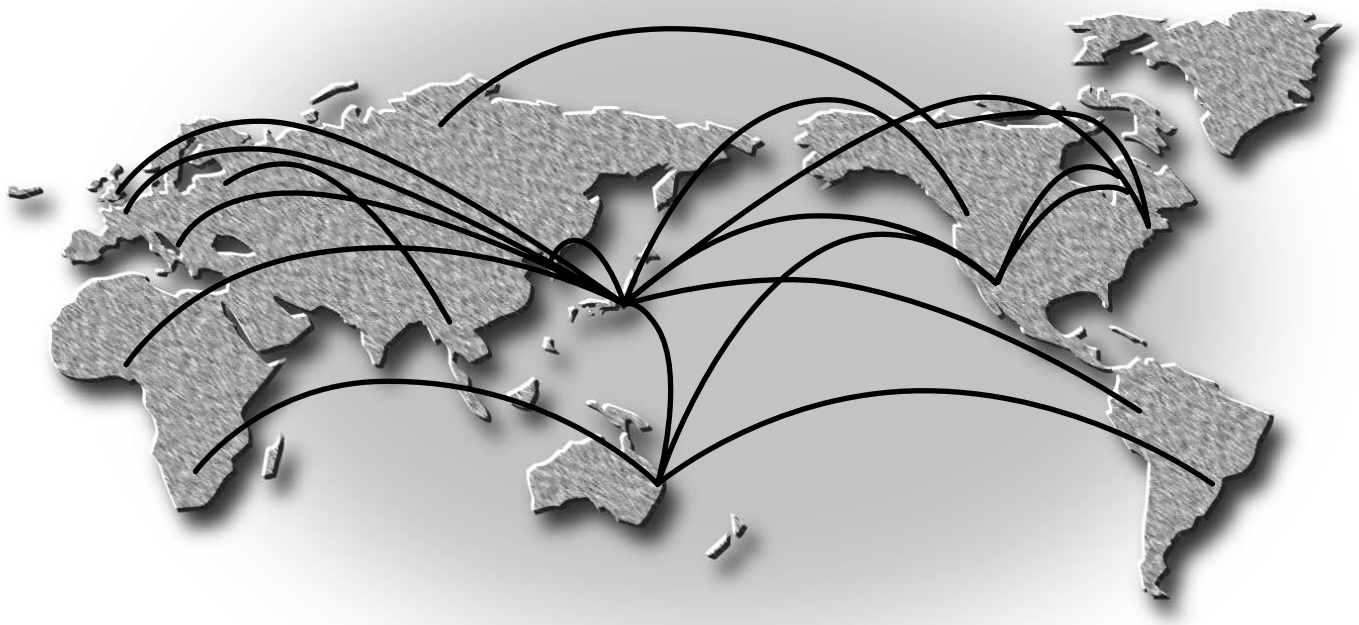
ISDN

REMOTE & BROADBAND ROUTER

コマンドリファレンス

Rev.6.02.14



YAMAHA

目次

1. コマンドリファレンスの見方 17
1.1 対応するプログラムのリビジョン 17
1.2 コマンドリファレンスの見方 17
1.3 インタフェース名について 17
1.4 no で始まるコマンドの入力形式について 18
1.5 相手先情報番号のモデルによる違いについて 18
1.6 コマンドの仕様変更について 18

2. ヘルプ 19
2.1 コンソールに対する簡易説明の表示 19
2.2 コマンド一覧の表示 19

3. 機器の設定 20
3.1 ログインパスワードの設定 20
3.2 管理パスワードの設定 20
3.3 セキュリティクラスの設定 20
3.4 ログインタイマの設定 20
3.5 タイムゾーンの設定 21
3.6 現在の日付けの設定 21
3.7 現在の時刻の設定 21
3.8 リモートホストによる時計の設定 21
3.9 NTP による時計の設定 21
3.10 コンソールの言語とコードの設定 22
3.11 コンソールの表示文字数の設定 22
3.12 コンソールの表示行数の設定 22
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 22
3.14 コンソールのプロンプト表示の設定 23
3.15 SYSLOG を受けるホストの IP アドレスの設定 23
3.16 SYSLOG ファシリティの設定 23
3.17 NOTICE タイプの SYSLOG を出力するか否かの設定 23
3.18 INFO タイプの SYSLOG を出力するか否かの設定 23
3.19 DEBUG タイプの SYSLOG を出力するか否かの設定 24
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 24
3.21 TCP/UDP の各種サービスの動作の設定 24
3.22 SYSLOG パケットの始点ポート番号の設定 24
3.23 マスタクロック用インタフェースの設定 25
3.24 電源の設定 25
3.25 温度監視の閾値の設定 25
3.26 LAN インタフェースの動作タイプの設定 26

4. ISDN 関連の設定 27
4.1 自分側の設定 27
4.1.1 自分の ISDN 番号の設定 27
4.1.2 課金額による発信制限の設定 28
4.1.3 PIAFS の発信方式の設定 28
4.1.4 PIAFS の着信を許可するか否かの設定 28
4.1.5 PIAFS 接続時の起動側の指定 29
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 29
4.1.7 常時接続の設定 29
4.1.8 プロバイダ接続がダウンした時にバックアップする接続先情報番号の指定 30
4.1.9 バックアップからの復帰待ち時間の設定 30
4.1.10 終端抵抗の設定 30
4.1.11 PP で使用するインタフェースの設定 30
4.2 相手側の設定 31
4.2.1 相手への発信順序の設定 31
4.2.2 自動接続の設定 31
4.2.3 自動切断の設定 32
4.2.4 着信許可の設定 32
4.2.5 発信許可の設定 32

4.2.6 再発信抑制タイマの設定 . . . 32
4.2.7 エラー切断後の再発信禁止タイマの設定 . . . 33
4.2.8 相手にコールバック要求を行うか否かの設定 . . . 33
4.2.9 コールバック要求タイプの設定 . . . 33
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 . . . 33
4.2.11 コールバック受け入れタイプの設定 . . . 33
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 . . . 34
4.2.13 コールバックタイマの設定 . . . 34
4.2.14 コールバック待機タイマの設定 . . . 34
4.2.15 ISDN 回線を切断するタイマ方式の指定 . . . 34
4.2.16 切断タイマの設定（ノーマル） . . . 35
4.2.17 入力切断タイマの設定（ノーマル） . . . 35
4.2.18 出力切断タイマの設定（ノーマル） . . . 35
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 . . . 36
4.2.20 切断タイマの設定（ファスト） . . . 36
4.2.21 切断タイマの設定（強制） . . . 36

5. IP の設定 . . . 37
5.1 インタフェース共通の設定 . . . 37
5.1.1 IP アドレスの設定 . . . 37
5.1.2 IP の静的経路情報の設定 . . . 38
5.1.3 IP パケットのフィルタの設定 . . . 39
5.1.4 フィルタセットの定義 . . . 40
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 . . . 40
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 . . . 41
5.1.7 動的フィルタの定義 . . . 41
5.1.8 動的フィルタのタイムアウトの設定 . . . 42
5.1.9 侵入検知機能の動作の設定 . . . 42
5.1.10 フィルタリングによるセキュリティの設定 . . . 43
5.1.11 IP パケットの TOS フィールドの書き換えの設定 . . . 44
5.1.12 インタフェースの MTU の設定 . . . 44
5.1.13 echo, discard, time サービスを動作させるか否かの設定 . . . 44
5.2 代理 ARP の設定 . . . 44
5.3 PP 側の設定 . . . 45
5.3.1 PP 側 IP アドレスの設定 . . . 45
5.3.2 リモート IP アドレスプールの設定 . . . 45
5.4 RIP の設定 . . . 46
5.4.1 RIP による経路の優先度の設定 . . . 46
5.4.2 RIP パケットの送信に関する設定 . . . 46
5.4.3 RIP パケットの受信に関する設定 . . . 46
5.4.4 RIP に関して信用できるゲートウェイの設定 . . . 47
5.4.5 RIP のフィルタリングの設定 . . . 47
5.4.6 RIP で加算するホップ数の設定 . . . 47
5.4.7 RIP2 での認証の設定 . . . 48
5.4.8 RIP2 での認証キーの設定 . . . 48
5.4.9 回線切断時の経路保持の設定 . . . 48
5.4.10 回線接続時の PP 側の RIP の動作の設定 . . . 48
5.4.11 回線接続時の PP 側の RIP 送出の時間間隔の設定 . . . 49
5.4.12 回線切断時の PP 側の RIP の動作の設定 . . . 49
5.4.13 回線切断時の PP 側の RIP 送出の時間間隔の設定 . . . 49
5.5 VRRP の設定 . . . 50
5.5.1 インタフェース毎の VRRP の設定 . . . 50
5.5.2 シャットダウントリガの設定 . . . 50

6. IPX の設定 . . . 51
6.1 インタフェース共通の設定 . . . 51
6.1.1 IPX パケットのフィルタの設定 . . . 52
6.1.2 静的な SAP テーブルの設定 . . . 53
6.1.3 IPX SAP Get Nearest Server Request に応答するか否かの設定 . . . 53
6.2 LAN 側の設定 . . . 53
6.2.1 LAN 側の IPX ネットワーク番号の設定 . . . 54

6.2.2 経路情報の追加 . . . 54
6.2.3 LAN 側の RIP/SAP ブロードキャストの設定 . . . 54
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 . . . 54
6.3 PP 側相手毎の IPX の設定 . . . 55
6.3.1 PP 側 IPX ネットワーク番号の設定 . . . 55
6.3.2 経路情報の追加 . . . 55
6.3.3 回線接続時の PP 側の RIP/SAP の動作の設定 . . . 55
6.3.4 回線接続時の PP 側の RIP/SAP 送出の時間間隔の設定 . . . 56
6.3.5 回線切断時の PP 側の RIP/SAP の動作の設定 . . . 56
6.3.6 回線切断時の PP 側の RIP/SAP 送出の時間間隔の設定 . . . 56
6.3.7 回線切断時に RIP/SAP 情報を保持するか否かの設定 . . . 56
6.3.8 IPXWAN 使用の設定 . . . 56
6.3.9 Timer/Information Request の再送間隔と最大再送回数の設定 . . . 57
6.3.10 IPXWAN プライマリネットワーク番号の設定 . . . 57
6.3.11 Watchdog パケットに対する代理応答の設定 . . . 57
6.3.12 Watchdog 代理応答の時間間隔の設定 . . . 57
6.3.13 SPX キープアライブ代理応答を行うか否かの設定 . . . 57
6.3.14 SPX キープアライブ代理応答のタイマの設定 . . . 58
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 . . . 58
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 . . . 58

7. ブリッジの設定 . . . 59
7.1 インタフェース共通の設定 . . . 59
7.1.1 ブリッジするインタフェースの設定 . . . 59
7.1.2 ブリッジのフィルタの設定 . . . 60
7.1.3 MAC アドレスのラーニングを行うか否かの設定 . . . 60
7.1.4 ラーニング情報消去タイマの設定 . . . 60
7.2 LAN 側の設定 . . . 61
7.2.1 LAN 側でのブリッジのフィルタリングの設定 . . . 61
7.3 PP 側相手毎のブリッジの設定 . . . 61
7.3.1 PP 側でのブリッジのフィルタリングの設定 . . . 61

8. PPP の設定 . . . 62
8.1 相手の名前とパスワードの設定 . . . 62
8.2 要求する認証タイプの設定 . . . 62
8.3 受け入れる認証タイプの設定 . . . 63
8.4 自分の名前とパスワードの設定 . . . 63
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 . . . 63
8.6 LCP 関連の設定 . . . 63
8.6.1 Magic Number オプション使用の設定 . . . 64
8.6.2 Maximum Receive Unit オプション使用の設定 . . . 64
8.6.3 Protocol Field Compression オプション使用の設定 . . . 64
8.6.4 lcp-restart パラメータの設定 . . . 64
8.6.5 lcp-max-terminate パラメータの設定 . . . 65
8.6.6 lcp-max-configure パラメータの設定 . . . 65
8.6.7 lcp-max-failure パラメータの設定 . . . 65
8.6.8 Configure-Request をすぐに送信するか否かの設定 . . . 65
8.6.9 PP 経由のキープアライブを使用するか否かの設定 . . . 65
8.6.10 PP 経由のキープアライブのログをとるか否かの設定 . . . 66
8.6.11 PP 経由のキープアライブの時間間隔の設定 . . . 66
8.6.12 専用線ダウン検出時の動作の設定 . . . 66
8.7 PAP 関連の設定 . . . 66
8.7.1 pap-restart パラメータの設定 . . . 66
8.7.2 pap-max-authreq パラメータの設定 . . . 66
8.8 CHAP 関連の設定 . . . 67
8.8.1 chap-restart パラメータの設定 . . . 67
8.8.2 chap-max-challenge パラメータの設定 . . . 67
8.9 IPCP 関連の設定 . . . 67
8.9.1 Van Jacobson Compressed TCP/IP 使用の設定 . . . 67

8.9.2 PP 側 IP アドレスのネゴシエーションの設定 . . . 67
8.9.3 ipcp-restart パラメータの設定 . . . 67
8.9.4 ipcp-max-terminate パラメータの設定 . . . 68
8.9.5 ipcp-max-configure パラメータの設定 . . . 68
8.9.6 ipcp-max-failure パラメータの設定 . . . 68
8.9.7 IPCP の MS 拡張オプションを使うか否かの設定 . . . 68
8.9.8 WINS サーバの IP アドレスの設定 . . . 68
8.10 IPXCP 関連の設定 . . . 69
8.10.1 ipxcp-restart パラメータの設定 . . . 69
8.10.2 ipxcp-max-terminate パラメータの設定 . . . 69
8.10.3 ipxcp-max-configure パラメータの設定 . . . 69
8.10.4 ipxcp-max-failure パラメータの設定 . . . 69
8.11 BCP 関連の設定 . . . 69
8.11.1 LAN Identification 使用の設定 . . . 69
8.11.2 Tinygram compression 使用の設定 . . . 70
8.11.3 bcp-restart パラメータの設定 . . . 70
8.11.4 bcp-max-terminate パラメータの設定 . . . 70
8.11.5 bcp-max-configure パラメータの設定 . . . 70
8.11.6 bcp-max-failure パラメータの設定 . . . 70
8.12 MSCBCP 関連の設定 . . . 70
8.12.1 mscbcp-restart パラメータの設定 . . . 70
8.12.2 mscbcp-maxretry パラメータの設定 . . . 71
8.13 CCP 関連の設定 . . . 71
8.13.1 全パケットの圧縮タイプの設定 . . . 71
8.13.2 ccp-restart パラメータの設定 . . . 71
8.13.3 ccp-max-terminate パラメータの設定 . . . 71
8.13.4 ccp-max-configure パラメータの設定 . . . 71
8.13.5 ccp-max-failure パラメータの設定 . . . 72
8.14 IPV6CP 関連の設定 . . . 72
8.14.1 IPV6CP を使用するか否かの設定 . . . 72
8.15 MP 関連の設定 . . . 72
8.15.1 MP を使用するか否かの設定 . . . 72
8.15.2 MP の制御方法の設定 . . . 72
8.15.3 MP のための負荷閾値の設定 . . . 73
8.15.4 MP の最大リンク数の設定 . . . 73
8.15.5 MP の最小リンク数の設定 . . . 73
8.15.6 MP のための負荷計測間隔の設定 . . . 73
8.15.7 MP のパケットを分割するか否かの設定 . . . 74
8.16 BACP 関連の設定 . . . 74
8.16.1 bacp-restart パラメータ の設定 . . . 74
8.16.2 bacp-max-terminate パラメータ の設定 . . . 74
8.16.3 bacp-max-configure パラメータ の設定 . . . 74
8.16.4 bacp-max-failure パラメータ の設定 . . . 74
8.16.5 bap-restart パラメータの設定 . . . 75
8.16.6 bap-max-retry パラメータの設定 . . . 75
8.17 PPPoE 関連の設定 . . . 75
8.17.1 PPPoE で使用する LAN インタフェースの指定 . . . 75
8.17.2 アクセスコンセントレータ名の設定 . . . 75
8.17.3 セッションの自動接続の設定 . . . 75
8.17.4 セッションの自動切断の設定 . . . 76
8.17.5 PADI パケットの最大再送回数の設定 . . . 76
8.17.6 PADI パケットの再送時間の設定 . . . 76
8.17.7 PADR パケットの最大再送回数の設定 . . . 76
8.17.8 PADR パケットの再送時間の設定 . . . 76
8.17.9 PPPoE セッションの切断タイマの設定 . . . 76
8.17.10 TCP パケットの MSS の制限の有無とサイズの指定 . . . 77

9. DHCP の設定 . . . 78
9.1 DHCP サーバ・リレーエージェント機能 . . . 78
9.1.1 DHCP の動作の設定 . . . 78
9.1.2 RFC2131 対応動作の設定 . . . 79

9.1.3 DHCP スコープの定義 . . . 80
9.1.4 DHCP 予約アドレスの設定 . . . 81
9.1.5 DHCP オプションの設定 . . . 82
9.1.6 リースする IP アドレスの重複をチェックするか否かの設定 . . . 83
9.1.7 DHCP サーバの指定の設定 . . . 83
9.1.8 DHCP サーバの選択方法の設定 . . . 83
9.1.9 DHCP BOOTREQUEST パケットの中継基準の設定 . . . 83
9.2 DHCP クライアント機能 . . . 84
9.2.1 要求する IP アドレスリース期間の設定 . . . 84
9.2.2 IP アドレス取得要求の再送回数と間隔の設定 . . . 84
9.2.3 DHCP クライアント ID オプションの設定 . . . 84
9.2.4 DHCP クライアントのホスト名の設定 . . . 85
9.2.5 DNS サーバアドレスを取得する LAN インタフェースの設定 . . . 85
9.2.6 DHCP クライアントの状態の表示 . . . 85

10. ICMP の設定 . . . 86
10.1 ICMP Echo Reply を送信するか否かの設定 . . . 86
10.2 ICMP Mask Reply を送信するか否かの設定 . . . 86
10.3 ICMP Parameter Problem を送信するか否かの設定 . . . 86
10.4 ICMP Redirect を送信するか否かの設定 . . . 86
10.5 ICMP Redirect 受信時の処理の設定 . . . 86
10.6 ICMP Time Exceeded を送信するか否かの設定 . . . 87
10.7 ICMP Timestamp Reply を送信するか否かの設定 . . . 87
10.8 ICMP Destination Unreachable を送信するか否かの設定 . . . 87
10.9 受信した ICMP のログを記録するか否かの設定 . . . 87
10.10 ステルス機能の設定 . . . 88
10.11 受信した ICMP のログを記録するか否かの設定 . . . 88
10.12 ICMP を送信するか否かの設定 . . . 88

11. フレームリレー関連の設定 . . . 89
11.1 カプセル化の種類の設定 . . . 89
11.2 DLCI の設定 . . . 90
11.3 PVC 状態確認手順の設定 . . . 90
11.4 InARP 使用の設定 . . . 90
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 . . . 90
11.6 FR 圧縮機能の設定 . . . 91
11.7 DLCI ごとのパラメータの設定 . . . 91
11.8 輻輳制御をするか否かの設定 . . . 91
11.9 回線に対する送信順序方式の設定 . . . 92
11.10 指定パケットに DE ビットを立てるか否かの設定 . . . 92

12. PRI 関連の設定 . . . 93
12.1 PRI 回線の種類の設定 . . . 94
12.2 情報チャネルとタイムスロットの設定 . . . 94
12.3 PP で使用するインタフェースの設定 . . . 94

13. IPsec の設定 . . . 95
13.1 事前共有鍵の登録 . . . 96
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 . . . 96
13.3 相手側のセキュリティ・ゲートウェイの名前の設定 . . . 96
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 . . . 96
13.5 自分側のセキュリティ・ゲートウェイの名前の設定 . . . 97
13.6 鍵交換の再送回数と間隔の設定 . . . 97
13.7 IKE が用いる暗号アルゴリズムの設定 . . . 97
13.8 IKE が用いるグループの設定 . . . 97
13.9 IKE が用いるハッシュアルゴリズムの設定 . . . 98
13.10 自分側の ID の設定 . . . 98
13.11 IKE のログの種類の設定 . . . 98
13.12 IKE ペイロードのタイプの設定 . . . 98
13.13 PFS を用いるか否かの設定 . . . 99
13.14 相手側の ID の設定 . . . 99

13.15 IKE の情報ペイロードを送信するか否かの設定 99
13.16 SA 関連の設定 99
13.16.1 SA の寿命の設定 100
13.16.2 SA の削除 100
13.16.3 SA の手動更新 100
13.16.4 SA を自動更新するか否かの設定 100
13.17 トンネルインタフェース関連の設定 100
13.17.1 使用する SA のポリシーの設定 100
13.17.2 IPComp によるデータ圧縮の設定 101
13.17.3 トンネルインタフェースの使用許可の設定 101
13.17.4 トンネルインタフェースの使用不許可の設定 101
13.17.5 トンネルインタフェース番号の選択 101
13.17.6 IKE キープアライブの設定 102
13.17.7 トンネルバックアップの設定 102
13.17.8 トンネルインタフェースに対する静的経路の無効化 102
13.18 トランスポートモード関連の設定 102

14. SNMP の設定 103
14.1 読み出し専用のコミュニティ名の設定 103
14.2 読み書き可能なコミュニティ名の設定 103
14.3 認証失敗時 (authenticationFailure) にトラップを送信するか否かの設定 103
14.4 SNMP によるアクセスを許可するホストの設定 103
14.5 sysContact の設定 104
14.6 sysLocation の設定 104
14.7 sysName の設定 104
14.8 SNMP トラップのコミュニティ名の設定 104
14.9 SNMP トラップの送信先の設定 104
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 105
14.11 PP インタフェースのアドレスの強制表示の設定 105
14.12 SNMP 送信パケットの始点アドレスの設定 105

15. RADIUS の設定 106
15.1 RADIUS による認証を使用するか否かの設定 106
15.2 RADIUS によるアカウントを使用するか否かの設定 106
15.3 RADIUS サーバの指定 106
15.4 RADIUS 認証サーバの指定 106
15.5 RADIUS アカウントサーバの指定 107
15.6 RADIUS 認証サーバの UDP ポートの設定 107
15.7 RADIUS アカウントサーバの UDP ポートの設定 107
15.8 RADIUS シークレットの設定 107
15.9 RADIUS 再送信パラメータの設定 107

16. NAT 機能 108
16.1 インタフェースへの NAT ディスクリプタ適用の設定 108
16.2 NAT ディスクリプタの動作タイプの設定 108
16.3 NAT 処理の外側 IP アドレスの設定 109
16.4 NAT 処理の内側 IP アドレスの設定 109
16.5 静的 NAT エントリの設定 109
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 110
16.7 静的 IP マスカレードエントリの設定 110
16.8 NAT の IP アドレスマップの消去タイマの設定 110
16.9 IP マスカレードテーブルの TTL 処理方式の設定 110
16.10 外側から受信したパケットに該当する変換テーブルが存在しないときの動作の設定 111
16.11 NAT のアドレス割当をログに記録するか否かの設定 111

17. DNS の設定 112
17.1 DNS を利用するか否かの設定 112
17.2 DNS サーバの IP アドレスの設定 112
17.3 DNS サーバを通知してもらう相手先情報番号の設定 112
17.4 DNS 問い合わせの内容に応じた DNS サーバの選択 113
17.5 DNS ドメイン名の設定 113
17.6 プライベートアドレスに対する問い合わせを処理するか否かの設定 114
17.7 DHCP/IPCP MS 拡張で DNS サーバを通知する順序の設定 114

17.8 SYSLOG 表示で DNS により名前解決するか否かの設定 . . . 114
17.9 静的 DNS レコードの登録 . . . 115

18. 優先制御／帯域制御 . . . 116
18.1 インタフェース速度の設定 . . . 116
18.2 クラス分けのためのフィルタ設定 . . . 116
18.3 キューイングアルゴリズムタイプの選択 . . . 119
18.4 デフォルトクラスの設定 . . . 119
18.5 クラス分けフィルタの適用 . . . 119
18.6 クラスの属性の設定 . . . 120
18.7 クラス毎のキュー長の設定 . . . 120
18.8 MP インタリーブの設定 . . . 121

19. OSPF . . . 122
19.1 OSPF の有効設定 . . . 122
19.2 OSPF の使用設定 . . . 122
19.3 OSPF による経路の優先度設定 . . . 122
19.4 OSPF のルータ ID 設定 . . . 122
19.5 外部プロトコルによる経路導入 . . . 123
19.6 外部経路導入に適用するフィルタ定義 . . . 123
19.7 OSPF エリア設定 . . . 124
19.8 エリアへの経路広告 . . . 124
19.9 スタブ的接続の広告 . . . 124
19.10 仮想リンク設定 . . . 125
19.11 指定インタフェースの OSPF エリア設定 . . . 126
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 . . . 127

20. IPv6 . . . 128
20.1 IPv6 アドレスの管理 . . . 128
20.1.1 インタフェースの IPv6 アドレスの設定 . . . 128
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 . . . 128
20.2 近隣探索 . . . 129
20.2.1 ルータ広告で配布するプレフィックスの定義 . . . 129
20.2.2 ルータ広告の送信の制御 . . . 129
20.3 経路制御 . . . 130
20.3.1 IPv6 の経路情報の追加 . . . 130
20.4 RIPng . . . 130
20.4.1 RIPng の使用の設定 . . . 130
20.4.2 インタフェースにおける RIPng の送信ポリシーの設定 . . . 130
20.4.3 インタフェースにおける RIPng の受信ポリシーの設定 . . . 131
20.4.4 インタフェースにおける信頼できる RIPng ゲートウェイの設定 . . . 131
20.4.5 RIPng の加算ホップ数の設定 . . . 131
20.4.6 RIPng で送受信する経路に対するフィルタリングの設定 . . . 131
20.4.7 回線接続時の PP 側の RIPng の動作の設定 . . . 132
20.4.8 回線接続時の PP 側の RIPng 送出の時間間隔の設定 . . . 132
20.4.9 回線切断時の PP 側の RIPng の動作の設定 . . . 132
20.4.10 回線切断時の PP 側の RIPng 送出の時間間隔の設定 . . . 132
20.4.11 RIPng による経路を回線切断時に保持するか否かの設定 . . . 133
20.5 フィルタの設定 . . . 133
20.5.1 IPv6 フィルタの定義 . . . 133
20.5.2 IPv6 フィルタの削除 . . . 133
20.5.3 IPv6 フィルタの適用 . . . 133
20.6 トンネルリング . . . 134
20.6.1 トンネルインタフェースの種別の設定 . . . 134
20.6.2 トンネルインタフェースの端点 IP アドレスの設定 . . . 134
20.7 管理ツール . . . 134
20.7.1 ping の実行 . . . 134
20.7.2 traceroute の実行 . . . 134

21. スケジュール . . . 135
21.1 スケジュールの設定 . . . 135

22. 操作 . . . 137

22.1 相手先情報番号の選択 137
22.2 設定に関する操作 137
22.2.1 終了 137
22.2.2 設定内容の保存 137
22.2.3 設定ファイルの削除 137
22.2.4 実行形式ファームウェアファイルの削除 138
22.2.5 設定ファイルの一覧 138
22.2.6 設定の初期化 138
22.2.7 遠隔地のルータの設定 138
22.2.8 遠隔地のルータからの設定に対する制限 138
22.3 動的情報のクリア操作 139
22.3.1 IP の動的経路情報のクリア 139
22.3.2 IPX の動的経路情報のクリア 139
22.3.3 IPX の動的 SAP 情報のクリア 139
22.3.4 ブリッジのラーニング情報のクリア 139
22.3.5 ログのクリア 139
22.3.6 アカウントのクリア 139
22.3.7 InARP のクリア 140
22.3.8 DNS キャッシュのクリア 140
22.3.9 PRI のステータス情報のクリア 140
22.3.10 NAT アドレステーブルのクリア 140
22.3.11 インタフェースの NAT アドレステーブルのクリア 140
22.3.12 IPv6 の動的経路情報の消去 140
22.3.13 近隣キャッシュの消去 140
22.4 その他の操作 141
22.4.1 相手先の使用不許可の設定 141
22.4.2 再起動 141
22.4.3 インタフェースの再起動 141
22.4.4 PP インタフェースの再起動 141
22.4.5 発信 142
22.4.6 切断 142
22.4.7 ping 142
22.4.8 traceroute 142
22.4.9 telnet 143
22.4.10 telnet サーバ機能の ON/OFF の設定 143
22.4.11 telnet サーバ機能の listen ポートの設定 143
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 144
22.4.13 PRI のループバックの実行 144
22.4.14 PRI のループバック待ち受けの設定 145
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 145

23. 設定の表示 146
23.1 機器設定の表示 146
23.2 すべての設定内容の表示 146
23.3 指定した PP の設定内容の表示 146
23.4 PC カードの内容の表示 146
23.5 マスタクロックを得ている回線の表示 146

24. 状態の表示 147
24.1 ARP テーブルの表示 147
24.2 インタフェースの状態の表示 147
24.3 各相手先の状態の表示 147
24.4 DHCP サーバの状態の表示 147
24.5 IP の経路情報テーブルの表示 148
24.6 IPX の経路情報テーブルの表示 148
24.7 IPv6 の経路情報の表示 148
24.8 近隣キャッシュの表示 148
24.9 SAP テーブルの表示 148
24.10 IPXWAN の状態の表示 148
24.11 ブリッジのラーニング情報の表示 148
24.12 RIP で得られた経路情報の表示 149

24.13 IPsec の SA の表示 149
24.14 VRRP の情報の表示 149
24.15 動的 NAT ディスクリプタのアドレスマップの表示 149
24.16 動作中の NAT ディスクリプタの適用リストの表示 149
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 149
24.18 OSPF 情報の表示 150

25. ロギング 151
25.1 ログの表示 151
25.2 アカウントの表示 151

コマンド索引

A

account threshold 28
account threshold pp 28
administrator 137
administrator password 20

B

bridge filter 60
bridge group 59
bridge interface filter 61
bridge interface learning 61
bridge learning 60
bridge learning expire 60
bridge pp filter 61
bridge pp learning 61
bridge use 59

C

clear account 139
clear account pp 139
clear arp 139
clear bridge learning 139
clear dns cache 140
clear inarp 140
clear ip dynamic routing 139
clear ipv6 dynamic routing 140
clear ipv6 neighbor cache 140
clear ipx dynamic routing 139
clear ipx dynamic sap 139
clear log 139
clear nat descriptor dynamic 140
clear nat descriptor interface dynamic 140
clear nat descriptor interface dynamic pp 140
clear nat descriptor interface dynamic tunnel . . . 140
clear pri status 140
cold start 138
connect 142
console character 22
console columns 22
console info 22
console lines 22
console prompt 23
copy exec 145

D

date 21
delete config 137
delete exec 138
dhcp client client-identifier 84
dhcp client hostname 85
dhcp duplicate check 83
dhcp relay select 83
dhcp relay server 83
dhcp relay threshold 83
dhcp scope 80
dhcp scope bind 81
dhcp scope option 82
dhcp server rfc2131 compliant 79
dhcp service 78
disconnect 142
dns domain 113
dns notice order 114
dns private address spoof 114
dns server dhcp 85
dns server ip_address 112
dns server pp 112
dns server select 113
dns static 115
dns syslog resolv 114

E

exit 137

F

fr backup 90
fr cir 91
fr compression use 91
fr congestion control 91
fr de 92
fr dlci 90
fr inarp 90
fr lmi 90
fr pp dequeue type 92

H

help 19

I

interface reset 141
interface reset pp 141
ip filter 39
ip filter directed-broadcast 41
ip filter dynamic 41
ip filter dynamic timer 42
ip filter set 40
ip filter source-route 40
ip host 115
ip icmp echo-reply send 86
ip icmp log 87
ip icmp mask-reply send 86
ip icmp parameter-problem send 18, 86
ip icmp redirect receive 86
ip icmp redirect send 86
ip icmp time-exceeded send 87
ip icmp timestamp-reply send 87
ip icmp unreachable send 87
ip interface address 37
ip interface dhcp lease time 84
ip interface dhcp retry 84
ip interface intrusion detection 42
ip interface mtu 44
ip interface nat descriptor 108
ip interface ospf area 126
ip interface ospf neighbor 127
ip interface proxyarp 44
ip interface rip auth key 48
ip interface rip auth text 48
ip interface rip auth type 48
ip interface rip filter 47
ip interface rip hop 47
ip interface rip receive 46
ip interface rip send 46

ip interface rip trust gateway 47
ip interface secondary address 37
ip interface secure filter 43
ip interface vrrp 50
ip interface vrrp shutdown trigger 50
ip pp address 37
ip pp intrusion detection 42
ip pp nat descriptor 108
ip pp ospf area 126
ip pp remote address 45
ip pp remote address pool 45
ip pp rip auth key 48
ip pp rip auth text 48
ip pp rip auth type 48
ip pp rip connect interval 49
ip pp rip connect send 48
ip pp rip disconnect interval 49
ip pp rip disconnect send 49
ip pp rip filter 47
ip pp rip hold routing 48
ip pp rip hop 47
ip pp rip receive 46
ip pp rip send 46
ip pp rip trust gateway 47
ip pp secure filter 43
ip route 38
ip routing 37
ip simple service 24
ip stealth 88
ip tos supersede 44
ip tunnel hide static route 102
ip tunnel intrusion detection 42
ip tunnel nat descriptor 108
ip tunnel ospf area 126
ip tunnel secure filter 43
ipsec auto refresh 100
ipsec ike duration ipsec-sa 100
ipsec ike encryption 97
ipsec ike group 97
ipsec ike hash 98
ipsec ike keepalive use 102
ipsec ike local address 96
ipsec ike local id 98
ipsec ike local name 97
ipsec ike log 98
ipsec ike payload type 98
ipsec ike pfs 99
ipsec ike pre-shared-key 96
ipsec ike remote address 96
ipsec ike remote id 99
ipsec ike remote name 96
ipsec ike retry 97
ipsec ike send info 99
ipsec ipcomp type 101
ipsec refresh sa 100
ipsec sa delete 100
ipsec sa policy 99
ipsec transport 102
ipsec tunnel 100
ipv6 filter 133
ipv6 filter delete 133
ipv6 icmp 88
ipv6 icmp log 88
ipv6 interface address 128
ipv6 interface rip filter 131
ipv6 interface rip receive 131
ipv6 interface rip send 130
ipv6 interface rip trust gateway 131
ipv6 interface rtadv send 129
ipv6 interface secure filter 133
ipv6 pp address 128
ipv6 pp rip connect interval 132
ipv6 pp rip connect send 132
ipv6 pp rip disconnect interval 132
ipv6 pp rip disconnect send 132
ipv6 pp rip filter 131
ipv6 pp rip hold routing 133
ipv6 pp rip hop 131
ipv6 pp rip receive 131
ipv6 pp rip send 130
ipv6 pp rip trust gateway 131
ipv6 pp rtadv send 129
ipv6 pp secure filter 133
ipv6 prefix 129
ipv6 rip use 130
ipv6 route 130
ipv6 stealth 88
ipv6 tunnel address 128
ipx filter 52
ipx interface frame type 53
ipx interface network 54
ipx interface ripsap broadcast 54
ipx interface route 54
ipx interface secure filter 54
ipx pp ipxwan primnet 57
ipx pp ipxwan retry 57
ipx pp ipxwan use 56
ipx pp network 55
ipx pp ripsap connect interval 56
ipx pp ripsap connect send 55
ipx pp ripsap disconnect interval 56
ipx pp ripsap disconnect send 56
ipx pp ripsap hold 56
ipx pp route 55
ipx pp routing 55
ipx pp secure filter 58
ipx pp serialization filter 58
ipx pp spx keepalive proxy 57
ipx pp spx keepalive timer 58
ipx pp watchdog interval 57
ipx pp watchdog proxy 57
ipx routing 51
ipx sap 53
ipx sap response 53
isdn arrive permit 32
isdn auto connect 31
isdn auto disconnect 32
isdn call block time 32
isdn call permit 32
isdn call prohibit time 33
isdn callback mscbcp user-specify 34
isdn callback permit 33
isdn callback permit type 33
isdn callback request 33
isdn callback request type 33
isdn callback response time 34
isdn callback wait time 34
isdn disconnect input time 35
isdn disconnect interval time 36
isdn disconnect output time 35
isdn disconnect policy 34
isdn disconnect time 35

isdn fast disconnect time 36
isdn forced disconnect time 36
isdn local address 27
isdn piafs arrive 28
isdn piafs call 28
isdn piafs control 29
isdn remote address 31
isdn remote call order 31
isdn terminator 30

L

lan type 26
leased backup 29
leased keepalive down 66
less config 146
less config pp 146
less file list 146
less log 151
line masterclock 25
line type 27, 94
login password 20
login timer 20

N

nat descriptor address inner 109
nat descriptor address outer 109
nat descriptor log 111
nat descriptor masquerade rlogin 110
nat descriptor masquerade static 110
nat descriptor masquerade ttl hold 110
nat descriptor static 109
nat descriptor timer 110
nat descriptor type 108
ntpdate 21

O

ospf area 124
ospf area network 124
ospf area stubhost 124
ospf configure refresh 122
ospf import filter 123
ospf import from 123
ospf preference 122
ospf router id 122
ospf use 122
ospf virtual-link 125

P

ping 142
ping6 134
pp always-on 29
pp auth accept 63
pp auth multi connect prohibit 63
pp auth myname 18, 63
pp auth request 62
pp auth username 18, 62
pp backup 30
pp backup recovery time 18, 30
pp bind 30, 94
pp disable 141
pp enable 141
pp encapsulation 89
pp keepalive interval 18, 66
pp keepalive log 18, 66
pp keepalive use 18, 65
pp select 137
ppp bacp maxconfigure 74
ppp bacp maxfailure 74
ppp bacp maxterminate 74
ppp bacp restart 74
ppp bap maxretry 75
ppp bap restart 75
ppp bcp lanid 69
ppp bcp maxconfigure 70
ppp bcp maxfailure 70
ppp bcp maxterminate 70
ppp bcp restart 70
ppp bcp tinycomp 70
ppp ccp maxconfigure 71
ppp ccp maxfailure 72
ppp ccp maxterminate 71
ppp ccp restart 71
ppp ccp type 71
ppp chap maxchallenge 67
ppp chap restart 67
ppp ipcp ipaddress 67
ppp ipcp maxconfigure 68
ppp ipcp maxfailure 68
ppp ipcp maxterminate 68
ppp ipcp msext 68
ppp ipcp restart 67
ppp ipcp vjc 67
ppp ipxcp maxconfigure 69
ppp ipxcp maxfailure 69
ppp ipxcp maxterminate 69
ppp ipxcp restart 69
ppp lcp acfc 63
ppp lcp magicnumber 64
ppp lcp maxconfigure 65
ppp lcp maxfailure 65
ppp lcp maxterminate 65
ppp lcp mru 64
ppp lcp pfc 64
ppp lcp restart 64
ppp lcp silent 65
ppp mp control 72
ppp mp divide 74
ppp mp interleave 121
ppp mp load threshold 73
ppp mp maxlink 73
ppp mp minlink 73
ppp mp timer 73
ppp mp use 72
ppp mscbcp maxretry 71
ppp mscbcp restart 70
ppp pap maxauthreq 66
ppp pap restart 66
pppoe access concentrator 75
pppoe auto connect 75
pppoe auto disconnect 76
pppoe disconnect time 76
pppoe padi maxretry 76
pppoe padi restart 76
pppoe padr maxretry 76
pppoe padr restart 76
pppoe tcp mss limit 77
pppoe use 75
pri leased channel 94
pri loopback active 144
pri loopback passive 145

pri loopback passive off 145

Q

queue class filter 116
queue interface class filter list 119
queue interface class property 120
queue interface default 119
queue interface length 120
queue interface type 119
queue pp class property 120
queue pp type 119
quit 137

R

radius account 106
radius account port 107
radius account server 107
radius auth 106
radius auth port 107
radius auth server 106
radius retry 107
radius secret 107
radius server 106
rdate 21
remote setup accept 138
remote setup interface 138
restart 141
rip preference 46
rip use 46

S

save 137
schedule at 135
security class 20
show account 151
show account pp 151
show arp 147
show bridge learning 148
show command 19
show config 146
show config list 138
show config pp 146
show environment 146
show file list 146
show ip rip table 149
show ip route 148
show ipsec sa 149
show ipv6 address 128
show ipv6 neighbor cache 148
show ipv6 route 148
show ipx ipxwan 148
show ipx route 148
show ipx sap 148
show line masterclock 146
show log 151
show nat descriptor address 149
show nat descriptor interface address 149
show nat descriptor interface bind 149
show status 147
show status dhcp 147
show status dhcpc 85
show status ospf 150
show status pp 147
show status vrrp 149
snmp community read-only 103
snmp community read-write 103
snmp display ipcp force 105
snmp enableauthentraps 103
snmp host 103
snmp local address 105
snmp syscontact 104
snmp syslocation 104
snmp sysname 104
snmp trap community 104
snmp trap host 104
snmp yrifppdisplayatmib2 105
speed interface 116
speed pp 116
syslog debug 24
syslog facility 23
syslog host 23
syslog info 23
syslog notice 23
syslog srcport 24
system power 2 use 25
system temperature threshold 25

T

telnet 143
telnetd host 144
telnetd listen 143
telnetd service 143
tftp host 24
time 21
timezone 21
traceroute 142
traceroute6 134
tunnel backup 102
tunnel disable 101
tunnel enable 101
tunnel encapsulation 18, 134
tunnel endpoint address 18, 134
tunnel select 101

W

wins server 68

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／ブロードバンドルータのファームウェア、**Rev.6.02.14** 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 で始まる形のものが並記されているコマンドが多数あります。no で始まる形式を使うと、特別な記述がない限り、そのコマンドの設定を削除し、デフォルト値に戻します。

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

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

1.5 相手先情報番号のモデルによる違いについて

相手先情報番号はモデルによって使用できる数値の範囲が異なります。

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

1.6 コマンドの仕様変更について

以下のコマンドは仕様変更されています。プログラムの古いリビジョンから Rev.6.02.14 以降へ変更する場合には注意が必要となります

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

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

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

[説明] セキュリティクラスを設定する。

[ノート] remote setup accept コマンドにより、遠隔地のルータからのログイン（remote setup）を細かくアクセス制限することができる。

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

3.4 ログインタイマの設定

[入力形式] login timer *time*
no login timer [*time*]

[パラメータ]
- *time*
  - 秒数 ..... キー入力がない場合に自動的にログアウトするまでの秒数（30.. 21474836）
  - clear ..... ログインタイマを設定しない

[説明] キー入力がない場合に自動的にログアウトするまでの時間を設定する。

[ノート] TELNET でログインした場合、clear が設定されていてもタイマ値は 300 秒として扱う。

[デフォルト値] 300

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

[説明]　タイムゾーンを設定する。

[デフォルト値]　jst

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 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 サーバはできるだけ近くのものを指定した方が良い。利用可能な NTP サーバについてはプロバイダに問い合わせること。
YAMAHA ルータ自身は NTP サーバになれない。
syslog キーワードを指定した場合には、コマンドの出力結果を INFO レベルの SYSLOG へ出力する。

3.10 コンソールの言語とコードの設定

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

[パラメータ] ○ *code*
- ascii .....英語で表示する、文字コードは ASCII
- sjis ..... 日本語で表示する、文字コードはシフト JIS
- euc ..... 日本語で表示する、文字コードは EUC

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

[ノート] 本コマンドの設定は、save コマンドで保存するまで show config コマンドによる設定の表示に反映されない。

[デフォルト値] sjis

3.11 コンソールの表示文字数の設定

[入力形式] console columns *col*
no console columns [*col*]

[パラメータ] ○ *col* .....コンソールの表示文字数 (80..200)

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

[ノート] 本コマンドの設定は、save コマンドで保存するまで show config コマンドによる設定の表示に反映されない。

[デフォルト値] 80

3.12 コンソールの表示行数の設定

[入力形式] console lines *lines*
no console lines [*lines*]

[パラメータ] ○ *lines*
- 整数 (10 ..100)
- infinity.....スクロールを止めない

[説明] コンソールの表示行数を設定する。
このコマンドは一般ユーザでも実行できる。

[ノート] 本コマンドの設定は、save コマンドで保存するまで show config コマンドによる設定の表示に反映されない。

[デフォルト値] 24

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 *info*
no console info *info*

[パラメータ] ○ *info*
- on.....表示する
- off.....表示しない

[説明] コンソールにシステムのメッセージを表示するか否かを設定する。

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

[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 *debug*
no syslog debug [*debug*]

[パラメータ] ◦ *debug*
- on ..... 出力する
- off ..... 出力しない

[説明] ISDN および、PPP のデバッグ情報等を SYSLOG で出力するか否かを設定する。

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

[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 [*host*]

[パラメータ] ◦ *host*
- IP アドレス ..... TFTP によりアクセスできるホストの IP アドレス（IPv6 アドレス可）
- any ..... すべてのホストから TFTP によりアクセスできる
- none ..... すべてのホストから TFTP によりアクセスできない

[説明] TFTP によりアクセスできるホストの 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 TCP/UDP の各種サービスの動作の設定

[入力形式] ip simple-service *switch*

[パラメータ] ◦ *switch* ..... 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

3.22 SYSLOG パケットの始点ポート番号の設定

[入力形式] syslog srcport *port*
no syslog srcport [*port*]

[パラメータ] ◦ *port* ..... 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

3.23　マスタクロック用インタフェースの設定

[入力形式]　line masterclock *interface*
no line masterclock

[パラメータ]　○ *interface*
- インタフェース名
- auto ..... 自動選択

[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。
auto を設定した場合は、実際に回線が接続されている BRI/PRI インタフェースの中からマスタクロックを供給するインタフェースを自動的に選択する。選択基準は、BRI よりは PRI を優先し、同じ回線種別の中ではより若番のポート番号を持つインタフェースを優先する。マスタとなるインタフェースの回線がダウンしてクロックを得られなくなった場合には、同じモジュール内のインタフェースを優先して、次のマスタクロック供給インタフェースを選択する。すべての回線がダウンしている場合には内部クロックを用いたフリーラン状態となる。
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。

[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いけない。

[デフォルト値]　auto

3.24　電源の設定

[入力形式]　system power *module* use *sw*
no system power *module* use [*sw*]

[パラメータ]　○ *module* ..... モジュール番号 (1,2)
○ *sw*
- on ..... モジュールを装着している
- off ..... モジュールを装着していない

[説明]　RT300i 専用のコマンド。
電源モジュールの装着状態を設定する。電源モジュールからの電源供給自体は、実際に装着すればこのコマンドに関係なく機能するが、このコマンドを設定することで電源モジュールの監視機能が正しく働くようになる。

[ノート]　電源モジュールを装着していないにも関わらず、*sw* を on に設定すると、監視機能が働き電源モジュールの異常を報告する。

[デフォルト値]　モジュール 1 = off
モジュール 2 = on

3.25　温度監視の閾値の設定

[入力形式]　system temperature threshold *t1 t2*
no system temperature threshold *t1 t2*

[パラメータ]　○ *t1* ..... 警告を発する温度 (℃)
○ *t2* ..... 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、*t1* 以上の温度になると SYSLOG や ALM ランプで警告を発する。一度、警告が発せられると、温度が *t2* を下回らない限り、ALM ランプは消えない。

[デフォルト値]　*t1* = 80
t2 = 75

3.26 LAN インタフェースの動作タイプの設定

[入力形式]

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

[パラメータ]

- *interface* .....LAN インタフェース名
- *speed_type*.....LAN 動作タイプ
  - auto .....自動判別
  - 10-hdx..... 10MHz 半二重
  - 10-fdx..... 10MHz 全二重
  - 100-hdx..... 100MHz 半二重
  - 100-fdx..... 100MHz 全二重
  - 省略時は auto
- *port* .....(スイッチングハブ内蔵機種のみ)
  - スイッチングハブのポート番号 (1 .. 4)
  - 省略時は全ポート
- *group_type*.....ポートの属するネットワークあるいは無効化の指定
  - primary .....指定ポートはプライマリアドレスネットワークに属する
  - secondary.....指定ポートはセカンダリアドレスネットワークに属する
  - disable .....指定ポートは使用しない
- *routing* .....IP ルーティング接続
  - on.....指定ポートをルーティング機能と接続する
  - off.....指定ポートをルーティング機能と接続しない
  - 省略時は on
- *sw* .....クロスストレート自動判別機能を使用するか否か (スイッチングハブインタフェースのみ)
  - on.....クロスストレート自動判別機能を使用する
  - off.....クロスストレート自動判別機能を使用しない

[説明]

指定した LAN インタフェースの速度と動作モードの種類を設定する。
キーワード port-based-ks8995e を指定するとネットワークに属するポートを限定し、ネットワーク間での IP 通信を制限することができる。

[ノート]

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

port-based-ks8995e と auto-crossover キーワードが使用できるのは RT105p と RT105e のみである。

port-based-ks8995e を指定した場合、primary 指定しかなされておらずかつ指定されていないポートがある場合には、残りのポートはセカンダリアドレスネットワークに属する。primary 指定と secondary 指定がなされ、かつどちらにも指定されていないポートがある場合には、そのポートは disable 指定されたものとみなされ、他との通信は一切遮断される。

ip-routing=off を指定されたネットワークのポートに接続されたホストは、それらのポートに接続されたホスト以外との通信は一切遮断される。YAMAHA ルータ自身との通信も遮断される。

YAMAHA ルータ自身からのブロードキャストパケットは、ip-routing=off の指定がされていない限り、どちらのネットワークにも送出される。動的経路制御の使用は制限される。

[デフォルト値]

speed_type = auto
port-based-ks8995e 指定なし
auto-crossover = on

[設定例]

例 1)

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

ポート 1,2 は 100BASE-TX 全二重、その他のポートはオートネゴシエーションで接続する。

例 2)

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

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

例 3)

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

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

4. ISDN 関連の設定

RT105p 及び RT105e では、ISDN に関する設定は使用できません。

4.1 自分側の設定

4.1.1 BRI 回線の種類の指定

[入力形式]
line type *interface line* [*channels*]
no line type *interface line* [*channels*]

[パラメータ]
- *interface* ..... BRI インタフェース名
- *line*
  - isdn, isdn-ntt..... ISDN 回線交換
  - l64..... ディジタル専用線、64kbit/s
  - l128..... ディジタル専用線、128kbit/s
- *channels* .....*line* パラメータが isdn 、isdn-ntt の場合のみ指定可
  - 1b..... B チャネルは 1 チャネルだけ使用
  - 2b..... B チャネルは 2 チャネルとも使用する

[説明]
BRI 回線の種類を指定する。設定の変更は、再起動か、あるいは該当インタフェースに対する interface reset コマンドの発行により反映される。

[ノート]
別の通信機器の発着信のために 1B チャネルを確保したい場合は *channels* パラメータを 1b に設定する。

[デフォルト値]
line = isdn
channels = 2b

4.1.2 自分の ISDN 番号の設定

[入力形式]
isdn local address *interface isdn_num*[*/sub_address*]
isdn local address *interface /sub_address*
no isdn local address *interface*

[パラメータ]
- *interface* ..... BRI/PRI インタフェース名
- *isdn_num* ..... ISDN 番号
- *sub_address* ..... ISDN サブアドレス (0x21 から 0x7e の ASCII 文字)

[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 [*interface*] *yen*
account threshold pp *yen*
no account threshold *interface* [*yen*]
no account threshold [*yen*]
no account threshold pp [*yen*]

[パラメータ]
◦ *interface* .....BRI/PRI インタフェース名
◦ *yen*
- 課金額 .....円 (10..21474836)
- off.....発信制限機能を使わない

[説明]
網から通知される課金の合計 (これは show account コマンドで表示される) の累計が指定した金額に達したらそれ以上の発信を行わないようにする。
account threshold コマンドではルータ全体の合計金額を設定し、*interface* パラメータを指定した場合には、それぞれのインタフェースでの合計金額、account threshold pp コマンドでは選択している相手先に対する発信での合計金額で制御を行う。
課金が網から通知されるのは通信切断時なので、長時間の接続の途中切断することはできず、この場合は制限はできない。この場合に対処するには、isdn forced disconnect time コマンドで通信中でも時間を監視して強制的に回線を切るような設定にしておく方法がある。また、課金合計は clear account コマンドで 0 にリセットでき、schedule at コマンドで定期的に clear account を実行するようにしておくと、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 *speed* [*64kmode*]
no isdn piafs call [*speed* [*64kmode*]]

[パラメータ]
◦ *speed*
- off ..... 発信を同期 PPP とする
- 32k ..... 発信を PIAFS 32k とする
- 64k ..... 発信を PIAFS 64k とする

◦ *64kmode*
- guarantee ..... PIAFS 64k の発信ではギャランティー方式を使用する
- best-effort..... PIAFS 64k の発信ではベストエフォート方式を使用する

[説明]
PIAFS モードの発信を可能にするか否かを設定する。
また、PIAFS モードの速度を選択する。
speed が off に設定されている場合には発信は同期 PPP になり、32k に設定されている場合には発信は PIAFS 32k に、64k に設定されている場合には発信は PIAFS 64k になる。
speed が 64k に設定されている場合には、*64kmode* の設定が有効になる。
64kmode が設定されていない、または guarantee に設定されている場合には、発信はギャランティー方式の PIAFS 64k になる。
64kmode が best-effort に設定されている場合には、発信はベストエフォート方式になる。

[ノート]
PIAFS 64k では特別なサブアドレスが用いられるため、ユーザがコマンドで設定した発サブアドレスは無視される。

[デフォルト値]
off

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。

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

[デフォルト値]
on

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。

[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。

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

[デフォルト値] call

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

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 常時接続の設定

[入力形式] pp always-on *sw* [*time*]

[パラメータ] ◦ *sw*
- on ..... 常時接続する
- off ..... 常時接続しない

◦ *time* ..... 再接続を要求するまでの時間間隔 (60-21474836 秒)

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

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

[デフォルト値] off

4.1.9 プロバイダ接続がダウンした時にバックアップする接続先情報番号の指定

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

[パラメータ] ○ *peer_num*
- バックアップする相手先情報番号
- none .....バックアップをしない

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

[ノート] PP 毎のコマンドである。

接続のダウンを検知するキープアライブ動作が必要なため、
・pp always-on on （専用線以外の場合）
・pp keepalive use lcp-echo （専用線の場合）
のいずれかの設定が同時に必要である。

プロバイダ接続のバックアップなど、バックアップ接続先にバックアップであることを通知する必要のない場合に使用する。

拠点間接続のバックアップでは、専用線接続による leased backup コマンドを使用することもできる。leased backup では相手先にバックアップ接続であることが通知されるので、経路が双方で切り換えられる。

[デフォルト値] none

4.1.10 バックアップからの復帰待ち時間の設定

[入力形式] pp backup recovery time *time*
no pp backup recovery time [*time*]

[パラメータ] ○ *time*
- 秒数 (1..21474836)
- off..... すぐに復帰

[説明] バックアップから復帰する場合には、すぐに復帰させるか、設定された時間だけ待ってから復帰するかを設定する。

[ノート] この設定は、すべての PP で共通に用いられる。また専用線バックアップでも FR バックアップでもこの設定が共通に用いられる。

[デフォルト値] off

4.1.11 終端抵抗の設定

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

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

[説明] 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

4.1.12 PP で使用するインタフェースの設定

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

[パラメータ] ○ *interface* .....BRI/PRI インタフェース名の並び

[説明] 選択されている相手先に対して実際に使用するインタフェースを設定する。

[デフォルト値] どのインタフェースともバインドされていない

4.2 相手側の設定

4.2.1 相手 ISDN 番号の設定

[入力形式] isdn remote address *call_arrive isdn_num*[*/sub_address*][*isdn_num_list*]
isdn remote address *call_arrive isdn_num* [*isdn_num_list*]
no isdn remote address *call_arrive* [*isdn_num*[*/sub_address*][*isdn_num_list*]]

[パラメータ]
- *call_arrive*
  - call ..... 発着信用
  - arrive ..... 着信専用
- *isdn_num* ..... ISDN 番号
- *sub_address* ..... ISDN サブアドレス (0x21 から 0x7e の ASCII 文字)
- *isdn_num_list* ..... ISDN 番号だけまたは ISDN 番号とサブアドレスの組を空白で区切った並び

[説明] 選択されている相手の ISDN 番号とサブアドレスを設定する。ISDN 番号には市外局番も含めて設定する。
選択されている相手が anonymous の場合は無意味である。
複数の ISDN 番号が設定されている場合、まず先頭の ISDN 番号での接続に失敗すると次に指定された ISDN 番号が使われる。同様に、それに失敗すると次の ISDN 番号を使うという動作を続ける。
MP のように相手先に対して複数チャ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ネルで切断された後では、最初に設定された ISDN 番号から発信に使用される。

[ノート] MP を使用する場合は、round にした方が効率がよい。

[デフォルト値] serial

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

[パラメータ] ○ *permit*
- on ..... 許可する
- off ..... 許可しない

[説明] 選択されている相手への発信を許可するか否かを設定する。

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

[デフォルト値] on

4.2.7 再発信抑制タイマの設定

[入力形式] isdn call block time *time*
no isdn call block time [*time*]

[パラメータ] ○ *time* ..... 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が異なる。

[ノート] 切断後すぐに発信ということを繰り返す状況では適当な値を設定すべきである。
isdn forced disconnect time コマンドと併用するとよい。

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

[パラメータ] ◦ *time*..... 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が異なる。

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

[パラメータ] ◦ *callback_request*
- on ..... 要求する
- off..... 要求しない

[説明] 選択されている相手に対してコールバック要求を行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 *type*
no isdn callback request type [*type*]

[パラメータ] ◦ *type*
- 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 *callback_permit*
no isdn callback permit [*callback_permit*]

[パラメータ] ◦ *callback_permit*
- on ..... 応じる
- off..... 応じない

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

[デフォルト値] off

4.2.12 コールバック受け入れタイプの設定

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

[パラメータ] ◦ *type1*, *type2*
- yamaha ..... ヤマハ方式
- 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] *type1* = yamaha
type2 = mscbcp

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

[パラメータ]
- *specify*
  - on ..... 許可する
  - off ..... 拒否する

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

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

[デフォルト値] off

4.2.14 コールバックタイマの設定

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

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

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

[デフォルト値] *t*ime = 5

4.2.15 コールバック待機タイマの設定

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

[パラメータ]
- *time* ..... 秒数 (1..60)

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

[デフォルト値] 60

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

[パラメータ]
- *type*
  - 1 ..... 単純トラフィック監視方式
  - 2 ..... 課金単位時間方式

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

[デフォルト値] 1

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

4.2.17 切断タイマの設定（ノーマル）

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

[パラメータ] ○ *time*
- 秒数 (1..21474836)
- off..... タイマを設定しない

[説明] 選択されている相手について PP 側からデータ受信がない場合の切断までの時間を設定する。秒数は 0.1 秒単位で設定できる。

[ノート] 例えば、UDP パケットを定期的に出すようなプログラムが暴走したような場合、本タイマを設定しておくことにより回線を切断することができる。
4.2.17 切断タイマの設定（ノーマル）のノート参照。

[デフォルト値] 120

4.2.19 出力切断タイマの設定（ノーマル）

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

[パラメータ] ○ *time*
- 秒数 (1..21474836)
- off..... タイマを設定しない

[説明] 選択されている相手について PP 側へのデータ送信がない場合の切断までの時間を設定する。秒数は 0.1 秒単位で設定できる。

[ノート] 例えば、UDP パケットを定期的に出すようなプログラムが暴走したような場合、本タイマを設定しておくことにより回線を切断することができる。
4.2.17 切断タイマの設定（ノーマル）のノート参照。

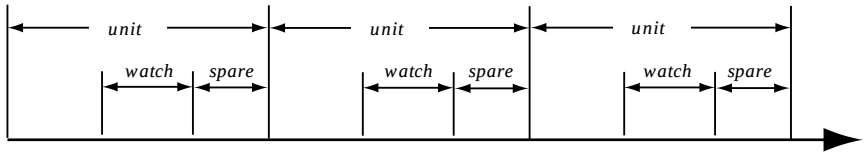
[デフォルト値] 120

4.2.20 課金単位時間方式での課金単位時間と監視時間の設定

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

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

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



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

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

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

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 *routing*
no ip routing [*routing*]

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

[説明] IP パケットをルーティングするかどうかを設定する。

[ノート] off の場合でも TELNET による設定や TFTP によるアクセス、PING 等は可能。

[デフォルト値] on

5.1.2 IP アドレスの設定

[入力形式] ip *interface* address *ip_address*/*mask* [broadcast *broadcast_ip*]
ip *interface* address dhcp
ip pp address *ip_address*/*mask* [broadcast *broadcast_ip*]
ip pp address dhcp
no ip *interface* address [*ip_address*/*mask*]
no ip pp address [*ip_address*/*mask*]

[パラメータ]
- *interface* ..... LAN インタフェース名
- *ip_addres* ..... IP アドレス xxx.xxx.xxx.xxx (xxx は 10 進数)
- dhcp ..... DHCP クライアントとして IP アドレスを取得する
- *mask*
  - xxx.xxx.xxx.xxx (xxx は 10 進数)
  - 0x に続く 16 進数
  - マスクビット数
- *broadcast_ip* ..... ブロードキャスト IP アドレス

[説明] インタフェースの IP アドレスとネットマスクを設定する。"broadcast *broadcast_ip*" を指定すると、ブロードキャストアドレスを指定できる。省略した場合には、ディレクティッドブロードキャストアドレスが使われる。
dhcp を指定すると、設定直後に DHCP クライアントとして IP アドレスを取得する

[ノート] LAN インタフェースに IP アドレスを設定していない場合には、RARP により IP アドレスを得ようとする。
PP インタフェースに IP アドレスを設定していない場合には、そのインタフェースは unnumbered として動作する。DHCP クライアントとして動作させた場合に取得したクライアント ID は、show status dhcpc コマンドで確認することができる。

[デフォルト値] IP アドレスは設定されていない
ディレクティッドブロードキャストアドレスが使われる

5.1.3 セカンダリ IP アドレスの設定

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

[パラメータ]
- *interface* ..... LAN インタフェース名
- *ip_address* ..... セカンダリ IP アドレス xxx.xxx.xxx.xxx (xxx は 10 進数)
- dhcp ..... DHCP クライアントとして IP アドレスを取得する
- *mask*
  - xxx.xxx.xxx.xxx (xxx は 10 進数)
  - 0x に続く 16 進数
  - マスクビット数

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

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

5.1.4 IP の静的経路情報の設定

[入力形式]

ip route *network* gateway *gateway* [*parameter*] [gateway *gateway* [*parameter*]]
no ip route *network* [*gateway...*]

[パラメータ]

◦ *network*
- default .....デフォルト経路
- IP アドレス .....送り先のホスト / マスクビット数 (省略時は 32)

◦ *gateway*
- IP アドレス ..... xxx.xxx.xxx.xxx (xxx は 10 進数)
- pp *pp_num* [dlci=*dlci*] ..... PP インタフェースへの経路
  "dlci=*dlci*" が指定された場合は、フレームリレーの DLCI への経路
  - *pp_num*
    - 相手先情報番号
    - anonymous
- pp anonymous name=*name*
  - *name* ..... PAP/CHAP による名前
- dhcp *interface*
  - *interface* .....DHCP クライアントとして動作する LAN インタフェース名
- tunnel *tunnel_num*.....Tunnel インタフェースへの経路

◦ *parameter* .....以下のパラメータを空白で区切り複数設定可能
- filter *number* [*number*..] ... フィルタ型経路の指定
  - *number* ..... フィルタの番号 (1..21474836) (空白で区切り複数設定可能)
- metric *metric* .....メトリックの指定
  - *metric* ..... メトリック値 (1..15) (省略時は 1)
- hide .....出力インタフェースがPPインタフェースの場合のみ有効なオプションで、回線が接続されている場合だけ経路が有効になることを意味する
- weight *weight*.....異なる経路間の比率を表す値
  - *weight*..... 経路への重み (1..2147483647、省略時は 1)

[説明]

IP の静的経路を設定する。
gateway のパラメータとしてフィルタ型経路を指定した場合には、記述されている順にフィルタを適用していき、適合したゲートウェイが選択される。
適合するゲートウェイが存在しない場合や、フィルタ型経路が指定されているゲートウェイが一つも記述されていない場合には、フィルタ型経路が指定されていないゲートウェイが選択される。
フィルタ型経路が指定されていないゲートウェイも存在しない場合には、その経路は存在しないものとして処理が継続される。
フィルタ型経路が指定されていないゲートウェイが複数記述された場合の経路の選択は、それらの経路を使用する時点でラウンドロビンにより決定される。

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

いずれの場合でも、hide キーワードが指定されているゲートウェイは、回線が接続している場合のみ有効で、回線が接続していない場合には評価されない。

[ノート]

既に存在する経路を上書きすることができる。

[設定例]

◦ デフォルトゲートウェイを 192.168.0.1 とする
```
# ip route default gateway 192.168.0.1
```

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

◦ マルチホーミングによる負荷分散を行う。デフォルトゲートウェイと して 2 経路持ち、PP1 には専用線 128k で、PP2 には専用線 64k で接続しており、かつ各専用線ダウン時の経路を無効としてパケットロスを防ぐ。
※ NAT 機能と専用線キープアライブの併用が必要となる。
```
# ip route default gateway pp 1 weight 2 hide gateway pp 2 weight 1 hide
```

5.1.5 IP パケットのフィルタの設定

[入力形式]　ip filter *filter_num pass_reject src_addr*[/*mask*][*dest_addr*[/*mask*][*protocol* [*src_port_list* [*dest_port_list*]]]]
no ip filter *filter_num* [*pass_reject*]

[パラメータ]

- *filter_num* ..... 静的フィルタ番号 (1..21474836)
- *pass_reject*
  - pass-log..... 一致すれば通す (ログに記録する)
  - pass-nolog..... 一致すれば通す (ログに記録しない)
  - reject-log ..... 一致すれば破棄する (ログに記録する)
  - reject-nolog..... 一致すれば破棄する (ログに記録しない)
  - restrict-log..... 回線が接続されていれば通し、切断されていれば破棄する (ログに記録する)
  - restrict-nolog..... 回線が接続されていれば通し、切断されていれば破棄する (ログに記録しない)
- *src_addr* ..... IP パケットの始点 IP アドレス
  - xxx.xxx.xxx.xxx xxx は
    - 10 進数
    - * (ネットマスクの対応するビットが 8 ビットとも 0 と同じ)
  - 間に - を挟んだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。
  - * (すべての IP アドレスに対応)
- *dest_addr* ..... IP パケットの終点 IP アドレス (*src_addr* と同じ形式)。
  省略時は 1 個の * と同じ。
- *mask*..... IP アドレスのビットマスク、省略時は 0xffffffff と同じ。
  src_addr 及び *dest_addr* がネットワークアドレスの場合にのみ指定可。
  - xxx.xxx.xxx.xxx (xxx は 10 進数)
  - 0x に続く 16 進数
  - マスクビット数
- *protocol* ..... フィルタリングするパケットの種類
  - プロトコルを表す 10 進数 (0..255)
  - プロトコルを表すニーモニック

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

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

省略時は * と同じ。

◦ *src_port_list* ..... UDP、TCP のソースポート番号
- ポート番号を表す 10 進数
- ポート番号を表すニーモニック (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 *filter_out*
no ip filter directed-broadcast [*filter_out*]

[パラメータ]
◦ *filter_out*
- on ..... フィルタアウトする
- off ..... フィルタアウトしない

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

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

[デフォルト値]
on

5.1.9 動的フィルタの定義

[入力形式]
ip filter dynamic *dyn_filter_num srcaddr dstaddr protocol* [*option* ...]
ip filter dynamic *dyn_filter_num srcaddr dstaddr filter filter_list* [in *filter_list*] [out *filter_list*] [*option* ...]
no ip filter dynamic *dyn_filter_num* [*dyn_filter_num*...]

[パラメータ]
◦ *dyn_filter_num* ..... 動的フィルタ番号 (1...21474836)
◦ *srcaddr* ..... 始点 IP アドレス
◦ *dstaddr* ..... 終点 IP アドレス
◦ *protocol* ..... プロトコル
- tcp
- udp
- ftp
- tftp
- domain
- www
- smtp
- pop3
- telnet

◦ *filter_list* ..... ip filter コマンドで登録されたフィルタ番号のリスト
◦ *option*
- syslog=*switch*
  - on .....コネクションの通信履歴を SYSLOG に残す
  - off.....コネクションの通信履歴を SYSLOG に残さない
- timeout=*time*
  - *time*.....データが流れなくなったときにコネクション情報を解放するまでの時間 (秒)

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

[デフォルト値]
syslog=on
timeout=60

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

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*]
ip pp intrusion detection *direction switch* [*option*]
ip tunnel intrusion detection *direction switch* [*option*]
no ip *interface* intrusion detection
no ip pp intrusion detection
no ip tunnel intrusion detection

[パラメータ]
- *interface*.....LAN インタフェース名
- *direction*.....観察するパケットの方向
  - in.....インタフェース側から内側へ
  - out.....インタフェース側から外側へ
- *switch*.....動作
  - on.....実行する
  - off.....実行しない
- *option*.....オプション
  - reject=*rjt*
    - on.....不正なパケットを破棄する
    - off .....不正なパケットを破棄しない

[説明] 指定したインタフェースで、指定された向きのパケットについて侵入を検知する。

[ノート] 危険性の高い攻撃については、reject オプションの設定に関わらず常にパケットを破棄する。

[デフォルト値] *switch* = off
reject = off

5.1.12 フィルタリングによるセキュリティの設定

[入力形式]

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

[パラメータ]

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

[説明]

ip filter コマンドによるパケットのフィルタを組み合わせて、インタフェースで送受信するパケットの種類を制限する。
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かればそのフィルタにより通過 / 廃棄が決定する。それ以降のフィルタは調べられない。すべてのフィルタにマッチしないパケットは廃棄される。
フィルタセットの名前を指定する書式では、指定されたフィルタセットが適用される。フィルタを調べる順序などは方向を指定する書式の方法に準ずる。定義されていないフィルタセットの名前が指定された場合には、フィルタは設定されていないものとして動作する。

[ノート]

フィルタリストを走査して、一致すると通過、破棄が決定する。

```
# ip filter 1 pass 192.168.0.0/24 *
# ip filter 2 reject 192.168.0.1
# ip lan1 secure filter in 1 2
```

この設定では、始点 IP アドレスが 192.168.0.1 であるパケットは、最初のフィルタ 1 で通過が決定してしまうため、フィルタ 2 での検査は行われない。そのため、フィルタ 2 は何も意味を持たない。
フィルタリストを操作した結果、どのフィルタにも一致しないパケットは破棄される。

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

[デフォルト値]

フィルタは設定されていない

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)
  以下のニーモニックが利用できる

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

- *precedence*
  - PRECEDENCE 値 (0..7)
  - *precedence* を省略した場合、PRECEDENCE 値は変更しない
- *filter_num* , *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*
ip pp mtu *mtu*
no ip *interface* mtu [*mtu*]
no ip pp mtu [*mtu*]

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

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

[入力形式]
ip simple-service *service*
no ip simple-service [*service*]

[パラメータ]
- *service*
  - on ..... TCP/UDP の各種サービスを動作させる
  - off ..... サービスを停止させる

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

[デフォルト値] on

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*
ip pp remote address dhcpc [*interface*]
no ip pp remote address [*ip_address*]

[パラメータ]
◦ *ip_address*
- IP アドレス .....xxx.xxx.xxx.xxx（xxx は 10 進数）
- dhcp ..... 自分自身の DHCP サーバ機能より IP アドレスを割り当てる

◦ dhcpc.....DHCP クライアントを利用することを示すキーワード
◦ *interface* .....DHCP クライアントとして動作する LAN インタフェース名（省略時は lan1）

[説明]
選択されている相手の PP 側の IP アドレスを設定する。
dhcp を設定した場合は、自分自身が DHCP サーバとして動作している必要がある。自分で管理している DHCP スコープの中から、IP アドレスを割り当てる。
装着されている BRI/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。
dhcpcを設定した場合は、interfaceで指定したLANインタフェースがDHCPクライアントとしてIPアドレスを取得し、そのアドレスを PP 側に割り当てる。取得できなかった場合は、0.0.0.0 を割り当てる。

[ノート]
実際に設定される IP アドレスは ppp ipcp ipaddress コマンドと相手の設定により決まる。自分側で設定した IP アドレスを xxx.xxx.xxx.xxx 、相手先が要求してくる IP アドレスを yyy.yyy.yyy.yyy とすると実際に設定される IP アドレスは次のようになる。

[デフォルト値]
相手側 IP アドレスは設定されていない

[設定例]
例えば、ルータ A 側が "no ip pp remote address"、"ppp ipcp ipaddress on" と設定し、接続するルータ B 側が "ip pp address yyy.yyy.yyy.yyy" と設定している場合には、実際のルータ A のPP 側のIP アドレスは "yyy.yyy.yyy.yyy " になることを意味する。

5.3.2 リモート IP アドレスプールの設定

[入力形式]
ip pp remote address pool *ip_address* [*ip_address...*]
ip pp remote address pool *ip_address-ip_address*
ip pp remote address pool *dhcp*
ip pp remote address pool dhcpc [*interface*]
no ip pp remote address pool

[パラメータ]
◦ *ip_address* ..... anonymous のためにプールする IP アドレス
◦ *ip_address-ip_address* .....IP アドレスの範囲
◦ *dhcp*..... 自分自身の DHCP サーバ機能を利用する
◦ dhcpc.....DHCP クライアントを利用することを示すキーワード
◦ *interface* .....DHCP クライアントとして動作する LAN インタフェース名（省略時は lan1）

[説明]
anonymous で相手に割り当てるための IP アドレスプールを設定する。
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。
dhcpcを設定した場合は、interfaceで指定したLANインタフェースがDHCPクライアントとしてIPアドレスを取得し、そのアドレスを割り当てる。取得できなかった場合は、0.0.0.0 を割り当てる。
RT300i では装着されている BRI/PRI インタフェースで利用できる ISDN Bch の数まで設定および DHCP クライアントで取得できる。RT140p では 8 個まで、RT140f、RT140i、RT140e では 4 個まで、それ以外は 2 個までとなる。PP として anonymous が選択された場合のみ有効である。

5.4 RIP の設定

5.4.1 RIP を使用するか否かの設定

[入力形式] rip use *rip_use*
no rip use *rip_use*

[パラメータ]
- *rip_use*
  - 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 *rip_preference*
no rip preference *rip_preference*

[パラメータ]
- *rip_preference* ..... 1 以上の数値

[説明] RIP により得られた経路の優先度を設定する。経路の優先度は 1 以上の数値で表され、数字が大きい程優先度が高い。スタティックと RIP など複数のプロトコルで得られた経路が食い違う場合には、優先度が高い方が採用される。優先度が同じ場合には時間的に先に採用された経路が有効となる。

[ノート] スタティック経路の優先度は 10000 で固定である。

[デフォルト値] 1000

5.4.3 RIP パケットの送信に関する設定

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

[パラメータ]
- *interface* ..... LAN インタフェース名
- *rip_send*
  - on ..... RIP パケットを送信する
  - off ..... RIP パケットを送信しない
- *version* ..... 送信する RIP のバージョン (1,2)
- broadcast ..... ip interface address コマンドで指定した broadcast address

[説明] 指定したインタフェースに対し、RIP パケットを送信するか否かを設定する。
"version *version*" で送信する RIP のバージョンを指定できる。

[デフォルト値] on version 1

5.4.4 RIP パケットの受信に関する設定

[入力形式] ip *interface* rip receive *rip_receive* [version *version* [*version*]]
ip pp rip receive *rip_receive* [version *version* [*version*]]
no ip *interface* rip receive [*rip_receive*...]
no ip pp rip receive [*rip_receive*...]

[パラメータ]
- *interface* ..... LAN インタフェース
- *rip_receive*
  - on ..... RIP パケットを受信する
  - off ..... RIP パケットを受信しない
- *version* ..... 受信する RIP のバージョン (1,2)

[説明] 指定したインタフェースに対し、RIP パケットを受信するか否かを設定する。
"version *version*" で受信する RIP のバージョンを指定できる。指定しない場合は、RIP1/2 ともに受信する。

[デフォルト値] *rip_receive* = on
version = 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 *interface* rip trust gateway [except] *gateway_list*
ip pp rip trust gateway [except] *gateway_list*
no ip *interface* rip trust gateway [[except] *gateway_list*]
no ip pp rip trust gateway [[except] *gateway_list*]

[パラメータ]
- *interface* ..... LAN インタフェース名
- *gateway_list* ..... 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 *interface* rip filter *direction filter_list*
ip pp rip filter *direction filter_list*
no ip *interface* rip filter *direction filter_list*
no ip pp rip filter *direction filter_list*

[パラメータ]
- *interface* ..... LAN インタフェース名
- *direction*
  - in..... 受信した RIP のフィルタリング
  - out..... 送信する RIP のフィルタリング
- *filter_list* ..... 空白で区切られた静的フィルタ番号の並び (100 個以内)

[説明]
インタフェースで送受信する RIP のフィルタリングを設定する。
ip filter コマンドで設定されたフィルタの始点 IP アドレスが、送受信する RIP の経路情報にマッチする場合は、フィルタが pass であればそれを処理し、reject であればその経路情報だけを破棄する。

[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 *interface* rip hop *direction hop*
ip pp rip hop *direction hop*
no ip *interface* rip hop *direction hop*
no ip pp rip hop *direction hop*

[パラメータ]
- *interface* ..... LAN インタフェース名
- *direction*
  - in..... 受信した RIP に加算する
  - out..... 送信する RIP に加算する
- *hop*..... 加算する値 (0..15)

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

[デフォルト値]
0

5.4.8 RIP2 での認証の設定

[入力形式]
ip *interface* rip auth type *type*
ip pp rip auth type *type*
no ip *interface* rip auth type [*type*]
no ip pp rip auth type [*type*]

[パラメータ]
- *interface* .....LAN インタフェース名
- *type*
  - none .....認証しない
  - text..... テキスト型の認証を行う

[説明] RIP2 を使用する場合のインタフェースでの認証の設定をする。none の場合は認証なし。text の場合はテキスト型の認証を行う。

[デフォルト値] none

5.4.9 RIP2 での認証キーの設定

[入力形式]
ip *interface* rip auth key *hex_key*
ip pp rip auth key *hex_key*
ip *interface* rip auth text *text_key*
ip pp rip auth text *text_key*
no ip *interface* rip auth key
no ip pp rip auth key

[パラメータ]
- *interface* .....LAN インタフェース名
- *hex_key* .....16 進数の列で表現された認証キー
- *text_key* .....文字列で表現された認証キー

[説明] RIP2 を使用する場合のインタフェースの認証キーを設定する。

[設定例]
```
# ip lan1 rip auth key text testing123
# ip pp rip auth key text "hello world"
# ip lan2 rip auth key 01 02 ff 35 8e 49 a8 3a 5e 9d
```

5.4.10 回線切断時の経路保持の設定

[入力形式]
ip pp rip hold routing *rip_hold*
no ip pp rip hold routing [*rip_hold*]

[パラメータ]
- *rip_hold*
  - on.....回線が切断されても RIP による経路を保持し続ける
  - off.....回線が切断されたら RIP による経路を破棄する

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

[デフォルト値] off

5.4.11 回線接続時の PP 側の RIP の動作の設定

[入力形式]
ip pp rip connect send *rip_action*
no ip pp rip connect send [*rip_action*]

[パラメータ]
- *rip_action*
  - interval..... ip pp rip connect interval コマンドで設定された時間間隔で RIP を送出する
  - update .....経路情報が変わった場合にのみ RIP を送出する

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

[デフォルト値] update

[設定例]
```
# ip pp rip connect interval 60
# ip pp rip connect send interval
```

5.4.12 回線接続時の PP 側の RIP 送出の時間間隔の設定

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

[パラメータ] ◦ *time*..... 秒数 (30..21474836)

[説明] 選択されている相手について回線接続時に RIP を送出する時間間隔を設定する。
ip pp rip send と ip pp rip receive コマンドが on 、ip pp rip connect send コマンドが interval の時に有効である。

[デフォルト値] 30

[設定例] # ip pp rip connect interval 60
ip pp rip connect send interval

5.4.13 回線切断時の PP 側の RIP の動作の設定

[入力形式] ip pp rip disconnect send *rip_action*
no ip pp rip disconnect send [*rip_action*]

[パラメータ] ◦ *rip_action*
- none ..... 回線切断時に RIP を送出しない
- interval ..... ip pp rip disconnect interval コマンドで設定された時間間隔で RIP を送出する
- update ..... 経路情報が変わった時にのみ RIP を送出する

[説明] 選択されている相手について回線切断時に RIP を送出する条件を設定する。

[デフォルト値] none

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

5.4.14 回線切断時の PP 側の RIP 送出の時間間隔の設定

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

[パラメータ] ◦ *time*..... 秒数 (30..21474836)

[説明] 選択されている相手について回線切断時に RIP を送出する時間間隔を設定する。
ip pp rip send と ip pp rip receive コマンドが on 、ip pp rip disconnect send コマンドで interval 設定に有効である。

[デフォルト値] 3600

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

5.5 VRRP の設定

5.5.1 インタフェース毎の VRRP の設定

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

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

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

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

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

5.5.2 シャットダウントリガの設定

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

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

[説明]
設定した VRRP グループでマスタールータとして動作している場合に、指定した条件によってシャットダウンすることを設定する。
- LAN インタフェース形式. ..... 指定した LAN インタフェースのリンクが落ちるとシャットダウンする。
- pp 形式 ..... 指定した PP 番号に該当する回線で通信できなくなった場合にシャットダ ウンする。通信できなくなるとは、ケーブルが抜けるなどレイヤ 1 が落ちた場合と、以下の場合である。
  - 回線が ISDN 回線である時は、呼が接続されていない場合
  - 回線が専用線である時には、LCP キープアライブによって通信相手が落ちたと判断した場合
  - 回線がフレームリレーであって "dlci=*dlci*" 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
- 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。

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
  - 0:0:0:0:0:1 .....FF:FF:FF:FF:FF:FE(2 桁以内の 16 進数以外に '*' も指定可)
  - * (すべての IPX ノード番号)
  - 省略時は一個の * と同じ
- *dst_net*.....終点 IPX ネットワーク番号 src_net と同じ形式。
- *dst_node*.....終点 IPX ノード番号 src_node と同じ形式。
- *type*.....IPX パケットタイプ
  - 10 進数 (0..255)
  - 16 進数 (0x0..0xFF)
  - ニーモニック文字列

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

  - 間に - をはさんだ 2 つの上項目、- を前につけた上項目、- を後ろにつけた上項目、これらは範囲を指定する。
  - 上項目のカンマで区切った並び (5 個以内)
  - * (すべての IPX パケットタイプ)
  - 省略時は一個の * と同じ
- *src_socket*.....始点ソケット番号
  - 10 進数 (0..65535)
  - 0x を先頭に持つ 4 桁以内の 16 進数
  - プロトコルを表すニーモニック

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

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

[説明]

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

[ノート]

IPX パケットタイプでは、"-xxx" は "0-xxx" の意味に、また "yyy-" は "yyy-255" の意味に取る。
ソケット番号では、"yyy-" は "yyy-65535" の意味に取る。
restrict-log および restrict-nolog を使ったフィルタは、回線が接続されている場合だけ通せば十分で、そのために回線に発信するまでもないようなパケットに対して有効である。

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 のニーモニック
  - printer ..... 0x0007 のニーモニック
- *server_name* ..... サーバ名
  - 'A' ～ 'Z','0' ～ '9','','-','@' で構成された 47 文字以内の文字列
- *network* ..... サーバの IPX ネットワーク番号 (0:0:0:1 .. FF:FF:FF:FE)
- *node_num* ..... サーバの IPX ノード番号 (0:0:0:0:0:1 .. FF:FF:FF:FF: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
  - プロトコルを表すニーモニック

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。

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

[デフォルト値] 0

6.2.2 LAN 側の IPX ネットワーク番号の設定

[入力形式]
ipx *interface* network *network*
no ipx *interface* network [*network*]

[パラメータ]
- *interface* .....LAN インタフェース名
- *network* .....IPX ネットワーク番号 (0:0:0:1 ..FF:FF:FF:FE)

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

[デフォルト値] IPX ネットワーク番号は設定されていない

6.2.3 経路情報の追加

[入力形式]
ipx *interface* route *network gateway hop* [*ticks*]
no ipx *interface* route *network* [*gateway hop* [*ticks*]]

[パラメータ]
- *interface* .....LAN インタフェース名
- *network* .....終点 IPX ネットワーク番号 (0:0:0:1 .. FF:FF:FF:FE)
- *gateway* .....ゲートウェイの IPX ノード番号 (0:0:0:0:0:1 .. FF:FF:FF:FF:FF:FE)
- *hop* .....ホップカウント (1..14)
- *ticks* .....ティック (1..65535)

[説明] IPX の経路情報テーブルに LAN 側の経路情報を追加する。

[ノート] ティックを省略した場合はホップカウントと同じになる。

6.2.4 LAN 側の RIP/SAP ブロードキャストの設定

[入力形式]
ipx *interface* ripsap broadcast *broadcast*
no ipx *interface* ripsap broadcast [*broadcast*]

[パラメータ]
- *interface* .....LAN インタフェース名
- *broadcast*
  - 秒数 (60..21474836)
  - off.....RIP/SAP をブロードキャストしない

[説明] LAN に対して RIP/SAP をブロードキャストする間隔を設定する。
off を設定すると、ブロードキャストしなくなる。

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

[デフォルト値] 60

6.2.5 LAN 側でのフィルタリングによるセキュリティの設定

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

[パラメータ]
- *interface* .....LAN インタフェース名
- *direction*
  - in .....LAN 側から入ってくる方向でフィルタを適用
  - out.....LAN 側へ出ていく方向でフィルタを適用
- *filter_list* .....100 個以内の空白で区切られたフィルタ番号の並び

[説明] LAN 側に対して適用する IPX フィルタを設定する。

[ノート] フィルタリストを走査して、一致すると通過、破棄が決定する。

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

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

6.3 PP 側相手毎の IPX の設定

6.3.1 IPX ルーティング許可の設定

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

[パラメータ] ◦ *routing*
- on ..... PP 側に IPX パケットをルーティングする
- off ..... PP 側に IPX パケットをルーティングしない

[説明] 選択されている相手について IPX パケットを PP 側にルーティングするかどうかを設定する。

[デフォルト値] off

6.3.2 PP 側 IPX ネットワーク番号の設定

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

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

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

[ノート] IPX ノード番号は通常デフォルトのままとする。

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

6.3.3 経路情報の追加

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

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

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

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

6.3.4 回線接続時の PP 側の RIP/SAP の動作の設定

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

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

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

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

[デフォルト値] update

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

6.3.5 回線接続時の PP 側の RIP/SAP 送出の時間間隔の設定

[入力形式] ipx pp ripsap connect interval *time*
no ipx pp ripsap connect interval [*time*]

[パラメータ] ○ *time* ..... 秒数 (60..21474836)

[説明] 選択されている相手について回線接続時に PP 側に RIP/SAP を送出する時間間隔を設定する。

[デフォルト値] 60

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

6.3.6 回線切断時の PP 側の RIP/SAP の動作の設定

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

[パラメータ] ○ *send*
- none ..... 回線切断時に RIP/SAP を送出しない
- interval ..... ipx pp ripsap disconnect interval コマンドで設定された時間間隔で RIP/SAP を送出する
- update ..... RIP/SAP テーブルに変更があった時だけ送出する

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

[デフォルト値] none

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

6.3.7 回線切断時の PP 側の RIP/SAP 送出の時間間隔の設定

[入力形式] ipx pp ripsap disconnect interval *interval*
no ipx pp ripsap disconnect interval [*interval*]

[パラメータ] ○ *interval* ..... 秒数 (60..21474836)

[説明] 選択されている相手について回線切断時に RIP/SAP を送出する時間間隔を設定する。

[デフォルト値] 60

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

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

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

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

[デフォルト値] *t1* = 7200
t2 = 60
t3 = 10

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

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

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

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

[デフォルト値] on

6.3.17 PP 側でのフィルタリングによるセキュリティの設定

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

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

[説明] PP 側に対し適用するフィルタを設定する。

[ノート] フィルタリストを走査して、一致すると通過、破棄が決定する。

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

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

7. ブリッジの設定

7.1 インタフェース共通の設定

7.1.1 ブリッジ使用許可の設定

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

[パラメータ] ◦ *use*
- on ..... ブリッジする
- off ..... ブリッジしない
- multicast ..... マルチキャストのみブリッジする

[説明] ブリッジを行うかどうかを設定する。

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

[デフォルト値] off

7.1.2 ブリッジするインタフェースの設定

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

[パラメータ] ◦ *interface_list*
- 相手先情報番号
- anonymous
- LAN インタフェース名

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

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

[デフォルト値] インタフェースは設定されていない

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

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

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]
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は消去されなくなる。

[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て、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て、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 *username password* [myname *myname mypass*] [*isdn1*] [clid [*isdn2*]] [mscbcp] [*ip_address*]
no pp auth username *username* [*password...*]

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

[説明] 相手の名前とパスワードを設定する。複数の設定が可能。
オプションで自分側の設定も入力ができる。
双方向で認証を行う場合には、相手のユーザ名が確定してから自分を相手に認証させるプロセスが動き始める。
これらのパラメータが設定されていない場合には、pp auth myname コマンドの設定が参照される。
オプションで ISDN 番号が設定でき、名前と結びついたルーティングやリモート IP アドレスに対しての発信を可能にする。isdn1 は発信用の ISDN アドレスである。*isdn1* を省略すると、この相手には発信しなくなる。
名前に '*' を与えた場合にはワイルドカードとして扱い、他の名前とマッチしなかった相手に対してその設定を使用する。
clid キーワードは発番号認証を利用することを指示する。このキーワードがない場合は発番号認証は行われない。発番号認証は *isdn2* があれば *isdn2* を用い、または *isdn2* がなければ *isdn1* を用い、一致したら認証は成功したとみなす。
mscbcp キーワードは MS コールバックを許可することを指示する。このユーザからの着信に対しては、同時に isdn callback permit on としてあれば MS コールバックの動作を行う。

8.2 要求する認証タイプの設定

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

[パラメータ]
- *auth*
  - none .....何も要求しない
  - pap .....PAP による認証を要求する
  - chap .....CHAP による認証を要求する
  - chap-pap .....CHAP もしくは PAP による認証を要求する
- arrive-only .....着信時にのみ PPP による認証を要求する

[説明] PAP と CHAP による認証を要求するかどうかを設定する。発信時には常に適用される。anonymous でない着信の場合には発番号により PP が選択されてから適用される。anonymous での着信時には、発番号による PP の選択が失敗した場合に適用される。
chap-pap キーワードの場合には、最初 CHAP を要求し、それが相手から拒否された場合には改めて PAP を要求するよう動作する。これにより、相手が PAP または CHAP の片方しかサポートしていない場合でも容易に接続できるようになる。
arrive-only キーワードが指定された場合には、着信時にのみ PPP による認証を要求するようになり、発信時には要求しない。
PP 毎のコマンドである。

[デフォルト値] none

8.3　受け入れる認証タイプの設定

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

[パラメータ]　◦ *accept*
- pap ..... PAP による認証を受け入れる
- chap ..... CHAP による認証を受け入れる
- 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 *myname password*
no pp auth myname [*myname password*]

[パラメータ]　◦ *myname* ..... 名前 (64 文字以内)
◦ *password* ..... パスワード (64 文字以内)

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

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

[入力形式]　pp auth multi connect prohibit *prohibit*
no pp auth multi connect prohibit [*prohibit*]

[パラメータ]　◦ *prohibit*
- on ..... 禁止する
- off ..... 禁止しない

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

[ノート]　定額制プロバイダを営む場合に便利である。ユーザ管理を RADIUS で行う場合には、二重接続の禁止は RADIUS サーバの方で対処する必要がある。
anonymous が選択された場合のみ有効である。

[デフォルト値]　off

8.6　LCP 関連の設定

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

[入力形式]　ppp lcp acfc *acfc*
no ppp lcp acfc [*acfc*]

[パラメータ]　◦ *acfc*
- on ..... 用いる
- off ..... 用いない

[説明]　選択されている相手について [PPP, LCP] の Address and Control Field Com pression 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 *magicnumber*
no ppp lcp magicnumber [*magicnumber*]

[パラメータ] ○ *magicnumber*
- on ..... 用いる
- off ..... 用いない

[説明] 選択されている相手について [PPP,LCP] の Magic Number オプションを用いるか否かを設定する。

[ノート] on を設定していても相手に拒否された場合は用いない。

[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 *mru* [*length*]
no ppp lcp mru [*mru* [*length*]]

[パラメータ] ○ *mru*
- on ..... 用いる
- off ..... 用いない

○ *length* ..... MRU の値 (1280..1792)

[説明] 選択されている相手について [PPP,LCP] の Maximum Receive Unit オプションを用いるか否かと、MRU の値を設定する。

[ノート] on を設定していても相手に拒否された場合は用いない。一般には on でよいが、このオプションをつけると接続できないルータに接続する場合には off にする。
データ圧縮を利用する設定の場合には、*length* パラメータの設定は常に 1792 として動作する。

[デフォルト値] *mru* = on
length = 1792

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

[入力形式] ppp lcp pfc *pfc*
no ppp lcp pfc [*pfc*]

[パラメータ] ○ *pfc*
- on ..... 用いる
- off ..... 用いない

[説明] 選択されている相手について [PPP,LCP] の Protocol Field Compression オプションを用いるか否かを設定する。

[ノート] on を設定していても相手に拒否された場合は用いない。また、このオプションを相手から要求された場合には、このコマンドの設定に関わらず常にアクセプトする。

[デフォルト値] off

8.6.5 lcp-restart パラメータの設定

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

[パラメータ] ○ *time* ..... ミリ秒 (20..10000)

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

[デフォルト値] 3000

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 PP 経由のキープアライブを使用するか否かの設定

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

[パラメータ] ○ *use*
- lcp-echo ..... LCP Echo Request/Reply を用いる
- off ..... キープアライブを使用しない

[説明] PP 経由のキープアライブを使用するか否かを設定する。

[ノート] PP 毎のコマンドである。

[デフォルト値] off

8.6.11 PP 経由のキープアライブのログをとるか否かの設定

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

[パラメータ] ◦ *log*
- on ..... ログをとる
- off ..... ログをとらない

[説明] PP 経由のキープアライブ (LCP ECHO) をログにとるか否かを設定する。

[ノート] この設定は、すべての PP で共通に用いられる。

[デフォルト値] on

8.6.12 PP 経由のキープアライブの時間間隔の設定

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

[パラメータ] ◦ *interval* ..... キープアライブパケットを送出する時間間隔 [秒](1..65535)
◦ *count* ..... この回数連続して応答がなければ相手側のルータをダウンしたと判定する (3..100)

[説明] 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] 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] *interval* = 30
count = 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 *action*
no leased keepalive down [*action*]

[パラメータ] ◦ *action*
- silent ..... 何もしない
- reset ..... ルータを再起動する

[説明] キープアライブによって専用線ダウンを検出した場合のルータの動作を設定する。

[デフォルト値] silent

8.7 PAP 関連の設定

8.7.1 pap-restart パラメータの設定

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

[パラメータ] ◦ *time* ..... ミリ秒 (20..10000)

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

[デフォルト値] 3000

8.7.2 pap-max-authreq パラメータの設定

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

[パラメータ] ◦ *count* ..... 回数 (1..10)

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

[デフォルト値] 10

8.8 CHAP 関連の設定

8.8.1 chap-restart パラメータの設定

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

[パラメータ] ◦ *time*..... ミリ秒 (20..10000)

[説明] 選択されている相手について [PPP,CHAP] challenge の再送時間を設定する。

[デフォルト値] 3000

8.8.2 chap-max-challenge パラメータの設定

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

[パラメータ] ◦ *count* ..... 回数 (1..10)

[説明] 選択されている相手について [PPP,CHAP] challenge の送信回数を設定する。

[デフォルト値] 10

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 *compression*
no ppp ipcp vjc [*compression*]

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

[説明] 選択されている相手について [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 *negotiation*
no ppp ipcp ipaddress [*negotiation*]

[パラメータ] ◦ *negotiation*
- on ..... ネゴシエーションする
- off..... ネゴシエーションしない

[説明] 選択されている相手について PP 側 IP アドレスのネゴシエーションをするか否かを設定する。

[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 *time*
no ppp ipcp 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,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 msext *msext*
no ppp ipcp msext [*msext*]

[パラメータ] ◦ *msext*
- 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 *time*
no ppp ipxcp 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、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 *count*
no ppp ipxcp 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、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 *count*
no ppp ipxcp 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、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 *count*
no ppp ipxcp 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、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 *lan_id*
no ppp bcp lanid [*lan_id*]

[パラメータ] ◦ *lan_id*
- 十六進数 (0x1 .. 0xfffffffe)
- 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 *compression*
no ppp bcp tinycomp [*compression*]

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

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

[デフォルト値] on

8.11.3 bcp-restart パラメータの設定

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

[パラメータ] ◦ *time*..... ミリ秒 (20..10000)

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

[デフォルト値] 3000

8.11.4 bcp-max-terminate パラメータの設定

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

[パラメータ] ◦ *count*..... 回数 (1..10)

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

[デフォルト値] 2

8.11.5 bcp-max-configure パラメータの設定

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

[パラメータ] ◦ *count*..... 回数 (1..10)

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

[デフォルト値] 10

8.11.6 bcp-max-failure パラメータの設定

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

[パラメータ] ◦ *count*..... 回数 (1..10)

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

[デフォルト値] 10

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 *time*
no ppp mscbcp restart [*time*]

[パラメータ] ◦ *time*.....ミリ秒 (20..10000)

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

[デフォルト値] 1000

8.12.2 mscbcp-maxretry パラメータの設定

[入力形式] ppp mscbcp maxretry *count*
no ppp mscbcp 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*
- stac0 ..... Stac LZS で圧縮する
- stac ..... Stac LZS で圧縮する
- cstac ..... Stac LZS で圧縮する（接続相手が Cisco ルータの場合）
- none ..... 圧縮しない

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

[ノート] Van Jacobson Compressed TCP/IP との併用も可能である。
パケットの取りこぼしで頻繁に CCP リセットが発生する環境では、設定を stac0 にして、パケット毎に圧縮するようにすれば良い。ただし接続先も stac0 に対応していなければならない。stac0 は stac よりも圧縮効率は落ちる。また、接続相手が Cisco ルータの場合に stac を適用するとデータ転送中に頻繁に CCP のリセットが発生して、データ転送速度が遅くなることがある。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 IPV6CP 関連の設定

8.14.1 IPV6CP を使用するか否かの設定

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

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

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

[デフォルト値] on

8.15 MP 関連の設定

8.15.1 MP を使用するか否かの設定

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

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

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

[デフォルト値] off

8.15.2 MP の制御方法の設定

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

[パラメータ] ○ *type*
- arrive ..... 自分が 1B 目の着信側の場合に MP を制御する
- both ..... 自分が 1B 目の発信着信いずれの場合でも MP を制御する
- call ..... 自分が 1B 目の発信側の場合に MP を制御する

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

[デフォルト値] call

8.15.3 MP のための負荷閾値の設定

[入力形式]
ppp mp load threshold *call_load call_count disc_load disc_count*
no ppp mp load threshold [*call_load call_count disc_load disc_count*]

[パラメータ]
- *call_load* ..... 発信負荷閾値 %(1..100)
- *call_count* ..... 回数 (1..100)
- *disc_load* ..... 切断負荷閾値 %(0..50)
- *disc_count* ..... 回数 (1..100)

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

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

8.15.4 MP の最大リンク数の設定

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

[パラメータ]
- *number* ..... リンク数

[説明]
選択されている相手について [PPP, MP] の最大リンク数を設定する。リンク数の最大値は、使用モデルで使用できる ISDN Bch の数までとなる。

[デフォルト値]
2

8.15.5 MP の最小リンク数の設定

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

[パラメータ]
- *number* ..... リンク数

[説明]
選択されている相手について [PPP,MP] の最小リンク数を設定する。

[デフォルト値]
1

8.15.6 MP のための負荷計測間隔の設定

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

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

[説明]
選択されている相手について [PPP, MP] のための負荷計測間隔を設定する。
単位は秒。負荷計測だけでなく、すべての MP の動作はこのコマンドで設定した間隔で行われる。

[デフォルト値]
10

8.15.7 MP のパケットを分割するか否かの設定

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

[パラメータ] ◦ *divide*
- on.....分割する
- off.....分割しない

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

[デフォルト値] on

8.16 BACP 関連の設定

8.16.1 bacp-restart パラメータ の設定

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

[パラメータ] ◦ *time*.....ミリ秒 (20..10000)

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

[デフォルト値] 3000

8.16.2 bacp-max-terminate パラメータ の設定

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

[パラメータ] ◦ *count*.....回数 (1..10)

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

[デフォルト値] 2

8.16.3 bacp-max-configure パラメータ の設定

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

[パラメータ] ◦ *count*.....回数 (1..10)

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

[デフォルト値] 10

8.16.4 bacp-max-failure パラメータ の設定

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

[パラメータ] ◦ *count*.....回数 (1..10)

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

[デフォルト値] 10

8.16.5 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

8.16.6 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

8.17 PPPoE 関連の設定

8.17.1 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

8.17.2 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。

8.17.3 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

8.17.4 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

8.17.5 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

8.17.6 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

8.17.7 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

8.17.8 PADR パケットの再送時間の設定

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

[パラメータ]
- *time* ..... ミリ秒 (20..10000)

[説明] PPPoE プロトコルにおける PADR パケットの再送時間を設定する。

[デフォルト値] 3000

8.17.9 PPPoE セッションの切断タイマの設定

[入力形式] pppoe disconnect time *time*
no pppoe disconnect time

[パラメータ]
- *time*
  - 秒数 (1..21474836)
  - off ..... タイマを設定しない

[説明] 選択されている相手に対して、タイムアウトにより PPPoE セッションを自動切断する時間を設定する。

[ノート] LCP と NCP パケットは監視対象外。

[デフォルト値] off

8.17.10　TCP パケットの MSS の制限の有無とサイズの指定

[入力形式]　pppoe tcp mss limit *length*
pppoe tcp mss limit

[パラメータ]　○ *length*
- データ長（1240..1452）
- auto ..... MSS を MTU の値に応じて制限する
- off ..... MSS を制限しない

[説明]　PPPoE セッション上で TCP パケットの MSS(Maximum Segment Size) を制限するかどうかを設定する。

[デフォルト値]　auto

9. DHCP の設定

本機は DHCP[1] 機能として、DHCP サーバ機能、DHCP リレーエージェント機能、DHCP クライアント機能を実装しています。DHCP 機能の利用により、基本的なネットワーク環境の自動設定を実現します。

DHCP クライアント機能は Windows 95, 98 や Windows NT 等で実装されており、これらと本機の DHCP サーバ機能、DHCP リレーエージェント機能を組み合わせることにより DHCP クライアントの基本的なネットワーク環境の自動設定を実現します。

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

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

9.1 DHCP サーバ・リレーエージェント機能

9.1.1 DHCP の動作の設定

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

[パラメータ] ○ *type*
- server .....DHCP サーバとして機能させる
- relay.....DHCP リレーエージェントとして機能させる

[説明] DHCP に関する機能を設定する。
DHCP リレーエージェント機能使用時には、NAT 機能を使用することはできない。

[デフォルト値] DHCP サービスは機能しない

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

9.1.2 RFC2131 対応動作の設定

[入力形式]

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

- *comp*
  - on ..... RFC2131 準拠
  - off ..... RFC1541 準拠
- *except*..... 指定した機能以外が RFC2131 対応となるキーワード
- *function*
  - broadcast-nak ..... DHCPNAK をブロードキャストで送る
  - none-domain-null ... ドメイン名の最後に NULL 文字を付加しない
  - remain-silent..... リース情報を持たないクライアントからの DHCPREQUEST を無視する
  - reply-ack..... DHCPNAK の代わりに許容値を格納した DHCPACK を返す
  - use-clientid..... クライアントの識別に Clinet-Identifer オプションを優先する

[説明]

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

- broadcast-nak ..... 同じサブネット上のクライアントに対しては DHCPNAK はブロードキャストで送る。DHCPREQUEST をクライアントが INIT-REBOOT state で送られてきたものに対しては、giaddr 宛てであれば Bbit を立てる。
- none-domain-null ... 本ドメイン名の最後に NULL 文字を付加しない。RFC1541 ではドメイン名の最後に NULL 文字を付加するかどうかは明確ではなかったが、RFC2131 では禁止された。一方、Windows NT/2000 の DHCP サーバは NULL 文字を付加している。そのため、Windows 系の OS での DHCP クライアントは NULL 文字があることを期待している節があり、NULL 文字がない場合には winipcfg.exe での表示が乱れるなどの問題が起きる可能性がある。
- remain-silent..... クライアントから DHCPREQUEST を受信した場合に、そのクライアントのリース情報を持っていない場合には DHCPNAK を送らないようにする。
- reply-ack..... クライアントから、リース期間などで許容できないオプション値 (リクエスト IP アドレスは除く) を要求された場合でも、DHCPNAK を返さずに許容値を格納した DHCPACK を返す。
- use-clientid..... クライアントの識別に chaddr フィールドより Client-Identifier オプションを優先して使用する。

[デフォルト値] on

9.1.3 DHCP スコープの定義

[入力形式] dhcp scope *scope_num ip_address-ip_address*/*netmask* [except *ex_ip* ...] [gateway *gw_ip*] [expire *time*] [maxexpire *time*]
no dhcp scope *scope_num* [*ip_address-ip_address*/*netmask* [except *ex_ip* ...] [gateway *gw_ip*] [expire *time*] [maxexpire *time*]]

[パラメータ]

- *scope_num* ..... スコープ番号 (1..65535)
- *ip_address-ip_address* ... 対象となるサブネットで割り当てる IP アドレスの範囲
- *netmask*
  - xxx.xxx.xxx.xxx (xxx は 10 進数)
  - 0x に続く 16 進数
  - マスクビット数
- *ex_ip* ..... IP アドレス指定範囲の中で除外する IP アドレス (空白で区切って複数指定可能)
- *gw_ip* ..... IP アドレス対象ネットワークのゲートウェイの IP アドレス
- *time* ..... 時間
  - 分 (1..21474836)
  - 時間 : 分
  - infinity ..... 無期限リース

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

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

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

9.1.4 DHCP 予約アドレスの設定

[入力形式]

dhcp scope bind *scope_num ip_address* [*type*] *id*
dhcp scope bind *scope_num ip_address mac_address*
dhcp scope bind *scope_num ip_address* ipcp
no dhcp scope bind *scope_num ip_address*

[パラメータ]

- *scope_num* ..... スコープ番号 (1..65535)
- *ip_address* ..... 予約する IP アドレス
- *type* ..... Client-Identifier オプションの type フィールドを決定する
  - text 0x00
  - ethernet 0x01
- *id*
  - *type* が ethernet の場合 .....MAC アドレス
  - *type* が text の場合 .....文字列
  - *type* が省略された場合 .....2 桁 16 進数の列で先頭は type フィールド
  - *mac_address* .....xx:xx:xx:xx:xx:xx (xx は 16 進数) 予約 DHCP クライアントの MAC アドレス
- *ipcp* ..... IPCP でリモート側に与えることを示す

[説明]

IP アドレスをリースする DHCP クライアントを固定的に設定する。

[ノート]

IP アドレスは、*scope_num* パラメータで指定された DHCP スコープ範囲内でなければならない。1 つの DHCP スコープ内では、1 つの MAC アドレスに複数の IP アドレスを設定することはできない。他の DHCP クライアントにリース中の IP アドレスを予約設定した場合、リース終了後にその IP アドレスの割り当てが行われる。dhcp scope コマンド、あるいは dhcp delete scope コマンドを実行した場合、関連する予約はすべて消去される。ipcp の指定は、同時に接続できる B チャ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-cliantid 機能を使用しない設定になっているか、もしくは DHCP クライアントが DHCP パケット中に Client-Identifier オプションを付けてこない場合でないと動作しない。

クライアントが Client-Identifier オプションを使う場合、コマンドの第 2 の書式での予約は、dhcp server compliant on あるいは use-cliantid 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-Identifer 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 complient 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-cliantid 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 complient off あるいは use-clientid 機能なしの場合

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

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

なお、クライアントとの相互動作に関して下記の留意点がある。

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

9.1.5 DHCP オプションの設定

[入力形式]

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

[パラメータ]

◦ *scope_num* ..... スコープ番号 (1..65535)

◦ *option* ..... オプション番号 (1..49,64..76,128..254) またはニーモニック

- 主なニーモニック

router	3
dns	6
hostname	12
domain	15
wins_server	44

◦ *value* ..... オプション値

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

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

[説明]

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

[ノート]

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

9.1.6 リースする IP アドレスの重複をチェックするか否かの設定

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

[パラメータ]
- *check1*..... LAN 内を対象とするチェックの確認用待ち時間
  - ミリ秒（1..1000）
  - off..... LAN 内を対象とするチェックを行わない
- *check2*..... LAN 外 (DHCP リレーエージェント経由) を対象とするチェックの確認用待ち時間
  - ミリ秒（1..3000）
  - off..... LAN 外 (DHCP リレーエージェント経由) を対象とするチェックを行わない

[説明]
DHCP サーバとして機能する場合、IP アドレスを DHCP クライアントにリースする直前に、その IP アドレスを使っているホストが他にいないことをチェックするか否かを設定する。

[ノート]
LAN 内のスコープに対しては ARP を、DHCP リレーエージェント経由のスコープに対しては PING を使ってチェックする。

[デフォルト値]
check1 = 100
check2 = 500

9.1.7 DHCP サーバの指定の設定

[入力形式]
dhcp relay server *host* [*host...*]
no dhcp relay server [*host* [*host...*]]

[パラメータ]
- *host1..host4* ..... 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 パケットを複写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。

9.1.8 DHCP サーバの選択方法の設定

[入力形式]
dhcp relay select *type*
no dhcp relay select [*type*]

[パラメータ]
- *type*
  - 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写中継される。

[デフォルト値]
hash

9.1.9 DHCP BOOTREQUEST パケットの中継基準の設定

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

[パラメータ]
- *time*..... 秒数 (0..65535)

[説明]
DHCP BOOTREQUEST パケットの secs フィールドとこのコマンドによる秒数を比較し、設定値より小さな secs フィールドを持つ DHCP BOOTREQUEST パケットはサーバに中継しないようにする。
これにより、同一 LAN 上に別の DHCP サーバがあるにも関わらず遠隔地の DHCP サーバにパケットを中継してしまうのを避けることができる。

[デフォルト値]
0

9.2 DHCP クライアント機能

9.2.1 要求する IP アドレスリース期間の設定

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

[パラメータ]
- *interface*.....LAN インタフェース名
- *time*
  - 分数 (1..21474836)
  - 時間 : 分

[説明] DHCP クライアントが要求する IP アドレスのリース期間を設定する。

[ノート] リース期間の要求が受け入れられなかった場合、要求しなかった場合は、DHCP サーバからのリース期間を利用する。

[デフォルト値] リース期間を要求しない

9.2.2 IP アドレス取得要求の再送回数と間隔の設定

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

[パラメータ]
- *interface*.....LAN インタフェース名
- *retry*
  - 回数 (1..100)
  - infinity.....無制限
- *interval* .....秒数 (1..100)

[説明] IP アドレスの取得に失敗したときにリトライする回数とその間隔を設定する。

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

9.2.3 DHCP クライアント ID オプションの設定

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

[デフォルト値]
- *interface*.....LAN インタフェース名
- type.....ID オプションの type フィールドの値を設定することを示すキーワード
- *type*.....ID オプションの type フィールドの値
- *id*
  - ASCII 文字列で表した ID
  - 2 桁の 16 進数列で表した ID
- *peer_num*..... 相手先情報番号
  - anonymous..... 匿名
  - leased..... 専用線
- *pool_num*.....ip pp remote address pool dhcpc コマンドで取得する IP アドレスの番号。例えば、ip pp remote address pool dhcpc コマンドで IP アドレスを 2 個取得できる機種で、*pool_num* に "1" または "2" を設定することで、それぞれのクライアント ID オプションに任意の ID を付けることができる。(1..ip pp remote address pool dhcpc コマンドで取得できる IP アドレスの最大数)

[説明] DHCP クライアント ID オプションの type フィールドと ID を設定する。

[デフォルト値] *type* = 1

9.2.4 DHCP クライアントのホスト名の設定

[入力形式]
dhcp client hostname *interface* primary *host*
dhcp client hostname *interface* secondary *host*
dhcp client hostname pp *peer_num host*
dhcp client hostname pool *pool_num host*
no dhcp client hostname *interface* primary [*host*]
no dhcp client hostname *interface* secondary [*host*]
no dhcp client hostname pp *peer_num* [*host*]
no dhcp client hostname pool *pool_num* [*host*]

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

[説明]
DHCP クライアントのホスト名を設定する。

[デフォルト値]
DHCP クライアントのホスト名は設定されていない

9.2.5 DNS サーバアドレスを取得する LAN インタフェースの設定

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

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

[説明]
DNS サーバアドレスを取得する LAN インタフェースを設定する。このコマンドで LAN インタフェース名が設定されていると、DNS で名前解決を行うときに、指定した LAN インタフェースで DHCP サーバから取得した DNS サーバアドレスに対して問い合わせを行う。DHCP サーバから DNS サーバアドレスを取得できなかった場合は名前解決を行わない。
dns server コマンドで DNS サーバが明示的に指定されているか、dns server select、dns server pp コマンドの設定により問い合わせをする DNS サーバが決められた場合には、その設定が優先される。

[ノート]
この機能は指定した LAN インターフェースが DHCP クライアントとして動作していなければならない。

[デフォルト値]
LAN インタフェースは設定されていない

9.2.6 DHCP クライアントの状態の表示

[入力形式]
show status dhcpc

[パラメータ]
なし

[説明]
DHCP クライアントの状態を表示する。
- クライアントの状態
  - インタフェース
  - IP アドレス (取得できないときはその状態)
  - DHCP サーバ
  - リース残時間
  - クライアント ID
  - ホスト名 (設定時)
- 共通情報
  - DNS サーバ
  - ゲートウェイ

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]　off

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

10.10 ステルス機能の設定

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

[パラメータ]
- all ..... すべてのインタフェースからのパケットに対してステルス動作を行う
- *interface* ..... 指定したインタフェースからのパケットに対してステルス動作を行う

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

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

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

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

[デフォルト値] ステルス動作を行わない

10.11 受信した ICMP のログを記録するか否かの設定

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

[パラメータ]
- *log*
  - on ..... 記録する
  - off ..... 記録しない

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

[デフォルト値] on

10.12 ICMP を送信するか否かの設定

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

[パラメータ]
- *type*
  - echo-reply ..... ICMP Echo Reply
  - parameter-problem ..... ICMP Parameter Problem
  - time-exceeded ..... ICMP Time Exceeded
  - unreachable ..... ICMP Destination Unreachable
  - packet-too-big ..... ICMP Packet Too Big
- *send*
  - on ..... 送信する
  - off ..... 送信しない

[説明] 受信した IPv6 パケットに対して ICMP を送信するか否かを設定する。

[デフォルト値] parameter-problem = off
その他 = on

11. フレームリレー関連の設定

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

PPP によるダイヤルアップ接続と専用線接続、フレームリレー接続では同じ HDLC[1] 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[2] 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[3] 状態確認手順の LMI[4] 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[5] です。InARP を使用するか否かは 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、最も若い PP インタフェースが代表となります。

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

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

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

11.1 カプセル化の種類の設定

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

[パラメータ]　○ *type*
- ppp ..... PPP でカプセル化する
- fr ..... フレームリレーでカプセル化する

[説明]　選択されている相手のカプセル化の種類を設定する。

[ノート]　フレームリレーでは IPXWAN の設定は無効（常に OFF)

[デフォルト値]　ppp

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

11.2 DLCI の設定

[入力形式] fr dlci *dlci_num*
no fr dlci [*dlci_num*]

[パラメータ] ◦ *dlci_num*
- 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 dlci 16 17 18

11.3 PVC 状態確認手順の設定

[入力形式] fr lmi *lmi*
no fr lmi [*lmi*]

[パラメータ] ◦ *lmi*
- 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 *inarp*
no fr inarp [*inarp*]

[パラメータ] ◦ *inarp*
- on.....使用する
- off.....使用しない

[説明] 選択されている相手について、InARP (Inverse Address Resolution Protocol) を使用して、相手の IP アドレスを自動取得するかどうかを設定する。この設定が on の場合でも、自分の PP 側のローカル IP アドレスが設定されていない場合 (unnumbered) は InARP は使用しない。
また、自分の PP 側ローカル IP アドレスが設定されていれば、相手から InARP のリクエストが来た場合、この設定に関わらず常にレスポンスを返す。

[ノート] ip pp address コマンドを参照

[デフォルト値] on

11.5 フレームリレーダウン時にバックアップする相手先情報番号の設定

[入力形式] fr backup dlci=*dlci_num peer_num*
no fr backup dlci=*dlci_num* [*peer_num*]

[パラメータ] ◦ *dlci_num*
- DLCI 値 (16..991)

◦ *peer_num*.....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 dlci=*dlci_num type*
no fr compression use dlci=*dlci_num* [*type*]

[パラメータ]
- *dlci_num*
  - DLCI 値 (16..991)
  - * (すべてのデータリンク)
- *type*
  - 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。*dlci_num* 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]
type = none

11.7 DLCI ごとのパラメータの設定

[入力形式]
fr cir dlci=*dlci_num cir* [slowstart-idle=*idle*] [bc=*bc_size*] [be=*be_size*] [s=*step_count*]
no fr cir dlci=*dlci_num* [*cir* []]

[パラメータ]
- *dlci_num* ..... DLCI 値 (16..991)
- *cir* ..... CIR 値 (bit/s 単位)
- *idle* ..... 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
- *bc_size* ..... 認定バーストサイズ (ビット)
- *be_size* ..... 超過バーストサイズ (ビット)
- *step_count* ..... 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]
idle = 20
bc=*be* = 7000
s=cir/bc_size/be_size 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 *control*
no fr congestion control [*control*]

[パラメータ]
- *control*
  - 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 *type*
no fr pp dequeue type [*type*]

[パラメータ]
- *type*
  - serial.....順次サーチ方式
  - round-robin..... ラウンドロビン方式

[説明] 同じフレームリレー回線に複数の PP インタフェースがバインドされている場合の送信順序方式を設定する。serial の場合には、同じフレームリレー回線にバインドされた PP インタフェースに対して順位を与え、順位の高い PP インタフェースから優先してパケットを送信する。round-robin の場合には、優先順位を設定せずにすべての PP インタフェースから均等にパケットを送信する。

[ノート] 相手先情報番号の若い PP インタフェースがより高い順位を持つものと定義する。

[デフォルト値] round-robin

11.10 指定パケットに DE ビットを立てるか否かの設定

[入力形式] fr de *protocol* filter dlci=*dlci_num filter_num_list*
no fr de *protocol* filter dlci=*dlci_num* [*filter_num_list*]

[パラメータ]
- *protocol*
  - ip .....IP パケット
  - ipx.....IPX パケット
  - bridge.....ブリッジするパケット
- *filter*.....固定のキーワード
- *dlci_num*
  - DLCI 値 (16..991)
  - * (すべてのデータリンク)
- *filter_num_list*.....静的フィルタ番号 (1..100) の並び

[説明] 指定パケットに DE ビットを立てるか否かを設定する。
filter_num_list で指定したフィルタを順番にパケットに対して適用し、マッチしたところでそのフィルタが pass、pass-log、pass-nolog、restrict、restrict-log、restrict-nolog のいずれかであれば DE ビットを立てる。reject、reject-log または reject-nolog である場合は DE ビットを立てない。フィルタ列の最後までマッチしなかった場合には DE ビットを立てない。

[デフォルト値] DE ビットは立てない

12. PRI関連の設定

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

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

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

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

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

(A): HSD，DA1500，スーパーリレー FR
(B): HSD の多重アクセスサービス
(C): INS ネット 1500
YBA-1PRI-N: 多重化非対応 PRI 拡張モジュール
YBA-1PRI-M: 多重化、回線交換対応 PRI 拡張モジュール
YMS15P: 多重化、回線交換対応オプションソフトウェア

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

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

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

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

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

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

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

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

12.1 PRI 回線の種類の設定

[入力形式] line type *interface line*
no line type *interface line*

[パラメータ]
- *interface* .....PRI インタフェース名
- *line*
  - isdn ,isdn-ntt .....ISDN 回線交換
  - leased .....ディジタル専用線

[説明] PRI 回線の種類を指定する。設定の変更は、再起動か、あるいは該当インタフェースに対する interface reset コマンドの発行により反映される。

[デフォルト値] leased

12.2 情報チャネルとタイムスロットの設定

[入力形式] pri leased channel *pri/info timeslot_head timeslot_num*
no pri leased channel *pri/info* [*timeslot_head timeslot_num*]

[パラメータ]
- *pri*.....PRI インタフェース名
- *info*.....情報チャネル番号 (1..24)
- *timeslot_head*.....先頭タイムスロット番号 (1..24)
- *timeslot_num* .....タイムスロット数 (1..24)

以下のニーモニックが使用可能

ニーモニック速度 (bit/s)	タイムスロット数
192k	3
256k	4
384k	6
512k	8
768k	12
1024k	16
1536k	24

[説明] 指定した PRI 回線内の情報チャネルを、先頭タイムスロット番号とタイムスロット数 (通信速度) で設定する。

[ノート] 設定変更時には再起動か、対象の PRI インタフェースに対する interface reset コマンドが必要である。
RT300i の多重化非対応の PRI 拡張モジュール (YBA-1PRI-N)、RT105p、RT140p(YMS15P なし) では、2 つ以上の情報チャネルは設定できない。

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*.....情報チャネル番号

[説明] 選択されている相手先に対して実際に使用するインタフェースを設定する。

[ノート] PRI 回線を専用線として使用する場合、pri leased channel コマンドで設定した情報チャネル番号を、インタフェース名に付加する必要がある。
例えば、pri leased channel 1/1 1 24 の場合は、pp bind pri1/1 となる。

[デフォルト値] どのインタフェースともバインドされていない

13. IPsec の設定

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

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

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

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

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

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

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

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

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

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

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

セキュリティ・ゲートウェイの識別子はモデルにより異なり、以下の表のようになります。

モデル	セキュリティ・ゲートウェイの識別子
RT300i + YBA-VPN	1 - 500
RT300i	1 - 100
RT140p	1 - 20
RT140f	1 - 20
RT140i	1 - 20
RT140e	1 - 20
RT105p	1 - 20
RT105i	1 - 20
RT105e	1 - 30

13.1 事前共有鍵の登録

[入力形式] ipsec ike pre-shared-key *gateway_id key*
ipsec ike pre-shared-key *gateway_id* text *text*
no ipsec ike pre-shared-key *gateway_id* [...]

[パラメータ]
- *gateway_id* .....セキュリティ・ゲートウェイの識別子
- *key* .....鍵となる 0x ではじまる 16 進数列 (最大 32 バイト)
- *text* ..... ASCII 文字列で表した鍵 (最大 32 文字)

[説明] 鍵交換に必要な事前共有鍵を登録する。設定されていない場合には、鍵交換は行われない。
鍵交換を行う相手ルータには同じ事前共有鍵が設定されている必要がある。

[デフォルト値] 事前共有鍵は設定されていない

[設定例]
ipsec ike pre-shared-key 1 text himitsu
ipsec ike pre-shared-key 8 0xCDEEEDC0CDEDCD

13.2 相手側セキュリティ・ゲートウェイの IP アドレスの設定

[入力形式] ipsec ike remote address *gateway_id ip_address*
no ipsec ike remote address *gateway_id* [*ip_address*]

[パラメータ]
- *gateway_id* .....セキュリティ・ゲートウェイの識別子
- *ip_address*
  - 相手側セキュリティ・ゲートウェイの IP アドレス
  - any.....自動選択

[説明] 相手側セキュリティ・ゲートウェイの IP アドレスを設定する。相手側セキュリティ・ゲートウェイ 1 つに対して 1 つ設定可能である。

13.3 相手側のセキュリティ・ゲートウェイの名前の設定

[入力形式] ipsec ike remote name *gateway name*
no ipsec ike remote name *gateway* [*name*]

[パラメータ]
- *gateway* .....セキュリティ・ゲートウェイの識別子
- *name* .....名前 (最大 32 文字)

[説明] 相手側のセキュリティ・ゲートウェイの名前を設定する。

13.4 自分側セキュリティ・ゲートウェイの IP アドレスの設定

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

[パラメータ]
- *gateway_id* .....セキュリティ・ゲートウェイの識別子
- *ip_address*
  - 自分側セキュリティ･ゲートウェイの IP アドレス
  - any.....自動選択
- *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* [*type*]
no ipsec ike local name *gateway_id* [*name*]

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

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

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
- *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、3DES-CBC と DES-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
- *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
- *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
- *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
- *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、debug レベルの SYSLOG で出力される。

[ノート] このコマンドが設定されていない場合には、最小限のログしか出力しない。複数の *type* パラメータを設定することもできる。

13.12 IKE ペイロードのタイプの設定

[入力形式] ipsec ike payload type *gateway_id type*
no ipsec ike payload type *gateway_id* [*type*]

[パラメータ]
- *gateway_id* ..... セキュリティ・ゲートウェイの識別子
- *type* ..... ペイロードのタイプ
  - 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
- *pfs*
  - on ..... 用いる
  - off ..... 用いない

[説明]　IKE で PFS(Perfect Forward Secrecy) を用いるか否かを設定する。

[ノート]　相手側のセキュリティ・ゲートウェイと同じように設定する必要がある。

[デフォルト値]　off

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
- *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 *gateway_id info*
no ipsec ike send info *gateway_id* [*info*]

[パラメータ]
- *gateway_id* ..... セキュリティ・ゲートウェイの識別子
- *info*
  - 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いけない。

13.16.1　SA のポリシーの定義

[入力形式]　ipsec sa policy *policy_id gateway_id* ah *ah_algorithm*
ipsec sa policy *policy_id gateway_id* esp *esp_algorithm* [*ah_algorithm*]
no ipsec sa policy *policy_id* [*gateway_id*]

[パラメータ]
- *policy_id* ..... ポリシー ID (1..255)
- *gateway_id* ..... セキュリティ・ゲートウェイの識別子
- ah ..... 認証ヘッダ (Authentication Header) を示すキーワード
- esp ..... 暗号ペイロード (Encapsulating Security Payload) を示すキーワード
- *ah_algorithm*
  - md5-hmac HMAC-MD5
  - sha-hmac ..... HMAC-SHA
- *esp_algorithm*
  - 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 SA の寿命の設定

[入力形式] ipsec ike duration *sa gateway_id second* [*kbytes*]
no ipsec ike duration *sa gateway_id* [*second* [*kbytes*]]

[パラメータ]
- *sa*
  - ipsec-sa.....IPsec SA
  - isakmp-sa.....ISAKMP SA
- *gateway_id* .....セキュリティ・ゲートウェイの識別子
- *second* .....秒数 (300..691200)
- *kbytes* .....キロ単位のバイト数 (100..100000)

[説明] IKE で提案する IPsec SA または ISAKMP SA の寿命を設定する。
kbytes パラメータを指定した場合には、*second* パラメータで指定した時間を経過するか指定したバイト数のデータが処理された後に SA は消滅する。

[デフォルト値] 28800 秒

13.16.3 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。

13.16.4 SA の手動更新

[入力形式] ipsec refresh sa

[パラメータ] なし

[説明] SA を手動で更新する。

[ノート] 管理されている SA をすべて削除して、IKE の状態を初期化する。

13.16.5 SA を自動更新するか否かの設定

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

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

[説明] SA を自動更新するか否かを設定する。

[ノート] 古い SA を削除せずに新しい SA を生成する。

[デフォルト値] off

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、ほとんど効果がない。一方、IPComp は IPsec による暗号化の前にデータ圧縮が行われるため、一定の効果が得られる。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力できない。

13.17.6 IKE キープアライブの設定

[入力形式] ipsec ike keepalive use *gateway use*
no ipsec ike keepalive use *gateway* [*use*]

[パラメータ]
- *gateway* ..... セキュリティゲートウェイの識別子
- *use*
  - on ..... 使用する
  - off ..... 使用しない

[説明] IKE のキープアライブを使用するか否かを設定する。

[デフォルト値] off

13.17.7 トンネルバックアップの設定

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

[パラメータ]
- *peer_num* ..... バックアップ先の相手先情報番号

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

[デフォルト値] none

13.17.8 トンネルインタフェースに対する静的経路の無効化

[入力形式] ip tunnel hide static route *hide*
no ip tunnel hide static route [*hide*]

[パラメータ]
- *hide*
  - on ..... 静的経路を無効化する
  - off ..... 静的経路を無効化しない

[説明] トンネルインタフェースが down しているときに、その TUNNEL インタフェースに対する静的経路を無効にするか否かを設定する。

[デフォルト値] off

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] ipsec transport *id policy_id* [*proto* [*src_port_list* [*dst_port_list*]]]
no ipsec transport *id* [*policy_id* [*proto* [*src_port_list* [*dst_port_list*]]]]

[パラメータ]
- *id* ..... トランスポート ID (1..255)
- *policy_id* ..... ポリシー ID (1..255)
- *proto* ..... プロトコル
- *src_port_list* ..... UDP、TCP のソースポート番号列
  - ポート番号を表す 10 進数
  - ポート番号を表すニーモニック
  - * (すべてのポート)
- *dst_port_list* ..... UDP、TCP のデスティネーションポート番号列
  - ポート番号を表す 10 進数
  - ポート番号を表すニーモニック
  - * (すべてのポート)

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

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

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

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

[設定例]
```
# snmp trap host 192.168.0.2
# snmp enableauthentraps 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*
- none ..... すべてのホストから SNMP によりアクセスできない
- any..... すべてのホストから SNMP によりアクセスできる
- IP アドレス ..... SNMP によるアクセスを許可するホストの IP アドレス

[説明] SNMP によるアクセスを許可するホストを設定する。

[デフォルト値] none

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

[設定例] # snmp syscontact “RT administrator”

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

[設定例] # snmp syslocation “RT room”

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

[設定例] # snmp sysname “RT300i with VPN module”

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 *sw*
no snmp display ipcp force

[パラメータ] ◦ *sw*
- on ..... IPCP により付与された IP アドレスを PP インタフェースのアドレスとして必ず表示する
- off ..... IPCP により付与された IP アドレスは PP インタフェースのアドレスとして必ずしも表示されない

[説明] 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。
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。
本コマンドを on に設定しておくと、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。

[デフォルト値] off

14.12 SNMP送信パケットの始点アドレスの設定

[入力形式] snmp local address *ip_address*
no snmp local address [*ip_address*]

[パラメータ] ◦ *ip_address* ..... IP アドレス

[説明] SNMP 送信パケットの始点 IP アドレスを設定する。

[デフォルト値] インタフェースに設定されているアドレスから自動選択

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 *auth*
no radius auth [*auth*]

[パラメータ] ◦ *auth*
- on.....使用する
- off.....使用しない

[説明] anonymous に対して何らかの認証を要求する設定の場合に、相手から受け取ったユーザネーム (PAP であれば UserID、CHAP であれば NAME) が、自分で持つユーザネーム (pp auth username コマンドで指定) の中に含まれていない場合には RADIUS サーバに問い合わせるか否かを設定する。

[ノート] RADIUS による認証と RADIUS によるアカウントは独立して使用できる。
サポートしているアトリビュートについては、WWW サイトのドキュメント <http://www.rtpro.yamaha.co.jp> を参照すること。

[デフォルト値] off

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 *account*
no radius account [*account*]

[パラメータ] ◦ *account*
- on.....使用する
- off.....使用しない

[説明] RADIUS によるアカウントを使用するか否かを設定する。

[ノート] RADIUS による認証と RADIUS によるアカウントは独立して使用できる。
サポートしているアトリビュートについては、WWW サイトのドキュメント <http://www.rtpro.yamaha.co.jp> を参照すること。

[デフォルト値] off

15.3 RADIUS サーバの指定

[入力形式] radius server *ip1* [*ip2*]
no radius server [*ip1* [*ip2*]]

[パラメータ] ◦ *ip1* .....RADIUS サーバ (正) の IP アドレス（IPv6 アドレス可）
◦ *ip2* .....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 *ip1* [*ip2*]
no radius auth server [*ip1* [*ip2*]]

[パラメータ] ◦ *ip1* .....RADIUS 認証サーバ (正) の IP アドレス（IPv6 アドレス可）
◦ *ip2* .....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] RFC2138 ではポート番号として 1812 を使うことになっている。

[デフォルト値] 1645

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] RFC2138 ではポート番号として 1813 を使うことになっている。

[デフォルト値] 1646

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。

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

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

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

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

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 *interface* nat descriptor *nat_descriptor_list*
ip pp nat descriptor *nat_descriptor_list*
ip tunnel nat descriptor *nat_descriptor_list*
no ip *interface* nat descriptor [*nat_descriptor_list*]
no ip pp nat descriptor [*nat_descriptor_list*]
no ip tunnel nat descriptor [*nat_descriptor_list*]

[パラメータ]

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

[説明]

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

[ノート]

インタフェースが LAN である場合、NAT ディスクリプタの OUTER アドレスに関しては、同一 LAN の ARP 要求に対して ARP 応答する。

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 *nat_descriptor type*
no nat descriptor type [*nat_descriptor type*]

[パラメータ]

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

[説明]

NAT 変換の動作タイプを指定する。

[ノート]

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

[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
ipcp	×	○	×
primary	○	×	×
secondary	○	×	×
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
  - 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 *nat_descriptor use*
no nat descriptor masquerade rlogin *nat_descriptor* [*use*]

[パラメータ]
- *nat_descriptor* ..... NAT ディスクリプタ番号 (1..21474836)
- *use*
  - on ..... 使用する
  - off ..... 使用しない

[説明] IP マスカレード使用時に rlogin、rcp、ssh の使用を許可するか否かを設定する。

[ノート] on にすると、rlogin、rcp と ssh のトラフィックに対してはポート番号を変換しなくなる。
また on の場合に rsh は使用できない。

[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 *nat_descriptor id inner_ip protocol port*
no nat descriptor masquerade static *nat_descriptor id* [*inner_ip protocol port*]

[パラメータ]
- *nat_descriptor* ..... NAT ディスクリプタ番号 (1..21474836)
- *id* ..... 静的 IP マスカレードエントリの識別情報 (1 以上の数値)
- *inner_ip* ..... 内側 IP アドレス (1 個)
- *protocol* ..... 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
- *port* ..... 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 *nat_descriptor time*
no nat descriptor timer *nat_descriptor* [*time*]

[パラメータ]
- *nat_descriptor* ..... NAT ディスクリプタ番号 (1..21474836)
- *time* ..... 消去タイマの秒数 (30..21474836)

[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 *type*
no nat descriptor masquerade ttl hold

[パラメータ]
- *type* ..... TTL を同期させる方法
  - all ..... すべてのコネクションを対象とする
  - ftp ..... FTP の制御チャ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 のように制御チャネルとデータチャネルからなるアプリケーションでは、制御チャ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、制御チャネルとデータチャ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ネルとデータチャ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　外側から受信したパケットに該当する変換テーブルが存在しないときの動作の設定

[入力形式]　nat descriptor masquerade incoming *nat_descriptor action* [*ip_address*]

[パラメータ]
- ○ *nat_descriptor*..... NAT ディスクリプタ番号 (1..21474836)
- ○ *action* ..... 動作
  - • through..... 変換せずに通す
  - • reject ..... 破棄して、TCP の場合は RST を返す
  - • discard..... 破棄して、何も返さない
  - • forward..... 指定されたホストに転送する
- ○ *ip_address* ..... 転送先の IP アドレス

[説明]　IP マスカレードで外側から受信したパケットに該当する変換テーブルが存在しないときの動作を設定する。ACTION が forward のときには IP_ADDRESS を設定する必要がある。

[デフォルト値]　reject

16.11　NAT のアドレス割当をログに記録するか否かの設定

[入力形式]　nat descriptor log *switch*

[パラメータ]
- ○ *switch*
  - • on ..... 記録する
  - • off..... 記録しない

[説明]　NAT のアドレス割当をログに記録するか否かを設定します。

[デフォルト値]　off

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 を利用するか否かの設定

[入力形式] dns service *service*
no dns service [*service*]

[パラメータ] ◦ *service*
- recursive ..... DNS リカーシブサーバとして動作する
- off..... サービスを停止させる

[説明] DNS リカーシブサーバとして動作するかどうかを設定する。off を設定すると、DNS 的機能は一切動作しない。また、ポート 53/udp も閉じられる。

[デフォルト値] recursive

17.2 DNS サーバの IP アドレスの設定

[入力形式] dns server *ip_address* [*ip_address* ...]
no dns server [*ip_address* ...]

[パラメータ] ◦ *ip_address*.....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

17.3 DNS サーバを通知してもらう相手先情報番号の設定

[入力形式] dns server pp *peer_num*
no dns server pp [*peer_num*]

[パラメータ] ◦ *peer_num*.....DNS サーバを通知してもらう相手先情報番号

[説明] DNS サーバを通知してもらう相手先情報番号を設定する。このコマンドで相手先情報番号が設定されていると、DNS での名前解決を行う場合に、まずこの相手先に発信して、そこで PPP の IPCP MS 拡張機能で通知された DNS サーバに対して問い合わせを行う。
相手先に接続できなかったり、接続できても DNS サーバの通知がなかった場合には名前解決は行われない。
dns server コマンドで DNS サーバが明示的に指定されている場合には、そちらの設定が優先される。dns server コマンドに指定したサーバから返事がない場合には、相手先への接続と DNS サーバの通知取得が行われる。

[ノート] この機能を使用する場合には、dns server pp コマンドで指定された相手先情報に、ppp ipcp msext on の設定が必要である。

[デフォルト値] DNS サーバを通知してもらう相手先は設定されていない

[設定例]
```
# pp select 2
pp2# ppp ipcp msext on
pp2# dns server pp 2
```

17.4　DNS 問い合わせの内容に応じた DNS サーバの選択

[入力形式]

dns server select *id server* [*type*] *query* [*original-sender*][restrict pp *connection-pp*]
dns server select *id* pp *pp_num* [*default-server*] [*type*] *query* [*original-sender*] [restrict pp *connection-pp*]
dns server select *id* dhcp *interface* [*default-server*] [*type*] *query* [*original-sender*] [restrict pp *connection-pp*]
dns server select *id* reject [*type*] *query* [*original-sender*]
no dns server select *id*

[パラメータ]

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

[説明]

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

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

17.5　DNS ドメイン名の設定

[入力形式]

dns domain *domain_name*
no dns domain [*domain_name*]

[パラメータ]

- *domain_name* ..... DNS ドメインを表す文字列

[説明]

ルータが所属する DNS ドメインを設定する。
名前解決に失敗した場合、このドメイン名を補完して再度解決を試みる。
ルータが DHCP サーバとして機能する場合、設定したドメイン名は DHCP クライアントに通知するためにも使用される。ルータのあるネットワークおよびそれが含むサブネットワークの DHCP クライアントに対して通知する。
空文字列を設定する場合には、dns domain とだけ入力する。

17.6 プライベートアドレスに対する問い合わせを処理するか否かの設定

[入力形式] dns private address spoof *spoof*
no dns private address spoof [*spoof*]

[パラメータ] ◦ *spoof*
- on.....処理する
- off.....処理しない

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

[デフォルト値] off

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

[入力形式] dns notice order *protocol server* [*server*]
no dns notice order *protocol* [*server* [*server*]]

[パラメータ] ◦ *protocol*
- dhcp .....DHCP による通知
- msext .....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
msext me server

17.8 SYSLOG 表示で DNS により名前解決するか否かの設定

[入力形式] dns syslog resolv *resolv*
no dns syslog resolv [*resolv*]

[パラメータ] ◦ *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

17.9　静的 DNS レコードの登録

[入力形式]

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

[パラメータ]

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

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

type パラメータ	name	*value*
a	FQDN	IP アドレス
ptr	IP アドレス	FQDN
mx	FQDN	FQDN
ns	FQDN	FQDN
cname	FQDN	FQDN

◦ *fqdn* ..... ドメイン名を含んだホスト名

[説明]

静的な DNS レコードを定義する。
ip host コマンドは、dns static コマンドで a と ptr を両方設定することを簡略化したものである。

[ノート]

問い合わせに対して返される DNS レコードは以下のような特徴を持つ。

◦ TTL フィールドには 1 がセットされる
◦ Answer セクションに回答となる DNS レコードが 1 つセットされるだけで、Authority/Additional セクションには DNS レコードがセットされない
◦ MX レコードの preference フィールドは 0 にセットされる

[設定例]

```
# ip host pc1.rtpro.yamaha.co.jp 133.176.200.1
# dns static ptr 133.176.200.2 pc2.yamaha.co.jp
# dns static cname mail.yamaha.co.jp mail2.yamaha.co.jp
```

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 *interface speed*
speed pp *speed*
no speed *interface speed*
no speed pp [*speed*]

[パラメータ]

- *interface* .....LAN インタフェース名
- *speed*.....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]

speed 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 *num class* ip *src_addr* [*dest_addr* [*proto* [*src_port* [*dest_port*]]]]
queue class filter *num class* ipx *src_net* [*src_node* [*dst_net* [*dst_node* [*type* [*src_socket* [*dst_ socket*]]]]]]
queue class filter *num class* bridge *src_mac* [*dst_mac* [*offset byte_list*]]
no queue class filter *num class* [*protocol ...*]

[パラメータ]

- *num*.....クラスフィルタの識別番号 (1..100)
- *class*.....クラス (1..16)

IP フィルタ

- *src_addr* .....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)
- *dest_addr* .....IP パケットの終点 IP アドレス (*src_addr* と同じ形式)。省略した場合は一個の * と同じ。
- *proto*.....フィルタリングするパケットの種類
  - プロトコルを表す 10 進数
  - プロトコルを表すニーモニック

icmp	1
tcp	6
udp	17

  - 上項目のカンマで区切った並び (5 個以内)
  - * (すべてのプロトコル)
  - established

省略時は * と同じ。

◦ *src_port* ..... UDP 、TCP のソースポート番号
- ポート番号を表す 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
- 0:0:0:0:0:1 ..... FF:FF:FF:FF:FF:FE(2 桁以内の 16 進数以外に '*' も指定可)
- * (すべての IPX ノード番号)
- 省略時は一個の * と同じ

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

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

◦ *type* ..... IPX パケットタイプ
- 10 進数 (0..255)
- 16 進数 (0x0..0xFF)
- ニーモニック文字列

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

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

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

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

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

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

ブリッジフィルタ

◦ *src_mac*.....始点 MAC アドレス
- x:xx:xx:xx:xx:xx
  - 16 進数
  - *
- * (すべての MAC アドレスに対応)

◦ *dst_mac*.....終点 MAC アドレス *src_mac* と同じ形式。省略時は一個の * 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 *interface* type *type*
queue pp type *type*
no queue *interface* type *type*
no queue pp type [*type*]

[パラメータ]

- *interface* ..... LAN インタフェース名
- *type*
  - fifo ..... First In, First Out 形式のキューイング
  - priority ..... 優先制御キューイング
  - cbq..... 帯域制御キューイング
  - wfq ..... Weighted Fair Queue 形式のキューイング

[説明]

指定したインタフェースに対して、キューイングアルゴリズムタイプを選択する。
fifo は最も基本的なキューである。fifo の場合、パケットは必ず先にルータに到着したものから送信される。パケットの順番が入れ替わることは無い。fifo キューにたまったパケットの数が queue interface length コマンドで指定した値を越えた場合、キューの再後尾、つまり最も最後に到着したパケットが破棄される。

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

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

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

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

[デフォルト値] fifo

18.4 デフォルトクラスの設定

[入力形式]

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

[パラメータ]

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

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

[デフォルト値] 2

18.5 クラス分けフィルタの適用

[入力形式]

queue *interface* class filter list *filter_list*
no queue *interface* class filter list [*filter_list*]

[パラメータ]

- *interface* ..... LAN インタフェース名、もしくは pp
- *filter_list* ..... 空白で区切られたクラスフィルタの並び

[説明] 指定した LAN インタフェースまたは選択されている PP に対して、queue class filter コマンドで設定したフィルタを適用する順番を設定する。フィルタにマッチしなかったパケットは、queue interface default class コマンドで指定したデフォルトクラスに分類される。

18.6 クラスの属性の設定

[入力形式]

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

[パラメータ]

- *interface* ..... LAN インタフェース名
- *class* ..... クラス (1..16)
- *bandwidth* ..... クラスに割り当てる帯域 (bit/s)
  数値の後ろに 'k'、'M' をつけるとそれぞれ kbit/s、Mbit/s として扱われる。また、数値の後ろに '%' をつけると、回線全体の帯域に帯するパーセンテージとなる。
- *parent* ..... 親クラスの番号 (0..16)
- *borrow* ..... 帯域が足りなくなった場合に親クラスから帯域を借りるか否かの設定
  - on ..... 借りる
  - off ..... 借りない
- *maxburst* ..... 連続送信できる最大パケット数 (1..10000)
- *minburst* ..... 安定送信中に連続送信できる最大パケット数 (1..10000)
- *packetsize* ..... クラスで流れるパケットの平均パケット長 (1..10000)

[説明]

指定したクラスの属性を設定する。

[ノート]

パラメータを指定する場合には、各キーワードを明記すること。
bandwidth 属性は必ず指定されなければならない。回線全体の帯域は、speed コマンドで設定される。クラスに割り当てる帯域は、親クラス以下の値でなければいけない。
クラス番号 0 はルートクラスを表す。ルートクラスは仮想的なクラスで、常に 100% の帯域を持ち、デフォルトでは他のクラスの親クラスになっている。ルートクラスに直接パケットを割り振ることはできず、その帯域は他のクラスに貸し出すためにだけ割り当てられている。
帯域が足りなくなった場合に、親クラスから帯域を借りてくる (borrow=on) と設定すると、このクラスの最大速度は親クラスの最大速度まで増えることができる。通常は 100% の帯域を持つルートクラスを親クラスとするので、クラスの帯域は回線速度一杯に広がることができる。この場合、*bandwidth* の設定は、回線が混雑している場合に他のクラスとどの程度の割り合いで帯域をわける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いけない。デフォルトクラスの設定を忘れると、デフォルトクラスに 100% の帯域が割り振られるため、対象とするクラスは常にデフォルトクラスより狭い帯域を割り当てられることになる。

[デフォルト値]

parent = 0
borrow = on
maxburst = 20
minburst = *maxburst* / 10
packetsize = 512

18.7 クラス毎のキュー長の設定

[入力形式]

queue *interface* length *len1* [*len2...len16*]
no queue *interface* length [*len1* [*len2...len16*]]

[パラメータ]

- *len1..len16* ..... 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のできるパケットの個数を指定する。設定を省略したクラスに関しては、最後に指定されたキュー長が残りのクラスにも適用される。

[デフォルト値]

200 (LAN、RT300i 以外の機種は 40)
20 (PP、全機種共通)

18.8　MP インタリーブの設定

[入力形式]　ppp mp interleave [*delay*] *switch*
no ppp mp interleave [[*delay*] *switch*]

[パラメータ]
- *delay* ..... 遅延（ミリ秒）
- *switch*
  - on ..... MP インタリーブを使用する
  - off ..... MP インタリーブを使用しない

[説明]　MP インタリーブを使用するかどうかを設定する。*delay* では、優先されるプロトコルで許容できる最大遅延を設定する。パケットをどのような大きさに分割するかは、*delay* の値と回線速度により決定される。

[ノート]　*delay* で設定した遅延が保証されるわけではない。
データの受信側でも同じ設定をしておかないと、効果が発揮されない。
同時に圧縮は利用できない。圧縮を利用する設定の場合、この機能は無視されるので、以下の設定で圧縮を無効にしておく必要がある。

```
ppp ccp type none
```

[デフォルト値]　*delay* = 30
switch = on

[設定例]

```
# queue class filter 1 4 ip VOIP-GATEWAY * * * *
# queue class filter 2 3 ip * * icmp * *
# queue class filter 3 1 ip * * * * *
# pp select 1
# pp bind bri2.1
# queue pp type priority
# queue class filter list 1 2 3
# isdn remote address call 03-123-4567
# ppp mp use on
# ppp mp interleave on
# ppp mp maxlink 1
# ppp ccp type none
# pp enable 1
```

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いけない。

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を使用するか否かを設定する。

[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 *protocol* [filter *filter_num*...]
no ospf import from [*protocol* [filter *filter_num*...]]

[パラメータ]
- *protocol* ..... OSPF の経路テーブルに導入する外部プロトコル
  - static ..... 静的経路
  - rip ..... RIP
- *filter_num* ..... フィルタ番号

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

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

経路を広告する場合のパラメータであるメトリック値、メトリックタイプ、タグは、フィルタの検査で該当した ospf import filter コマンドで指定されたものを使う。filter キーワード以降を省略した場合には、以下のパラメータを使用する。
- *metric* = 1
- *type* = 2
- *tag* = 1

[デフォルト値] 外部経路は導入しない

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 *filter_num* [not] *kind ip_address/mask*...[*parameter*...]
no ospf import filter *filter_num* [[not] *kind ip_address/mask*...[*parameter*...]]

[パラメータ]
- *filter_num* ..... フィルタ番号
- *kind* ..... フィルタ種別
  - include ..... 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)
  - refines ..... 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)
  - equal ..... 指定したネットワークアドレスに一致する経路
- *ip_address/mask* ..... 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
- *parameter* ..... 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
  - metric ..... メトリック値 (0..16777215)
  - type ..... メトリックタイプ (1..2)
  - tag ..... 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 項で指定されてはじめて効果を持つ。
ip_address/mask では、ネットワークアドレスを設定する。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。

kind では、経路の検査方法を設定する。
- include ..... 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
- refines ..... 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
- equal ..... 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

kind 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。

parameter 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 metric、type、tag 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。
- *metric* = 1
- *type* = 2
- *tag* = 1

19.7 OSPF エリア設定

[入力形式] ospf area *area* [auth=*auth*] [stub [cost=*cost*]]
no ospf area *area* [auth=*auth*] [stub [cost=*cost*]]

[パラメータ]
- *area*
  - backbone .....バックボーンエリア
  - 1 以上の数値 .....非バックボーンエリア
  - IP アドレス表記 (0.0.0.0 は不可) 非バックボーンエリア
- *auth*.....認証を行う
  - text..... プレーンテキスト認証
  - md5 .....MD5 認証
- *cost* .....0 以上の数値

[説明] OSPF エリアを設定する。
- stub [cost=*cost*] .....スタブエリアであることを指定する。*cost* 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 *area network/mask* [restrict]
no ospf area network *area network/mask* [restrict]

[パラメータ]
- *area*
  - backbone .....バックボーンエリア
  - 1 以上の数値 .....非バックボーンエリア
  - IP アドレス表記 (0.0.0.0 は不可) 非バックボーンエリア
- *network* .....IP アドレス
- *mask*.....ネットマスク長

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

19.9 スタブ的接続の広告

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

[パラメータ]
- *area*
  - backbone .....バックボーンエリア
  - 1 以上の数値 .....非バックボーンエリア
  - IP アドレス表記 (0.0.0.0 は不可) 非バックボーンエリア
- *host*.....IP アドレス
- *cost* .....1 以上の数値

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

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 ..... 非バックボーンエリア
- IP アドレス表記 (0.0.0.0 は不可) 非バックボーンエリア

◦ *parameters*.....*name*=*value* の列

[説明] 仮想リンクを設定する。仮想リンクは *router_id* で指定したルータに対して、*area* で指定したエリアを経由して設定される。*parameters* では、仮想リンクのパラメータが設定できる。パラメータは *name*=*value* の形で指定され、以下の種類がある。

name	*value*	**説明**
retransimit-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いけない。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
retransimit-interval = 5 秒
transmit-delay = 1 秒
hello-interval = 10 秒
dead-interval = 40 秒
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...*]
ip pp ospf area *area* [*parameters...*]
ip tunnel ospf area *area* [*parameters...*]
no ip *interface* ospf area *area* [*parameters...*]
no ip pp ospf area [*area* [*parameters...*]]
no ip pp ospf area [*area* [*parameters...*]]

[パラメータ]

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

[説明]

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

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

[ノート]

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

point-to-multipoint を利用する場合には、フレームリレーの PVC はフルメッシュである必要はなく、一部が欠けたパ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

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

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

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

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

◦ hello-interval/dead-interval について
hello-interval/ dead-interval の値は、そのインタフェースから直接通信できるすべての近隣ルータとの間で同じ値でなくてはいけない。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
retransimit-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*
ipv6 pp address *ipv6_address/prefix_len*
ipv6 tunnel address *ipv6_address/prefix_len*
no ipv6 *interface* address *ipv6_address/prefix_len*
no ipv6 pp address *ipv6_address/prefix_len*
no ipv6 tunnel address *ipv6_address/prefix_len*

[パラメータ]

- *interface* .....LAN インタフェース
- *ipv6_address*.....IPv6 アドレス
- *prefix_len* .....プレフィックス長

[説明]

インタフェースに IPv6 アドレスを付与する。

[ノート]

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

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 *prefix_id prefix*/*prefix_len* [valid_lifetime=*time*] [preferred_lifetime=*time*] [l_flag=*sw*] [a_flag=*sw*]
no ipv6 prefix *prefix_id*

[パラメータ]
- *prefix_id* ..... プレフィックス番号
- *prefix*..... プレフィックス
- *prefix_len*..... プレフィックス長
- valid_lifetime ..... プレフィックスの有効寿命（60..15552000）
- preferred_lifetime ..... プレフィックスの推奨寿命（60..15552000）
- *time*..... 時間設定
  - *YYYY-MM-DD,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）
- l_flag ..... on-link フラグ
- a_flag..... autonomous address configuration フラグ
- *sw*
  - on
  - off

[説明]
ルータ広告で配布するプレフィックスを定義する。実際に広告するためには、ipv6 *interface* rtadv prefix コマンドの設定が必要である。
time では寿命を秒数または寿命が尽きる時刻のいずれかを設定できる。*time* として数値（60 以上 15552000 以下) を設定すると、その秒数を寿命として広告する。*time* として時刻を設定すると、その時刻に寿命が尽きるものとして寿命を計算し、広告する。時刻を設定する場合は、上記のフォーマットに従う。最終有効期間とはアドレスが無効になるまでの時間であり、推奨有効期間とはアドレスを新たな接続での使用が不可となる時間である。また、on-link フラグはプレフィックスがそのデータリンクに固有である時に on とする。autonomous address configuration フラグはプレフィックスを自律アドレス設定で使うことができる場合に on とする。

[ノート]
リンクローカルのプレフィックスを設定することはできない。

[デフォルト値]
valid_lifetime = 2592000
preferred_lifetime = 604800
l_flag = on
a_flag = on

20.2.2 ルータ広告の送信の制御

[入力形式]
ipv6 *interface* rtadv send *prefix_id* [*prefix_id*...] [m_flag=*sw*] [o_flag=*sw*]
ipv6 pp rtadv send *prefix_id* [*prefix_id*...] [m_flag=*sw*] [o_flag=*sw*]
no ipv6 *interface* rtadv send
no ipv6 pp rtadv send

[パラメータ]
- *interface* ..... LAN インタフェース
- *prefix_id* ..... プレフィックス番号
- m_flag..... managed address configuration フラグ
- o_flag..... other stateful configuration フラグ
- *switch*
  - on
  - off

[説明]
インタフェースごとにルータ広告の送信を制御する。送信されるプレフィックスとして、ipv6 prefix コマンドで設定されたものが用いられる。managed address configuration フラグを off とすることで、ネットワークに接続されているホストのステートレス自動設定が許され、ホスト自身でアドレス設定がなされる。また other stateful configuration フラグを off とすることで、ホストはオプションとして格納されているプレフィックスリストを調べることになる。

[デフォルト値]
m_flag = off
o_flag = off

20.3 経路制御

20.3.1 IPv6 の経路情報の追加

[入力形式]
ipv6 route *network* gateway *gateway* [*parameter*] [gateway *gateway* [*parameter*]]
no ipv6 route *network*

[パラメータ]
- *network*
  - IP アドレス .....IPv6 アドレス / プレフィックス長
  - default .....デフォルト経路
- *gateway* .....ゲートウェイ
  - IP アドレス % スコープ識別子
  - pp *pp_num* [dlci=*dlci*] ..... PP インタフェースへの経路
    "dlci=*dlci*" が指定された場合は、フレームリレーの DLCI への経路
    - *pp_num*
      - 相手先情報番号
      - anonymous
  - pp anonymous name=*name*
    - *name* ..... PAP/CHAP による名前
  - tunnel *tunnel_num* ..... トンネルインタフェースへの経路
- *parameter* .....以下のパラメータを空白で区切り複数設定可能
  - metric *metric* .....メトリックの指定
    - *metric* ..... メトリック値 (1..15) (省略時は 1)
  - hide .....出力インタフェースが PP インタフェースの場合のみ有効なオプションで、回線が接続されている場合だけ経路が有効になることを意味する

[説明]
IPv6 の経路情報を追加する。LAN インタフェースが複数ある機種ではスコープ識別子でインタフェースを指定する必要がある。インタフェースに対応するスコープ識別子は show ipv6 address コマンドで表示される。
LAN インタフェースがひとつである機種に関しては、スコープ識別子が省略されると LAN1 が指定されたものとして扱う。

20.4 RIPng

20.4.1 RIPng の使用の設定

[入力形式]
ipv6 rip use *use*
no ipv6 rip use

[パラメータ]
- *use*
  - on.....RIPng を使う
  - off.....RIPng を使わない

[説明]
RIPng を使うか否かを設定する。

[デフォルト値]
off

20.4.2 インタフェースにおける RIPng の送信ポリシーの設定

[入力形式]
ipv6 *interface* rip send *send*
ipv6 pp rip send *send*
no ipv6 *interface* rip send
no ipv6 pp rip send

[パラメータ]
- *interface* .....LAN インタフェース
- *send*
  - on.....RIPng を送信する
  - off.....RIPng を送信しない

[説明]
RIPng の送信ポリシーを設定する。

[デフォルト値]
off

20.4.3 インタフェースにおける RIPng の受信ポリシーの設定

[入力形式]
ipv6 *interface* rip receive *sw*
ipv6 pp rip receive *sw*
no ipv6 *interface* rip receive
no ipv6 pp rip receive

[パラメータ]
- *interface* ..... LAN インタフェース
- *sw* ..... スイッチ
  - on ..... 受信した RIPng パケットを処理する
  - off ..... 受信した RIPng パケットを無視する

[説明]
RIPng の受信ポリシーを設定する。

[デフォルト値]
on

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

[入力形式]
ipv6 *interface* rip trust gateway [except] *gateway* [*gateway* ...]
ipv6 pp rip trust gateway [except] *gateway* [*gateway* ...]
no ipv6 *interface* rip trust gateway
no ipv6 pp rip trust gateway

[パラメータ]
- *interface* ..... LAN インタフェース
- *gateway* ..... IPv6 アドレス

[説明]
信頼できる RIPng ゲートウェイを設定する。
except キーワードを指定していない場合には、列挙したゲートウェイを信用できるゲートウェイとし、それらからの RIP だけを受信する。
except キーワードを指定した場合は、列挙したゲートウェイを信用できないゲートウェイとし、それらを除いた他のゲートウェイからの RIP だけを受信する。

20.4.5 RIPng の加算ホップ数の設定

[入力形式]
ipv6 pp rip hop *direction hop*
no ipv6 pp rip hop

[パラメータ]
- *direction* ..... 方向
  - in ..... 受信時に加算する
  - out ..... 送信時に加算する
- *hop* ..... 加算ホップ数（0..15）

[説明]
PP インタフェースで送受信する RIPng のメトリックに対して加算するホップ数を設定する。

[デフォルト値]
0

20.4.6 RIPng で送受信する経路に対するフィルタリングの設定

[入力形式]
ipv6 *interface* rip filter *direction filter_list* [*filter_list...*]
ipv6 pp rip filter *direction filter_list* [*filter_list...*]
no ipv6 *interface* rip filter
no ipv6 pp rip filter

[パラメータ]
- *interface* ..... LAN インタフェース
- *direction* ..... 方向
  - in ..... 内向きのパケットを対象にする
  - out ..... 外向きのパケットを対象にする
- *filter_list* ..... フィルタ番号

[説明]
PP インタフェースで送受信する RIPng パケットに対して適用するフィルタを設定する。

[デフォルト値]
フィルタは設定されていない

20.4.7 回線接続時の PP 側の RIPng の動作の設定

[入力形式] ipv6 pp rip connect send *action*
no ipv6 pp rip connect send

[パラメータ] ○ *action*
- interval……ipv6 pp rip connect interval コマンドで設定された時間間隔で RIPng を送出する
- update……経路情報が変わった時にのみ RIPng を送出する

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

[デフォルト値] update

[設定例] # ipv6 pp rip connect interval 60
ipv6 pp rip connect send interval

20.4.8 回線接続時の PP 側の RIPng 送出の時間間隔の設定

[入力形式] ipv6 pp rip connect interval *time*
no ipv6 pp rip connect interval

[パラメータ] ○ *time*……秒数 (30..21474836)

[説明] 選択されている相手について回線接続時に RIP を送出する時間間隔を設定する。

[デフォルト値] 30

[設定例] # ipv6 pp rip connect interval 60
ipv6 pp rip connect send interval

20.4.9 回線切断時の PP 側の RIPng の動作の設定

[入力形式] ipv6 pp rip disconnect send *action*
no ipv6 pp rip disconnect send

[パラメータ] ○ *action*
- none……RIPng を送信しない
- interval……ipv6 pp rip disconnect interval コマンドで設定された時間間隔で RIPng を送出する
- update……経路情報が変わった時にのみ RIPng を送信する

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

[デフォルト値] none

[設定例] # ipv6 pp rip disconnect interval 1800
ipv6 pp rip disconnect send interval

20.4.10 回線切断時の PP 側の RIPng 送出の時間間隔の設定

[入力形式] ipv6 pp rip disconnect interval *time*
no ipv6 pp rip disconnect interval

[パラメータ] ○ *time*……秒数（30..21474836）

[説明] 選択されている相手について回線切断時に RIP を送出する時間間隔を設定する。

[デフォルト値] 3600

[設定例] # ipv6 pp rip disconnect interval 1800
ipv6 pp rip disconnect send interval

20.4.11 RIPng による経路を回線切断時に保持するか否かの設定

[入力形式] ipv6 pp rip hold routing *hold*
no ipv6 pp rip hold routing

[パラメータ]
- *hold*
  - on ..... 保持する
  - off ..... 保持しない

[説明] PP インタフェースから RIPng で得られた経路を、回線が切断されたときに保持するか否かを設定する。

[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* ..... プレフィックス長
- *dst_address* ..... IP パケットの終点 IP アドレス (*src_addr* と同じ形式)。
  省略時は 1 個の * と同じ。
- *protocol* ..... フィルタリングするパケットの種類 (ip filter コマンドに準ずる)
- *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...*]
ipv6 pp secure filter *direction filter_list* [*filter_list...*]
no ipv6 *interface* secure filter *direction*
no ipv6 pp secure filter *direction*

[パラメータ]
- *interface* ..... LAN インタフェース
- *direction* ..... 方向
  - in ..... 内向きのパケットを対象にする
  - out ..... 外向きのパケットを対象にする
- *filter_list* ..... 静的フィルタ番号

[説明] IPv6 フィルタをインタフェースに適用する。

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
  - ipsec ..... IPsec tunnel mode
  - ipip ..... IPv6 over IPv4 tunnel または IPv4 over IPv6 tunnel

[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端点 IP アドレスの設定

[入力形式] tunnel endpoint address [*local*] *remote*
no tunnel endpoint address [[*local*] *remote*]

[パラメータ]
- *local* ..... 自分側のトンネルインタフェース端点の IP アドレス
- *remote* ..... 相手側のトンネルインタフェース端点の IP アドレス

[説明] トンネルインタフェース端点の IP アドレスを設定する。IP アドレスは IPv4/IPv6 いずれのアドレスも設定できるが、LOCAL と REMOTE では IPv4/IPv6 の種別が揃っていなくてはいけない。トンネルインタフェース端点として IPv4 アドレスを設定した場合には、IPv4 over IPv4 トンネルと IPv6 over IPv4 トンネルが、IPv6 アドレスを設定した場合には IPv4 over IPv6 トンネルと IPv6 over IPv4 トンネルが利用できる。

local を省略した場合は、適当なインタフェースの IP アドレスが利用される。

[ノート] このコマンドにより設定した IP アドレスが利用されるのは、tunnel encapsulation コマンドの設定値が ipip の場合だけである。IPsec トンネルでは、トンネル端点は ipsec ike local address **及び** ipsec ike remote address コマンドにより設定される。

[デフォルト値] IP アドレスは設定されていない

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、または名前
- *scope_id* ..... スコープ ID
- *interface* ..... LAN インタフェース
- *pp_num* ..... PP 番号
- *count* ..... 送信回数（1..21474836）

[説明] 指定した宛先に対して ICMPv6 Echo Request を送信する。
スコープ ID は、show ipv6 address コマンドで表示できる。

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、または名前

[説明] 指定した宛先までの経路を調べて表示する。

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
1,2	1 月と 2 月
2-	2 月から 12 月まで
2-7	2 月から 7 月まで
-7	1 月から 7 月まで
*	毎月

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

◦ *time*..... 時刻
- 時 (0..23 または *): 分 (0..59 または *)
- startup ..... 起動時

◦ *peer_num*
- 相手先情報番号
- anonymous

◦ *tunnel_num* ..... トンネルインタフェースの番号

◦ *command*..... 実行するコマンド (制限あり)

[説明]

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

[ノート]

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

[設定例]

◦ ウィークデイの 8:00 ～ 17:00 だけ接続を許可する

```
# schedule at 1 */mon-fri 8:00 pp 1 isdn auto connect on
# schedule at 2 */mon-fri 17:00 pp 1 isdn auto connect off
# schedule at 3 */mon-fri 17:05 * disconnect 1
```

◦ 毎時 0 分から 15 分間だけ接続を許可する

```
# schedule at 1 *:00 pp 1 isdn auto connect on
# schedule at 2 *:15 pp 1 isdn auto connect off
# schedule at 3 *:15 * disconnect 1
```

◦ 今度の元旦にルーティングを切替える

```
# schedule at 1 1/1 0:0 * ip route NETWORK gateway pp 2
```

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際に指定すると、設定内容を不揮発性メモリに保存して終了

[説明] ルータへのログインを終了、または管理ユーザから抜ける。
設定を変更して保存せずに管理ユーザから抜けようとすると、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、起動時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*

[パラメータ]
- *file* ..... 削除するファイル名
  - 内蔵フラッシュ ROM の設定ファイル (0..9)
  - ext0:*name*..... PCMCIA Flash ATA カードの設定ファイル

[説明] 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 *file*

[パラメータ]
- *file* ..... 削除するファイル名
  - ext0:*name* ..... PCMCIA Flash ATA カードの設定ファイル

[説明] 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ことに注意。

22.2.8 遠隔地のルータの設定

[入力形式]
remote setup *interface* [*isdn_num*[/*sub_address*]]
remote setup *interface* dlci=*dlci*

[パラメータ]
- *interface* ..... BRI、PRI インタフェース名
- *isdn_num* ..... ISDN 番号
- *sub_address* ..... ISDN サブアドレス (0x21 から 0x7e の ASCII 文字)
- *dlci* ..... フレームリレーの DLCI 番号

[説明] 指定したインタフェースを利用して、遠隔地のルータの設定をする。
インタフェースには BRI、PRI とも利用でき、また、ISDN、専用線、フレームリレーいずれの場合でも設定できる。

[ノート] 専用線の場合は、*isdn_num*、*sub_address* パラメータは不要。

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 *isdn_num*[/*sub_address*] [*isdn_num_list*]
remote setup accept any
remote setup accept none

[パラメータ]
- *isdn_num* ..... ISDN 番号
- *sub_address* ..... ISDN サブアドレス (0x21 から 0x7e の ASCII 文字)
- *isdn_num_list* ..... ISDN 番号だけまたは ISDN 番号とサブアドレス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*
clear nat descriptor interface dynamic pp *peer_num*
clear nat descriptor interface dynamic tunnel *tunnel_num*

[パラメータ] ◦ *interface* ..... LAN インタフェース名
◦ *peer_num* ..... 相手先情報番号
◦ *tunnel_num* ..... トンネルインタフェース番号

[説明] インタフェースに適用されている NAT アドレステーブルをクリアする。

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 *peer_num*
no pp enable

[パラメータ]　◦ *peer_num*
- 相手先情報番号
- anonymous
- all

[説明]　相手先を使用できる状態にする。
工場出荷時、すべての相手先は disable 状態なので、使用する場合は必ずこのコマンドで enable 状態にしなければならない。

22.4.2 相手先の使用不許可の設定

[入力形式]　pp disable *peer_num*

[パラメータ]　◦ *peer_num*
- 相手先情報番号
- anonymous
- all

[説明]　相手先を使用できない状態にする。
相手先の設定を行う場合は disable 状態であることが望ましい。

22.4.3 再起動

[入力形式]　restart
restart [*binary*][*file*]

[パラメータ]　◦ *binary*..... PCMCIA Flash ATA カードの実行形式ファイル名
◦ *file* ..... 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 *interface* [*interface* ...]

[パラメータ]　◦ *interface* ..... 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 [*pp_num*]

[パラメータ]　◦ *pp_num*
- 相手先情報番号
- anonymous

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

22.4.6 発信

[入力形式] connect *peer_num*

[パラメータ]
- *peer_num*.....発信相手の相手先情報番号

[説明] 手動で発信する。

22.4.7 切断

[入力形式] disconnect *peer_num*

[パラメータ]
- *peer_num*
  - 切断する相手先情報番号
  - all..... すべて
  - anonymous ..... anonymous のすべて
  - anonymous1..anonymous16..... 指定した anonymous

[説明] 手動で切断する。

22.4.8 ping

[入力形式] ping *host* [*count*]

[パラメータ]
- *host*
  - ping をかけるホストの IP アドレス (xxx.xxx.xxx.xxx (xxx は 10 進数))
  - ping をかけるホストの名称
- *count*
  - 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。
count パラメータを省略すると、相手からの応答があったかどうかだけを表示する。

22.4.9 traceroute

[入力形式] traceroute *host* [noresolv]

[パラメータ]
- *host*
  - traceroute をかけるホストの IP アドレス (xxx.xxx.xxx.xxx (xxx は 10 進数))
  - traceroute をかけるホストの名称
- 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 *host* [*port* [*mode* [*negotiation* [*abort*]]]]

[パラメータ]
- *host* ..... TELNET をかける相手のホスト名、もしくは IP アドレス
- *port* ..... 使用するポート番号
  - 10 進数
  - ポート番号のニーモニック
  - 省略時は 23 (TELNET)
- *mode* ..... telnet 通信 (送信) の動作モード
  - character ..... 文字単位で通信する
  - line ..... 行単位で通信する
  - auto ..... *port* パラメータの設定値により *charactor/line* を選択
  - 省略時は auto
- *negotiation* ..... telnet オプションのネゴシエーションの選択
  - on ..... ネゴシエーションする
  - off ..... ネゴシエーションしない
  - auto ..... *port* パラメータの設定値により on/off を選択
  - 省略時は auto
- *abort* ..... TELNET クライアントを強制的に終了させるためのアボートキー
  - 10 進数の ASCII コード
  - 省略時は 29(^])

[説明] TELNET クライアントを実行する。

[ノート] character モードは、通常の TELNET サーバなどへの接続のための透過的な通信を行う。
line モードは、入力行を編集して行単位の通信を行う。行編集の終了は、改行コード (CR:0x0d または LF:0x0a) の入力で判断する。

ポート番号による機能自動選択について
1. telnet 通信の動作モードの自動選択
   port 番号が 23 の場合は文字単位モードとなり、そうでない場合は行単位モードとなる。

2. telnet オプションのネゴシエーションの自動選択
   port 番号が 23 の場合はネゴシエーションし、そうでない場合はネゴシエーションしない。

[デフォルト値] *port* = 23
mode = auto
negotiation = auto
abort = 29

22.4.11 telnet サーバ機能の ON/OFF の設定

[入力形式] telnetd service *service*

[パラメータ]
- *service*
  - on ..... telnet サーバ機能を有効にする
  - off ..... telnet サーバ機能を停止させる

[説明] telnet サーバ機能の利用を選択する。

[ノート] telnet サーバが停止している場合、telnet サーバはアクセス要求に一切応答しない。

[デフォルト値] on

22.4.12 telnet サーバ機能の listen ポートの設定

[入力形式] telnetd listen *port*

[パラメータ]
- *port* ..... telnet サーバ機能の待ち受け (listen) ポート番号 (1..65535)

[説明] telnet サーバ機能の listen ポートを選択する。

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

[デフォルト値] 23

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 ..... 全ポートに属するネットワーク内ならば許可する
  - *interface* ..... LAN インタフェース名、指定 LAN インタフェースに属するネットワーク内ならば許可する
  - none ..... すべてのホストからのアクセスを禁止する

[説明] telnet サーバへアクセスできるホストの IP アドレスを設定する。

[ノート] ニーモニックをリストにすることはできない。
lan の場合、primary および secondary が clear では無く、ネットワークアドレスと directed broadcast address を除くホストアドレスからのリクエストを許可する。
設定後の新しい telnet 接続から適用される。

[デフォルト値] any

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)

data	擬似ランダムパターン
1	2^6-1
2	2^7-1
3	2^9-1
4	$2^{11}-1$

- *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ので、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ると、自動的に通信モードに復帰する。

[ノート] ループバック A の場合は、PRI コネクタを外した状態で行う必要がある。タイムスロットループバックを実行する前に、相手ルータはループバック待ち受け状態になっている必要がある。save コマンドを実行しても不揮発性メモリには保存されない。専用回線に対してのみ実行可能。
RT105p ではタイムスロットキーワードの指定はできない。

22.4.15 PRI のループバック待ち受けの設定

[入力形式]
pri loopback passive *pri* remote
pri loopback passive *pri* payload
pri loopback passive *pri* timeslot *head number*
pri loopback passive *pri* off

[パラメータ]
- *pri* ..... PRI 番号 (1..4)
- remote ..... ループバックポイントが PRI コネクタであることを示すキーワード
- payload ..... ループバックポイントがペイロードであることを示すキーワード
- timeslot ..... タイムスロットループバックを示すキーワード
- *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]
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。remote および payload キーワードの場合は、24B すべてのタイムスロットがループバックされる。timeslot キーワードの場合には、指定したタイムスロットに対してだけループバックテストされる。pri loopback passive off コマンドを実行すると、ループバックテストを終了して待ち受けモードから通常の通信モードへ復帰する。

[ノート]
ループバックテストの結果は、実行側にしか表示されない。RT140p ではディップスイッチを変更して再起動することによってもこのコマンドと同様のモードにすることが可能。ただし、ループバックテスト終了後に再びディップスイッチの変更と再起動が必要。save コマンドを実行しても不揮発性メモリには保存されない。専用回線に対してのみ実行可能。
RT105p ではタイムスロットキーワードの指定はできない。

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]
copy exec *file* internal

[パラメータ]
- *file* ..... コピー元のファイル名
  - ext0:*name* ..... PCMCIA Flash ATA カードの実行形式ファイル名
- internal ..... 保存先を示すキーワード

[説明]
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 [*peer_num*]
less config pp [*peer_num*]

[パラメータ] ◦ *peer_num*
- 相手先情報番号
- anonymous
- *peer_num* 省略時、選択されている相手について表示する

[説明] show config 、less config コマンドの表示の中から、指定した相手先情報番号に関するものだけを表示する。

23.4 PC カードの内容の表示

[入力形式] show file list *location*
less file list *location*

[パラメータ] ◦ *location* .....表示するファイルのある位置
- internal.....内蔵フラッシュ ROM
- ext0 .....外付け Flash ATA カード

[説明] 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
- *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
- *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*
show nat descriptor interface bind pp
show nat descriptor interface bind tunnel

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

[説明] NAT ディスクリプタと適用インタフェースのリストを表示する。

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*
show nat descriptor interface address pp *peer_num*
show nat descriptor interface address tunnel *tunnel_num*

[パラメータ] ◦ *interface* ..... LAN インタフェース名
◦ *peer_num* ..... 相手先情報番号
◦ *tunnel_num* ..... トンネルインタフェース番号

[説明] インタフェースに適用されている NAT ディスクリプタのアドレスマップを表示する。

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. ロギング

25.1 ログの表示

[入力形式] show log
less log

[パラメータ] なし

[説明] パワーオンからのログを表示する。
- パワーオンの日時
- 不揮発性メモリに設定を保存した日時
- 設定のためのログインの記録
- 接続した日時、発着
- 回線の種類
- 接続失敗の原因
- 切断した日時、接続時間、ISDN 料金

25.2 アカウントの表示

[入力形式] show account
show account *interface*
show account pp [*peer_num*]

[パラメータ]
- *interface* ..... BRI、PRI インタフェース名
- *peer_num*
  - 相手先情報番号
  - anonymous
  - *peer_num* 省略時、選択されている相手について表示する

[説明] 以下の項目を表示
- 発信回数
- 着信回数
- ISDN 料金の総計

[ノート] 電源 OFF や再起動により、それまでの課金情報がクリアされる。
課金額は通信の切断時に NTT から ISDN で通知される料金情報を集計しているため、割引サービスなどを利用している場合には、最終的に NTT から請求される料金とは異なる場合がある。また、NTT 以外の通信事業者を利用して通信した場合には料金情報は通知されないため、アカウントとしても集計されない 。

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

V836460 0112 CP