名
○ ip_addressバックアップ先のゲートウェイの IP アドレス
○ peer_numバックアップ先の相手先情報番号
○ tunnel_num トンネルインタフェース番号
○ switch1バックアップの受け側のルータを 2 台に分けるか否か
 • on 分ける
 • off 分けない
○ switch2LAN/PP インタフェースのバックアップにしたがってトンネルを作り直すか否か
 • on 作り直す
 • off 作り直さない

[説明] トンネルインタフェースに障害が発生したときにバックアップとして利用するインタフェースを指定する。

switch-route オプションについては、以下の 2 つの条件を満たすときに on を設定する。

- バックアップの受け側に 2 台のルータがあり、一方がバックアップ元の回線に接続し、もう一方がバックアップ先の回線に接続している。
- バックアップ先の回線に接続しているルータのファームウェアがこのリビジョンよりも古い。

[デフォルト値] none
switch1 = off
switch2 = on

[適用モデル]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

15.28 トランスポートモード関連の設定

15.28.1 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..21474836)
○ proto プロトコル
○ src_port_listUDP、TCP のソースポート番号列
 • ポート番号を表す十進数
 • ポート番号を表すニーモニック
 • * (すべてのポート)
○ dst_port_listUDP、TCP のデスティネーションポート番号列
 • ポート番号を表す十進数
 • ポート番号を表すニーモニック
 • * (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	RT105i	RT105e
---------	---------	--------	--------	--------

16. 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。

16.1 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。

16.1.1 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 を閉じる。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="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

16.1.2 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> pp bind <i>tunnel_num-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。 第 2 書式は anonymous インタフェースを使って多数の接続先を登録するために複数連続したトンネルインタフェースをバインドする場合に用いる。					
[ノート]	PPTP は PP 毎に設定する。 tunnel encapsulation コマンドで pptp 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="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

16.1.3 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="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

16.1.4 PPTP ホスト名の設定

[入力形式]	pptp hostname <i>name</i> no ptp hostname [<i>name</i>]					
[パラメータ]	◦ <i>name</i>ホスト名 (64 バイト以下)					
[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 pp 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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

16.1.5 PPTP パケットのウィンドウサイズの設定

[入力形式]	pptp window size <i>size</i> no ptp window size [<i>size</i>]					
[パラメータ]	◦ <i>size</i>パケットサイズ (1..128)					
[説明]	受信済みで無応答の PPTP パケットをバッファに入れることができるパケットの最大数を設定する。					
[デフォルト値]	32					
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

16.1.6 PPTP の動作モードの設定

[入力形式]	pptp call-id mode <i>mode</i> no ptp call-id mode [<i>mode</i>]					
[パラメータ]	◦ <i>mode</i> <ul style="list-style-type: none"> • 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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

16.1.7 PPTP 暗号鍵生成のための要求する認証方式の設定

[入力形式]	pp auth request <i>auth</i> [arrive-only] no pp auth request [<i>auth</i>]					
[パラメータ]	◦ <i>auth</i> <ul style="list-style-type: none"> • 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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

16.1.8 PPTP 暗号鍵生成のための受け入れ可能な認証方式の設定

[入力形式]	pp auth accept <i>auth</i> [<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> <ul style="list-style-type: none"> • 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="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

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

[入力形式]	pptp syslog <i>syslog</i> no pptp syslog [<i>syslog</i>]					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>syslog</i> <ul style="list-style-type: none"> • on 出力する • off 出力しない 					
[説明]	PPTP のコネクション制御の syslog を出力するか否かを設定する。 キーブアライブ用の Echo-Request, Echo-Reply については出力されない。					
[デフォルト値]	off					
[適用モデル]	<table border="1" style="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

16.2 リモートアクセス VPN 機能

16.2.1 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]	<ul style="list-style-type: none"> ○ <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 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="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

16.2.2 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="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

16.2.3 PPTP キープアライブの設定

[入力形式]	pptp keepalive use <i>use</i> no pptp keepalive use [<i>use</i>]					
[パラメータ]	◦ <i>use</i> <ul style="list-style-type: none"> • 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="background-color: #cccccc;">RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

16.2.4 PPTP キープアライブのログ設定

[入力形式]	pptp keepalive log <i>log</i> no pptp keepalive log [<i>log</i>]					
[パラメータ]	◦ <i>log</i> <ul style="list-style-type: none"> • 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="background-color: #cccccc;">RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

16.2.5 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 <i>interval</i> [<i>count</i>] no pptp keepalive interval [<i>interval count</i>]					
[パラメータ]	◦ <i>interval</i>インターバル (1..65535) ◦ <i>count</i>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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="background-color: #cccccc;">RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

16.2.6 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 <i>mode</i> no ppp ccp no-encryption [<i>mode</i>]					
[パラメータ]	◦ <i>mode</i> <ul style="list-style-type: none"> • 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="background-color: #cccccc;">RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

17. SNMPの設定

SNMP(Simple Network Management Protocol; RFC1157)の設定を行うことにより、SNMP管理ソフトウェアに対してネットワーク管理情報のモニタと変更を行うことができますようになります。この時YAMAHAルータはSNMPエージェントとなります。

YAMAHAルータはMIB (Management information Base)としてRFC1213(MIB-II)とプライベートMIBに対応しています。プライベートMIBについては<http://www.rtrpro.yamaha.co.jp/>にある情報を参照してください。

SNMPにより情報を交換するグループをコミュニティと呼びます。コミュニティ間のアクセスには、読み出し専用(read-only)と読み書き可能(read-write)の2つのアクセスモードがあります。

YAMAHAルータの状態を通知するSNMPメッセージをトラップと呼びます。どのようなトラップを送信するかは**snmp trap enable snmp**コマンドで設定し、受信するホストは**snmp trap host**コマンドで設定します。

読み出し専用のコミュニティ名と送信トラップのコミュニティ名の初期値は“public”になっています。SNMP管理ソフトウェア側のコミュニティ名も“public”の場合が多いので、セキュリティを重要視する場合は適切なコミュニティ名に設定変更します。コミュニティ名にログインパスワードや管理パスワードを使用しないように注意してください。

工場出荷状態ではSNMPによるアクセス許可に関する**snmp host**コマンドの設定がnoneであるので、YAMAHAルータへのSNMPによるアクセスは一切できない状態にあります。また、トラップの受信ホストを設定する**snmp trap host**コマンドの設定がclearであるので、どこにもトラップを送信しません。

17.1 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 <i>host</i> [<i>ro_community</i> [<i>rw_community</i>]] snmp host any no snmp host <i>host</i> no snmp host any					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>host</i> <ul style="list-style-type: none"> • SNMPによるアクセスを許可するホストのIPアドレス • any.....すべてのホストからSNMPによりアクセスできる ○ <i>ro_community</i>..... Read-Only コミュニティ文字列 ○ <i>rw_community</i> Read-Write コミュニティ文字列 					
[説明]	SNMPによるアクセスを許可するホストを設定する。 anyを設定した場合は任意のホストからのSNMPによるアクセスを許可する。 IPアドレスでホストを指定した場合には、同時にコミュニティ文字列も設定できる。Read-Write コミュニティ文字列を省略した場合には、Read-Write アクセスが禁止される。Read-Only コミュニティ文字列も省略した場合には、コミュニティ文字列には snmp community コマンドの設定が用いられる。					
[ノート]	Rev.7.01.12からコマンドの入力形式が拡張された。					
[デフォルト値]	すべてのホストからのSNMPによるアクセスを禁止					
[適用モデル]	<table border="1" style="width: 100%; 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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

17.2 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="width: 100%; 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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

17.3 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 (1 文字以上 16 文字以内)					
[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。					
[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>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

17.4 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 (1 文字以上 16 文字以内)					
[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。					
[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>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

17.5 sysContact の設定

[入力形式]	snmp syscontact name no snmp syscontact [name]					
[パラメータ]	○ <i>name</i>sysContact として登録する名称 (255 文字以内の文字列)					
[説明]	MIB 変数 sysContact を設定する。空白を含ませるためには、パラメータ全体をダブルクォート (")、もしくはシングルクォート (') で囲む。 sysContact は一般的に、管理者の名前や連絡先を記入しておく変数である。					
[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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

17.6 sysLocation の設定

[入力形式]	snmp syslocation name no snmp syslocation [name]					
[パラメータ]	○ <i>name</i>sysLocation として登録する名称 (255 文字以内の文字列)					
[説明]	MIB 変数 sysLocation を設定する。空白を含ませるためには、パラメータ全体をダブルクォート (")、もしくはシングルクォート (') で囲む。 sysLocation は一般的に、機器の設置場所を記入しておく変数である。					
[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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

17.7 sysName の設定

[入力形式]	snmp sysname name no snmp sysname [name]					
[パラメータ]	○ <i>name</i> sysName として登録する名称 (255 文字以内の文字列)					
[説明]	MIB 変数 sysName を設定する。空白を含ませるためには、パラメータ全体をダブルクォート (")、もしくはシングルクォート (') で囲む。 sysName は一般的に、機器の名称を記入しておく変数である。					
[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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

17.8 SNMP トラップを送信するか否かの設定

[書式]	snmp trap enable snmp trap [trap...] snmp trap enable snmp all no snmp trap enable snmp					
[設定値]	○ <i>trap</i> トラップの種類 <ul style="list-style-type: none"> • coldstart 全設定初期化時 • warmstart 再起動時 • linkup リンクアップ時 • linkdown リンクダウン時 • authenticationfailure 認証失敗時 ○ <i>all</i> すべてのトラップを送信することを示すキーワード					
[説明]	SNMP トラップを送信するか否かを設定する。 'all' を設定した場合には、すべてのトラップを送信する。個別にトラップを設定した場合には、設定されたトラップだけが送信される。					
[ノート]	このコマンドは従来リビジョンの snmp enableauthentraps コマンドを置き換える。 authenticationFailure トラップを送信するか否かはこのコマンドによって制御される。 linkDown トラップについては、 snmp trap send linkdown コマンドによってインタフェース毎に制御できる。 あるインタフェースについて、linkDown トラップが送信されるか否かは、 snmp trap send linkdown コマンドで送信が許可されており、かつ、このコマンドでも許可されている場合に限られる。					
[初期値]	all					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

17.9 SNMP の LinkDown トラップの送信制御の設定

[入力形式]	snmp trap send linkdown interface [interface_num] switch snmp trap send linkdown pp [peer_num] switch snmp trap send linkdown tunnel [tunnel_num] switch no snmp trap send linkdown interface no snmp trap send linkdown pp [peer_num] no snmp trap send linkdown tunnel [tunnel_num]					
[パラメータ]	○ <i>interface</i> <ul style="list-style-type: none"> • LAN インタフェース名 • BRI インタフェース名 ○ <i>peer_num</i> 相手先情報番号 ○ <i>tunnel_num</i> トンネルインタフェース番号 ○ <i>switch</i> <ul style="list-style-type: none"> • on 送信する • off 送信しない 					
[説明]	指定したインタフェースの LinkDown トラップを送信するか否かを設定する。					
[デフォルト値]	on					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

17.10 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]	◦ <i>name</i>送信トラップのコミュニティ名 (1 文字以上 16 文字以内)					
[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。					
[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>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

17.11 SNMP トラップの送信先の設定

[入力形式]	snmp trap host host [community] no snmp trap host host [community]					
[パラメータ]	◦ <i>host</i>SNMP トラップを送信する先のホストの IP アドレス ◦ <i>community</i>コミュニティ名					
[説明]	SNMP トラップを送信するホストを指定する。コマンドを複数設定することで、複数のホストを同時に指定できる。トラップ送信時のコミュニティ文字列にはこのコマンドの設定値が用いられるが、省略されている場合には snmp trap community コマンドの設定値が用いられる。					
[ノート]	Rev.7.00.26 以降で <i>community</i> パラメータが指定可能。					
[デフォルト値]	SNMP トラップを送信しない					
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

17.12 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]	◦ <i>switch</i> <ul style="list-style-type: none"> • 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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

17.13 トンネルインタフェースの情報を MIB2 の範囲で表示するか否かの設定

[入力形式]	snmp yriftunneldisplayatmib2 switch no snmp yriftunneldisplayatmib2					
[パラメータ]	◦ <i>switch</i> <ul style="list-style-type: none"> • on.....MIB 変数 yrifTunnelDisplayAtMib2 を "enabled(1)" とする • off.....MIB 変数 yrifTunnelDisplayAtMib2 を "disabled(2)" とする 					
[説明]	MIB 変数 yrifTunnelDisplayAtMib2 の値をセットする。この MIB 変数はトンネルインタフェースを MIB2 の範囲で表示するかどうかを決定する。Rev.4 以前と同じ表示にする場合には、MIB 変数を "enabled(1)" に、つまり、このコマンドで on を設定する。					
[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>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

17.14 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>switch</i> no snmp display ipcp force					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>switch</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="width: 100%; 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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

18. RADIUS の設定

ISDN 接続のための認証とアカウントを RADIUS サーバを利用して管理できます。PPTP 接続のための認証とアカウントの管理はサポートされません。

18.1 RADIUS による認証を使用するか否かの設定

[入力形式]	radius auth <i>auth</i> no radius auth [<i>auth</i>]					
[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="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

18.2 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 <i>account</i> no radius account [<i>account</i>]					
[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="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

18.3 RADIUS サーバの指定

[入力形式]	radius server <i>ip1</i> [<i>ip2</i>] no radius server [<i>ip1</i> [<i>ip2</i>]]					
[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]	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。					
[ノート]	RADIUS には認証とアカウントの 2 つの機能があり、それぞれのサーバは radius auth server / radius account server コマンドで個別に設定できる。 radius server コマンドでの設定は、これら個別の設定が行われていない場合に有効となり、認証、アカウントいずれでも用いられる。					
[適用モデル]	<table border="1" style="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

18.4 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="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

18.5 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="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

18.6 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="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

18.7 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="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

18.8 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	RT105i	RT105e
---------	---------	--------	--------	--------

18.9 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	RT105i	RT105e
---------	---------	--------	--------	--------

19. 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。

19.1 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"> ◦ <i>interface</i> LAN インタフェース名 ◦ <i>nat_descriptor_list</i> 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%; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

19.2 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"> ◦ <i>nat_descriptor</i> NAT ディスクリプタ番号 (1..21474836) ◦ <i>type</i> <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】	<i>nat-masquerade</i> は、動的 NAT 変換できなかったパケットを IP マスカレード変換で救う。例えば、外側アドレスが 16 個利用可能の場合は先勝ちで 15 個 NAT 変換され、残りは IP マスカレード変換される。					
【デフォルト値】	none					
【適用モデル】	<table border="1" style="width: 100%; text-align: center;"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

19.3 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	RT105i	RT105e
---------	---------	---------	--------	--------	--------

19.4 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	RT105i	RT105e
---------	---------	---------	--------	--------	--------

19.5 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	RT105i	RT105e
---------	---------	---------	--------	--------	--------

19.6 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"> • on..... 使用する • off..... 使用しない 					
[説明]	IP マスカレード使用時に rlogin、rcp、ssh の使用を許可するか否かを設定する。					
[ノート]	on にすると、rlogin、rcp と ssh のトラフィックに対してはポート番号を変換しなくなる。また on の場合に rsh は使用できない。					
[デフォルト値]	off					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

19.7 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 [outer_port=]inner_port</i> no nat descriptor masquerade static <i>nat_descriptor id [inner_ip protocol [outer_port=]inner_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> <ul style="list-style-type: none"> • tcp..... TCP プロトコル • udp..... UDP プロトコル • icmp..... icmp プロトコル • プロトコル番号..... IANA で割り当てられている protocol numbers ○ <i>outer_port</i>..... 固定する外側ポート番号 (ニーモニック) ○ <i>inner_port</i>..... 固定する内側ポート番号 (ニーモニック) 					
[説明]	IP マスカレードによる通信でポート番号変換を行わないようにポートを固定する。					
[ノート]	<i>outer_port</i> と <i>inner_port</i> を指定した場合には IP マスカレード適用時にインタフェースの外側から内側へのパケットは <i>outer_port</i> から <i>inner_port</i> に、内側から外側へのパケットは <i>inner_port</i> から <i>outer_port</i> へとポート番号が変換される。 <i>outer_port</i> を指定せず、 <i>inner_port</i> のみの場合はポート番号の変換はされない。					
[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="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

19.8 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="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

19.9 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 <i>type</i> no nat descriptor masquerade ttl hold					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>type</i> <ul style="list-style-type: none"> • all.....同じホストによるすべての TCP コネクションを対象 • ftp.....FTP の制御チャンネルのみを対象 					
[説明]	<p>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において、データチャンネル上でのデータ転送中に、対応する制御チャンネルが消滅することによるデータ通信不良が発生しないようにするために、制御チャンネルとデータチャンネルの両 IP マスカレードテーブルの TTL を同期させる方法を設定する。</p> <p>all と設定した場合には、同じホストによるすべてのコネクションに対応するテーブルの TTL を同期させる。 ftp と設定した場合には、FTP コネクションに対応するテーブルの TTL のみを同期させる。</p>					
[ノート]	all と設定した場合には、多くのテーブルの TTL が同期して、多くのテーブルが残留するために、内部リソースが枯渇することがある。					
[デフォルト値]	all					
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

19.10 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 <i>nat_descriptor</i> action [<i>ip_address</i>] no nat descriptor masquerade incoming <i>nat_descriptor</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>action</i> <ul style="list-style-type: none"> • 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 ◦ <i>ip_address</i>.....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。 <i>action</i> が forward のときには <i>ip_address</i> を設定する必要がある。					
[デフォルト値]	reject					
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

19.11 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 <i>nat_descriptor</i> start [<i>port_num</i>] no nat descriptor masquerade port range <i>nat_descriptor</i> [start [<i>port_num</i>]]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>nat_descriptor</i>.....NAT ディスクリプタの識別番号 (1..21474836) ◦ <i>start</i>.....開始ポート番号 (1024..65534) ◦ <i>port_num</i> <ul style="list-style-type: none"> • ポートの個数 (1024..4096) • 省略時は 4096 個 					
[説明]	IP マスカレードで利用するポート番号の範囲を設定する。 $start+port_num \leq 65535$ でなくてはならない。					
[デフォルト値]	60000 4096					
[適用モデル]	<table border="1" style="border-collapse: collapse; width: 100%; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

19.12 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	RT105i	RT105e
---------	---------	--------	--------	--------

19.13 IP マスカレードで変換しないポート番号の範囲の設定

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

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

19.14 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	RT105i	RT105e
---------	---------	--------	--------	--------

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

リカーシブサーバ機能は、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。

20.1 DNS を利用するか否かの設定

[入力形式]	dns service <i>service</i> no dns service [<i>service</i>]					
[パラメータ]	◦ <i>service</i> <ul style="list-style-type: none"> • recursive DNS 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="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

20.2 DNS サーバの IP アドレスの設定

[入力形式]	dns server <i>ip_address</i> [<i>ip_address</i> ...] no dns server [<i>ip_address</i> ...]					
[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="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

20.3 DNS ドメイン名の設定

[入力形式]	dns domain <i>domain_name</i> no dns domain [<i>domain_name</i>]					
[パラメータ]	◦ <i>domain_name</i> DNS ドメインを表す文字列					
[説明]	ルータが所属する DNS ドメインを設定する。 ルータのホストとしての機能 (ping, tracert) を使うときに名前解決に失敗した場合、このドメイン名を補完して再度解決を試みる。ルータが DHCP サーバ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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

20.4 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 <i>peer_num</i> no dns server pp [<i>peer_num</i>]					
[パラメータ]	○ <i>peer_num</i> 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ったり、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 msexton 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]	<pre># pp select 2 pp2# ppp ipcp msexton pp2# dns server pp 2</pre>					
[適用モデル]	<table border="1" style="width: 100%; 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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

20.5 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 <i>protocol server</i> [<i>server</i>] no dns notice order <i>protocol</i> [<i>server</i> [<i>server</i>]]					
[パラメータ]	○ <i>protocol</i> <ul style="list-style-type: none"> • <i>dhcp</i> DHCP による通知 • <i>msexton</i> IPCP MS 拡張による通知 ○ <i>server</i> <ul style="list-style-type: none"> • <i>none</i> 一切通知しない • <i>me</i> 本機自身 • <i>server</i> 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。 <i>none</i> 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。 <i>me</i> 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。 <i>server</i> 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 <i>me</i> が続く場合は先頭の 1 つだけと本機自身を、 <i>server</i> 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]	<pre>dhcp me server msexton me server</pre>					
[適用モデル]	<table border="1" style="width: 100%; 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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

20.6 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 <i>spoof</i> no dns private address spoof [<i>spoof</i>]					
[パラメータ]	○ <i>spoof</i> <ul style="list-style-type: none"> • <i>on</i> 処理する • <i>off</i> 処理しない 					
[説明]	<i>on</i> 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]	<i>off</i>					
[適用モデル]	<table border="1" style="width: 100%; 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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

20.7 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 <i>resolv</i> no dns syslog resolv [<i>resolv</i>]					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>resolv</i> <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="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

20.8 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 <i>id server</i> [<i>server2</i>] [<i>type</i>] <i>query</i> [<i>original-sender</i>][<i>restrict pp connection-pp</i>] dns server select <i>id pp peer_num</i> [<i>default-server</i>] [<i>type</i>] <i>query</i> [<i>original-sender</i>] [<i>restrict pp connection-pp</i>] dns server select <i>id dhcp interface</i> [<i>default-server</i>] [<i>type</i>] <i>query</i> [<i>original-sender</i>] [<i>restrict pp connection-pp</i>] dns server select <i>id reject</i> [<i>type</i>] <i>query</i> [<i>original-sender</i>] no dns server select <i>id</i>					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>id</i>DNS サーバ選択テーブルの番号 ○ <i>server</i>プライマリ DNS サーバの IP アドレス ○ <i>server2</i>セカンダリ DNS サーバの IP アドレス ○ <i>type</i>.....DNS レコードタイプ <ul style="list-style-type: none"> • <i>a</i>.....ホストの IP アドレス • <i>ptr</i>.....IP アドレスの逆引き用のポインタ • <i>mx</i>.....メールサーバ • <i>ns</i>.....ネームサーバ • <i>cname</i>別名 • <i>any</i>.....すべてのタイプにマッチする • 省略時は <i>a</i> ○ <i>query</i>.....DNS 問い合わせの内容 <ul style="list-style-type: none"> • <i>type</i> が <i>a</i>、<i>mx</i>、<i>ns</i>、<i>cname</i> の場合 <i>query</i> はドメイン名を表す文字列であり、後方一致とする。例えば、"yamaha.co.jp"であれば、<i>comm.yamaha.co.jp</i>、<i>rtpro.yamaha.co.jp</i> 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。 • <i>type</i> が <i>ptr</i> の場合 <i>query</i> は IP アドレス (<i>ip_address/masklen</i>) であり、<i>masklen</i> を省略したときは IP アドレスにのみマッチし、<i>masklen</i> を指定したときはネットワークアドレスに含まれるすべての IP アドレスにマッチする。DNS 問い合わせに含まれる <i>.in-addr.arpa</i> 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。 ○ <i>original-sender</i>DNS 問い合わせの送信元の IP アドレスの範囲 ○ <i>connection-pp</i>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 ○ <i>peer_num</i>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 ○ <i>interface</i>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 ○ <i>default-server</i><i>peer_num</i> 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]	<p>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 <i>query</i> 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。</p> <p><i>reject</i> キーワードを使用した書式の場合、<i>query</i> 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。</p> <p><i>restrict pp</i> 節が指定されていると、<i>connection-pp</i> 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。</p>					
[ノート]	セカンダリ DNS サーバ <i>server2</i> は Rev.7.00.26, 6.03.25 以降で指定可能。					
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

20.9 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* 名前のタイプ

- *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.rtp.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	RT105i	RT105e
---------	---------	--------	--------	--------

21. 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くほど優先順位が高くなります。

パケットの処理アルゴリズムは、**queue interface type** コマンドにより、優先制御、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。

21.1 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 (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 (PP インタフェースの場合)					
[適用モデル]	<table border="1" style="width: 100%; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

21.2 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(xxx は十進数) • * (ネットマスクの対応するビットが 8 ビットとも 0 と同じ。すべての IP アドレスに対応) ◦ <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"> • プロトコルを表す十進数 • プロトコルを表すニーモニック <table border="1" style="margin-left: 40px; text-align: center;"> <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 • 省略時は * と同じ。 	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

- ポート番号を表す十進数
- ポート番号を表す二一モニク (一部)

二一モニク	ポート番号	二一モニク	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

- 0:0:0:1 FF:FF:FF:FE (2 桁以内の十六進数以外に '*' 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

- 0:0:0:0:1 FF:FF:FF:FF:FE (2 桁以内の十六進数以外に '*' も指定可)
- * (すべての IPX ノード番号)
- 省略時は一つの * 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

- 十進数 (0..255)
- 十六進数 (0x0..0xFF)
- 二一モニク文字列

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)
- 省略時は一つの * と同じ

○ *src_socket* 始点ソケット番号

- 十進数 (0..65535)
- 0x を先頭に持つ 4 桁以内の十六進数
- プロトコルを表す二一モニク

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)
- 省略時は一つの * 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
 - *xx:xx:xx:xx:xx:xx* (*xx* は十六進数)
 - * (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* オフセットを表す十進数 (イーサネットフレームの始点 MAC アドレスの直後を 0 とするバイト数)
- *byte_list*
 - バイト列
 - *xx* (*xx* は 2 桁の十六進数)
 - 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	RT105i	RT105e
---------	---------	---------	--------	--------	--------

21.3 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
 - *shaping* 帯域制御

[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、設定がいら無いということである。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 BRI と PRI インタフェースに対する帯域制御を行う。PP インタフェースにだけ設定できる。**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。

shaping は LAN インタフェースに対する帯域制御を行なう。LAN インタフェースにだけ設定できる。

[デフォルト値] *fifo*

[適用モデル]	RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	---------	--------	--------	--------

21.4 MP インタリーブの設定

[入力形式]	ppp mp interleave [<i>delay</i>] <i>switch</i> no ppp mp interleave [[<i>delay</i>] <i>switch</i>]					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>delay</i> 遅延 (ミリ秒) ○ <i>switch</i> <ul style="list-style-type: none"> • 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。 <i>delay</i> 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、 <i>delay</i> の値と回線速度により決定される。					
[ノート]	<p><i>delay</i> 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。</p> <p style="padding-left: 20px;">ppp ccp type none</p>					
[デフォルト値]	<i>delay</i> = 30 <i>switch</i> = on					
[設定例]	<pre># 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</pre>					
[適用モデル]	<table border="1" style="width: 100%; text-align: center;"> <tr> <td style="background-color: #cccccc;">RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

21.5 クラス分けフィルタの適用

[入力形式]	queue interface class filter list <i>filter_list</i> queue pp class filter list <i>filter_list</i> no queue interface class filter list [<i>filter_list</i>] no queue pp class filter list [<i>filter_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>filter_list</i> 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]	<table border="1" style="width: 100%; text-align: center;"> <tr> <td style="background-color: #cccccc;">RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

21.6 クラス毎のキュー長の設定

[入力形式]	queue interface length <i>len1</i> [<i>len2</i> ... <i>len16</i>] queue pp length <i>len1</i> [<i>len2</i> ... <i>len16</i>] no queue interface length [<i>len1</i> [<i>len2</i> ... <i>len16</i>]] no queue pp length [<i>len1</i> [<i>len2</i> ... <i>len16</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>len1</i>..<i>len16</i>..... クラス 1 からクラス 16 のキュー長 (1..10000) 					
[説明]	インタフェースに対して、指定したクラスのキューに入ること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%; text-align: center;"> <tr> <td style="background-color: #cccccc;">RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

21.7 クラスの属性の設定

[入力形式] **queue interface class property class** bandwidth=*bandwidth* [parent=*parent*] [borrow=*borrow*] [maxburst=*maxburst*] [minburst=*minburst*] [packetsize=*packetsize*]
queue pp class property class bandwidth=*bandwidth* [parent=*parent*] [borrow=*borrow*] [maxburst=*maxburst*] [minburst=*minburst*] [packetsize=*packetsize*]
no queue interface class property class [bandwidth=*bandwidth* ...]
no queue pp class property class [bandwidth=*bandwidth* ...]

- [パラメータ]
- *interface* LAN インタフェース名
 - *class* クラス (1..16)
 - *bandwidth* 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。
 - *parent* 親クラスの番号 (0..16)
 - *borrow* 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
 - on 借りる
 - off 借りない
 - *maxburst* 連続送信できる最大パケット数 (1..10000)
 - *minburst* 安定送信中に連続送信できる最大パケット数 (1..10000)
 - *packetsize* 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] 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。
bandwidth 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。
 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。
 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 (**borrow=on**) 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、**bandwidth** 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り合いで帯域をわけかの目安として使われる。
 帯域を借りてこない設定 (**borrow=off**) だと、このクラスの最大速度は **bandwidth** 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。
 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。

[デフォルト値] *parent* = 0
borrow = on
maxburst = 20
minburst = *maxburst* / 10
packetsize = 512

[適用モデル]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

21.8 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	RT105i	RT105e
---------	---------	--------	--------	--------

22. 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。

22.1 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】	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

22.2 OSPF の使用設定

【入力形式】	ospf use use no ospf use [use]					
【パラメータ】	<ul style="list-style-type: none"> ◦ use <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】	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

22.3 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】	◦ preference OSPF による経路の優先度 (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】	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

22.4 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】	◦ router_id 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】	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

22.5 外部プロトコルによる経路導入

[入力形式]	ospf import from <i>protocol</i> [<i>filter filter_num...</i>] no ospf import from [<i>protocol</i> [<i>filter filter_num...</i>]]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>protocol</i> OSPFの経路テーブルに導入する外部プロトコル <ul style="list-style-type: none"> • <i>static</i> 静的経路 • <i>rip</i> RIP • <i>bgp</i> BGP ◦ <i>filter_num</i> フィルタ番号 					
[説明]	<p>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。</p> <p><i>filter_num</i> 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。</p> <p>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。</p> <ul style="list-style-type: none"> • <i>metric</i> = 1 • <i>type</i> = 2 • <i>tag</i> = 1 					
[デフォルト値]	外部経路は導入しない					
[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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

22.6 外部経路導入に適用するフィルタ定義

[入力形式]	ospf import filter <i>filter_num</i> [<i>not</i>] <i>kind ip_address/mask...</i> [<i>parameter...</i>] no ospf import filter <i>filter_num</i> [[<i>not</i>] <i>kind ip_address/mask...</i>] [<i>parameter...</i>]]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>filter_num</i> フィルタ番号 ◦ <i>kind</i> <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 <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="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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

22.7 OSPF エリア設定

[入力形式]	ospf area area [auth= <i>auth</i>] [stub [cost= <i>cost</i>]] no ospf area area [auth= <i>auth</i>] [stub [cost= <i>cost</i>]]					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>area</i> <ul style="list-style-type: none"> • 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 ○ <i>auth</i> <ul style="list-style-type: none"> • text プレーンテキスト認証 • md5 MD5 認証 ○ <i>cost</i>..... 0 以上の数値 ○ stub [cost=<i>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、エリアボーダー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。 					
[説明]	OSPF エリアを設定する。					
[デフォルト値]	認証は行わない スタブエリアではない					
[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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

22.8 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]	<ul style="list-style-type: none"> ○ <i>area</i> <ul style="list-style-type: none"> • 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 ○ <i>network</i> IP アドレス ○ <i>mask</i>..... 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。 <i>restrict</i> 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]	<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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

22.9 スタブ的接続の広告

[入力形式]	ospf area stubhost area host [cost <i>cost</i>] no ospf area stubhost area host					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>area</i> <ul style="list-style-type: none"> • 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 ○ <i>host</i> IP アドレス ○ <i>cost</i>..... 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]	<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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

22.10 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*
 ● 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。

NAME	VALUE	説明
retransmit-interval	秒数	LSA を連続して送る場合の再送間隔を秒単位で設定する。
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 は十進数で 0 ~ 255、KEY は文字列で 16 文字以内。MD5 認証鍵は 2 つまで設定できる。複数の MD5 認証鍵が設定されている場合には、送信パケットは同じ内容のパケットを複数個、それぞれの鍵による認証データを付加して送信する。受信時には鍵 ID が一致する鍵が比較対象となる。
md5-sequence-mode	second	送信時刻の秒数
	increment	単調増加

[ノート] ○ hello-interval/dead-interval について
 hello-interval と dead-interval の値は、そのインタフェースから直接通信できるすべての近隣ルータ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。

Rev.7.00.26 だけは、md5-sequence-mode の設定は increment の動作となっている。それ以外のリビジョンでは second の動作となっている。

[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
 md5-sequence-mode = second

[適用モデル]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

22.11 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 インタフェース名
- 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。

NAME	VALUE	説明
type	broadcast	ブロードキャスト
	point-to-point	ポイント・ポイント
	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。
cost	コスト	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。(0 .. 65535) $COST = 100000 / S$
priority	優先度	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。(0 .. 255)
retransmit-interval	秒数	LSA を連続して送る場合の再送間隔を秒単位で設定する。
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	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。
poll-interval	秒数	非ブロードキャストリンクでのみ有効なパラメータで、近隣ルータ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。
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。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 は十進数で 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。
md5-sequence-mode	second increment	送信時刻の秒数 単調増加

【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るなくてはならない。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いけい。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
md5-sequence-mode = second

[適用モデル]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

22.12 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*LAN 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 | RT105i | RT105e |
|---------|---------|--------|--------|--------|

23. BGP

23.1 BGPの起動の設定

[入力形式]	bgp use <i>use</i> no bgp use [<i>use</i>]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>use</i> <ul style="list-style-type: none"> • on 起動する • off 起動しない 					
[説明]	BGP を起動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="width: 100%; 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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

23.2 経路の集約の設定

[入力形式]	bgp aggregate <i>ip_address/mask</i> filter <i>filter_num</i> ... no bgp aggregate <i>ip_address/mask</i> [filter <i>filter_num</i> ...]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>ip_address/mask</i> <ul style="list-style-type: none"> • IP アドレス / ネットマスク • all すべてのネットワーク ◦ <i>filter_num</i> フィルタ番号 (1 .. 2147483647) 					
[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; 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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

23.3 経路を集約するためのフィルタの設定

[入力形式]	bgp aggregate filter <i>filter_num</i> protocol [reject] <i>kind</i> <i>ip_address/mask</i> ... no bgp aggregate filter <i>filter_num</i> protocol [[reject] <i>kind</i> <i>ip_address/mask</i> ...]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>filter_num</i> フィルタ番号 (1 .. 2147483647) ◦ <i>protocol</i> <ul style="list-style-type: none"> • static 静的経路 • rip RIP • ospf OSPF • bgp BGP • all すべてのプロトコル ◦ <i>kind</i> <ul style="list-style-type: none"> • 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 ◦ <i>ip_address/mask</i> <ul style="list-style-type: none"> • IP アドレス / ネットマスク • all すべてのネットワーク 					
[説明]	BGP で広告する経路を集約するためのフィルタを定義する。このコマンドで定義したフィルタは、 bgp aggregate コマンドの filter 節で指定されてはじめて効果を持つ。 <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。 <i>kind</i> の前に reject キーワードを置くと、その経路は集約されない。					
[適用モデル]	<table border="1" style="width: 100%; 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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

23.4 AS 番号の設定

[入力形式]	bgp autonomous-system <i>as</i> no bgp autonomous-system [<i>as</i>]					
[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"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

23.5 ルータ ID の設定

[入力形式]	bgp router id <i>ip_address</i> no bgp router id [<i>ip_address</i>]					
[パラメータ]	◦ <i>ip_address</i> 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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

23.6 BGP による経路の優先度の設定

[入力形式]	bgp preference <i>preference</i> no bgp preference [<i>preference</i>]					
[パラメータ]	◦ <i>preference</i> 優先度 (1 .. 2147483647)					
[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、数字が大きいかほど優先度が高い。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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

23.7 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 <i>filter filter_num</i> ... no bgp export remote_as [<i>filter filter_num</i> ...]					
[パラメータ]	◦ <i>remote_as</i> 相手の AS 番号 (1..65535) ◦ <i>filter_num</i> フィルタ番号 (1 .. 2147483647)					
[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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

23.8 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 <i>filter_num</i> [reject] <i>kind ip_address/mask ... [parameter]</i> no bgp export filter <i>filter_num</i> [[reject] <i>kind ip_address/mask ... [parameter]</i>]						
[パラメータ]	<ul style="list-style-type: none"> ○ <i>filter_num</i> フィルタ番号 (1 .. 2147483647) ○ <i>kind</i> <ul style="list-style-type: none"> • 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 ○ <i>ip_address/mask</i> <ul style="list-style-type: none"> • IP アドレス / ネットマスク • all すべてのネットワーク ○ <i>parameter</i> TYPE=VALUE の組 <table border="1" style="margin-left: 20px; border-collapse: collapse; width: 100%;"> <thead> <tr> <th style="text-align: left;">TYPE</th> <th style="text-align: left;">VALUE</th> <th style="text-align: left;">説明</th> </tr> </thead> <tbody> <tr> <td>preference</td> <td>0..255</td> <td>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</td> </tr> </tbody> </table> 	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
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]	<p>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 <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。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 reject キーワードを置くと、その経路が拒否される。</p>						
[ノート]	<i>preference</i> 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。 <i>preference</i> ...0						
[設定例]	<pre># 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</pre>						
[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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e	
RTX2000	RTX1000	RT300i	RT105i	RT105e			

23.9 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 [<i>from_as</i>] [<i>filter filter_num ...</i>] no bgp import remote_as protocol [<i>from_as</i>] [<i>filter filter_num ...</i>]					
[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> <ul style="list-style-type: none"> • static 静的経路 • rip RIP • ospf OSPF • bgp BGP • aggregate 集約経路 ○ <i>from_as</i> 導入する経路を受信した AS (<i>protocol</i> で bgp を指定したときのみ) (1..65535) ○ <i>filter_num</i> フィルタ番号 (1 .. 2147483647) 					
[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="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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

23.10 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]	<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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

23.11 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]
- *filter_num* フィルタ番号 (1 .. 2147483647)
 - *kind*
 - 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
metric	1..16777215	MED(Multi-Exit Discriminator) で通知するメトリック値 (指定しないときは MED を送信しない)

[説明] BGP に導入する経路に適用するフィルタを定義する。このコマンドで定義したフィルタは、**bgp import** コマンドの *filter* 節で指定されてはじめて効果を持つ。
ip_address/mask では、ネットワークアドレスを設定する。複数の設定があるときには、プレフィックスが最も長く一致する設定が採用される。
kind の前に **reject** キーワードを置くと、その経路が拒否される。

[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。
 metric ... 1

[設定例] # **bgp import filter** 1 include 10.0.0.0/16 172.16.0.0/16
 # **bgp import filter** 2 reject equal 192.168.0.0/24

[適用モデル]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

23.12 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	RT105i	RT105e
---------	---------	--------	--------	--------

24. IPv6

24.1 共通の設定

24.1.1 IPv6 パケットを扱うか否かの設定

[入力形式]	ipv6 routing <i>routing</i> no ipv6 routing [<i>routing</i>]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>routing</i> <ul style="list-style-type: none"> • 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

24.1.2 IPv6 インタフェースのリンク MTU の設定

[入力形式]	ipv6 interface mtu <i>mtu</i> ipv6 pp mtu <i>mtu</i> no ipv6 interface mtu <i>mtu</i> no ipv6 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 (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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

24.1.3 TCP セッションの MSS 制限の設定

[書式]	ipv6 interface tcp mss limit <i>mss</i> ipv6 pp tcp mss limit <i>mss</i> ipv6 tunnel tcp mss limit <i>mss</i> no ipv6 interface tcp mss limit [<i>mss</i>] no ipv6 pp tcp mss limit [<i>mss</i>] no ipv6 tunnel tcp mss limit [<i>mss</i>]					
[設定値]	<ul style="list-style-type: none"> ◦ <i>interface</i> LAN インタフェース名 ◦ <i>mss</i> <ul style="list-style-type: none"> • MSS の最大長 (536 .. 1440) • auto 自動設定 • off 設定しない 					
[説明]	インタフェースを通過する TCP セッションの MSS を制限する。インタフェースを通過する TCP パケットを監視し、MSS オプションの値が設定値を越えている場合には、設定値に書き換える。キーワード auto を指定した場合には、インタフェースの MTU、もしくは PP インタフェースの場合で相手の MRU 値が分かる場合にはその MRU 値から計算した値に書き換える。					
[ノート]	PPPoE 用の PP インタフェースに対しては、 pppoe tcp mss limit コマンドでも TCP セッションの MSS を制限することができる。このコマンドと pppoe tcp mss limit コマンドの両方が有効な場合は、MSS はどちらかより小さな方の値に制限される。					
[初期値]	off					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

24.2 IPv6 アドレスの管理

24.2.1 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 interface address auto
ipv6 pp address *ipv6_address/prefix_len*
ipv6 tunnel address *ipv6_address/prefix_len*
no ipv6 interface address *ipv6_address/prefix_len*
no ipv6 interface address auto
no ipv6 pp address *ipv6_address/prefix_len*
no ipv6 tunnel address *ipv6_address/prefix_len*

[パラメータ] ○ *interface*LAN インタフェース名
○ *ipv6_address*.....IPv6 アドレス
○ auto.....LAN インタフェースの自動設定を行うことを示すキーワード
○ *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。
複数の LAN インタフェースで自動設定機能を利用することができる。その場合、デフォルト経路は最後に自動設定が完了したインタフェースに向く。

[適用モデル]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

24.2.2 インタフェースのプレフィックスに基づく IPv6 アドレスの設定

[入力形式] **ipv6 interface prefix** *ipv6_prefix/prefix_len*
ipv6 pp prefix *ipv6_prefix/prefix_len*
ipv6 tunnel prefix *ipv6_prefix/prefix_len*
no ipv6 interface prefix *ipv6_prefix/prefix_len*
no ipv6 pp prefix *ipv6_prefix/prefix_len*
no ipv6 tunnel prefix *ipv6_prefix/prefix_len*

[パラメータ] ○ *interface*LAN インタフェース名
○ *ipv6_prefix*.....IPv6 プレフィックスのアドレス部分
○ *prefix_len*IPv6 プレフィックス長

[説明] インタフェースに IPv6 アドレスを付与する。類似のコマンドに **ipv6 interface address** コマンドがあるが、このコマンドではアドレスではなくプレフィックスのみを指定する。プレフィックス以降の部分は MAC アドレスに基づいて自動的に補完する。このときに使用する MAC アドレスは、設定しようとするインタフェースに割り当てられているものが使われる。ただし、MAC アドレスを持たない PP インタフェースやトンネルインタフェースでは LAN1 インタフェースの MAC アドレスを使用する。

なお、類似の名前を持つ **ipv6 prefix** コマンドはルータ広告で通知するプレフィックスを定義するものであり、IPv6 アドレスを付与するものではない。しかしながら、通常の運用では、インタフェースに付与する IPv6 アドレスのプレフィックスとルータ広告で通知するプレフィックスは同じであるから、双方のコマンドに同じプレフィックスを設定することが多い。

[ノート] このコマンドで設定された IPv6 アドレスは **show ipv6 address** コマンドで確認できる。

[適用モデル]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

24.3 近隣探索

24.3.1 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 <i>prefix_id prefix/len</i> [<i>valid_lifetime=time</i>] [<i>preferred_lifetime=time</i>] [<i>l_flag=switch</i>] [<i>a_flag=switch</i>] no ipv6 prefix <i>prefix_id</i>					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>prefix_id</i> プレフィックス番号 ○ <i>prefix</i> プレフィックス ○ <i>prefix_len</i> プレフィックス長 ○ <i>valid_lifetime</i> プレフィックスの有効寿命 (60..15552000) ○ <i>preferred_lifetime</i> プレフィックスの推奨寿命 (60..15552000) ○ <i>time</i> 時間設定 <ul style="list-style-type: none"> • <i>YYYY-MM-DD,bb:mm[:ss]</i> <ul style="list-style-type: none"> ▪ <i>YYYY</i> 年 (1980..2079) ▪ <i>MM</i> 月 (01..12) ▪ <i>DD</i> 日 (01..31) ▪ <i>bb</i> 時 (00..23) ▪ <i>mm</i> 分 (00..59) ▪ <i>ss</i> 秒 (00..59、省略時は 00) ○ <i>l_flag</i> on-link フラグ ○ <i>a_flag</i> autonomous address configuration フラグ ○ <i>switch</i> <ul style="list-style-type: none"> • on • off 					
[説明]	<p>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。</p> <p><i>time</i> 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。<i>time</i> 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。<i>time</i> として時刻を設定すると、その時刻に寿命が尽きるものとして寿命を計算し、広告する。時刻を設定する場合は、上記のフォーマットに従う。有効寿命とはアドレスが無効になるまでの時間であり、推奨寿命とはアドレスを新たな接続での使用が不可となる時間である。また、on-link フラグはプレフィックスがそのデータリンクに固有である時に on とする。autonomous address configuration フラグはプレフィックスを自律アドレス設定で使うことができる場合に on とする。</p>					
[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]	<pre>valid_lifetime = 2592000 preferred_lifetime = 604800 l_flag = on a_flag = on</pre>					
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

24.3.2 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=switch1] [o_flag=switch2] ipv6 pp rtadv send prefix_id [prefix_id...] [m_flag=switch1] [o_flag=switch2] no ipv6 interface rtadv send no ipv6 pp rtadv send					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>interface</i>LAN インタフェース名 ◦ <i>prefix_id</i>プレフィックス番号 ◦ <i>m_flag</i>managed address configuration フラグ ルータ広告 (RA) による自動設定とは別に、DHCP6 に代表される RA 以外の手段によるアドレス自動設定をホストに許可させるか否かの設定。 ◦ <i>switch1</i> <ul style="list-style-type: none"> • <i>on</i>許可しない • <i>off</i>許可する (これを許可しても RA による自動設定は行われる) ◦ <i>o_flag</i>other stateful configuration フラグ ルータ広告以外の手段により IPv6 アドレス以外のオプション情報をホストに自動的に取得させるか否かの設定。 ◦ <i>switch2</i> <ul style="list-style-type: none"> • <i>on</i>取得させない • <i>off</i>取得させる 					
[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。また、 m_flag および o_flag を利用して、管理するホストがルータ広告以外のステートフル自動設定情報をどのように解釈するかを設定する事も出来る。					
[デフォルト値]	m_flag = off o_flag = off					
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

24.4 経路制御

24.4.1 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]	<ul style="list-style-type: none"> ◦ <i>network</i> <ul style="list-style-type: none"> • IPv6 アドレス / プレフィックス長 • <i>default</i>デフォルト経路 ◦ <i>gateway</i>ゲートウェイ <ul style="list-style-type: none"> • IP アドレス % スコープ識別子 • <i>pp peer_num [dpci=dpci] ...</i> PP インタフェースへの経路 "dpci=dpci" 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>peer_num</i> <ul style="list-style-type: none"> ◻ 相手先情報番号 ◻ <i>anonymous</i> • <i>pp anonymous name=name</i> <ul style="list-style-type: none"> ▪ <i>name</i> PAP/CHAP による名前 • <i>tunnel tunnel_num</i> トンネル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>metric metric</i>メトリックの指定 <ul style="list-style-type: none"> ▪ メトリック値 (1..15) ▪ 省略時は 1 • <i>hide</i>出カインタフェースが 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 LAN 1 が指定されたものとして扱う。					
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

24.5 RIPng

24.5.1 RIPng の使用の設定

[入力形式]	ipv6 rip use use no ipv6 rip use					
[パラメータ]	<ul style="list-style-type: none"> ○ use <ul style="list-style-type: none"> • 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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

24.5.2 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 ipv6 tunnel rip send send no ipv6 interface rip send no ipv6 pp rip send no ipv6 tunnel rip send					
[パラメータ]	<ul style="list-style-type: none"> ○ interface LAN インタフェース名 ○ send <ul style="list-style-type: none"> • 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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

24.5.3 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 receive ipv6 pp rip receive receive ipv6 tunnel rip receive receive no ipv6 interface rip receive no ipv6 pp rip receive no ipv6 tunnel rip receive					
[パラメータ]	<ul style="list-style-type: none"> ○ interface LAN インタフェース名 ○ receive <ul style="list-style-type: none"> • 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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

24.5.4 RIPng の加算ホップ数の設定

[入力形式]	ipv6 interface rip hop direction hop ipv6 pp rip hop direction hop no ipv6 interface rip hop no ipv6 pp rip hop					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>direction</i> <ul style="list-style-type: none"> • <i>in</i> 受信時に加算する • <i>out</i> 送信時に加算する ◦ <i>hop</i> 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]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

24.5.5 インタフェースにおける信頼できる RIPng ゲートウェイの設定

[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]	<ul style="list-style-type: none"> ◦ <i>interface</i> LAN インタフェース名 ◦ <i>gateway</i> IPv6 アドレス 					
[説明]	<p>信頼できる RIPng ゲートウェイを設定する。</p> <p><i>except</i> 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。</p> <p><i>except</i> 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。</p>					
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

24.5.6 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...] ipv6 tunnel rip filter direction filter_list [filter_list...] no ipv6 interface rip filter no ipv6 pp rip filter no ipv6 tunnel rip filter					
[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> 内向きのパケットを対象にする • <i>out</i> 外向きのパケットを対象にする ◦ <i>filter_list</i> 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]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

24.5.7 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]	○ action <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="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

24.5.8 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]	○ 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。					
[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="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

24.5.9 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]	○ action <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="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

24.5.10 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

24.5.11 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]	<ul style="list-style-type: none"> ○ <i>bold</i> <ul style="list-style-type: none"> • 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

24.6 フィルタの設定

24.6.1 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]]] no ipv6 filter filter_num					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>filter_num</i>静的フィルタ番号 (1..21474836) ○ <i>pass_reject</i>フィルタのタイプ (ip filter コマンドに準ずる) ○ <i>src_address</i>IP パケットの始点 IP アドレス ○ <i>prefix_len</i>プレフィックス長 ○ <i>dst_address</i> <ul style="list-style-type: none"> • IP パケットの終点 IP アドレス (<i>src_addr</i> と同じ形式) • 省略時は 1 個の * と同じ。 ○ <i>protocol</i> <ul style="list-style-type: none"> • 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 ○ <i>src_port_list</i>UDP、TCP のソースポート番号 (ip filter コマンドに準ずる) ○ <i>dst_port_list</i>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]	<p>近隣探索に関するパケットとは以下の 4 つを意味する。</p> <ul style="list-style-type: none"> • neighbor advertisement • neighbor solicitation • router advertisement • router solicitation 					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

24.6.2 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...] ipv6 tunnel secure filter direction filter_list [filter_list...] no ipv6 interface secure filter direction no ipv6 pp secure filter direction no ipv6 tunnel secure filter direction					
[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"> • 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 ○ <i>filter_list</i>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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

24.6.3 IPv6 動的フィルタの定義

【入力形式】	<pre> ipv6 filter dynamic <i>dyn_filter_num srcaddr dstaddr protocol</i> [<i>option ...</i>] ipv6 filter dynamic <i>dyn_filter_num srcaddr dstaddr filter filter_list</i> [<i>in_filter_list</i>] [<i>out_filter_list</i>] [<i>option ...</i>] no ipv6 filter dynamic <i>dyn_filter_num</i> [<i>dyn_filter_num...</i>] </pre>					
【パラメータ】	<ul style="list-style-type: none"> ○ <i>dyn_filter_num</i> 動的フィルタ番号 (1..21474836) ○ <i>srcaddr</i> 始点 IPv6 アドレス ○ <i>dstaddr</i> 終点 IPv6 アドレス ○ <i>protocol</i> プロトコルのニーモニック <ul style="list-style-type: none"> • tcp • udp • ftp • tftp • domain • www • smtp • pop3 • telnet ○ <i>filter_list</i> ipv6 filter コマンドで登録されたフィルタ番号のリスト ○ <i>option</i> <ul style="list-style-type: none"> • <i>syslog=switch</i> <ul style="list-style-type: none"> ■ <i>on</i> コネクションの通信履歴を syslog に残す ■ <i>off</i> コネクションの通信履歴を syslog に残さない • <i>timeout=time</i> <ul style="list-style-type: none"> ■ <i>time</i> データが流れなくなったときにコネクション情報を解放するまでの秒数 					
【説明】	<p>IPv6 の動的フィルタを定義する。第 1 書式では、あらかじめルータに登録されているアプリケーション名を指定する。第 2 書式では、ユーザがアクセス制御のルールを記述する。キーワードの filter、in、out の後には、ipv6 filter コマンドで定義されたフィルタ番号を設定する。</p> <p>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。</p> <p>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。</p> <p>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。</p>					
【デフォルト値】	<pre> syslog = on timeout = 60 </pre>					
【適用モデル】	<table border="1" style="width: 100%; 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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

25. ネットボランチ DNS サービスの設定

ネットボランチ DNS とは、一種のダイナミック DNS 機能であり、ルータの IP アドレスをヤマハが運営するネットボランチ DNS サーバに希望の名前で登録することができる。そのため、動的 IP アドレス環境でのサーバ公開や拠点管理などに用いることができます。IP アドレスの登録、更新などの手順には独自のプロトコルを用いるため、他のダイナミック DNS サービスとの互換性はありませ

ん。

ヤマハが運営するネットボランチ DNS サーバは現時点では無料、無保証の条件で運営されている。利用料金は必要無いが、ネットボランチ DNS サーバに対して名前が登録できること、および登録した名前が引けることは保証できません。また、ネットボランチ DNS サーバは予告無く停止することがあることに注意してください。

ネットボランチ DNS には、ホストアドレスサービスと電話番号サービスの 2 種類がありますが、本書で記述するモデルでは電話番号サービスは利用できません。

ネットボランチ DNS では、個々の RT シリーズ、ネットボランチシリーズルータを MAC アドレスで識別しているため、機器の入れ換えなどをした場合には同じ名前がそのまま利用できる保証はありません。

25.1 ネットボランチ DNS サービスの使用の可否

[入力形式] **netvolante-dns use interface switch**
netvolante-dns use pp switch
no netvolante-dns use interface switch
no netvolante-dns use pp [switch]

[パラメータ] ◦ *interface*LAN インタフェース名
 ◦ *switch*
 • *auto*自動更新する
 • *off*自動更新しない

[説明] ネットボランチ DNS サービスを使用するか否かを設定する。
 IP アドレスが更新された時にネットボランチ DNS サーバに自動で IP アドレスを更新する。

[デフォルト値] auto

[適用モデル]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

25.2 ネットボランチ DNS サーバに手動で更新する

[入力形式] **netvolante-dns go interface**
netvolante-dns go pp peer_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

[説明] ネットボランチ DNS サーバに手動で IP アドレスを更新する。

[適用モデル]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

25.3 ネットボランチ DNS サーバから削除する

[入力形式] **netvolante-dns delete go interface [host]**
netvolante-dns delete go pp peer_num [host]

[パラメータ] ◦ *interface*LAN インタフェース名
 ◦ *peer_num*相手先情報番号
 ◦ *host*ホスト名

[説明] 登録した IP アドレスをネットボランチ DNS サーバから削除する。
 インタフェースの後にホスト名を指定することで、指定したホスト名のみを削除可能。

[適用モデル]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

25.4 ネットボランチ DNS サービスで使用するポート番号の設定

[入力形式]	netvolante-dns port <i>port</i> no netvolante-dns port [<i>port</i>]					
[パラメータ]	◦ <i>port</i> ポート番号 (1..65535)					
[説明]	ネットボランチ DNS サービスで使用するポート番号を設定する。					
[デフォルト値]	2002					
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

25.5 ネットボランチ DNS サーバに登録済みのホスト名一覧を取得

[入力形式]	netvolante-dns get hostname list <i>interface</i> netvolante-dns get hostname list pp <i>peer_num</i> netvolante-dns get hostname list all					
[パラメータ]	◦ <i>interface</i> LAN インタフェース名 ◦ <i>peer_num</i> 相手先情報番号 ◦ <i>all</i> すべてのインタフェース					
[説明]	ネットボランチ DNS サーバに登録済みのホスト名一覧を取得し、表示する。					
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

25.6 ホスト名の登録

[入力形式]	netvolante-dns hostname host <i>interface host</i> [duplicate] netvolante-dns hostname host pp <i>host</i> [duplicate] no netvolante-dns hostname host <i>interface</i> [<i>host</i> [duplicate]] no netvolante-dns hostname host pp [<i>host</i> [duplicate]]					
[パラメータ]	◦ <i>interface</i> LAN インタフェース名 ◦ <i>host</i> ホスト名 (128 文字以内)					
[説明]	<p>ネットボランチ DNS サービス (ホストアドレスサービス) で使用するホスト名を設定する。ネットボランチ DNS サーバから取得されるホスト名は、『(ホスト名).(サブドメイン).netvolante.jp』という形になる。(ホスト名)はこのコマンドで設定した名前となり、(サブドメイン)はネットボランチ DNS サーバから割り当てられる。(サブドメイン)をユーザが指定することはできない。</p> <p>このコマンドを一番最初に設定する際は、(ホスト名)部分のみを設定する。ネットボランチ DNS サーバに対する登録・更新が成功すると、コマンドが上記の完全な FQDN の形になって保存される。</p> <p>duplicate を付加すると、1 台のルータで異なるインタフェースに同じ名前を登録できる</p>					
[デフォルト値]	なし					
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

25.7 通信タイムアウトの設定

[入力形式]	netvolante-dns timeout <i>interface time</i> netvolante-dns timeout pp <i>time</i> no netvolante-dns timeout <i>interface</i> [<i>time</i>] no netvolante-dns timeout pp [<i>time</i>]					
[パラメータ]	◦ <i>interface</i> LAN インタフェース名 ◦ <i>time</i> タイムアウト秒数 (1..180)					
[説明]	ネットボランチ DNS サーバとの間の通信がタイムアウトするまでの時間を秒単位で設定する。					
[デフォルト値]	30					
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

25.8 ホスト名を自動生成するか否かの設定

[入力形式]	netvolante-dns auto hostname <i>interface switch</i> netvolante-dns auto hostname pp <i>switch</i> no netvolante-dns auto hostname <i>interface [switch]</i> no netvolante-dns auto hostname pp [<i>switch</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>switch</i> <ul style="list-style-type: none"> • <i>on</i> 自動生成する • <i>off</i> 自動生成しない 					
[説明]	<p>ホスト名の自動生成機能を利用するか否かを設定する。自動生成されるホスト名は、『y' + (MAC アドレス下 6 桁).auto.netvolante.jp』という形になる。</p> <p>このコマンドを 'on' に設定して、netvolante-dns go コマンドを実行すると、ネットボランチ DNS サーバから上記のホスト名が割り当てられる。割り当てられたドメイン名は、show status netvolante-dns コマンドで確認することができる。</p>					
[デフォルト値]	off					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

25.9 ネットボランチ DNS サーバの設定

[入力形式]	netvolante-dns server <i>ip_address</i> netvolante-dns server <i>name</i> no netvolante-dns server [<i>ip_address</i>] no netvolante-dns server [<i>name</i>]					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>ip_address</i>IP アドレス ○ <i>name</i> ドメイン名 					
[説明]	<p>ネットボランチ DNS サーバの IP アドレスまたはホスト名を設定する。</p>					
[デフォルト値]	netvolante-dns.netvolante.jp					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

26. スケジュール

26.1 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 schedule 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。
 第2、第3書式で指定された場合には、それぞれあらかじめ指定された相手先情報番号 / トンネル番号での、**pp select / tunnel select** コマンドが発行済みであるように動作する。
schedule at コマンドは複数指定でき、同じ時刻に指定されたものは *id* の小さな順に実行される。

以下のコマンドは指定できない。

administrator、**administrator password**、**cold start**、**console info** と **console prompt** を除く **console** で始まるコマンド、**date**、**exit**、**help**、**interface reset**、**less** で始まるコマンド、**login password**、**login timer**、**ping**、**ping6**、**pp select**、**provider interface dns server**、**provider interface name**、**quit**、**remote setup**、**save**、**schedule at**、**show** で始まるコマンド、**telnet**、**time**、**timezone**、**traceroute**、**traceroute6**、**tunnel select**

[ノート] 入力時、*command* パラメータに対して TAB キーによるコマンド補完は行わぬが、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	RT105i	RT105e
---------	---------	--------	--------	--------

27. 操作

27.1 相手先情報番号の選択

[入力形式]	pp select <i>peer_num</i> no pp select					
[パラメータ]	◦ <i>peer_num</i> <ul style="list-style-type: none"> • 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。 no pp select コマンドは pp select none コマンドと同じ動作をする。					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.2 トンネルインタフェース番号の選択

[入力形式]	tunnel select <i>tunnel_num</i> no tunnel select					
[パラメータ]	◦ <i>tunnel_num</i> <ul style="list-style-type: none"> • トンネルインタフェース番号 • none トンネルインタフェースを選択しない 					
[説明]	トンネルモードの設定や表示の対象となるトンネルインタフェース番号を選択する。					
[ノート]	本コマンドの操作は、一般ユーザでも実行できる。 プロンプトが tunnel の場合は、pp 関係のコマンドは入力できない。 no tunnel select コマンドは tunnel select none コマンドと同じ動作をする。					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.3 設定に関する操作

27.3.1 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.3.2 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.3.3 設定内容の保存

[入力形式]	save save <i>[filename [comment]]</i>					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>filename</i> 設定を保存するファイル名 <ul style="list-style-type: none"> • 内蔵 Flash ROM の設定ファイル (0.9) • <i>ext0:filename</i>..... PCMCIA Flash ATA カードの設定ファイル ○ <i>comment</i> 設定ファイルのコメント 					
[説明]	<p>現在の設定内容を不揮発性メモリに保存する。</p> <p>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 <i>filename</i> として 0..9 のみ指定可能。RTX1000 では <i>filename</i> として 0 のみ指定可能。</p>					
[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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.3.4 設定ファイルの削除

[入力形式]	delete config filename					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>filename</i> 削除するファイル名 <ul style="list-style-type: none"> • 内蔵フラッシュ ROM の設定ファイル (0.9) • <i>ext0:name</i>..... PCMCIA Flash ATA カードの設定ファイル 					
[説明]	<p>保存されている設定ファイルを削除する。</p> <p>RTX2000 では <i>filename</i> として 0..9 のみ指定可能。RTX1000 では <i>filename</i> として 0 のみ指定可能。</p>					
[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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.3.5 実行形式ファームウェアファイルの削除

[入力形式]	delete exec filename					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>filename</i> 削除するファイル名 <ul style="list-style-type: none"> • <i>ext0:name</i>..... PCMCIA Flash ATA カードの設定ファイル 					
[説明]	<p>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。</p>					
[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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.3.6 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]	<p>内蔵 Flash ROM に保存されている設定ファイルのファイル名、日時、コメントの一覧を表示する。</p>					
[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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.3.7 設定の初期化

[入力形式]	cold start					
[パラメータ]	なし					
[説明]	<p>工場出荷時の設定に戻し、再起動する。</p> <p>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。</p>					
[ノート]	<p>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。</p>					
[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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.3.8 遠隔地のルータの設定

[入力形式]	remote setup interface [isdn_num[/sub_address]] remote setup interface dlci=dlci					
[パラメータ]	<ul style="list-style-type: none"> ◦ interface <ul style="list-style-type: none"> • BRI インタフェース名 • PRI インタフェース名 ◦ isdn_num.....ISDN 番号 ◦ sub_address.....ISDN サブアドレス (0x21 から 0x7e の ASCII 文字列) ◦ dlci..... 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 とも利用でき、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、isdn_num、sub_address 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: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.3.9 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 no remote setup accept					
[パラメータ]	<ul style="list-style-type: none"> ◦ isdn_num.....ISDN 番号 ◦ sub_address.....ISDN サブアドレス (0x21 から 0x7e の ASCII 文字列) ◦ isdn_num_list..... ISDN 番号だけまたは ISDN 番号とサブアドレスを空白で区切った並び ◦ any..... すべての遠隔地のルータからの設定を許可することを示すキーワード ◦ none..... すべての遠隔地のルータからの設定を拒否することを示すキーワード 					
[説明]	自分のルータの設定を許可する相手先を設定する。					
[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: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.4 動的情報のクリア操作

27.4.1 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]	<ul style="list-style-type: none"> ◦ interface <ul style="list-style-type: none"> • BRI インタフェース名 • PRI インタフェース名 ◦ peer_num <ul style="list-style-type: none"> • 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 (第 1 書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]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.4.2 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: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.4.3 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"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.4.4 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】	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.4.5 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】	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.4.6 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】	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.4.7 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】	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.4.8 InARP のクリア

【入力形式】	clear inarp [<i>peer_num</i>]					
【パラメータ】	<ul style="list-style-type: none"> ◦ <i>peer_num</i> <ul style="list-style-type: none"> • 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】	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.4.9 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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.4.10 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]	◦ <i>pri</i>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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.4.11 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]	◦ <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]	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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.4.12 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]	◦ <i>interface</i>LAN インタフェース名 ◦ <i>peer_num</i>相手先情報番号 ◦ <i>tunnel_num</i>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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.4.13 IPv6 の動的経路情報の消去

[入力形式]	clear ipv6 dynamic routing					
[パラメータ]	なし					
[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]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.4.14 近隣キャッシュの消去

[入力形式]	clear ipv6 neighbor cache					
[パラメータ]	なし					
[説明]	近隣キャッシュを消去する。					
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.5 その他の操作

27.5.1 相手先の使用許可の設定

[入力形式]	pp enable peer_num no pp enable peer_num					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>peer_num</i> <ul style="list-style-type: none"> • 相手先情報番号 • <i>anonymous</i> • <i>all</i>..... すべての相手先情報番号 					
[説明]	<p>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 <i>disable</i> 状態なので、使用する場合は必ずこのコマンドで <i>enable</i> 状態にしなければならぬ。</p>					
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.5.2 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]	<ul style="list-style-type: none"> ◦ <i>peer_num</i> <ul style="list-style-type: none"> • 相手先情報番号 • <i>anonymous</i> • <i>all</i>..... すべての相手先情報番号 					
[説明]	<p>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 <i>disable</i> 状態であることが望ましい。</p>					
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.5.3 再起動

[入力形式]	restart restart [binary][file]					
[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 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"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.5.4 インタフェースの再起動

[入力形式]	interface reset interface [interface ...]					
[パラメータ]	<ul style="list-style-type: none"> ◦ <i>interface</i> <ul style="list-style-type: none"> • LAN インタフェース名 • BRI インタフェース名 • PRI 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。 LAN インタフェースでは、オートネゴシエーションする設定になっていればオートネゴシエーション手順が起動される。 BRI と PRI インタフェースでは、回線種別を line type コマンドで変更した場合には、本コマンドでインタフェースを再起動する必要がある。 なお、MP を使用しているインタフェースに対しては、interface reset pp コマンドを使用する。</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バインドされているすべての相手先情報番号の通信を停止した状態で、また回線種別を変更する場合には回線を抜いた状態で実行すること。					
[適用モデル]	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.5.5 PP インタフェースの再起動[入力形式] **interface reset pp** [*peer_num*][パラメータ] ◦ *peer_num*
• 相手先情報番号
• anonymous

[説明] 選択した相手先番号にバインドされているインタフェースをリセットする。MP を使用しているインタフェースに対して使用する。

[適用モデル]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

27.5.6 発信[入力形式] **connect** *peer_num*[パラメータ] ◦ *peer_num*.....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]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

27.5.7 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.....すべての相手先情報番号
• anonymous anonymous のすべて
• 指定した anonymous (anonymous1 ..)

[説明] 手動で切断する。

[適用モデル]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

27.5.8 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 は十進数))
• traceroute をかけるホストの名称
◦ noresolvDNS による解決を行わないことを示すキーワード

[説明] 指定したホストまでの経路を調べて表示する。

[適用モデル]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

27.5.9 traceroute6 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	RT105i	RT105e
---------	---------	--------	--------	--------

27.5.10 ping

[入力形式]	ping [-s <i>datalen</i>] [-c <i>count</i>] [-sa <i>ip_address</i>] <i>host</i>					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>datalen</i> データ長 (64 .. 65535) ○ <i>count</i> 実行回数 (1..21474836) ○ <i>ip_address</i> 始点 IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数)) ○ <i>host</i> <ul style="list-style-type: none"> • ping をかけるホストの IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数)) • ping をかけるホストの名称 					
[説明]	ICMP Echo を指定したホストに送出し、ICMP Echo Reply が送られてくるのを待つ。送られてきたら、その旨表示する。コマンドが終了すると簡単な統計情報を表示する。 <i>count</i> パラメータを省略すると、Ctrl+c キーを入力するまで実行を継続する。					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.5.11 ping6 の実行

[入力形式]	ping6 <i>destination</i> [<i>count</i>] ping6 <i>destination scope_id</i> [<i>count</i>] ping6 <i>destination interface</i> [<i>count</i>] ping6 <i>destination</i> pp <i>peer_num</i> [<i>count</i>]					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>destination</i> 送信する宛先の IPv6 アドレス、または名前 ○ <i>scope_id</i> スコープ ID ○ <i>interface</i> LAN インタフェース名 ○ <i>peer_num</i> 相手先情報番号 ○ <i>count</i> 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.5.12 TELNET サーバ機能の ON/OFF の設定

[入力形式]	telnetd service <i>service</i> no telnetd service					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>service</i> <ul style="list-style-type: none"> • 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.5.13 TELNET サーバ機能の listen ポートの設定

[入力形式]	telnetd listen <i>port</i> no telnetd listen					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>port</i> 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.5.14 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...]**
no telnetd host

[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二一モニク
- 1 個の IP アドレスまたは間にマイナス (-) をはさんだ IP アドレス (範囲指定)、及びこれらを任意に並べたもの
- any.....すべてのホストからのアクセスを許可する
- none.....すべてのホストからのアクセスを禁止する

[説明] TELNET 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] 二一モニクをリストにすることはできない。
 設定後の新しい TELNET 接続から適用される。

[デフォルト値] any

[適用モデル]	RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	---------	--------	--------	--------

27.5.15 TELNET クライアント

[入力形式] **telnet host [port [mode [negotiation [abort]]]]**

[パラメータ] ○ *host*.....TELNET をかける相手の IP アドレス、またはホスト名

○ *port*.....使用するポート番号

- 十進数
- ポート番号の二一モニク
- 省略時は 23 (TELNET)

○ *mode*.....TELNET 通信 (送信) の動作モード

- character.....文字単位で通信する
- line.....行単位で通信する
- auto.....*port* パラメータの設定値により *character/line* を選択
- 省略時は auto

○ *negotiation*.....TELNET オプションのネゴシエーションの選択

- on.....ネゴシエーションする
- off.....ネゴシエーションしない
- auto.....*port* パラメータの設定値により on/off を選択
- 省略時は auto

○ *abort*.....TELNET クライアントを強制的に終了させるためのアボートキー

- 十進数の ASCII コード
- 省略時は 29(^)

[説明] TELNET クライアントを実行する。

[ノート] character モードは、通常の TELNET サーバ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	RT105i	RT105e
---------	---------	---------	--------	--------	--------

27.5.16 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 filename internal**

[パラメータ] ○ *filename*.....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	RT105i	RT105e
---------	---------	---------	--------	--------	--------

27.5.17 IPv4 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 ip connection session_id [channel_id]					
【パラメータ】	<ul style="list-style-type: none"> ◦ <i>session_id</i> セッションの識別子 ◦ <i>channel_id</i> 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】	<table border="1" style="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.5.18 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】	<ul style="list-style-type: none"> ◦ <i>session_id</i> セッションの識別子 ◦ <i>channel_id</i> 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】	<table border="1" style="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

27.5.19 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】	<ul style="list-style-type: none"> ◦ <i>pri</i> PRI 番号 (1..4) ◦ <i>a</i> ループバック A を示すキーワード ◦ <i>timeslot</i> タイムスロットループバックを示すキーワード ◦ <i>data</i> 送信データパターン (1..4) <table border="1" style="margin-left: 40px; border-collapse: collapse; width: 200px;"> <thead> <tr> <th style="text-align: center;"><i>data</i></th> <th style="text-align: center;">擬似ランダムパターン</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">1</td> <td style="text-align: center;">$2^6 - 1$</td> </tr> <tr> <td style="text-align: center;">2</td> <td style="text-align: center;">$2^7 - 1$</td> </tr> <tr> <td style="text-align: center;">3</td> <td style="text-align: center;">$2^9 - 1$</td> </tr> <tr> <td style="text-align: center;">4</td> <td style="text-align: center;">$2^{11} - 1$</td> </tr> </tbody> </table> <ul style="list-style-type: none"> ◦ <i>bead</i> 先頭タイムスロット番号 (1..24) ◦ <i>number</i> タイムスロット数 (1..24) 	<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	$2^{11} - 1$
<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	$2^{11} - 1$										
【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。 <i>a</i> 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。 <i>timeslot</i> 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。										
【適用モデル】	<table border="1" style="display: inline-table; 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;">RT105i</td> <td style="text-align: center;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e					
RTX2000	RTX1000	RT300i	RT105i	RT105e							

27.5.20 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]	<ul style="list-style-type: none"> ○ <i>pri</i>PRI 番号 (1..4) ○ <i>remote</i>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 ○ <i>payload</i>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 ○ <i>timeslot</i>タイムスロットループバックを示すキーワード ○ <i>bead</i>先頭タイムスロット番号 (1..24) ○ <i>number</i>タイムスロット数 (1..24) 					
[説明]	<p>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。</p>					
[ノート]	<p>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。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。</p>					
[適用モデル]	<table border="1" style="width: 100%; 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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

28. 設定の表示

28.1 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。 <ul style="list-style-type: none"> • 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) • ファン、内部温度の状態 (RTX2000 のみ) 					
【適用モデル】	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

28.2 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】	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

28.3 指定した PP の設定内容の表示

【入力形式】	show config pp [<i>peer_num</i>] less config pp [<i>peer_num</i>]					
【パラメータ】	◦ <i>peer_num</i> <ul style="list-style-type: none"> • 相手先情報番号 • anonymous • 省略時、選択されている相手について表示する 					
【説明】	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】	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

28.4 ファイル情報の一覧の表示

【入力形式】	show file list <i>location</i> less file list <i>location</i>					
【パラメータ】	◦ <i>location</i> 表示するファイルのある位置 <ul style="list-style-type: none"> • 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 <i>location</i> として <i>internal</i> のみ指定可能。					
【適用モデル】	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

28.5 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					
【パラメータ】	なし					
【説明】	すべてのインタフェースについて、付与されている IPv6 アドレスを表示する。					
【適用モデル】	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

28.6 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	RT105i	RT105e
---------	---------	--------	--------	--------

29. 状態の表示

29.1 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。					
【ノート】	ARP テーブルのエントリ数は LAN インタフェース数の 256 倍である。 ARP エントリの保持時間は 1200 秒固定である。					
【適用モデル】	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

29.2 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】	<ul style="list-style-type: none"> ◦ <i>interface</i> <ul style="list-style-type: none"> • LAN インタフェース名 • BRI インタフェース名 • PRI 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】	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

29.3 各相手先の状態の表示

【入力形式】	show status pp [peer_num]					
【パラメータ】	<ul style="list-style-type: none"> ◦ <i>peer_num</i> <ul style="list-style-type: none"> • 相手先情報番号 • anonymous • 省略時、選択されている相手について表示する 					
【説明】	<p>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。</p> <ul style="list-style-type: none"> • 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】	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

29.4 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】	<ul style="list-style-type: none"> ◦ <i>destination</i> <ul style="list-style-type: none"> • 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】	<p>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。</p>					
【適用モデル】	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

29.5 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	RT105i	RT105e
---------	---------	--------	--------	--------

29.6 IPv6 の経路情報の表示

[入力形式] **show ipv6 route**

[パラメータ] なし

[説明] IPv6 の経路情報を表示する。

[適用モデル]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

29.7 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	RT105i	RT105e
---------	---------	--------	--------	--------

29.8 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	RT105i	RT105e
---------	---------	--------	--------	--------

29.9 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**
- 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	RT105i	RT105e
---------	---------	--------	--------	--------

29.10 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 文字は八進数で表示される。

[適用モデル]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

29.11 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】	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

29.12 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】	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

29.13 IPsec の SA の表示

【入力形式】	show ipsec sa [id] show ipsec sa gateway [gateway_id] [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"> • セキュリティ・ゲートウェイの識別子 • 省略時はすべてのセキュリティ・ゲートウェイの SA のサマリを表示する。 ○ <i>detail</i> 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"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

29.14 VRRP の情報の表示

【入力形式】	show status vrrp [interface [vrid]]					
【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"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

29.15 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 [nat_descriptor]					
【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) • <i>all</i> すべての NAT ディスクリプタ番号 					
【説明】	<i>nat_descriptor</i> を省略した場合にはすべての NAT ディスクリプタ番号について表示する。 動的な NAT ディスクリプタのアドレスマップを表示する。					
【適用モデル】	<table border="1"> <tr> <td>RTX2000</td> <td>RTX1000</td> <td>RT300i</td> <td>RT105i</td> <td>RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

29.16 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** *interface*
show nat descriptor interface bind pp
show nat descriptor interface bind tunnel

[パラメータ] ◦ *interface*LAN インタフェース名

[説明] NAT ディスクリプタと適用インタフェースのリストを表示する。

[適用モデル]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

29.17 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	RT105i	RT105e
---------	---------	--------	--------	--------

29.18 PPTP の状態の表示

[入力形式] **show status pptp**

[パラメータ] なし

[説明] PPTP の状態や GRE の統計情報などを表示する。

[適用モデル]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------

29.19 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

- databaseOSPF 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	RT105i	RT105e
---------	---------	--------	--------	--------

29.20 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	RT105i	RT105e
---------	---------	--------	--------	--------

29.21 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]	<p>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。</p> <ul style="list-style-type: none"> • 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

29.22 DHCP クライアントの状態の表示

[入力形式]	show status dhcpc					
[パラメータ]	なし					
[説明]	<p>DHCP クライアントの状態を表示する。</p> <ul style="list-style-type: none"> ○ クライアントの状態 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • DNS サーバ • ゲートウェイ 					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

29.23 バックアップ状態の表示

[入力形式]	show status backup					
[パラメータ]	なし					
[説明]	バックアップの設定されたインタフェースについて、バックアップの状態を表示する。					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

29.24 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 [<i>direction</i>] show ip connection pp [<i>peer_num</i>] [<i>direction</i>] show ip connection tunnel [<i>tunnel_num</i>] [<i>direction</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 ○ <i>tunnel_num</i> トンネルインタフェース番号 ○ <i>direction</i> <ul style="list-style-type: none"> • <i>in</i> 入力方向 • <i>out</i> 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

29.25 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 [<i>direction</i>] show ipv6 connection pp [<i>peer_num</i>] [<i>direction</i>] show ipv6 connection tunnel [<i>tunnel_num</i>] [<i>direction</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 ○ <i>tunnel_num</i> トンネルインタフェース番号 ○ <i>direction</i> <ul style="list-style-type: none"> ● <i>in</i> 入力方向 ● <i>out</i> 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]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

29.26 ネットワーク監視機能の状態の表示

[入力形式]	show status ip keepalive					
[パラメータ]	なし					
[説明]	ネットワーク監視機能の状態を表示する。					
[ノート]	Rev.7.01 以上で実行可能。					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

29.27 侵入情報の履歴の表示

[入力形式]	show ip intrusion detection interface [<i>direction</i>] show ip intrusion detection pp [<i>peer_num</i>] [<i>direction</i>] show ip intrusion detection tunnel [<i>tunnel_num</i>] [<i>direction</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 ○ <i>tunnel_num</i> トンネルインタフェース番号 ○ <i>direction</i> <ul style="list-style-type: none"> ● <i>in</i> 入力方向 ● <i>out</i> 出力方向 					
[説明]	最近の侵入情報を表示する。各インタフェースの各方向ごとに最大 50 件まで表示できる。					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

29.28 相手先ごとの接続時間情報の表示

[入力形式]	show pp connect time [<i>peer_num</i>]					
[パラメータ]	<ul style="list-style-type: none"> ○ <i>peer_num</i> <ul style="list-style-type: none"> ● 相手先情報番号 ● anonymous ● 省略時、選択されている相手について表示 					
[説明]	選択されている相手の接続時間情報を表示する。					
[適用モデル]	<table border="1" style="display: inline-table; border-collapse: collapse;"> <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;">RT105i</td> <td style="padding: 2px 10px;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

29.29 ネットボランチ DNS サービスに関する設定の表示

[入力形式]	show status netvolante-dns interface show status netvolante-dns pp [peer_num]					
[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> <ul style="list-style-type: none"> • 相手先情報番号 • 省略時、選択されている相手について表示 					
[説明]	<p>ダイナミック DNS に関する設定を表示する。</p> <p>[表示内容]</p> <pre> ネットボランチ DNS サービス: AUTO/OFF インタフェース: INTERFACE ホストアドレス: aaa.bbb.netvolante.jp 電話アドレス: 01234567.tel.netvolante.jp IP アドレス: aaa.bbb.ccc.ddd 最新更新日時: 2001/01/25 15:00:00 タイムアウト: 30sec </pre>					
[適用モデル]	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20%;">RTX2000</td> <td style="width: 20%;">RTX1000</td> <td style="width: 20%;">RT300i</td> <td style="width: 20%;">RT105i</td> <td style="width: 20%;">RT105e</td> </tr> </table>	RTX2000	RTX1000	RT300i	RT105i	RT105e
RTX2000	RTX1000	RT300i	RT105i	RT105e		

30. ログイン

30.1 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	RT105i	RT105e
---------	---------	--------	--------	--------

30.2 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 インタフェース名
- PRI インタフェース名

○ *peer_num*

- 相手先情報番号
- anonymous
- 省略時、選択されている相手について表示する

[説明] 以下の項目を表示

- 発信回数
- 着信回数
- ISDN 料金の総計

[ノート] 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	RT105i	RT105e
---------	---------	--------	--------	--------

30.3 通信履歴の表示

[入力形式] **show history**

[パラメータ] なし

[説明] 通信履歴を表示する。

[適用モデル]

RTX2000	RTX1000	RT300i	RT105i	RT105e
---------	---------	--------	--------	--------



本書は大豆油インクで印刷しています。
本書は無塩素紙(ECF:無塩素紙漂白パルプ)を使用しています。

