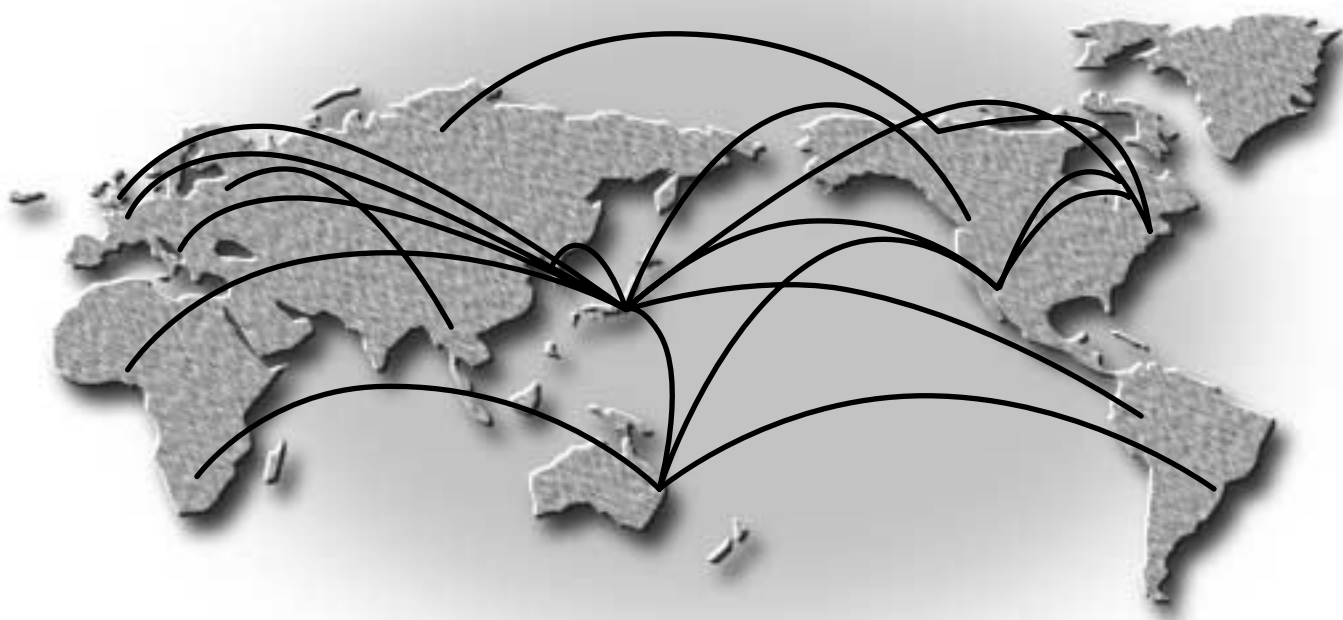


***REMOTE ROUTER***

**コマンドリファレンス**

---



本書の記載内容の一部または全部を無断で転載することを禁じます。  
本書の記載内容は将来予告なく変更されることがあります。  
本製品を使用した結果発生した情報の消失等の損失については、当社では責任を負いかねます。  
保証は本製品物損の範囲に限ります。予めご了承ください。  
本書の内容については万全を期して作成致しておりますが、記載漏れやご不審な点がございましたらご一報くださいますようお願い致します。

イーサネットは富士ゼロックス社の登録商標です。  
Windows は米国 Microsoft 社の登録商標です。  
NetWare は米国 Novell,Inc. の登録商標です。  
INS ネット 64 は日本電信電話株式会社の登録商標です。

1.	コマンドリファレンスの見方	15
1.1	対応するプログラムのリビジョン	15
1.2	コマンドリファレンスの見方	15
1.3	インタフェース名について	15
1.4	no で始まるコマンドの入力形式について	16
2.	ヘルプ	17
2.1	コンソールに対する簡易説明の表示	17
2.2	コマンド一覧の表示	17
3.	機器の設定	18
3.1	ログインパスワードの設定	18
3.2	管理パスワードの設定	18
3.3	セキュリティクラスの設定	18
3.4	ログインタイマの設定	18
3.5	タイムゾーンの設定	19
3.6	現在の日付けの設定	19
3.7	現在の時刻の設定	19
3.8	リモートホストによる時計の設定	19
3.9	NTP による時計の設定	19
3.10	コンソールの言語とコードの設定	20
3.11	コンソールの表示文字数の設定	20
3.12	コンソールの表示行数の設定	20
3.13	コンソールにシステムメッセージを表示するか否かの設定	20
3.14	コンソールのプロンプト表示の設定	21
3.15	SYSLOG を受けるホストの IP アドレスの設定	21
3.16	SYSLOG ファシリティの設定	21
3.17	NOTICE タイプの SYSLOG を出力するか否かの設定	21
3.18	INFO タイプの SYSLOG を出力するか否かの設定	21
3.19	DEBUG タイプの SYSLOG を出力するか否かの設定	22
3.20	TFTP によりアクセスできるホストの IP アドレスの設定	22
3.21	LAN インタフェースの速度タイプの設定	22
3.22	TCP/UDP の各種サービスの動作の設定	22
3.23	SYSLOG パケットの始点ポート番号の設定	22
3.24	マスタクロック用インタフェースの設定	23
3.25	電源 2 の設定	23
3.26	温度監視の閾値の設定	23
4.	ISDN 関連の設定	24
4.1	自分側の設定	24
4.1.1	自分の ISDN 番号の設定	24
4.1.2	課金額による発信制限の設定	25
4.1.3	PIAFS の発信方式の設定	25
4.1.4	PIAFS の着信を許可するか否かの設定	26
4.1.5	PIAFS 接続時の起動側の指定	26
4.1.6	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	26
4.1.7	バックアップからの復帰待ち時間の設定	26
4.1.8	終端抵抗の設定	27
4.1.9	PP で使用するインタフェースの設定	27
4.2	相手側の設定	27
4.2.1	相手への発信順序の設定	28
4.2.2	自動接続の設定	28
4.2.3	自動切断の設定	28
4.2.4	着信許可の設定	28
4.2.5	発信許可の設定	29
4.2.6	再発信抑制タイマの設定	29
4.2.7	エラー切断後の再発信禁止タイマの設定	29
4.2.8	相手にコールバック要求を行うか否かの設定	29
4.2.9	コールバック要求タイプの設定	29
4.2.10	相手からのコールバック要求に応じるか否かの設定	30
4.2.11	コールバック受け入れタイプの設定	30
4.2.12	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	30

4.2.13	コールバックタイマの設定	30
4.2.14	コールバック待機タイマの設定	30
4.2.15	ISDN 回線を切断するタイマ方式の指定	31
4.2.16	切断タイマの設定 (ノーマル)	31
4.2.17	入力切断タイマの設定 (ノーマル)	31
4.2.18	出力切断タイマの設定 (ノーマル)	31
4.2.19	課金単位時間方式での課金単位時間と監視時間の設定	32
4.2.20	切断タイマの設定 (ファスト)	32
4.2.21	切断タイマの設定 (強制)	32
5.	IP の設定	33
5.1	インタフェース共通の設定	33
5.1.1	IP アドレスの設定	33
5.1.2	IP の静的経路情報の設定	34
5.1.3	IP パケットのフィルタの設定	35
5.1.4	フィルタセットの定義	36
5.1.5	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	36
5.1.6	Directed-Broadcast パケットをフィルタアウトするか否かの設定	37
5.1.7	動的フィルタの定義	37
5.1.8	動的フィルタのタイムアウトの設定	38
5.1.9	侵入検知機能の動作の設定	38
5.1.10	フィルタリングによるセキュリティの設定	39
5.1.11	IP パケットの TOS フィールドの書き換えの設定	39
5.1.12	インタフェースの MTU の設定	40
5.2	代理 ARP の設定	40
5.3	PP 側の設定	40
5.3.1	PP 側 IP アドレスの設定	40
5.3.2	リモート IP アドレスプールの設定	41
5.4	RIP の設定	41
5.4.1	RIP による経路の優先度の設定	41
5.4.2	RIP パケットの送信に関する設定	41
5.4.3	RIP パケットの受信に関する設定	42
5.4.4	RIP に関して信用できるゲートウェイの設定	42
5.4.5	RIP のフィルタリングの設定	42
5.4.6	RIP で加算するホップ数の設定	42
5.4.7	RIP2 での認証の設定	43
5.4.8	RIP2 での認証キーの設定	43
5.4.9	回線切断時の経路保持の設定	43
5.4.10	回線接続時の PP 側の RIP の動作の設定	43
5.4.11	回線接続時の PP 側の RIP 送出の時間間隔の設定	43
5.4.12	回線切断時の PP 側の RIP の動作の設定	44
5.4.13	回線切断時の PP 側の RIP 送出の時間間隔の設定	44
5.5	VRRP の設定	44
5.5.1	インタフェース毎の VRRP の設定	44
5.5.2	シャットダウントリガの設定	45
6.	IPX の設定	46
6.1	インタフェース共通の設定	46
6.1.1	IPX パケットのフィルタの設定	47
6.1.2	静的な SAP テーブルの設定	48
6.1.3	IPX SAP Get Nearest Server Request に応答するか否かの設定	48
6.2	LAN 側の設定	48
6.2.1	LAN 側の IPX ネットワーク番号の設定	49
6.2.2	経路情報の追加	49
6.2.3	LAN 側の RIP/SAP ブロードキャストの設定	49
6.2.4	LAN 側でのフィルタリングによるセキュリティの設定	49
6.3	PP 側相手毎の IPX の設定	50
6.3.1	PP 側 IPX ネットワーク番号の設定	50
6.3.2	経路情報の追加	50
6.3.3	回線接続時の PP 側の RIP/SAP の動作の設定	50
6.3.4	回線接続時の PP 側の RIP/SAP 送出の時間間隔の設定	51

6.3.5	回線切断時の PP 側の RIP/SAP の動作の設定	51
6.3.6	回線切断時の PP 側の RIP/SAP 送出の時間間隔の設定	51
6.3.7	回線切断時に RIP/SAP 情報を保持するか否かの設定	51
6.3.8	IPXWAN 使用の設定	51
6.3.9	Timer/Information Request の再送間隔と最大再送回数の設定	52
6.3.10	IPXWAN プライマリネットワーク番号の設定	52
6.3.11	Watchdog パケットに対する代理応答の設定	52
6.3.12	Watchdog 代理応答の時間間隔の設定	52
6.3.13	SPX キープアライブ代理応答を行うか否かの設定	52
6.3.14	SPX キープアライブ代理応答のタイマの設定	53
6.3.15	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	53
6.3.16	PP 側でのフィルタリングによるセキュリティの設定	53
7.	ブリッジの設定	54
7.1	インタフェース共通の設定	54
7.1.1	ブリッジするインタフェースの設定	54
7.1.2	ブリッジのフィルタの設定	55
7.1.3	MAC アドレスのラーニングを行うか否かの設定	55
7.1.4	ラーニング情報消去タイマの設定	55
7.2	LAN 側の設定	56
7.2.1	LAN 側でのブリッジのフィルタリングの設定	56
7.3	PP 側相手毎のブリッジの設定	56
7.3.1	PP 側でのブリッジのフィルタリングの設定	56
8.	PPP の設定	57
8.1	相手の名前とパスワードの設定	57
8.2	要求する認証タイプの設定	57
8.3	受け入れる認証タイプの設定	58
8.4	自分の名前とパスワードの設定	58
8.5	同一 username を持つ相手からの二重接続を禁止するか否かの設定	58
8.6	LCP 関連の設定	58
8.6.1	Magic Number オプション使用の設定	59
8.6.2	Maximum Receive Unit オプション使用の設定	59
8.6.3	Protocol Field Compression オプション使用の設定	59
8.6.4	Icp-restart パラメータの設定	59
8.6.5	Icp-max-terminate パラメータの設定	60
8.6.6	Icp-max-configure パラメータの設定	60
8.6.7	Icp-max-failure パラメータの設定	60
8.6.8	Configure-Request をすぐに送信するか否かの設定	60
8.6.9	専用線キープアライブを使用するか否かの設定	60
8.6.10	専用線キープアライブのログをとるか否かの設定	61
8.6.11	専用線キープアライブの時間間隔の設定	61
8.6.12	専用線ダウン検出時の動作の設定	61
8.7	PAP 関連の設定	61
8.7.1	pap-max-authreq パラメータの設定	61
8.8	CHAP 関連の設定	62
8.8.1	chap-max-challenge パラメータの設定	62
8.9	IPCP 関連の設定	62
8.9.1	PP 側 IP アドレスのネゴシエーションの設定	62
8.9.2	ipcp-restart パラメータの設定	62
8.9.3	ipcp-max-terminate パラメータの設定	63
8.9.4	ipcp-max-configure パラメータの設定	63
8.9.5	ipcp-max-failure パラメータの設定	63
8.9.6	IPCP の MS 拡張オプションを使うか否かの設定	63
8.9.7	WINS サーバの IP アドレスの設定	63
8.10	IPXCP 関連の設定	64
8.10.1	ipxcp-max-terminate パラメータの設定	64
8.10.2	ipxcp-max-configure パラメータの設定	64
8.10.3	ipxcp-max-failure パラメータの設定	64

8.11	BCP 関連の設定	64
8.11.1	Tinygram compression 使用の設定	65
8.11.2	bcp-restart パラメータの設定	65
8.11.3	bcp-max-terminate パラメータの設定	65
8.11.4	bcp-max-configure パラメータの設定	65
8.11.5	bcp-max-failure パラメータの設定	65
8.12	MSCBCP 関連の設定	65
8.12.1	mscbcp-maxretry パラメータの設定	66
8.13	CCP 関連の設定	66
8.13.1	ccp-restart パラメータの設定	66
8.13.2	ccp-max-terminate パラメータの設定	66
8.13.3	ccp-max-configure パラメータの設定	66
8.13.4	ccp-max-failure パラメータの設定	67
8.14	MP 関連の設定	67
8.14.1	MP の制御方法の設定	67
8.14.2	MP のための負荷閾値の設定	67
8.14.3	MP の最大リンク数の設定	68
8.14.4	MP の最小リンク数の設定	68
8.14.5	MP のための負荷計測間隔の設定	68
8.14.6	MP のパケットを分割するか否かの設定	68
8.15	BACP 関連の設定	68
8.15.1	bacp-max-terminate パラメータ の設定	69
8.15.2	bacp-max-configure パラメータ の設定	69
8.15.3	bacp-max-failure パラメータ の設定	69
8.15.4	bap-restart パラメータの設定	69
8.15.5	bap-max-retry パラメータの設定	69
8.16	PPPoE 関連の設定	69
8.16.1	PPPoE で使用する LAN インタフェースの指定	69
8.16.2	アクセスコンセントレータ名の設定	70
8.16.3	セッションの自動接続の設定	70
8.16.4	セッションの自動切断の設定	70
8.16.5	PADI パケットの最大再送回数の設定	70
8.16.6	PADI パケットの再送時間の設定	70
8.16.7	PADR パケットの最大再送回数の設定	70
8.16.8	PADR パケットの再送時間の設定	71
8.16.9	PPPoE セッションの切断タイマの設定	71
8.16.10	TCP パケットの MSS の制限の有無とサイズの指定	71
9.	DHCP の設定	72
9.1	DHCP の動作の設定	72
9.2	RFC2131 対応動作の設定	73
9.3	DHCP スコープの定義	74
9.4	DHCP 予約アドレスの設定	75
9.5	DHCP オプションの設定	76
9.6	リースする IP アドレスの重複をチェックするか否かの設定	77
9.7	DHCP サーバの指定の設定	77
9.8	DHCP サーバの選択方法の設定	77
9.9	DHCP BOOTREQUEST パケットの中継基準の設定	77
10.	ICMP の設定	78
10.1	ICMP Echo Reply を送信するか否かの設定	78
10.2	ICMP Mask Reply を送信するか否かの設定	78
10.3	ICMP Parameter Problem を送信するか否かの設定	78
10.4	ICMP Redirect を送信するか否かの設定	78
10.5	ICMP Redirect 受信時の処理の設定	78
10.6	ICMP Time Exceeded を送信するか否かの設定	79
10.7	ICMP Timestamp Reply を送信するか否かの設定	79
10.8	ICMP Destination Unreachable を送信するか否かの設定	79
10.9	受信した ICMP のログを記録するか否かの設定	79
11.	フレームリレー関連の設定	80
11.1	カプセル化の種類の設定	80

11.2	DLCIの設定	81
11.3	PVC 状態確認手順の設定	81
11.4	InARP 使用の設定	81
11.5	フレームリレーダウン時にバックアップする相手先情報番号の設定	81
11.6	FR 圧縮機能の設定	82
11.7	DLCI ごとのパラメータの設定	82
11.8	輻輳制御をするか否かの設定	82
11.9	回線に対する送信順序方式の設定	83
11.10	指定パケットに DE ビットを立てるか否かの設定	83
12.	PRI 関連の設定	84
12.1	PRI 回線の種類の設定	84
12.2	情報チャンネルとタイムスロットの設定	84
12.3	PP で使用するインタフェースの設定	85
13.	IPsec の設定	86
13.1	事前共有鍵の登録	86
13.2	相手側セキュリティ・ゲートウェイの IP アドレスの設定	87
13.3	相手側のセキュリティゲートウェイの名前の設定	87
13.4	自分側セキュリティ・ゲートウェイの IP アドレスの設定	87
13.5	自分側のセキュリティゲートウェイの名前の設定	87
13.6	鍵交換の再回数と間隔の設定	87
13.7	IKE が用いる暗号アルゴリズムの設定	88
13.8	IKE が用いるグループの設定	88
13.9	IKE が用いるハッシュアルゴリズムの設定	88
13.10	自分側の ID の設定	88
13.11	IKE のログの種類の設定	89
13.12	IKE ペイロードのタイプの設定	89
13.13	PFS を用いるか否かの設定	89
13.14	相手側の ID の設定	89
13.15	IKE の情報ペイロードを送信するか否かの設定	90
13.16	SA 関連の設定	90
13.16.1	IPsec SA の寿命の設定	90
13.16.2	ISAKMP SA の寿命の設定	90
13.16.3	SA の削除	91
13.16.4	SA の手動更新	91
13.16.5	SA を自動更新するか否かの設定	91
13.17	トンネルインタフェース関連の設定	91
13.17.1	使用する SA のポリシーの設定	91
13.17.2	IPComp によるデータ圧縮の設定	92
13.17.3	トンネルインタフェースの使用許可の設定	92
13.17.4	トンネルインタフェースの使用不許可の設定	92
13.17.5	トンネルインタフェース番号の選択	92
13.18	トランスポートモード関連の設定	93
14.	SNMP の設定	94
14.1	読み出し専用のコミュニティ名の設定	94
14.2	読み書き可能なコミュニティ名の設定	94
14.3	認証失敗時 (authenticationFailure) にトラップを送信するか否かの設定	94
14.4	SNMP によるアクセスを許可するホストの設定	94
14.5	sysContact の設定	94
14.6	sysLocation の設定	95
14.7	sysName の設定	95
14.8	SNMP トラップのコミュニティ名の設定	95
14.9	SNMP トラップの送信先の設定	95
14.10	PP インタフェースの情報を MIB2 の範囲で表示するか否かの設定	95
14.11	PP インタフェースのアドレスの強制表示の設定	96
15.	RADIUS の設定	97
15.1	RADIUS による認証を使用するか否かの設定	97
15.2	RADIUS によるアカウントを使用するか否かの設定	97

15.3	RADIUS サーバの指定	97
15.4	RADIUS 認証サーバの指定	97
15.5	RADIUS アカウントサーバの指定	98
15.6	RADIUS 認証サーバの UDP ポートの設定	98
15.7	RADIUS アカウントサーバの UDP ポートの設定	98
15.8	RADIUS シークレットの設定	98
15.9	RADIUS 再送信パラメータの設定	98
16.	NAT 機能	99
16.1	インタフェースへの NAT ディスクリプタ適用の設定	99
16.2	NAT ディスクリプタの動作タイプの設定	99
16.3	NAT 処理の外側 IP アドレスの設定	100
16.4	NAT 処理の内側 IP アドレスの設定	100
16.5	静的 NAT エントリの設定	100
16.6	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	101
16.7	静的 IP マスカレードエントリの設定	101
16.8	NAT の IP アドレスマップの消去タイマの設定	101
16.9	IP マスカレードテーブルの TTL 処理方式の設定	101
16.10	NAT のアドレス割当をログに記録するか否かの設定	102
17.	DNS の設定	103
17.1	DNS サーバの IP アドレスの設定	103
17.2	DNS サーバを通知してもらう相手先情報番号の設定	103
17.3	DNS 問い合わせの内容に応じた DNS サーバの選択	104
17.4	DNS ドメイン名の設定	104
17.5	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	104
17.6	DHCP/IPCP MS 拡張で DNS サーバを通知する順序の設定	105
17.7	SYSLOG 表示で DNS により名前解決するか否かの設定	105
17.8	静的 DNS レコードの登録	105
18.	優先制御 / 帯域制御	106
18.1	インタフェース速度の設定	106
18.2	クラス分けのためのフィルタ設定	106
18.3	キューイングアルゴリズムタイプの選択	109
18.4	デフォルトクラスの設定	109
18.5	クラス分けフィルタの適用	109
18.6	クラスの属性の設定	110
18.7	クラス毎のキュー長の設定	110
18.8	MP インタリーブの設定	111
19.	OSPF	112
19.1	OSPF の有効設定	112
19.2	OSPF の使用設定	112
19.3	OSPF による経路の優先度設定	112
19.4	OSPF のルータ ID 設定	112
19.5	外部プロトコルによる経路導入	113
19.6	外部経路導入に適用するフィルタ定義	113
19.7	OSPF エリア設定	114
19.8	エリアへの経路広告	114
19.9	スタブ的接続の広告	114
19.10	仮想リンク設定	115
19.11	指定インタフェースの OSPF エリア設定	116
19.12	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	117
20.	IPv6	118
20.1	IPv6 アドレスの管理	118
20.1.1	インタフェースの IPv6 アドレスの設定	118
20.1.2	インタフェースに付与されている IPv6 アドレスの表示	118
20.2	近隣探索	119
20.2.1	ルータ広告で配布するプレフィックスの定義	119
20.2.2	ルータ広告の送信の制御	119
20.3	経路制御	120
20.3.1	IPv6 の経路情報の追加	120



20.4	RIPng の設定	120
20.4.1	インタフェースにおける RIPng の送信ポリシーの設定	120
20.4.2	インタフェースにおける RIPng の受信ポリシーの設定	121
20.4.3	インタフェースにおける信頼できる RIPng ゲートウェイの設定	121
20.4.4	RIPng の加算ホップ数の設定	121
20.4.5	RIPng で送受信する経路に対するフィルタリングの設定	121
20.4.6	回線接続時の PP 側の RIPng の動作の設定	121
20.4.7	回線接続時の PP 側の RIPng 送出の時間間隔の設定	122
20.4.8	回線切断時の PP 側の RIPng の動作の設定	122
20.4.9	回線切断時の PP 側の RIPng 送出の時間間隔の設定	122
20.4.10	RIPng による経路を回線切断時に保持するか否かの設定	122
20.5	フィルタの設定	122
20.5.1	IPv6 フィルタの定義	122
20.5.2	IPv6 フィルタの削除	123
20.5.3	IPv6 フィルタの適用	123
20.6	トンネルリング	123
20.6.1	トンネルインタフェースの種類の設定	123
20.6.2	トンネルインタフェースの自分側の IPv4 アドレスの設定	123
20.6.3	トンネルインタフェースの相手側の IPv4 アドレスの設定	123
20.6.4	トンネルインタフェースの相手側の IPv6 アドレスの設定	124
20.7	管理ツール	124
20.7.1	ping の実行	124
20.7.2	traceroute の実行	124
21.	スケジュール	125
21.1	スケジュールの設定	125
22.	操作	126
22.1	相手先情報番号の選択	126
22.2	設定に関する操作	126
22.2.1	終了	126
22.2.2	設定内容の保存	126
22.2.3	設定ファイルの削除	126
22.2.4	実行形式ファームウェアファイルの削除	127
22.2.5	設定ファイルの一覧	127
22.2.6	設定の初期化	127
22.2.7	遠隔地のルータの設定	127
22.2.8	遠隔地のルータからの設定に対する制限	127
22.3	動的情報のクリア操作	128
22.3.1	IP の動的経路情報のクリア	128
22.3.2	IPX の動的経路情報のクリア	128
22.3.3	IPX の動的 SAP 情報のクリア	128
22.3.4	ブリッジのラーニング情報のクリア	128
22.3.5	ログのクリア	128
22.3.6	アカウントのクリア	128
22.3.7	InARP のクリア	129
22.3.8	DNS キャッシュのクリア	129
22.3.9	PRI のステータス情報のクリア	129
22.3.10	NAT アドレステーブルのクリア	129
22.3.11	インタフェースの NAT アドレステーブルのクリア	129
22.3.12	IPv6 の動的経路情報の消去	129
22.3.13	近隣キャッシュの消去	129
22.4	その他の操作	130
22.4.1	相手先の使用不許可の設定	130
22.4.2	再起動	130
22.4.3	インタフェースの再起動	130
22.4.4	PP インタフェースの再起動	130
22.4.5	発信	131
22.4.6	切断	131
22.4.7	ping	131
22.4.8	traceroute	131

22.4.9	telnet	132
22.4.10	telnet サーバ機能の ON/OFF の設定	132
22.4.11	telnet サーバ機能の listen ポートの設定	132
22.4.12	telnet サーバへアクセスできるホストの IP アドレスの設定	133
22.4.13	PRI のループバックの実行	133
22.4.14	PRI のループバック待ち受けの設定	134
22.4.15	ファームウェアファイルを内蔵フラッシュ ROM にコピー	134
23.	設定の表示	135
23.1	機器設定の表示	135
23.2	すべての設定内容の表示	135
23.3	指定した PP の設定内容の表示	135
23.4	PC カードの内容の表示	135
23.5	マスタクロックを得ている回線の表示	135
24.	状態の表示	136
24.1	ARP テーブルの表示	136
24.2	インタフェースの状態の表示	136
24.3	各相手先の状態の表示	136
24.4	DHCP サーバの状態の表示	136
24.5	IP の経路情報テーブルの表示	137
24.6	IPX の経路情報テーブルの表示	137
24.7	IPv6 の経路情報の表示	137
24.8	近隣キャッシュの表示	137
24.9	SAP テーブルの表示	137
24.10	IPXWAN の状態の表示	137
24.11	ブリッジのラーニング情報の表示	137
24.12	RIP で得られた経路情報の表示	138
24.13	IPsec の SA の表示	138
24.14	VRRP の情報の表示	138
24.15	動的 NAT ディスクリプタのアドレスマップの表示	138
24.16	動作中の NAT ディスクリプタの適用リストの表示	138
24.17	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	138
24.18	OSPF 情報の表示	138
25.	ログイン	139
25.1	ログの表示	139
25.2	アカウントの表示	139

# コマンド索引

## A

account threshold	25
account threshold pp	25
administrator	126
administrator password	18

## B

bridge filter	55
bridge group	54
bridge interface filter	56
bridge interface learning	56
bridge learning	55
bridge learning expire	55
bridge pp filter	56
bridge pp learning	56
bridge use	54

## C

clear account	128
clear account pp	128
clear arp	128
clear bridge learning	128
clear dns cache	129
clear inarp	129
clear ip dynamic routing	128
clear ipv6 dynamic routing	129
clear ipv6 neighbor cache	129
clear ipx dynamic routing	128
clear ipx dynamic sap	128
clear log	128
clear nat descriptor dynamic	129
clear nat descriptor interface dynamic	129
clear pri status	129
cold start	127
connect	131
console character	20
console columns	20
console info	20
console lines	20
console prompt	21
copy exec	134

## D

date	19
delete config	126
delete exec	127
dhcp duplicate check	77
dhcp relay select	77
dhcp relay server	77
dhcp relay threshold	77
dhcp scope	74
dhcp scope bind	75
dhcp scope option	76
dhcp server rfc2131 compliant	73
dhcp service	72
disconnect	131
dns domain	104
dns notice order	105
dns private address spoof	104
dns server ip_address	103
dns server pp	103
dns server select	104
dns static	105
dns syslog resolv	105

## E

exit	126
------	-----

## F

fr backup	81
fr cir	82
fr compression use	82
fr congestion control	82
fr de	83
fr dlci	81
fr inarp	81
fr lmi	81
fr pp dequeue type	83

## H

help	17
------	----

## I

interface reset	130
interface reset pp	130
ip filter	35
ip filter directed-broadcast	37
ip filter dynamic	37
ip filter dynamic timer	38
ip filter set	36
ip filter source-route	36
ip host	105
ip icmp echo-reply send	78
ip icmp log	79
ip icmp mask-reply send	78
ip icmp parameter-problem send	78
ip icmp redirect receive	78
ip icmp redirect send	78
ip icmp time-exceeded send	79
ip icmp timestamp-reply send	79
ip icmp unreachable send	79
ip interface address	33
ip interface intrusion detection	38
ip interface mtu	40
ip interface nat descriptor	99
ip interface ospf area	116
ip interface ospf neighbor	117
ip interface proxyarp	40
ip interface rip auth key	43
ip interface rip auth text	43
ip interface rip auth type	43
ip interface rip filter	42
ip interface rip hop	42
ip interface rip receive	42
ip interface rip send	41
ip interface rip trust gateway	42
ip interface secondary address	33
ip interface secure filter	39
ip interface vrrp	44
ip pp remote address	40
ip pp remote address pool	41
ip pp rip connect interval	43
ip pp rip connect send	43
ip pp rip disconnect interval	44
ip pp rip disconnect send	44
ip pp rip hold routing	43
ip route	34
ip routing	33
ip simple service	22

ip tos supersede	39	ipx routing	46
ip tunnel local address	123	ipx sap response	48
ip tunnel remote address	123	isdn arrive permit	28
ipsec auto refresh	91	isdn auto connect	28
ipsec ike duration ipsec-sa	90	isdn auto disconnect	28
ipsec ike duration isakmp-sa	90	isdn call block time	29
ipsec ike encryption	88	isdn call permit	29
ipsec ike group	88	isdn call prohibit time	29
ipsec ike hash	88	isdn callback mscbcu user-specify	30
ipsec ike local address	87	isdn callback permit	30
ipsec ike local id	88	isdn callback permit type	30
ipsec ike local name	87	isdn callback request	29
ipsec ike log	89	isdn callback request type	29
ipsec ike payload type	89	isdn callback response time	30
ipsec ike pfs	89	isdn callback wait time	30
ipsec ike pre-shared-key	86	isdn disconnect input time	31
ipsec ike remote address	87	isdn disconnect interval time	32
ipsec ike remote id	89	isdn disconnect output time	31
ipsec ike remote name	87	isdn disconnect policy	31
ipsec ike retry	87	isdn disconnect time	31
ipsec ike send info	90	isdn fast disconnect time	32
ipsec ipcomp type	92	isdn forced disconnect time	32
ipsec refresh sa	91	isdn local address	24
ipsec sa delete	91	isdn piafs arrive	26
ipsec sa policy	90	isdn piafs call	25
ipsec transport	93	isdn piafs control	26
ipsec tunnel	91	isdn remote address	27
ipv6 filter	122	isdn remote call order	28
ipv6 filter delete	123	isdn terminator	27
ipv6 interface address	118		
ipv6 interface rip filter	121	<b>L</b>	
ipv6 interface rip receive	121	leased backup	26
ipv6 interface rip send	120	leased backup recovery time	26
ipv6 interface rip trust gateway	121	leased keepalive down	61
ipv6 interface rtadv send	119	leased keepalive interval	61
ipv6 interface secure filter	123	leased keepalive log	61
ipv6 pp rip connect interval	122	leased keepalive use	60
ipv6 pp rip connect send	121	less config	135
ipv6 pp rip disconnect send	122	less config pp	135
ipv6 pp rip hold routing	122	less file list	135
ipv6 pp rip hop	121	less log	139
ipv6 prefix	119	line masterclock	23
ipv6 rip use	120	line type	24, 84
ipv6 route	120	login password	18
ipv6 tunnel remote address	124	login timer	18
ipx filter	47		
ipx interface frame type	48	<b>N</b>	
ipx interface network	49	nat descriptor address inner	100
ipx interface ripsap broadcast	49	nat descriptor address outer	100
ipx interface route	49	nat descriptor log	102
ipx interface secure filter	49	nat descriptor masquerade rlogin	101
ipx pp ipxwan primnet	52	nat descriptor masquerade static	101
ipx pp ipxwan retry	52	nat descriptor masquerade ttl hold	101
ipx pp ipxwan use	51	nat descriptor static	100
ipx pp network	50	nat descriptor timer	101
ipx pp ripsap connect interval	51	nat descriptor type	99
ipx pp ripsap connect send	50	ntpdate	19
ipx pp ripsap disconnect interval	51		
ipx pp ripsap disconnect send	51	<b>O</b>	
ipx pp ripsap hold	51	ospf area	114
ipx pp route	50	ospf area network	114
ipx pp routing	50	ospf area stubhost	114
ipx pp secure filter	53	ospf configure refresh	112
ipx pp serialization filter	53	ospf import filter	113
ipx pp spx keepalive proxy	52	ospf import from	113
ipx pp spx keepalive timer	53	ospf preference	112
ipx pp watchdog interval	52	ospf router id	112
ipx pp watchdog proxy	52		

ospf use	112	pppoe access concentrator	70
ospf virtual-link	115	pppoe auto connect	70
<b>P</b>			
ping	131	pppoe auto disconnect	70
ping6	124	pppoe disconnect time	71
pp auth accept	58	pppoe padi maxretry	70
pp auth multi connect prohibit	58	pppoe padi restart	70
pp auth myname	58	pppoe padr maxretry	70
pp auth request	57	pppoe padr restart	71
pp auth username	57	pppoe tcp mss limit	71
pp bind	27, 85	pppoe use	69
pp disable	130	pri leased channel	84
pp enable	130	pri loopback active	133
pp encapsulation	80	pri loopback passive	134
pp select	126	pri loopback passive off	134
ppp bacp maxconfigure	69	<b>Q</b>	
ppp bacp maxfailure	69	queue class filter	106
ppp bacp maxterminate	69	queue interface class filter list	109
ppp bacp restart	68	queue interface class property	110
ppp bap maxretry	69	queue interface default	109
ppp bap restart	69	queue interface length	110
ppp bcp lanid	64	queue interface type	109
ppp bcp maxconfigure	65	quit	126
ppp bcp maxfailure	65	<b>R</b>	
ppp bcp maxterminate	65	radius account	97
ppp bcp restart	65	radius account port	98
ppp bcp tinycomp	65	radius account server	98
ppp ccp maxconfigure	66	radius auth port	98
ppp ccp maxfailure	67	radius auth server	97
ppp ccp maxterminate	66	radius retry	98
ppp ccp restart	66	radius secret	98
ppp ccp type	66	radius server	97
ppp chap maxchallenge	62	rdate	19
ppp chap restart	62	remote setup accept	127
ppp ipcp ipaddress	62	remote setup interface	127
ppp ipcp maxconfigure	63	restart	130
ppp ipcp maxfailure	63	rip preference	41
ppp ipcp maxterminate	63	rip use	41
ppp ipcp msex	63	<b>S</b>	
ppp ipcp restart	62	save	126
ppp ipcp vjc	62	schedule at	125
ppp ipxcp maxconfigure	64	security class	18
ppp ipxcp maxfailure	64	show account	139
ppp ipxcp maxterminate	64	show account pp	139
ppp ipxcp restart	64	show arp	136
ppp lcp acfc	58	show bridge learning	137
ppp lcp magicnumber	59	show command	17
ppp lcp maxconfigure	60	show config	135
ppp lcp maxfailure	60	show config list	127
ppp lcp maxterminate	60	show config pp	135
ppp lcp mru	59	show environment	135
ppp lcp pfc	59	show file list	135
ppp lcp restart	59	show ip rip table	138
ppp lcp silent	60	show ip route	137
ppp mp control	67	show ipsec sa	138
ppp mp divide	68	show ipv6 neighbor cache	137
ppp mp interleave	111	show ipv6 route	137
ppp mp load threshold	67	show ipx ipxwan	137
ppp mp maxlink	68	show ipx route	137
ppp mp minlink	68	show ipx sap	137
ppp mp timer	68	show line masterclock	135
ppp mp use	67	show log	139
ppp msbcpc maxretry	66	show nat descriptor address	138
ppp msbcpc restart	65	show nat descriptor interface address	138
ppp pap maxauthreq	61		
ppp pap restart	61		

show nat descriptor interface bind . . . . .	138
show status . . . . .	136
show status dhcp . . . . .	136
show status ospf . . . . .	138
show status pp . . . . .	136
show status vrrp . . . . .	138
snmp community read-only . . . . .	94
snmp community read-write . . . . .	94
snmp display ipcp force . . . . .	96
snmp enableauthentraps . . . . .	94
snmp host . . . . .	94
snmp syscontact . . . . .	94
snmp syslocation . . . . .	95
snmp sysname . . . . .	95
snmp trap community . . . . .	95
snmp trap host . . . . .	95
snmp yrifppdisplayatmib2 . . . . .	95
speed interface . . . . .	106
syslog debug . . . . .	22
syslog facility . . . . .	21
syslog host . . . . .	21
syslog info . . . . .	21
syslog notice . . . . .	21
syslog srcport . . . . .	22
system power 2 use . . . . .	23
system temperature threshold . . . . .	23

## T

telnet . . . . .	132
telnetd host . . . . .	133
telnetd listen . . . . .	132
telnetd service . . . . .	132
tftp host . . . . .	22
time . . . . .	19
timezone . . . . .	19
traceroute . . . . .	131
traceroute6 . . . . .	124
tunnel disable . . . . .	92
tunnel enable . . . . .	92
tunnel encapsulation . . . . .	123
tunnel select . . . . .	92

## W

wins server . . . . .	63
-----------------------	----

## 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 リモートルータのファームウェア、Rev.6.02.02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。

### 1.3 インタフェース名について

コマンドの入力形式において、ルータの各インタフェースを指定するためにインタフェース名を利用します。

インタフェース名は、インタフェース種別とインタフェース番号を間に空白をおかずに続けて表記します。インタフェース種別には、"lan"、"bri"、"pri" があります。インタフェース番号は、インタフェースの種別ごとに起動時に検出された順番で振られていきます。

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

例：

メインモジュール上の LAN	lan1
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 で始まる形のもので並記されているコマンドが多数あります。no で始まる形式を使うと、特別な記述がない限り、そのコマンドの設定を削除し、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。



## 2. ヘルプ

### 2.1 コンソールに対する簡易説明の表示

---

- [入力形式] help
- [パラメータ] なし
- [説明] コンソールの使用方法の簡単な説明を表示する。

### 2.2 コマンド一覧の表示

---

- [入力形式] show command
- [パラメータ] なし
- [説明] コマンドの名称とその簡単な説明を一覧表示する。

### 3. 機器の設定

#### 3.1 ログインパスワードの設定

---

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

#### 3.2 管理パスワードの設定

---

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

#### 3.3 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 ]	<i>level</i> 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> 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> 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。
[ デフォルト値 ]	<i>level</i> = 1 <i>forget</i> = on <i>telnet</i> = off

#### 3.4 ログインタイムの設定

---

[ 入力形式 ]	login timer <i>time</i> no login timer [ <i>time</i> ]
[ パラメータ ]	<i>time</i> 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 ..... ログインタイムを設定しない
[ 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ム値は 300 秒として扱う。
[ デフォルト値 ]	300

### 3.5 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  
                             日本標準時 (+09:00)  
                             世界標準時 (+00:00)
- [説明]            タイムゾーンを設定する。
- [デフォルト値]   `jst`

### 3.6 現在の日付けの設定

---

- [入力形式]      `date date`
- [パラメータ]      `date.....` `yyyy-mm-dd` または `yyyy/mm/dd`
- [説明]            現在の日付けを設定する。

### 3.7 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。

### 3.8 リモートホストによる時計の設定

---

- [入力形式]      `rdate host [syslog]`
- [パラメータ]      `host`  
                             リモートホストの IP アドレス (`xxx.xxx.xxx.xxx` (`xxx` は 10 進数))  
                             ホストの名称  
                             `syslog`..... 出力結果を SYSLOG へ出力することを表すキーワード
- [説明]            ルータの時計を、パラメータで指定したホストの時間に合わせる。  
                             このコマンドが実行されるとホストの TCP の 37 番ポートに接続する。
- [ノート]          YAMAHA リモート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。

### 3.9 NTP による時計の設定

---

- [入力形式]      `ntpdate ntp_server [syslog]`
- [パラメータ]      `ntp_server`  
                             NTP サーバの IP アドレス (`xxx.xxx.xxx.xxx` (`xxx` は 10 進数))  
                             NTP サーバの名称  
                             `syslog`..... 出力結果を SYSLOG へ出力することを表すキーワード
- [説明]            NTP を利用してルータの時計を設定する。このコマンドが実行されるとホストの UDP の 123 番ポートに接続する。
- [ノート]          インターネットに接続している場合には、`rdate` コマンドを使用した場合よりも精密な計合わせが可能になる。  
                             NTP サーバとして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。  
                             本機自身は NTP サーバとはなれない。  
                             `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。

## 3.10 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> ascii ..... 英語で表示する、文字コードはシフト ASCII euc ..... 日本語で表示する、文字コードはシフト EUC sjis ..... 日本語で表示する、文字コードはシフト JIS
[ 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。
[ デフォルト値 ]	sjis
[ 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。

## 3.11 コンソールの表示文字数の設定

---

[ 入力形式 ]	console columns <i>col</i> no console columns [ <i>col</i> ]
[ パラメータ ]	<i>col</i> ..... コンソールの表示文字数 (80..200)
[ 説明 ]	コンソールの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。
[ デフォルト値 ]	80
[ 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。

## 3.12 コンソールの表示行数の設定

---

[ 入力形式 ]	console lines <i>lines</i> no console lines [ <i>lines</i> ]
[ パラメータ ]	<i>lines</i> 10 ..... 100 の整数 infinity ..... スクロールを止めない
[ 説明 ]	コンソールの表示行数を設定する。 このコマンドは一般ユーザでも実行できる。
[ デフォルト値 ]	24
[ 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。

## 3.13 コンソールにシステムメッセージを表示するか否かの設定

---

[ 入力形式 ]	console info <i>info</i> no console info <i>info</i>
[ パラメータ ]	<i>info</i> 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

### 3.14 コンソールのプロンプト表示の設定

---

- [入力形式] console prompt *prompt*  
no console prompt [*prompt*]
- [パラメータ] *prompt*..... コンソールのプロンプトの先頭文字列 (16 文字以内)
- [説明] コンソールのプロンプト表示を設定する。空文字列も設定できる。
- [デフォルト値] 空文字列

### 3.15 SYSLOG を受けるホストの IP アドレスの設定

---

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

### 3.16 SYSLOG ファシリティの設定

---

- [入力形式] syslog facility *facility*  
no syslog facility [*facility*]
- [パラメータ] *facility*  
0..23  
user.....1  
local0..local7 .....16..27
- [説明] SYSLOG のファシリティを設定する。
- [デフォルト値] user

### 3.17 NOTICE タイプの SYSLOG を出力するか否かの設定

---

- [入力形式] syslog notice *notice*  
no syslog notice [*notice*]
- [パラメータ] *notice*  
on ..... 出力する  
off ..... 出力しない
- [説明] IP フィルタ、IPX フィルタ、ブリッジフィルタで落したパケット情報等を SYSLOG で出力するか否か設定する。
- [デフォルト値] off

### 3.18 INFO タイプの SYSLOG を出力するか否かの設定

---

- [入力形式] syslog info *info*  
no syslog info [*info*]
- [パラメータ] *info*  
on ..... 出力する  
off ..... 出力しない
- [説明] ISDN の呼制御情報等を SYSLOG で出力するか否か設定する。
- [デフォルト値] on

## 3.19 DEBUG タイプの SYSLOG を出力するか否かの設定

---

[ 入力形式 ]	syslog debug <i>debug</i> no syslog debug [ <i>debug</i> ]
[ パラメータ ]	<i>debug</i> 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 で出力するか否かが設定する。
[ 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 に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

## 3.20 TFTP によりアクセスできるホストの IP アドレスの設定

---

[ 入力形式 ]	tftp host host no tftp host [ <i>host</i> ]
[ パラメータ ]	<i>host</i> IP アドレス..... TFTP によりアクセスできるホストの IP アドレス (IPv6 アドレス可) any.....すべてのホストから TFTP によりアクセスできる none.....すべてのホストから TFTP によりアクセスできない
[ 説明 ]	TFTP によりアクセスできるホストの IP アドレスを設定する。
[ ノート ]	セキュリティの観点から、プログラムのリビジョンアップや設定ファイルの読み書きが終了したらすぐに none にする。
[ デフォルト値 ]	none

## 3.21 LAN インタフェースの速度タイプの設定

---

[ 入力形式 ]	lan type <i>interface type</i>
[ パラメータ ]	<i>interface</i> .....LAN インタフェース名 <i>type</i> auto.....速度自動設定 100-fdx.....100BASE-TX 全二重 100-hdx.....100BASE-TX 半二重 10-fdx.....10BASE-T 全二重 10-hdx.....10BASE-T 半二重
[ 説明 ]	指定した LAN インタフェースの種類を設定する。
[ デフォルト値 ]	auto

## 3.22 TCP/UDP の各種サービスの動作の設定

---

[ 入力形式 ]	ip simple-service <i>switch</i>
[ パラメータ ]	<i>switch</i> .....TCP/UDP の各種サービス on.....動作させる off.....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どうかを設定する。
[ デフォルト値 ]	on

## 3.23 SYSLOG パケットの始点ポート番号の設定

---

[ 入力形式 ]	syslog srcport <i>port</i> no syslog srcport [ <i>port</i> ]
[ パラメータ ]	<i>port</i> .....ポート番号 (1..65535)
[ 説明 ]	本機が送信する SYSLOG パケットの始点ポート番号を設定する。
[ デフォルト値 ]	514

### 3.24 マスタクロック用インタフェースの設定

[入力形式]	line masterclock <i>auto</i> line masterclock <i>interface</i> no line masterclock
[パラメータ]	<i>auto</i> ..... 自動選択 <i>interface</i> ..... インタフェース名
[説明]	RT300i 専用のコマンド。 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。 <i>auto</i> を設定した場合は、実際に回線が接続されている BRI/PRI インタフェースの中からマスタクロックを供給するインタフェースを自動的に選択する。選択基準は、BRI よりも PRI を優先し、同じ回線種別の中ではより若番のポート番号を持つインタフェースを優先する。マスタとなるインタフェースの回線がダウンしてクロックを得られなくなった場合には、同じモジュール内のインタフェースを優先して、次のマスタクロック供給インタフェースを選択する。すべての回線がダウンしている場合には内部クロックを用いたフリーラン状態となる。 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。
[デフォルト値]	<i>auto</i>
[ノート]	すべての BRI/PRI はマスタクロックに同期するので、それらに接続されている回線もお互いに同期している必要がある。日本国内の通信事業者が提供する実回線は、すべて NTT を基準として同期しているはずなので、その点では問題はない。一部の BRI/PRI に、構内網など独自に構築した回線や、疑似交換機などを接続する場合には、マスタクロックと同期していない回線ではクロックシフトによるビットエラーが発生する可能性があることに注意しなくてはならない。

### 3.25 電源 2 の設定

[入力形式]	system power 2 use <i>sw</i> no system power 2 use [ <i>sw</i> ]
[パラメータ]	<i>sw</i> ..... 電源 2 の装着状態 <i>on</i> ..... 電源 2 を装着している <i>off</i> ..... 電源 2 を装着していない
[説明]	RT300i 専用のコマンド。 電源 2 を装着状態を設定する。電源 2 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 2 の監視機能が正しく働くようになる。
[ノート]	電源 2 を装着していないにも関わらず、 <i>sw</i> を <i>on</i> に設定すると、監視機能が働き電源 2 の異常を報告する。
[デフォルト値]	<i>off</i>

### 3.26 温度監視の閾値の設定

[入力形式]	system temperature threshold <i>t1 t2</i> no system temperature threshold <i>t1 t2</i>
[パラメータ]	<i>t1</i> ..... 警告を発する温度 ( ) <i>t2</i> ..... 警告を解除する温度 ( )
[説明]	RT300i 専用のコマンド。 本体内部の温度を監視して、 <i>t1</i> 以上の温度になると SYSLOG や ALM ランプで警告を発する。一度、警告が発せられると、温度が <i>t2</i> を下回らない限り、ALM ランプは消えない。
[デフォルト値]	<i>t1</i> = 80 <i>t2</i> = 75

## 4. ISDN 関連の設定

### 4.1 自分側の設定

#### 4.1.1 BRI 回線の種類の指定

---

[ 入力形式 ]	line type <i>interface line</i> [ <i>channels</i> ] no line type <i>interface line</i> [ <i>channels</i> ]
[ パラメータ ]	<i>interface</i> .....BRI インタフェース名 <i>line</i> <i>isdn, isdn-ntt</i> .....ISDN 回線交換 <i>l64</i> ..... デジタル専用線、64kbit/s <i>l128</i> ..... デジタル専用線、128kbit/s <i>channels</i> ..... <i>type</i> パラメータが <i>isdn</i> 、 <i>isdn-ntt</i> の場合のみ指定可 <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。
[ デフォルト値 ]	<i>line</i> = <i>isdn</i> <i>channels</i> = <i>2b</i>
[ 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。

#### 4.1.2 自分の ISDN 番号の設定

---

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



## 4.1.3 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>yen</i> ] no account threshold <i>interface</i> [ <i>yen</i> ] no account threshold pp [ <i>yen</i> ]
[パラメータ]	<i>interface</i> ..... BRI/PRI インタフェース名 <i>yen</i> 課金額 ..... 円 (10..21474836) off ..... 発信制限機能を使わない
[説明]	網から通知される課金の合計 (これは show account コマンドで表示される) の累計が指定した金額に達したらそれ以上の発信を行わないようにする。 account threshold コマンドではルータ全体の合計金額を設定し、 <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。 課金が網から通知されるのは通信切断時なので、長時間の接続の途中切断することはできず、この場合は制限はできない。この場合に対処するには、isdn forced disconnect time コマンドで通信中でも時間を監視して強制的に回線を切るような設定しておく方法がある。また、課金合計は clear account コマンドで 0 にリセットでき、schedule at コマンドで定期的に clear account を実行するようにしておく、毎月一定額以内に課金を抑えるといったことが自動で可能になる。
[ノート]	電源 OFF や再起動により、それまでの課金情報がクリアされることに注意。課金額は通信の切断時に NTT から ISDN で通知される料金情報に基づくため、割引サービスなどを利用している場合には、最終的に NTT から請求される料金とは異なる場合がある。また、NTT 以外の通信事業者を利用して通信した場合には料金情報は通知されない。
[デフォルト値]	off

## 4.1.4 PIAFS の発信方式の設定

[入力形式]	isdn piafs call <i>speed</i> [ <i>64kmode</i> ] no isdn piafs call [ <i>speed</i> [ <i>64kmode</i> ]]
[パラメータ]	<i>speed</i> 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> guarantee ..... PIAFS 64k の発信ではギャランティー方式を使用する best-effort ..... PIAFS 64k の発信ではベストエフォート方式を使用する
[説明]	PIAFS モードの発信を可能にするか否かを設定する。 また、PIAFS モードの速度を選択する。 <i>switch</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 になる。 また、64k に設定されている場合には、発信は PIAFS 64k になる。 <i>switch</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。 <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。 <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。
[デフォルト値]	off
[ノート]	PIAFS 64k では特別なサブアドレスが用いられ、ユーザが設定した発サブアドレスは無視される。

4.1.5 PIAFS の着信を許可するか否かの設定

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

4.1.6 PIAFS 接続時の起動側の指定

- [ 入力形式 ]     isdn piafs control *switch*
- [ パラメータ ]     *switch*  
                    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。
- [ 設定例 ]         # pp select *number*  
                    # isdn piafs control call  
                    # pp enable *number*  
                    ( *number* は相手先情報番号 )
- [ ノート ]         本コマンドの設定と、発信 / 着信の組み合わせにより、起動側となるか被起動側となるかが以下のように決定される。

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

- [ デフォルト値 ]  call

4.1.7 専用線がダウンした時にバックアップする相手先情報番号の設定

- [ 入力形式 ]     leased backup *peer\_num*  
                  no leased backup [*peer\_num*]
- [ パラメータ ]     *peer\_num*  
                    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

4.1.8 バックアップからの復帰待ち時間の設定

- [ 入力形式 ]     leased backup recovery time *time*  
                  no leased backup recovery time [*time*]
- [ パラメータ ]     *time*  
                    秒数 (1..21474836)  
                    off.....すぐに復帰
- [ 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。  
                    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

#### 4.1.9 終端抵抗の設定

---

[入力形式]	isdn terminator <i>interface terminator</i> no isdn terminator <i>interface [terminator]</i>
[パラメータ]	<i>interface</i> ..... BRI インタフェース名 <i>terminator</i> on ..... 終端抵抗を ON にする off ..... 終端抵抗を OFF にする
[説明]	RT300i 専用のコマンド。指定した BRI インタフェースの終端抵抗を ON または OFF にする。
[ノート]	DSU に直結する場合には必ず on にする。 バス配線されている場合、バスの終端でなければ off にする。
[デフォルト値]	off

#### 4.1.10 PP で使用するインタフェースの設定

---

[入力形式]	pp bind <i>interface [interface]</i> no pp bind [ <i>interface</i> ]
[パラメータ]	<i>interface</i> ..... BRI/PRI インタフェース名
[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

### 4.2 相手側の設定

#### 4.2.1 相手 ISDN 番号の設定

---

[入力形式]	isdn remote address <i>call_arrive isdn_num[/sub_address][isdn_num_list]</i> isdn remote address <i>call_arrive isdn_num [isdn_num_list]</i> no isdn remote address <i>call_arrive [isdn_num[/sub_address]][isdn_num_list]</i>
[パラメータ]	<i>call_arrive</i> call ..... 発着信用 arrive ..... 着信専用 <i>isdn_num</i> ..... ISDN 番号 <i>sub_addres</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を空白で区切った並び
[説明]	選択されている相手の ISDN 番号とサブアドレスを設定する。ISDN 番号には市外局番も含めて設定する。 選択されている相手が anonymous または leased の場合は無意味である。 複数の ISDN 番号が設定されている場合、まず先頭の ISDN 番号での接続に失敗すると次に指定された ISDN 番号が使われる。同様に、それに失敗すると次の ISDN 番号を使うという動作を続ける。 MP のように相手先に対して複数チャンネルで接続しようとする際に発信する順番は、isdn remote call order コマンドで設定する。

## 4.2.2 相手への発信順序の設定

- [ 入力形式 ]      isdn remote call order *order*  
no isdn remote call order [*order*]
- [ パラメータ ]      *order*  
                    round .....ラウンドロビン方式  
                    serial.....順次サーチ方式
- [ 説明 ]            isdn remote address call コマンドで複数の ISDN 番号が設定されている場合に意味を持つ。MP を使用する場合などのように、相手先に対して同時に複数のチャンネルで接続しようとする際に、どのような順番で ISDN 番号を選択するかを設定する。  
round を指定した場合は、isdn remote address call コマンドで最初に設定した ISDN 番号で発信した次の発信時に、このコマンドで次に設定された ISDN 番号を使う。このように順次ずれていき、最後に設定された番号で発信した次には、最初に設定された ISDN 番号を使い、これを繰り返す。  
serial を指定した場合は、発信時には必ず最初に設定された ISDN 番号を使い、何らかの理由で接続できなかった場合は次に設定された ISDN 番号で発信し直す。  
なお round、serial いずれの設定の場合でも、どことも接続されていない状態や相手先とすべてのチャンネルで切断された後では、最初に設定された ISDN 番号から発信に使用される。
- [ ノート ]            MP を使用する場合は、round にした方が効率が良い。
- [ デフォルト値 ]    serial

## 4.2.3 自動接続の設定

- [ 入力形式 ]      isdn auto connect *auto*  
no isdn auto connect [*auto*]
- [ パラメータ ]      *auto*  
                    on.....自動接続する  
                    off.....自動接続しない
- [ 説明 ]            選択されている相手について自動接続するか否かを設定する。
- [ デフォルト値 ]    on

## 4.2.4 自動切断の設定

- [ 入力形式 ]      isdn auto disconnect *auto*  
no isdn auto disconnect [*auto*]
- [ パラメータ ]      *auto*  
                    on.....自動切断する  
                    off.....自動切断しない
- [ 説明 ]            選択されている相手について自動切断するか否かを設定する。  
各種切断タイマの設定を変更せずに、自動切断を無効にしたい場合に使用する。
- [ ノート ]            schedule at コマンドと併用して、テレホーダイ時間中に自動切断しないようにしたい場合等に有効。  
anonymous に対して使用する事はできない。
- [ デフォルト値 ]    on

## 4.2.5 着信許可の設定

- [ 入力形式 ]      isdn arrive permit *arrive*  
no isdn arrive permit [*arrive*]
- [ パラメータ ]      *arrive*  
                    on.....許可する  
                    off.....許可しない
- [ 説明 ]            選択されている相手からの着信を許可するか否かを設定する。
- [ ノート ]            isdn arrive permit、isdn call permit コマンドとも off を設定した場合は通信できない。
- [ デフォルト値 ]    on

#### 4.2.6 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> 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

#### 4.2.7 再発信抑制タイマの設定

---

[入力形式]	isdn call block time <i>time</i> no isdn call block time [ <i>time</i> ]
[パラメータ]	<i>time</i> ..... 秒数 (0..15)
[説明]	選択されている相手との通信が切断された後、同じ相手に対し再度発信するのを禁止する時間を設定する。秒数は 0.1 秒単位で設定できる。 isdn call prohibit time コマンドによるタイマはエラーで切断された場合だけに適用されるが、このコマンドによるタイマは正常切断でも適用される点異なる。
[ノート]	切断後すぐに発信ということを繰り返す状況では適当な値を設定すべきである。 isdn forced disconnect time コマンドと併用するとよい。
[デフォルト値]	0

#### 4.2.8 エラー切断後の再発信禁止タイマの設定

---

[入力形式]	isdn call prohibit time <i>time</i> no isdn call prohibit time [ <i>time</i> ]
[パラメータ]	<i>time</i> ..... 秒数 (60..21474836)
[説明]	選択されている相手に発信しようとして失敗した場合に、同じ相手に対し再度発信するのを禁止する時間を設定する。秒数は 0.1 秒単位で設定できる。 isdn call block time コマンドによるタイマは切断後に常に適用されるが、このコマンドによるタイマはエラー切断にのみ適用される点異なる。
[デフォルト値]	60

#### 4.2.9 相手にコールバック要求を行うか否かの設定

---

[入力形式]	isdn callback request <i>callback_request</i> no isdn callback request [ <i>callback_request</i> ]
[パラメータ]	<i>callback_request</i> 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

#### 4.2.10 コールバック要求タイプの設定

---

[入力形式]	isdn callback request type <i>type</i> no isdn callback request type [ <i>type</i> ]
[パラメータ]	<i>type</i> 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

## 4.2.11 相手からのコールバック要求に応じるか否かの設定

---

[ 入力形式 ]	isdn callback permit <i>callback_permit</i> no isdn callback permit [ <i>callback_permit</i> ]
[ パラメータ ]	<i>callback_permit</i> 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

## 4.2.12 コールバック受け入れタイプの設定

---

[ 入力形式 ]	isdn callback permit type <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> 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> = mscbc

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

---

[ 入力形式 ]	isdn callback mscbc user-specify <i>specify</i> no isdn callback mscbc user-specify [ <i>specify</i> ]
[ パラメータ ]	<i>specify</i> 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する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

## 4.2.14 コールバックタイムの設定

---

[ 入力形式 ]	isdn callback response time <i>type time</i>
[ パラメータ ]	<i>type</i> 1b.....1B でコールバックする場合 2b.....2B もしくは any でコールバックする場合 <i>time</i> .....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 ]	<i>time</i> =5

## 4.2.15 コールバック待機タイムの設定

---

[ 入力形式 ]	isdn callback wait time <i>time</i> no isdn callback wait time [ <i>time</i> ]
[ パラメータ ]	<i>time</i> .....秒数 (1..60)
[ 説明 ]	選択されている相手にコールバックを要求し、それが受け入れられていったん回線が切断されてから、このタイ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

## 4.2.16 ISDN 回線を切断するタイマ方式の指定

[入力形式]	isdn disconnect policy <i>type</i> no isdn disconnect policy [ <i>type</i> ]
[パラメータ]	<i>type</i> 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的方式であり、isdn disconnect time、isdn disconnect input time、isdn disconnect output time の 3 つのタイマコマンドでトラフィックを監視し、一定時間パケットが流れなくなった時点で回線を切断する。 課金単位時間方式では、課金単位時間と監視時間を isdn disconnect interval time コマンドで設定し、監視時間中にパケットが流れなければ課金単位時間の倍数の時間で回線を切断する。通信料金を減らす効果が期待できる。
[デフォルト値]	1

## 4.2.17 切断タイマの設定 (ノーマル)

[入力形式]	isdn disconnect time <i>time</i> no isdn disconnect time [ <i>time</i> ]
[パラメータ]	<i>time</i> 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

## 4.2.18 入力切断タイマの設定 (ノーマル)

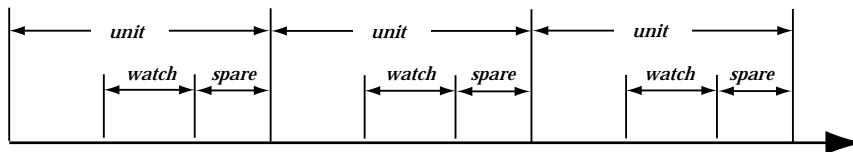
[入力形式]	isdn disconnect input time <i>time</i> no isdn disconnect input time [ <i>time</i> ]
[パラメータ]	<i>time</i> 秒数 (1..21474836) off..... タイマを設定しない
[説明]	選択されている相手について PP 側からデータ受信がない場合の切断までの時間を設定する。秒数は 0.1 秒単位で設定できる。
[ノート]	例えば、UDP パケットを定期的に出すようなプログラムが暴走したような場合、本タイマを設定しておくことにより回線を切断することができる。 4.2.17 切断タイマの設定 (ノーマル) のノート参照。
[デフォルト値]	120

## 4.2.19 出力切断タイマの設定 (ノーマル)

[入力形式]	isdn disconnect output time <i>time</i> no isdn disconnect output time [ <i>time</i> ]
[パラメータ]	<i>time</i> 秒数 (1..21474836) off..... タイマを設定しない
[説明]	選択されている相手について PP 側へのデータ送信がない場合の切断までの時間を設定する。秒数は 0.1 秒単位で設定できる。
[ノート]	例えば、UDP パケットを定期的に出すようなプログラムが暴走したような場合、本タイマを設定しておくことにより回線を切断することができる。 4.2.17 切断タイマの設定 (ノーマル) のノート参照。
[デフォルト値]	120

## 4.2.20 課金単位時間方式での課金単位時間と監視時間の設定

- [ 入力形式 ]    `isdn disconnect interval time unit watch spare`  
                   `no isdn disconnect interval time [unit watch spare]`
- [ パラメータ ]    *unit*..... 課金単位時間  
                   秒数 (1..21474836)  
                   off
- watch*..... 監視時間  
                   秒数 (1..21474836)  
                   off
- spare*..... 切断余裕時間  
                   秒数 (1..21474836)  
                   off
- [ 説明 ]            課金単位時間方式で使われる、課金単位時間と監視時間を設定する。秒数は 0.1 秒単位で設定できる。それぞれの意味は下図参照。



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

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

## 4.2.21 切断タイマの設定 (ファスト)

- [ 入力形式 ]    `isdn fast disconnect time time`  
                   `no isdn fast disconnect time [time]`
- [ パラメータ ]    *time*  
                   秒数 (1..21474836)  
                   off..... タイマを設定しない
- [ 説明 ]            ある宛先について、パケットがルーティングされ、そこへ発信しようとしたが、ISDN 回線が他の接続先により塞がっていて発信できない場合に、ISDN 回線を塞いでいる相手先についてこのタイマが動作を始める。このタイマで指定した時間の間、パケットが全く流れなかったらその相手先を切断して、発信待ちの宛先を接続する。秒数は 0.1 秒単位で設定できる。
- なお、`isdn auto connect` コマンドが `off` の場合はこのタイマは無視される。
- [ デフォルト値 ]    20

## 4.2.22 切断タイマの設定 (強制)

- [ 入力形式 ]    `isdn forced disconnect time time`  
                   `no isdn forced disconnect time [time]`
- [ パラメータ ]    *time*  
                   秒数 (1..21474836)  
                   off..... タイマを設定しない
- [ 説明 ]            選択されている相手に接続する最大時間を設定する。秒数は 0.1 秒単位で設定できる。パケットをやりとりしていても、このコマンドで設定した時間が経過すれば強制的に回線を切断する。ダイヤルアップ接続でインターネット側からの無効なパケット (ping アタック等) が原因で回線が自動切断できない場合に有効。 `isdn call block time` コマンドと併用するとよい。
- [ デフォルト値 ]    off



## 5. IP の設定

### 5.1 インタフェース共通の設定

#### 5.1.1 IP パケットを扱うか否かの設定

---

[入力形式]	ip routing <i>routing</i> no ip routing [ <i>routing</i> ]
[パラメータ]	<i>routing</i> 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

#### 5.1.2 IP アドレスの設定

---

[入力形式]	ip <i>interface</i> address <i>ip_address/mask</i> [ <i>broadcast broadcast_ip</i> ] no ip <i>interface</i> address [ <i>ip_address/mask</i> ]
[パラメータ]	<i>interface</i> ..... LAN インタフェース名、もしくは pp <i>ip_address</i> ..... IP アドレス xxx.xxx.xxx.xxx (xxx は 10 進数) <i>mask</i> xxx.xxx.xxx.xxx (xxx は 10 進数) 0x に続く 16 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]	インタフェースの IP アドレスとネットマスクを設定する。“broadcast <i>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。
[ノート]	LAN インタフェースに IP アドレスを設定していない場合には、RARP により IP アドレスを得ようとする。PP インタフェースに IP アドレスを設定していない場合には、そのインタフェースは unnumbered として動作する。
[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

#### 5.1.3 セカンダリ IP アドレスの設定

---

[入力形式]	ip <i>interface</i> secondary address <i>ip_address[/mask]</i> no ip <i>interface</i> secondary address [ <i>ip_address/mask</i> ]
[パラメータ]	<i>interface</i> ..... LAN インタフェース名、もしくは pp <i>ip_address</i> ..... セカンダリ IP アドレス xxx.xxx.xxx.xxx (xxx は 10 進数) <i>mask</i> xxx.xxx.xxx.xxx (xxx は 10 進数) 0x に続く 16 進数 マスクビット数
[説明]	LAN 側のセカンダリ IP アドレスとネットマスクを設定する。
[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。 PP インタフェースに対してはセカンダリアドレスは設定できない。

## 5.1.4 IP の静的経路情報の設定

[ 入力形式 ]	ip route <i>network</i> gateway <i>gateway</i> [ <i>parameter</i> ] [ <i>gateway gateway</i> [ <i>parameter</i> ]] no ip route <i>network</i> [ <i>gateway</i> ..]
[ パラメータ ]	<p><i>network</i></p> <p>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)</p> <p><i>gateway</i></p> <p>IP アドレス ..... xxx.xxx.xxx.xxx (xxx は 10 進数) pp <i>pp_num</i> [<i>dlci=dlci</i>] ..... PP インタフェースへの経路 "dlci=<i>dlci</i>" が指定された場合は、フレームリレーの DLCI への経路</p> <p><i>pp_num</i></p> <p>PP 番号 (RT105i:1..30, その他 :1..100)</p> <p>anonymous</p> <p>pp anonymous name=<i>name</i></p> <p><i>name</i> ..... PAP/CHAP による名前</p> <p>tunnel <i>tunnel_num</i> ..... Tunnel インタフェースへの経路</p> <p><i>parameter</i> ..... 以下のパラメータを空白で区切り複数設定可能</p> <p>filter <i>number</i> [<i>number</i>..] ... フィルタ型経路の指定 <i>number</i> ..... フィルタの番号 (1..21474836) (空白で区切り複数設定可能)</p> <p>metric <i>metric</i> ..... メトリックの指定 <i>metric</i> ..... メトリック値 (1..15) (省略時は 1)</p> <p>hide ..... 出力インタフェースが PP インタフェースの場合のみ有効なオプションで、回線が接続されている場合だけ経路が有効になることを意味する</p> <p>weight <i>weight</i> ..... 異なる経路間の比率を表す値 <i>weight</i> ..... 経路への重み (1..2147483647、省略時は 1)</p>
[ 説明 ]	<p>IP の静的経路を設定する。</p> <p><i>gateway</i> のパラメータとしてフィルタ型経路を指定した場合には、記述されている順にフィルタを適用していき、適合したゲートウェイが選択される。</p> <p>適合するゲートウェイが存在しない場合や、フィルタ型経路が指定されているゲートウェイが一つも記述されていない場合には、フィルタ型経路が指定されていないゲートウェイが選択される。</p> <p>フィルタ型経路が指定されていないゲートウェイも存在しない場合には、その経路は存在しないものとして処理が継続される。</p> <p>フィルタ型経路が指定されていないゲートウェイが複数記述された場合の経路の選択は、それらの経路を使用する時点でラウンドロビンにより決定される。</p> <p>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。</p>
[ ノート ]	既に存在する経路を上書きすることができる。
[ 設定例 ]	<p>デフォルトゲートウェイを 192.168.0.1 とする</p> <pre># ip route default gateway 192.168.0.1</pre> <p>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</p> <pre># ip route 192.168.1.0/24 gateway pp 1</pre>

## 5.1.5 IP パケットのフィルタの設定

[入力形式] ip filter *filter\_num* *pass\_reject* *src\_addr*[/*mask*][*dest\_addr*[/*mask*]][*protocol* [*src\_port\_list* [*dest\_port\_list*]]]  
no ip filter *filter\_num* [*pass\_reject*]

[パラメータ] *filter\_num* ..... 静的フィルタ番号 (1..2147483647)  
*pass\_reject*  
pass-log ..... 一致すれば通す (ログに記録する)  
pass-nolog ..... 一致すれば通す (ログに記録しない)  
reject-log ..... 一致すれば破棄する (ログに記録する)  
reject-nolog ..... 一致すれば破棄する (ログに記録しない)  
restrict-log ..... 回線が接続されていれば通し、切断されていれば破棄する  
(ログに記録する)  
restrict-nolog ..... 回線が接続されていれば通し、切断されていれば破棄する  
(ログに記録しない)  
*src\_addr* ..... IP パケットの始点 IP アドレス  
xxx.xxx.xxx.xxx xxx は  
10 進数  
\* (ネットマスクの対応するビットが 8 ビットとも 0 と同じ)  
間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。  
\* (すべての IP アドレスに対応)  
*dest\_addr* ..... IP パケットの終点 IP アドレス (*src\_addr* と同じ形式)。  
省略時は 1 個の \* と同じ。  
*mask* ..... IP アドレスのビットマスク、省略時は 0xffffffff と同じ。  
*src\_addr* 及び *dest\_addr* がネットワークアドレスの場合にのみ指定可。  
xxx.xxx.xxx.xxx (xxx は 10 進数)  
0x に続く 16 進数  
マスクビット数  
*protocol* ..... フィルタリングするパケットの種類  
プロトコルを表す 10 進数 (0..255)  
プロトコルを表すニーモニック

ニーモニック	10 進数	説明
icmp	1	icmp パケット
icmp-error	-	特定の TYPE コードの icmp パケット
icmp-info	-	特定の TYPE コードの icmp パケット
tcp	6	tcp パケット
tcpfin	-	FIN フラグの立っている tcp パケット
tcprst	-	RST フラグの立っている tcp パケット
		ACK フラグの立っている tcp パケット
established	-	内から外への接続は許可するが、 外から内への接続は拒否する機能
udp	17	udp パケット
ah	51	IPsec の ah パケット
esp	50	IPsec の esp パケット

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)  
省略時は \* と同じ。

*src\_port\_list*.....UDP、TCP のソースポート番号  
 ポート番号を表す 10 進数  
 ポート番号を表すニーモニック (一部)

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

間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。  
 上項目のカンマで区切った並び (10 個以内)

\* (すべてのポート)

省略時は \* と同じ。

*dest\_port\_list*.....UDP、TCP のデスティネーションポート番号

- [ 説明 ] IP パケットのフィルタを設定する。本コマンドで設定されたフィルタは *ip interface secure filter*、*ip filter set*、*ip filter dynamic*、及び *ip interface rip filter* コマンドで用いられる。
- [ ノート ] *restrict-log* 及び *restrict-nolog* を使ったフィルタは、回線が接続されている場合だけ通せば十分で、そのために回線に発信するまでもないようなパケットに対して有効。例えば、時計をあわせる NTP パケット。  
*"ip filter pass \* \* icmp,tcp telnet"* などのように、TCP/UDP 以外のプロトコルとポート番号の両方が指定されている場合、TCP/UDP 以外のパケットに関しては、ポート番号の指定をチェックしない。  
*"ip filter pass \* \* \* telnet"* などのように、TCP/UDP と明記せずにポート番号を指定していた場合、TCP/UDP 以外もフィルタに該当する。
- [ 設定例 ] # *ip filter 3 pass-nolog 172.20.10.\* 172.21.192.0/18 tcp ftp*

### 5.1.6 フィルタセットの定義

- [ 入力形式 ] *ip filter set name direction filter\_list [filter\_list ...]*  
*no ip filter set name [direction ...]*
- [ パラメータ ] *name*..... フィルタセットの名前を表す文字列  
*direction*  
   *in* ..... 入力方向のフィルタ  
   *out*..... 出力方向のフィルタ  
*filter\_list*..... 100 個以内の、空白で区切られたフィルタ番号の並び
- [ 説明 ] フィルタセットを定義する。フィルタセットは、in/out のフィルタをそれぞれ定義し、RADIUS による指定や、*ip interface secure filter* コマンドによりインタフェースに適用される。

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

- [ 入力形式 ] *ip filter source-route filter\_out*  
*no ip filter source-route [filter\_out]*
- [ パラメータ ] *filter\_out*  
   *on*..... フィルタアウトする  
   *off*..... フィルタアウトしない
- [ 説明 ] Source-route オプション付き IP パケットをフィルタアウトするか否かを設定する。
- [ デフォルト値 ] *on*

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

[入力形式]	ip filter directed-broadcast <i>filter_out</i> no ip filter directed-broadcast [ <i>filter_out</i> ]
[パラメータ]	<i>filter_out</i> on ..... フィルタアウトする off ..... フィルタアウトしない
[説明]	終点 IP アドレスが Directed-Broadcast アドレス宛になっている IP パケットをルータが接続されているネットワークにブロードキャストするか否かを設定する。
[ノート]	いわゆる smurf 攻撃を防止するためには on にしておく。
[デフォルト値]	on

## 5.1.9 動的フィルタの定義

[入力形式]	ip filter dynamic <i>dyn_filter_num srcaddr dstaddr protocol [option ...]</i> ip filter dynamic <i>dyn_filter_num srcaddr dstaddr filter filter_list [in filter_list] [out filter_list] [option ...]</i> no ip filter dynamic <i>dyn_filter_num [dyn_filter_num...]</i>
[パラメータ]	<i>dyn_filter_num</i> ..... 動的フィルタ番号 (1...2147483647) <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 tcp udp ftp tftp domain www smtp pop3 telnet <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> syslog= <i>switch</i> on ..... コネクションの通信履歴を syslog に残す off ..... コネクションの通信履歴を syslog に残さない timeout= <i>time</i> <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]	動的フィルタを定義する。第 1 書式では、あらかじめルータに登録されているアプリケーション名を指定する。第 2 書式では、ユーザがアクセス制御のルールを記述する。キーワードの filter、in、out の後には、ip filter コマンドで定義されたフィルタ番号を設定する。 filter キーワードの後に記述されたフィルタに該当するコネクション (トリガ) を検出したら、それ以降 in キーワードと out キーワードの後に記述されたフィルタに該当するコネクションを通過させる。in キーワードはトリガの方向に対して逆方向のアクセスを制御し、out キーワードは動的フィルタと同じ方向のアクセスを制御する。なお、ip filter コマンドの IP アドレスは無視される。pass/reject の引数も同様に無視される。 プロトコルとして tcp や udp を指定した場合には、アプリケーションに固有な処理は実施されない。特定のアプリケーションを扱う必要がある場合には、アプリケーション名を指定する。
[デフォルト値]	syslog=on timeout=60
[設定例]	# ip filter 10 ** udp * snmp # ip filter dynamic 1 ** filter 10

## 5.1.10 動的フィルタのタイムアウトの設定

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

## 5.1.11 侵入検知機能の動作の設定

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

## 5.1.12 フィルタリングによるセキュリティの設定

- [入力形式] `ip interface secure filter direction [filter_list...] [dynamic filter_list...]`  
`ip interface secure filter name name`  
`no ip interface secure filter direction [filter_list]`  
`no ip interface secure filter [name [name]]`
- [パラメータ] *interface* ..... LAN インタフェース名、pp、tunnel  
*direction*  
  in..... 受信したパケットのフィルタリング  
  out..... 送信するパケットのフィルタリング  
*filter\_list* ..... 100 個以内の、空白で区切られたフィルタ番号の並び  
*name* ..... フィルタセットの名前を表す文字列  
dynamic ..... キーワード後に動的フィルタの番号を記述する
- [説明] ip filter コマンドによるパケットのフィルタを組み合わせ、インタフェースで送受信するパケットの種類を制限する。  
方向を指定する書式では、それぞれの方向に対して適用するフィルタ列をフィルタ番号で指定する。指定された番号のフィルタが順番に適用され、パケットにマッチするフィルタが見つければそのフィルタにより通過 / 廃棄が決定する。それ以降のフィルタは調べられない。すべてのフィルタにマッチしないパケットは廃棄される。  
フィルタセットの名前を指定する書式では、指定されたフィルタセットが適用される。フィルタを調べる順序などは方向を指定する書式の方法に準ずる。定義されていないフィルタセットの名前が指定された場合には、フィルタは設定されていないものとして動作する。
- [ノート] フィルタリストを走査して、一致すると通過、破棄が決定する。  
# ip filter 1 pass 192.168.0.0/24 \*  
# ip filter 2 reject 192.168.0.1  
# ip lan1 secure filter in 1 2  
この設定では、始点 IP アドレスが 192.168.0.1 であるパケットは、最初のフィルタ 1 で通過が決定してしまうため、フィルタ 2 での検査は行われぬ。そのため、フィルタ 2 は何も意味を持たない。  
フィルタリストを操作した結果、どのフィルタにも一致しないパケットは破棄される。
- PP Anonymous で認証に RADIUS を利用する場合で、RADIUS サーバから送られた Access-Response にアトリビュート 'Filter-Id' がついていた場合には、その値に指定されたフィルタセットを適用し、ip pp secure filter コマンドの設定は無視される。  
ただしアトリビュート "Filter-Id" が存在しない場合には、ip pp secure filter コマンドの設定がフィルタとして利用される。
- [デフォルト値] フィルタは設定されていない

## 5.1.13 IP パケットの TOS フィールドの書き換えの設定

- [入力形式] `ip tos supersede 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* , *filter\_num\_list*..... 静的フィルタの番号 (1..100)
- [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。

## 5.1.14 インタフェースの MTU の設定

- 
- [ 入力形式 ]     ip *interface* mtu *mtu*  
                  no ip *interface* mtu [*mtu*]
- [ パラメータ ]     *interface*.....LAN インタフェース名、もしくは pp  
                  *mtu*..... 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

## 5.2 代理 ARP の設定

- 
- [ 入力形式 ]     ip *interface* proxyarp proxyarp  
                  no ip *interface* proxyarp [*proxyarp*]
- [ パラメータ ]     *interface*.....LAN インタフェース名  
                  *proxyarp*  
                  on.....代理 ARP 動作をする  
                  off.....代理 ARP 動作をしない
- [ 説明 ]           代理 ARP 動作をするか否か設定する。
- [ デフォルト値 ]   off

## 5.3 PP 側の設定

## 5.3.1 PP 側 IP アドレスの設定

- 
- [ 入力形式 ]     ip pp remote address *ip\_address*  
                  no ip pp remote address [*ip\_address*]
- [ パラメータ ]     *ip\_address*  
                  IP アドレス..... xxx.xxx.xxx.xxx (xxx は 10 進数)  
                  dhcp.....自分自身の DHCP サーバ機能より IP アドレスを割り当てる
- [ 説明 ]           選択されている相手の PP 側の IP アドレスを設定する。  
                  dhcp を設定した場合は、自分自身が DHCP サーバとして動作している必要がある。自分で管理している DHCP スコープの中から、IP アドレスを割り当てる。  
                  装着されている BRI/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。  
                  PP として anonymous が選択された場合のみ有効である。
- [ ノート ]         実際に設定される IP アドレスは ppp ipcp ipaddress コマンドと相手の設定により決まる。自分側で設定した IP アドレスを xxx.xxx.xxx.xxx、相手先が要求してくる IP アドレスを yyy.yyy.yyy.yyy とすると実際に設定される IP アドレスは次のようになる。
- [ デフォルト値 ]   相手側 IP アドレスは設定されていない
- [ 設定例 ]         例えば、ルータ A 側が "no ip pp remote address"、"ppp ipcp ipaddress on" と設定し、接続するルータ B 側が "ip pp local 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。



### 5.3.2 リモート IP アドレスプールの設定

---

[入力形式]	ip pp remote address pool <i>ip_address</i> [ <i>ip_address...</i> ] ip pp remote address pool <i>ip_address-ip_address</i> ip pp remote address pool <i>dhcp</i> no ip pp remote address pool
[パラメータ]	<i>ip_address</i> ..... anonymous のためにプールする IP アドレス <i>ip_address-ip_address</i> ..... IP アドレスの範囲 <i>dhcp</i> ..... 自分自身の DHCP サーバ機能を利用する
[説明]	anonymous で相手に割り当てるための IP アドレスプールを設定する。 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。 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。 PP として anonymous が選択された場合のみ有効である。

## 5.4 RIP の設定

### 5.4.1 RIP を使用するか否かの設定

---

[入力形式]	rip use <i>rip_use</i> no rip use <i>rip_use</i>
[パラメータ]	<i>rip_use</i> 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

### 5.4.2 RIP による経路の優先度の設定

---

[入力形式]	rip preference <i>rip_preference</i> no rip preference <i>rip_preference</i>
[パラメータ]	<i>rip_preference</i> ..... 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

### 5.4.3 RIP パケットの送信に関する設定

---

[入力形式]	ip <i>interface</i> rip send <i>rip_send</i> [ <i>version version</i> [broadcast]] no ip <i>interface</i> rip send [ <i>rip_send...</i> ]
[パラメータ]	<i>interface</i> ..... LAN インタフェース名、もしくは pp <i>rip_send</i> on ..... RIP パケットを送信する off ..... RIP パケットを送信しない <i>version</i> ..... 送信する RIP のバージョン <i>broadcast</i> ..... ip interface address コマンドで指定した broadcast address
[説明]	指定したインタフェースに対し、RIP パケットを送信するか否かを設定する。 "version <i>version</i> " で送信する RIP のバージョンを指定できる。
[デフォルト値]	on version 1

## 5.4.4 RIP パケットの受信に関する設定

---

[ 入力形式 ]	ip <i>interface</i> rip receive <i>rip_receive</i> [version <i>version</i> [ <i>version</i> ]] no ip <i>interface</i> rip receive [ <i>rip_receive</i> ..]
[ パラメータ ]	<i>interface</i> ..... LAN インタフェース名、もしくは pp <i>rip_receive</i> 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> ..... RIP のバージョンを表し、1 または 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 とともに受信する。
[ デフォルト値 ]	<i>rip_receive</i> = on <i>version</i> = 1 2

## 5.4.5 RIP に関して信用できるゲートウェイの設定

---

[ 入力形式 ]	ip <i>interface</i> rip trust gateway [except] <i>gateway_list</i> no ip <i>interface</i> rip trust gateway [[except] <i>gateway_list</i> ]
[ パラメータ ]	<i>interface</i> ..... LAN インタフェース名、もしくは pp <i>gateway_list</i> ..... 10 個以内の IP アドレスの並び
[ 説明 ]	RIP に関して信用できる、あるいは信用できないゲートウェイを設定する。 except キーワードを指定していない場合には、列挙したゲートウェイを信用できるゲートウェイとし、それらからの RIP だけを受信する。 except キーワードを指定した場合は、列挙したゲートウェイを信用できないゲートウェイとし、それらを除いた他のゲートウェイからの RIP だけを受信する。
[ デフォルト値 ]	信用できる、あるいは信用できないゲートウェイは設定されておらず、すべてのホストからの RIP を信用できるものとして扱う

## 5.4.6 RIP のフィルタリングの設定

---

[ 入力形式 ]	ip <i>interface</i> rip filter <i>direction filter_list</i> no ip <i>interface</i> rip filter <i>direction filter_list</i>
[ パラメータ ]	<i>interface</i> ..... LAN インタフェース名、もしくは pp <i>direction</i> 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

## 5.4.7 RIP で加算するホップ数の設定

---

[ 入力形式 ]	ip <i>interface</i> rip hop <i>direction hop</i> no ip <i>interface</i> rip hop <i>direction hop</i>
[ パラメータ ]	<i>interface</i> ..... LAN インタフェース名、もしくは pp <i>direction</i> in ..... 受信した RIP に加算する out ..... 送信する RIP に加算する <i>hop</i> ..... 加算する値 (0..15)
[ 説明 ]	インタフェースで送受信する RIP に加算するホップ数を設定する。
[ デフォルト値 ]	0

## 5.4.8 RIP2 での認証の設定

---

[入力形式]	<code>ip interface rip auth type <i>type</i></code> <code>no ip interface rip auth type [<i>type</i>]</code>
[パラメータ]	<i>interface</i> ..... LAN インタフェース名、もしくは pp <i>type</i> 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

## 5.4.9 RIP2 での認証キーの設定

---

[入力形式]	<code>ip interface rip auth key <i>hex_key</i></code> <code>ip interface rip auth text <i>text_key</i></code> <code>no ip interface rip auth key</code>
[パラメータ]	<i>interface</i> ..... LAN インタフェース名、もしくは pp <i>hex_key</i> ..... 16 進数の列で表現された認証キー <i>text_key</i> ..... 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]	<code># ip lan1 rip auth key text testing123</code> <code># ip pp rip auth key text "hello world"</code> <code># ip lan2 rip auth key 01 02 ff 35 8e 49 a8 3a 5e 9d</code>

## 5.4.10 回線切断時の経路保持の設定

---

[入力形式]	<code>ip pp rip hold routing <i>rip_hold</i></code> <code>no ip pp rip hold routing [<i>rip_hold</i>]</code>
[パラメータ]	<i>rip_hold</i> 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 version ..... RIP のバージョンを表し、1 または 2
[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

## 5.4.11 回線接続時の PP 側の RIP の動作の設定

---

[入力形式]	<code>ip pp rip connect send <i>rip_action</i></code> <code>no ip pp rip connect send [<i>rip_action</i>]</code>
[パラメータ]	<i>rip_action</i> 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
[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

## 5.4.12 回線接続時の PP 側の RIP 送出の時間間隔の設定

---

[入力形式]	<code>ip pp rip connect interval <i>time</i></code> <code>no ip pp rip connect interval [<i>time</i>]</code>
[パラメータ]	<i>time</i> ..... 秒数 (30..21474836)
[説明]	選択されている相手について回線接続時に RIP を送出する時間間隔を設定する。 ip pp routing protocol コマンドが rip、ip pp rip connect send コマンドが interval の時に有効である。
[デフォルト値]	30

## 5.4.13 回線切断時の PP 側の RIP の動作の設定

---

[ 入力形式 ]	ip pp rip disconnect send <i>rip_action</i> no ip pp rip disconnect send [ <i>rip_action</i> ]
[ パラメータ ]	<i>rip_action</i> 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

## 5.4.14 回線切断時の PP 側の RIP 送出の時間間隔の設定

---

[ 入力形式 ]	ip pp rip disconnect interval <i>time</i> no ip pp rip disconnect interval [ <i>time</i> ]
[ 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 routing protocol コマンドで rip、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

## 5.5 VRRP の設定

## 5.5.1 インタフェース毎の VRRP の設定

---

[ 入力形式 ]	ip <i>interface</i> vrrp <i>vrid</i> <i>ip_address</i> [priority= <i>priority</i> ] [preempt= <i>preempt</i> ] [auth= <i>auth</i> ] no ip <i>interface</i> vrrp <i>vrid</i> [ <i>vrid</i> ...]
[ 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 on off <i>auth</i> ..... 8 文字以内のテキスト認証文字列
[ 説明 ]	指定した VRRP グループを利用することを設定する。 同じ VRRP グループに所属するルータの間では、VRID 及び仮想ルータの IP アドレスを一致させておかななくては いけない。これらが食い違った場合の動作は予測できない。 <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

## 5.5.2 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 pp-num [dcli=dcli] ip interface vrrp shutdown trigger vrid route network [nexthop] no ip interface vrrp shutdown trigger vrid interface no ip interface vrrp shutdown trigger vrid pp pp-num [...] no ip interface vrrp shutdown trigger vrid route network</pre>
[パラメータ]	<pre>interface ..... LAN インタフェース名 vrid ..... VRRP グループ ID (1..255) pp-num ..... PP 番号 dcli ..... DLCI 番号 network   ネットワークアドレス   IP アドレス / マスク長   default nexthop   インタフェース名   IP アドレス</pre>
[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> <p>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。</p> <p>pp 形式..... 指定した PP 番号に該当する回線で通信できなくなった場合にシャットダウンする。通信できなくなるとは、ケーブルが抜けるなどレイヤ 1 が落ちた場合と、以下の場合である。</p> <p>回線が ISDN 回線である時は、呼が接続されていない場合</p> <p>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</p> <p>回線が FR 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</p> <p>route 形式..... 指定した経路が経路テーブルに存在しないか、NEXTHop で指定したインタフェースもしくは IP アドレスで指定するゲートウェイに向いていない場合に、シャットダウンする。NEXTHop を省略した場合には、経路がどのような先を向いていても存在する限りはシャットダウンしない。</p>

## 6. IPX の設定

### 6.1 インタフェース共通の設定

#### 6.1.1 IPX パケットを扱うか否かの設定

---

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

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

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

[ デフォルト値 ]  off

## 6.1.2 IPX パケットのフィルタの設定

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

[パラメータ] *filter\_num* ..... 静的フィルタの番号 (1..100)

*pass\_reject*

*pass-log* ..... 一致すれば通す (ログに記録する)  
*pass-nolog* ..... 一致すれば通す (ログに記録しない)  
*reject-log* ..... 一致すれば破棄する (ログに記録する)  
*reject-nolog* ..... 一致すれば破棄する (ログに記録しない)  
*restrict-log* ..... 回線が接続されていれば通し、切断されていれば破棄する (ログに記録する)  
*restrict-nolog* ..... 回線が接続されていれば通し、切断されていれば破棄する (ログに記録しない)

*src\_net* ..... 始点 IPX ネットワーク番号

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

*src\_node* ..... 始点 IPX ノード番号

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

*dst\_net* ..... 終点 IPX ネットワーク番号 *src\_net* と同じ形式。

*dst\_node* ..... 終点 IPX ノード番号 *src\_node* と同じ形式。

*type* ..... IPX パケットタイプ

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

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

間に - をはさんだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。  
 上項目のカンマで区切った並び (5 個以内)  
 \* (すべての IPX パケットタイプ)  
 省略時は一個の \* と同じ

*src\_socket* ..... 始点ソケット番号

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

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

間に - をはさんだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。  
 上項目のカンマで区切った並び (5 個以内)  
 \* (すべてのソケット番号)  
 省略時は一個の \* と同じ

*dst\_socket* ..... 終点ソケット番号 *src\_socket* と同じ形式。

[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 lan 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。

6.1.3 静的な SAP テーブルの設定

[ 入力形式 ] ipx sap *service\_type* *server\_name* *network* *node\_num* *socket* *hop*  
no ipx sap *service\_type* *server\_name* [*network* *node\_num* *socket* *hop*]

[ パラメータ ] *service\_type* ..... サービスタイプ  
10 進数 (0..65535)  
0x に続く 4 桁以内の 16 進数  
file ..... 0x0004 の二モニク  
printer ..... 0x0007 の二モニク  
*server\_name* ..... サーバ名  
'A' ~ 'Z','0' ~ '9',';',',','@' で構成された 47 文字以内の文字列  
*network* ..... サーバの IPX ネットワーク番号 (0:0:0:1 .. FF:FF:FF:FE)  
*node\_num* ..... サーバの IPX ノード番号 (0:0:0:0:1 .. FF:FF:FF:FF:FE)  
*socket* ..... ソケット番号  
10 進数 (0..65535)  
0x に続く 4 桁以内の 16 進数  
プロトコルを表す二モニク

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

*hop* ..... ホップカウント (1..14)

[ 説明 ] SAP テーブルを設定する。

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

[ 入力形式 ] ipx sap response *response*  
no ipx sap response [*response*]

[ パラメータ ] *response*  
on ..... 応答する  
off ..... 応答しない

[ 説明 ] IPX SAP Get Nearest Server Request に応答するか否かを設定する。

[ デフォルト値 ] on

6.2 LAN 側の設定

6.2.1 イーサネットフレームタイプの設定

[ 入力形式 ] ipx *interface* frame type *type*  
no ipx *interface* frame type [*type*]

[ パラメータ ] *interface* ..... LAN インタフェース名  
*type*  
0 ..... IEEE 802.3 Raw  
1 ..... Ethernet II、イーサネットタイプは 0x8137  
2 ..... IEEE 802.3 + IEEE 802.2, SAP は 0xE0  
3 ..... IEEE 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



## 6.2.2 LAN 側の IPX ネットワーク番号の設定

---

[入力形式]	<code>ipx interface network <i>network</i></code> <code>no ipx interface network [<i>network</i>]</code>
[パラメータ]	<i>interface</i> ..... LAN インタフェース名 <i>network</i> ..... 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

## 6.2.3 経路情報の追加

---

[入力形式]	<code>ipx interface route <i>network gateway hop [ticks]</i></code> <code>no ipx interface route <i>network [gateway hop [ticks]]</i></code>
[パラメータ]	<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 (0:0:0:0:0:1 .. 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。

## 6.2.4 LAN 側の RIP/SAP ブロードキャストの設定

---

[入力形式]	<code>ipx interface ripsap broadcast <i>broadcast</i></code> <code>no ipx interface ripsap broadcast [<i>broadcast</i>]</code>
[パラメータ]	<i>interface</i> ..... LAN インタフェース名 <i>broadcast</i> 秒数 (60..21474836) <i>off</i> ..... 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。 <i>off</i> 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

## 6.2.5 LAN 側でのフィルタリングによるセキュリティの設定

---

[入力形式]	<code>ipx interface secure filter <i>direction filter_list</i></code> <code>no ipx interface secure filter <i>direction [filter_list]</i></code>
[パラメータ]	<i>interface</i> ..... LAN インタフェース名 <i>direction</i> <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> ..... 100 個以内の空白で区切られたフィルタ番号の並び
[説明]	LAN 側に対して適用する IPX フィルタを設定する。
[ノート]	フィルタリストを走査して、一致すると通過、破棄が決定する。 <code>ipx filter 1 pass 0:0:1:*</code> <code>ipx filter 2 reject 0:0:1:1</code> <code>ipx lan secure filter in 1 2</code> 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。

## 6.3 PP 側相手毎の IPX の設定

## 6.3.1 IPX ルーティング許可の設定

---

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

## 6.3.2 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 <i>network</i> [ <i>network</i> [ <i>node_num</i> ]]
[ パラメータ ]	<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: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

## 6.3.3 経路情報の追加

---

[ 入力形式 ]	ipx pp route <i>network</i> [ <i>name</i> ] <i>hops</i> [ <i>ticks</i> ] ipx pp route <i>network</i> [ <i>dlci=dlci_num</i> ] <i>hops</i> [ <i>ticks</i> ] no ipx pp route <i>network</i> [ <i>network</i> ...]
[ パラメータ ]	<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>hop</i> .....ホップカウント (1..14) <i>ticks</i> .....ティック (1..65535) <i>dlci_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。

## 6.3.4 回線接続時の PP 側の RIP/SAP の動作の設定

---

[ 入力形式 ]	ipx pp ripsap connect send <i>send</i> no ipx pp ripsap connect send [ <i>send</i> ]
[ パラメータ ]	<i>send</i> 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

### 6.3.5 回線接続時の PP 側の RIP/SAP 送出の時間間隔の設定

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

### 6.3.6 回線切断時の PP 側の RIP/SAP の動作の設定

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

### 6.3.7 回線切断時の PP 側の RIP/SAP 送出の時間間隔の設定

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

### 6.3.8 回線切断時に RIP/SAP 情報を保持するか否かの設定

- [入力形式]     `ipx pp ripsap hold hold`  
                   `no ipx pp ripsap hold [hold]`
- [パラメータ]     `hold`  
                   `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`

### 6.3.9 IPXWAN 使用の設定

- [入力形式]     `ipx pp ipxwan use use`  
                   `no ipx pp ipxwan use [use]`
- [パラメータ]     `use`  
                   `on` ..... 接続時に IPXWAN を用いてパラメータのネゴシエーションを行う  
                   `off` ..... パラメータのネゴシエーションは IPXCP で行い、IPXWAN は用いない
- [説明]            回線接続時のパラメータネゴシエーションの手順として IPXWAN を用いるかどうかを設定する。
- [デフォルト値]  `on`

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

- [ 入力形式 ] ipx pp ipxwan retry *interval max*  
no ipx pp ipxwan retry [*interval max*]
- [ パラメータ ] *interval* .....秒数 (10..21474836)  
*max* .....最大再送回数 (0..10)
- [ 説明 ] IPXWAN の Timer/Information Request の再送間隔と最大再送回数を設定する。
- [ デフォルト値 ] *interval* = 20  
*max* = 3

## 6.3.11 IPXWAN プライマリネットワーク番号の設定

- [ 入力形式 ] ipx pp ipxwan primnet *network*  
no ipx pp ipxwan primnet [*network*]
- [ パラメータ ] *network*.....IPXWAN プライマリネットワーク番号 (0:0:0:1 .. FF:FF:FF:FE)
- [ 説明 ] IPXWAN で用いるプライマリネットワーク番号を設定する。
- [ デフォルト値 ] PP 側インタフェースの MAC アドレスの下位 32 ビット

## 6.3.12 Watchdog パケットに対する代理応答の設定

- [ 入力形式 ] ipx pp watchdog proxy *proxy*  
no ipx pp watchdog proxy [*proxy*]
- [ パラメータ ] *proxy*  
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

## 6.3.13 Watchdog 代理応答の時間間隔の設定

- [ 入力形式 ] ipx pp watchdog interval *interval*  
no ipx pp watchdog interval [*interval*]
- [ パラメータ ] *interval* .....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

## 6.3.14 SPX キープアライブ代理応答を行うか否かの設定

- [ 入力形式 ] ipx pp spx keepalive proxy *proxy*  
no ipx pp spx keepalive proxy [*proxy*]
- [ パラメータ ] *proxy*  
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

## 6.3.15 SPX キープアライブ代理応答のタイマの設定

---

[入力形式]	<code>ipx pp spx keepalive timer <i>t1</i> [<i>t2</i> [<i>t3</i>]]</code> <code>no ipx pp spx keepalive timer <i>t1</i> [<i>t2</i> [<i>t3</i>]]</code>
[パラメータ]	<i>t1</i> ..... 秒数 (30..21474836) <i>t2</i> ..... 秒数 (30..65535) <i>t3</i> ..... 秒数 (1..65535)
[説明]	SPX キープアライブ代理応答のためのタイマ値を設定する。それぞれのタイマ値の意味は次の通り。 <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

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

---

[入力形式]	<code>ipx pp serialization filter <i>filter</i></code> <code>no ipx pp serialization filter [<i>filter</i>]</code>
[パラメータ]	<i>filter</i> 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

## 6.3.17 PP 側でのフィルタリングによるセキュリティの設定

---

[入力形式]	<code>ipx pp secure filter <i>direction filter_list</i></code> <code>no ipx pp secure filter <i>direction</i> [<i>filter_list</i>]</code>
[パラメータ]	<i>direction</i> 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 <i>filter_list</i> ..... 30 個以内の空白で区切られたフィルタ番号の並び
[説明]	PP 側に対し適用するフィルタを設定する。
[ノート]	フィルタリストを走査して、一致すると通過、破棄が決定する。 <code>ipx filter 1 pass 0:0:1:*</code> <code>ipx filter 2 reject 0:0:1:1</code> <code>ipx pp secure filter in 1 2</code> 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。

## 7. ブリッジの設定

### 7.1 インタフェース共通の設定

#### 7.1.1 ブリッジ使用許可の設定

---

[ 入力形式 ]	bridge use <i>use</i> no bridge use [ <i>use</i> ]
[ パラメータ ]	<i>use</i> on.....ブリッジする off.....ブリッジしない multicast .....マルチキャストのみブリッジする
[ 説明 ]	ブリッジを行うかどうかを設定する。
[ ノート ]	このスイッチが on でも、ip routing on であれば、IP パケットはブリッジング対象外となる。 同様に ipx routing on であれば、IPX パケットはブリッジング対象外となる。
[ デフォルト値 ]	off

#### 7.1.2 ブリッジするインタフェースの設定

---

[ 入力形式 ]	bridge group <i>interface_list</i> no bridge group [ <i>interface_list</i> ]
[ パラメータ ]	<i>interface_list</i> 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 インターフェース数まで設定できる。
[ ノート ]	anonymous を含める場合には、相手先情報番号を同時に指定することはできない。
[ デフォルト値 ]	インタフェースは設定されていない
[ 設定例 ]	LAN1 ポートと LAN2 ポート間でブリッジする # bridge group lan1 lan2  LAN2 ポートと相手先情報番号 3 の間でブリッジする # bridge group lan2 3

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

## 7.1.4 MAC アドレスのラーニングを行うか否かの設定

- [入力形式] bridge learning *learning*  
no bridge learning [*learning*]
- [パラメータ] *learning*  
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

## 7.1.5 ラーニング情報消去タイマの設定

- [入力形式] bridge learning expire *time*  
no bridge learning expire [*time*]
- [パラメータ] *time*  
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

## 7.2 LAN 側の設定

## 7.2.1 ラーニング情報の設定

- 
- [ 入力形式 ] bridge *interface* learning *mac\_address*  
no bridge *interface* learning *mac\_address*
- [ パラメータ ] *interface*.....LAN インタフェース名  
*mac\_address*..... *xx:xx:xx:xx:xx:xx* (*xx* は 16 進数)
- [ 説明 ] LAN 側インタフェースに対して MAC アドレスのラーニング情報を設定する。
- [ ノート ] ラーニング情報は全体で 30 個まで設定できる。

## 7.2.2 LAN 側でのブリッジのフィルタリングの設定

- 
- [ 入力形式 ] bridge *interface* filter *direction filter\_list*  
no bridge *interface* filter *direction [filter\_list]*
- [ パラメータ ] *interface*..... LAN インタフェース名  
*direction*  
in..... LAN 側から入ってくるパケットのフィルタリング  
out..... LAN 側に出ていくパケットのフィルタリング  
*filter\_list*.....空白で区切られた静的フィルタ番号の並び (100 個以内)
- [ 説明 ] 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の制限を設定する。
- [ デフォルト値 ] フィルタは設定されていない

## 7.3 PP 側相手毎のブリッジの設定

## 7.3.1 ラーニング情報の設定

- 
- [ 入力形式 ] bridge pp learning *mac\_address [dlci=dlci\_num]*  
no bridge pp learning *mac\_address [dlci=dlci\_num]*
- [ パラメータ ] *mac\_address*.....*XX:XX:XX:XX:XX:XX* (*XX* は 16 進数)  
*dlci\_num*.....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。

## 7.3.2 PP 側でのブリッジのフィルタリングの設定

- 
- [ 入力形式 ] bridge pp filter *direction filter\_list*  
no bridge pp filter *direction [filter\_list]*
- [ パラメータ ] *direction*  
in..... PP 側から入ってくるパケットのフィルタリング  
out..... PP 側に出ていくパケットのフィルタリング  
*filter\_list*.....空白で区切られた静的フィルタ番号の並び (100 個以内)
- [ 説明 ] PP 側を通るパケットについて bridge filter コマンドによるパケットのフィルタを組み合わせ、ブリッジするパケットの種類の制限を設定する。
- [ デフォルト値 ] フィルタは設定されていない



## 8. PPP の設定

### 8.1 相手の名前とパスワードの設定

[入力形式]	pp auth username <i>username</i> <i>password</i> [ <i>myname myname mypass</i> ] [ <i>isdn1</i> ] [ <i>clid</i> [ <i>isdn2</i> ]] [ <i>mscbcp</i> ] [ <i>ip_address</i> ] no pp auth username <i>username</i> [ <i>password</i> ...]
[パラメータ]	<i>username</i> ..... 名前 (32 文字以内) <i>password</i> ..... パスワード (32 文字以内) <i>myname</i> ..... 自分側の設定を入力するためのキーワード <i>myname</i> ..... 自分側のユーザ名 <i>mypass</i> ..... 自分側のパスワード <i>isdn1</i> ..... 相手の ISDN アドレス <i>clid</i> ..... 発番号認証を利用することを示すキーワード <i>isdn2</i> ..... 発番号認証に用いられる ISDN アドレス <i>mscbcp</i> ..... MS コールバックを許可することを示すキーワード <i>ip_address</i> ..... 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。 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ぬ。 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。

### 8.2 要求する認証タイプの設定

[入力形式]	pp auth request <i>auth</i> [ <i>arrive-only</i> ] no pp auth request [ <i>auth</i> [ <i>arrive-only</i> ]]
[パラメータ]	<i>auth</i> <i>none</i> ..... 何も要求しない <i>pap</i> ..... PAP による認証を要求する <i>chap</i> ..... CHAP による認証を要求する <i>chap-pap</i> ..... CHAP もしくは PAP による認証を要求する <i>arrive-only</i> ..... 着信時のみ PPP による認証を要求する
[説明]	PAP と CHAP による認証を要求するかどうかを設定する。発信時には常に適用される。anonymous でない着信の場合には発番号により PP が選択されてから適用される。anonymous での着信時には、発番号による PP の選択が失敗した場合に適用される。 chap-pap キーワードの場合には、最初 CHAP を要求し、それが相手から拒否された場合には改めて PAP を要求するよう動作する。これにより、相手が PAP または CHAP の片方しかサポートしていない場合でも容易に接続できるようになる。 arrive-only キーワードが指定された場合には、着信時のみ PPP による認証を要求するようになり、発信時には要求しない。 PP 毎のコマンドである。
[デフォルト値]	none

## 8.3 受け入れる認証タイプの設定

---

[ 入力形式 ]	pp auth accept <i>accept</i> no pp auth accept [ <i>accept</i> ]
[ パラメータ ]	<i>accept</i> pap.....PAP による認証を受け入れる chap.....CHAP による認証を受け入れる pap chap.....PAP と CHAP のいずれによる認証も受け入れる chap pap.....PAP と CHAP のいずれによる認証も受け入れる
[ 説明 ]	相手からの PPP 認証要求を受け入れるかどうかを設定する。発信時には常に適用される。anonymous でない着信の場合には発番号により PP が選択されてから適用される。anonymous での着信時には、発番号による PP の選択が失敗した場合に適用される。 このコマンドで認証を受け入れる設定になっていても、pp auth myname コマンドで自分の名前とパスワードが設定されていなければ、認証を拒否する。 PP 毎のコマンドである。
[ デフォルト値 ]	認証を受け入れない

## 8.4 自分の名前とパスワードの設定

---

[ 入力形式 ]	pp auth myname <i>myname password</i> no pp auth myname [ <i>myname password</i> ]
[ パラメータ ]	<i>myname</i> .....名前 (32 文字以内) <i>password</i> .....パスワード (32 文字以内)
[ 説明 ]	PAP または CHAP で相手に送信する自分の名前とパスワードを設定する。 PP 毎のコマンドである。

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

---

[ 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 ]	<i>prohibit</i> on.....禁止する off.....禁止しない
[ 説明 ]	pp auth username で登録した同一 <i>username</i> を持つ相手からの二重接続を禁止するか否かを設定する。
[ デフォルト値 ]	off
[ 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。

## 8.6 LCP 関連の設定

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

---

[ 入力形式 ]	ppp lcp acfc <i>acfc</i> no ppp lcp acfc [ <i>acfc</i> ]
[ パラメータ ]	<i>acfc</i> 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

### 8.6.2 Magic Number オプション使用の設定

---

[入力形式]	ppp lcp magicnumber <i>magicnumber</i> no ppp lcp magicnumber [ <i>magicnumber</i> ]
[パラメータ]	<i>magicnumber</i> 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

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

---

[入力形式]	ppp lcp mru <i>mru</i> [ <i>length</i> ] no ppp lcp mru [ <i>mru</i> [ <i>length</i> ]]
[パラメータ]	<i>mru</i> 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

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

---

[入力形式]	ppp lcp pfc <i>pfc</i> no ppp lcp pfc [ <i>pfc</i> ]
[パラメータ]	<i>pfc</i> 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

### 8.6.5 lcp-restart パラメータの設定

---

[入力形式]	ppp lcp restart <i>time</i> no ppp lcp 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,LCP] の configure-request、terminate-request の再送時間を設定する。
[デフォルト値]	3000

## 8.6.6 lcp-max-terminate パラメータの設定

- 
- [ 入力形式 ]    ppp lcp maxterminate *count*  
no ppp lcp maxterminate [*count*]
- [ パラメータ ]    *count*.....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

## 8.6.7 lcp-max-configure パラメータの設定

- 
- [ 入力形式 ]    ppp lcp maxconfigure *count*  
no ppp lcp maxconfigure [*count*]
- [ パラメータ ]    *count*.....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

## 8.6.8 lcp-max-failure パラメータの設定

- 
- [ 入力形式 ]    ppp lcp maxfailure *count*  
no ppp lcp maxfailure [*count*]
- [ パラメータ ]    *count*.....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

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

- 
- [ 入力形式 ]    ppp lcp silent *sw*
- [ パラメータ ]    *sw*  
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

## 8.6.10 専用線キープアライブを使用するか否かの設定

- 
- [ 入力形式 ]    leased keepalive use *use*  
no leased keepalive use [*use*]
- [ パラメータ ]    *use*  
on.....使用する  
off.....使用しない
- [ 説明 ]        専用線使用時にキープアライブを使用するか否かを設定する。
- [ ノート ]       複数 WAN ポートモデルでは PP 毎のコマンドである。
- [ デフォルト値 ] off

---

### 8.6.11 専用線キープアライブのログをとるか否かの設定

[入力形式]	leased keepalive log <i>log</i> no leased keepalive log [ <i>log</i> ]
[パラメータ]	<i>log</i> on ..... ログをとる off ..... ログをとらない
[説明]	キープアライブ (LCP ECHO) をログにとるか否かを設定する。
[ノート]	複数 WAN ポートモデルでは PP 毎のコマンドである。
[デフォルト値]	on

---

### 8.6.12 専用線キープアライブの時間間隔の設定

[入力形式]	leased keepalive interval <i>interval</i> [ <i>count</i> ] no leased keepalive interval [ <i>interval</i> [ <i>count</i> ]]
[パラメータ]	<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>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)
[説明]	LCP ECHO によるキープアライブパケットを送出する時間間隔とダウン検出を判定する回数を設定する。
[ノート]	複数 WAN ポートモデルでは PP 毎のコマンドである。 一度 LCP ECHO Request に対するリプライが返ってこないのを検出したら、その後の監視タイマは 1 秒に短縮される。
[デフォルト値]	<i>interval</i> = 30 <i>count</i> = 6

---

### 8.6.13 専用線ダウン検出時の動作の設定

[入力形式]	leased keepalive down <i>action</i> no leased keepalive down [ <i>action</i> ]
[パラメータ]	<i>action</i> 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

## 8.7 PAP 関連の設定

---

### 8.7.1 pap-restart パラメータの設定

[入力形式]	ppp pap restart <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

---

### 8.7.2 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

## 8.8 CHAP 関連の設定

## 8.8.1 chap-restart パラメータの設定

---

[ 入力形式 ]	ppp chap restart <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

## 8.8.2 chap-max-challenge パラメータの設定

---

[ 入力形式 ]	ppp chap maxchallenge <i>count</i> no ppp chap maxchallenge [ <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,CHAP] challenge の送信回数を設定する。
[ デフォルト値 ]	10

## 8.9 IPCP 関連の設定

## 8.9.1 Van Jacobson Compressed TCP/IP 使用の設定

---

[ 入力形式 ]	ppp ipcp vjc <i>compression</i> no ppp ipcp vjc [ <i>compression</i> ]
[ パラメータ ]	<i>compression</i> 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

## 8.9.2 PP 側 IP アドレスのネゴシエーションの設定

---

[ 入力形式 ]	ppp ipcp ipaddress <i>negotiation</i> no ppp ipcp ipaddress [ <i>negotiation</i> ]
[ パラメータ ]	<i>negotiation</i> 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

## 8.9.3 ipcp-restart パラメータの設定

---

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

---

#### 8.9.4 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]     *count*..... 回数 (1..10)
- [説明]            選択されている相手について [PPP,IPCP] の terminate-request の送信回数を設定する。
- [デフォルト値]  2

---

#### 8.9.5 ipcp-max-configure パラメータの設定

---

- [入力形式]     ppp ipcp maxconfigure *count*  
no ppp ipcp maxconfigure [*count*]
- [パラメータ]     *count*..... 回数 (1..10)
- [説明]            選択されている相手について [PPP,IPCP] の configure-request の送信回数を設定する。
- [デフォルト値]  10

---

#### 8.9.6 ipcp-max-failure パラメータの設定

---

- [入力形式]     ppp ipcp maxfailure *count*  
no ppp ipcp maxfailure [*count*]
- [パラメータ]     *count*..... 回数 (1..10)
- [説明]            選択されている相手について [PPP,IPCP] の configure-nak の送信回数を設定する。
- [デフォルト値]  10

---

#### 8.9.7 IPCP の MS 拡張オプションを使うか否かの設定

---

- [入力形式]     ppp ipcp msex *msex*  
no ppp ipcp msex [*msex*]
- [パラメータ]     *msex*  
                  on ..... 使用する  
                  off ..... 使用しない
- [説明]            選択されている相手について、[PPP,IPCP] の MS 拡張オプションを使うか否かを設定する。  
IPCP の Microsoft 拡張オプションを使うように設定すると、DNS サーバの IP アドレスと WINS (Windows Internet Name Service) サーバの IP アドレスを、接続した相手である Windows マシンに渡すことができる。渡すための DNS サーバや WINS サーバの IP アドレスはそれぞれ、dns server コマンドおよび wins server コマンドで設定する。
- [デフォルト値]  off

---

#### 8.9.8 WINS サーバの IP アドレスの設定

---

- [入力形式]     wins server *server1* [*server2*]  
no wins server [*server1* [*server2*]]
- [パラメータ]     *server, server*..... IP アドレス (xxx.xxx.xxx.xxx (xxx は 10 進数))
- [説明]            WINS (Windows Internet Name Service) サーバの IP アドレスを設定する。
- [ノート]          IPCP の MS 拡張オプションおよび DHCP でクライアントに渡すための WINS サーバの IP アドレスを設定する。ルータはこのサーバに対し WINS クライアントとしての動作は一切行わない。
- [デフォルト値]  WINS サーバは設定されていない

## 8.10 IPXCP 関連の設定

## 8.10.1 ipxcp-restart パラメータの設定

---

[ 入力形式 ]	ppp ipxcp restart <i>time</i> no ppp ipxcp 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、IPXCP] の configure-request、terminate-request の再送時間を設定する。
[ デフォルト値 ]	3000

## 8.10.2 ipxcp-max-terminate パラメータの設定

---

[ 入力形式 ]	ppp ipxcp maxterminate <i>count</i> no ppp ipxcp 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、IPXCP] の terminate-request の送信回数を設定する。
[ デフォルト値 ]	2

## 8.10.3 ipxcp-max-configure パラメータの設定

---

[ 入力形式 ]	ppp ipxcp maxconfigure <i>count</i> no ppp ipxcp 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、IPXCP] の configure-request の送信回数を設定する。
[ デフォルト値 ]	10

## 8.10.4 ipxcp-max-failure パラメータの設定

---

[ 入力形式 ]	ppp ipxcp maxfailure <i>count</i> no ppp ipxcp 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、IPXCP] の configure-nak の送信回数を設定する。
[ デフォルト値 ]	10

## 8.11 BCP 関連の設定

## 8.11.1 LAN Identification 使用の設定

---

[ 入力形式 ]	ppp bcp lanid <i>lan_id</i> no ppp bcp lanid [ <i>lan_id</i> ]
[ パラメータ ]	<i>lan_id</i> 0x1..... 0xFFFFFFFFe off..... LAN-Identification を使用しない
[ 説明 ]	LAN-Identification の値を設定する。
[ デフォルト値 ]	off



### 8.11.2 Tinygram compression 使用の設定

---

[入力形式]	ppp bcp tinycomp <i>compression</i> no ppp bcp tinycomp [ <i>compression</i> ]
[パラメータ]	<i>compression</i> on..... 使用する off..... 使用しない
[説明]	Tinygram compression を使用するか否かを設定する。
[デフォルト値]	on

### 8.11.3 bcp-restart パラメータの設定

---

[入力形式]	ppp bcp restart <i>time</i> no ppp bcp 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, BCP] の configure-request、terminate-request の再送時間を設定する。
[デフォルト値]	3000

### 8.11.4 bcp-max-terminate パラメータの設定

---

[入力形式]	ppp bcp maxterminate <i>count</i> no ppp bcp 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, BCP] の terminate-request の送信回数を設定する。
[デフォルト値]	2

### 8.11.5 bcp-max-configure パラメータの設定

---

[入力形式]	ppp bcp maxconfigure <i>count</i> no ppp bcp 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, BCP] の configure-request の送信回数を設定する。
[デフォルト値]	10

### 8.11.6 bcp-max-failure パラメータの設定

---

[入力形式]	ppp bcp maxfailure <i>count</i> no ppp bcp 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, BCP] の configure-nak の送信回数を設定する。
[デフォルト値]	10

## 8.12 MSCBCP 関連の設定

### 8.12.1 mscbcp-restart パラメータの設定

---

[入力形式]	ppp mscbcp restart <i>time</i> no ppp mscbcp 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, MSCBCP] の request/Response の再送時間を設定する。
[デフォルト値]	1000

## 8.12.2 mscbcpc-maxretry パラメータの設定

- 
- [ 入力形式 ]     ppp mscbcpc maxretry *count*  
                  no ppp mscbcpc maxretry [*count*]
- [ パラメータ ]     *count*.....回数 (1..30)
- [ 説明 ]            選択されている相手について [PPP, MSCBCP] の request/Response の再送回数を設定する。
- [ デフォルト値 ]  30

## 8.13 CCP 関連の設定

## 8.13.1 全パケットの圧縮タイプの設定

- 
- [ 入力形式 ]     ppp ccp type *type*  
                  no ppp ccp type [*type*]
- [ パラメータ ]     *type*  
                  stac..... Stac LZS で圧縮する  
                  cstac ..... Stac LZS で圧縮する ( 接続相手が Cisco ルータの場合 )  
                  none ..... 圧縮しない
- [ 説明 ]            選択されている相手について [PPP,CCP] 圧縮方式を選択する。
- [ ノート ]         Van Jacobson Compressed TCP/IP との併用も可能である。  
                  接続相手が Cisco ルータの場合には stac の設定では、データ転送中に頻繁に CCP のリセットが発生して、データ転送速度が遅くなることがある。そのような場合には、設定を cstac に変更すると状況が改善することがある。
- [ デフォルト値 ]  stac

## 8.13.2 ccp-restart パラメータの設定

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

## 8.13.3 ccp-max-terminate パラメータの設定

- 
- [ 入力形式 ]     ppp ccp maxterminate *count*  
                  no ppp ccp maxterminate [*count*]
- [ パラメータ ]     *count*.....回数 (1..10)
- [ 説明 ]            選択されている相手について [PPP, CCP] の terminate-request の送信回数を設定する。
- [ デフォルト値 ]  2

## 8.13.4 ccp-max-configure パラメータの設定

- 
- [ 入力形式 ]     ppp ccp maxconfigure *count*  
                  no ppp ccp maxconfigure [*count*]
- [ パラメータ ]     *count*.....回数 (1..10)
- [ 説明 ]            選択されている相手について [PPP, CCP] の configure-request の送信回数を設定する。
- [ デフォルト値 ]  10

### 8.13.5 ccp-max-failure パラメータの設定

---

- [入力形式]     ppp ccp maxfailure *count*  
no ppp ccp maxfailure [*count*]
- [パラメータ]     *count*..... 回数 (1..10)
- [説明]            選択されている相手について [PPP, CCP] の configure-nak の送信回数を設定する。
- [デフォルト値]  10

## 8.14 MP 関連の設定

### 8.14.1 MP を使用するか否かの設定

---

- [入力形式]     ppp mp use *use*  
no ppp mp use [*use*]
- [パラメータ]     *use*  
                  on ..... 使用する  
                  off ..... 使用しない
- [説明]            選択されている相手について MP を使用するか否かを選択する。  
on に設定していても、LCP の段階で相手とのネゴシエーションが成立しなければ MP を使わずに通信する。
- [デフォルト値]  off

### 8.14.2 MP の制御方法の設定

---

- [入力形式]     ppp mp control *type*  
no ppp mp control [*type*]
- [パラメータ]     *type*  
                  arrive ..... 自分が 1B 目の着信側の場合に MP を制御する  
                  both ..... 自分が 1B 目の発信着信いずれの場合でも MP を制御する  
                  call ..... 自分が 1B 目の発信側の場合に MP を制御する
- [説明]            選択されている相手について MP を制御して 2B 目の発信 / 切断を行う場合を設定する。通常は default のように自分が 1B 目の発信側の場合だけ制御するようにしておく。
- [デフォルト値]  call

### 8.14.3 MP のための負荷閾値の設定

---

- [入力形式]     ppp mp load threshold *call\_load call\_count disc\_load disc\_count*  
no ppp mp load threshold [*call\_load call\_count disc\_load disc\_count*]
- [パラメータ]     *call\_load*..... 発信負荷閾値 %(1..100)  
                  *call\_count*..... 回数 (1..100)  
                  *disc\_load*..... 切断負荷閾値 %(0..50)  
                  *disc\_count*..... 回数 (1..100)
- [説明]            選択されている相手について [PPP, MP] の 2B 目を発信したり切断したりする場合のデータ転送負荷の閾値を設定する。  
負荷は回線速度に対する % で評価し、送受信で大きい方の値を採用する。*call\_load* を超える負荷が *call\_count* 回繰り返されたら 2B 目の発信を行う。逆に *disc\_load* を下回る負荷が *disc\_count* 回繰り返されたら 2B 目を切断する。
- [デフォルト値]  *call\_load* = 70  
                  *call\_count* = 1  
                  *disc\_load* = 30  
                  *disc\_count* = 2

## 8.14.4 MP の最大リンク数の設定

---

[ 入力形式 ]	ppp mp maxlink <i>number</i> no ppp mp maxlink [ <i>number</i> ]
[ パラメータ ]	<i>number</i> ..... リンク数
[ 説明 ]	選択されている相手について [PPP, MP] の最大リンク数を設定する。リンク数の最大値は、使用モデルで使用できる ISDN Bch の数までとなる。
[ デフォルト値 ]	2

## 8.14.5 MP の最小リンク数の設定

---

[ 入力形式 ]	ppp mp minlink <i>number</i> no ppp mp minlink [ <i>number</i> ]
[ パラメータ ]	<i>number</i> ..... 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

## 8.14.6 MP のための負荷計測間隔の設定

---

[ 入力形式 ]	ppp mp timer <i>time</i> no ppp mp timer [ <i>time</i> ]
[ パラメータ ]	<i>time</i> ..... 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

## 8.14.7 MP のパケットを分割するか否かの設定

---

[ 入力形式 ]	ppp mp divide <i>divide</i> no ppp mp divide [ <i>divide</i> ]
[ パラメータ ]	<i>divide</i> 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

## 8.15 BACP 関連の設定

## 8.15.1 bacp-restart パラメータ の設定

---

[ 入力形式 ]	ppp bacp restart <i>time</i> no ppp bacp 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, BACP] の configure-request、terminate-request の再送時間を設定する。
[ デフォルト値 ]	3000

---

### 8.15.2 bacp-max-terminate パラメータ の設定

---

- [入力形式]     ppp bacp maxterminate *count*  
no ppp bacp maxterminate [*count*]
- [パラメータ]     *count*..... 回数 (1..10)
- [説明]            選択されている相手について [PPP, BACP] の terminate-request の送信回数を設定する。
- [デフォルト値]  2

---

### 8.15.3 bacp-max-configure パラメータ の設定

---

- [入力形式]     ppp bacp maxconfigure *count*  
no ppp bacp maxconfigure [*count*]
- [パラメータ]     *count*..... 回数 (1..10)
- [説明]            選択されている相手について [PPP, BACP] の configure-request の送信回数を設定する。
- [デフォルト値]  10

---

### 8.15.4 bacp-max-failure パラメータ の設定

---

- [入力形式]     ppp bacp maxfailure *count*  
no ppp bacp maxfailure [*count*]
- [パラメータ]     *count*..... 回数 (1..10)
- [説明]            選択されている相手について [PPP, BACP] の configure-nak を送る回数を設定する。
- [デフォルト値]  10

---

### 8.15.5 bap-restart パラメータの設定

---

- [入力形式]     ppp bap restart *time*  
no ppp bap restart [*time*]
- [パラメータ]     *time*..... ミリ秒 (20..10000)
- [説明]            選択されている相手について [PPP, BAP] の configure-request、terminate-request の再送時間を設定する。
- [デフォルト値]  1000

---

### 8.15.6 bap-max-retry パラメータの設定

---

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

## 8.16 PPPoE 関連の設定

---

### 8.16.1 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

## 8.16.2 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。

## 8.16.3 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

## 8.16.4 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

## 8.16.5 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

## 8.16.6 PADI パケットの再送時間の設定

- 
- [ 入力形式 ]    pppoe padi restart *time*  
                  no pppoe padi restart
- [ パラメータ ]    *time*..... ミリ秒 (20..10000)
- [ 説明 ]            PPPoE プロトコルにおける PADI パケットの再送時間を設定する。
- [ デフォルト値 ] 3000

## 8.16.7 PADR パケットの最大再送回数の設定

- 
- [ 入力形式 ]    pppoe padr maxretry *times*  
                  no pppoe padr maxretry
- [ パラメータ ]    *times*..... 回数 (1..10)
- [ 説明 ]            PPPoE プロトコルにおける PADR パケットの最大再送回数を設定する。
- [ デフォルト値 ] 5

## 8.16.8 PADR パケットの再送時間の設定

---

[入力形式]	pppoe padr restart <i>time</i> 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

## 8.16.9 PPPoE セッションの切断タイムの設定

---

[入力形式]	pppoe disconnect time <i>time</i> no pppoe disconnect time
[パラメータ]	<i>time</i> 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。
[デフォルト値]	off

## 8.16.10 TCP パケットの MSS の制限の有無とサイズの指定

---

[入力形式]	pppoe tcp mss limit <i>length</i> pppoe tcp mss limit
[パラメータ]	<i>length</i> データ長 (1240..1452) auto ..... MSS を MTU の値に応じて制限する off..... MSS を制限しない
[説明]	PPPoE セッション上で TCP パケットの MSS を制限するかどうかを設定する。
[デフォルト値]	auto

## 9. DHCP の設定

本機は DHCP<sup>1</sup> 機能として、DHCP サーバ機能、DHCP リレーエージェント機能を実装しています。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 dhcp` コマンドにより知ることができます。

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

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

IP アドレスの範囲は複数の設定が可能であり、それぞれの範囲を DHCP スコープ番号で管理します。DHCP クライアントからの設定要求があると DHCP サーバは DHCP スコープの中で未割り当ての IP アドレスを自動的に通知します。なお、特定の DHCP クライアントに特定の IP アドレスを固定的にリースする場合には、`dhcp scope` コマンドで定義したスコープ番号を用いて `dhcp scope bind` コマンドで予約します。予約の解除は `dhcp scope unbind` コマンドで行います。IP アドレスのリース期間には時間指定と無期限の両方が可能であり、これは `dhcp scope` コマンドの `expire` 及び `maxexpire` キーワードのパラメータで指定します。リース状況は `show dhcp status` 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。

### 9.1 DHCP の動作の設定

---

[ 入力形式 ]	<code>dhcp service <i>type</i></code> <code>no dhcp service [<i>type</i>]</code>
[ パラメータ ]	<i>type</i> <code>server</code> ..... DHCP サーバとして機能させる <code>relay</code> ..... 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

---

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



## 9.2 RFC2131 対応動作の設定

[入力形式]	<pre> dhcp server rfc2131 compliant <i>comp</i> dhcp server rfc2131 compliant [except] <i>function</i> [<i>function..</i>] no dhcp server rfc2131 compliant  <i>comp</i>   on ..... RFC2131 準拠   off ..... RFC1541 準拠 <i>except</i>..... 指定した機能以外が RFC2131 対応となるキーワード  <i>function</i>   broadcast-nak ..... DHCPNAK をブロードキャストで送る   none-domain-null... ドメイン名の最後に NULL 文字を付加しない   remain-silent ..... リース情報を持たないクライアントからの DHCPREQUEST を無視する   reply-ack ..... DHCPNAK の代わりに許容値を格納した DHCPACK を返す   use-clientid..... クライアントの識別に Client-Identifier オプションを優先する </pre>
[説明]	<p>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。</p> <p>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。</p> <p><b>broadcast-nak</b> ..... 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。</p> <p><b>none-domain-null</b>... 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。</p> <p><b>remain-silent</b> ..... 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。</p> <p><b>reply-ack</b> ..... 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。</p> <p><b>use-clientid</b> ..... 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。</p>
[デフォルト値]	on

## 9.3 DHCP スコープの定義

- [ 入力形式 ] `dhcp scope scope_num ip_address-ip_address/netmask [except ex_ip ...] [gateway gw_ip] [expire time] [maxexpire time]`  
`no dhcp scope scope_num [ip_address-ip_address/netmask [except ex_ip ...] [gateway gw_ip] [expire time] [maxexpire time]]`
- [ パラメータ ] `scope_num`.....スコープ番号 (1..65535)  
`ip_address-ip_address`...対象となるサブネットでの割り当てる IP アドレスの範囲  
`netmask`  
`xxx.xxx.xxx.xxx` (xxx は 10 進数)  
0x に続く 16 進数  
マスクビット数  
`ex_ip`.....IP アドレス指定範囲の中で除外する IP アドレス (空白で区切って複数指定可能)  
`gw_ip`.....IP アドレス対象ネットワークのゲートウェイの IP アドレス  
`time`.....時間  
分 (1..21474836)  
時間: 分  
`infinity`.....無期限リース
- [ 説明 ] DHCP サーバとして割り当てる IP アドレスの範囲を設定する。  
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 ] `expire time = 72:00`  
`maxexpire time = 72:00`

## 9.4 DHCP 予約アドレスの設定

- [入力形式] dhcp scope bind *scope\_num ip\_address [type] id*  
 dhcp scope bind *scope\_num ip\_address mac\_address*  
 dhcp scope bind *scope\_num ip\_address ipcp*  
 no dhcp scope bind *scope\_num ip\_address*
- [パラメータ] *scope\_num*..... スコープ番号 (1..65535)  
*ip\_address*..... 予約する IP アドレス  
*type*..... Client-Identifier オプションの type フィールドを決定する  
 text..... 0x00  
 ethernet ..... 0x01  
*id*  
*type* が ethernet の場合 ..... MAC アドレス  
*type* が text の場合 ..... 文字列  
*type* が省略された場合 ..... 2 桁 16 進数の列で先頭は type フィールド  
*mac\_address* ..... xx:xx:xx:xx:xx:xx (xx は 16 進数) 予約 DHCP クライアントの MAC アドレス  
*ipcp*..... IPCP でリモート側に与えることを示す
- [説明] IP アドレスをリースする DHCP クライアントを固定的に設定する。
- [ノート] IP アドレスは、*scope\_num* パラメータで指定された DHCP スコープ範囲内でなければならない。1 つの DHCP スコープ内では、1 つの MAC アドレスに複数の IP アドレスを設定することはできない。他の DHCP クライアントにリース中の IP アドレスを予約設定した場合、リース終了後にその IP アドレスの割り当てが行われる。dhcp scope コマンド、あるいは dhcp delete scope コマンドを実行した場合、関連する予約はすべて消去される。ipcp の指定は、同時に接続できる B チャネルの数に限られる。また、ipcp で与えるアドレスや擬似 LAN に与えるアドレスは、LAN 側のスコープから選択される。
- コマンドの第 1 の書式を使う場合は、あらかじめ dhcp server rfc2131 compliant on あるいは use-clientid 機能を使用するよう設定されていなければならない。また dhcp server rfc2131 compliant off あるいは use-clientid 機能が使用されないよう設定された時点で、コマンドの第 2 の書式によるもの以外の予約は消去される。
- コマンドの第 1 の書式でのクライアント識別子は、クライアントがオプションで送ってくる値を設定する。*type* パラメータを省略した場合には、*type* フィールドの値も含めて入力する。*type* パラメータにキーワードを指定する場合には *type* フィールド値は一意に決定されるので Client-Identifier フィールドの値のみを入力する。
- コマンドの第 2 の書式による MAC アドレスでの予約は、クライアントの識別に DHCP パケットの chaddr フィールドを用いる。この形の予約機能は、RT の設定が dhcp server rfc2131 compliant off あるいは use-clientid 機能を使用しない設定になっているか、もしくは DHCP クライアントが DHCP パケット中に Client-Identifier オプションを付けてこない場合でないとは動作しない。
- クライアントが Client-Identifier オプションを使う場合、コマンドの第 2 の書式での予約は、dhcp server 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-Identifer 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られ、Client-Identifier オプションが存在する場合にはこの設定は無視される

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

すなわち、リースしているクライアントとして MAC アドレスが表示されていれば Client-Identifier オプションは使用されておらず、16 進文字列あるいは文字列でクライアントが表示されていれば、Client-Identifier オプションが使われている。この場合、Client-Identifier オプションを使うクライアントへの予約は、ここで表示される 16 進文字列あるいは文字列を使用する。

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

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

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

なお、クライアントとの相互作用に関して下記の留意点がある。

個々の機能を単独で用いるとクライアント側の思わぬ動作を招く可能性があるため、dhcp server rfc2131 compliant on あるいは dhcp server rfc2131 compliant off で使用することを推奨する。

ルータの再起動、スコープの再設定などでリース情報が消去されている場合、アドレス延長要求時、あるいはリース期間内のクライアントの再起動時、クライアントの使用する IP アドレスが変わることがある。

これを防ぐために 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、RT がリース情報を持たないクライアントからの DHCPREQUEST に DHCPNAK を返さず無視する。

この結果、リース期限満了時にクライアントが出す DHCPDISCOVER に Requested IP Address オプションが含まれていれば、そのクライアントには引き続き同じ IP アドレスをリースできる。

## 9.5 DHCP オプションの設定

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

[ パラメータ ] *scope\_num*.....スコープ番号 (1..65535)  
*option*..... オプション番号 (1..49,64..76,128..254) またはニーモニック  
主なニーモニック

router	3
dns	6
hostname	12
domain	15
wins_server	44

*value* ..... オプション値

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

1 オクテット整数	0..255
2 オクテット整数	0..65535
2 オクテット数の配列	2 オクテット整数をコンマ (,) で並べたもの
4 オクテット整数	0..4294967295
IP アドレス	IP アドレス
IP アドレスの配列	IP アドレスをコンマ (,) で並べたもの
文字列	文字列
スイッチ	"on", "off", "1", "0" のいずれか
バイナリ	2 桁 16 進数をコンマ (,) で並べたもの

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

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

## 9.6 リースする IP アドレスの重複をチェックするか否かの設定

---

[入力形式]	dhcp duplicate check <i>check1 check2</i> no dhcp duplicate check
[パラメータ]	<i>check1</i> ..... 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 <i>check2</i> ..... LAN 外 (DHCP リレーエージェント経由) を対象とするチェックの確認用待ち時間 ミリ秒 (1..3000) off..... LAN 外 (DHCP リレーエージェント経由) を対象とするチェックを行わない
[説明]	DHCP サーバとして機能する場合、IP アドレスを DHCP クライアントにリースする直前に、その IP アドレスを使っているホストが他にいないことをチェックするか否かを設定する。
[ノート]	LAN 内のスコープに対しては ARP を、DHCP リレーエージェント経由のスコープに対しては PING を使ってチェックする。
[デフォルト値]	<i>check1</i> = 100 <i>check2</i> = 500

## 9.7 DHCP サーバの指定の設定

---

[入力形式]	dhcp relay server <i>host</i> [ <i>host...</i> ] no dhcp relay server [ <i>host</i> [ <i>host...</i> ]]
[パラメータ]	<i>host1..host4</i> ..... DHCP サーバの IP アドレス
[説明]	DHCP BOOTREQUEST パケットを中継するサーバを最大 4 つまで設定する。 サーバが複数指定された場合は、BOOTREQUEST パケットを複製してすべてのサーバに中継するか、あるいは 1 つだけサーバを選択して中継するかは dhcp relay select コマンドの設定で決定される。

## 9.8 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]	<i>type</i> 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 chaddr フィールドを引数とするので、同一の DHCP クライアントに対しては常に同じサーバ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

## 9.9 DHCP BOOTREQUEST パケットの中継基準の設定

---

[入力形式]	dhcp relay threshold <i>time</i> no dhcp relay threshold [ <i>time</i> ]
[パラメータ]	<i>time</i> ..... 秒数 (0..65535)
[説明]	DHCP BOOTREQUEST パケットの secs フィールドとこのコマンドによる秒数を比較し、設定値より小さな secs フィールドを持つ DHCP BOOTREQUEST パケットはサーバに中継しないようにする。 これにより、同一 LAN 上に別の DHCP サーバがあるにも関わらず遠隔地の DHCP サーバにパケットを中継してしまうのを避けることができる。
[デフォルト値]	0

## 10. ICMP の設定

### 10.1 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

### 10.2 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

### 10.3 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 ] on

### 10.4 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

### 10.5 ICMP Redirect 受信時の処理の設定

---

- [ 入力形式 ] ip icmp redirect receive *action*  
no ip icmp redirect receive [*action*]
- [ パラメータ ] *action*  
on.....処理する  
off.....無視する
- [ 説明 ] ICMP Redirect を受信した場合に、それを処理して自分の経路テーブルに反映させるか、あるいは無視するかを設定する。
- [ デフォルト値 ] off

## 10.6 ICMP Time Exceeded を送信するか否かの設定

---

- [入力形式]      ip icmp time-exceeded send *send*  
                   no ip icmp time-exceeded send [*send*]
- [パラメータ]    *send*  
                   on ..... 送信する  
                   off ..... 送信しない
- [説明]            受信した IP パケットの TTL が 0 になってしまったため、そのパケットを破棄した場合に、同時にパケットの送信元に対して ICMP Time Exceeded を送信するか否かを設定する。
- [デフォルト値]  on

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

---

- [入力形式]      ip icmp timestamp-reply send *send*  
                   no ip icmp timestamp-reply send [*send*]
- [パラメータ]    *send*  
                   on ..... 送信する  
                   off ..... 送信しない
- [説明]            ICMP Timestamp を受信した場合に、ICMP Timestamp Reply を返すか否かを設定する。
- [デフォルト値]  on

## 10.8 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]    *send*  
                   on ..... 送信する  
                   off ..... 送信しない
- [説明]            経路テーブルに宛先が見つからない場合や、あるいは ARP が解決できなくて IP パケットを破棄することになった場合に、同時にパケットの送信元に対して ICMP Destination Unreachable を送信するか否かを設定する。
- [デフォルト値]  on

## 10.9 受信した ICMP のログを記録するか否かの設定

---

- [入力形式]      ip icmp log *log*  
                   no ip icmp log [*log*]
- [パラメータ]    *log*  
                   on ..... 記録する  
                   off ..... 記録しない
- [説明]            受信した ICMP を debug タイプのログに記録するか否かを設定する。
- [デフォルト値]  on

## 11. フレームリレー関連の設定

本機は、アクセス回線として BRI/PRI を利用した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 HDLC<sup>1</sup> 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。

DLCI<sup>2</sup> 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 PVC<sup>3</sup> 状態確認手順の LMI<sup>4</sup> 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 InARP<sup>5</sup> です。InARP を使用するかどうかは `fr inarp` コマンドで設定します。

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

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

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

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

このデータ圧縮機能を使用するか否かは `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、1 BRI モデルでは leased インタフェースが代表となり、それ以外のモデルでは最も若い PP インタフェースが代表となります。

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

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

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

### 11.1 カプセル化の種類の設定

[ 入力形式 ]	<code>pp encapsulation <i>type</i></code> <code>no pp encapsulation [<i>type</i>]</code>
[ パラメータ ]	<i>type</i> 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

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



## 11.2 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]	<i>dlci_num</i> 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

## 11.3 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]	<i>lmi</i> 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

## 11.4 InARP 使用の設定

---

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

## 11.5 フレームリレーダウン時にバックアップする相手先情報番号の設定

---

[入力形式]	fr backup dlc= <i>dlci_num</i> <i>peer_num</i> no fr backup dlc= <i>dlci_num</i> [ <i>peer_num</i> ]
[パラメータ]	<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。

## 11.6 FR 圧縮機能の設定

---

[ 入力形式 ]	fr compression use dci= <i>dci_num</i> <i>type</i> no fr compression use dci= <i>dci_num</i> [ <i>type</i> ]
[ パラメータ ]	<i>dci_num</i> DLCI 値 (16..991) * (すべてのデータリンク) <i>type</i> 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>dci_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

## 11.7 DLCI ごとのパラメータの設定

---

[ 入力形式 ]	fr cir dci= <i>dci_num</i> <i>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 dci= <i>dci_num</i> [ <i>cir</i> []]
[ パラメータ ]	<i>dci_num</i> ..... DLCI 値 (16..991) <i>cir</i> ..... CIR 値 (bit/s 単位) <i>idl</i> ..... スロースタート状態に戻るまでのアイドル時間 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 bc= <i>be</i> = 7000 <i>s</i> = <i>cir</i> / <i>bc_size</i> / <i>be_size</i> から計算される値

## 11.8 輻輳制御をするか否かの設定

---

[ 入力形式 ]	fr congestion control <i>control</i> no fr congestion control [ <i>control</i> ]
[ パラメータ ]	<i>control</i> 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

## 11.9 回線に対する送信順序方式の設定

[入力形式]	fr pp dequeue type <i>type</i> no fr pp dequeue type [ <i>type</i> ]
[パラメータ]	<i>type</i> 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。1BRI モデルでは、これに加えて、leased が最も高い順位を持つものと定義する。
[デフォルト値]	round-robin

## 11.10 指定パケットに DE ビットを立てるか否かの設定

[入力形式]	fr de <i>protocol</i> filter dci= <i>dci_num</i> <i>filter_num_list</i> no fr de <i>protocol</i> filter dci= <i>dci_num</i> [ <i>filter_num_list</i> ]
[パラメータ]	<i>protocol</i> ip ..... IP パケット ipx ..... IPX パケット bridge ..... ブリッジするパケット <i>filter</i> ..... 固定のキーワード <i>dci_num</i> DLCI 値 (16..991) * (すべてのデータリンク) <i>filter_num_list</i> ..... 静的フィルタ番号 (1..100) の列
[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

## 12. PRI 関連の設定

RT300i は、オプションの PRI 拡張モジュールを装着することにより一次群速度インタフェース (PRI:Primary Rate Interface) に対応します。多重化非対応の PRI 拡張モジュール (製品番号: YBA-1PRI-N) は、多重化されていない 192kbit/s ~ 1.5Mbit/s の高速デジタル専用線や DA1500、およびフレームリレーサービスなどに最適です。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 対地まで多重化された高速デジタル専用線や、INS1500 を利用することができます。

RT140p は、標準で一次群速度インタフェースに対応しており、オプションの多重化ソフトウェア (YMS15P) を追加することにより、最大 24 対地まで多重化された高速デジタル専用線や、INS1500 を利用することができます。

PRI 専用線を使用するには、PRI ネットワーク提供者との契約で指定された情報チャンネルやタイムスロットなどを `pri leased channel` コマンドで設定します。PRI を通じてパケットをやりとりするためには、`pp bind` コマンドで相手先情報番号と関連付けます。

また、現在の PRI 関連の情報は `show status pri` コマンドで確認することができます。

PRI 専用線に対して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で折り返して、送信データと折り返されたデータを比較して正常性の検証を行います。

ループバックポイントは、主にハードウェアに対して行うループバック A と回線上にデータを流して折り返し試験を行うタイムスロットループバックがあります。

ループバック A では試験ルータの PRI コネクタ部分で折り返し、タイムスロットループバックでは指定したタイムスロットを使用して相手ルータからデータを折り返し受信します。

ループバックを実行するには、コンソールコマンドから実行します。ループバック試験を行う前に、通常の通信を `pp disable` コマンド等で停止させてから行います。

タイムスロットループバックでは、相手側ルータは `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。

なお、ループバック試験中のメッセージはデータ送信側のコンソールにだけ表示されます。

### 12.1 PRI 回線の種類の設定

[ 入力形式 ]	<code>line type <i>interface type</i></code> <code>no line type <i>interface type</i></code>
[ パラメータ ]	<code><i>interface</i>.....PRI インタフェース名</code> <code><i>type</i></code> <code><i>isdn</i> <i>isdn-ntt</i>.....ISDN 回線交換</code> <code><i>leased</i>.....デジタル専用線</code>
[ 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 <code>interface reset</code> コマンドの発行により反映される。
[ デフォルト値 ]	<code>leased</code>

### 12.2 情報チャンネルとタイムスロットの設定

[ 入力形式 ]	<code>pri leased channel <i>pri/info timeslot_head timeslot_num</i></code> <code>no pri leased channel <i>pri/info [timeslot_head timeslot_num]</i></code>
[ パラメータ ]	<code><i>pri</i>.....PRI インタフェース名</code> <code><i>info</i>.....情報チャンネル番号 (1..24)</code> <code><i>timeslot_head</i>.....先頭タイムスロット番号 (1..24)</code> <code><i>timeslot_num</i>.....タイムスロット数 (1..24)</code>

以下の二ーモニックが使用可能

二ーモニック速度 (bit/s)	タイムスロット数
64k	1
128k	2
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] 同じ情報チャンネルに対する設定を変更するには、あらかじめ `no pri leased channel` で設定を削除しておく必要がある。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。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の設定はできない。

### 12.3 PP で使用するインタフェースの設定

---

- [入力形式] `pp bind interface/pri_num [interface/info]`  
`no pp bind [interface/info]`
- [パラメータ] `interface` ..... PRI インタフェース名  
`pri_num` ..... インタフェース番号  
`info` ..... 情報チャンネル番号
- [説明] 選択されている相手先に対して実際に使用するインタフェースを設定する。
- [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
- [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。

## 13. IPsec の設定

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

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

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

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

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

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

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

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

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

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

リビジョン系列	IPsec リリース 1	IPsec リリース 2	IPsec リリース 3
3.00	3.00.09 ~ 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 ~

### 13.1 事前共有鍵の登録

[ 入力形式 ]	<code>ipsec ike pre-shared-key gateway_id key</code> <code>ipsec ike pre-shared-key gateway_id text text</code> <code>no ipsec ike pre-shared-key gateway_id [...]</code>
[ パラメータ ]	<i>gateway_id</i> ..... セキュリティ・ゲートウェイの識別子 (1..20) <i>key</i> ..... 鍵となる 0x で始まる 16 進数列 (最大 32 バイト) <i>text</i> ..... ASCII 文字列で表した鍵 (最大 32 文字)
[ 説明 ]	鍵交換に必要な事前共有鍵を登録する。この設定されていない場合には、鍵交換は行われず。 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 ]	<code>ipsec ike pre-shared-key 1 text himitsu</code> <code>ipsec ike pre-shared-key 8 0xCDEEDC0CEDCD</code>

### 13.2 相手側セキュリティ・ゲートウェイの IP アドレスの設定

---

- [入力形式] ipsec ike remote address *gateway\_id ip\_address*  
no ipsec ike remote address *gateway\_id [ip\_address]*
- [パラメータ] *gateway\_id*..... セキュリティ・ゲートウェイの識別子 (1..20)  
*ip\_address*  
相手側セキュリティ・ゲートウェイの IP アドレス  
any..... 自動選択
- [説明] 相手側セキュリティ・ゲートウェイの IP アドレスを設定する。相手側セキュリティ・ゲートウェイ 1 つに対して 1 つ設定可能である。

### 13.3 相手側のセキュリティゲートウェイの名前の設定

---

- [入力形式] ipsec ike remote name *gateway name*  
no ipsec ike remote name *gateway [name]*
- [パラメータ] *gateway* ..... セキュリティゲートウェイの識別子 (1..20)  
*name* ..... 名前 (最大 32 文字)
- [説明] 相手側のセキュリティゲートウェイの名前を設定する。

### 13.4 自分側セキュリティ・ゲートウェイの IP アドレスの設定

---

- [入力形式] ipsec ike local address *gateway\_id ip\_address*  
ipsec ike local address *gateway\_id vrrp interface vrid*  
no ipsec ike local address *gateway\_id [ip\_address]*
- [パラメータ] *gateway\_id*..... セキュリティ・ゲートウェイの識別子 (1..20)  
*ip\_address*  
自分側セキュリティ・ゲートウェイの IP アドレス  
any..... 自動選択  
*interface* ..... LAN インタフェース名  
*vrid*..... VRRP グループ ID (1..255)
- [説明] 自分側セキュリティ・ゲートウェイの IP アドレスを設定する。  
vrrp タイプの指定方式では、VRRP マスターとして動作している場合のみ、指定した LAN インタフェース / VRRP グループ ID の仮想 IP アドレスを自分側 セキュリティ・ゲートウェイアドレスとして利用する。VRRP マスターでない場合には鍵交換は行わない。
- [ノート] 本コマンドが設定されていない場合には、相手側のセキュリティ・ゲートウェイに近いインタフェースの IP アドレスを用いて IKE を起動する。

### 13.5 自分側のセキュリティゲートウェイの名前の設定

---

- [入力形式] ipsec ike local name *gateway\_id name*  
no ipsec ike local name *gateway\_id [name]*
- [パラメータ] *gateway\_id* ..... セキュリティゲートウェイの識別子 (1..20)  
*name* ..... 名前 (最大 32 文字)
- [説明] 自分側のセキュリティゲートウェイの名前を設定する。

### 13.6 鍵交換の再送回数と間隔の設定

---

- [入力形式] ipsec ike retry *count interval*  
no ipsec ike retry [*count interval*]
- [パラメータ] *count* ..... 再送回数 (1..50)  
*interval* ..... 再送間隔の秒数 (1..100)
- [説明] 鍵交換が失敗した場合に鍵交換を繰り返す回数とその時間間隔を設定する。
- [デフォルト値] *count* = 10  
*interval* = 5

### 13.7 IKE が用いる暗号アルゴリズムの設定

---

- [ 入力形式 ]    ipsec ike encryption *gateway\_id algorithm*  
no ipsec ike encryption *gateway\_id [algorithm]*
- [ パラメータ ]    *gateway\_id* ..... セキュリティ・ゲートウェイの識別子 (1..20)  
*algorithm* ..... 暗号アルゴリズム  
          3des-cbc ..... 3DES-CBC  
          des-cbc ..... DES-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、DES-CBC と 3DES-CBC を用いることができる。
- [ デフォルト値 ]    des-cbc

### 13.8 IKE が用いるグループの設定

---

- [ 入力形式 ]    ipsec ike group *gateway\_id group [group]*  
no ipsec ike group *gateway\_id [group [group]]*
- [ パラメータ ]    *gateway\_id* ..... セキュリティ・ゲートウェイの識別子 (1..20)  
*group* ..... グループ識別子  
          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

### 13.9 IKE が用いるハッシュアルゴリズムの設定

---

- [ 入力形式 ]    ipsec ike hash *gateway\_id algorithm*  
no ipsec ike hash *gateway\_id [algorithm]*
- [ パラメータ ]    *gateway\_id* ..... セキュリティ・ゲートウェイの識別子 (1..20)  
*algorithm* ..... ハッシュアルゴリズム  
          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

### 13.10 自分側の ID の設定

---

- [ 入力形式 ]    ipsec ike local id *gateway\_id ip\_address[/mask]*  
no ipsec ike local id *gateway\_id [ip\_address[/mask]]*
- [ パラメータ ]    *gateway\_id* ..... セキュリティ・ゲートウェイの識別子 (1..20)  
*ip\_address* ..... IP アドレス  
*mask* ..... ネットマスク
- [ 説明 ]        IKE のフェーズ 2 で用いる自分側の ID を設定する。
- [ ノート ]        このコマンドが設定されていない場合には、ID を送信しない。*mask* パラメータを省略した場合は、タイプ 1 の ID が送信される。また、*mask* パラメータを指定した場合は、タイプ 4 の ID が送信される。



### 13.11 IKE のログの種類の設定

---

- [入力形式]     ipsec ike log *gateway\_id type* [*type*]  
                   no ipsec ike log *gateway\_id* [*type*]
- [パラメータ]    *gateway\_id*..... セキュリティ・ゲートウェイの識別子 (1..20)  
                   *type* ..... 出力するログの種類  
                   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、syslog の debug レベルで出力される。
- [ノート]         このコマンドが設定されていない場合には、最小限のログしか出力しない。複数の *type* パラメータを設定することもできる。

### 13.12 IKE ペイロードのタイプの設定

---

- [入力形式]     ipsec ike payload type *gateway\_id type*  
                   no ipsec ike payload type *gateway\_id* [*type*]
- [パラメータ]    *gateway\_id*..... セキュリティ・ゲートウェイの識別子 (1..20)  
                   *type* ..... ペイロードのタイプ  
                   1..... IPsec リリース 2 以前  
                   2..... IPsec リリース 3
- [説明]           IKE ペイロードのタイプを設定する。YAMAHA リモートルータの古いリビジョンと接続する場合には、タイプを 1 に設定する必要がある。
- [デフォルト値]  2

### 13.13 PFS を用いるか否かの設定

---

- [入力形式]     ipsec ike pfs *gateway\_id pfs*  
                   no ipsec ike pfs *gateway\_id* [*pfs*]
- [パラメータ]    *gateway\_id*..... セキュリティ・ゲートウェイの識別子 (1..20)  
                   *pfs*  
                   on ..... 用いる  
                   off..... 用いない
- [説明]           IKE で PFS 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

### 13.14 相手側の ID の設定

---

- [入力形式]     ipsec ike remote id *gateway\_id ip\_address*[/*mask*]  
                   no ipsec ike remote id *gateway\_id* [*ip\_address*[/*mask*]]
- [パラメータ]    *gateway\_id*..... セキュリティ・ゲートウェイの識別子 (1..20)  
                   *ip\_address*..... IP アドレス  
                   *mask*..... ネットマスク
- [説明]           IKE のフェーズ 2 で用いる相手側の ID を設定する。
- [ノート]         このコマンドが設定されていない場合には ID を送信しない。  
                   *mask* パラメータを省略した場合は、タイプ 1 の ID が送信される。また、*mask* パラメータを指定した場合は、タイプ 4 の ID が送信される。

## 13.15 IKE の情報ペイロードを送信するか否かの設定

---

[ 入力形式 ]	ipsec ike send info <i>gateway_id</i> <i>info</i> no ipsec ike send info <i>gateway_id</i> [ <i>info</i> ]
[ パラメータ ]	<i>gateway_id</i> ..... セキュリティ・ゲートウェイの識別子 (1..20) <i>info</i> 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

## 13.16 SA 関連の設定

再起動されるとすべての SA がクリアされることに注意しなくてはならない。

## 13.16.1 SA のポリシーの定義

---

[ 入力形式 ]	ipsec sa policy <i>policy_id</i> <i>gateway_id</i> ah <i>ah_algorithm</i> ipsec sa policy <i>policy_id</i> <i>gateway_id</i> esp <i>esp_algorithm</i> [ <i>ah_algorithm</i> ] no ipsec sa policy <i>policy_id</i> [ <i>gateway_id</i> ]
[ パラメータ ]	<i>policy_id</i> ..... ポリシー ID (1..255) <i>gateway_id</i> ..... セキュリティ・ゲートウェイの識別子 (1..20) 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 <i>ah_algorithm</i> md5-hmac ..... HMAC-MD5 sha-hmac ..... HMAC-SHA <i>esp_algorithm</i> 3des-cbc ..... 3DES-CBC des-cbc ..... DES-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。

## 13.16.2 IPsec SA の寿命の設定

---

[ 入力形式 ]	ipsec ike duration ipsec-sa <i>gateway_id</i> <i>second</i> [ <i>kbytes</i> ] no ipsec ike duration ipsec-sa <i>gateway_id</i> [ <i>second</i> [ <i>kbytes</i> ]]
[ パラメータ ]	<i>gateway_id</i> ..... セキュリティ・ゲートウェイの識別子 (1..20) <i>second</i> ..... 秒数 (300..691200) <i>kbytes</i> ..... キロ単位のバイト数 (100..100000)
[ 説明 ]	IKE で提案する IPsec SA の寿命を設定する。 <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。
[ デフォルト値 ]	28800

## 13.16.3 ISAKMP SA の寿命の設定

---

[ 入力形式 ]	ipsec ike duration isakmp-sa <i>gateway_id</i> <i>second</i> [ <i>kbytes</i> ] no ipsec ike duration isakmp-sa <i>gateway_id</i> [ <i>second</i> [ <i>kbytes</i> ]]
[ パラメータ ]	<i>gateway_id</i> ..... セキュリティ・ゲートウェイの識別子 (1..20) <i>second</i> ..... 秒数 (300..691200) <i>kbytes</i> ..... キロ単位のバイト数 (100..100000)
[ 説明 ]	IKE で提案する ISAKMP SA の寿命を設定する。 <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。
[ デフォルト値 ]	28800

#### 13.16.4 SA の削除

---

- [入力形式] ipsec sa delete *id*
- [パラメータ] *id*
- [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。

#### 13.16.5 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。

#### 13.16.6 SA を自動更新するか否かの設定

---

- [入力形式] ipsec auto refresh *refresh*  
no ipsec auto refresh [*refresh*]
- [パラメータ] *refresh*  
on ..... 自動更新する  
off ..... 自動更新しない
- [説明] SA を自動更新するか否かを設定する。
- [ノート] 古い SA を削除せずに新しい SA を生成する。
- [デフォルト値] off

### 13.17 トンネルインタフェース関連の設定

---

#### 13.17.1 使用する SA のポリシーの設定

---

- [入力形式] ipsec tunnel *policy\_id*  
no ipsec tunnel [*policy\_id*]
- [パラメータ] *policy\_id*..... 整数 (1..255)
- [説明] 選択されているトンネルインタフェースで使用する SA のポリシーを設定する。
- [デフォルト値] SA のポリシーは設定されていない

## 13.17.2 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 ]     *type*  
          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ことになり、ほとんど効果が無い。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、一定の効果が得られる。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、例えば本機の出力インタフェースが LAN であってもデータ圧縮効果を期待できる。
- [ デフォルト値 ]   none

## 13.17.3 トンネルインタフェースの使用許可の設定

- [ 入力形式 ]     tunnel enable *tunnel\_num*  
no tunnel enable
- [ パラメータ ]     *tunnel\_num*  
          トンネルインタフェース番号 (1..20)  
          all.....すべてのトンネルインタフェース
- [ 説明 ]           トンネルインタフェースを使用できる状態にする。  
工場出荷時は、すべてのトンネルインタフェースは disable 状態であり、使用する場合は本コマンドにより、インタフェースを有効にしなければならない。

## 13.17.4 トンネルインタフェースの使用不許可の設定

- [ 入力形式 ]     tunnel disable *tunnel\_num*
- [ パラメータ ]     *tunnel\_num*  
          トンネルインタフェース番号 (1..20)  
          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、disable 状態で行うのが望ましい。

## 13.17.5 トンネルインタフェース番号の選択

- [ 入力形式 ]     tunnel select *tunnel\_num*
- [ パラメータ ]     *tunnel\_num*  
          トンネルインタフェース番号 (1..20)  
          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六できない。

## 13.18 トランスポートモード関連の設定

## 13.18.1 トランスポートモードの定義

---

[入力形式]	<code>ipsec transport <i>id</i> <i>policy_id</i> [<i>proto</i> [<i>src_port_list</i> [<i>dst_port_list</i>]]]</code> <code>no ipsec transport <i>id</i> [<i>policy_id</i> [<i>proto</i> [<i>src_port_list</i> [<i>dst_port_list</i>]]]]</code>
[パラメータ]	<i>id</i> ..... トランスポート ID (1..255) <i>policy_id</i> ..... ポリシー ID (1..255) <i>proto</i> ..... プロトコル <i>src_port_list</i> ..... UDP、TCP のソースポート番号列 ポート番号を表す 10 進数 ポート番号を表す二進モニック * (すべてのポート) <i>dst_port_list</i> ..... UDP、TCP のデスティネーションポート番号列 ポート番号を表す 10 進数 ポート番号を表す二進モニック * (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、 <i>proto</i> 、 <i>src_port_list</i> 、 <i>dst_port_list</i> 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

## 14. SNMP の設定

### 14.1 読み出し専用のコミュニティ名の設定

---

- [ 入力形式 ]     snmp community read-only *name*  
no snmp community read-only [*name*]
- [ パラメータ ]     *name*..... SNMP によるアクセスモードが読み出し専用であるコミュニティ名
- [ 説明 ]           SNMP によるアクセスモードが読み出し専用であるコミュニティ名を設定する。名称は 1 文字以上 16 文字以内。
- [ デフォルト値 ]   public

### 14.2 読み書き可能なコミュニティ名の設定

---

- [ 入力形式 ]     snmp community read-write *name*  
no snmp community read-write [*name*]
- [ パラメータ ]     *name*..... SNMP によるアクセスモードが読み書き可能であるコミュニティ名
- [ 説明 ]           SNMP によるアクセスモードが読み書き可能であるコミュニティ名を設定する。名称は 1 文字以上 16 文字以内。
- [ デフォルト値 ]   空文字列

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

---

- [ 入力形式 ]     snmp enableauthentraps *send*  
no snmp enableauthentraps [*send*]
- [ パラメータ ]     *send*  
                  on.....送信する  
                  off.....送信しない
- [ 説明 ]           MIB 変数 snmpEnableAuthenTraps を設定する。  
これを off にすると、誤ったコミュニティ名を持つパケットを受信した場合にトラップを送信しない。SNMP トラップは snmp trap host コマンドで指定されたホストに対して送信される。
- [ デフォルト値 ]   on

### 14.4 SNMP によるアクセスを許可するホストの設定

---

- [ 入力形式 ]     snmp host *host*  
no snmp host [*host*]
- [ パラメータ ]     *host*  
                  IP アドレス .....SNMP によるアクセスを許可するホストの IP アドレス  
                  any.....すべてのホストから SNMP によりアクセスできる  
                  none .....すべてのホストから SNMP によりアクセスできない
- [ 説明 ]           SNMP によるアクセスを許可するホストを設定する。
- [ デフォルト値 ]   none

### 14.5 sysContact の設定

---

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

## 14.6 sysLocation の設定

---

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

## 14.7 sysName の設定

---

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

## 14.8 SNMP トラップのコミュニティ名の設定

---

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

## 14.9 SNMP トラップの送信先の設定

---

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

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

---

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

## 14.11 PP インタフェースのアドレスの強制表示の設定

[ 入力形式 ]	snmp display ipcp force <i>sw</i> no snmp display ipcp force
[ パラメータ ]	<p><i>sw</i></p> <p>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</p> <p>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</p>
[ 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 に設定しておくこと、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



## 15. RADIUS の設定

### 15.1 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]	<i>auth</i> 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 < <a href="http://www.rtpro.yamaha.co.jp">http://www.rtpro.yamaha.co.jp</a> > を参照すること。
[デフォルト値]	off

### 15.2 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]	<i>account</i> 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 < <a href="http://www.rtpro.yamaha.co.jp">http://www.rtpro.yamaha.co.jp</a> > を参照すること。
[デフォルト値]	off

### 15.3 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]	<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。 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。

### 15.4 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]	<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。

### 15.5 RADIUS アカウントサーバの指定

---

- [ 入力形式 ]      `radius account server ip1 [ip2]`  
                   `no radius account server [ip1 [ip2]]`
- [ パラメータ ]      `ip1` .....RADIUS アカウントサーバ ( 正 ) の IP アドレス ( IPv6 アドレス可 )  
                   `ip2` .....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。

### 15.6 RADIUS 認証サーバの UDP ポートの設定

---

- [ 入力形式 ]      `radius auth port port_num`  
                   `no radius auth port [port_num]`
- [ パラメータ ]      `port_num` .....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 ]          新しい RFC 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

### 15.7 RADIUS アカウントサーバの UDP ポートの設定

---

- [ 入力形式 ]      `radius account port port_num`  
                   `no radius account port [port_num]`
- [ パラメータ ]      `port_num` .....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 ]          新しい RFC 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

### 15.8 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。

### 15.9 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`

## 16. NAT 機能

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

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

本機では、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。

### 16.1 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]	ip <i>interface</i> nat descriptor <i>nat_descriptor_list</i> no ip <i>interface</i> nat descriptor [ <i>nat_descriptor_list</i> ]
[パラメータ]	<i>interface</i> ..... LAN インタフェース名、または、pp、tunnel <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 LAN 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。

### 16.2 NAT ディスクリプタの動作タイプの設定

[入力形式]	nat descriptor type <i>nat_descriptor type</i> no nat descriptor type [ <i>nat_descriptor type</i> ]
[パラメータ]	<i>nat_descriptor</i> ..... NAT ディスクリプタ番号 (1..21474836) <i>type</i> ..... NAT ディスクリプタの動作タイプ none ..... NAT 変換機能を利用しない nat ..... 動的 NAT 変換と静的 NAT 変換を利用 masquerade ..... 静的 NAT 変換と IP マスカレード変換 nat-masquerade..... 動的 NAT 変換と静的 NAT 変換と IP マスカレード変換
[説明]	NAT 変換の動作タイプを指定する。
[ノート]	nat-masquerade は、動的 NAT 変換できなかったパケットを IP マスカレード変換で救う。例えば、外側アドレスが 16 個利用可能な場合は先勝ちで 15 個 NAT 変換され、残りは IP マスカレード変換される。
[デフォルト値]	none

### 16.3 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 |
|------------------|-----|----|------|
| <i>ipcp</i>      | x   |    | x    |
| <i>primary</i>   |     | x  | x    |
| <i>secondary</i> |     | x  | x    |
| IP アドレス          |     |    |      |
- [ デフォルト値 ]   *ipcp*

### 16.4 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らを任意に並べたもの  
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*

### 16.5 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。

## 16.6 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]	<i>nat_descriptor</i> ..... NAT ディスクリプタ番号 (1..21474836) <i>use</i> 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

## 16.7 静的 IP マスカレードエントリの設定

[入力形式]	nat descriptor masquerade static <i>nat_descriptor id inner_ip protocol port</i> no nat descriptor masquerade static <i>nat_descriptor id [inner_ip protocol port]</i>
[パラメータ]	<i>nat_descriptor</i> ..... NAT ディスクリプタ番号 (1..21474836) <i>id</i> ..... 静的 IP マスカレードエントリの識別情報 (1 以上の数値) <i>inner_ip</i> ..... 内側 IP アドレス (1 個) <i>protocol</i> ..... 対象プロトコル 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>port</i> ..... 固定するポート番号 (ニーモニック) または、ポート番号の範囲指定
[説明]	IP マスカレードによる通信でポート番号変換を行わないようにポートを固定する。

## 16.8 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 [time]</i>
[パラメータ]	<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)
[説明]	動的に生成された NAT 管理テーブルから自動的に消去されるまでの時間を設定する。
[デフォルト値]	900

## 16.9 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]	<i>type</i> ..... TTL を同期させる方法 all..... すべてのコネクションを対象とする ftp..... FTP の制御チャンネルのみを対象とする
[説明]	本コマンドによって IP マスカレードテーブルの TTL の扱いを制御することができる。通常、テーブルの TTL は単調に減少するが、FTP のように制御チャンネルとデータチャンネルからなるアプリケーションでは、制御チャンネルに対応するテーブルをデータ転送中に削除するべきではないため、制御チャンネルとデータチャンネルの両テーブルの TTL を同期させている。 ただし、現時点では制御チャンネルとデータチャンネルの対応を把握することが難しいため、同じホスト間の通信について、すべてのコネクションを関係づけ TTL を同期させている。しかし、このような動作では、多くのテーブルの TTL が同期し多くのテーブルが長く残留するという現象が起きる。 さらに、状況によっては、ルータのメモリが枯渇する可能性もあるため、この処理を FTP の制御チャンネルに限定し、メモリの枯渇を予防する選択肢を設ける。TTL の同期を FTP の制御チャンネルに限定する場合には、パラメータに ftp を設定する。FTP に限定せず、従来と同じように動作させるためには、パラメータに all を設定する。
[デフォルト値]	all

### 16.10 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設定します。
  
- [ デフォルト値 ]  off

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

リカーシブサーバ機能は、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。

### 17.1 DNS サーバの IP アドレスの設定

---

[入力形式]	dns server ip_address [ <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

### 17.2 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つたり、接続できても DNS サーバの通知がなかった場合には名前解決は行われない。 dns server コマンドで DNS サーバが明示的に指定されている場合には、そちらの設定が優先される。dns server コマンドに指定したサーバから返事がない場合には、相手先への接続と DNS サーバの通知取得が行われる。
[ノート]	この機能を使用する場合には、dns server pp コマンドで指定された相手先情報に、ppp ipcp 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

## 17.3 DNS 問い合わせの内容に応じた DNS サーバの選択

[ 入力形式 ]	<pre>dns server select <i>id</i> server [<i>type</i>] <i>query</i> [<i>original-sender</i>][restrict pp <i>connection-pp</i>] dns server select <i>id</i> pp <i>pp_num</i> [<i>default-server</i>] [<i>type</i>] <i>query</i> [<i>original-sender</i>] [restrict pp <i>connection-pp</i>] no dns server select <i>id</i></pre>
[ パラメータ ]	<pre><i>id</i> ..... DNS サーバ選択テーブルの番号 <i>server</i> ..... DNS サーバの IP アドレス <i>type</i> ..... DNS レコードタイプ (省略時は a)   a ..... ホストの IP アドレス   ptr ..... IP アドレスの逆引き用のポインタ   mx ..... メールサーバ   ns ..... ネームサーバ   cname ..... 別名   any ..... すべてのタイプにマッチする <i>query</i> ..... DNS 問い合わせの内容   <i>type</i> が a、mx、ns、cname の場合     <i>query</i> はドメイン名を表す文字列であり、後方一致とする。例えば、"yamaha.co.jp"であれば、comm.yamaha.co.jp、rtpro.yamaha.co.jp などにマッチする。   <i>type</i> が ptr の場合     <i>query</i> は IP アドレス (<i>ip_address</i>[/<i>masklen</i>]) であり、<i>masklen</i> を省略したときは IP アドレスにのみマッチし、<i>masklen</i> を指定したときはネットワークアドレスに含まれるすべての IP アドレスにマッチする。DNS 問い合わせに含まれる .in-addr.arpa ドメインで記述された FQDN は、IP アドレスへ変換された後に比較される。 <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番号 <i>pp_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番号 <i>default-server</i> ..... <i>pp_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</pre>
[ 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>

## 17.4 DNS ドメイン名の設定

[ 入力形式 ]	<pre>dns domain <i>domain_name</i> no dns domain [<i>domain_name</i>]</pre>
[ パラメータ ]	<pre><i>domain_name</i> ..... DNS ドメインを表す文字列</pre>
[ 説明 ]	<p>ルータが所属する DNS ドメインを設定する。名前解決に失敗した場合、このドメイン名を補完して再度解決を試みる。ルータが DHCP サーバとして機能する場合、設定したドメイン名は DHCP クライアントに通知するためにも使用される。ルータのあるネットワークおよびそれが含むサブネットワークの DHCP クライアントに対して通知する。空文字列を設定する場合には、dns domain とだけ入力する。</p>

## 17.5 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 ]	<pre>dns private address spoof <i>spoof</i> no dns private address spoof [<i>spoof</i>]</pre>
[ パラメータ ]	<pre><i>spoof</i>   on ..... 処理する   off ..... 処理しない</pre>
[ 説明 ]	<p>on の場合、DNS リカーシブサーバ機能で、プライベートアドレスの PTR レコードに対する問い合わせに対し、上位サーバに問い合わせを転送することなく、自分でその問い合わせに対し "NXDomain"、すなわち「そのようなレコードはない」というエラーを返す。</p>
[ デフォルト値 ]	off



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

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

## 17.7 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 resolv`  
`no dns syslog resolv [resolv]`
- [パラメータ] *resolv*  
`on` ..... 解決する  
`off` ..... 解決しない
- [説明] SYSLOG 表示で DNS により名前解決するか否かを設定する。
- [デフォルト値] `off`

## 17.8 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> |
|--------------------|-------------|--------------|
| <code>a</code>     | FQDN        | IP アドレス      |
| <code>ptr</code>   | IP アドレス     | FQDN         |
| <code>mx</code>    | FQDN        | FQDN         |
| <code>ns</code>    | FQDN        | FQDN         |
| <code>cname</code> | 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`

## 18. 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。

### 18.1 インタフェース速度の設定

[ 入力形式 ]	speed <i>interface speed</i> no speed <i>interface [speed]</i>
[ パラメータ ]	<i>interface</i> .....LAN インタフェース名、もしくは pp <i>speed</i> ..... インタフェース速度 (bit/s)
[ 説明 ]	指定したインタフェースに対して、インタフェースの速度を設定する。帯域制御のためのパラメータ計算に用いられるもので、実際の速度を設定できるわけではない。物理的な速度と一致しているのが望ましい。MP により動的に回線速度が変動する場合などは、最低限の速度に設定しておく。
[ ノート ]	<i>speed</i> パラメータの後ろに 'k' または 'M' をつけると、それぞれ kbit/s、Mbit/s として扱われる。
[ デフォルト値 ]	0

### 18.2 クラス分けのためのフィルタ設定

[ 入力形式 ]	queue class filter <i>num class ip src_addr [dest_addr [proto [src_port [dest_port]]]]</i> queue class filter <i>num class ipx src_net [src_node [dst_net [dst_node [type [src_socket [dst_socket]]]]]]</i> queue class filter <i>num class bridge src_mac [dst_mac [offset byte_list]]</i> no queue class filter <i>num class [protocol ...]</i>						
[ パラメータ ]	<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)						
	IP フィルタ						
	<i>src_addr</i> .....IP パケットの始点 IP アドレス xxx.xxx.xxx.xxx xxx 10 進数 * ( ネットマスクの対応するビットが 8 ビットとも 0 と同じ ) * ( すべての IP アドレスに対応 )						
	<i>dest_addr</i> .....IP パケットの終点 IP アドレス (src_address と同じ形式)。省略した場合は一個の * と同じ。						
	<i>proto</i> ..... フィルタリングするパケットの種類 プロトコルを表す 10 進数 プロトコルを表すニーモニック						
	<table border="1"> <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>	icmp	1	tcp	6	udp	17
icmp	1						
tcp	6						
udp	17						
	上項目のカンマで区切った並び (5 個以内) * ( すべてのプロトコル ) established						

省略時は \* と同じ。

*src\_port* ..... UDP、TCP のソースポート番号  
 ポート番号を表す 10 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
ftp	20,21
ftpdata	20
telnet	23
smtp	25
domain	53
gopher	70
finger	79
www	80
pop3	110
sunrpc	111
ident	113
ntp	123
nntp	119
snmp	161
syslog	514
printer	515
talk	517
route	520
uucp	540

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 16 進数以外に '\*' も指定可)  
 \* (すべての IPX ネットワーク番号)  
*src\_node* ..... 始点 IPX ノード番号  
 0:0:0:0:1 ..... FF:FF:FF:FF:FE (2 桁以内の 16 進数以外に '\*' も指定可)  
 \* (すべての IPX ノード番号)  
 省略時は一個の \* と同じ  
*dst\_net* ..... 終点 IPX ネットワーク番号 *src\_net* と同じ形式  
*dst\_node* ..... 終点 IPX ノード番号 *src\_node* と同じ形式  
*type* ..... IPX パケットタイプ

10 進数 (0..255)  
 16 進数 (0x0..0xFF)  
 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)  
 省略時は一個の \* と同じ

*src\_socket*.....始点ソケット番号  
 10 進数 (0..65535)  
 0x を先頭に持つ 4 桁以内の 16 進数  
 プロトコルを表すニーモニック

<i>ncp</i>	0x0451
<i>sap</i>	0x0452
<i>rip</i>	0x0453
<i>netbios</i>	0x0455
<i>diag</i>	0x0456
<i>serialization</i>	0x0457

間に - をはさんだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。  
 上項目のカンマで区切った並び (5 個以内)

\* (すべてのソケット番号)  
 省略時は一個の \* と同じ

*dst\_socket*.....終点ソケット番号 *src\_socket* と同じ形式。

#### ブリッジフィルタ

*src\_mac*.....始点 MAC アドレス  
 x:xx:xx:xx:xx:xx  
 16 進数  
 \*

\* (すべての MAC アドレスに対応)

*dst\_mac*.....終点 MAC アドレス *src\_mac* と同じ形式。省略時は一個の \* と同じ

*offset*.....オフセットを表す 10 進数 (イーサネットフレームの始点 MAC アドレスの直後を 0 とする  
 バイト数)

#### *byte\_list*

バイト列  
 xx (xx は 2 桁の 16 進数)  
 上項目のカンマで区切った並び (16 個以内)  
 \* (すべてのバイト表現)

#### [ 説明 ]

クラス分けのためのフィルタを設定する。  
 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。

### 18.3 キューイングアルゴリズムタイプの選択

[入力形式]	queue <i>interface</i> type <i>type</i> no queue <i>interface</i> type [ <i>type</i> ]
[パラメータ]	<i>interface</i> ..... LAN インタフェース名、もしくは pp <i>type</i> fifo ..... First In, First Out 形式のキューイング wfq ..... Weighted Fair Queue 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
[説明]	<p>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。</p> <p>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。</p> <p>LAN インタフェースのデフォルトは fifo である。</p> <p>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。</p> <p>wfq のもう一つの特徴は、設定がいらぬということである。設定するところがないため、優先制御や帯域制御に比べて細かい調整はできないが、簡単にフロー間での帯域のバランスを図ることができる。</p> <p>PP インタフェースのデフォルトは wfq である。</p> <p>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。</p> <p>cbq は帯域制御を行う。queue interface class property コマンドで各クラスに割り振る帯域をあらかじめ設定しておき、queue class filter コマンドおよび queue interface class filter list コマンドでクラス分けされたパケットが指定の帯域になるように送信する。</p>
[デフォルト値]	fifo

### 18.4 デフォルトクラスの設定

[入力形式]	queue <i>interface</i> default class <i>class</i> no queue <i>interface</i> default class [ <i>class</i> ]
[パラメータ]	<i>interface</i> ..... LAN インタフェース名、もしくは pp <i>class</i> ..... 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

### 18.5 クラス分けフィルタの適用

[入力形式]	queue <i>interface</i> class filter list <i>filter_list</i> no queue <i>interface</i> class filter list [ <i>filter_list</i> ]
[パラメータ]	<i>interface</i> ..... LAN インタフェース名、もしくは pp <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。

## 18.6 クラスの属性の設定

[ 入力形式 ]	queue <i>interface</i> class property <i>class</i> bandwidth= <i>bandwidth</i> [parent= <i>parent</i> ] [borrow= <i>borrow</i> ] [maxburst= <i>maxburst</i> ] [minburst= <i>minburst</i> ] [packetsize= <i>packetsize</i> ] no queue <i>interface</i> class property <i>class</i> [bandwidth= <i>bandwidth</i> ...]
[ パラメータ ]	<i>interface</i> .....LAN インタフェース名、もしくは pp <i>class</i> .....クラス (1..16) <i>bandwidth</i> .....クラスに割り当てる帯域 (bit/s) 数値の後ろに 'k'、'M' をつけるとそれぞれ kbit/s、Mbit/s として扱われる。また、数値 の後ろに '%' をつけると、回線全体の帯域に帯するパーセンテージとなる。 <i>parent</i> .....親クラスの番号 (0..16) <i>borrow</i> .....帯域が足りなくなった場合に親クラスから帯域を借りるか否かの設定 on.....借りる off.....借りない <i>maxburst</i> .....連続送信できる最大パケット数 (1..10000) <i>minburst</i> .....安定送信中に連続送信できる最大パケット数 (1..10000) <i>packetsize</i> .....クラスで流れるパケットの平均パケット長 (1..10000)
[ 説明 ]	指定したクラスの属性を設定する。
[ ノート ]	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 ]	<i>parent</i> = 0 <i>borrow</i> = on <i>maxburst</i> = 20 <i>minburst</i> = <i>maxburst</i> / 10 <i>packetsize</i> = 512

## 18.7 クラス毎のキュー長の設定

[ 入力形式 ]	queue <i>interface</i> length <i>len1</i> [ <i>len2</i> ... <i>len16</i> ] no queue <i>interface</i> length [ <i>len1</i> [ <i>len2</i> ... <i>len16</i> ]]
[ パラメータ ]	<i>len1</i> .. <i>len16</i> .....クラス 1 からクラス 16 のキュー長
[ 説明 ]	インタフェースに対して、指定したクラスのキューに入ることでできるパケットの個数を指定する。設定を省略したクラスに関しては、最後に指定されたキュー長が残りのクラスにも適用される。
[ デフォルト値 ]	200 (LAN インタフェース、その他の機種は 40) 20 (PP、全機種共通)

## 18.8 MP インタリーブの設定

[入力形式]	<code>ppp mp interleave [<i>delay</i>] <i>switch</i></code> <code>no ppp mp interleave [[<i>delay</i>] <i>switch</i>]</code>
[パラメータ]	<i>delay</i> ..... 遅延 (ミリ秒) <i>switch</i> <i>on</i> ..... MP インタリーブを使用する <i>off</i> ..... MP インタリーブを使用しない
[説明]	MP インタリーブを使用するかどうかを設定する。DELAY では、優先されるプロトコルで許容できる最大遅延を設定する。パケットをどのような大きさに分割するかは、DELAY の値と回線速度により決定される。
[ノート]	DELAY で設定した遅延が保証されるわけではない。 データの受信側でも同じ設定をしておかないと、効果が発揮されない。 同時に圧縮は利用できない。圧縮を利用する設定の場合、この機能は無視されるので、以下の設定で圧縮を無効にしておく必要がある。 <code>ppp ccp type none</code>
[デフォルト値]	<i>sw</i> = off <i>delay</i> = 30
[設定例]	<code># queue class filter 1 4 ip VOIP-GATEWAY * * * *</code> <code># queue class filter 2 3 ip * * icmp * *</code> <code># queue class filter 3 1 ip * * * * *</code> <code># pp select 1</code> <code># pp bind bri2.1</code> <code># queue pp type priority</code> <code># queue class filter list 1 2 3</code> <code># isdn remote address call 03-123-4567</code> <code># ppp mp use on</code> <code># ppp mp interleave on</code> <code># ppp mp maxlink 1</code> <code># ppp ccp type none</code> <code># pp enable 1</code>

## 19. 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。

### 19.1 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。

### 19.2 OSPFの使用設定

---

- [ 入力形式 ]      ospf use *switch*  
no ospf use [*switch*]
- [ パラメータ ]    *switch*  
                  on.....OSPFを使用する  
                  off.....OSPFを使用しない
- [ 説明 ]            OSPFを使用するかどうかを設定する。
- [ デフォルト値 ]  off

### 19.3 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を表す 1 以上の数値
- [ 説明 ]            OSPFによる経路の優先度を設定する。優先度は 1 以上の数値で表され、数字が大きい程優先度が高い。OSPFとRIPなど複数のプロトコルで得られた経路が食い違う場合には、優先度が高い方が採用される。優先度が同じ場合には時間的に先に採用された経路が有効となる。
- [ ノート ]         静的経路の優先度は 10000 で固定である。
- [ デフォルト値 ]  2000

### 19.4 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



## 19.5 外部プロトコルによる経路導入

[入力形式]	ospf import from <i>protocol</i> [filter <i>f</i> filter_num...] no ospf import from [ <i>protocol</i> [filter <i>f</i> filter_num...]]
[パラメータ]	<i>protocol</i> ..... OSPF の経路テーブルに導入する外部プロトコル <i>static</i> ..... 静的経路 <i>rip</i> ..... RIP <i>filter_num</i> ..... フィルタ番号
[説明]	OSPF の経路テーブルに外部プロトコルによる経路を導入するかどうかを設定する。導入された経路は外部経路として他の OSPF ルータに広告される。  <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。  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。 <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

## 19.6 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> [not] <i>kind</i> <i>ip_address/mask</i> ...[ <i>parameter</i> ...] no ospf import filter <i>filter_num</i> [[not] <i>kind</i> <i>ip_address/mask</i> ...[ <i>parameter</i> ...]]
[パラメータ]	<i>filter_num</i> ..... フィルタ番号 <i>kind</i> ..... フィルタ種別 <i>include</i> ..... 指定したネットワークアドレスに含まれる経路 (ネットワークアドレス自身を含む) <i>refines</i> ..... 指定したネットワークアドレスに含まれる経路 (ネットワークアドレス自身は含まない) <i>equal</i> ..... 指定したネットワークアドレスに一致する経路 <i>ip_address/mask</i> ..... ネットワークアドレスをあらわす IP アドレスとマスク長 <i>parameter</i> ..... 外部経路を広告する場合のパラメータで以下の種類がある <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]	OSPF の経路テーブルに外部経路を導入する際に適用するフィルタを定義する。このコマンドで定義したフィルタは、ospf import from コマンドの filter 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、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。  <i>kind</i> では、経路の検査方法を設定する。 <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  <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。  <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。 <i>metric</i> = 1 <i>type</i> = 2 <i>tag</i> = 1

## 19.7 OSPF エリア設定

---

[ 入力形式 ]	ospf area <i>area</i> [auth= <i>auth</i> ] [stub [cost= <i>cost</i> ]] no ospf area <i>area</i> [auth= <i>auth</i> ] [stub [cost= <i>cost</i> ]]
[ パラメータ ]	<i>area</i> 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> ..... 認証を行う text ..... プレーンテキスト認証 md5 ..... MD5 認証 <i>cost</i> ..... 0 以上の数値
[ 説明 ]	OSPF エリアを設定する。 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。COST を指定しないとデフォルト経路の広告は行われない。
[ デフォルト値 ]	認証は行わない スタブエリアではない

## 19.8 エリアへの経路広告

---

[ 入力形式 ]	ospf area network <i>area network/mask</i> [restrict] no ospf area network <i>area network/mask</i> [restrict]
[ パラメータ ]	<i>area</i> 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。restrict キーワードが指定された場合には、範囲内の経路は要約した経路も広告しない。

## 19.9 スタブ的接続の広告

---

[ 入力形式 ]	ospf area stubhost <i>area host</i> [cost <i>cost</i> ] no ospf area stubhost <i>area host</i>
[ パラメータ ]	<i>area</i> 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。

## 19.10 仮想リンク設定

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

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

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

**MD5 認証鍵について**  
MD5 認証鍵を複数設定できる機能は、MD5 認証鍵を円滑に変更するためである。通常の運用では、MD5 認証鍵は 1 つだけ設定しておく。MD5 認証鍵を変更する場合は、まず 1 つのルータで新旧の MD5 認証鍵を 2 つ設定し、その後、近隣ルータで MD5 認証鍵を新しいものに変更していく。そして、最後に 2 つの鍵を設定したルータで古い鍵を削除すれば良い。

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

## 19.11 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...*]  
no ip *interface* ospf area [*area* [*parameters...*]]

[ パラメータ ] *interface*.....LAN インタフェース、pp  
*area*  
backbone .....バックボーンエリア  
1 以上の数値 .....非バックボーンエリア  
IP アドレス表記 (0.0.0.0 は不可) 非バックボーンエリア  
*parameters*.....name=value の列

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

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

[ ノート ] *name* パラメータの *type* について  
*name* パラメータの *type* として、LAN インタフェースは broadcast のみが許される。PP インタフェースは、PPP を利用する場合は point-to-point、FR 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。  
FR で non-broadcast (NBMA) を利用する場合には、FR の各拠点間のすべての間で PVC が設定されており、FR に接続された各ルータは他のルータと直接通信できるような状態、すなわちフルメッシュになっていない。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、FR の PVC はフルメッシュである必要はなく、一部が欠けたパーシャル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通るトラフィックは大きくなる。non-broadcast では、broadcast と同じように指定ルータが選定され、HELLO などの OSPF トラフィックは各ルータと指定ルータの間だけに限定されるが、point-to-multipoint ではすべての通信可能なルータペアの間に point-to-point リンクがあるという考え方なので、OSPF トラフィックもすべての通信可能なルータペアの間でやりとりされる。

**passive** について

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

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

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

**hello-interval/dead-interval** について

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

**MD5 認証鍵** について

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

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

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

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

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

[パラメータ] *interface* ..... インタフェース名  
*ip\_address* ..... 近隣ルータの IP アドレス

[説明] 非ブロードキャスト型のネットワークに接続されている OSPF ルータを指定する。  
**eligible** キーワードが指定されたルータは指定ルータとして適格であることを表す。

## 20. IPv6

### 20.1 IPv6 アドレスの管理

#### 20.1.1 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`  
                  `no ipv6 interface address ipv6_address/prefix_len`

[ パラメータ ]     *interface*.....LAN インタフェース、pp、tunnel  
                  *ipv6\_address*.....IPv6 アドレス  
                  *prefix\_len*.....プレフィックス長

[ 説明 ]            インタフェースにIPv6 アドレスを付与する。

[ ノート ]          このコマンドで付与したアドレスは、show ipv6 address コマンドで確認することができる。

#### 20.1.2 インタフェースに付与されているIPv6 アドレスの表示

---

[ 入力形式 ]     `show ipv6 address`

[ 説明 ]          すべてのインタフェースについて、付与されているIPv6 アドレスを表示する。

## 20.2 近隣探索

## 20.2.1 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/prefix_len</i> [valid_lifetime= <i>time</i> ] [preferred_lifetime= <i>time</i> ] [ <i>l_flag</i> = <i>sw</i> ] [ <i>a_flag</i> = <i>sw</i> ] no ipv6 prefix <i>prefix_id</i>
[パラメータ]	<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 valid_lifetime ..... プレフィックスの有効寿命 (60..15552000) preferred_lifetime ..... プレフィックスの推奨寿命 (60..15552000) <i>time</i> ..... 時間設定 YYYY-MM-DD, hh:mm[:ss] YYYY ..... 年 (1980..2079) MM ..... 月 (01..12) DD ..... 日 (01..31) hh ..... 時 (00..23) mm ..... 分 (00..59) ss ..... 秒 (00..59、省略時は00) <i>l_flag</i> ..... on-link フラグ <i>a_flag</i> ..... autonomous address configuration フラグ <i>sw</i> on off
[説明]	ルータ広告で配布するプレフィックスを定義する。実際に広告するためには、ipv6 <i>interface</i> rtadv prefix コマンドの設定が必要である。 <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 15552000 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。最終有効期間とはアドレスが無効になるまでの時間であり、推奨有効期間とはアドレスを新たな接続での使用が不可となる時間である。また、on-link フラグはプレフィックスがそのデータリンクに固有である時に on とする。autonomous address configuration フラグはプレフィックスを自律アドレス設定で使うことができる場合に on とする。
[デフォルト値]	valid_lifetime = 2592000 preferred_lifetime = 604800 <i>l_flag</i> = on <i>a_flag</i> = on
[説明]	
[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。

## 20.2.2 ルータ広告の送信の制御

---

[入力形式]	ipv6 <i>interface</i> rtadv send <i>prefix_id</i> [ <i>prefix_id</i> ...] [ <i>m_flag</i> = <i>sw</i> ] [ <i>o_flag</i> = <i>sw</i> ] no ipv6 <i>interface</i> rtadv send
[パラメータ]	<i>interface</i> ..... LAN インタフェース、pp <i>prefix_id</i> ..... プレフィックス番号 <i>m_flag</i> ..... managed address configuration フラグ <i>o_flag</i> ..... other stateful configuration フラグ <i>switch</i> on off
[説明]	インタフェースごとにルータ広告の送信を制御する。送信されるプレフィックスとして、ipv6 prefix コマンドで設定されたものが用いられる。managed address configuration フラグを off とすることで、ネットワークに接続されているホストのステートレス自動設定が許され、ホスト自身でアドレス設定がなされる。また other stateful configuration フラグを off とすることで、ホストはオプションとして格納されているプレフィックスリストを調べることになる。
[デフォルト値]	<i>m_flag</i> = off <i>o_flag</i> = off

## 20.3 経路制御

## 20.3.1 IPv6 の経路情報の追加

---

[ 入力形式 ]	<code>ipv6 route <i>network</i> gateway <i>gateway</i> [<i>parameter</i>] [gateway <i>gateway</i> [<i>parameter</i>]]</code> <code>no ipv6 route <i>network</i></code>
[ パラメータ ]	<p><i>network</i></p> <p>IP アドレス .....IPv6 アドレス / プレフィックス長  <i>default</i> .....デフォルト経路</p> <p><i>gateway</i>.....ゲートウェイ  IP アドレス % スコープ識別子  <i>pp pp_num</i> [<i>dlci=dlci</i>] ..... PP インタフェースへの経路  "dlci=<i>dlci</i>" が指定された場合は、フレームリレーの DLCI への経路</p> <p><i>pp_num</i></p> <p>PP 番号 (RT105i:1..30, その他 :1..100)  <i>anonymous</i></p> <p><i>pp anonymous name=name</i></p> <p><i>name</i> ..... PAP/CHAP による名前</p> <p><i>tunnel tunnel_num</i>..... Tunnel インタフェースへの経路  <i>filter_num</i>..... フィルタ番号</p> <p><i>parameter</i>.....以下のパラメータを空白で区切り複数設定可能</p> <p><i>filter number</i> [<i>number.</i>]... フィルタ型経路の指定  <i>number</i> ..... フィルタの番号 (1..100) (空白で区切り複数設定可能)</p> <p><i>metric metric</i> .....メトリックの指定  <i>metric</i>.....メトリック値 (1..15) (省略時は 1)</p> <p><i>hide</i> .....出力インタフェースが PP インタフェースの場合のみ有効なオプションで、回線が接続されている場合だけ経路が有効になることを意味する</p>
[ 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 <code>show ipv6 address</code> コマンドで表示される。LAN インタフェースがひとつである機種に関しては、スコープ識別子が省略されると LAN1 が指定されたものとして扱う。

## 20.4 RIPng の設定

---

[ 入力形式 ]	<code>ipv6 rip use <i>switch</i></code> <code>no ipv6 rip use</code>
[ パラメータ ]	<p><i>destination</i>.....スイッチ  <i>on</i>.....RIPng を使う  <i>off</i>.....RIPng を使わない</p>
[ 説明 ]	RIPng を使うかどうかを設定する。
[ デフォルト値 ]	<code>off</code>

## 20.4.1 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 ]	<code>ipv6 <i>interface</i> rip send <i>switch</i></code> <code>no ipv6 <i>interface</i> rip send</code>
[ パラメータ ]	<p><i>interface</i>.....LAN インタフェース、pp  <i>switch</i>.....スイッチ  <i>on</i>.....RIPng を送信する  <i>off</i>.....RIPng を送信しない</p>
[ 説明 ]	RIPng の送信ポリシーを設定する。
[ デフォルト値 ]	<code>off</code>



#### 20.4.2 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 <i>interface</i> rip receive <i>sw</i> no ipv6 <i>interface</i> rip receive
[パラメータ]	<i>interface</i> ..... LAN インタフェース、pp <i>sw</i> ..... スイッチ on ..... 受信した RIPng パケットを処理する off ..... 受信した RIPng パケットを無視する
[説明]	RIPng の受信ポリシーを設定する。
[デフォルト値]	on

#### 20.4.3 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 <i>interface</i> rip trust gateway [except] <i>gateway</i> [ <i>gateway</i> ...] no ipv6 <i>interface</i> rip trust gateway
[パラメータ]	<i>interface</i> ..... LAN インタフェース、pp <i>gateway</i> ..... IPv6 アドレス
[説明]	信頼できる RIPng ゲートウェイを設定する。 except キーワードを指定していない場合には、列挙したゲートウェイを信用できるゲートウェイとし、それらからの RIP だけを受信する。 except キーワードを指定した場合は、列挙したゲートウェイを信用できないゲートウェイとし、それらを除いた他のゲートウェイからの RIP だけを受信する。

#### 20.4.4 RIPng の加算ホップ数の設定

---

[入力形式]	ipv6 pp rip hop <i>direction</i> <i>hop</i> no ipv6 pp rip hop
[パラメータ]	<i>direction</i> ..... 方向 in..... 受信時に加算する out..... 送信時に加算する <i>hop</i> ..... 加算ホップ数 (1..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

#### 20.4.5 RIPng で送受信する経路に対するフィルタリングの設定

---

[入力形式]	ipv6 <i>interface</i> rip filter <i>direction</i> <i>filter_list</i> [ <i>filter_list</i> ...] no ipv6 <i>interface</i> rip filter
[パラメータ]	<i>interface</i> ..... LAN インタフェース、pp <i>direction</i> ..... 方向 in..... 内向きのパケットを対象にする out..... 外向きのパケットを対象にする <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]	clear

#### 20.4.6 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 <i>action</i> no ipv6 pp rip connect send
[パラメータ]	<i>action</i> ..... 動作 interval ..... 一定の間隔で RIPng を送信する update ..... 経路情報が変化したときのみ 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]	update

#### 20.4.7 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.....送出間隔 [ 秒 ](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

#### 20.4.8 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.....動作`  
                   `none .....RIPng を送信しない`  
                   `interval.....一定の間隔で RIPng を送信する`  
                   `update .....経路情報が変化したときのみ 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

#### 20.4.9 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.....送出間隔 [ 秒 ] ( 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

#### 20.4.10 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 hold`  
                   `no ipv6 pp rip hold routing`
- [ パラメータ ]    `hold.....保持するか否か`  
                   `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

### 20.5 フィルタの設定

#### 20.5.1 IPv6 フィルタの定義

---

- [ 入力形式 ]    `ipv6 filter filter_num pass_reject src_address[/prefix_len] [dst_address[/prefix_len]]`  
                   `[protocol [src_port_list [dst_port_list]]]`
- [ パラメータ ]    `filter_num.....静的フィルタ番号 ( 1..2147483647 )`  
                   `pass_reject.....フィルタのタイプ (ip filter コマンドに準ずる )`  
                   `src_address .....IP パケットの始点 IP アドレス`  
                   `prefix_len .....プリフィクス長`  
                   `dst_address .....IP パケットの終点 IP アドレス (src_addr と同じ形式 )。`  
                   省略時は 1 個の \* と同じ。  
                   `protocol.....フィルタリングするパケットの種類 (ip filter コマンドに準ずる )`  
                   `src_port_list.....UDP、TCP のソースポート番号 (ip filter コマンドに準ずる )`  
                   `dst_port_list.....UDP、TCP のデスティネーションポート番号`
- [ 説明 ]            IPv6 のフィルタを定義する。

---

### 20.5.2 IPv6 フィルタの削除

---

- [入力形式]     **ipv6 filter delete *filter\_num***  
                   **no ipv6 filter *filter\_num***
- [パラメータ]     ***filter\_num*** ..... フィルタ番号 (1..100)
- [説明]            IPv6 のフィルタを削除する。

---

### 20.5.3 IPv6 フィルタの適用

---

- [入力形式]     **ipv6 *interface* secure filter *direction filter\_list [filter\_list...]***  
                   **no ipv6 *interface* secure filter *direction***
- [パラメータ]     ***interface*** ..... LAN インタフェース、pp  
                   ***direction*** ..... 方向  
                   **in** ..... 内向きのパケットを対象にする  
                   **out** ..... 外向きのパケットを対象にする  
                   ***filter\_list*** ..... 静的フィルタ番号
- [説明]            IPv6 フィルタをインタフェースに適用する。

## 20.6 トンネルリング

---

### 20.6.1 トンネルインタフェースの種別の設定

---

- [入力形式]     **tunnel encapsulation *type***  
                   **no tunnel encapsulation**
- [パラメータ]     ***type*** ..... トンネルインタフェースの種別  
                   **6over4** ..... IPv6 over IPv4 tunnel  
                   **4over6** ..... IPv4 over IPv6 tunnel  
                   **ipsec** ..... IPsec tunnel mode
- [説明]            トンネルインタフェースの種別を設定する。
- [デフォルト値]   **ipsec**

---

### 20.6.2 トンネルインタフェースの自分側の IPv4 アドレスの設定

---

- [入力形式]     **ip tunnel local address *ipv4\_address***  
                   **no ip tunnel local address**
- [パラメータ]     ***ipv4\_address*** ..... IPv4 アドレス
- [説明]            トンネルインタフェースの自分側の IPv4 アドレスを設定する。
- [ノート]          IPv6 over IPv4 トンネルを使用する場合には、本コマンドを設定する必要がある。

---

### 20.6.3 トンネルインタフェースの相手側の IPv4 アドレスの設定

---

- [入力形式]     **ip tunnel remote address *ipv4\_address***  
                   **no ip tunnel remote address**
- [パラメータ]     ***ipv4\_address*** ..... IPv4 アドレス
- [説明]            トンネルインタフェースの相手側の IPv4 アドレスを設定する。
- [ノート]          IPv6 over IPv4 トンネルを使用する場合には、本コマンドを設定する必要がある。

#### 20.6.4 トンネルインタフェースの相手側の IPv6 アドレスの設定

---

- [ 入力形式 ]    `ipv6 tunnel remote address ipv6_address`  
                   `no ip tunnel remote address`
- [ パラメータ ]    `ipv6_address.....IPv6 アドレス`
- [ 説明 ]            トンネルインタフェースの相手側の IPv6 アドレスを設定する。
- [ ノート ]         IPv4 over IPv6 トンネルを使用するには、本コマンドを設定する必要がある。

### 20.7 管理ツール

#### 20.7.1 ping の実行

---

- [ 入力形式 ]    `ping6 destination [count]`  
                   `ping6 destination scope_id [count]`  
                   `ping6 destination interface [count]`  
                   `ping6 destination pp pp_num [count]`
- [ パラメータ ]    `destination.....送信する宛先の IPv6 アドレス`  
                   `scope_id.....スコープ ID`  
                   `interface.....LAN インタフェース`  
                   `pp_num.....PP 番号`  
                   `count.....送信回数 ( 1..21474836 )`
- [ 説明 ]            指定した宛先に対して ICMPv6 Echo Request を送信する。  
                   スコープ ID は、`show ipv6 address` コマンドで表示できる。

#### 20.7.2 traceroute の実行

---

- [ 入力形式 ]    `traceroute6 destination`
- [ パラメータ ]    `destination.....送信する宛先の IPv6 アドレス`
- [ 説明 ]            指定した宛先までの経路を調べて表示する。

## 21. スケジュール

### 21.1 スケジュールの設定

[入力形式] `schedule at id [date] time command...`  
`schedule at id [date] time pp peer_num command...`  
`schedule at id [date] time tunnel tunnel_num command...`  
`no scudule at id [[date]...]`

[パラメータ] `id`..... スケジュール番号  
`date`..... 日付 (省略可)  
 月 / 日  
 省略時は \*/\* とみなす

月の設定例	設定内容
1,21	月と2月
2-2	月から12月まで
2-72	月から7月まで
-7	1月から7月まで
*	毎月

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

`time`..... 時刻  
 時 (0..23 または \*): 分 (0..59 または \*)  
`startup` ..... 起動時  
`peer_num`  
 相手先情報番号  
`anonymous`  
`leased`  
`tunnel_num`..... トンネルインタフェースの番号  
`command`..... 実行するコマンド (制限あり)

[説明] `time` で指定した時刻に `command` で指定されたコマンドを実行する。  
 2、3番目の形式で指定された場合には、それぞれあらかじめ指定された相手先 / トンネル番号での、`pp select` / `tunnel select` コマンドが発行済みであるように動作する。  
`schedule at` コマンドは複数指定でき、同じ時刻に指定されたものは `id` の小さな順に実行される。  
 以下のコマンドは指定できない。  
`administrator`、`administrator password`、`cold start`、`console` で始まるコマンド、  
`date`、`help`、`login password`、`login timer`、`ping`、`line type`、`quit`、`remote setup`、`save`、`show` で始まるコマンド、`time`、`timezone`、`traceroute`

[ノート] 入力時、`command` パラメータに対して TAB キーによるコマンド補完は行わぬが、シンタックスエラーなどは実行時まで検出されない。`schedule at` コマンドにより指定されたコマンドを実行する場合には、何を実行しようとしたかを INFO タイプの SYSLOG に出力する。  
`date` に数字と曜日を混在させて指定はできない。  
`startup` を指定したスケジュールはルータ起動時に実行される。電源を入れたらすぐ発信したい場合などに便利。

[設定例] `ウィークデイの 8:00 ~ 17:00 だけ接続を許可する`  
`# schedule at 1 */mon-fri 8:00 pp 1 isdn auto connect on`  
`# schedule at 2 */mon-fri 17:00 pp 1 isdn auto connect off`  
`# schedule at 3 */mon-fri 17:05 * disconnect 1`  
  
`毎時 0 分から 15 分間だけ接続を許可する`  
`# schedule at 1 *:00 pp 1 isdn auto connect on`  
`# schedule at 2 *:15 pp 1 isdn auto connect off`  
`# schedule at 3 *:15 * disconnect 1`  
  
`今度の元旦にルーティングを切替える`  
`# schedule at 1 1/1 0:0 * ip route NETWORK gateway pp 2`

## 22. 操作

### 22.1 相手先情報番号の選択

---

[ 入力形式 ]     pp select *peer\_num*

[ パラメータ ]     *peer\_num*  
                     相手先情報番号  
                     none .....相手を選択しない  
                     anonymous .....ISDN 番号が不明である相手の設定

[ 説明 ]            設定や表示の対象となる相手先情報番号を選択する。以降プロンプトには、console prompt コマンドで設定した文字列と相手先情報番号が続けて表示される。  
                     none を指定すると、プロンプトに相手先情報番号を表示しない。

[ ノート ]          この操作コマンドは一般ユーザでも実行できる。

### 22.2 設定に関する操作

#### 22.2.1 管理ユーザへの移行

---

[ 入力形式 ]     administrator

[ パラメータ ]     なし

[ 説明 ]            このコマンドを発行してからでないと、ルータの設定は変更できない。また操作コマンドも実行できない。  
                     コマンド入力後、管理パスワードを入力しなければならない。

#### 22.2.2 終了

---

[ 入力形式 ]     quit  
                     quit *save*  
                     exit  
                     exit *save*

[ パラメータ ]     *save* .....管理ユーザから抜ける場合に *save* を指定すると、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。

#### 22.2.3 設定内容の保存

---

[ 入力形式 ]     save  
                     save [*filename* [*comment*]]

[ パラメータ ]     *filename* .....設定を保存するファイル名  
                     0..9 .....内蔵 Flash ROM の設定ファイル (0..9)  
                     ext0:*filename* .....PCMCIA Flash ATA カードの設定ファイル  
                     *comment* .....設定ファイルのコメント

[ 説明 ]            現在の設定内容を不揮発性メモリに保存する。  
                     第 2 書式は、RT300i 専用のコマンド。  
                     RT300i では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、起動場合に使用した設定ファイルに保存する。

#### 22.2.4 設定ファイルの削除

---

[ 入力形式 ]     delete config *file*

[ デフォルト値 ]   *file* .....削除するファイル名  
                     内蔵フラッシュ ROM の設定ファイル (0..9)  
                     ext0:*name* .....PCMCIA Flash ATA カードの設定ファイル

[ 説明 ]            RT300i 専用のコマンド。保存されている設定ファイルを削除する。

### 22.2.5 実行形式ファームウェアファイルの削除

---

[入力形式]	delete exec <i>file</i>
[パラメータ]	<i>file</i> ..... 削除するファイル名 <i>ext0:name</i> ..... PCMCIA Flash ATA カードの設定ファイル
[説明]	RT300i 専用のコマンド。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。

### 22.2.6 設定ファイルの一覧

---

[入力形式]	show config list
[パラメータ]	なし
[説明]	RT300i 専用のコマンド。内蔵 Flash ROM に保存されている設定ファイルの一覧を表示する。

### 22.2.7 設定の初期化

---

[入力形式]	cold start
[パラメータ]	なし
[説明]	工場出荷時の設定に戻し、再起動する。 コマンド実行時に管理パスワードを入力する必要がある。
[ノート]	内蔵 Flash ROM の設定ファイルがすべて削除される。

### 22.2.8 遠隔地のルータの設定

---

[入力形式]	remote setup <i>interface</i> [ <i>isdn_num</i> / <i>sub_address</i> ] remote setup <i>interface</i> dlci= <i>dlci</i>
[パラメータ]	<i>interface</i> ..... BRI、PRI インタフェース名 <i>isdn_num</i> ..... ISDN 番号 <i>sub_address</i> ..... ISDN サブアドレス (0x21 から 0x7e の ASCII 文字) <i>dlci</i> ..... フレームリレーの DLCI 番号
[説明]	指定したインタフェースを利用して、遠隔地のルータの設定をする。 インタフェースには BRI、PRI とも利用でき、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、 <i>isdn_num</i> 、 <i>sub_address</i> パラメータは不要。

### 22.2.9 遠隔地のルータからの設定に対する制限

---

[入力形式]	remote setup accept <i>isdn_num</i> / <i>sub_address</i> remote setup accept any remote setup accept none
[パラメータ]	<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 none ..... すべての遠隔地のルータからの設定を拒否する
[説明]	自分のルータの設定を許可する相手先を設定する。
[デフォルト値]	any

## 22.3 動的情報のクリア操作

## 22.3.1 ARP テーブルのクリア

---

[ 入力形式 ] clear arp  
 [ パラメータ ] なし  
 [ 説明 ] ARP テーブルをクリアする。

## 22.3.2 IP の動的経路情報のクリア

---

[ 入力形式 ] clear ip dynamic routing  
 [ パラメータ ] なし  
 [ 説明 ] 動的に設定された IP の経路情報をクリアする。

## 22.3.3 IPX の動的経路情報のクリア

---

[ 入力形式 ] clear ipx dynamic routing  
 [ パラメータ ] なし  
 [ 説明 ] 動的に設定された IPX の経路情報をクリアする。

## 22.3.4 IPX の動的 SAP 情報のクリア

---

[ 入力形式 ] clear ipx dynamic sap  
 [ パラメータ ] なし  
 [ 説明 ] IPX SAP テーブル中、動的に得られた SAP 情報をクリアする。

## 22.3.5 ブリッジのラーニング情報のクリア

---

[ 入力形式 ] clear bridge learning  
 [ パラメータ ] なし  
 [ 説明 ] 動的に受け取ったブリッジのラーニング情報をすべて消去する。  
 [ ノート ] bridge *interface* learning add コマンドで設定したものは消去されない。

## 22.3.6 ログのクリア

---

[ 入力形式 ] clear log  
 [ パラメータ ] なし  
 [ 説明 ] ログをクリアする。

## 22.3.7 アカウントのクリア

---

[ 入力形式 ] clear account  
 clear account *interface*  
 clear account pp [*peer\_num*]  
 [ パラメータ ] *interface*.....BRI、PRI インタフェース名  
*peer\_num*.....相手先情報番号、省略時は現在選択している相手先  
 [ 説明 ] 指定したインタフェース (1 番目の入力形式では、すべての合計) に関するアカウントをクリアする。



---

### 22.3.8 InARP のクリア

---

- [入力形式]      `clear inarp [peer_num]`
- [パラメータ]    `peer_num`..... 相手先情報番号、省略時は現在選択している相手先
- [説明]            InARP で得られた相手 IP アドレスをクリアし、InARP が on なら再度 InARP を開始する。

---

### 22.3.9 DNS キャッシュのクリア

---

- [入力形式]      `clear dns cache`
- [パラメータ]    なし
- [説明]            DNS リカーシブサーバで持っているキャッシュをクリアする。

---

### 22.3.10 PRI のステータス情報のクリア

---

- [入力形式]      `clear pri status pri`
- [パラメータ]    `pri`..... PRI 番号 (1..4)
- [説明]            PRI のステータス情報をクリアする。

---

### 22.3.11 NAT アドレステーブルのクリア

---

- [入力形式]      `clear nat descriptor dynamic nat_descriptor`
- [パラメータ]    `nat_descriptor`  
                  NAT ディスクリプタ番号 (1..21474836)  
                  `all`..... すべての NAT ディスクリプタ番号
- [説明]            NAT アドレステーブルをクリアする。
- [ノート]          通信中にアドレス管理テーブルをクリアした場合、通信が一時的に不安定になる可能性がある。

---

### 22.3.12 インタフェースの NAT アドレステーブルのクリア

---

- [入力形式]      `clear nat descriptor interface dynamic interface [number]`
- [パラメータ]    `interface` ..... LAN インタフェース名、pp、tunnel  
                  `number`..... pp、tunnel の場合の相手先番号
- [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。

---

### 22.3.13 IPv6 の動的経路情報の消去

---

- [入力形式]      `clear ipv6 dynamic routing`
- [説明]            経路制御プロトコルが得た IPv6 の経路情報を消去する。

---

### 22.3.14 近隣キャッシュの消去

---

- [入力形式]      `clear ipv6 neighbor cache`
- [説明]            近隣キャッシュを消去する。

## 22.4 その他の操作

## 22.4.1 相手先の使用許可の設定

---

[ 入力形式 ]	pp enable <i>peer_num</i> no pp enable
[ パラメータ ]	<i>peer_num</i> 相手先情報番号 anonymous
[ 説明 ]	相手先を使用できる状態にする。 工場出荷時、すべての相手先は disable 状態なので、使用する場合は必ずこのコマンドで enable 状態にしなければならない。

## 22.4.2 相手先の使用不許可の設定

---

[ 入力形式 ]	pp disable <i>peer_num</i>
[ パラメータ ]	<i>peer_num</i> 相手先情報番号 anonymous all
[ 説明 ]	相手先を使用できない状態にする。 相手先の設定を行う場合は disable 状態であることが望ましい。

## 22.4.3 再起動

---

[ 入力形式 ]	restart restart [ <i>binary</i> ][ <i>file</i> ]
[ パラメータ ]	<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 内蔵フラッシュ ROM の設定ファイル (0..9) PCMCIA Flash ATA カードの設定ファイル名
[ 説明 ]	第 2 書式は RT300i 専用のコマンド。ルータを再起動する。第 2 の書式では起動時の設定ファイルを指定できる。

## 22.4.4 インタフェースの再起動

---

[ 入力形式 ]	interface reset <i>interface</i> [ <i>interface</i> ...]
[ パラメータ ]	<i>interface</i> ..... インタフェース名
[ 説明 ]	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、PRI では、回線種別を line type コマンドで変更した場合には、本コマンドでインタフェースを再起動する必要がある。 なお、MP を使用しているインタフェースに対しては、interface reset pp コマンドを使用する。
[ ノート ]	line type コマンド、pp bind コマンド、経路情報などすべての設定を整えた後に実行する。対象とするインタフェースが bind されているすべての pp の通信を停止した状態で、また回線種別を変更する場合には回線を抜いた状態で実行すること。

## 22.4.5 PP インタフェースの再起動

---

[ 入力形式 ]	interface reset pp [ <i>pp_num</i> ]
[ パラメータ ]	<i>pp_num</i> pp 番号 (1..100) 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。

## 22.4.6 発信

---

[入力形式]	connect <i>peer_num</i>
[パラメータ]	<i>peer_num</i> ..... 発信相手の相手先情報番号
[説明]	手動で 発信する。

## 22.4.7 切断

---

[入力形式]	disconnect <i>peer_num</i>
[パラメータ]	<i>peer_num</i> 切断する相手先情報番号 all..... すべて anonymous..... anonymous のすべて anonymous1..anonymous16 ..... 指定した anonymous
[説明]	手動で切断する。

## 22.4.8 ping

---

[入力形式]	ping <i>host</i> [ <i>count</i> ]
[パラメータ]	<i>host</i> ping をかけるホストの IP アドレス (xxx.xxx.xxx.xxx (xxx は 10 進数)) ping をかけるホストの名称 <i>count</i> 実行回数 (1..21474836) infinity ..... Ctrl+C を入力するまで繰り返す
[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、相手からの応答があったかどうかだけを表示する。

## 22.4.9 traceroute

---

[入力形式]	traceroute <i>host</i> [noresolv]
[パラメータ]	<i>host</i> traceroute をかけるホストの IP アドレス (xxx.xxx.xxx.xxx (xxx は 10 進数)) traceroute をかけるホストの名称 noresolv ..... DNS による解決を行わないためのキーワード
[説明]	指定したホストまでの経路を調べて表示する。

## 22.4.10 telnet

---

[ 入力形式 ]	telnet <i>host</i> [ <i>port</i> [ <i>mode</i> [ <i>negotiation</i> [ <i>abort</i> ]]]]
[ パラメータ ]	<p><i>host</i>..... TELNET をかける相手のホスト名、もしくは IP アドレス</p> <p><i>port</i>..... 使用するポート番号</p> <p>10 進数 ポート番号の二モニック 省略時は 23 (TELNET)</p> <p><i>mode</i>..... telnet 通信 (送信) の動作モード</p> <p><i>character</i>..... 文字単位で通信する</p> <p><i>line</i>..... 行単位で通信する</p> <p><i>auto</i>..... <i>port</i> パラメータの設定値により <i>character/line</i> を選択 省略時は auto</p> <p><i>negotiation</i>..... telnet オプションのネゴシエーションの選択</p> <p><i>on</i>..... ネゴシエーションする</p> <p><i>off</i>..... ネゴシエーションしない</p> <p><i>auto</i>..... <i>port</i> パラメータの設定値により on/off を選択 省略時は auto</p> <p><i>abort</i>..... 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</p> <p>10 進数の ASCII コード 省略時は 29(^)</p>
[ 説明 ]	TELNET クライアントを実行する。
[ ノート ]	<p><i>character</i> 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。</p> <p><i>line</i> 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。</p> <p>ポート番号による機能自動選択について</p> <ol style="list-style-type: none"> <li>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。</li> <li>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。</li> </ol>
[ デフォルト値 ]	<p><i>port</i> = 23</p> <p><i>mode</i> = auto</p> <p><i>negotiation</i> = auto</p> <p><i>abort</i> = 29</p>

## 22.4.11 telnet サーバ機能の ON/OFF の設定

---

[ 入力形式 ]	telnetd service <i>service</i>
[ パラメータ ]	<p><i>service</i></p> <p><i>on</i>..... telnet サーバ機能を有効にする</p> <p><i>off</i>..... telnet サーバ機能を停止させるする</p>
[ 説明 ]	telnet サーバ機能の利用を選択する。
[ デフォルト値 ]	on
[ ノート ]	<p>変更した設定値は再起動しなければ動作に反映されない。</p> <p>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。</p>

## 22.4.12 telnet サーバ機能の listen ポートの設定

---

[ 入力形式 ]	telnetd listen <i>port</i>
[ パラメータ ]	<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。
[ デフォルト値 ]	23
[ ノート ]	<p>変更した設定値は再起動しなければ動作に反映されない。</p> <p>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。</p> <p>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。</p>

## 22.4.13 telnet サーバへアクセスできるホストの IP アドレスの設定

- [入力形式] telnetd host *ip\_range* [*ip\_range*...]
- [パラメータ] *ip\_range*  
telnet サーバへアクセスを許可するホストの IP アドレス範囲のリストまたはニーモニック  
1 個の IP アドレスまたは間にマイナス(-)をはさんだ IP アドレス (範囲指定)、及びこれらを任意に並べたもの  
any..... すべてのホストからのアクセスを許可する  
lan..... LAN ポートと WAN ポートに属するネットワーク内ならば許可する  
lan1..... LAN ポートに属するネットワーク内ならば許可する  
lan2..... WAN ポートに属するネットワーク内ならば許可する  
none ..... すべてのホストからのアクセスを禁止する
- [説明] telnet サーバへアクセスできるホストの IP アドレスを設定する。
- [デフォルト値] any
- [ノート] ニーモニックをリストにすることはできない。  
lan の場合、primary および secondary が clear では無く、ネットワークアドレスと directed broadcast address を除くホストアドレスからのリクエストを許可する。  
設定後の新しい telnet 接続から適用される。

## 22.4.14 PRI のループバックの実行

- [入力形式] pri loopback active *pri a data*  
pri loopback active *pri timeslot head num data*
- [パラメータ] *pri*..... PRI 番号 (1..4)  
*a*..... ループバック A を示すキーワード  
*timeslot*..... タイムスロットループバックを示すキーワード  
*data*..... 送信データパターン (1..4)
- | <i>data</i> | 擬似ランダムパターン |
|-------------|------------|
| 1           | 26-1       |
| 2           | 27-1       |
| 3           | 29-1       |
| 4           | 211-1      |
- head*..... 先頭タイムスロット番号 (1..24)  
*number*..... タイムスロット数 (1..24)
- [説明] 指定したデータパターンを送信して、ループバックテストを行う。コマンドを実行する場合に、管理パスワードを入力する必要がある。a キーワードの場合は、24B すべてのタイムスロットがループバックする。ループバックするポイントはルータの PRI コネクタの直前であり、PRI コネクタにケーブルを接続しているとその先の機器を破壊する可能性があるため、必ずケーブルを抜いてからテストを行わなければならない。timeslot キーワードの場合には、指定したタイムスロットに対してだけループバックテストを行う。データがループバックするのは、接続相手のルータなので、あらかじめ相手のルータをループバックを待ち受けるモードに設定しておく必要がある。ループバックテストが終了すると、自動的に通信モードに復帰する。
- [ノート] ループバック A の場合は、PRI コネクタを外した状態で行う必要がある。タイムスロットループバックを実行する前に、相手ルータはループバック待ち受け状態になっている必要がある。save コマンドを実行しても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。

## 22.4.15 PRI のループバック待ち受けの設定

---

[ 入力形式 ]	<code>pri loopback passive <i>pri</i> remote</code> <code>pri loopback passive <i>pri</i> payload</code> <code>pri loopback passive <i>pri</i> timeslot <i>head number</i></code> <code>pri loopback passive off</code>
[ パラメータ ]	<code><i>pri</i></code> ..... PRI 番号 (1..4) <code><i>remote</i></code> ..... 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 <code><i>payload</i></code> ..... 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 <code><i>timeslot</i></code> ..... タイムスロットループバックを示すキーワード <code><i>head</i></code> ..... 先頭タイムスロット番号 (1..24) <code><i>number</i></code> ..... タイムスロット数 (1..24)
[ 説明 ]	相手からのタイムスロットループバックテストに対して待ち受けるモードに入る。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。 <code>remote</code> および <code>payload</code> 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。 <code>timeslot</code> 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。 <code>pri loopback passive off</code> コマンドを実行すると、ループバックテストを終了して待ち受けモードから通常の通信モードへ復帰する。
[ ノート ]	ループバックテストの結果は、実行側にしか表示されない。ディップスイッチを変更して再起動することによってもこのコマンドと同様のモードにすることが可能。ただし、ループバックテスト終了後に再びディップスイッチの変更と再起動が必要。 <code>save</code> 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。

## 22.4.16 ファームウェアファイルを内蔵フラッシュ ROM にコピー

---

[ 入力形式 ]	<code>copy exec <i>file</i> internal</code>
[ パラメータ ]	<code><i>file</i></code> ..... コピー元のファイル名 <code><i>ext0:name</i></code> ..... PCMCIA Flash ATA カードの実行形式ファイル名 <code><i>internal</i></code> ..... 保存先を示すキーワード
[ 説明 ]	RT300i 専用のコマンド。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。

## 23. 設定の表示

### 23.1 機器設定の表示

---

[入力形式]	show environment
[パラメータ]	なし
[説明]	以下の項目が表示される。 システムのリビジョン CPU、メモリの使用量(%) 動作しているファームウェアファイルと起動時に使用した設定ファイルの名前 起動時刻、現在時刻、起動してから現在までの経過時間 セキュリティクラス 電源、ファン、内部温度の状態 (RT300i のみ)

### 23.2 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。

### 23.3 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> 相手先情報番号 anonymous leased <i>peer_num</i> 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。

### 23.4 PC カードの内容の表示

---

[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 internal ..... 内蔵フラッシュ ROM ext0 ..... 外付け Flash ATA カード
[説明]	RT300i 専用のコマンド。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。

### 23.5 マスタクロックを得ている回線の表示

---

[入力形式]	show line masterclock
[パラメータ]	なし
[説明]	RT300i 専用のコマンド。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。

## 24. 状態の表示

### 24.1 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。

### 24.2 インタフェースの状態の表示

---

- [ 入力形式 ]     show status *interface*
- [ パラメータ ]   *interface* .....LAN、BRI、PRI のインタフェース名
- [ 説明 ]         インタフェースの状態を表示する。

### 24.3 各相手先の状態の表示

---

- [ 入力形式 ]     show status pp [*peer\_num*]
- [ パラメータ ]   *peer\_num*  
                   相手先情報番号  
                   anonymous  
                   leased (1BRI モデルのみ)  
                   *peer\_num* 省略時、選択されている相手について表示する
- [ 説明 ]         各相手先の接続中または最後に接続された場合の状態を表示する。  
                   現在接続されているか否か  
                   直前の呼の状態  
                   接続 ( 切断 ) した日時  
                   回線の種類  
                   通信時間  
                   切断理由  
                   通信料金  
                   相手とこちらの PP 側 IP アドレス  
                   正常に送信したパケットの数  
                   送信エラーの数と内分け  
                   正常に受信したパケットの数  
                   受信エラーの数と内分け  
                   PPP の状態  
                   CCP の状態  
                   その他

### 24.4 DHCP サーバの状態の表示

---

- [ 入力形式 ]     show status dhcp
- [ パラメータ ]   なし
- [ 説明 ]         各 DHCP スコープのリース状況を表示する。以下の項目が表示される。  
                   DHCP スコープのリース状態  
                   DHCP スコープ番号  
                   ネットワークアドレス  
                   割り当て中 IP アドレス  
                   割り当て中クライアント MAC アドレス  
                   リース残時間  
                   予約済 ( 未使用 ) IP アドレス  
                   DHCP スコープの全 IP アドレス数  
                   除外 IP アドレス数  
                   割り当て中 IP アドレス数  
                   利用可能アドレス数 ( うち予約済 IP アドレス数



### 24.5 IP の経路情報テーブルの表示

---

- [入力形式]      show ip route [*destination*]
- [パラメータ]    *destination*..... 相手先 IP アドレス  
省略時、経路情報テーブル全体を表示する。
- [説明]           IP の経路情報テーブルまたは相手先 IP アドレスへのゲートウェイを表示する。  
ネットマスクは設定時の表現に関わらず連続するビット数で表現される。  
フレームリレーの場合は DLCI の値が表示される。

### 24.6 IPX の経路情報テーブルの表示

---

- [入力形式]      show ipx route
- [パラメータ]    なし
- [説明]           IPX の経路情報テーブルを表示する。  
フレームリレーの場合は DLCI の値が表示される。

### 24.7 IPv6 の経路情報の表示

---

- [入力形式]      show ipv6 route
- [説明]           IPv6 の経路情報を表示する。

### 24.8 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。

### 24.9 SAP テーブルの表示

---

- [入力形式]      show ipx sap
- [パラメータ]    なし
- [説明]           IPX SAP テーブルを表示する。  
非 ASCII 文字は 8 進数で表示される。

### 24.10 IPXWAN の状態の表示

---

- [入力形式]      show ipx ipxwan [*peer\_num*]
- [パラメータ]    *peer\_num*  
相手先情報番号  
anonymous  
leased  
*peer\_num* 省略時、選択されている相手先について表示する。
- [説明]           IPXWAN の状態を表示する。
- [ノート]         複数 WAN ポートモデルでは leased を指定することはできない。

### 24.11 ブリッジのラーニング情報の表示

---

- [入力形式]      show bridge learning
- [パラメータ]    なし
- [説明]           ブリッジの MAC アドレスのラーニング情報を表示する。  
フレームリレーの場合は DLCI の値が表示される。

### 24.12 RIP で得られた経路情報の表示

---

- [ 入力形式 ]     show ip rip table
- [ パラメータ ]   なし
- [ 説明 ]         RIP で得られた経路情報を表示する。

### 24.13 IPsec の SA の表示

---

- [ 入力形式 ]     show ipsec sa [*id*]
- [ パラメータ ]    *id* ..... SA の識別子
- [ 説明 ]         IPsec の SA の状態を表示する。  
*id* で与えられた識別子を持つ SA の情報を表示する。*id* を指定していない場合は、すべての SA を表示する。

### 24.14 VRRP の情報の表示

---

- [ 入力形式 ]     show status vrrp [*interface* [*vrid*]]
- [ パラメータ ]    *interface* ..... LAN インタフェース名  
*vrid* ..... VRRP グループ ID (1..255)
- [ 説明 ]         VRRP の情報を表示する。

### 24.15 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 ]    *nat\_descriptor*  
                  NAT ディスクリプタ番号 (1..21474836)  
                  all ..... すべての NAT ディスクリプタ番号
- [ 説明 ]         *nat\_descriptor* を省略した場合にはすべての NAT ディスクリプタ番号について表示する。  
動的な NAT ディスクリプタのアドレスマップを表示する。

### 24.16 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*
- [ パラメータ ]    *interface* ..... LAN インタフェース名、pp、tunnel
- [ 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。

### 24.17 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* [*number*]
- [ パラメータ ]    *interface* ..... LAN インタフェース名、pp、tunnel  
*number* ..... pp、tunnel の場合の相手先番号
- [ 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。

### 24.18 OSPF 情報の表示

---

- [ 入力形式 ]     show status ospf *info*
- [ パラメータ ]    *info* ..... 表示する情報の種類  
                  database ..... OSPF のデータベース  
                  neighbor ..... 近隣ルータ  
                  interface ..... 各インタフェースの状態  
                  virtual-link ..... バーチャルリンクの状態
- [ 説明 ]         OSPF の各種情報を表示する。

## 25. ログイン

### 25.1 ログの表示

---

〔入力形式〕	show log less log
〔パラメータ〕	なし
〔説明〕	<p>パワーオンからのログを表示する。</p> <p>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</p>

### 25.2 アカウントの表示

---

〔入力形式〕	show account show account <i>interface</i> show account pp [ <i>peer_num</i> ]
〔パラメータ〕	<p><i>interface</i> ..... BRI、PRI インタフェース名</p> <p><i>peer_num</i> 相手先情報番号 anonymous leased (1BRI モデルのみ) <i>peer_num</i> 省略時、選択されている相手について表示する</p>
〔説明〕	<p>以下の項目を表示</p> <p>発信回数 着信回数 ISDN 料金の総計</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。</p> <p>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。</p>