REMOTE ROUTER

コマンドリファレンス

ヤマハ株式会社

1999. 10. 12

♣ 本書の記載内容の一部または全部を無断で転載することを禁じます。

♣ 本書の記載内容は将来予告なく変更されることがあります。

♣ 本製品を使用した結果発生した情報の消失等の損失については、当社では責任を負いかねます。保証は本製品物損の範囲に限ります。予めご了承ください。

♣ 本書の内容については万全を期して作成致しておりますが、記載漏れやご不審な点がございましたらご一報くださいますようお願い致します。

※ イーサネットは富士ゼロックス社の登録商標です。
※ Cisco は米国 Cisco Systems,Inc. の商標です。
※ NetWare は米国 Novell,Inc. の登録商標です。
※ Microsoft, Windows は米国 Microsoft Corporation の登録商標です。
※ Stac LZS は米国 Hi/fn 社の登録商標です。

目 次

1 コマンドリファレンスの見方 1

1.1 対応するプログラムのリビジョン 1
1.2 コマンドリファレンスの見方 1
1.3 モデルによる違いについて 1
1.4 デフォルト値の変更について 2

2 ヘルプ 3

2.1 コンソールに対する簡易説明の表示 3
2.2 コマンド一覧の表示 3

3 機器の設定 3

3.1 ログインパスワードの設定 3
3.2 管理パスワードの設定 3
3.3 ルータの名称の設定 3
3.4 セキュリティクラスの設定 4
3.5 ログインタイマの設定 4
3.6 タイムゾーンの設定 5
3.7 現在の日付けの設定 5
3.8 現在の時刻の設定 5
3.9 コンソールの言語とコードの設定 5
3.10 コンソールの表示文字数の設定 6
3.11 コンソールの表示行数の設定 6
3.12 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 6
3.13 コンソールのプロンプト表示の設定 6
3.14 SYSLOG を受けるホストの IP アドレスの設定 7
3.15 SYSLOG ファシリティの設定 7
3.16 NOTICE タイプの SYSLOG を出力するか否かの設定 7
3.17 INFO タイプの SYSLOG を出力するか否かの設定 8
3.18 DEBUG タイプの SYSLOG を出力するか否かの設定 8
3.19 SYSLOG パケットの始点ポート番号の設定 8
3.20 LAN インタフェースパケットのダンプを SYSLOG へ出力するか否かの設定 9
3.21 PP インタフェースパケットのダンプを SYSLOG へ出力するか否かの設定 9
3.22 TFTP によりアクセスできるホストの IP アドレスの設定 10

4 ISDN 関連の設定 11

4.1 自分側の設定 11

4.1.1 PP 側の回線の種類の指定 11

4.1.2 自分の ISDN 番号の設定 11

4.1.3 課金額による発信制限の設定 12

4.1.4 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 12

4.1.5 バックアップからの復帰待ち時間の設定 13

4.1.6 終端抵抗の設定 13

4.1.7 PP と BRI のバインドの設定 13

4.1.8 PIAFS の発信を許可するか否かの設定 14

4.1.9 PIAFS の着信を許可するか否かの設定 14

4.2 相手毎の設定 15

4.2.1 相手 ISDN 番号の設定 15

4.2.2 相手への発信順序の設定 15

4.2.3 自動接続の設定 16

4.2.4 自動切断の設定 16

4.2.5 相手にコールバック要求を行なうか否かの設定 16

4.2.6 相手からのコールバック要求に応じるか否かの設定 17

4.2.7 着信許可の設定 17

4.2.8 発信許可の設定 17

4.2.9 エラー切断後の再発信禁止タイマの設定 18

4.2.10 再発信抑制タイマの設定 18

4.2.11 コールバック要求タイプの設定 19

4.2.12 コールバック受け入れタイプの設定 19

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 19

4.2.14 コールバックタイマの設定 20

4.2.15 コールバック待機タイマの設定 20

4.2.16 ISDN 回線を切断するタイマ方式の指定 20

4.2.17 切断タイマの設定（ノーマル） 21

4.2.18 入力切断タイマの設定（ノーマル） 21

4.2.19 出力切断タイマの設定（ノーマル） 21

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 22

4.2.21 切断タイマの設定（ファスト） 22

4.2.22 切断タイマの設定（強制） 23

4.2.23 相手先毎の課金額による発信制限の設定 23

4.2.24 同じ相手に対して連続して認証に失敗できる回数の設定 23

5 フレームリレー関連の設定 24

5.1 PP 側でのカプセル化の種類の設定 . . . 25
5.2 PP 側フレームリレーでの DLCI の設定 . . . 25
5.3 PP 側フレームリレーでの PVC 状態確認手順の設定 . . . 25
5.4 PP 側フレームリレーでの InARP 使用の設定 . . . 26
5.5 フレームリレーがダウンした時にバックアップする相手先情報番号の設定 . . . 26
5.6 FR 圧縮機能の設定 . . . 26
5.7 DLCI ごとのパラメータの設定 . . . 27
5.8 輻輳制御をするか否かの設定 . . . 27
5.9 回線に対する送信順序方式の設定 . . . 28
5.10 指定パケットに DE ビットを立てるか否かの設定 . . . 28

6 PRI 関連の設定 29

6.1 PP 側の PRI 回線の種類の設定 . . . 29
6.2 情報チャネルとタイムスロットの設定 . . . 30
6.3 情報チャネルとタイムスロットの削除 . . . 30
6.4 PP と PRI のバインドの設定 . . . 30

7 IP の設定 31

7.1 LAN,PP 共通の設定 . . . 31
7.1.1 IP パケットを扱うか否かの設定 . . . 31
7.1.2 IP パケットのフィルタの設定 . . . 31
7.1.3 IP パケットのフィルタの削除 . . . 33
7.1.4 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 . 33
7.1.5 Directed–Broadcast パケットをフィルタアウトするか否かの設定 . . . 33
7.1.6 IP パケットの TOS フィールドの書き換えの設定 . . . 34
7.2 LAN 側の設定 . . . 35
7.2.1 IP アドレスの設定 . . . 35
7.2.2 LAN 側のセカンダリ IP アドレスの設定 . . . 36
7.2.3 ネットマスクの設定 . . . 36
7.2.4 ブロードキャストアドレスの設定 . . . 37
7.2.5 経路情報の追加 . . . 37
7.2.6 経路情報の削除 . . . 38
7.2.7 動的経路制御の設定 . . . 38
7.2.8 RIP のフィルタリングの設定 . . . 39
7.2.9 RIP に関して信用できるゲートウェイの設定 . . . 39
7.2.10 LAN 側 RIP2 での認証の設定 . . . 40
7.2.11 LAN 側 RIP2 での認証キーの設定 . . . 40
7.2.12 Proxy ARP の設定 . . . 41

7.2.13 LAN 側でのフィルタリングによるセキュリティの設定 41
7.2.14 LAN インタフェースの MTU の設定 42
7.3 PP 側相手毎の IP の設定 42
7.3.1 自分の PP 側 IP アドレスの設定 42
7.3.2 相手の PP 側 IP アドレスの設定 43
7.3.3 リモート IP アドレスプールの設定 43
7.3.4 PP 側のネットマスクの設定 44
7.3.5 経路情報の追加 44
7.3.6 経路情報の削除 45
7.3.7 PP 側の動的経路制御の設定 45
7.3.8 回線接続時の PP 側の RIP の動作の設定 45
7.3.9 回線接続時の PP 側の RIP 送出の時間間隔の設定 46
7.3.10 回線切断時の PP 側の RIP の動作の設定 46
7.3.11 回線切断時の PP 側の RIP 送出の時間間隔の設定 46
7.3.12 回線切断時の動的経路制御情報の保持 46
7.3.13 RIP のフィルタリングの設定 47
7.3.14 RIP ホップ加算数の設定 47
7.3.15 RIP に関して信用できるゲートウェイの設定 47
7.3.16 PP 側 RIP2 での認証の設定 48
7.3.17 PP 側 RIP2 での認証キーの設定 48
7.3.18 PP 側でのフィルタリングによるセキュリティの設定 49
7.3.19 回線切断時の LAN 側への RIP 動作の設定 49
7.3.20 PP インタフェースの MTU の設定 50

8 IPsec の設定 51

8.1 事前共有鍵の登録 52
8.2 相手側セキュリティ・ゲートウェイの IP アドレスの設定 52
8.3 自分側セキュリティ・ゲートウェイの IP アドレスの設定 53
8.4 鍵交換の再送回数と間隔の設定 53
8.5 IKE が用いる暗号アルゴリズムの設定 53
8.6 IKE が用いるグループの設定 54
8.7 IKE が用いるハッシュアルゴリズムの設定 54
8.8 自分側の ID の設定 55
8.9 IKE のログの種類の設定 55
8.10 IKE ペイロードのタイプの設定 56
8.11 PFS を用いるか否かの設定 56
8.12 相手側の ID の設定 56
8.13 IKE の情報ペイロードを送信するか否かの設定 57

8.14 SA 関連の設定 . . . 58
8.14.1 SA のポリシーの定義 . . . 58
8.14.2 SA のポリシーの削除 . . . 58
8.14.3 IPsec SA の寿命の設定 . . . 58
8.14.4 ISAKMP SA の寿命の設定 . . . 59
8.14.5 SA の削除 . . . 59
8.14.6 SA の手動更新 . . . 59
8.14.7 SA を自動更新するか否かの設定 . . . 59
8.15 トンネルインタフェース関連の設定 . . . 60
8.15.1 使用する SA のポリシーの設定 . . . 60
8.15.2 静的トンネル経路情報の追加 . . . 60
8.15.3 静的トンネル経路情報の削除 . . . 60
8.15.4 トンネルインタフェースに対するフィルタリングの設定 . . . 61
8.16 トランスポートモード関連の設定 . . . 62
8.16.1 トランスポートモードの定義 . . . 62
8.16.2 トランスポートモードの削除 . . . 62

9 IPX の設定 63
9.1 LAN,PP 共通の設定 . . . 63
9.1.1 IPX パケットを扱うか否かの設定 . . . 63
9.1.2 IPX パケットのフィルタの設定 . . . 63
9.1.3 IPX パケットのフィルタの削除 . . . 65
9.1.4 静的な SAP テーブルの設定 . . . 65
9.1.5 静的な SAP テーブルの削除 . . . 66
9.1.6 IPX SAP Get Nearest Server Request に応答するか否かの設定 . . . 66
9.2 LAN 側の設定 . . . 67
9.2.1 イーサネットフレームタイプの設定 . . . 67
9.2.2 LAN 側の IPX ネットワーク番号の設定 . . . 67
9.2.3 経路情報の追加 . . . 68
9.2.4 経路情報の削除 . . . 68
9.2.5 LAN 側の RIP/SAP ブロードキャストの設定 . . . 68
9.2.6 LAN 側でのフィルタリングによるセキュリティの設定 . . . 69
9.3 PP 側相手毎の IPX の設定 . . . 69
9.3.1 IPX ルーティング許可の設定 . . . 69
9.3.2 PP 側 IPX ネットワーク番号の設定 . . . 70
9.3.3 経路情報の追加 . . . 70
9.3.4 経路情報の削除 . . . 70
9.3.5 回線接続時の PP 側の RIP/SAP の動作の設定 . . . 71

9.3.6 回線接続時の PP 側の RIP/SAP 送出の時間間隔の設定 71
9.3.7 回線切断時の PP 側の RIP/SAP の動作の設定 71
9.3.8 回線切断時の PP 側の RIP/SAP 送出の時間間隔の設定 72
9.3.9 回線切断時に RIP/SAP 情報を保持するか否かの設定 72
9.3.10 IPXWAN 使用の設定 72
9.3.11 Timer/Information Request の再送間隔と最大再送回数の設定 72
9.3.12 IPXWAN プライマリネットワーク番号の設定 73
9.3.13 Watchdog パケットに対する代理応答の設定 73
9.3.14 Watchdog 代理応答の時間間隔の設定 73
9.3.15 SPX キープアライブ代理応答を行うか否かの設定 73
9.3.16 SPX キープアライブ代理応答のタイマの設定 74
9.3.17 IPX シリアライゼーションパケットをフィルタアウトするか否かの設定 74
9.3.18 PP 側でのフィルタリングによるセキュリティの設定 75

10 ブリッジの設定 76

10.1 LAN,PP 共通の設定 76
10.1.1 ブリッジ使用許可の設定 76
10.1.2 ブリッジするインタフェースの設定 76
10.1.3 ブリッジのフィルタの設定 77
10.1.4 ブリッジのフィルタの削除 77
10.1.5 ブリッジする相手先の設定 78
10.1.6 MAC アドレスのラーニングを行なうか否かの設定 78
10.1.7 ラーニング情報消去タイマの設定 78
10.2 LAN 側の設定 79
10.2.1 ラーニング情報の設定 79
10.2.2 ラーニング情報の削除 79
10.2.3 LAN 側でのブリッジのフィルタリングの設定 79
10.3 PP 側相手毎のブリッジの設定 80
10.3.1 ラーニング情報の設定 80
10.3.2 ラーニング情報の削除 80
10.3.3 PP 側でのブリッジのフィルタリングの設定 80

11 PPP の設定 81

11.1 相手の名前とパスワードの設定 81
11.2 要求する認証タイプの設定 81
11.3 受け入れる認証タイプの設定 82
11.4 自分の名前とパスワードの設定 82
11.5 自分の名前の消去 82
11.6 相手の名前の削除 82

11.7 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 83
11.8 LCP 関連の設定 83
11.8.1 Address & Control Field Compression オプション使用の設定 83
11.8.2 Magic Number オプション使用の設定 83
11.8.3 Maximum Receive Unit オプション使用の設定 84
11.8.4 Protocol Field Compression オプション使用の設定 84
11.8.5 パラメータ lcp-restart の設定 84
11.8.6 パラメータ lcp-max-terminate の設定 85
11.8.7 パラメータ lcp-max-configure の設定 85
11.8.8 パラメータ lcp-max-failure の設定 85
11.8.9 専用線キープアライブを使用するか否かの設定 85
11.8.10 専用線キープアライブのログをとるか否かの設定 86
11.8.11 専用線キープアライブの時間間隔の設定 86
11.8.12 専用線ダウン検出時の動作の設定 86
11.9 PAP 関連の設定 87
11.9.1 パラメータ pap-restart の設定 87
11.9.2 パラメータ pap-max-authreq の設定 87
11.10CHAP 関連の設定 87
11.10.1 パラメータ chap-restart の設定 87
11.10.2 パラメータ chap-max-challenge の設定 87
11.11IPCP 関連の設定 88
11.11.1 Van Jacobson Compressed TCP/IP 使用の設定 88
11.11.2 PP 側 IP アドレスのネゴシエーションの設定 88
11.11.3 パラメータ ipcp-restart の設定 88
11.11.4 パラメータ ipcp-max-terminate の設定 89
11.11.5 パラメータ ipcp-max-configure の設定 89
11.11.6 パラメータ ipcp-max-failure の設定 89
11.11.7 IPCP の MS 拡張オプションを使うか否かの設定 89
11.11.8 WINS サーバの IP アドレスの設定 90
11.12IPXCP 関連の設定 90
11.12.1 パラメータ ipxcp-restart の設定 90
11.12.2 パラメータ ipxcp-max-terminate の設定 90
11.12.3 パラメータ ipxcp-max-configure の設定 90
11.12.4 パラメータ ipxcp-max-failure の設定 91
11.13BCP 関連の設定 91
11.13.1 LAN Identification 使用の設定 91
11.13.2 Tinygram compression 使用の設定 91
11.13.3 パラメータ bcp-restart の設定 91

11.13.4 パラメータ bcp-max-terminate の設定 92
11.13.5 パラメータ bcp-max-configure の設定 92
11.13.6 パラメータ bcp-max-failure の設定 92
11.13.7 パラメータ mscbcp-restart の設定 92
11.13.8 パラメータ mscbcp-maxretry の設定 93
11.14CCP 関連の設定 93
11.14.1 全パケットの圧縮タイプの設定 93
11.14.2 パラメータ ccp-restart の設定 93
11.14.3 パラメータ ccp-max-terminate の設定 93
11.14.4 パラメータ ccp-max-configure の設定 94
11.14.5 パラメータ ccp-max-failure の設定 94
11.15MP 関連の設定 94
11.15.1 MP を使用するか否かの設定 94
11.15.2 MP の制御方法の設定 94
11.15.3 MP のための負荷閾値の設定 95
11.15.4 MP の最大リンク数の設定 95
11.15.5 MP の最小リンク数の設定 95
11.15.6 MP のための負荷計測間隔の設定 96
11.15.7 MP のパケットを分割するか否かの設定 96
11.16BACP 関連の設定 96
11.16.1 パラメータ bacp-restart の設定 96
11.16.2 パラメータ bacp-max-terminate の設定 96
11.16.3 パラメータ bacp-max-configure の設定 97
11.16.4 パラメータ bacp-max-failure の設定 97
11.16.5 パラメータ bap-restart の設定 97
11.16.6 パラメータ bap-max-retry の設定 97

12 DHCP の設定 **98**

12.1 DHCP の動作の設定 98
12.2 DHCP スコープの定義 99
12.3 DHCP スコープの削除 99
12.4 DHCP 予約アドレスの設定 100
12.5 DHCP 予約アドレスの解除 100
12.6 DHCP サーバの指定の設定 100
12.7 DHCP サーバの選択方法の設定 101
12.8 DHCP BOOTREQUEST パケットの中継基準の設定 101
12.9 DHCP オプションの設定 102
12.10リースする IP アドレスの重複をチェックするか否かの設定 103

13 SNMP の設定 104

13.1 読み出し専用のコミュニティ名の設定 . . . 104
13.2 読み書き可能なコミュニティ名の設定 . . . 104
13.3 認証失敗時 (authenticationFailure) にトラップを送信するか否かの設定 . . . 104
13.4 SNMP によるアクセスを許可するホストの設定 . . . 105
13.5 sysContact の設定 . . . 105
13.6 sysLocation の設定 . . . 105
13.7 sysName の設定 . . . 105
13.8 送信トラップのコミュニティ名の設定 . . . 106
13.9 トラップの受信ホストの設定 . . . 106

14 ICMP の設定 107

14.1 ICMP Echo Reply を送信するか否かの設定 . . . 107
14.2 ICMP Mask Reply を送信するか否かの設定 . . . 107
14.3 ICMP Parameter Problem を送信するか否かの設定 . . . 107
14.4 ICMP Redirect を送信するか否かの設定 . . . 108
14.5 ICMP Redirect 受信時の処理の設定 . . . 108
14.6 ICMP Time Exceeded を送信するか否かの設定 . . . 108
14.7 ICMP Timestamp Reply を送信するか否かの設定 . . . 108
14.8 ICMP Destination Unreachable を送信するか否かの設定 . . . 109
14.9 受信した ICMP のログを記録するか否かの設定 . . . 109

15 RADIUS の設定 110

15.1 RADIUS サーバの指定 . . . 110
15.2 RADIUS 認証サーバの指定 . . . 110
15.3 RADIUS 認証サーバの UDP ポートの設定 . . . 110
15.4 RADIUS アカウントサーバの指定 . . . 111
15.5 RADIUS アカウントサーバの UDP ポートの設定 . . . 111
15.6 RADIUS シークレットの設定 . . . 111
15.7 RADIUS 再送信パラメータの設定 . . . 111
15.8 RADIUS による認証を使用するか否かの設定 . . . 112
15.9 RADIUS によるアカウントを使用するか否かの設定 . . . 112

16 NAT の設定 113

16.1 NAT を使うか否かの設定 . . . 113
16.2 IP Masquerade を使用するか否かの設定 . . . 113
16.3 IP Masquerade 使用時に rlogin,rcp と ssh を許可するか否かの設定 . . . 114
16.4 静的 IP Masquerade エントリの設定 . . . 114
16.5 静的 IP Masquerade エントリの削除 . . . 115

16.6 NAT のグローバル IP アドレスの設定 115
16.7 NAT の対象とするプライベートアドレスの範囲の設定 115
16.8 NAT の IP アドレスマップの消去タイマの設定 116
16.9 動的に生成された NAT のグローバルアドレスとプライベートアドレスの組の消去 . . 116
16.10NAT 関連の設定の表示 116
16.11NAT のグローバルアドレスとプライベートアドレスのマップの表示 117

17 NAT ディスクリプタ機能 118
17.1 LAN インタフェースへの NAT ディスクリプタ適用の設定 118
17.2 PP インタフェースへの NAT ディスクリプタ適用の設定 118
17.3 トンネルインタフェースへの NAT ディスクリプタ適用の設定 119
17.4 NAT ディスクリプタの動作タイプの設定 119
17.5 NAT 処理の外側 IP アドレスの設定 120
17.6 NAT 処理の内側 IP アドレスの設定 120
17.7 静的 NAT エントリの設定 121
17.8 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 121
17.9 静的 IP マスカレードエントリの設定 121
17.10NAT の IP アドレスマップの消去タイマの設定 122
17.11NAT ディスクリプタの削除 122
17.12静的 NAT エントリの削除 122
17.13静的 IP マスカレードエントリの削除 122
17.14設定した NAT ディスクリプタの設定状態表示 122
17.15動的 NAT ディスクリプタのアドレスマップの表示 123
17.16動作中の NAT ディスクリプタの適用リストの表示 123
17.17LAN 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 123
17.18PP 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 123
17.19トンネルインタフェースの NAT ディスクリプタのアドレスマップの表示 123
17.20NAT アドレステーブルのクリア 124
17.21LAN インタフェースの NAT アドレステーブルのクリア 124
17.22PP インタフェースの NAT アドレステーブルのクリア 124
17.23トンネルインタフェースの NAT アドレステーブルのクリア 124

18 DNS の設定 125
18.1 DNS サーバの IP アドレスの設定 125
18.2 DNS サーバを通知してもらう相手先情報番号の設定 125
18.3 DNS ドメイン名の設定 126
18.4 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 126
18.5 DHCP/IPCP MS 拡張で DNS サーバを通知する順序の設定 127
18.6 SYSLOG 表示で DNS により名前解決するか否かの設定 127

18.7 静的 DNS レコードの登録 128
18.8 静的 DNS レコードの削除 129
18.9 静的 DNS レコードの表示 129

19 アナログ通信機能の設定 130

19.1 キー操作とコンソールコマンドの対応 131
19.2 アナログポートを使うか否かの設定 132
19.3 アナログポートの ISDN 番号の設定 132
19.4 アナログポートに接続する機器の指定 133
19.5 アナログポートの発信者番号を通知するか否かの設定 133
19.6 相手先番号による即時発信を許可するか否かの設定 134
19.7 グローバル着信を許可するか否かの設定 134
19.8 アナログポートでの識別着信をするか否かの設定 135
19.9 識別着信リストの登録 135
19.10識別着信リストの削除 136
19.11サブアドレス無し着信を許可するか否かの設定 136
19.12異なる種類の通信機器からの着信を許可するか否かの設定 137
19.13話中着信を許可するか否かの設定 137
19.14優先着信機能の設定 138
19.15着信ベルリストの登録 138
19.16着信ベルリストの削除 139
19.17ダイヤル桁間タイマの設定 139
19.18フッキングを判定する時間の設定 139
19.19フッキング後にキー操作を受け入れる時間の設定 140
19.20フッキング及びオンフック検出を無効と判断する時間の設定 140
19.21フレックスホン機能の使用パターンの設定 141
19.22着信転送先アドレスの設定 141
19.23着信転送トーキの設定 142
19.24着信転送を起動するタイミングの設定 142
19.25着信転送が拒否された時の動作の設定 143
19.26送話 PAD の設定 143
19.27受話 PAD の設定 144
19.28ナンバー・ディスプレイを使用するか否かの設定 144
19.29MP 時に電話発着信のために 1B チャネルに落すか否かの設定 145
19.30TEL ポートへの切断信号の送出の設定 145
19.31DTMF 検出レベルの設定 146
19.32受信 DTMF 信号の最小時間の設定 146
19.33i ・ナンバーサービスのポート番号の設定 147

20 メール着信確認機能の設定 **148**

20.1 メールサーバの設定 148
20.2 メールチェックの実行 148
20.3 メールチェックの実行を許可するか否かの設定 149
20.4 メールチェックによる LED の消灯 149
20.5 メールチェックの状態表示 149
20.6 メールチェックタイムアウトの設定 149

21 RVS-COM 対応関連の設定 **150**

21.1 SERIAL ポートでの送話 PAD の設定 150
21.2 SERIAL ポートでの受話 PAD の設定 150
21.3 SERIAL ポートでの着信を許可するか否かの設定 150
21.4 アナログ機器を呼び出す時間の設定 151
21.5 RVS-COM に関する設定の表示 151

22 優先制御 / 帯域制御 **152**

22.1 インタフェース速度の設定 152
22.2 クラス分けのためのフィルタ設定 153
22.3 クラス分けフィルタの削除 156
22.4 キューイングアルゴリズムタイプの選択 156
22.5 デフォルトクラスの設定 156
22.6 クラス分けフィルタの適用 157
22.7 クラスの属性の設定 158
22.8 クラスの属性の削除 159
22.9 クラス毎のキュー長の設定 159
22.10キュークラスフィルタの表示 159
22.11インタフェース毎のキューの表示 160

23 TA 機能 **161**

23.1 コンソールコマンド 161
23.1.1 AT コマンドモードへの移行 161
23.1.2 コンソール速度の設定 161
23.1.3 デフォルトのコンソールのタイプの指定 161
23.1.4 擬似 LAN 接続を許可するか否かの設定 162
23.2 AT コマンド 162
23.2.1 S レジスタの詳細 171
23.2.2 リザルトコード詳細 172

24 操作 **173**

24.1 相手先情報番号の選択 . . . 173
24.2 トンネルインタフェース番号の選択 . . . 173
24.3 設定に関する操作 . . . 173
24.3.1 管理ユーザへの移行 . . . 173
24.3.2 設定内容の保存 . . . 174
24.3.3 終了 . . . 174
24.3.4 相手先の初期化 . . . 174
24.3.5 トンネルインタフェースの初期化 . . . 174
24.3.6 相手先毎の設定の複写 . . . 175
24.3.7 設定の初期化 . . . 175
24.3.8 遠隔地のルータの設定 . . . 175
24.3.9 遠隔地のルータからの設定に対する制限 . . . 176
24.4 動的情報のクリア操作 . . . 176
24.4.1 ARP テーブルのクリア . . . 176
24.4.2 IP の動的経路情報のクリア . . . 176
24.4.3 IPX の動的経路情報のクリア . . . 176
24.4.4 IPX の動的 SAP 情報のクリア . . . 177
24.4.5 ブリッジのラーニング情報のクリア . . . 177
24.4.6 ログのクリア . . . 177
24.4.7 アカウントのクリア . . . 177
24.4.8 相手先毎のアカウントの消去 . . . 177
24.4.9 アナログポートに関するアカウントのクリア . . . 178
24.4.10 InARP のクリア . . . 178
24.4.11 DNS キャッシュのクリア . . . 178
24.4.12 PRI のステイタス情報のクリア . . . 178
24.5 スケジュール . . . 179
24.5.1 スケジュールの設定 . . . 179
24.5.2 スケジュールの削除 . . . 180
24.5.3 スケジュールの確認 . . . 180
24.6 その他の操作 . . . 181
24.6.1 相手先の使用許可の設定 . . . 181
24.6.2 相手先の使用不許可の設定 . . . 181
24.6.3 BRI インタフェースの使用許可の設定 . . . 181
24.6.4 BRI インタフェースの使用不許可の設定 . . . 181
24.6.5 トンネルインタフェースの使用許可の設定 . . . 182
24.6.6 トンネルインタフェースの使用不許可の設定 . . . 182
24.6.7 再起動 . . . 182

24.6.8 発信 . . . 182
24.6.9 切断 . . . 183
24.6.10 ping . . . 183
24.6.11 traceroute . . . 183
24.6.12 リモートホストによる時計の設定 . . . 184
24.6.13 NTP による時計の設定 . . . 184
24.6.14 telnet . . . 185
24.6.15 PRI のループバックの実行 . . . 186
24.6.16 PRI のループバック待ち受けの設定 . . . 187

25 設定の表示 188

25.1 機器設定の表示 . . . 188
25.1.1 機器設定の表示 . . . 188
25.1.2 SYSLOG 関連の表示 . . . 188
25.1.3 TFTP 関連の表示 . . . 188
25.1.4 すべての設定内容の表示 . . . 189
25.1.5 指定した PP の設定内容の表示 . . . 189
25.1.6 PP 毎の設定内容の表示 . . . 189
25.2 相手先一覧の表示 . . . 190
25.2.1 相手先一覧の表示 . . . 190
25.3 ISDN 関連の表示 . . . 190
25.3.1 自分側設定の表示 . . . 190
25.3.2 相手側設定の表示 . . . 191
25.4 フレームリレー関連の表示 . . . 192
25.4.1 PP 側フレームリレー設定の表示 . . . 192
25.4.2 DLCI の表示 . . . 192
25.5 IP 関連の表示 . . . 192
25.5.1 IP パケットのフィルタの一覧表示 . . . 192
25.5.2 IP パケットのフィルタの表示 . . . 192
25.5.3 LAN 側 IP 設定の表示 . . . 193
25.5.4 IP パケットの TOS フィールドの書き換え設定の表示 . . . 193
25.5.5 PP 側 IP 設定の表示 . . . 194
25.6 IPX 関連の表示 . . . 194
25.6.1 IPX パケットのフィルタの一覧表示 . . . 194
25.6.2 IPX パケットのフィルタの表示 . . . 195
25.6.3 LAN 側 IPX 設定の表示 . . . 195
25.6.4 PP 側 IPX 設定の表示 . . . 196
25.7 ブリッジ関連の表示 . . . 196

25.7.1 ブリッジのフィルタの一覧表示 196
25.7.2 ブリッジのフィルタの表示 197
25.7.3 LAN 側ブリッジ設定の表示 197
25.7.4 PP 側ブリッジ設定の表示 197
25.8 PPP の設定の表示 198
25.8.1 認証関連の設定の表示 198
25.8.2 LCP 関連の設定の表示 198
25.8.3 PAP 関連の設定の表示 199
25.8.4 CHAP 関連の設定の表示 199
25.8.5 IPCP 関連の設定の表示 200
25.8.6 IPXCP 関連の設定の表示 200
25.8.7 BCP 関連の設定の表示 201
25.8.8 MSCBCP 関連の設定の表示 201
25.8.9 BACP 関連の設定の表示 202
25.8.10 CCP 関連の設定の表示 202
25.8.11 MP 関連の設定の表示 203
25.9 DHCP スコープの表示 204
25.10DHCP サーバの状態の表示 204
25.11SNMP 関連の設定の表示 205
25.12ICMP 関連の設定の表示 205
25.13RADIUS 関連の設定の表示 205
25.14DNS 関連の設定の表示 206
25.15WINS 関連の設定の表示 206
25.16アナログ関係の設定の表示 206

26 状態の表示 207

26.1 ARP テーブルの表示 207
26.2 LAN 側の状態の表示 207
26.3 PP 側の状態の表示 207
26.4 PRI の状態の表示 208
26.5 各相手先の状態の表示 208
26.6 IP の経路情報テーブルの表示 209
26.7 IPX の経路情報テーブルの表示 209
26.8 SAP テーブルの表示 209
26.9 IPXWAN の状態の表示 209
26.10ブリッジのラーニング情報の表示 209
26.11アナログ関係の状態の表示 210
26.12IPsec の SA の状態の表示 210

27 ロギング **211**

27.1 ログの表示 211

27.2 アカウントの表示 211

27.3 相手先毎のアカウントの表示 212

27.4 アナログ関係のアカウントの表示 212

索 引

account threshold, 12
administrator, 173
administrator password, 3, 131
analog arrive another-device permit, 131, 137
analog arrive dte permit, 131, 150
analog arrive dte timer, 131, 151
analog arrive global permit, 131, 134
analog arrive inumber-port, 131, 147
analog arrive number display, 131, 144
analog arrive prior-port, 131, 138
analog arrive restrict, 131, 135
analog arrive restrict list add, 131, 135
analog arrive restrict list delete, 131, 136
analog arrive ring-while-talking permit, 2, 131, 137
analog arrive ringer-type list add, 131, 138
analog arrive ringer-type list delete, 131, 139
analog arrive without-subaddress permit, 131, 136
analog device type, 131, 133
analog disc-signal, 131, 145
analog dtmf level, 131, 146
analog dtmf minimum time, 146
analog hooking inhibit timer, 131, 140
analog hooking timer, 131, 139
analog hooking wait timer, 131, 140
analog local address, 131, 132
analog local address notice, 131, 133
analog mp prior, 131, 145
analog pad receive, 131, 144
analog pad receive dte, 131, 150
analog pad send, 131, 143
analog pad send dte, 131, 150
analog rapid call, 131, 134
analog supplementary-service, 131, 141
analog supplementary-service call-deflection address, 131, 141
analog supplementary-service call-deflection reject, 131, 143
analog supplementary-service call-deflection ringer, 131, 142
analog supplementary-service call-deflection talkie, 131, 142
analog use, 131, 132
analog wait dial timer, 131, 139

bri disable, 181
bri enable, 181
bri line, 11
bri terminator, 13
bridge filter, 77
bridge filter delete, 77
bridge forwarding, 78
bridge group, 76, 78
bridge lan filter, 79
bridge lan learning add, 79
bridge lan learning delete, 79
bridge learning, 78
bridge learning expire, 78
bridge pp filter, 80
bridge pp learning add, 80
bridge pp learning delete, 80
bridge use, 76

clear account, 177
clear analog account, 131, 178
clear arp, 176
clear bridge learning, 177
clear dns cache, 178
clear inarp, 178
clear ip dynamic routing, 176
clear ipx dynamic routing, 176
clear ipx dynamic sap, 177
clear log, 177
clear nat descriptor dynamic, 124
clear nat descriptor interface dynamic lan, 124
clear nat descriptor interface dynamic pp, 124
clear nat descriptor interface dynamic tunnel, 124
clear nat dynamic, 116
clear pp account, 177
clear pri status, 178
cold start, 175
connect, 182
console character, 5
console columns, 6
console info, 6
console lines, 6
console prompt, 6

date, 5
dhcp delete scope, 99, 102
dhcp duplicate check, 103
dhcp relay select, 98, 101

dhcp relay server, 98, 100
dhcp relay threshold, 101
dhcp scope, 98, 99
dhcp scope bind, 98, 100
dhcp scope option, 102
dhcp scope unbind, 98, 100
dhcp service, 98
disconnect, 183
dns domain, 125, 126
dns notice order, 127
dns private address spoof, 126
dns server, 98, 102, 125, 127
dns server pp, 125
dns static, 128
dns static delete, 129
dns syslog resolv, 127

exit, 174

fr backup, 26
fr cir, 27
fr compression use, 24, 26
fr congestion control, 27
fr de, 28
fr dlci, 24, 25
fr inarp, 24, 26
fr lmi, 24, 25
fr pp dequeue type, 28

help, 3

ip filter, 31
ip filter delete, 33
ip filter directed-broadcast, 33
ip filter source-route, 33
ip host, 128
ip host delete, 129
ip icmp echo-reply send, 107
ip icmp log, 109
ip icmp mask-reply send, 107
ip icmp parameter-problem send, 107
ip icmp redirect receive, 2, 108
ip icmp redirect send, 108
ip icmp time-exceeded send, 108
ip icmp timestamp-reply send, 108
ip icmp unreachable send, 109
ip lan address, 35, 120, 131
ip lan broadcast, 37
ip lan mtu, 42
ip lan nat descriptor, 118
ip lan netmask, 36, 131
ip lan proxyarp, 41
ip lan rip auth key, 40
ip lan rip auth type , 40
ip lan rip filter, 39
ip lan rip listen, 39
ip lan route add, 37
ip lan route delete, 38
ip lan routing protocol, 38
ip lan secondary address, 36, 120
ip lan secure filter, 41
ip pp hide static route, 49
ip pp hold routing, 46
ip pp local address, 42
ip pp mtu, 50
ip pp nat descriptor, 118
ip pp netmask, 44
ip pp remote address, 43
ip pp remote address pool, 43
ip pp rip auth key, 48
ip pp rip auth type, 48
ip pp rip connect interval, 46
ip pp rip connect send, 45
ip pp rip disconnect interval, 46
ip pp rip disconnect send, 46
ip pp rip filter, 47
ip pp rip hop, 47
ip pp rip listen, 47
ip pp route add, 44
ip pp route delete, 45
ip pp routing protocol, 45
ip pp secure filter, 49
ip routing, 31
ip tos supersede, 34
ip tunnel nat descriptor, 118
ip tunnel route add, 51, 60
ip tunnel route delete, 51, 60
ip tunnel secure filter, 61
ip tunnnel nat descriptor, 119
ipsec auto refresh, 51, 59
ipsec ike duration ipsec-sa, 51, 58
ipsec ike duration isakmp-sa, 51, 59
ipsec ike encryption, 53
ipsec ike group, 54
ipsec ike hash, 54
ipsec ike local address, 53

ipsec ike local id, 55
ipsec ike log, 55
ipsec ike payload type, 56
ipsec ike pfs, 56
ipsec ike remote address, 51, 52
ipsec ike remote id, 56
ipsec ike retry, 53
ipsec ike send info, 57
ipsec pre-shared-key, 51, 52
ipsec refresh sa, 51, 59
ipsec sa delete, 51, 59
ipsec sa policy, 51, 58
ipsec sa policy delete, 58
ipsec transport, 51, 62
ipsec transport delete, 51, 62
ipsec tunnel, 60
ipx filter, 63
ipx filter delete, 65
ipx lan frame type, 67
ipx lan network, 67
ipx lan ripsap broadcast, 68
ipx lan route add, 68
ipx lan route delete, 68
ipx lan secure filter, 69
ipx pp ipxwan primnet, 73
ipx pp ipxwan retry, 72
ipx pp ipxwan use, 72
ipx pp network, 70
ipx pp ripsap connect interval, 71
ipx pp ripsap connect send, 71
ipx pp ripsap disconnect interval, 72
ipx pp ripsap disconnect send, 71
ipx pp ripsap hold, 2, 72
ipx pp route add, 70
ipx pp route delete, 70
ipx pp routing, 69
ipx pp secure filter, 75
ipx pp serialization filter, 74
ipx pp spx keepalive proxy, 73
ipx pp spx keepalive timer, 74
ipx pp watchdog interval, 73
ipx pp watchdog proxy, 73
ipx routing, 63
ipx sap add, 65
ipx sap delete, 66
ipx sap response, 66
isdn arrive permit, 17
isdn auto connect, 16
isdn auto disconnect, 16
isdn call block time, 18
isdn call permit, 17
isdn call prohibit auth-error count, 23
isdn call prohibit time, 18
isdn callback mscbcp user-specify, 19
isdn callback permit, 17
isdn callback permit type, 19
isdn callback request, 16
isdn callback request type, 19
isdn callback response time, 20
isdn callback wait time, 20
isdn disconnect input time, 21
isdn disconnect interval time, 22
isdn disconnect output time, 21
isdn disconnect policy, 20
isdn disconnect time, 21
isdn fast disconnect time, 22
isdn forced disconnect time, 23
isdn local address, 11
isdn piafs arrive, 14
isdn piafs call, 14
isdn remote address, 15
isdn remote call order, 15

lan queue class filter list, 157
lan queue class property, 158
lan queue class property clear, 159
lan queue default class, 156
lan queue length, 159
lan queue type, 152, 156
lan speed, 152, 158
leased backup, 12, 26
leased backup recovery time, 13
leased keepalive down, 86
leased keepalive interval, 86
leased keepalive log, 86
leased keepalive use, 85
less config, 189
less config pp, 189
less log, 211
login password, 3, 131
login timer, 4

mail-check go, 148
mail-check led off, 149
mail-check prohibit, 149

mail-check server, 148
mail-check timeout, 149

nat address global, 115, 120
nat address private, 115, 120
nat descriptor address inner, 118, 120, 121
nat descriptor address outer, 118, 120, 121
nat descriptor delete, 122
nat descriptor masquerade rlogin, 121
nat descriptor masquerade static, 121
nat descriptor masquerade static delete, 122
nat descriptor static, 121
nat descriptor static delete, 122
nat descriptor timer, 122
nat descriptor type, 119
nat masquerade, 113
nat masquerade rlogin, 114
nat masquerade static, 114
nat masquerade static delete, 115
nat timer, 116
nat use, 113
ntpdate, 125, 184

packetdump lan, 9
packetdump pp, 9
ping, 125, 183
pp account threshold, 23
pp auth accept, 82
pp auth clear myname, 82
pp auth delete username, 82
pp auth multi connect prohibit, 83
pp auth myname, 82
pp auth request, 81
pp auth username, 81
pp bind bri, 13
pp bind pri, 29, 30, 175
pp copy, 175
pp default, 174
pp disable, 29, 181
pp enable, 181
pp encapsulation, 24, 25
pp line, 11
pp queue class filter list, 157
pp queue class property, 158
pp queue class property clear, 159
pp queue default class, 156, 157
pp queue length, 159
pp queue type, 152, 156
pp select, 173
pp speed, 152, 158
ppp bacp maxconfigure, 97
ppp bacp maxfailure, 97
ppp bacp maxterminate, 96
ppp bacp restart, 96
ppp bap maxretry, 97
ppp bap restart, 97
ppp bcp lanid, 91
ppp bcp maxconfigure, 92
ppp bcp maxfailure, 92
ppp bcp maxterminate, 92
ppp bcp restart, 91
ppp bcp tinycomp, 91
ppp ccp maxconfigure, 94
ppp ccp maxfailure, 94
ppp ccp maxterminate, 93
ppp ccp restart, 93
ppp ccp type, 93
ppp chap maxchallenge, 2, 87
ppp chap restart, 87
ppp ipcp ipaddress, 88
ppp ipcp maxconfigure, 89
ppp ipcp maxfailure, 89
ppp ipcp maxterminate, 89
ppp ipcp msext, 89, 125
ppp ipcp restart, 88
ppp ipcp vjc, 88
ppp ipxcp maxconfigure, 90
ppp ipxcp maxfailure, 91
ppp ipxcp maxterminate, 90
ppp ipxcp restart, 90
ppp lcp acfc, 83
ppp lcp magicnumber, 83
ppp lcp maxconfigure, 85
ppp lcp maxfailure, 85
ppp lcp maxterminate, 85
ppp lcp mru, 84
ppp lcp pfc, 84
ppp lcp restart, 84
ppp mp control, 94
ppp mp divide, 96
ppp mp load threshold, 95
ppp mp maxlink, 95
ppp mp minlink, 95
ppp mp timer, 96
ppp mp use, 94

ppp mscbcp maxretry, 93
ppp mscbcp restart, 92
ppp pap maxauthreq, 2, 87
ppp pap restart, 87
pri leased channel, 29, 30, 175
pri leased delete channel, 30
pri line, 29
pri loopback active, 29, 186
pri loopback passive, 29, 187

queue class filter, 152, 153, 157
queue class filter delete, 156
queue class filter list, 155
quit, 174

radius account, 112
radius account port, 111
radius account server, 111
radius auth, 112
radius auth port, 110
radius auth server, 110
radius retry, 111
radius secret, 111
radius server, 110, 111
rdate, 125, 184
remote setup, 175
remote setup accept, 176
restart, 182

save, 174, 186, 187
schedule at, 16, 179
schedule delete, 180
security class, 4
serial default, 4, 161, 174
serial pseudo-lan, 162
serial speed, 161, 174
serial ta, 161
show account, 211
show analog account, 212
show analog config, 206
show analog config dte, 151
show arp, 207
show auth, 198
show bridge filter, 197
show bridge filter list, 196
show bridge lan, 197
show bridge learning, 209
show bridge pp, 197
show command, 2, 3
show config, 52, 189
show config pp, 189
show dhcp, 98, 204
show dhcp scope, 204
show dhcp status, 98, 204
show dlci, 24, 192
show dns, 206
show dns static, 129
show environment, 188
show fr, 24, 192
show ip filter, 192
show ip filter list, 192
show ip host, 129
show ip icmp, 205
show ip lan, 193
show ip pp, 194
show ip route, 209
show ip tos supersede, 34, 193
show ipsec sa, 51, 59, 210
show ipx filter, 195
show ipx filter list, 194
show ipx ipxwan, 209
show ipx lan, 195
show ipx pp, 196
show ipx route, 209
show ipx sap, 209
show isdn local, 190
show isdn remote, 191
show lan queue, 152, 160
show log, 211
show mail-check status, 149
show nat address, 117
show nat config, 116
show nat descriptor address, 123
show nat descriptor config, 122
show nat descriptor interface address lan, 123
show nat descriptor interface address pp, 123
show nat descriptor interface address tunnnel, 123
show nat descriptor interface bind, 123
show pp account, 23, 212
show pp config, 189
show pp queue, 152, 160
show ppp bacp, 202
show ppp bcp, 201
show ppp ccp, 202
show ppp chap, 199

show ppp ipcp, 200
show ppp ipxcp, 200
show ppp lcp, 198
show ppp mp, 203
show ppp mscbcp, 201
show ppp pap, 199
show queue class filter, 152, 159
show radius, 205
show remote list, 190
show schedule, 180
show snmp, 205
show status analog, 210
show status bri, 207
show status lan, 207
show status pp, 208
show status pri, 29, 208
show syslog, 188
show tftp, 188
show wins, 206
snmp community read-only, 104
snmp community read-write, 104
snmp enableauthentraps, 104
snmp host, 105
snmp syscontact, 105
snmp syslocation, 105
snmp sysname, 105
snmp trap community, 106
snmp trap host, 106
syslog debug, 8
syslog facility, 7
syslog host, 7
syslog info, 8
syslog notice, 7
syslog srcport, 8
sysname, 3

telnet, 125, 185
tftp host, 10
time, 5
timezone, 5
traceroute, 125, 183
tunnel default, 174
tunnel disable, 51, 182
tunnel enable, 51, 182
tunnel select, 51, 173

wins server, 90, 102

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 **RT200i**、**RT140p**、**RT140f**、**RT140i**、**RT140e**、**RT103i** 及び **RTA50i** プログラムの **Rev.2.02.44**、**Rev.3.00.44**、**Rev.3.01.13**、**Rev.3.03.35**、**Rev.4.00.22** 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プログラムや、マニュアル類及び差分については以下に示す anonymous FTP サーバにある情報を参照してください。

ftp.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。

一つ一つのコマンドは次の項目の組合せで説明します。

項目	説明
[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。本書の文中では小文字に統一してあります。コマンドの名称部分とキーワードは太字 (**Bold face**) で、パラメータ部分は斜体 (*italic face*) で表します。括弧 ([]) で囲まれたパラメータは省略可能であることを表します。
[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]	このコマンドを使用する場合に特に注意すべき事柄を述べます。
[デフォルト値]	このコマンドのデフォルト値を示します。
[設定例]	このコマンドの具体例を示します。

1.3 モデルによる違いについて

YAMAHA リモートルータのコンソールの使用方法は基本的にどのモデルも同じですが、パラメータの範囲や使えるコマンド等に若干の違いがあります。

1. 相手先情報番号として使える範囲は **RT200i**、**RT140p**、**RT140i**、**RT140e** では 1–100 までであり、**RT103i** と **RTA50i** では 1–30 までです。

モデル	相手先情報番号の範囲
RT200i	1–100
RT140p, RT140f, RT140i, RT140e	1–100
RT103i	1–30
RTA50i	1–30

2. BRI 番号として使える範囲は **RT200i** では 1–4(4 ポートモデル) または 1–8(8 ポートモデル) であり、**RT140p**、**RT140f**、**RT140i** では 1 と 2 です。

モデル	BRI 番号の範囲
RT200i(4 ポートモデル)	1–4
RT200i(8 ポートモデル)	1–8
RT140p, RT140f, RT140i	1, 2
RT140e	1

3. PP 番号のキーワード **leased** を指定できるのは **RT103i** 及び **RTA50i** だけです。
4. モデルにより入力形式のパラメータ指定が異なるコマンドについては、本コマンドリファレンスの [入力形式] 及び [ノート] に記載します。

5. モデルにより使用できるコマンドと使用できないコマンドがあります。使用できるかどうかは、お使いの YAMAHA リモートルータのコンソールから **show command** コマンドやヘルプ機能を使用することで確認してください。

機能名称	**RT200i**	**RT140p**	**RT140f**	**RT140i**	**RT140e**	**RT103i**	**RTA50i**
PIAFS	—	○	○	○	○	○	○
フレームリレー	○	○	○	○	○	○	—
PRI	—	○	—	—	—	—	—
IPsec	○	○	○	○	○	○	—
IPX	○	○	○	○	○	○	—
ブリッジ	○	○	○	○	○	○	—
SNMP	○	○	○	○	○	○	—
RADIUS	○	○	○	○	○	○	—
NAT	—	—	—	—	—	—	○
NAT ディスクリプタ機能	○	○	○	○	○	○	—
アナログ通信	—	—	—	—	—	—	○
メール着信確認機能	—	—	—	—	—	—	○
RVS-COM 対応	—	—	—	—	—	—	○
優先制御 / 帯域制御	○	○	○	○	○	○	—
TA 機能	—	—	—	—	—	—	○

1.4 デフォルト値の変更について

過去に変更されたデフォルト値とそのコマンドの一覧を以下に示します。リビジョンを変更する場合には注意してください。

1. **ipx pp ripsap hold** ... Rev.1.04.03 以降から **on**
2. **ip icmp redirect receive** ... Rev.1.05.05 以降から **off**
3. **analog arrive ring-while-talking permit** ... **RTA50i のみ** Rev.3.02.21 以降から **off**
4. **ppp pap maxauthreq** ... **RTA50i のみ** Rev.3.03.28 以降から 10
5. **ppp chap maxchallenge** ... **RTA50i のみ** Rev.3.03.28 以降から 10

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設定する。コマンド入力後、パスワードを問い合わせる。

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 8 文字以内で設定する。コマンド入力後、パスワードを問い合わせる。

3.3 ルータの名称の設定

[入力形式] **sysname** *name*

[パラメータ]
- *name* ... ルータの名称

[説明] MIB 変数 sysName を設定する。

[デフォルト値] 空文字列

3.4 セキュリティクラスの設定

[入力形式] **security class** *level forget telnet*

[パラメータ]

- *level*
  - **1** ... シリアルでも TELNET でも、遠隔地のルータからでもログインできる
  - **2** ... シリアルと TELNET からは設定できるが、遠隔地のルータからはログインできない
  - **3** ... シリアルからのみログインできる
- *forget*
  - **on** ... 設定したパスワードの代わりに w,lXlma 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。

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

3.5 ログインタイマの設定

[入力形式] **login timer** *time*

[パラメータ]

- *time*
  - 秒数 ... キー入力がない時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] キー入力がない時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。
RTA50i の場合、**serial default ta** に設定されていると、このコマンドで設定した時間後に AT コマンドモードへ復帰する。

[デフォルト値] 300

3.6 タイムゾーンの設定

[入力形式] **timezone** *timezone*

[パラメータ]
- *timezone*
  - −12:00 ~ +11:59 ... 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)

[説明] タイムゾーンを設定する。

[デフォルト値] **jst**

3.7 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。

3.8 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。

3.9 コンソールの言語とコードの設定

[入力形式] **console character** *code*

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

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

[デフォルト値] **sjis**

3.10 コンソールの表示文字数の設定

[入力形式] **console columns** *col*

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

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

[デフォルト値] 80

3.11 コンソールの表示行数の設定

[入力形式] **console lines** *lines*

[パラメータ] • *lines* ... コンソールの表示行数
  ◦ 10..100 の整数
  ◦ **infinity** ... スクロールを止めない

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

[デフォルト値] 24

3.12 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*

[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。

[デフォルト値] **off**

3.13 コンソールのプロンプト表示の設定

[入力形式] **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

3.14 SYSLOG を受けるホストの IP アドレスの設定

[入力形式] **syslog host** *host*

[パラメータ]
- *host*
  - ip_address ... SYSLOG を受けるホストの IP アドレス
  - **clear** ... ログを SYSLOG でレポートしない

[説明] SYSLOG を受けるホストの IP アドレスを設定する。

[ノート] **syslog debug on** にすると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] **clear**

3.15 SYSLOG ファシリティの設定

[入力形式] **syslog facility** *facility*

[パラメータ]
- *facility*
  - 0..23
  - **user** ... 1
  - **local0** ~ **local7** ...16 ~ 23

[説明] SYSLOG のファシリティを設定する。

[デフォルト値] **user**

3.16 NOTICE タイプの SYSLOG を出力するか否かの設定

[入力形式] **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**

3.17 INFO タイプの SYSLOG を出力するか否かの設定

[入力形式] **syslog info** *info*

[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**

3.18 DEBUG タイプの SYSLOG を出力するか否かの設定

[入力形式] **syslog debug** *debug*

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

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

[ノート] **on** にすると大量のデバッグメッセージを送信するので、**syslog host** に設定するホスト側には十分なディスク領域を確保しておき、必要なデータが得られたらすぐに **off** にすること。

[デフォルト値] **off**

3.19 SYSLOG パケットの始点ポート番号の設定

[入力形式] **syslog srcport** *port*

[パラメータ]
- *port* ... ポート番号 (1..65535)

[説明] 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

3.20 LAN インタフェースパケットのダンプを SYSLOG へ出力するか否かの設定

[入力形式] 1. **packetdump lan** *[count]*
2. **packetdump lan1** *[count]*
3. **packetdump lan2** *[count]*

[パラメータ]
- *count*
  - パケット数 (1..21474836)
  - **off** ... 出力しない
  - **infinity** ... **off** にするまで出力する

[説明] LAN インタフェースを入出力するパケットのダンプ情報を DEBUG タイプの SYSLOG で出力するか否か設定する。

[デフォルト値] 100

3.21 PP インタフェースパケットのダンプを SYSLOG へ出力するか否かの設定

[入力形式] **packetdump pp** *[peer_number] [count]*

[パラメータ]
- *count*
  - パケット数 (1..21474836)
  - **off** ... 出力しない
  - **infinity** ... **off** にするまで出力する
- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は選択されている相手について表示する

[説明] 選択されている相手について、PP インタフェースを入出力するパケットのダンプ情報を DEBUG タイプの SYSLOG で出力するか否か設定する。

[デフォルト値] 100

3.22 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*

[パラメータ]
- *host*
  - ip_address ... TFTP によりアクセスできるホストの IP アドレス
  - **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** にすること。

[デフォルト値] **none**

4 ISDN 関連の設定

4.1 自分側の設定

4.1.1 PP 側の回線の種類の指定

[入力形式]

1. **pp line** *line [channels]* ... RT103i,RTA50i
2. **bri line** *bri line [channels]*

[パラメータ]

- *line*
  - **isdn** ... 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
- *bri* ... BRI 番号
- *channels*
  - **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] PP 側の回線を指定する。デフォルト以外に設定した場合には、必ず再起動すること。

[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時は *channels* を **1b** にする。

[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]

1. **isdn local address** *isdn_number*/*sub_address*
2. **isdn local address** *isdn_number*
3. **isdn local address** /*sub_address*
4. **isdn local address** /
5. **bri local address** *bri isdn_number*/*sub_address*
6. **bri local address** *bri isdn_number*
7. **bri local address** *bri* /*sub_address*
8. **bri local address** *bri* / ... RT200i, RT140p, RT140f, RT140i, RT140e

[パラメータ]

- *isdn_number* ... ISDN 番号
- *sub_address* ... ISDN サブアドレス (0x21 から 0x7e の ASCII 文字)
- *bri* ... BRI 番号

[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した方が良い。

4.1.3 課金額による発信制限の設定

[入力形式] **account threshold** *yen*

[パラメータ]
- *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。
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で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が良い。また、課金合計は **clear account** コマンドで 0 にリセットできるので、**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。

[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 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_number*

[パラメータ]
- *peer_number*
  - 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] 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を設定する。

[デフォルト値] **none**

4.1.5 バックアップからの復帰待ち時間の設定

[入力形式] **leased backup recovery time** *time*

[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ときに、すぐに復帰させるか、設定された時間だけ待ってから復帰するかを設定する。

[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**

4.1.6 終端抵抗の設定

[入力形式] **bri terminator** *bri terminate*

[パラメータ]
- *bri* ... BRI 番号
- *terminate*
  - **on** ... ON にする
  - **off** ... OFF にする

[説明] 指定した BRI 番号の終端抵抗を 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**

4.1.7 PP と BRI のバインドの設定

[入力形式] **pp bind bri** *bri [bri...]*

[パラメータ]
- *bri*
  - BRI 番号
  - **all** ... 全ての BRI 番号とバインドする
  - **none** ... どの BRI 番号ともバインドしない

[説明] 選択されている相手 にバインドされる BRI 番号を設定する。

[ノート] デフォルトではどの BRI 番号ともバインドされていないことに注意。

[デフォルト値] **none**

4.1.8 PIAFS の発信を許可するか否かの設定

[入力形式] **isdn piafs call** *call*

[パラメータ]
- *call*
  - **32k** ... PIAFS 32kbit/s で発信
  - **64k** ... PIAFS 64kbit/s で発信
  - **off** ... 同期 PPP で発信

[説明] PIAFS の発信を許可するか否かを設定する。

[ノート] PIAFS 64kbit/s の通信では特別なサブアドレスが使用されるため、ユーザが指定したサブアドレスは無視される。

[デフォルト値] **off**

4.1.9 PIAFS の着信を許可するか否かの設定

[入力形式] **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。

[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**

4.2 相手毎の設定

4.2.1 相手 ISDN 番号の設定

[入力形式]
1. **isdn remote address** *call_arrive isdn_number /sub_address [isdn_number_list]*
2. **isdn remote address** *call_arrive isdn_number [isdn_number_list]*

[パラメータ]
- *call_arrive*
  - **call** ... 発着信用
  - **arrive** ... 着信専用
- *isdn_number* ... ISDN 番号
- *sub_address* ... ISDN サブアドレス (0x21 から 0x7e の ASCII 文字)
- *isdn_number_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 (最大 8 つ)

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

[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 の場合は、**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は、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 の場合は、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*

[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*

[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。
RTA50i でのみ使用可能。また、**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 相手にコールバック要求を行なうか否かの設定

[入力形式] **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なうか否かを設定する。

[デフォルト値] **off**

4.2.6 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*

[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**

4.2.7 着信許可の設定

[入力形式] **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** とも **off** を設定した時は通信できない。

[デフォルト値] **on**

4.2.8 発信許可の設定

[入力形式] **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** とも **off** を設定した時は通信できない。

[デフォルト値] **on**

4.2.9 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*

[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時に、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

4.2.10 再発信抑制タイマの設定

[入力形式] **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時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。
RTA50i のかんたん設定ページからプロバイダ登録を行なった場合には、自動的に 15 秒にセットされる。

[デフォルト値] 0

4.2.11 コールバック要求タイプの設定

[入力形式] **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時のコールバック方式を設定する。

[デフォルト値] **yamaha**

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]*

[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*

[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時にはコールバックするために利用可能な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時には、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** *kind time*

[パラメータ]
- *kind*
  - **1b** ... 1B でコールバックする時
  - **2b** ... 2B もしくは any でコールバックする時
- *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] **1b** では 0 秒、**2b** では 5 秒

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*

[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*

[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**

4.2.17 切断タイマの設定 (ノーマル)

[入力形式] **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時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*

[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時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時、この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(21ページ) 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*

[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時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時、この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(21ページ) の [ノート] 参照。

[デフォルト値] 120

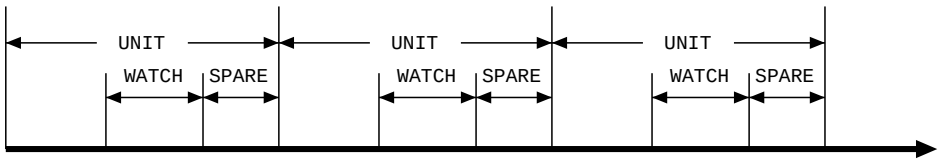
4.2.20 課金単位時間方式での課金単位時間と監視時間の設定

[入力形式] **isdn disconnect interval time** *unit watch spare*

[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のとおり :



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

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

4.2.21 切断タイマの設定 (ファスト)

[入力形式] **isdn fast disconnect time** *time*

[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別の宛先へのパケットが LAN 側から到着している時の切断タイマを設定する。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** の時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*

[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。

[ノート] 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。
RTA50i のかんたん設定ページからプロバイダ登録を行なった場合には、自動的に 32400 秒にセットされる。

[デフォルト値] **off**

4.2.23 相手先毎の課金額による発信制限の設定

[入力形式] **pp account threshold** *yen*

[パラメータ]
- *yen*
  - 課金額 ... 円 (10..21474836)
  - **off** ... 課金額による発信制限機能を使わない

[説明] 選択されている相手において、網から通知される課金累計額 (これは **show pp account** コマンドで表示される金額) 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。

[ノート] **RTA50i** のかんたん設定ページからプロバイダ登録を行なった場合には、自動的に 10,000 円にセットされる。

[デフォルト値] **off**

4.2.24 同じ相手に対して連続して認証に失敗できる回数の設定

[入力形式] **isdn call prohibit auth-error count** *count*

[パラメータ]
- *count*
  - **off** ... 連続した認証の失敗が発生しても発呼を続ける
  - 連続して認証に失敗できる回数 (1..21474836)

[説明] 連続して認証に失敗できる回数を設定する。ここで設定した回数だけ連続して認証に失敗したときには、その後は、同じ相手に対して発呼しない。なお、以下のコマンドを実行すると、再び発呼が可能となる。pp auth accept / pp auth requst / pp auth myname / pp auth username / pp auth clear myname / pp auth delete username

[デフォルト値] 5

5 フレームリレー関連の設定

YAMAHA リモートルータは、アクセス回線が 64kbit/s または 128kbit/s の高速ディジタル専用線である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。また、現在のフレームリレー関連の情報は **show fr** コマンドで確認することができます。

DLCI[2] はフレームリレーネットワークへアクセスする回線インタフェースのアドレスです。1 本の回線に複数の DLCI を取得すると、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** コマンドで行ないます。

自動取得の場合には PVC[3] 状態確認手順の LMI[4] により行なわれます。YAMAHA リモートルータは 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。ルータに設定されている 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。

YAMAHA リモートルータの特徴として、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 local address** コマンド) を設定せず、PP 側は 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 リモートルータどうしであれば、unnumbered でダイナミックルーティングが可能です。具体的な使用方法は設定例を参照してください。

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 1/5 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(*1) 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 **RT103i** で 16、**RT200i** と **RT140** シリーズでは 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。

また本機能を利用できる機種は **RT200i**、**RT140** シリーズと **RT103i** です。

同じフレームリレー回線にインタフェースを複数バインドする場合、1BRI モデルでは **leased** インタフェースが代表となり、それ以外のモデルでは最も若い PP インタフェースが代表となります。

pp encapsulation fr の設定は、関係する全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ときには、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ときには、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**

[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

コマンドで明示的に設定されていないときには、**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とき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ときは、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。

5.1 PP 側でのカプセル化の種類の設定

[入力形式] **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**

5.2 PP 側フレームリレーでの DLCI の設定

[入力形式] **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 の場合は PVC 状態確認手順により DLCI を自動取得する。

[ノート] **fr lmi off** でない場合にこのコマンドで 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
```

5.3 PP 側フレームリレーでの PVC 状態確認手順の設定

[入力形式] **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なう
  - **ansi** ... ANSI T1.617 Annex D に基づいて状態確認を行なう
  - **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 が無い場合に **fr lmi off** に設定しておかないと、回線ダウンとみなされるので注意。

[デフォルト値] **q933**

5.4 PP 側フレームリレーでの InARP 使用の設定

[入力形式] **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 local address** コマンドを参照。

[デフォルト値] **on**

5.5 フレームリレー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] **fr backup dlci**=*dlci_num peer_number*

[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)
- *peer_number* ... バックアップする相手先情報番号

[説明] 指定した DLCI がダウンした時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。

5.6 FR 圧縮機能の設定

[入力形式] **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**

5.7 DLCI ごとのパラメータの設定

[入力形式]

1. **fr cir dlci**=*dlci_num cir* [**slowstart-idle**= *idle*] [**bc**= *bc_size*] [**be**= *be_size*] [**s**= *step_count*]
2. **fr cir clear**

[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
- **clear** ... 設定を削除する

[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] **slowstart-idle** = 20
bc = **be** = 7000
s = *cir/bc_size/be_size* から計算される値

5.8 輻輳制御をするか否かの設定

[入力形式] **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] 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**

5.9 回線に対する送信順序方式の設定

[入力形式] **fr pp dequeue type** *type*

[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インタフェースがバインドされている時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インタフェースに対して順位を与え、順位の高い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全ての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インタフェースがより高い順位を持つものと定義する。1BRI モデルでは、これに加えて、LEASED が最も高い順位を持つものと定義する。

[デフォルト値] **round-robin**

5.10 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]
1. **fr de** *protocol* **filter dlci**=*dlci_num filter_number_list*
2. **fr de** *protocol* **filter dlci**=*dlci_num* **clear**

[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_number_list* ... フィルタの番号 (1..100)
- **clear** ... 設定を削除

[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_number_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-log**、**pass-nolog**、**restrict-log**、**restrict-nolog** のいずれかであれば DE ビットを立てる。**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時には DE ビットを立てない。

[デフォルト値] **clear**

6 PRI 関連の設定

YAMAHA リモートルータ **RT140p** は、一次群速度インタフェース (PRI:Primary Rate Interface) の専用回線に対応しています (オプションで回線交換に対応)。使用できる通信速度は 64kbit/s から 1.5Mbit/s であり、64kbit/s ごとの B チャネル単位で設定が可能です。

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

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

PRI の専用回線に対してループバック試験を行なうことができます。ループバック試験は、指定したデータを指定したループバックポイントで折り返して、送信データと折り返されたデータを比較して正常性の検証を行ないます。

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

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

RT140p においてループバックを実行するには、ディップスイッチを設定して行なう方法と、コンソールコマンドにより行なう方法があります。いずれの場合でも、通常の通信を **pp disable** コマンド等で停止させてから行なうようにします。ディップスイッチを使用した場合には、試験後にディップスイッチを元にもどしてから再起動が必要です。コンソールコマンド **pri loopback active** を使用する場合には、試験後に通信可能状態に復帰します。

タイムスロットループバックでは、相手側ルータは **pri loopback passive** コマンドで待ち受け状態にしておく必要があります。

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

6.1 PP 側の PRI 回線の種類の設定

[入力形式] **pri line** *pri line*

[パラメータ]
- *pri* ...PRI 番号 (1)
- *line*
  - **leased** ... 専用線

[説明] PP 側の PRI 回線の種類を設定する。デフォルト以外に設定した場合には、必ず再起動すること。

[デフォルト値] **leased**

6.2 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*

[パラメータ]
- *pri* ...PRI 番号 (1)
- *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
64k	1
128k	2
192k	3
256k	4
384k	6
512k	8
768k	12
1024k	16
1536k	24

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

[ノート] 同じ情報チャネルに対する設定を変更するには、予め **pri leased delete channel** コマンドの実行が必要。設定変更時には **restart** が必要。2 つ以上の情報チャネルの設定はできない。

6.3 情報チャネルとタイムスロットの削除

[入力形式] **pri leased delete channel** *pri/info*

[パラメータ]
- *pri* ...PRI 番号 (1)
- *info* ... 情報チャネル番号 (1..24)

[説明] 指定した PRI 回線に対して、指定した情報チャネルの設定を削除する。

6.4 PP と PRI のバインドの設定

[入力形式]
1. **pp bind pri** *pri/info*
2. **pp bind pri none**

[パラメータ]
- *pri* ...PRI 番号 (1)
- *info* ... 情報チャネル番号 (1..24)
- **none** ... どの PRI ともバインドしない

[説明] 選択されている相手にバインドされる PRI 情報チャネルを設定する。

[ノート] デフォルトではどの PRI 情報チャネルともバインドされていないことに注意。

[デフォルト値] **none**

7 IP の設定

7.1 LAN,PP 共通の設定

7.1.1 IP パケットを扱うか否かの設定

[入力形式] **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。このスイッチを **on** にしないと PP 側の IP 関連は一切動作しない。

[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**

7.1.2 IP パケットのフィルタの設定

[入力形式] **ip filter** *filter_number pass_reject src_addr[/mask] [dest_addr[/mask] [proto [src_port_list[dest_port_list]]]]*

[パラメータ]
- *filter_number* ... 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_addr* ... IP パケットの始点 IP アドレス
  - xxx.xxx.xxx.xxx xxx は
    - 十進数
    - * (ネットマスクの対応するビットが 8 ビットとも 0 と同じ)
  - 間に – をはさんだ 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。
  - * (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)。省略した時は一個の*と同じ。
- *mask* ... IP アドレスのビットマスク、省略した時は 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 は十進数)
  - 0x に続く十六進数
  - マスクビット数

- *proto* ... フィルタリングするパケットの種類
  - プロトコルを表す十進数
  - プロトコルを表すニーモニック

icmp	1
tcp	6
udp	17

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

  省略した時は*と同じ。
- *src_port* ... UDP、TCP のソースポート番号
  - ポート番号を表す十進数
  - ポート番号を表すニーモニック (一部)

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

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

  省略した時は*と同じ。
- *dest_port* ... UDP、TCP のデスティネーションポート番号

[説明] IP パケット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 **ip lan secure filter** コマンド、**ip pp secure filter** コマンド、**ip lan rip filter** コマンド、及び **ip pp 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時だけ通せば十分で、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。

RTA50i ではいくつかの番号が予約されていることに注意。

[設定例]
```
# ip filter 3 pass-nolog 172.20.10.* 172.21.192.0/0xffffc000 tcp ftp
```

7.1.3 IP パケットのフィルタの削除

[入力形式] **ip filter delete** *filter_number*

[パラメータ] • *filter_number* ... フィルタの番号 (1..100)

[説明] 指定された番号の IP のフィルタを削除する。

7.1.4 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*

[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] **off**

7.1.5 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*

[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] **off**

7.1.6 IP パケットの TOS フィールドの書き換えの設定

[入力形式]

1. **ip tos supersede** *N tos [***precedence=** *precedence] filter_number [filter_number_list]*
2. **ip tos supersede** *N* **clear**

[パラメータ]

- *N* ... 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* を省略した場合は PRECEDENCE 値は変更しない
- *filter_number, filter_number_list* ... フィルタの番号 (1..100)
- **clear** ... 設定を削除

[説明]

IP パケットを中継するときに 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_number* 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-log**、**pass-nolog**、**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-log** または **reject-nolog** である場合は書き換えずに処理を終わる。

[ノート]

このコマンドの設定内容については **show ip tos supersede** コマンドで確認できる。

[デフォルト値]

clear

7.2 LAN 側の設定

7.2.1 IP アドレスの設定

[入力形式]

1. **ip lan address** *ip_address[/netmask]*
2. **ip lan1 address** *ip_address[/netmask]*
3. **ip lan2 address** *ip_address[/netmask]*
4. **ip lan address clear**
5. **ip lan1 address clear**
6. **ip lan2 address clear**

[パラメータ]

- *ip_address* ... xxx.xxx.xxx.xxx (xxx は十進数)
- *netmask*
  - xxx.xxx.xxx.xxx(xxx は十進数)
  - 0x に続く十六進数
  - マスクビット数
- **clear** ... RARP により IP アドレスを決定する

[説明]

LAN 側の IP アドレスとネットマスクを設定する。

[ノート]

ip_address を設定すると、その IP アドレスが固定的に使用される。
clear を指定すると、パワーオン時に RARP により IP アドレスを取得しにいく。RARP で IP アドレスが取得できなかった場合、LAN に対して IP の動作を行なわない。
netmask パラメータを設定しない場合には、ネットマスクは変更無しとして扱う。

[デフォルト値]

clear ... RT200i, RT140p, RT140f, RT140i, RT140e, RT103i
192.168.0.1 ... RTA50i

7.2.2 LAN 側のセカンダリ IP アドレスの設定

[入力形式]

1. **ip lan secondary address** *ip_address/netmask*
2. **ip lan1 secondary address** *ip_address/netmask*
3. **ip lan2 secondary address** *ip_address/netmask*
4. **ip lan secondary address clear**
5. **ip lan1 secondary address clear**
6. **ip lan2 secondary address clear**

[パラメータ]

- *ip_address* ... xxx.xxx.xxx.xxx (xxx は十進数)
- *netmask*
  - xxx.xxx.xxx.xxx(xxx は十進数)
  - 0x に続く十六進数
  - マスクビット数
- **clear** ... セカンダリ IP アドレスをクリアする

[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。

[デフォルト値] **clear**

7.2.3 ネットマスクの設定

[入力形式]

1. **ip lan netmask** *netmask*
2. **ip lan1 netmask** *netmask*
3. **ip lan2 netmask** *netmask*

[パラメータ]

- *netmask*
  - xxx.xxx.xxx.xxx(xxx は十進数)
  - 0x に続く十六進数
  - マスクビット数
  - **class** ... class A,B,C を解釈して自動設定する

[説明] LAN 側のネットマスクを設定する。

[デフォルト値] **class**

7.2.4 ブロードキャストアドレスの設定

[入力形式]
1. **ip lan broadcast** *broadcast_address*
2. **ip lan1 broadcast** *broadcast_address*
3. **ip lan2 broadcast** *broadcast_address*

[パラメータ]
- *broadcast_address*
  - **0** ... 0.0.0.0 を用いる
  - **1** ... 255.255.255.255 を用いる
  - **2** ... ネットワークアドレス + オール 0 を用いる
  - **3** ... ネットワークアドレス + オール 1 を用いる

[説明] LAN 側のブロードキャストアドレスのタイプを設定する。受信に関してはすべてのタイプをブロードキャストアドレスとして認識する。

[デフォルト値] **1**

7.2.5 経路情報の追加

[入力形式]
1. **ip lan route add** *net_host destination[/mask] gateway metric*
2. **ip lan1 route add** *net_host destination[/mask] gateway metric*
3. **ip lan2 route add** *net_host destination[/mask] gateway metric*

[パラメータ]
- *net_host*
  - **net** ... *destination* がネットワークの時に指定する
  - **host** ... *destination* がホストの時に指定する
- *destination* ... 送り先のホスト / ネットワーク IP アドレス
  - xxx.xxx.xxx.xxx (xxx は十進数)
  - **default**
- *mask* ... 送り先がネットワークである時のネットマスク
  - xxx.xxx.xxx.xxx(xxx は十進数)
  - 0x に続く十六進数
  - マスクビット数
- *gateway* ... ゲートウェイの IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))
- *metric* ... 送り先に到達するまでのゲートウェイの数

[説明] 経路情報テーブルに LAN 側の経路情報を追加する。

[ノート] 既に経路情報テーブルに *destination* が存在する時は追加されない。

7.2.6 経路情報の削除

[入力形式]
1. **ip lan route delete** *destination*
2. **ip lan1 route delete** *destination*
3. **ip lan2 route delete** *destination*

[パラメータ]
- *destination* ... 送り先のホスト / ネットワーク IP アドレス
  - xxx.xxx.xxx.xxx (xxx は十進数)
  - **default**

[説明] 経路情報テーブルから LAN 側の経路情報を削除する。

7.2.7 動的経路制御の設定

[入力形式]
1. **ip lan routing protocol** *routing_protocol*
2. **ip lan1 routing protocol** *routing_protocol*
3. **ip lan2 routing protocol** *routing_protocol*

[パラメータ]
- *routing_protocol*
  - **none** ... LAN 側に RIP を出さない
  - **rip** ... 動的経路制御として RIP(バージョン 1) を使う
  - **rip2** ... 動的経路制御として RIP2(マルチキャスト) を使う
  - **rip2-broadcast** ... 動的経路制御として RIP2(ブロードキャスト) を使う

[説明] LAN 側の動的経路制御を設定する。
rip2、**rip2-broadcast** はともに RIP2 を使用することを意味するが、**rip2** では RIP2 広告パケットをマルチキャストで送信するのに対し、**rip2-broadcast** ではそれをブロードキャストで送信する。受信に関しては、マルチキャスト、ブロードキャストとも設定に関わらず可能。

[デフォルト値] **rip**

7.2.8 RIP のフィルタリングの設定

[入力形式]
1. **ip lan rip filter** *direction filter_list*
2. **ip lan1 rip filter** *direction filter_list*
3. **ip lan2 rip filter** *direction filter_list*

[パラメータ]
- *direction*
  - **in** ... LAN 側から受信した RIP のフィルタリング
  - **out** ... LAN 側へ送出する RIP のフィルタリング
- *filter_list*
  - 空白で区切られた *filter_number* の並び (10 個以内)
  - **clear**(フィルタリングしない)

[説明] LAN 側から受信する RIP、並びに LAN 側に送出する 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 IP パケットのフィルタの *src_addr* パラメータ部分を用いる。

[デフォルト値] **in**、**out** とも **clear**

7.2.9 RIP に関して信用できるゲートウェイの設定

[入力形式]
1. **ip lan rip listen** *gateway_list*
2. **ip lan1 rip listen** *gateway_list*
3. **ip lan2 rip listen** *gateway_list*

[パラメータ]
- *gateway_list*
  - **all** ... すべてのゲートウェイの RIP を受け入れる
  - **none** ... すべてのゲートウェイの RIP を受け入れない
  - IP アドレスの並び (10 個以内) ... 指定されたゲートウェイからの RIP のみ受け入れる
  - **except** に続く IP アドレスの並び (10 個以内) ... 指定されたゲートウェイからの RIP は受け入れない

[説明] RIP に関して信用できるゲートウェイ、または信用できないゲートウェイを設定する。

[デフォルト値] **all**

7.2.10 LAN 側 RIP2 での認証の設定

[入力形式] 1. **ip lan rip auth type** *type*

2. **ip lan1 rip auth type** *type*

3. **ip lan2 rip auth type** *type*

[パラメータ]
- *type*
  - **none** ... 認証しない
  - **text** ... テキスト型の認証を行なう

[説明] LAN 側で RIP2 を使用する時の認証の設定をする。
none の場合は認証なし。
text の時はテキスト型の認証を行う。

[デフォルト値] **none**

7.2.11 LAN 側 RIP2 での認証キーの設定

[入力形式] 1. **ip lan rip auth key** *key*

2. **ip lan1 rip auth key** *key*

3. **ip lan2 rip auth key** *key*

[パラメータ]
- *key*
  - 十六進数列 ... RIP2 での認証キーを設定する
  - **clear** ... RIP2 での認証キーを削除する
  - **text** ... テキスト型の認証キーを設定する

[説明] LAN 側で RIP2 を使用する時の認証キーを設定する。
clear の場合は認証なし。
text の時は text の後ろに文字列で入力する。

[設定例]
```
# ip lan rip auth key text testing123
# ip lan rip auth key text ‘‘hello world’’
# ip lan rip auth key 01 02 ff 35 8e 49 a8 3a 5e 9d
```

7.2.12 Proxy ARP の設定

[入力形式]
1. **ip lan proxyarp** *proxyarp*
2. **ip lan1 proxyarp** *proxyarp*
3. **ip lan2 proxyarp** *proxyarp*

[パラメータ]
- *proxyarp*
  - **on** ... 返す
  - **off** ... 返さない

[説明] Proxy ARP を返すか否か設定する。

[デフォルト値] **off**

7.2.13 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]
1. **ip lan secure filter** *direction filter_list*
2. **ip lan1 secure filter** *direction filter_list*
3. **ip lan2 secure filter** *direction filter_list*

[パラメータ]
- *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 filter_number の並び (100 個以内)
  - **clear** (フィルタリングしない)

[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、LAN 側を通るパケットの種類の制限を設定する。

[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。

```
ip filter 1 pass 192.168.*.*
ip filter 2 reject 192.168.1.5
ip 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時は破棄になる。

[デフォルト値] **clear**

7.2.14 LAN インタフェースの MTU の設定

[入力形式] 1. **ip lan mtu** mtu
2. **ip lan1 mtu** mtu
3. **ip lan2 mtu** mtu

[パラメータ] • *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] Rev.4.00.11 とそれ以前のリビジョンでは、LAN インタフェースの MTU は 1500 に固定である。

[デフォルト値] 1500

7.3 PP 側相手毎の IP の設定

7.3.1 自分の PP 側 IP アドレスの設定

[入力形式] 1. **ip pp local address** *ip_address[/netmask]*
2. **ip pp local address clear**

[パラメータ] • *ip_address* ... xxx.xxx.xxx.xxx (xxx は十進数)
• *netmask*
  ◦ xxx.xxx.xxx.xxx(xxx は十進数)
  ◦ 0x に続く十六進数
  ◦ マスクビット数
• **clear** ... 自分の PP 側 IP アドレスを設定しない

[説明] 選択されている相手について自分の PP 側の IP アドレスとネットマスクを設定する。

[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。

ip pp local address の設定	**ppp ipcp ipaddress on**		**ppp ipcp ipaddress off**
	相手側設定あり	相手側設定なし	
clear	yyy.yyy.yyy.yyy	Unnumbered	Unnumbered
xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx または接続不可	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx

[デフォルト値] **clear**

[設定例] 例えば、ルータ A 側が **ip pp local address clear**、**ppp ipcp ipaddress on** と設定し、接続するルータ B 側が **ip pp remote 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** になることを意味します。

7.3.2 相手の PP 側 IP アドレスの設定

[入力形式] **ip pp remote address** *ip_address*

[パラメータ]

- *ip_address*
  - xxx.xxx.xxx.xxx (xxx は十進数)
  - **clear**

[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。

[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。

ip pp remote address の設定	**ppp ipcp ipaddress on**		**ppp ipcp ipaddress off**
	相手側設定あり	相手側設定なし	
clear	yyy.yyy.yyy.yyy	Unnumbered	Unnumbered
xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx または接続不可	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx

[デフォルト値] **clear**

[設定例] 例えば、ルータ A 側が **ip pp remote address clear**、**ppp ipcp ipaddress on** と設定し、接続するルータ B 側が **ip pp local address yyy.yyy.yyy.yyy** と設定している場合には、実際のルータ A の PP 側の IP アドレスは **yyy.yyy.yyy.yyy** になることを意味します。

7.3.3 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*

[パラメータ]

- *ip_address*
  - IP アドレス列 ... **anonymous** のためにプールする IP アドレス
  - **clear** ... プールした IP アドレスをクリアする

[説明] **ip pp remote address** コマンドで利用できるアドレスプールを設定する。
RT200i では 16 個まで、**RT140p** では 28 個まで、**RT140f, RT140i, RT140e** では 4 個まで、それ以外では 2 個まで設定できる。
PP として **anonymous** が選択された時のみ有効である。

7.3.4 PP 側のネットマスクの設定

[入力形式] **ip pp netmask** *netmask*

[パラメータ]

- *netmask*
  - xxx.xxx.xxx.xxx(xxx は十進数)
  - 0x に続く十六進数
  - マスクビット数
  - **class** ... class A,B,C を解釈する

[説明] 選択されている相手について PP 側のネットマスクを設定する。

[デフォルト値] **class**

7.3.5 経路情報の追加

[入力形式]

1. **ip pp route add** *net_host destination[/mask] [name] metric*
2. **ip pp route add** *net_host destination[/mask] [gateway] metric*
3. **ip pp route add** *net_host destination[/mask]* [**dlci**=*dlci_num*] *metric*

[パラメータ]

- *net_host*
  - **net** ... *destination* がネットワークの時に指定する
  - **host** ... *destination* がホストの時に指定する
- *destination* ... 送り先のホスト / ネットワーク IP アドレス
  - xxx.xxx.xxx.xxx (xxx は十進数)
  - **default**
- *mask* ... 送り先がネットワークである時のネットマスク
  - xxx.xxx.xxx.xxx(xxx は十進数)
  - 0x に続く十六進数
  - マスクビット数
- *name* ... 名前 (16 文字以内)
- *gateway* ... ゲートウェイの IP アドレス
- *dlci_num* ... ゲートウェイの DLCI
- *metric* ... 送り先に到達するまでのゲートウェイの数

[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 IP アドレスまたは DLCI を書くことが可能。IP アドレスで指定した場合は、InARP により相手の DLCI に対応する IP アドレスが分かっている必要がある。

[ノート] 既に経路情報テーブルに *destination* が存在する時は追加されない。
name パラメータは、**anonymous** が選択された時のみ有効である。

7.3.6 経路情報の削除

[入力形式] **ip pp route delete** *destination*

[パラメータ]
- *destination* ... 送り先のホスト / ネットワーク IP アドレス
  - xxx.xxx.xxx.xxx (xxx は十進数)
  - **default**

[説明] 選択されている相手について、経路情報テーブルから PP 側の経路情報を削除する。

7.3.7 PP 側の動的経路制御の設定

[入力形式] **ip pp routing protocol** *routing_protocol*

[パラメータ]
- *routing_protocol*
  - **none** ... PP 側に RIP を出さない
  - **rip** ... 動的経路制御として RIP(バージョン 1) を使う
  - **rip2** ... 動的経路制御として RIP2(マルチキャスト) を使う
  - **rip2-broadcast** ... 動的経路制御として RIP2(ブロードキャスト) を使う

[説明] 選択されている相手について PP 側の動的経路制御を設定する。
rip2、**rip2-broadcast** はともに RIP2 を使用することを意味するが、**rip2** では RIP2 広告パケットをマルチキャストで送信するのに対し、**rip2-broadcast** ではそれをブロードキャストで送信する。受信に関しては、マルチキャスト、ブロードキャストとも設定に関わらず可能。

[デフォルト値] **none**

7.3.8 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*

[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接続時に RIP を送出する条件を設定する。

[デフォルト値] **update**

7.3.9 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*

[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 routing protocol コマンドが **rip**、**ip pp rip connect send** コマンドが **interval** の時に有効である。

[デフォルト値] 30

7.3.10 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*

[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**

7.3.11 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*

[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 routing protocol コマンドが **rip**、**ip pp rip disconnect send** コマンドが **interval** の時に有効である。

[デフォルト値] 3600

7.3.12 回線切断時の動的経路制御情報の保持

[入力形式] **ip pp hold routing** *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変更された動的経路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] **off**

7.3.13 RIP のフィルタリングの設定

[入力形式] **ip pp rip filter** *direction filter_list*

[パラメータ]
- *direction*
  - **in** ... PP 側から受信した RIP のフィルタリング
  - **out** ... PP 側へ送出する RIP のフィルタリング
- *filter_list*
  - 空白で区切られた filter_number の並び (10 個以内)
  - **clear**(フィルタリングしない)

[説明] PP 側から受信する RIP、並びに PP 側に送出する 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 IP パケットのフィルタの *src_addr* パラメータ部分を用いる。

[デフォルト値] **in**,**out** とも **clear**

7.3.14 RIP ホップ加算数の設定

[入力形式] **ip pp rip hop** *direction hop_count*

[パラメータ]
- *direction*
  - **in** ... PP 側から入ってきた RIP のホップカウントに加算する
  - **out** ... PP 側へ出ていく RIP のホップカウントに加算する
- *hop_count* ... 加算する値 (0..15)

[説明] 選択されている相手について PP 側の RIP のホップカウントに加算する値を設定する。

[デフォルト値] **in**,**out** とも 0

7.3.15 RIP に関して信用できるゲートウェイの設定

[入力形式] **ip pp rip listen** *listen*

[パラメータ]
- *listen*
  - **on** ... RIP を受け入れる
  - **off** ... RIP を受け入れない

[説明] 選択されている相手のゲートウェイからの RIP に関して信用するか否かを設定する。

[デフォルト値] **on**

7.3.16 PP 側 RIP2 での認証の設定

[入力形式] **ip pp rip auth type** *type*

[パラメータ]
- *type*
  - **none** ... 認証しない
  - **text** ... テキスト型の認証を行なう

[説明] 選択されている相手について RIP2 を使用する時の認証の設定をする。
none の場合は認証なし。
text の時はテキスト型の認証を行う。

[デフォルト値] **none**

7.3.17 PP 側 RIP2 での認証キーの設定

[入力形式] **ip pp rip auth key** *key*

[パラメータ]
- *key*
  - 十六進数列 ... RIP2 での認証キーを設定する
  - **clear** ... RIP2 での認証キーを削除する
  - **text** ... テキスト型の認証キーを設定する

[説明] 選択されている相手について PP 側で RIP2 を使用する時の認証キーを設定する。
clear の場合は認証なし。
text の時は **text** の後ろに文字列で入力する。

[デフォルト値] **clear**

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

7.3.18 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] **ip pp secure filter** *direction filter_list*

[パラメータ]

- *direction*
  - **in** ... PP 側から入ってきたパケットのフィルタリング
  - **out** ... PP 側へ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 filter_number の並び (100 個以内)
  - **clear** (フィルタリングしない)

[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、PP 側を通るパケットの種類の制限を設定する。

[ノート] フィルタリストを走査して、一致すると通過、破棄が決定される。

```
ip filter 1 pass 192.168.*.*
ip filter 2 reject 192.168.1.5
ip 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時は破棄になる。

[デフォルト値] **clear**

7.3.19 回線切断時の LAN 側への RIP 動作の設定

[入力形式] **ip pp hide static route** *hide*

[パラメータ]

- *hide*
  - **on** ... RIP で広告しない
  - **off** ... RIP で広告する

[説明] 回線切断時に、その PP に関するスタティックルーティングを LAN 側 に RIP で広告するか否かを設定する。

[ノート] **on** にした時には、回線接続及び切断時に IP ルーティングテーブルのキャッシュは自動的にクリアされる。

[デフォルト値] **off**

7.3.20 PP インタフェースの MTU の設定

[入力形式] **ip pp mtu** *mtu*

[パラメータ] • *mtu* ... MTU の値 (64..1500)

[説明] 選択されている相手について、PP インタフェースの MTU の値を設定する。

[ノート] Rev.4.00.11 とそれ以前のリビジョンでは、PP インタフェースの MTU は 1500 に固定である。

[デフォルト値] 1500

8 IPsec の設定

YAMAHA リモートルータは、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 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** コマンドで行ないます。**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 VPN(Virtual Private Network) のように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 WAN 回線に流し、ルータが IPsec に必要な処理をすべて行なうので、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に対する経路情報の設定は **ip tunnel route add** コマンドで、またその削除は **ip tunnel route delete** コマンドで行ないます。トンネルインタフェースを使用するか使用しないかは、それぞれ **tunnel enable**、**tunnel disable** コマンドを使用します。

相手先情報番号による設定		トンネルインタフェース番号による設定
pp enable		**tunnel enable**
pp disable		**tunnel disable**
pp select	⟺	**tunnel select**
pp default		**tunnel default**
ip pp route add		**ip tunnel route add**
ip pp route delete		**ip tunnel route delete**

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ない、使用をやめるには **ipsec transport delete** 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 YAMAHA リモートルータ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 ~	—	—
3.01	3.01.07	3.01.11 ~	—
4.00	—	4.00.02 ~ 4.00.14	4.00.18 ~

8.1 事前共有鍵の登録

[入力形式] 1. **ipsec pre-shared-key** *host key*

2. **ipsec pre-shared-key** *host* **text** *text*

3. **ipsec pre-shared-key** *host* **clear**

[パラメータ]
- *host* ... 鍵交換を行なうセキュリティ・ゲートウェイの IP アドレス
- *key* ... 鍵となる 0x ではじまる十六進数列 (最大 32 バイト)
- **text** ... 鍵をテキストで入力することを示すキーワード
- *text* ... ASCII 文字列で表した鍵 (最大 32 文字)
- **clear** ... 指定したセキュリティ・ゲートウェイに対する鍵をクリアする

[説明] 鍵交換に必要な事前共有鍵を登録する。これが設定されていない場合、鍵交換は行われない。鍵交換を行な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。
最大 10 個まで登録できる。

[ノート] 登録状況は **show config** コマンドで確認する。

[デフォルト値] **clear**

[設定例]
```
# ipsec pre-shared-key 192.168.1.1 text himitsu
# ipsec pre-shared-key 192.168.10.1 0xCDEEEDC0CDEDCD
```

8.2 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*

[パラメータ]
- *gateway_id* ... セキュリティ・ゲートウェイの識別子 (1..20)
- *ip_address*
  - IP アドレス
  - **clear** ... IP アドレスをクリア

[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。
RT103i では *gateway_id* パラメータは最大 10 である。

[デフォルト値] **clear**

8.3 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*

[パラメータ]
- *gateway_id* ... セキュリティ・ゲートウェイの識別子 (1..20)
- *ip_address*
  - IP アドレス
  - **clear** ... IP アドレスをクリア

[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。
RT103i では *gateway_id* パラメータは最大 10 である。

[ノート] **clear** を設定したときには、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。

[デフォルト値] **clear**

8.4 鍵交換の再送回数と間隔の設定

[入力形式] **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] 鍵交換が失敗した時に鍵交換を繰り返す回数とその時間間隔を設定します。

[デフォルト値] *count* = 10
interval = 5

8.5 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*

[パラメータ]
- *gateway_id* ... セキュリティ・ゲートウェイの識別子 (1..20)
- *algorithm* ... 暗号アルゴリズム
  - **3des-cbc** ... 3DES–CBC
  - **des-cbc** ... DES–CBC

[説明] IKE が用いる暗号アルゴリズムを設定する。
RT103i では *gateway_id* パラメータは最大 10 である。

[ノート] IKE で始動側として働くときには、このコマンドで設定されたアルゴリズムを提案する。応答側として働くときはこのコマンドの設定に関係なく、DES-CBC と 3DES-CBC を用いることができる。

[デフォルト値] **des-cbc**

8.6 IKE が用いるグループの設定

[入力形式] **ipsec ike group** *gateway_id group [group]*

[パラメータ]
- *gateway_id* ... セキュリティ・ゲートウェイの識別子 (1..20)
- *group* ... グループ識別子
  - **modp768**
  - **modp1024**

[説明] IKE で用いるグループを設定する。
RT103i では *gateway_id* パラメータは最大 10 である。

[ノート] IKE で始動側として働くときにはこのコマンドで設定されたグループを提案する。応答側として働くとき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ときには、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ときは、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**

8.7 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*

[パラメータ]
- *gateway_id* ... セキュリティ・ゲートウェイの識別子 (1..20)
- *algorithm* ... ハッシュアルゴリズム
  - **md5** ... MD5
  - **sha** ... SHA

[説明] IKE が用いるハッシュアルゴリズムを設定する。
RT103i では *gateway_id* パラメータは最大 10 である。

[ノート] IKE で始動側として働くときには、このコマンドで設定されたアルゴリズムを提案する。応答側として働くときはこのコマンドの設定に関係なく、MD5 と SHA を用いることができる。

[デフォルト値] **md5**

8.8 自分側の ID の設定

[入力形式] 1. **ipsec ike local id** *gateway_id ip_address[/mask]*

2. **ipsec ike local id** *gateway_id clear*

[パラメータ]
- *gateway_id* ... セキュリティ・ゲートウェイの識別子 (1..20)
- *ip_address* ... IP アドレス
- *mask* ... ネットマスク
- **clear** ... IP アドレスをクリア

[説明] IKE のフェーズ 2 で用いる自分側の ID を設定する。
RT103i では *gateway_id* パラメータは最大 10 である。

[ノート] **clear** を設定したときには、ID を送信しない。*mask* パラメータを省略したときは、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ときは、タイプ 4 の ID が送信される。

[デフォルト値] **clear**

8.9 IKE のログの種類の設定

[入力形式] 1. **ipsec ike log** *gateway_id type [type ...]*

2. **ipsec ike log** *gateway_id clear*

[パラメータ]
- *gateway_id* ... セキュリティ・ゲートウェイの識別子 (1..20)
- *type* ... 出力するログの種類
  - **message-info** ... IKE メッセージの内容
  - **payload-info** ... ペイロードの処理内容
  - **key-info** ... 鍵計算の処理内容
- **clear** ... ログの種類を設定しない

[説明] 出力するログの種類を設定する。ログはすべて、syslog の debug レベルで出力される。
RT103i では *gateway_id* パラメータは最大 10 である。

[ノート] **clear** を設定したときには、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。

[デフォルト値] **clear**

8.10 IKE ペイロードのタイプの設定

[入力形式] **ipsec ike payload type** *gateway_id type*

[パラメータ]
- *gateway_id* ... セキュリティ・ゲートウェイの識別子 (1..20)
- *type* ... ペイロードのタイプ
  - **1** ... Rev.3.01.11 ~ Rev.4.00.14 で使用しているもの
  - **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ときには、タイプを 1 に設定する必要がある。
RT103i では *gateway_id* パラメータは最大 10 である。

[デフォルト値] **2**

8.11 PFS を用いるか否かの設定

[入力形式] **ipsec ike pfs** *gateway_id pfs*

[パラメータ]
- *gateway_id* ... セキュリティ・ゲートウェイの識別子 (1..20)
- *pfs*
  - **on** ... 用いる
  - **off** ... 用いない

[説明] IKE で PFS を用いるか否かを設定する。
RT103i では *gateway_id* パラメータは最大 10 である。

[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**

8.12 相手側の ID の設定

[入力形式]
1. **ipsec ike remote id** *gateway_id ip_address[/mask]*
2. **ipsec ike remote id** *gateway_id clear*

[パラメータ]
- *gateway_id* ... セキュリティ・ゲートウェイの識別子 (1..20)
- *ip_address* ... IP アドレス
- *mask* ... ネットマスク
- **clear** ... IP アドレスをクリア

[説明] IKE のフェーズ 2 で用いる相手側の ID を設定する。
RT103i では *gateway_id* パラメータは最大 10 である。

[ノート] **clear** を設定したときには ID を送信しない。
mask パラメータを省略したときは、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ときは、タイプ 4 の ID が送信される。

[デフォルト値] **clear**

8.13 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*

[パラメータ]
- *gateway_id* ... セキュリティ・ゲートウェイの識別子 (1..20)
- *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。
RT103i では *gateway_id* パラメータは最大 10 である。

[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**

8.14 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。

8.14.1 SA のポリシーの定義

[入力形式] 1. **ipsec sa policy** *policy-id ip_address* **ah** *ah_algorithm*

2. **ipsec sa policy** *policy-id ip_address* **esp** *esp_algorithm [ah_algorithm]*

[パラメータ]
- *policy-id* ... ポリシー ID(1..255)
- *ip_address* ... 対向となるセキュリティ・ゲートウェイの IP アドレス
- **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及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及びトランスポートモードで使用可能。

8.14.2 SA のポリシーの削除

[入力形式] **ipsec sa policy delete** *policy-id*

[パラメータ]
- *policy-id* ... ポリシー ID(1..255)

[説明] 指定したポリシー ID のポリシーを削除する。

8.14.3 IPsec SA の寿命の設定

[入力形式] **ipsec ike duration ipsec-sa** *gateway_id second [kbytes]*

[パラメータ]
- *gateway_id* ... セキュリティ・ゲートウェイの識別子 (1..20)
- *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 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。
RT103i では *gateway_id* パラメータは最大 10 である。

[デフォルト値] 28800

8.14.4 ISAKMP SA の寿命の設定

[入力形式] **ipsec ike duration isakmp-sa** *gateway_id second [kbytes]*

[パラメータ]
- *gateway_id* ... セキュリティ・ゲートウェイの識別子 (1..20)
- *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 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。
RT103i では *gateway_id* パラメータは最大 10 である。

[デフォルト値] 28800

8.14.5 SA の削除

[入力形式] **ipsec sa delete** *id*

[パラメータ]
- *id*
  - SA の ID(1..128)
  - **all** ... すべての SA

[説明] 指定した SA を削除する。
RT200i, RT140p, RT140f, RT140i, RT140e 以外では ID は 32 までである。SA の ID は自動的に付与されるので、**show ipsec sa** コマンドで確認すること。

8.14.6 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。

8.14.7 SA を自動更新するか否かの設定

[入力形式] **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**

8.15 トンネルインタフェース関連の設定

8.15.1 使用する SA のポリシーの設定

[入力形式] **ipsec tunnel** *policy-id*

[パラメータ]
- *policy-id*
  - ポリシー ID(1..255)
  - **clear** ... ポリシーをクリアする

[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 のポリシーを設定します。

[デフォルト値] **clear**

8.15.2 静的トンネル経路情報の追加

[入力形式] **ip tunnel route add** *net_host destination[/mask] metric*

[パラメータ]
- *net_host*
  - **net** ... *destination* がネットワークの時に指定する
  - **host** ... *destination* がホストの時に指定する
- *destination* ... 送り先のホスト / ネットワーク IP アドレス
  - xxx.xxx.xxx.xxx (xxx は十進数)
  - **default**
- *mask* ... 送り先がネットワークである時のネットマスク
  - xxx.xxx.xxx.xxx(xxx は十進数)
  - 0x に続く十六進数
  - マスクビット数
- *metric* ... 送り先に到達するまでのゲートウェイの数 (1..15)

[説明] 経路情報テーブルにトンネルインタフェースに対する経路情報を追加する。

[ノート] 既に経路情報テーブルに *destination* が存在する時は追加されない。

8.15.3 静的トンネル経路情報の削除

[入力形式] **ip tunnel route delete** *destination*

[パラメータ]
- *destination* ... 送り先のホスト / ネットワーク IP アドレス
  - xxx.xxx.xxx.xxx (xxx は十進数)
  - **default**

[説明] 経路情報テーブルから指定したトンネルインタフェースの経路情報を削除する。

8.15.4 トンネルインタフェースに対するフィルタリングの設定

[入力形式] **ip tunnel secure filter** *direction filter_list*

[パラメータ]

- *direction*
  - **in** ... トンネル側から入ってくるパケットのフィルタリング
  - **out** ... トンネル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 filter_number の並び (100 個以内)
  - **clear** (フィルタリングしない)

[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、トンネルインタフェースを通るパケットの種類の制限を設定する。

[デフォルト値] **clear**

8.16 トランスポートモード関連の設定

8.16.1 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]]]*

[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
  - ポート番号を表す十進数
  - ポート番号を表すニーモニック
  - *(すべてのポート)
- *dst_port_list* ... UDP、TCP のデスティネーションポート番号列
  - ポート番号を表す十進数
  - ポート番号を表すニーモニック
  - *(すべてのポート)

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

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

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

8.16.2 トランスポートモードの削除

[入力形式] **ipsec transport delete** *id*

[パラメータ]
- *id* ... トランスポート ID(1..255)

[説明] 定義してあるトランスポートモードを削除する。

9 IPX の設定

9.1 LAN,PP 共通の設定

9.1.1 IPX パケットを扱うか否かの設定

[入力形式] **ipx routing** *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**

9.1.2 IPX パケットのフィルタの設定

[入力形式] **ipx filter** *filter_number pass_reject src_net[src_node[dst_net[dst_node[type [src_socket[dst_socket]]]]]]*

[パラメータ]
- *filter_number* ... フィルタの番号 (1..100)
- *pass_reject*
  - **pass-log** ... 一致すれば通す (ログに記録する)
  - **pass-nolog** ... 一致すれば通す (ログに記録しない)
  - **reject-log** ... 一致すれば破棄する (ログに記録する)
  - **reject-nolog** ... 一致すれば破棄する (ログに記録しない)
  - **restrict-log** ... 回線が接続されていれば通し、切断されていれば破棄する (ログに記録する)
  - **restrict-nolog** ... 回線が接続されていれば通し、切断されていれば破棄する (ログに記録しない)
- *src_net* ... 始点 IPX ネットワーク番号
  - 0:0:0:1 ... FF:FF:FF:FE(2 桁以内の十六進数以外に '*' も指定可)
  - * (すべての IPX ネットワーク番号)
- *src_node* ... 始点 IPX ノード番号
  - 0:0:0:0:0:1 ... FF:FF:FF:FF:FF:FE(2 桁以内の十六進数以外に '*' も指定可)
  - *(すべての IPX ノード番号)

  省略した時は一個の*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
  - 十進数 (0..255)
  - 十六進数 (0x0..0xFF)
  - ニーモニック文字列

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

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

  省略した時は一個の*と同じ
- *src_socket* ... 始点ソケット番号
  - 十進数 (0..65535)
  - 0x を先頭に持つ 4 桁以内の十六進数
  - プロトコルを表すニーモニック

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

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

  省略した時は一個の*と同じ
- *dst_socket* ... 終点ソケット番号　　*src_socket* と同じ形式。

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

[ノート] IPX パケットタイプでは、“–xxx” は “0–xxx” の意味に、また “yyy–” は “yyy–255” の意味に取る。
ソケット番号では、 “yyy–” は “yyy–65535” の意味に取る。

restrict-log 及び **restrict-nolog** を使ったフィルタは、回線が接続されている時だけ通せば十分で、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。

9.1.3 IPX パケットのフィルタの削除

[入力形式] **ipx filter delete** *filter_number*

[パラメータ]
- *filter_number* ... フィルタの番号 (1..100)

[説明] 指定された番号の IPX のフィルタを削除する。

9.1.4 静的な SAP テーブルの設定

[入力形式] **ipx sap add** *service_type server_name network node_number socket hop*

[パラメータ]
- *service_type* ... サービスタイプ
  - 十進数 (0..65535)
  - 0x に続く 4 桁以内の十六進数
  - **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_number* ... 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
  - 十進数 (0..65535)
  - 0x に続く 4 桁以内の十六進数
  - プロトコルを表すニーモニック

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。

9.1.5 静的な SAP テーブルの削除

[入力形式] **ipx sap delete** *service_type server_name*

[パラメータ]
- *service_type* ... サービスタイプ
  - 十進数 (0..65535)
  - 0x を先頭に持つ 4 桁以内の十六進数
  - **file** ... 0x0004 のニーモニック
  - **print** ... 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

[説明] 静的に設定された SAP テーブルを削除する。

9.1.6 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*

[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**

9.2 LAN 側の設定

9.2.1 イーサネットフレームタイプの設定

[入力形式]
1. **ipx lan frame type** *type*
2. **ipx lan1 frame type** *type*
3. **ipx lan2 frame type** *type*

[パラメータ]
- *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。
複数 LAN ポートモデルでは [入力形式] の 2 または 3 番目の形式で設定する。
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

9.2.2 LAN 側の IPX ネットワーク番号の設定

[入力形式]
1. **ipx lan network** *network*
2. **ipx lan1 network** *network*
3. **ipx lan2 network** *network*

[パラメータ]
- *network*
  - IPX ネットワーク番号 (0:0:0:1 .. FF:FF:FF:FE)
  - **clear** ... IPX ネットワーク番号をクリアする (0:0:0:0)

[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。
複数 LAN ポートモデルでは [入力形式] の 2 または 3 番目の形式で設定する。

[デフォルト値] **lan, lan1** に対しては 0:0:0:1、**lan2** に対しては **clear**

9.2.3 経路情報の追加

[入力形式]
1. **ipx lan route add** *network gateway hop [ticks]*
2. **ipx lan1 route add** *network gateway hop [ticks]*
3. **ipx lan2 route add** *network gateway hop [ticks]*

[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)
- *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。
複数 LAN ポートモデルでは [入力形式] の 2 または 3 番目の形式で設定する。

[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時はホップカウントと同じになる。

9.2.4 経路情報の削除

[入力形式]
1. **ipx lan route delete** *network*
2. **ipx lan1 route delete** *network*
3. **ipx lan2 route delete** *network*

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

[説明] 経路情報テーブルから LAN 側の経路情報を削除する。
複数 LAN ポートモデルでは [入力形式] の 2 または 3 番目の形式で設定する。

9.2.5 LAN 側の RIP/SAP ブロードキャストの設定

[入力形式]
1. **ipx lan ripsap broadcast** *broadcast*
2. **ipx lan1 ripsap broadcast** *broadcast*
3. **ipx lan2 ripsap broadcast** *broadcast*

[パラメータ]
- *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かどうかを選択する。
複数 LAN ポートモデルでは [入力形式] の 2 または 3 番目の形式で設定する。

[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] 60

9.2.6 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] 1. **ipx lan secure filter** *direction filter_list*

2. **ipx lan1 secure filter** *direction filter_list*

3. **ipx lan2 secure filter** *direction filter_list*

[パラメータ]
- *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*
  - 空白で区切られた *filter_number* の並び (30 個以内)
  - **clear** (フィルタリングしない)

[説明] LAN 側に対して適用する IPX フィルタを設定する。
複数 LAN ポートモデルでは [入力形式] の 2 または 3 番目の形式で設定する。

[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時は破棄になる。

[デフォルト値] **clear**

9.3 PP 側相手毎の IPX の設定

9.3.1 IPX ルーティング許可の設定

[入力形式] **ipx pp routing** *routing*

[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**

9.3.2 PP 側 IPX ネットワーク番号の設定

[入力形式] **ipx pp network** *network [node_number]*

[パラメータ]
- *network* ... IPX ネットワーク番号
  - 0:0:0:1 ... FF:FF:FF:FE
  - **clear**(IPX ネットワーク番号無し)
- *node_number* ... 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 **clear**、IPX ノード番号は MAC アドレス

9.3.3 経路情報の追加

[入力形式]
1. **ipx pp route add** *network [name] hops [ticks]*
2. **ipx pp route add** *network [***dlci**=*dlci_num] hops [ticks]*

[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)
- *ticks* ... 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 を書くことが可能。

[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時はホップカウントの 55 倍になる。
name パラメータは、**anonymous** が選択された時のみ有効である。

9.3.4 経路情報の削除

[入力形式] **ipx pp route delete** *network*

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

[説明] 選択されている相手について経路情報テーブルから PP 側の経路情報を削除する。

9.3.5 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*

[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時だけ送出する

[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**

9.3.6 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*

[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

9.3.7 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*

[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**

9.3.8 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*

[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

9.3.9 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*

[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。

[ノート] 実際の設定を確認する場合は **show ipx pp** コマンドで行なうこと。
リビジョン 1.03 まではデフォルトが **off** である。

[デフォルト値] **on**

9.3.10 IPXWAN 使用の設定

[入力形式] **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なう
  - **off** ... パラメータのネゴシエーションは IPXCP で行ない、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**

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

[入力形式] **ipx pp ipxwan retry** *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] $interval = 20$
$max = 3$

9.3.12 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*

[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

9.3.13 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*

[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**

9.3.14 Watchdog 代理応答の時間間隔の設定

[入力形式] **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

9.3.15 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*

[パラメータ]
- *proxy*
  - **on** ... 代理応答を行う
  - **off** ... 代理応答を行なわない

[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**

9.3.16 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]]*

[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 YAMAHA リモートルータが 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

9.3.17 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*

[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**

9.3.18 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*

[パラメータ]

- *direction*
  - **in** ... PP 側から入って来る方向でフィルタを適用
  - **out** ... PP 側へ出て行く方向でフィルタを適用
- *filter_list*
  - 空白で区切られた filter_number の並び (30 個以内)
  - **clear** (フィルタリングしない)

[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時は破棄になる。

[デフォルト値] **clear**

10 ブリッジの設定

10.1 LAN,PP 共通の設定

10.1.1 ブリッジ使用許可の設定

[入力形式] **bridge use** *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] ブリッジを行な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**

10.1.2 ブリッジするインタフェースの設定

[入力形式] **bridge group** *interface_list*

[パラメータ]
- *interface_list*
  - 相手先情報番号
  - **anonymous**
  - **leased**
  - LAN インタフェース名 (**lan, lan1, lan2,...**)

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

[ノート] このコマンドが実行されない場合は、**lan1** と PP1 間でブリッジされる。
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。また、複数 WAN ポートモデルの場合は、**leased** は指定できない。

[デフォルト値] 複数 LAN ポートモデル ... **lan1 1**
1 LAN ポートモデル ... **lan 1**

[設定例] **RT140e** の LAN1 ポートと LAN2 ポート間でブリッジする。

```
# bridge group lan1 lan2
```

RT140e の 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
```

10.1.3 ブリッジのフィルタの設定

[入力形式] **bridge filter** *filter_number pass_reject src_mac[dst_mac[offset byte_list]]*

[パラメータ]

- *filter_number* ... フィルタの番号 (1..10)
- *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 は
    - 十六進数
    - *
  - *(すべての MAC アドレスに対応)
- *dst_mac* ... 終点 MAC アドレス　　*src_mac* と同じ形式。省略した時は一個の*と同じ
- *offset* ... オフセットを表す十進数 (イーサネットフレームの始点 MAC アドレスの直後を 0 とするバイト数)
- *byte_list*
  - バイト列
    - XX(XX は 2 桁の十六進数)
    - 上項目のカンマで区切った並び (16 個以内)
  - *(すべてのバイト表現)

[説明] 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** 及び **restrict-nolog** を使ったフィルタは、回線が接続されている時だけ通せば十分で、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。

10.1.4 ブリッジのフィルタの削除

[入力形式] **bridge filter delete** *filter_number*

[パラメータ]

- *filter_number* ... フィルタの番号 (1..10)

[説明] 指定された番号のブリッジのフィルタを削除する。

10.1.5 ブリッジする相手先の設定

[入力形式] **bridge forwarding** *peer_number_list*

[パラメータ]
- *peer_number_list*
  - 相手先情報番号
  - **anonymous**
  - **leased**

[説明] ブリッジする相手先を設定する。
このコマンドは **bridge group** コマンドと等価である。例えば、**bridge group lan1 1 2 = bridge forwarding 1 2** など。
相手先は WAN 回線数の 2 倍まで設定できる。

[ノート] このコマンドを実行しない時には LAN インタフェースと PP1 の間でブリッジされる。
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。
また、複数 WAN ポートモデルの場合は **leased** は指定できない。

[デフォルト値] 1

10.1.6 MAC アドレスのラーニングを行なうか否かの設定

[入力形式] **bridge learning** *learning*

[パラメータ]
- *learning*
  - **on** ... 行なう
  - **off** ... 行なわない

[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時に終点 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**

10.1.7 ラーニング情報消去タイマの設定

[入力形式] **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時には、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。

[デフォルト値] **off**

10.2 LAN 側の設定

10.2.1 ラーニング情報の設定

[入力形式] 1. **bridge lan learning add** *mac_address*
2. **bridge lan1 learning add** *mac_address*
3. **bridge lan2 learning add** *mac_address*

[パラメータ] • *mac_address* ... XX:XX:XX:XX:XX:XX (XX は十六進数)

[説明] LAN 側インタフェースに対して MAC アドレスのラーニング情報を設定する。
複数 LAN ポートモデルでは [入力形式] の 2 または 3 番目の形式で設定する。

[ノート] 設定されたラーニング情報は **bridge lan learning delete** コマンドでないと消去されない。ラーニング情報は全体で 30 個まで設定できる。

10.2.2 ラーニング情報の削除

[入力形式] 1. **bridge lan learning delete** *mac_address*
2. **bridge lan1 learning delete** *mac_address*
3. **bridge lan2 learning delete** *mac_address*

[パラメータ] • *mac_address* ... XX:XX:XX:XX:XX:XX (XX は十六進数)

[説明] LAN 側の MAC アドレスのラーニング情報を削除する。
複数 LAN ポートモデルでは [入力形式] の 2 または 3 番目の形式で設定する。

10.2.3 LAN 側でのブリッジのフィルタリングの設定

[入力形式] 1. **bridge lan filter** *direction filter_list*
2. **bridge lan1 filter** *direction filter_list*
3. **bridge lan2 filter** *direction filter_list*

[パラメータ] • *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 filter_number の並び (10 個以内)
  ◦ **clear**(フィルタリングしない)

[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。
複数 LAN ポートモデルでは [入力形式] の 2 または 3 番目の形式で設定する。

[デフォルト値] **clear**

10.3 PP 側相手毎のブリッジの設定

10.3.1 ラーニング情報の設定

[入力形式] **bridge pp learning add** *mac_address [***dlci=***dlci_num]*

[パラメータ]
- *mac_address* ... XX:XX:XX:XX:XX:XX(XX は十六進数)
- *dlci_num* ... ゲートウェイの DLCI

[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、ラーニング情報として DLCI を指定することが可能。

[ノート] 設定されたラーニング情報は **bridge pp learning delete** コマンドでないと消去されない。ラーニング情報は全体で 30 個まで設定できる。

10.3.2 ラーニング情報の削除

[入力形式] **bridge pp learning delete** *mac_address*

[パラメータ]
- *mac_address* ... XX:XX:XX:XX:XX:XX (XX は十六進数)

[説明] PP 側の MAC アドレスのラーニング情報を削除する。

10.3.3 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*

[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 filter_number の並び (10 個以内)
  - **clear**(フィルタリングしない)

[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] **clear**

11 PPP の設定

11.1 相手の名前とパスワードの設定

[入力形式] **pp auth username** *username password [isdn1] [***clid** *[isdn2]] [***mscbcp***] [ip_address]*

[パラメータ]
- *username* ... 名前 (32 文字以内)
- *password* ... パスワード (32 文字以内)
- *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* ... 相手の IP アドレス (**ip pp remote address** に対応)

[説明] 相手の名前とパスワードを設定する。複数設定可。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 '*' を与えた時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。
キーワード **clid** 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。
キーワード **mscbcp** 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。

11.2 要求する認証タイプの設定

[入力形式] **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

[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 の選択が失敗した時に適用される。キーワード **chap-pap** 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。オプション引数 **arrive-only** が指定された時には、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**

11.3 受け入れる認証タイプの設定

[入力形式] **pp auth accept** *accept*

[パラメータ]
- *accept*
  - **none** ... 認証を受け入れない
  - **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 の選択が失敗した時に適用される。PP 毎のコマンドである。

[デフォルト値] **none**

11.4 自分の名前とパスワードの設定

[入力形式] **pp auth myname** *myname password*

[パラメータ]
- *myname* ... 名前 (32 文字以内)
- *password* ... パスワード (32 文字以内)

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

11.5 自分の名前の消去

[入力形式] **pp auth clear myname**

[パラメータ] なし

[説明] 自分の名前とパスワードを消去する。

11.6 相手の名前の削除

[入力形式] **pp auth delete username** *username*

[パラメータ]
- *username* ... 名前 (32 文字以内)

[説明] パラメータで指定した相手の名前とそのパスワードを削除する。

11.7 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*

[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時便利。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 が選択された時のみ有効である。

[デフォルト値] **off**

11.8 LCP 関連の設定

11.8.1 Address & Control Field Compression オプション使用の設定

[入力形式] **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 & Control Field Compression オプションを用いるか否かを設定する。

[ノート] **on** を設定していても相手に拒否された時は用いない。また、このオプションを相手から要求された時には、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**

11.8.2 Magic Number オプション使用の設定

[入力形式] **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時は用いない。

[デフォルト値] **on**

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

[入力形式] **ppp lcp mru** *mru [length]*

[パラメータ]
- *mru*
  - **on** ... 用いる
  - **off** ... 用いない
- *length*
  - **1500** ... 1500bytes
  - **1792** ... 1792bytes

[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 の長さを設定する。

[ノート] **on** を設定していても相手に拒否された時は用いない。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時には **off** にする。
データが圧縮されている時には、*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**

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

[入力形式] **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時は用いない。また、このオプションを相手から要求された時には、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**

11.8.5 パラメータ lcp-restart の設定

[入力形式] **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

11.8.6 パラメータ lcp-max-terminate の設定

[入力形式] **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

11.8.7 パラメータ lcp-max-configure の設定

[入力形式] **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

11.8.8 パラメータ lcp-max-failure の設定

[入力形式] **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

11.8.9 専用線キープアライブを使用するか否かの設定

[入力形式] **leased keepalive use** *use*

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

[説明] 専用線使用時にキープアライブを使用するか否かを設定する。

[ノート] 複数 WAN ポートモデルでは PP 毎のコマンドである。

[デフォルト値] **off**

11.8.10 専用線キープアライブのログをとるか否かの設定

[入力形式] **leased keepalive log** *log*

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

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

[ノート] 複数 WAN ポートモデルでは PP 毎のコマンドである。

[デフォルト値] **on**

11.8.11 専用線キープアライブの時間間隔の設定

[入力形式] **leased keepalive interval** *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 (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] 複数 WAN ポートモデルでは PP 毎のコマンドである。
一度 LCP ECHO Request に対するリプライが返ってこないのを検出したら、その後の監視タイマは 1 秒に短縮される。

[デフォルト値] *interval* = 30
count = 6

11.8.12 専用線ダウン検出時の動作の設定

[入力形式] **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時のルータの動作を設定する。

[ノート] 複数 WAN ポートモデルでは PP 毎のコマンドである。

[デフォルト値] **silent**

11.9 PAP 関連の設定

11.9.1 パラメータ pap-restart の設定

[入力形式] **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

11.9.2 パラメータ pap-max-authreq の設定

[入力形式] **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] 2
10 ... RTA50i

11.10 CHAP 関連の設定

11.10.1 パラメータ chap-restart の設定

[入力形式] **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

11.10.2 パラメータ chap-max-challenge の設定

[入力形式] **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] 2
10 ... RTA50i

11.11 IPCP 関連の設定

11.11.1 Van Jacobson Compressed TCP/IP 使用の設定

[入力形式] **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時は用いない。

[デフォルト値] **off**

11.11.2 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*

[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。

[ノート] 7.3.1自分の PP 側 IP アドレス設定コマンド、7.3.2相手の PP 側 IP アドレス設定コマンドを参照。

[デフォルト値] **off**

11.11.3 パラメータ ipcp-restart の設定

[入力形式] **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

11.11.4 パラメータ ipcp-max-terminate の設定

[入力形式] **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

11.11.5 パラメータ ipcp-max-configure の設定

[入力形式] **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

11.11.6 パラメータ ipcp-max-failure の設定

[入力形式] **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

11.11.7 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*

[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**

11.11.8 WINS サーバの IP アドレスの設定

[入力形式] 1. **wins server** *SERVER1 [SERVER2]*

2. **wins server clear**

[パラメータ]
- *SERVER1, SERVER2* ... *ip_address*(xxx.xxx.xxx.xxx(xxx は十進数))
- **clear** ... WINS サーバの IP アドレスを設定しない

[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] **clear**

11.12 IPXCP 関連の設定

11.12.1 パラメータ ipxcp-restart の設定

[入力形式] **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

11.12.2 パラメータ ipxcp-max-terminate の設定

[入力形式] **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

11.12.3 パラメータ ipxcp-max-configure の設定

[入力形式] **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

11.12.4 パラメータ ipxcp-max-failure の設定

[入力形式] **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

11.13 BCP 関連の設定

11.13.1 LAN Identification 使用の設定

[入力形式] **ppp bcp lanid** *lan_id*

[パラメータ]
- *lan_id*
  - 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**

11.13.2 Tinygram compression 使用の設定

[入力形式] **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**

11.13.3 パラメータ bcp-restart の設定

[入力形式] **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

11.13.4 パラメータ bcp-max-terminate の設定

[入力形式] **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

11.13.5 パラメータ bcp-max-configure の設定

[入力形式] **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

11.13.6 パラメータ bcp-max-failure の設定

[入力形式] **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

11.13.7 パラメータ mscbcp-restart の設定

[入力形式] **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

11.13.8 パラメータ mscbcp-maxretry の設定

[入力形式] **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

11.14 CCP 関連の設定

11.14.1 全パケットの圧縮タイプの設定

[入力形式] **ppp ccp type** *type*

[パラメータ] • *type*
- **stac** ... Stac LZS で圧縮する
- **cstac** ... Stac LZS で圧縮する (接続相手が Cisco ルータの場合)
- **3stac** ... Stac LZS で圧縮する (一部機器)
- **none** ... 圧縮しない

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

[ノート] Van Jacobson Compressed TCP/IP との併用も可能である。
接続相手が Cisco ルータの場合に Stac LZS を使用する場合には、必ず **cstac** を選択し、それ以外の相手との間で Stac LZS を使用する場合には **stac** を選択する。

[デフォルト値] **stac**

11.14.2 パラメータ ccp-restart の設定

[入力形式] **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

11.14.3 パラメータ ccp-max-terminate の設定

[入力形式] **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

11.14.4 パラメータ ccp-max-configure の設定

[入力形式] **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

11.14.5 パラメータ ccp-max-failure の設定

[入力形式] **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

11.15 MP 関連の設定

11.15.1 MP を使用するか否かの設定

[入力形式] **ppp mp use** *use*

[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。

[ノート] **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**

11.15.2 MP の制御方法の設定

[入力形式] **ppp mp control** *type*

[パラメータ]
- *type*
  - **arrive** ... 自分が 1B 目の着信側の時に 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 目の発信側の時に 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 目の発信側の時だけ制御するようにしておく。

[デフォルト値] **call**

11.15.3 MP のための負荷閾値の設定

[入力形式] **ppp mp load threshold** *call_load call_count disc_load disc_count*

[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時のデータ転送負荷の閾値を設定する。
負荷は回線速度に対する % で評価し、送受信で大きい方の値を採用する。*call_load* を超える負荷が *call_count* 回繰り返されたら 2B 目の発信を行なう。逆に *disc_load* を下回る負荷が *disc_count* 回繰り返されたら 2B 目を切断する。

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

11.15.4 MP の最大リンク数の設定

[入力形式] **ppp mp maxlink** *number*

[パラメータ]
- *number* ... リンク数 (1..16)

[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、使用モデルの BRI 回線数の 2 倍までとなる。

[デフォルト値] 2

11.15.5 MP の最小リンク数の設定

[入力形式] **ppp mp minlink** *number*

[パラメータ]
- *number* ... リンク数 (1..16)

[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

11.15.6 MP のための負荷計測間隔の設定

[入力形式] **ppp mp timer** *time*

[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

11.15.7 MP のパケットを分割するか否かの設定

[入力形式] **ppp mp divide** *divide*

[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。

[ノート] 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この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**

11.16 BACP 関連の設定

11.16.1 パラメータ bacp-restart の設定

[入力形式] **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

11.16.2 パラメータ bacp-max-terminate の設定

[入力形式] **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

11.16.3 パラメータ bacp-max-configure の設定

[入力形式] **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

11.16.4 パラメータ bacp-max-failure の設定

[入力形式] **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

11.16.5 パラメータ bap-restart の設定

[入力形式] **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

11.16.6 パラメータ bap-max-retry の設定

[入力形式] **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

12 DHCP の設定

YAMAHA リモートルータは DHCP[6] 機能として、DHCP サーバ機能と DHCP リレーエージェント機能を実装しています。DHCP クライアント機能は Windows 95 や Windows NT 等で実装されており、これらと YAMAHA リモートルータの 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。現在どのようになっているかは **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** コマンドで行ないます。IP アドレスのリース期間には時間指定と無期限の両方が可能であり、これは **dhcp scope** コマンドの **expire** 及び **maxexpire** キーワードのパラメータで指定します。リース状況は **show 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。

12.1 DHCP の動作の設定

[入力形式] **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
  - **off** ... サーバとしてもリレーエージェントとしても機能しない

[説明] DHCP に関する機能を設定する。

[ノート] 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] **off** ... RT200i, RT140p, RT140f, RT140i, RT140e, RT103i
server... RTA50i

[6] Dynamic Host Configuration Protocol; RFC1541

12.2 DHCP スコープの定義

[入力形式] **dhcp scope** *N IP–IP/mask* [**except** *ex_ip ...*] [**gateway** *gw_ip*] [**expire** *time*] [**maxexpire** *time*]

[パラメータ]
- *N* ... スコープ番号 (1..65535)
- *IP–IP* ... 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
- *mask* ... ネットマスク
  - xxx.xxx.xxx.xxx(xxx は十進数)
  - 0x に続く十六進数
  - マスクビット数
- *ex_ip* ... ip_address 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_address 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

12.3 DHCP スコープの削除

[入力形式] **dhcp delete scope** *scope_num*

[パラメータ]
- *scope_num* ... スコープ番号 (1..65535)

[説明] DHCP サーバとして使用する DHCP スコープ設定を削除する。

[ノート] 関連する予約情報も消去される。

12.4 DHCP 予約アドレスの設定

[入力形式] **dhcp scope bind** *scope_num ip_address mac_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
- *mac_address* ... XX:XX:XX:XX:XX:XX (XX は十六進数) 予約 DHCP クライアントの MAC アドレス

[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。
bind された IP アドレスは、たとえ DHCP スコープ中に他に割り当て可能な IP アドレスがなくなった場合でも、その対応する MAC アドレス以外のホストには割り当てられない。

[ノート] IP アドレスは、*scope_num* パラメータで指定された DHCP スコープ内にあるものでなければならない。ひとつの DHCP スコープ内では、ひとつの 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。

12.5 DHCP 予約アドレスの解除

[入力形式] **dhcp scope unbind** *scope_num ip_address*

[パラメータ]
- *scope_num* ... スコープ番号 (1..65535)
- *ip_address* ... 予約を解除する IP アドレス

[説明] IP アドレスの予約を解除する。

12.6 DHCP サーバの指定の設定

[入力形式] **dhcp relay server** *host1 [host2 [host3 [host4]]]*

[パラメータ]
- *host1 ... host4*
  - ip_address ... 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、あるいは一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。

12.7 DHCP サーバの選択方法の設定

[入力形式] **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 が指定された時は、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** が指定された時は、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**

12.8 DHCP BOOTREQUEST パケットの中継基準の設定

[入力形式] **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

12.9 DHCP オプションの設定

[入力形式] **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 オクテット整数の配列	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] **dhcp delete 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。

12.10 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*

[パラメータ]

- *CHECK1*
  - **on** ... LAN 内を対象とするチェックを行う
  - **off** ... LAN 内を対象とするチェックを行わない
- *CHECK2*
  - **on** ... 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う
  - **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とき、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* ... **on**
CHECK2 ... **on**

13 SNMP の設定

13.1 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*

[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**

13.2 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*

[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] **private**

13.3 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*

[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時にトラップを送信しない。これを受信するホストは **snmp trap host** コマンドで指定されたホスト。

[デフォルト値] **on**

13.4 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*

[パラメータ]
- *host*
  - ip_address ... SNMP によるアクセスを許可するホストの IP アドレス
  - **any** ... すべてのホストから SNMP によりアクセスできる
  - **none** ... すべてのホストから SNMP によりアクセスできない

[説明] SNMP によるアクセスを許可するホストを設定する。

[デフォルト値] **none**

13.5 sysContact の設定

[入力形式] **snmp syscontact** *name*

[パラメータ]
- *name* ... sysContact として登録する名称

[説明] YAMAHA リモートルータの管理者を表す MIB 変数 sysContact を設定する。
名称は 255 文字以内。空文字列可。

[デフォルト値] 空文字列

13.6 sysLocation の設定

[入力形式] **snmp syslocation** *name*

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

[説明] YAMAHA リモートルータの設置場所を表す MIB 変数 sysLocation を設定する。
名称は 255 文字以内。空文字列可。

[デフォルト値] 空文字列

13.7 sysName の設定

[入力形式] **snmp sysname** *name*

[パラメータ]
- *name* ... sysName として登録する名称

[説明] YAMAHA リモートルータの SNMP に対する管理上の機器名称を表す MIB 変数 sysName を設定する。
名称は 255 文字以内。空文字列可。

[ノート] このコマンドと同じように MIB 変数 sysName を設定するコマンドとして **sysname** コマンドがある。**sysname** コマンドの方が拡張されているので、そちらを使うことが望ましい。

[デフォルト値] 空文字列

13.8 送信トラップのコミュニティ名の設定

[入力形式] **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**

13.9 トラップの受信ホストの設定

[入力形式] **snmp trap host** *host*

[パラメータ]
- *host*
  - ip_address ... トラップを受信するホストの IP アドレス
  - **clear** ... トラップをどこにも送信しない

[説明] トラップを受信するホストを設定する。
clear の場合はどこにも送信しない。

[デフォルト値] **clear**

14 ICMP の設定

14.1 ICMP Echo Reply を送信するか否かの設定

[入力形式] **ip icmp echo-reply send** *send*

[パラメータ]
- *send*
  - **on** ... 送信する
  - **off** ... 送信しない

[説明] ICMP Echo Reply を出すか否かを設定する。

[デフォルト値] **on**

14.2 ICMP Mask Reply を送信するか否かの設定

[入力形式] **ip icmp mask-reply send** *send*

[パラメータ]
- *send*
  - **on** ... 送信する
  - **off** ... 送信しない

[説明] ICMP Mask Reply を出すか否かを設定する。

[デフォルト値] **on**

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

[入力形式] **ip icmp parameter-problem send** *send*

[パラメータ]
- *send*
  - **on** ... 送信する
  - **off** ... 送信しない

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

[デフォルト値] **on**

14.4 ICMP Redirect を送信するか否かの設定

[入力形式] **ip icmp redirect send** *send*

[パラメータ]
- *send*
  - **on** ... 送信する
  - **off** ... 送信しない

[説明] ICMP Redirect を出すか否かを設定する。

[デフォルト値] **on**

14.5 ICMP Redirect 受信時の処理の設定

[入力形式] **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 を受けた場合に処理するか無視するかを設定する。

[ノート] Rev.1.04.09 以前のリビジョンでは、今回のリビジョンのデフォルト動作と異なる。

[デフォルト値] **off**

14.6 ICMP Time Exceeded を送信するか否かの設定

[入力形式] **ip icmp time-exceeded send** *send*

[パラメータ]
- *send*
  - **on** ... 送信する
  - **off** ... 送信しない

[説明] ICMP Time Exceeded を出すか否かを設定する。

[デフォルト値] **on**

14.7 ICMP Timestamp Reply を送信するか否かの設定

[入力形式] **ip icmp timestamp-reply send** *send*

[パラメータ]
- *send*
  - **on** ... 送信する
  - **off** ... 送信しない

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

[デフォルト値] **on**

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

[入力形式] **ip icmp unreachable send** *send*

[パラメータ]
- *send*
  - **on** ... 送信する
  - **off** ... 送信しない

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

[デフォルト値] **on**

14.9 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*

[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**

15 RADIUS の設定

15.1 RADIUS サーバの指定

[入力形式] **radius server** *IP1 [IP2]*

[パラメータ]
- *IP1* ... RADIUS サーバ (正) の IP アドレス
- *IP2* ... RADIUS サーバ (副) の IP アドレス

[説明] RADIUS サーバを設定する。
副サーバは省略できる。

15.2 RADIUS 認証サーバの指定

[入力形式] 1. **radius auth server** *IP1 [IP2]*

2. **radius auth server clear**

[パラメータ]
- *IP1* ... RADIUS 認証サーバ (正) の IP アドレス
- *IP2* ... RADIUS 認証サーバ (副) の IP アドレス
- **clear**... 設定の消去

[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ときは、2 番目のサーバに問い合わせを行なう。

[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時は、**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。

15.3 RADIUS 認証サーバの UDP ポートの設定

[入力形式] **radius auth port** *port_number*

[パラメータ]
- port_number... UDP ポート番号

[説明] RADIUS 認証サーバの UDP ポート番号を設定する。

[ノート] 新しい RFC ではポート番号として 1812 を使うことになっている。

[デフォルト値] 1645

15.4 RADIUS アカウントサーバの指定

[入力形式] 1. **radius account server** *IP1 [IP2]*

2. **radius account server clear**

[パラメータ]
- *IP1* ... RADIUS アカウントサーバ (正) の IP アドレス
- *IP2* ... RADIUS アカウントサーバ (副) の IP アドレス
- **clear**... 設定の消去

[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ときは、2 番目のサーバに問い合わせを行なう。

[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時は、**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 UDP ポートの設定

[入力形式] **radius account port** *port_number*

[パラメータ]
- port_number... UDP ポート番号

[説明] RADIUS アカウントサーバの UDP ポート番号を設定する。

[ノート] 新しい RFC ではポート番号として 1813 を使うことになっている。

[デフォルト値] 1646

15.6 RADIUS シークレットの設定

[入力形式] **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。
空文字列を設定するときにはパラメータ部分に "" を入力する。

15.7 RADIUS 再送信パラメータの設定

[入力形式] **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

15.8 RADIUS による認証を使用するか否かの設定

[入力形式] **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時に、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] 認証において利用するアトリビュートとしては { User,Chap} -Password と Framed-IP-Address、それに Framed-Compression だけである。Framed-IP-Address は **ip pp remote address** コマンド相当として用いる。Framed-Compression は VJ-Compression のみ有効。その他のアトリビュートはたとえ RADIUS サーバから受信したとしても無視する。

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。

[デフォルト値] **off**

15.9 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*

[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。

STOP 時に次のアトリビュートを送信する。
ACCT_SESSION_TIME、ACCT_INPUT_PACKETS、
ACCT_INPUT_OCTETS、ACCT_OUTPUT_PACKETS、
ACCT_OUTPUT_OCTETS

それぞれの値は **show status pp** コマンドで表示されるものとは必ずしも一致していない可能性がある。

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。

[デフォルト値] **off**

16 NAT の設定

本章の NAT 機能は **RTA50i** に NAT を適用する場合のコマンドである。その他のモデルでは次章の NAT ディスクリプタ機能に記載のコマンドを使用する。

NAT[7]はグローバル IP アドレス空間とプライベート IP アドレス空間をつなぐための仕組みである。

プライベート空間からグローバル空間へ投げられるパケットは始点 IP アドレスとしてプライベートアドレスを持つが、 YAMAHA リモートルータの NAT 機能はそのパケットの始点 IP アドレスをグローバルアドレスに変換してからグローバル空間へ中継する。逆に、グローバル空間から投げられたパケットは終点 IP アドレスとしてグローバルアドレスを持っているが、それはプライベートアドレスに変換してからプライベート空間に投げる。

16.1 NAT を使うか否かの設定

[入力形式] **nat use** *use*

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

[説明] NAT を使用するか否かを設定する。

[ノート] NAT 機能使用時には、DHCP リレーエージェント機能を使用することはできない。

[デフォルト値] **off**

16.2 IP Masquerade を使用するか否かの設定

[入力形式] **nat masquerade** *use*

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

[説明] **on** にすると、複数のプライベート IP アドレスを一つのグローバル IP アドレスにまとめて通信できるようになる。

[ノート] **nat use on** に設定されていなければ機能しない。

[デフォルト値] **off**

[7] Network Address Translator;RFC1631

16.3 IP Masquerade 使用時に rlogin,rcp と ssh を許可するか否かの設定

[入力形式] **nat masquerade rlogin** *permit*

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

[説明] IP Masquerade 使用時に rlogin,rcp と ssh 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**

16.4 静的 IP Masquerade エントリの設定

[入力形式] **nat masquerade static** *id private_address proto port*

[パラメータ]
- *id* ... 1 以上の番号
- *private_address* ... プライベート空間のホストの IP アドレス
- *proto*
  - **tcp** ... TCP プロトコル
  - **udp** ... UDP プロトコル
- *port* ... ポート番号またはニーモニック

[説明] 静的 IP Masquerade エントリを設定する。この設定を行なうことにより、グローバルアドレス空間からプライベートアドレス空間へセッションを開始することができる。*id* パラメータはエントリを識別するための番号である。
グローバルアドレス空間から IP Masquerade で使用している IP アドレスの指定された *proto* の *port* に対してパケットが来た場合には、NAT と同様にアドレスだけを変換しポート番号は変換せずに、指定したプライベートアドレス空間側のホストへ中継される。

[ノート] 設定変更は、回線切断時に行なうことが望ましい。

[設定例] 192.168.0.0/24 のプライベートアドレスにおいて、端末型接続でインターネット接続している場合に WWW サーバである 192.168.0.2 を公開する場合。

```
# nat use on
# nat masquerade on
# nat masquerade static 1 192.168.0.2 tcp www
```

192.168.0.2 から CU–SeeMe を使えるようにする。

```
# nat use on
# nat masquerade on
# nat masquerade static 1 192.168.0.2 tcp 7648,7649
# nat masquerade static 2 192.168.0.2 tcp 7650-7652
# nat masquerade static 11 192.168.0.2 udp 7648
# nat masquerade static 12 192.168.0.2 udp 7649-7652
```

16.5 静的 IP Masquerade エントリの削除

[入力形式] **nat masquerade static delete** *id*

[パラメータ] • *id* ... 1 以上の番号

[説明] *id* パラメータで指定された静的 IP Masquerade エントリを削除する。

16.6 NAT のグローバル IP アドレスの設定

[入力形式] **nat address global** *global_range [global[=private] ...]*

[パラメータ] • *global_range*

- ip_address ... 1 つのグローバル IP アドレス
- ip_address – ip_address ... グローバル IP アドレスの範囲
- **ipcp** ... IPCP の IP アドレスオプションで割り当てられたアドレスをグローバル IP アドレスとして用いる。この場合、後続の引数は指定できない。

• *global, private*

- ip_address ... 結び付けるグローバル IP アドレスとプライベート IP アドレス。

[説明] NAT でグローバル IP アドレスとして扱うアドレスの範囲を指定する。
また、グローバル IP アドレスとプライベート IP アドレスを固定して結びつけることもできる。

[ノート] IP Masquerade が有効な時 (**nat masquerade on**) には、固定したプライベート IP アドレスを割り当てられていない最初のグローバル IP アドレスが IP Masquerade 用として使用される。

[デフォルト値] **ipcp**

16.7 NAT の対象とするプライベートアドレスの範囲の設定

[入力形式] **nat address private** *private*

[パラメータ] • *private*

- **auto** ... すべての IP アドレスをプライベート IP アドレスとして取り扱う
- ip_address... NAT の対象とする 1 つのプライベート IP アドレス
- ip_address – ip_address ...NAT の対象とするプライベート IP アドレスの範囲

[説明] NAT の対象とするプライベート IP アドレスの範囲を指定する。
このコマンドで指定されなかった IP アドレスは NAT の対象とはされず、通常のルーティングのルールに則って配送される。

[デフォルト値] **auto**

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 timer** *time*

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

[説明] 動的に生成されたグローバルアドレスとプライベートアドレスのマップを消去するまでの時間を設定する。
グローバルアドレスが **ipcp** である組も、回線が切断された時ではなく、このタイマにより組を消去する。

[デフォルト値] 900

16.9 動的に生成された NAT のグローバルアドレスとプライベートアドレスの組の消去

[入力形式] **clear nat dynamic**

[パラメータ] なし

[説明] NAT により動的に生成された全てのグローバルアドレスとプライベートアドレスの組を消去する。

16.10 NAT 関連の設定の表示

[入力形式] **show nat config** *[peer_number]*

[パラメータ]
- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は選択されている相手について表示する

[説明] 以下の項目が表示される。

- nat use
- nat masquerade
- nat address global
- nat address private
- nat timer

16.11 NAT のグローバルアドレスとプライベートアドレスのマップの表示

[入力形式] **show nat address** *[peer_number]*

[パラメータ]
- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は選択されている相手について表示する

[説明] グローバルアドレスとプライベートアドレスのマップを表示する。

17 NAT ディスクリプタ機能

本章の NAT ディスクリプタ機能は **RTA50i** 以外のモデルに NAT を適用する場合のコマンドである。**RTA50i** では前章の NAT 機能に記載のコマンドを使用する。

NAT ディスクリプタ機能は、従来の NAT 機能 (前章参照) の拡張であり、より汎用的、体系的に NAT 機能を利用するための枠組みを提供する。主な特徴は、より細かなアドレス変換規則を記述できることと、LAN インタフェースに対してアドレス変換規則を適用できることである。

アドレス変換規則を表す記述を NAT ディスクリプタと呼ぶ。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る。アドレス空間の記述には、**nat descriptor address inner**、**nat descriptor address outer** コマンドを用いる。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ある。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る。

NAT ディスクリプタは LAN インタフェース、PP インタフェースとトンネルインタフェースに適用することができる。LAN インタフェースに適用するときには **ip lan nat descriptor** コマンドを、PP インタフェースに適用するときには **ip pp nat descriptor** コマンドを、トンネルインタフェースに適用するときには **ip tunnel nat descriptor** コマンドを用いる。

NAT ディスクリプタは動作タイプ属性を持つ。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ときには、該当する動作タイプを選択する必要がある。

17.1 LAN 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]
1. **ip lan nat descriptor** *nat_descriptor_list*
2. **ip lan1 nat descriptor** *nat_descriptor_list*
3. **ip lan2 nat descriptor** *nat_descriptor_list*

[パラメータ]
- *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)
  - **clear**... NAT ディスクリプタを適用しない

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

[ノート] LAN 側に設定された 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。

[デフォルト値] **clear**

17.2 PP 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 pp nat descriptor** *nat_descriptor_list*

[パラメータ]
- *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)
  - **clear**... NAT ディスクリプタを適用しない

[説明] 適用された PP 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。

[デフォルト値] **clear**

17.3 トンネル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 tunnnel nat descriptor** *nat_descriptor_list*

[パラメータ]
- *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)
  - **clear**... NAT ディスクリプタを適用しない

[説明] 適用されたトンネル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。

[デフォルト値] **clear**

17.4 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*

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

[説明] NAT 変換の動作タイプを指定する。

[ノート] **none** は **nat use off** かつ **nat masquerade off** 相当。
nat は **nat use on** かつ **nat masquerade off** 相当。
masquerade は、**nat use on** かつ **nat masquerade on** に相当する。
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**

17.5 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*

[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)、及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 lan address** コマンドで設定されている IP アドレス
  - **secondary** ... **ip lan secondary address** コマンドで設定されている IP アドレス

[説明] **nat address global** コマンドに相当する。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以下の表のように意味が異なる。

	適用インタフェース	
	LAN	PP
ipcp	処理不可	ipcp
primary	処理可能	処理不可
secondary	処理可能	処理不可
IP アドレス	処理可能	処理可能

[デフォルト値] **ipcp**

17.6 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*

[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)、及びこれらを任意に並べたもの
  - **auto** ... 全て

[説明] **nat address private** コマンドに相当する。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。
適用されるインタフェースにより以下の表のように意味が異なる。

	適用インタフェース	
	LAN	PP
auto	all	all
IP アドレス	処理可能	処理可能

[デフォルト値] **auto**

17.7 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]*

[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。

17.8 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*

[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**

17.9 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*

[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
- *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なわないようにポートを固定する。

17.10 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*

[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

17.11 NAT ディスクリプタの削除

[入力形式] **nat descriptor delete** *nat_descriptor*

[パラメータ]
- *nat_descriptor* ... NAT ディスクリプタ番号 (1..21474836)

[説明] 指定された NAT ディスクリプタ番号の設定を削除 (初期化) する。

17.12 静的 NAT エントリの削除

[入力形式] **nat descriptor static delete** *nat_descriptor id*

[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)

[説明] 静的 NAT エントリを削除する。

17.13 静的 IP マスカレードエントリの削除

[入力形式] **nat descriptor masquerade static delete** *nat_descriptor id*

[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..21474836)

[説明] 静的 IP マスカレードエントリを削除する。

17.14 設定した NAT ディスクリプタの設定状態表示

[入力形式] **show nat descriptor config** *nat_descriptor*

[パラメータ]
- *nat_descriptor* ... NAT ディスクリプタ番号 (1..21474836)

[説明] NAT ディスクリプタの設定状態を表示する。

17.15 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
- *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

[説明] 動的な NAT ディスクリプタのアドレスマップを表示する。

17.16 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**

[パラメータ] なし

[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。

17.17 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]
1. **show nat descriptor interface address lan**
2. **show nat descriptor interface address lan1**
3. **show nat descriptor interface address lan2**

[パラメータ] なし

[説明] 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を表示する。

17.18 PP 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 pp** *peer_number*

[パラメータ]
- *peer_number*
  - 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
  - **leased** ... 専用線の時の設定

[説明] 指定した相手先情報番号の NAT ディスクリプタのアドレスマップを表示する。

17.19 トンネルインタフェースの 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 tunnnel** *tunnel_interface*

[パラメータ]
- *tunnel_interface* ... トンネルインタフェース番号 (1..20)

[説明] 指定したトンネルインタフェース番号の NAT ディスクリプタのアドレスマップを表示する。

[ノート] **RT103i** ではトンネルインタフェース数は 10 までである。

17.20 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。

17.21 LAN 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]
1. **clear nat descriptor interface dynamic lan**
2. **clear nat descriptor interface dynamic lan1**
3. **clear nat descriptor interface dynamic lan2**

[パラメータ] なし

[説明] LAN インタフェースの NAT アドレステーブルをクリアする。

17.22 PP 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 pp** *peer_number*

[パラメータ]
- *peer_number*
  - 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
  - **leased** ... 専用線の時の設定

[説明] 指定した相手先情報番号の NAT アドレステーブルをクリアする。

17.23 トンネルインタフェースの NAT アドレステーブルのクリア

[入力形式] **clear nat descriptor interface dynamic tunnel** *tunnel_interface*

[パラメータ]
- *tunnel_interface* ... トンネルインタフェース番号 (1..20)

[説明] 指定したトンネルインタフェースの NAT アドレステーブルをクリアする。

[ノート] **RT103i** ではトンネルインタフェース数は 10 までである。

18 DNS の設定

YAMAHA リモートルータは、DNS(Domain Name Service) 機能として名前解決とリカーシブサーバ機能を持ちます。ネームサーバとなることはできません。

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、YAMAHA リモートルータ宛に届いた DNS 問い合わせパケットを **dns server** コマンドで設定された DNS ネームサーバに中継します。最大 256 件のキャッシュを持ちます。

DNS の機能を使用するためには、**dns server** と **dns domain** コマンドの両方を設定しておく必要があります。また、この 2 つの設定は DHCP サーバ機能において、DHCP クライアントの設定情報にも使用されます。

18.1 DNS サーバの IP アドレスの設定

[入力形式] **dns server** *ip_address [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)
  - **clear**

[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] **clear**

18.2 DNS サーバを通知してもらう相手先情報番号の設定

[入力形式] **dns server pp** *peer_number*

[パラメータ]
- *peer_number*
  - DNS サーバを通知してもらう相手先情報番号
  - **none**

[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ときに、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] **none**

18.3 DNS ドメイン名の設定

[入力形式] **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及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。

18.4 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*

[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**

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

[入力形式] **dns notice order** *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** ... YAMAHA リモートルータ自身
  - **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 YAMAHA リモートルータ自身の 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** が続く時は先頭の 1 つだけと RT 自身を、**server** 単独で設定されている時には先頭の 2 つだけを通知する。

[デフォルト値] **dhcp me server**
msext me server

18.6 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*

[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**

18.7 静的 DNS レコードの登録

[入力形式] 1. **ip host** *fqdn value*

2. **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* ... 完全修飾ドメイン名 (Fully Qualified Domain Name の略)

[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 prt 133.176.200.2 pc2.yamaha.co.jp
# dns static cname mail.yamaha.co.jp mail2.yamaha.co.jp
```

18.8 静的 DNS レコードの削除

[入力形式] 1. **ip host delete** *fqdn*

2. **dns static delete** *type name*

[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* ... *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*
a	FQDN
ptr	IP アドレス
mx	FQDN
ns	FQDN
cname	FQDN

- *fqdn* ... 完全修飾ドメイン名 (Fully Qualified Domain Name の略)

[説明] 静的な DNS レコードを削除定義する。

18.9 静的 DNS レコードの表示

[入力形式] 1. **show ip host**

2. **show dns static**

[パラメータ] なし

[説明] 静的な DNS レコードを表示する。

19 アナログ通信機能の設定

アナログ通信機能を有するモデルは **RTA50i** のみであり、その他のモデルではこの機能は使用できません。**RTA50i** のアナログ通信機能の設定は、アナログポートに接続した PB 電話機のキー操作でも可能ですが、ここではコンソールからのコマンドについてだけ述べます。キー操作による設定手順は取扱説明書を参照してください。キー操作とコンソールコマンドの対応表は次ページに示します。

アナログ通信機能は、**RTA50i** が ISDN 回線に接続されている場合にだけ利用できます。高速ディジタル専用線やフレームリレー網に接続した場合には、アナログポートに接続したアナログ通信機器は内線通話以外は使用できません。

アナログポートにはさまざまなアナログ通信機器が接続できますが、これらの中で電話機なのか G2/G3 FAX なのかを区別して着信させることが可能です。ポートに接続する機器は **analog device type** コマンドで指定し、このコマンドによる設定と同じ機器からの着信だけに応答するか否かは、**analog arrive another-device permit** コマンドで設定します。また、発信時には、設定した機器種別の情報が付きます。

アナログポートには、識別着信リストと呼ぶリストがあり、このリストに一致した着信だけを許可したり拒否したりすることができます。識別着信リストへの登録は **analog arrive restrict list add** コマンド、削除は **analog arrive restrict list delete** コマンドで行ないます。実際の許可拒否動作はポート毎に行なうことができ、**analog arrive restrict** コマンドにより動作を指定します。

RTA50i のアナログポートへの着信ベル音は 3 種類あり、着信ベルリストへ登録することで呼び分けることができます。着信ベルリストへの登録は **analog arrive ringer-type list add** コマンド、削除は **analog arrive ringer-type list delete** コマンドで行ないます。着信許可された通信はこの着信ベルリストと照合され、設定された音種の着信ベル音を鳴らします。着信ベルリストのどれにも一致しない場合には通常の着信ベル音が使用されます。

RTA50i はフレックスホン機能[8]と、その一部機能を擬似的に行なう擬似フレックスホンをサポートします。フレックスホン機能は NTT の交換機側で提供される機能であり、擬似フレックスホン機能はそれと同様な機能を **RTA50i** のソフトウェアでシミュレーションします。これらの機能を使用するためには **analog supplementary-service** コマンドで NTT との契約形態を設定します。このコマンドで設定された機能だけが使用可能となります。

フレックスホン及び擬似フレックスホンの操作は、アナログ電話機による通話中にフッキングまたはその電話機のキー操作の組合せにより行ないます。具体的な操作方法は取扱説明書及び活用ガイドを参照してください。フッキング操作をユーザの好みに合わせたりするための各種タイマがあり、それらをコマンドにより調節することができます。詳しくは **analog wait dial timer**, **analog hooking timer**, **analog hooking wait timer**, **analog hooking inhibit timer**, の各コマンドの項を参照してください。

RTA50i のアナログポートの電気的入出力レベルは調節することができます。受話器からの音声が大きくてキンキンした音になったりモデムの通信がうまくいかない場合には、**analog pad send**, **analog pad receive** コマンドで送話と受話レベルをカット＆トライで調節します。

アナログ通信機能の設定は **show analog config** コマンドで確認することができます。また、アナログ通信機器だけの課金額や通話時間は **show analog account** コマンドで知ることができます。

[8] NTT との契約が必要な有料サービス。

19.1 キー操作とコンソールコマンドの対応

機能	機能番号	対応するコンソールコマンド
TEL ポートのダイヤル番号設定	11	**analog local address**
TEL ポートのサブアドレス設定	12	**analog local address**
通信機器の種類設定	13	**analog device type**
アナログポート使用制限の設定	14	**analog use**
発信者番号通知	21	**analog local address notice**
即時発信	22	**analog rapid call**
グローバル着信	31	**analog arrive global permit**
識別着信	32	**analog arrive restrict**
識別着信の番号登録	33	**analog arrive restrict list add**
サブアドレスなしの着信	34	**analog arrive without-subaddress permit**
通信機器種別指定の着信	35	**analog arrive another-device permit**
話中着信	36	**analog arrive ring-while-talking permit**
優先着信ポート	37	**analog arrive prior-port**
着信ベル設定	38	**analog arrive ringer-type list add**
ナンバー ・ディスプレイ機能	39	**analog arrive number display**
ダイヤル桁の間隔設定 (秒)	41	**analog wait dial timer**
フッキング判定時間 (1/10 秒)	42	**analog hooking timer**
フッキング後の操作有効時間 (秒)	43	**analog hooking wait timer**
フッキング, オンフック無効時間 (秒)	44	**analog hooking inhibit timer**
擬似切断信号の設定	45	**analog disc-signal**
コールウェイティング機能	52	**analog supplementary-service**
通信中転送機能	53	**analog supplementary-service**
三者通話機能	54	**analog supplementary-service**
着信転送機能	55	**analog supplementary-service**
着信転送先番号登録	56	**analog supplementary-service call-deflection address**
着信転送トーキ設定	57	**analog supplementary-service call-deflection talkie**
着信転送起動タイミング設定	58	**analog supplementary-service call-deflection ringer**
着信転送失敗時の動作設定	59	**analog supplementary-service call-deflection reject**
送話 PAD の音量設定	61	**analog pad send**, **analog pad send dte**
受話 PAD の音量設定	62	**analog pad receive**, **analog pad receive dte**
DTMF 検出レベルの設定	63	**analog dtmf level**
RVS-COM 着信の設定	64	**analog arrive dte permit**
アナログ呼び出し時間の設定 (秒)	65	**analog arrive dte timer**
LAN 側のルータ IP アドレス設定	71	**ip lan address**
LAN 側のネットマスク設定	72	**ip lan netmask**
BOD の設定	73	**analog mp prior**
i ・ナンバーの設定	81	**analog arrive inumber-port**
アナログポート設定の消去	91	—
識別着信の番号削除	92	**analog arrive restrict list delete**
着信ベルの番号削除	93	**analog arrive ringer-type list delete**
料金情報の消去	94	**clear analog account**
アナログポート設定の全消去	99	—
パスワードの設定	00	**login password**, **administrator password**

19.2 アナログポートを使うか否かの設定

[入力形式] **analog use** *port use*

[パラメータ]
- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *use*
  - **on** ... 発着信可能として使用する
  - **off** ... 使用しない
  - **call-only** ... 発信専用として使用
  - **arrive-only** ... 着信専用として使用

[説明] アナログポートを使用するか否かを設定する。**off** 以外にしないとアナログ通信機能は一切使用できない。

[デフォルト値] **on**

19.3 アナログポートの ISDN 番号の設定

[入力形式]
1. **analog local address** *port isdn_number/sub_address*
2. **analog local address** *port isdn_number*
3. **analog local address** *port /sub_address*
4. **analog local address** *port /*

[パラメータ]
- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *isdn_number* ... ISDN 番号
- *sub_address* ... ISDN サブアドレス (0x21 から 0x7e の ASCII 文字)

[説明] アナログポートの 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した方が良い。

[ノート] PB 電話機からの設定では、サブアドレスとして数字しか設定できない。

19.4 アナログポートに接続する機器の指定

[入力形式] **analog device type** *port type*

[パラメータ]
- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *type* ... 接続する機器の種類
  - **any** ... 通信機器の指定無し
  - **tel** ... 電話
  - **fax** ... G2/G3 FAX

[説明] アナログポートに接続する機器を指定する。
これを設定すると、*type* パラメータが **any** の場合には HLC をつけずに、それ以外では指定した HLC をつけて発信する。また着信時には *port* パラメータで指定したポートへは *type* パラメータで指定した以外の着信に応答しなくなる。

[デフォルト値] *type* = **any**

19.5 アナログポートの発信者番号を通知するか否かの設定

[入力形式] **analog local address notice** *port notice*

[パラメータ]
- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *notice*
  - **on** ... 通知する
  - **off** ... 通知しない

[説明] アナログポートに設定した発信者番号を相手に通知するか否かを設定する。
相手に通知される番号は **analog local address** コマンドで設定されたものである。

[ノート] 契約時に発信者番号通知サービスを選択しない場合には、常に通知されなくなる。

[デフォルト値] **off**

19.6 相手先番号による即時発信を許可するか否かの設定

[入力形式] **analog rapid call** *port rapid*

[パラメータ]

- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *rapid*
  - **on** ... 許可する
  - **off** ... 拒否する

[説明] 相手先番号による即時発信を許可するか否かを設定する。

[ノート] ダイヤル終了後、一定時間の経過を待たずに発信を開始することを即時発信と呼ぶ。即時発信の対象となるかどうかは、即時発信対象に登録されているか否かで判定される。

[デフォルト値] **on**

19.7 グローバル着信を許可するか否かの設定

[入力形式] **analog arrive global permit** *port permit*

[パラメータ]

- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *permit*
  - **on** ... 許可する
  - **off** ... 拒否する

[説明] グローバル着信を許可するか否かを設定する。

[ノート] グローバル着信の場合、着信時に着番号情報要素が着いてこない。グローバル着信を使用するためには、ダイヤルイン契約の際に利用指定が必要。

[デフォルト値] **on**

19.8 アナログポートでの識別着信をするか否かの設定

[入力形式] **analog arrive restrict** *port restrict*

[パラメータ]

- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *restrict*
  - **permit** ... 着信許可
  - **reject** ... 着信拒否
  - **none** ... 識別着信しない

[説明] アナログポートで識別着信をするか否かを設定する。
analog arrive restrict list add コマンドで登録された識別着信リストに対しての着信動作を決定する。**permit** の場合には、発番号が登録リストに含まれれば着信許可となり、それ以外は着信拒否となる。**reject** の場合には、発番号が登録リストに含まれれば着信拒否となり、それ以外は着信許可となる。**none** の場合には、全ての発番号に対して着信許可となる。

[デフォルト値] **reject**

19.9 識別着信リストの登録

[入力形式] **analog arrive restrict list add** *port number isdn_number/[sub_address]*

[パラメータ]

- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *number* ... 識別着信リストの登録番号
- *isdn_number* ... ISDN 番号
- *sub_address* ... ISDN サブアドレス (0x21 から 0x7e の ASCII 文字)

[説明] 識別着信用の ISDN 番号を識別着信リストへ登録する。

[ノート] 登録番号とは、識別着信リストの中で管理される通し番号である。また、識別着信リストはアナログポート毎に管理される個別のリストである。

19.10 識別着信リストの削除

[入力形式] **analog arrive restrict list delete** *port number*

[パラメータ]
- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *number* ... 識別着信用の登録番号

[説明] パラメータで指定された登録番号を識別着信リストから削除する。

19.11 サブアドレス無し着信を許可するか否かの設定

[入力形式] **analog arrive without-subaddress permit** *port permit*

[パラメータ]
- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *permit*
  - **on** ... 許可する
  - **off** ... 拒否する

[説明] サブアドレス情報要素の無い着信を許可するか否かを設定する。
analog local address コマンドを使用してポート毎に異なるサブアドレスを設定しておくと、ポートを区別して着信することが可能になる。

[ノート] 公衆電話や携帯電話からの着信にはサブアドレス情報要素が付いてこない。

[デフォルト値] **on**

19.12 異なる種類の通信機器からの着信を許可するか否かの設定

[入力形式] **analog arrive another-device permit** *port permit*

[パラメータ]
- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *permit*
  - **on** ... 許可する
  - **off** ... 許可しない

[説明] 異なる種類の通信機器からの着信を許可するか否かを設定する。

[ノート] 着信時の HLC 情報要素と **analog device type** コマンドにより設定された機器を比較して、着信整合性を調べる。

[デフォルト値] **on**

19.13 話中着信を許可するか否かの設定

[入力形式] **analog arrive ring-while-talking permit** *port permit*

[パラメータ]
- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *permit*
  - **on** ... 許可する
  - **off** ... 許可しない

[説明] 話中着信を許可するか否かを設定する。

[ノート] この設定が **on** になっていないと、フレックスホンのコールウェイティングも擬似コールウェイティングも使用できない。
Rev.3.02.21 からデフォルト値が **on** から **off** へ変更された。

[デフォルト値] **off**

19.14 優先着信機能の設定

[入力形式] **analog arrive prior-port** *port priority*

[パラメータ]
- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
  - **off** ... 平等に呼び出す
- *priority*
  - **1** ... 優先順位 1 位
  - **2** ... 優先順位 2 位
  - **3** ... 優先順位 3 位

[説明] どのポートを優先的に呼び出すかを設定する。

[ノート] TEL ポート間で優先順位の重複があっても構わない。すべての TEL ポートど同一優先順位に設定した場合、優先着信は行なわれずにすべての TEL ポートが呼び出される。

[デフォルト値] *priority* = **2**

19.15 着信ベルリストの登録

[入力形式] **analog arrive ringer-type list add** *port type number isdn_number/[sub_address]*

[パラメータ]
- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *type* ... 着信時のベル音の種類 (1,2)
- *number* ... リスト番号 (0..9)
- *isdn_number* ... ISDN 番号
- *sub_address* ... ISDN サブアドレス (0x21 から 0x7e の ASCII 文字)

[説明] 着信ベルリストを登録する。

[ノート] *type* パラメータで指定される着信ベル音の種類と、通常の着信時のベル音及び内線着信ベル音は異なる。

19.16 着信ベルリストの削除

[入力形式] **analog arrive ringer-type list delete** *port type number*

[パラメータ]
- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *type* ... 着信時のベル音の種類 (1..3)
- *number* ... リスト番号 (0..9)

[説明] パラメータで指定したリスト番号を着信ベルリストから削除する。

19.17 ダイヤル桁間タイマの設定

[入力形式] **analog wait dial timer** *port time*

[パラメータ]
- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *time* ... 秒数 (1..59)

[説明] ダイヤル桁間タイマ値を設定する。
ダイヤル中にこのタイマ値を越えてキー操作が無いと発信動作を開始する。秒数は 1 秒単位で設定できる。

[デフォルト値] 4

19.18 フッキングを判定する時間の設定

[入力形式] **analog hooking timer** *port time*

[パラメータ]
- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *time* ... 秒数 (0.5..2)

[説明] フッキングとして判断する最大の時間を設定する。
この時間を越えてアナログポートに接続された通信機器のフックスイッチを押し続けた場合はオンフックとみなして切断処理される。秒数は 0.1 秒単位で設定できる。

[デフォルト値] 1

19.19 フッキング後にキー操作を受け入れる時間の設定

[入力形式] **analog hooking wait timer** *port time*

[パラメータ]
- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *time*
  - 秒数 (1..9)

[説明] フッキング後にキー操作を受け入れる時間を設定する。
フレックスホン機能を利用するためのフック操作を行なった後、次のフッキングまたはオンフック操作を受け入れる時間である。秒数は 1 秒単位で設定できる。

[デフォルト値] 4

19.20 フッキング及びオンフック検出を無効と判断する時間の設定

[入力形式] **analog hooking inhibit timer** *port time*

[パラメータ]
- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *time*
  - 秒数 (1..3)
  - **off** ... 0 秒

[説明] 着信応答後から、フッキング及びオンフック検出を無効と判断する時間を設定する。秒数は 1 秒単位で設定できる。

[ノート] 着信応答後の数秒間、直流ループ断が発生するようなホームテレホン等を接続した場合に有効。通常は **off** でよい。

[デフォルト値] **off**

19.21 フレックスホン機能の使用パターンの設定

[入力形式]

1. **analog supplementary-service** [**network**] *func1 [func2 ... func6]*
2. **analog supplementary-service pseudo** *func1 [func2 ... func6]*
3. **analog supplementary-service clear**

[パラメータ]

- **network** ... 網提供のフレックスホンを示すキーワード
- *func1, func2, func3, func4, func5, func6*
  - **call-waiting** ... コールウェイティング機能使用を示すキーワード
  - **call-transfer** ... 通信中転送機能使用を示すキーワード
  - **add-on** ... 三者通話機能使用を示すキーワード
  - **call-deflection 1** ... TEL1 ポートでの着信転送機能使用を示すキーワード
  - **call-deflection 2** ... TEL2 ポートでの着信転送機能使用を示すキーワード
  - **call-deflection 3** ... TEL3 ポートでの着信転送機能使用を示すキーワード
- **pseudo** ... 擬似機能使用を示すキーワード
- **clear** ... 全ての機能を使用しない

[説明]　フレックスホン機能の使用パターンを設定する。

[ノート]　着信転送機能を実際に動作させるためには、着信転送先アドレスの設定 (**analog supplementary-service call-deflection address** コマンド) が必要。

[デフォルト値]　**pseudo call-waiting**

19.22 着信転送先アドレスの設定

[入力形式]　**analog supplementary-service call-deflection address** *port isdn_number / [sub_address]*

[パラメータ]

- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *isdn_number* ... ISDN 番号
- *sub_address* ... サブアドレス (0x21 から 0x7e の ASCII 文字)

[説明]　着信転送先アドレスを登録する。

[ノート]　網提供のフレックスホンによる着信転送では、サブアドレスの指定は無効となる。

19.23 着信転送トーキの設定

[入力形式] **analog supplementary-service call-deflection talkie** *port transfer originator*

[パラメータ]

- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *transfer* ... 転送トーキ
  - **on** ... あり
  - **off** ... なし
- *originator* ... 転送元トーキ
  - **on** ... あり
  - **off** ... なし

[説明] 着信転送におけるトーキのありなしを設定する。

[ノート] 転送トーキは、網提供の着信転送使用時に、転送される相手側で聞こえる音声ガイドであり、転送元トーキは、着信転送を起動した **RTA50i** のポートに接続した通信機器側で聞こえる音声ガイドのこと。
なお、擬似機能による着信転送使用時には転送トーキは無い。

[デフォルト値] *transfer* = **off**
originator = **off**

19.24 着信転送を起動するタイミングの設定

[入力形式] **analog supplementary-service call-deflection ringer** *port count*

[パラメータ]

- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *count*
  - 回数 (1..10) ... 指定回数着信ベルを鳴らした後に起動する
  - **off** ... 着信ベルを鳴らさずにすぐに起動開始する

[説明] 着信転送を起動するタイミングを設定する。
タイミングは 3 秒周期のリズムを 1 回とカウントする。

[デフォルト値] **off**

19.25 着信転送が拒否された時の動作の設定

[入力形式] **analog supplementary-service call-deflection reject** *port action*

[パラメータ]

- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *action*
  - **busy** ... 着信に対し、ビジートーン (話中) を返す
  - **alert** ... 着信に対して応答する

[説明] 着信転送を行おうとして、網からそれを拒否された時の動作を設定する。**busy** の場合には、着信に対しビジー (話中) を返すので、電話をかけてきた方にはビジートーンが返り、通話はできない。**alert** の場合には、呼出を返すと同時に手元の電話機のベルを鳴らすので、ここで受話器をとれば通話できる。

[デフォルト値] **alert**

19.26 送話 PAD の設定

[入力形式] **analog pad send** *port pad*

[パラメータ]

- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *pad*
  - **−3dB** ... 3dB PAD 挿入
  - **−6dB** ... 6dB PAD 挿入
  - **−9dB** ... 9dB PAD 挿入
  - **off** ... PAD なし

[説明] 送話 PAD を設定する。

[デフォルト値] **off**

19.27 受話 PAD の設定

[入力形式] **analog pad receive** *port pad*

[パラメータ]
- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *pad*
  - **−3dB** ... 3dB PAD 挿入
  - **−6dB** ... 6dB PAD 挿入
  - **−9dB** ... 9dB PAD 挿入
  - **off** ... PAD なし

[説明] 受話 PAD を設定する。

[デフォルト値] **off**

19.28 ナンバー・ディスプレイを使用するか否かの設定

[入力形式] **analog arrive number display** *port use*

[パラメータ]
- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *use*
  - **on** ... 使用する
  - **off** ... 使用しない

[説明] 指定したアナログポートでナンバー・ディスプレイを使用するか否かを設定する。

[デフォルト値] **off**

19.29 MP 時に電話発着信のために 1B チャネルに落すか否かの設定

[入力形式] **analog mp prior** *port down*

[パラメータ]

- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *down*
  - **on** ... 落す
  - **off** ... 落さない

[説明] MP 時に 2B チャネルでデータ通信中、電話の発着信を行なうためにデータ通信のチャネル数を 1B に落すか否かを設定する。

[デフォルト値] **on**

19.30 TEL ポートへの切断信号の送出の設定

[入力形式] **analog disc-signal** *port use*

[パラメータ]

- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *use*
  - **on** ... 使用する
  - **off** ... 使用しない

[説明] 指定したアナログポートで TEL ポートへの切断信号を送出するか否かを設定する。**on** に設定すると、発信側が先に通信を切断した場合に、極性反転して擬似的な切断信号をその TEL ポートへ送出する。

[デフォルト値] **on**

19.31 DTMF 検出レベルの設定

[入力形式] **analog dtmf level** *port level*

[パラメータ]
- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *level* ... 検出レベル dB(–30..0)

[説明] アナログポートの DTMF 信号検出レベルを設定する。

[デフォルト値] –18

19.32 受信 DTMF 信号の最小時間の設定

[入力形式] **analog dtmf minimum time** *port time*

[パラメータ]
- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *time* ... ミリ秒 (1..49)

[説明] 受信する DTMF 信号の最小時間を設定する。ここで設定した時間よりも短い DTMF 信号は受信しても無視される。

[ノート] あまり小さな時間に設定すると誤動作の原因となる。

[デフォルト値] 45

19.33 i ・ナンバーサービスのポート番号の設定

[入力形式]

1. **analog arrive inumber-port** *port [inum_port] [inum_port]*
2. **analog arrive inumber-port** *port* **all**
3. **analog arrive inumber-port** *port* **none**

[パラメータ]

- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート
- *inum_port* ... i ・ナンバーサービスのポート番号 (1, 2)
- **all** ... i ・ナンバーサービスのポート番号 1,2 両方を対応する
- **none** ... i ・ナンバーサービスのポート番号に対応させない

[説明]

i ・ナンバーサービスで網から送られるポート番号を、RTA50i のアナログポートに対応付ける。対応付けたポート番号が送られてきたら、そのアナログポートが着信を受ける。'all' を設定したときには、どのポート番号が送られてきても着信を受ける。'none' を設定したときには、どのポート番号が送られてきても着信を受けない。

[デフォルト値]

i ・ナンバーサービスのポート番号と同じ番号のアナログポートが着信を受ける。

20 メール着信確認機能の設定

メール着信確認機能を有するモデルは **RTA50i** のみであり、その他のモデルではこの機能は使用できません。この機能はプロバイダに新しいメールがあるかどうかを **RTA50i** が確認して、その結果を L1 LED を点滅させたり、ブラウザで確かめたりする機能です。

この機能に対応するプロバイダ等の最新情報については YAMAHA ISDN ホームページの情報をご覧ください。

メール着信の確認をするメールサーバは **mail-check server** コマンドで設定します。サーバは最大 4 つまで設定できます。

設定されたサーバに対して確認の実行を行なうには **mail-check go** コマンドを実行します。ブラウザからの設定では定期的に自動的に実行することも可能です。

未読のメールがあると、本体 L1 LED の点滅で知らせます。ブラウザを使用すれば具体的な未読の数も知ることができます。コンソールから実行結果を確かめるには、**show mail-check status** コマンドを実行します。L1 LED の点滅を止めるには **mail-check led off** コマンドを実行します。L1 LED は最後のチェック結果を表示しているだけ、ということに注意が必要です。また、L1 LED の点灯状態では回線の状態を表示してますが、点滅状態ではメールの着信確認だけに使用されているので、点滅を消すまで回線状態を知ることはできなくなります。

20.1 メールサーバの設定

[入力形式]

1. **mail-check server** *N destination* **pop3** *userid password [name]*
2. **mail-check server** *N* **clear**

[パラメータ]

- *N* ... サーバ番号 (1..4)
- *destination*
  - メールサーバの IP アドレス
  - ホスト名
  - **clear** ... メールサーバの宛先なし
- **pop3** ... メール通信プロトコル (POP3) を表すキーワード
- *userid* ... ユーザ ID(32 文字以内)
- *password* ... パスワード (32 文字以内)
- *name* ... 識別名 (32 文字以内)

[説明] メールサーバの IP アドレス等の情報を設定する。

20.2 メールチェックの実行

[入力形式] **mail-check go** *N*

[パラメータ]

- *N* ... サーバ番号 (1..4)

[説明] メールチェックを実行する。結果は L1 LED の点滅で知らされる。
実行後、10 分経過しないと再実行できない。

[ノート] 既に接続中のプロバイダにないメールサーバに対してこのコマンドを実行すると、パスワード情報などが暗号化されずにインターネット上に流れるので注意が必要。

20.3 メールチェックの実行を許可するか否かの設定

[入力形式] **mail-check prohibit** *N prohibit*

[パラメータ]
- *N* ... サーバ番号 (1..4)
- *prohibit*
  - **on** ... 実行禁止
  - **off** ... 実行許可

[説明] メール着信確認の実行を許可するか否かを設定する。

[デフォルト値] **off**

20.4 メールチェックによる LED の消灯

[入力形式] **mail-check led off** *[N]*

[パラメータ]
- **off** ... LED の消灯を表すキーワード
- *N* ... サーバ番号 (1..4) (省略時は全てのサーバ番号)

[説明] メール着信を通知する L1 LED の点滅を止める。

20.5 メールチェックの状態表示

[入力形式] **show mail-check status** *[N]*

[パラメータ]
- *N* ... サーバ番号 (1..4) (省略時は全てのサーバ番号)

[説明] 先のメールチェックの実行結果を表示する。

20.6 メールチェックタイムアウトの設定

[入力形式] **mail-check timeout** *N time*

[パラメータ]
- *N* ... サーバ番号 (1..4)
- *time* ... メール到着チェック時にタイムアウトするまでの秒数 (1..180)

[説明] メールチェックでのタイムアウトするまでの時間を設定する。メールサーバに対するアクセスに時間がかかる場合はこの値を大きくする。

21 RVS-COM 対応関連の設定

21.1 SERIAL ポートでの送話 PAD の設定

[入力形式] **analog pad send dte** *pad*

[パラメータ]
- *pad*
  - **−3dB** ... 3dB PAD 挿入
  - **−6dB** ... 6dB PAD 挿入
  - **−9dB** ... 9dB PAD 挿入
  - **off** ... PAD なし

[説明] RVS-COM で FAX/TEL 使用時の送話 PAD を設定する。

[デフォルト値] **off**

21.2 SERIAL ポートでの受話 PAD の設定

[入力形式] **analog pad receive dte** *pad*

[パラメータ]
- *pad*
  - **−3dB** ... 3dB PAD 挿入
  - **−6dB** ... 6dB PAD 挿入
  - **−9dB** ... 9dB PAD 挿入
  - **off** ... PAD なし

[説明] RVS-COM で FAX/TEL 使用時の受話 PAD を設定する。

[デフォルト値] **off**

21.3 SERIAL ポートでの着信を許可するか否かの設定

[入力形式] **analog arrive dte permit** *permit*

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

[説明] アナログの着信が来たときに SERIAL ポートで着信を受けるか否かを設定する。

[デフォルト値] **on**

21.4 アナログ機器を呼び出す時間の設定

[入力形式] **analog arrive dte timer** *time*

[パラメータ]
- *time*
  - アナログ機器を呼び出す秒数 (5..160)
  - **off** ... 即座に SERIAL ポートだけに着信させる

[説明] RVS-COM のために SERIAL ポートで着信を受けるまで、アナログポートの機器を呼び出す時間を指定する。指定時間後パソコンに着信させる。SERIAL ポートに接続された PC 上で RVS-COM が起動されていなければこの設定は無効。

[デフォルト値] 15

21.5 RVS-COM に関する設定の表示

[入力形式] **show analog config dte**

[パラメータ] なし

[説明] RVS-COM に関する設定を表示する。

22 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、という処理を行ないます。

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。

クラス分けの設定は、**show queue class filter** コマンドで確認することができます。

パケットの処理アルゴリズムは、**lan queue type** 及び **pp queue 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。キューの設定と状態は、**show lan queue** 及び **show pp queue** コマンドで確認することができます。

22.1 インタフェース速度の設定

[入力形式]
1. **lan speed** *speed*
2. **lan1 speed** *speed*
3. **lan2 speed** *speed*
4. **pp speed** *speed*

[パラメータ]
- *speed* ... インタフェース速度 (bit/s)

[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、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

22.2 クラス分けのためのフィルタ設定

[入力形式]

1. **queue class filter** *num class protocol src_addr [dest_addr[proto[src_port [dest_port]]]]*
2. **queue class filter** *num class protocol src_net[src_node[dst_net[dst_node[type [src_socket[dst_socket]]]]]]*
3. **queue class filter** *num class protocol src_mac[dst_mac[offset byte_list]]*

[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)
- *protocol* ... パケットのプロトコル
  - **ip**... IP パケット
  - **ipx**... IPX パケット
  - **bridge**... ブリッジするパケット
- *src_addr* ... IP パケットの始点 IP アドレス
  - xxx.xxx.xxx.xxx xxx は
    - 十進数
    - * (ネットマスクの対応するビットが 8 ビットとも 0 と同じ)
  - * (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_address* と同じ形式)。省略した時は一個の*と同じ。
- *proto* ... フィルタリングするパケットの種類
  - プロトコルを表す十進数
  - プロトコルを表すニーモニック

icmp	1
tcp	6
udp	17

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

  省略した時は*と同じ。

- *src_port* ... UDP、TCP のソースポート番号
  - ポート番号を表す十進数
  - ポート番号を表すニーモニック (一部)

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

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

  省略した時は*と同じ。
- *dest_port* ... UDP、TCP のデスティネーションポート番号
- *src_net* ... 始点 IPX ネットワーク番号
  - 0:0:0:1 ... FF:FF:FF:FE(2 桁以内の十六進数以外に '*' も指定可)
  - * (すべての IPX ネットワーク番号)
- *src_node* ... 始点 IPX ノード番号
  - 0:0:0:0:0:1 ... FF:FF:FF:FF:FF:FE(2 桁以内の十六進数以外に '*' も指定可)
  - *(すべての IPX ノード番号)

  省略した時は一個の*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
  - 十進数 (0..255)
  - 十六進数 (0x0..0xFF)
  - ニーモニック文字列

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

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

  省略した時は一個の*と同じ

- *src_socket* ... 始点ソケット番号
  - 十進数 (0..65535)
  - 0x を先頭に持つ 4 桁以内の十六進数
  - プロトコルを表すニーモニック

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

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

  省略した時は一個の*と同じ
- *dst_socket* ... 終点ソケット番号　　*src_socket* と同じ形式。
- *src_mac* ... 始点 MAC アドレス
  - XX:XX:XX:XX:XX:XX は
    - 十六進数
    - *
  - *(すべての MAC アドレスに対応)
- *dst_mac* ... 終点 MAC アドレス　　*src_mac* と同じ形式。省略した時は一個の*と同じ
- *offset* ... オフセットを表す十進数 (イーサネットフレームの始点 MAC アドレスの直後を 0 とするバイト数)
- *byte_list*
  - バイト列
    - XX(XX は 2 桁の十六進数)
    - 上項目のカンマで区切った並び (16 個以内)
  - *(すべてのバイト表現)

[説明]　クラス分けのためのフィルタを設定する。
IP パケットの場合は入力形式 1、IPX パケットの場合は入力形式 2、ブリッジパケットの場合は入力形式 3 で設定する。
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 class filter list** コマンドで設定する。

22.3 クラス分けフィルタの削除

[入力形式] **queue class filter delete** *filter_number*

[パラメータ]
- *filter_number* ... クラスフィルタの識別番号 (1..100)

[説明] 指定したクラス分けフィルタを削除する。

22.4 キューイングアルゴリズムタイプの選択

[入力形式]
1. **lan queue type** *type*
2. **lan1 queue type** *type*
3. **lan2 queue type** *type*
4. **pp queue type** *type*

[パラメータ]
- *type*
  - **fifo**... 優先制御/帯域制御なし (FIFO)
  - **priority** ... 優先制御キューイング
  - **cbq** ... 帯域制御キューイング

[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、キューイングアルゴリズムタイプを選択する。

[デフォルト値] **fifo**

22.5 デフォルトクラスの設定

[入力形式]
1. **lan queue default class** *class*
2. **lan1 queue default class** *class*
3. **lan2 queue default class** *class*
4. **pp queue default class** *class*

[パラメータ]
- *class* ... クラス (1..16)

[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、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

22.6 クラス分けフィルタの適用

[入力形式]

1. **lan queue class filter list** *filter_list*
2. **lan1 queue class filter list** *filter_list*
3. **lan2 queue class filter list** *filter_list*
4. **pp queue class filter list** *filter_list*

[パラメータ]

- *filter_list*
  - 空白で区切られたクラスフィルタの並び
  - **clear** (フィルタリングしない)

[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、**pp queue 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。

22.7 クラスの属性の設定

[入力形式]

1. **lan queue class property** *class* **bandwidth**=*value1* **parent**=*value2* **borrow**=*value3* **maxburst**=*value4* **minburst**=*value5* **packetsize**=*value6* **priority**=*value7*
2. **lan1 queue class property** *class* **bandwidth**=*value1* **parent**=*value2* **borrow**=*value3* **maxburst**=*value4* **minburst**=*value5* **packetsize**=*value6* **priority**=*value7*
3. **lan2 queue class property** *class* **bandwidth**=*value1* **parent**=*value2* **borrow**=*value3* **maxburst**=*value4* **minburst**=*value5* **packetsize**=*value6* **priority**=*value7*
4. **pp queue class property** *class* **bandwidth**=*value1* **parent**=*value2* **borrow**=*value3* **maxburst**=*value4* **minburst**=*value5* **packetsize**=*value6* **priority**=*value7*

[パラメータ]

- *class* ... クラス (1..16)
- **bandwidth** ... クラスに割り当てる帯域を示すキーワード
- *value1* ... 1 以上の整数 (bit/s 単位)
  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** ... 親クラスを示すキーワード
- *value2* ... クラス (0..16)
- **borrow** ... 帯域不足時に親クラスから帯域を借りるか否かを示すキーワード
- *value3*
  - **on** ... 借りる
  - **off** ... 借りない
- **maxburst** ... 連続送信できる最大パケット数を示すキーワード
- *value4* ... 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を示すキーワード
- *value5* ... 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を示すキーワード
- *value6* ... オクテット数 (1..10000)
- **priority** ... CBQ における優先順位を示すキーワード
- *value7* ... 優先順位 (1..8)

[説明]

指定したクラスの属性を設定する。

[ノート]

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、**lan speed**、**pp 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。
value2 パラメータで 0 はルートクラスを示す。
value7 パラメータは、優先制御で用いられるパラメータとは異なるので注意が必要。

[デフォルト値] *value2* = 0
value3 = **on**
value4 = 20
value5 = *value4* / 10
value6 = 512
value7 = 1

22.8 クラスの属性の削除

[入力形式]
1. **lan queue class property clear** *class*
2. **lan1 queue class property clear** *class*
3. **lan2 queue class property clear** *class*
4. **pp queue class property clear** *class*

[パラメータ]
- *class* ... クラス (1..16)

[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、指定したクラスの属性を削除する。

22.9 クラス毎のキュー長の設定

[入力形式]
1. **lan queue length** *len0 [len1 ... len15]*
2. **lan1 queue length** *len0 [len1 ... len15]*
3. **lan2 queue length** *len0 [len1 ... len15]*
4. **pp queue length** *len0 [len1 ... len15]*

[パラメータ]
- *len0...len15* ... 0 から 15 番目のクラスのキュー長

[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、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] 20

22.10 キュークラスフィルタの表示

[入力形式] **show queue class filter** *[filter_number]*

[パラメータ]
- *filter_number* ... クラスフィルタの識別番号 (1..100)

[説明] キュークラスフィルタを表示する。
filter_num パラメータを省略した場合は全てを表示する。

22.11 インタフェース毎のキューの表示

[入力形式]

1. **show lan queue** *[peer_number]*
2. **show lan1 queue** *[peer_number]*
3. **show lan2 queue** *[peer_number]*
4. **show pp queue** *[peer_number]*

[パラメータ]

- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**

[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、キューの設定および状態を表示する。

[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。

23 TA 機能

RTA50i では、SERIAL ポートにコンピュータなどを接続することにより TA として機能します。
TA 機能の設定は AT コマンドで行ないます。

AT コマンドモードからのコンソールコマンド入力状態にもどるためには AT&R コマンドを実行します。コンソールコマンド入力状態から AT コマンドの入力を行なうためには **serial ta** コマンドを実行します。

23.1 コンソールコマンド

23.1.1 AT コマンドモードへの移行

[入力形式] **serial ta**

[パラメータ] なし

[説明] AT コマンドモードへ切替える。

[ノート] 一般ユーザの使用可能。
シリアルポートからのアクセス以外では実行不可能。

23.1.2 コンソール速度の設定

[入力形式] **serial speed** *speed*

[パラメータ]
- *speed*
  - **2400** ... 2400bit/s
  - **4800** ... 4800bit/s
  - **9600** ... 9600bit/s
  - **19200** ... 19200bit/s
  - **38400** ... 38400bit/s
  - **57600** ... 57600bit/s
  - **115200** ... 115200bit/s
  - **230400** ... 230400bit/s

[説明] シリアルポートの速度を設定する。

[ノート] SERIAL ポートのコンソールから設定変更するとその後通信できなくなることに注意。
TELNET やリモートセットアップ、TFTP により変更することが望ましい。

[デフォルト値] **115200**

23.1.3 デフォルトのコンソールのタイプの指定

[入力形式] **serial default** *type*

[パラメータ]
- *type*
  - **console** ... コンソール
  - **ta** ... AT コマンド

[説明] デフォルトのコンソールのタイプを指定する。

[デフォルト値] **ta**

23.1.4 擬似 LAN 接続を許可するか否かの設定

[入力形式] **serial pseudo-lan** *pseudo-lan*

[パラメータ]
- *pseudo-lan*
  - **on** ... 許可
  - **off** ... 不許可

[説明] 擬似 LAN 接続を許可するか否かを設定する。

[デフォルト値] **on**

23.2 AT コマンド

A	
入力形式	ATA
パラメータ	なし
説明	着信に対して応答

D		
入力形式	ATD	
パラメータ	0-9, *, # /	着番号情報 or 着サブアドレス情報 サブアドレス区切子
	; N	選択信号送出後コマンドモードに遷移する 再ダイヤルする
	S=n	短縮番号 n に発信する (AT&Zn 参照)
	R	コールバック用の発信
	その他	全て無視する (エラーではない)
説明	指定された相手に発信	
設定例	03–123–4567 へダイヤルする→ ATD031234567	
	03–123–4567/123 へダイヤルする→ ATD031234567/123	
	再ダイヤルする → ATDN	
	短縮 3 番へダイヤルする → ATDS=3	

E		
入力形式	ATEn	
パラメータ	n=0 n=1	入力されたコマンドをエコーバックしない 入力されたコマンドをエコーバックする (default)
説明	コマンド入力に対するエコーの有無の指定	

H	
入力形式	ATH
パラメータ	なし
説明	切断復旧処理の起動

I		
入力形式	ATIn	
パラメータ	n=0	製品名表示
	n=1	ファームウェアのリビジョン表示
	n=2	製造メーカ名を表示する
	n=3	診断情報等の表示
説明	製品情報等の表示	

N		
入力形式	ATNn	
パラメータ	n=0	DTE 速度 (default)
	n=1	2400 bit/s
	n=2	4800 bit/s
	n=3	9600 bit/s
	n=4	19200 bit/s
	n=5	38400 bit/s
	n=6	57600 bit/s
説明	発信時の V.110 回線速度の指定	
ノート	DTE 速度を越える速度が指定された場合は ERROR となるので、 それ以下の速度の設定を改めて行なう必要がある。	

O	
入力形式	ATO
パラメータ	なし
説明	オンラインコマンドモードからオンラインデータ状態への遷移

Q		
入力形式	ATQn	
パラメータ	n=0	入力されたコマンドに対する応答あり (default)
	n=1	入力されたコマンドに対する応答なし
説明	コマンド入力に対する応答の有無の指定	

S		
入力形式	ATSr?	
パラメータ	r	S レジスタのレジスタ番号 ([S レジスタの詳細] 参照)
説明	S レジスタの値の表示	

S		
入力形式	ATSr=n	
パラメータ	r	S レジスタのレジスタ番号 ([S レジスタの詳細] 参照)
	n	S レジスタの値 ([S レジスタの詳細] 参照)
説明	S レジスタの値の設定	

V		
入力形式	ATVn	
パラメータ	n=0	数字形式 (numeric form) で出力
	n=1	文字形式 (verbose form) で出力 (default)
説明	リザルトコードと情報テキストの表示フォーマットの指定	
ノート	数字形式 / 文字形式の対応はリザルトコードセット表を参照	

W		
入力形式	ATWn	
パラメータ	n=0	通信速度表示には DTE 速度を使用
	n=2	通信速度表示には回線速度を使用 (default)
説明	CONNECT の通信速度の指定	

X		
入力形式	ATXn	
パラメータ	n=0	通信速度表示なし、BT 検出なし、DT 検出なし
	n=1	通信速度表示あり、BT 検出なし、DT 検出なし (default)
	n=2	通信速度表示あり、BT 検出なし、DT 検出あり
	n=3	通信速度表示あり、BT 検出あり、DT 検出なし
	n=4	通信速度表示あり、BT 検出あり、DT 検出あり
説明	CONNECT の通信速度表示とトーン検出の指定	
ノート	表示の詳細はリザルトコードセット表を参照	

Z	
入力形式	ATZ
パラメータ	なし
説明	シリアルポートのリセットとユーザプロファイルの読み出し

&C		
入力形式	AT&Cn	
パラメータ	n=0	常時 ON
	n=1	リモート DTE の RS 信号 (=受信キャリア) に応じて変化 (default)
説明	CD 信号線の制御	

&D		
入力形式	AT&Dn	
パラメータ	n=0	何もしない
	n=1	オンラインモードならばコマンドモードに遷移
	n=2	回線切断 (default)
	n=3	回線切断、シリアルポートのリセット
説明	DTR 信号の ON から OFF への変化に対する処理	

&F	
入力形式	AT&F
パラメータ	なし
説明	工場出荷設定に戻す

&K		
入力形式	AT&Kn	
パラメータ	n=0	なし
	n=1	RS/CS フロー制御 (default)
	n=2	XON/XOFF フロー制御
説明	DTE フロー制御	

&N		
入力形式	AT&Nn	
パラメータ	n=0	着信中に ON(default)
	n=1	着信から通信終了まで ON
	n=2	着信中に ON(1 秒) と OFF(2 秒) の繰り返し
説明	CI 信号線の制御	

&Q		
入力形式	AT&Qn	
パラメータ	n=0	V.110
	n=1	非同期/同期 PPP(default)
説明	発信時のプロトコル選択	

&R	
入力形式	AT&R
パラメータ	なし
説明	コンソールコマンド入力状態へ移行

&S		
入力形式	AT&Sn	
パラメータ	n=0	常時 ON (default)
	n=2	リモート DTE の DTR 信号に応じて変化
説明	DSR 信号線の制御	

&V		
入力形式	AT&Vn	
パラメータ	n=0	現在のパラメータと S レジスタの内容の表示
	n=1	ユーザプロファイルの内容の表示
説明	現在のパラメータとユーザプロファイルの内容の表示	

&W	
入力形式	AT&W
パラメータ	なし
説明	現在のパラメータをユーザプロファイルへ保存

&Z		
入力形式	AT&Zn=s	
パラメータ	n=0 ~ 9	短縮番号のインデックス
	s	短縮番号
	0-9、*、#	加入者番号情報 or サブアドレス情報
	/	サブアドレス区切子
	-、(、)	無視する (エラーではない)
説明	短縮番号の登録	
設定例	03–123–4567 を短縮 2 番に登録→ AT&Z2=031234567	

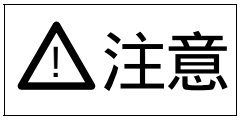
&Z		
入力形式	AT&Zn	
パラメータ	なし	0 ~ 9 の全ての登録番号表示
	n=0 ~ 9	0 ~ 9 の登録番号表示
説明	短縮番号の表示	

&Z		
入力形式	AT&Zn=	
パラメータ	n=0 ~ 9	0 ~ 9 の登録番号削除
説明	短縮番号の削除	

$A	
入力形式	AT$A
パラメータ	なし
説明	直前の通信料金の取り出し (下注参照)

$B	
入力形式	AT$B
パラメータ	なし
説明	累積通信料金表示 (下注参照)

$C	
入力形式	AT$C
パラメータ	なし
説明	直前の通信の切断コードの取り出し (下注参照)



電源 OFF や再起動により、それまでの課金情報やログ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。

$D	
入力形式	AT$D
パラメータ	なし
説明	累積通信料金の初期化

$G		
入力形式	AT$Gn	
パラメータ	n=0	グローバル着信しない
	n=1	グローバル着信する (default)
説明	グローバル着信の有無	

$H		
入力形式	AT$Hn	
パラメータ	n=0	HLC が異なる端末からの着信は受け付けない
	n=1	HLC が異なる端末からの着信も受け付ける (default)
説明	着信時における HLC による通信可能性確認の有無	

$I		
入力形式	AT$In	
パラメータ	n=0	着信しない
	n=1	着信する (default)
説明	自己アドレス登録時のサブアドレスなし着信の扱いの設定	

$L		
入力形式	AT$Ln	
パラメータ	n=0	発信アドレス情報なし (default)
	n=1	発信アドレス情報あり
	n=2	RVS–COM 用の表示形式
説明	着信時のリザルトコード RING の表示形式	

$M		
入力形式	AT$Mn	
パラメータ	n=0	MP 機能は使用不可 (default)
	n=1	MP 機能は使用可
説明	MP 機能使用の設定	

$N		
入力形式	AT$Nn	
パラメータ	n=0	スループット BOD 使用しない (default)
	n=1	スループット BOD 使用する
説明	スループット BOD の設定	

$P		
入力形式	AT$Pn	
パラメータ	n=0	発信者番号を通知しない
	n=1	発信者番号を通知する (default)
説明	発信者番号通知の有無	

$R		
入力形式	AT$Rn	
パラメータ	n=0	コールバック用の着信を受け付けない (default)
	n=1	コールバック用の着信を受け付ける
説明	コールバックの有無	

$S		
入力形式	AT$Sn	
パラメータ	n=0	識別着信しない (default)
	n=1	識別着信する
説明	識別着信の有無	

$V		
入力形式	AT$Vn	
パラメータ	n=0	制御キャラクタを 2 バイト文字に変換しない (default)
	n=1	制御キャラクタを 2 バイト文字に変換する
説明	非同期/同期 PPP 変換での制御キャラクタの 2 バイト文字変換	

$W		
入力形式	AT$Wn=s	
パラメータ	n=0 ~ 9	識別番号のインデックス
	s	識別番号
	0-9、*、#	着番号情報 or 着サブアドレス情報
	/	サブアドレス区切子
	-、(、)	無視する (エラーではない)
説明	識別番号の登録	
設定例	識別 2 番 03–123–4567/2 → AT$W2=031234567/2	

$W		
入力形式	AT$Wn	
パラメータ	なし	0 ~ 9 の全ての登録番号表示
	n=0 ~ 9	0 ~ 9 の登録番号表示
説明	識別番号の表示	

$W		
入力形式	AT$Wn=	
パラメータ	n=0 ~ 9	0 ~ 9 の登録番号削除
説明	識別番号の削除	

$Z		
入力形式	AT$Z=s	
パラメータ	s	自己アドレス
	0-9、*、#	加入者番号情報 or サブアドレス情報
	/	サブアドレス区切子
	-、(、)	無視する (エラーではない)
説明	自己アドレスの登録	
設定例	自己アドレス 03–123–4567/9 → AT$Z=031234567/9	

$Z	
入力形式	AT$Z
パラメータ	なし
説明	自己アドレスの表示

$Z	
入力形式	AT$Z=
パラメータ	なし
説明	自己アドレスの削除

@A		
入力形式	AT@A=s	
パラメータ	s	擬似 LAN 接続用番号
	0-9、*、#	番号
	-、(、)	無視する (エラーではない)
説明	擬似 LAN 接続用のダイヤル番号の登録	
デフォルト値	****	

@A	
入力形式	AT@A
パラメータ	なし
説明	擬似 LAN 接続用のダイヤル番号の表示

@A	
入力形式	AT@A=
パラメータ	なし
説明	擬似 LAN 接続用のダイヤル番号の削除

@B		
入力形式	AT@Bs	
パラメータ	s	DHCP または IP アドレス
	0.0.0.0	DHCP 使用 (default)
	xxx.xxx.xxx.xxx	IP アドレス
説明	擬似 LAN 接続時の IP アドレスの登録	

@C		
入力形式	AT@Cn	
パラメータ	n=0	コンソール
	n=1	AT コマンド (default)
説明	デフォルトのコンソールモードの設定	
ノート	起動時とログインタイマのタイムアウト時、ここで設定されているモードになる	

@D		
入力形式	AT@Dn	
パラメータ	n=0	DTE 使用不可
	n=1	2400bit/s
	n=2	4800bit/s
	n=3	9600bit/s
	n=4	19200bit/s
	n=5	38400bit/s
	n=6	57600bit/s
	n=7	115200bit/s(default)
	n=8	230400bit/s
説明	DTE 速度未検出時のデフォルト DTE 速度の指定	

@F		
入力形式	AT@Fn	
パラメータ	n=0	TA で着信しない
	n=1	TA で着信する (default)
説明	TA での着信の許可 / 不許可の指定	

@G		
入力形式	AT@G/u/p/	
パラメータ	u	ユーザ名 (32 文字以内)
	p	パスワード (32 文字以内)
	/	文字区切子 (任意の一文字が使用可能)
説明	MP 時の CHAP 認証のユーザ名とパスワードの設定	
ノート	ユーザ名やパスワード文字列の中に'/' が含まれる場合は、'=' や'?' 等の文字を区切子として使用する。	
設定例	ユーザ名 RTA50i、パスワード himitsu → AT@G/RTA50i/himitsu/ ユーザ名 RTA50i、パスワード (/123) → AT@G?RTA50i?(/123)?	

23.2.1 S レジスタの詳細

番号	設定範囲	単位	内容
0	0 1 ~ 255 (default:1)	 回	自動応答なし 指定回数の呼び出し後に自動応答
1	0 ~ 255 (default:0)	 回	呼出カウント (注 :read only、設定不可)
2	0 ~ 127 (default:43)	 (code)	エスケープシーケンスを構成する文字
3	0 ~ 127 (default:13)	 (code)	復帰文字 (終端文字)
4	0 ~ 127 (default:10)	 (code)	改行文字
5	0 ~ 127 (default:8)	 (code)	後退文字 (編集文字)
7	1 ~ 50 (default:30)	 秒	発信時相手応答待ち時間 (注 :総合ディジタル通信端末等の接続の技術的条件第 4 条)
10	0 ~ 255 (default:0)	 0.1 秒	キャリア断許容時間 (注 :キャリア=同期パターン/同期フラグ)
12	0 ~ 255 (default:50)	 20m 秒	エスケープシーケンスガードタイム
20	1 ~ 100 (default:70)	 %	スループット BOD で 2B チャネル目の接続を始める回線の負荷率 (回線速度に対する%値)。ATS20 を越える負荷が ATS21 回繰り返されると 2B チャネル目を接続。
21	1 ~ 100 (default:1)	 回	スループット BOD で 2B チャネル目の接続を始める回線の負荷率の回数。ATS20 を越える負荷が ATS21 回繰り返されると 2B チャネル目を接続。
22	1 ~ 100 (default:30)	 %	スループット BOD で 2B チャネル目の切断を始める回線の負荷率 (回線速度に対する%値)。ATS22 を下回る負荷が ATS23 回繰り返されると 2B チャネル目を切断。
23	1 ~ 100 (default:2)	 回	スループット BOD で 2B チャネル目の切断を始める回線の負荷率の回数。ATS22 を下回る負荷が ATS23 回繰り返されると 2B チャネル目を切断。
30	0 1 ~ 30 (default:10)	 分	自動切断しない 指定時間内にデータ送受信がなければ切断 (擬似 LAN 接続では無効)
38	0 ~ 255 (default:10)	 0.1 秒	DTR 許容断時間
42	0 ~ 255 (default:0)	 (bit 表現)	現在の DTE–TA 間速度とプロトコル (read only、設定不可)
43	0 ~ 255 (default:0)	 (bit 表現)	現在の TA–TA 間速度とプロトコル (read only、設定不可)
64	0 1 ~ 127 (default:0)	 (code)	データポート用の呼に HLC なし データポート用の呼に HLC あり (注 :JT-Q931 LLC の高位レイヤ特性識別)

番号	設定範囲	単位	内容
96	1 ~ 255 (default:60)	 秒	コールバック起動側での着信監視タイマ
97	0 1 ~ 255 (default:60)	 秒	コールバック被起動側ですぐ折り返し コールバック被起動側で折り返すまでの待ち時間

S レジスタの S64 の設定値の設定範囲は 10 進数で 0 から 127 までの全ての整数です。その中で決められているものだけを以下の表で示します。

10 進数	16 進数	意味
1	01	電話
4	04	Ｇ２／３ＦＡＸ
33	21	Ｇ４ＦＡＸ
49	31	テレテックス
50	32	ビデオテックス
53	35	テレックス
56	38	メッセージハンドリングシステム (ＭＨＳ)
65	41	ＯＳＩアプリケーション

23.2.2 リザルトコード詳細

数字形式、文字形式のリザルトコードセットによる違いを以下の表に示します。

ATX の設定		n=0	n=1	n=2	n=3	n=4
数字形式	文字形式					
0	OK	○	○	○	○	○
1	CONNECT	○	−	−	−	−
2	RING (注)	○	○	○	○	○
3	NO CARRIER	○	○	○	○	○
4	ERROR	○	○	○	○	○
6	NO DIALTONE	−	−	○	−	○
7	BUSY	−	−	−	○	○
10	CONNECT 2400	−	○	○	○	○
11	CONNECT 4800	−	○	○	○	○
12	CONNECT 9600	−	○	○	○	○
13	CONNECT 19200	−	○	○	○	○
14	CONNECT 38400	−	○	○	○	○
15	CONNECT 57600	−	○	○	○	○
16	CONNECT 64000	−	○	○	○	○
17	CONNECT 115200	−	○	○	○	○
18	CONNECT 128000	−	○	○	○	○
19	CONNECT 230400	−	○	○	○	○

注) AT$L0 に設定すると、文字形式での RING 表示の後ろの発信番号を省略できます。

24 操作

24.1 相手先情報番号の選択

[入力形式] **pp select** *peer_number*

[パラメータ]
- *peer_number*
  - 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
  - **leased** ... 専用線の時の設定

[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。
複数 WAN ポートモデルでは **leased** を指定することはできない。

24.2 トンネルインタフェース番号の選択

[入力形式] **tunnel select** *tunnel_number*

[パラメータ]
- *tunnel_number*
  - トンネルインタフェース番号 (1..20)
  - **none** ... トンネル先を選択しない

[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。以降プロンプトには、**console prompt** コマンドで設定した文字列とトンネルインタフェース番号が続けて表示される。
none を指定すると、プロンプトにトンネルインタフェース番号を表示しない。

[ノート] この操作コマンドは一般ユーザでも実行できる。
プロンプトが tunnel のときに PP 関係のコマンドは入力できない。
RT103i ではトンネルインタフェース数は 10 までである。

24.3 設定に関する操作

24.3.1 管理ユーザへの移行

[入力形式] **administrator**

[パラメータ] なし

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

24.3.2 設定内容の保存

[入力形式] 1. **save**

2. **save all** RTA50i

[パラメータ] なし

[説明] 現在の設定内容を不揮発性メモリに保存する。入力形式 2 は **RTA50i** でのみ使用可能。**RTA50i** で入力形式 1 を実行した場合、TA に関する設定及び **serial default** と **serial speed** コマンドの設定値は保存されない。

24.3.3 終了

[入力形式] 1. **quit**

2. **quit save**

3. **exit**

4. **exit save**

[パラメータ]
- **save** ... 管理ユーザから抜ける時に **save** を指定すると、設定内容を不揮発性メモリに保存して終了する

[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。

24.3.4 相手先の初期化

[入力形式] **pp default** *peer_number*

[パラメータ]
- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**

[説明] 指定した相手先の設定をデフォルト値にもどす。

[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。

24.3.5 トンネルインタフェースの初期化

[入力形式] **tunnel default** *tunnel_number*

[パラメータ]
- *tunnel_number*
  - トンネルインタフェース番号 (1..20)
  - **all** ... 全てのトンネルインタフェース

[説明] 指定したトンネル先の設定をデフォルト値にもどす。

[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。
RT103i ではトンネルインタフェース数は 10 までである。

24.3.6 相手先毎の設定の複写

[入力形式] **pp copy** *peer_number1 peer_number2*

[パラメータ]
- *peer_number1, peer_number2*
  - 相手先情報番号
  - **anonymous**

[説明] *peer_number1* の設定内容を *peer_number2* の設定に複写する。経路情報テーブルの内容は複写されない。

24.3.7 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、設定を保存した後再起動する。
コマンド実行時に管理パスワードを問い合わせる。

24.3.8 遠隔地のルータの設定

[入力形式]
1. **remote setup** *isdn_number*/*sub_address* [**dlci**=*dlci_num*] ... RT103i,RTA50i
2. **remote setup** *isdn_number* [**dlci**=*dlci_num*] ... RT103i,RTA50i
3. **remote setup bri** *isdn_number*/*sub_address* [**dlci**=*dlci_num*]
4. **remote setup bri** *isdn_number* [**dlci**=*dlci_num*]
5. **remote setup** *pri/info* ... RT140p

[パラメータ]
- *isdn_number* ... ISDN 番号
- *sub_address* ... ISDN サブアドレス (0x21 から 0x7e の ASCII 文字)
- *dlci_num* ... DLCI 番号
- *bri* ... BRI 番号
- *pri* ... PRI 番号 (1)
- *info* ... 情報チャネル番号 (1..24)

[説明] 遠隔地のルータの設定をする。

[ノート] 専用線またはフレームリレー接続の場合には *isdn_number* 及び *sub_address* パラメータは不要である。
フレームリレー接続の場合は、遠隔地のルータを特定するための DLCI の指定が必要。
PRI 回線に接続されたルータの場合は、 [入力形式] の 5 番目を使用する。事前に PRI 関連の **pri leased channel** コマンドと **pp bind pri** コマンドが設定済みでなければならない。
RTA50i の場合は、管理パスワードが設定されている必要がある。

24.3.9 遠隔地のルータからの設定に対する制限

[入力形式] 1. **remote setup accept** *isdn_number/sub_address*

2. **remote setup accept** *isdn_number [isdn_number_list]*

3. **remote setup accept any**

4. **remote setup accept none**

[パラメータ]
- *isdn_number* ... ISDN 番号
- *sub_address* ... ISDN サブアドレス (0x21 から 0x7e の ASCII 文字)
- *isdn_number_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。
相手先が 1 ヶ所の場合には、 [入力形式] の 1 または 2 番目の形式で設定する。

[デフォルト値] **any**

24.4 動的情報のクリア操作

24.4.1 ARP テーブルのクリア

[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。

24.4.2 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。

24.4.3 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。

24.4.4 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。

24.4.5 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 lan learning add** コマンドや、**bridge pp learning add** コマンドで設定したものは消去されない。

24.4.6 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。

24.4.7 アカウントのクリア

[入力形式] **clear account**

[パラメータ] なし

[説明] データ通信に関する合計アカウントと、全てのアナログポートのアカウントをクリアする。相手先情報番号ごとのアカウントとシリアルポートのアカウントはクリアされない。

24.4.8 相手先毎のアカウントの消去

[入力形式] **clear pp account** *[peer_number]*

[パラメータ]

- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は選択されている相手について消去する

[説明] 選択されている相手のアカウントを消去する。

24.4.9 アナログポートに関するアカウントのクリア

[入力形式] **clear analog account** *[port]*

[パラメータ]
- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート

[説明] 選択されているかまたは指定したアナログポートに関するアカウントをクリアする。*port* キーワードを省略した場合には、全てのアナログポートのアカウントがクリアされる。

24.4.10 InARP のクリア

[入力形式] **clear inarp** *[peer_number]*

[パラメータ]
- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は選択されている相手について表示する

[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。

24.4.11 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 リゾルバで持っているキャッシュをクリアする。

24.4.12 PRI のステイタス情報のクリア

[入力形式] **clear pri status** *pri*

[パラメータ]
- *pri* ...PRI 番号 (1)

[説明] PRI のステイタス情報をクリアする。

24.5 スケジュール

24.5.1 スケジュールの設定

[入力形式] **schedule at** *[date] time peer_number command*

[パラメータ]

- *date* ... 日付 省略可
  - 月/日
  - 省略した時は */* とみなす

月の指定例	意味
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

日の指定例	意味
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_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
  - *peer_number* を省略した時は相手先情報番号を指定しないという意味になる
  - *(実行するコマンドが *peer_number* を指定する必要が無い場合)
- *command* ... 実行するコマンド 制限あり

[説明] *time* で指定した時刻に *peer_number* で指定した相手先に *command* を実行する。**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コマンドを設定した順番に実行される。実行順は **show schedule** コマンドで確認する。
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, pp copy, pp default, pp line, 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なうが、シンタックスエラーなどは実行時まで検出されない。**schedule at** コマンドにより指定されたコマンドを実行する時には、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時などに便利。

[設定例] 1. ウィークデイの 8:00 ~ 17:00 だけ接続を許可する

```
# schedule at */mon-fri 8:00 1 isdn auto connect on
# schedule at */mon-fri 17:00 1 isdn auto connect off
# schedule at */mon-fri 17:05 * disconnect 1
```

2. 毎時 0 分から 15 分間だけ接続を許可する

```
# schedule at *:00 1 isdn auto connect on
# schedule at *:15 1 isdn auto connect off
# schedule at *:15 * disconnect 1
```

3. 今度の元旦にルーティングを切替える

```
# schedule at 1/1 0:0 1 ip pp route delete NETWORK
# schedule at 1/1 0:0 2 ip pp route add net NETWORK 1
```

24.5.2 スケジュールの削除

[入力形式] **schedule delete** *schedule_number*

[パラメータ] • *schedule_number* ... スケジュール番号

[説明] スケジュール番号で示されるスケジュールを削除する。
スケジュール番号は **show schedule** コマンドで表示される番号。

24.5.3 スケジュールの確認

[入力形式] **show schedule**

[パラメータ] なし

[説明] スケジュールをスケジュール番号とともに表示する。

24.6 その他の操作

24.6.1 相手先の使用許可の設定

[入力形式] **pp enable** *peer_number*

[パラメータ]
- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
  - **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、使用する時は必ずこのコマンドで **enable** 状態にしなければならない。

[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。

24.6.2 相手先の使用不許可の設定

[入力形式] **pp disable** *peer_number*

[パラメータ]
- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
  - **all**

[説明] 相手先を使用できない状態にする。
相手先の設定を行なう時は **disable** 状態であることが望ましい。

[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。

24.6.3 BRI インタフェースの使用許可の設定

[入力形式] **bri enable** *bri*

[パラメータ]
- *bri* ... BRI 番号

[説明] BRI インタフェースを使用できる状態にする。
工場出荷時、複数 WAN ポートモデルの BRI インタフェースは **disable** 状態なので、使用する時は必ずこのコマンドで **enable** 状態にしなければならない。

24.6.4 BRI インタフェースの使用不許可の設定

[入力形式] **bri disable** *bri*

[パラメータ]
- *bri* ... BRI 番号

[説明] BRI インタフェースを使用できない状態にする。
相手先の設定を行なう時は **disable** 状態であることが望ましい。

24.6.5 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_number*

[パラメータ]
- *tunnel_number*
  - トンネルインタフェース番号 (1..20)
  - **all** ... 全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、すべてのトンネルインタフェースは **disable** 状態なので、使用する時は必ずこのコマンドで **enable** 状態にしなければならない。
RT103i ではトンネルインタフェース数は 10 までである。

24.6.6 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_number*

[パラメータ]
- *tunnel_number*
  - トンネルインタフェース番号 (1..20)
  - **all** ... 全てのトンネルインタフェース

[説明] トンネルインタフェースを使用できない状態にする。
トンネル先の設定を行なう時は **disable** 状態であることが望ましい。
RT103i ではトンネルインタフェース数は 10 までである。

24.6.7 再起動

[入力形式] **restart**

[パラメータ] なし

[説明] ルータを再起動する。

[ノート] コンソールから、または TFTP により回線種別を切替える設定を行なった場合には再起動が必要となる。

24.6.8 発信

[入力形式] **connect** *peer_number*

[パラメータ]
- *peer_number* ... 発信相手の相手先情報番号

[説明] 手動で発信する。

24.6.9 切断

[入力形式] **disconnect** *peer_number*

[パラメータ]
- *peer_number*
  - 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。

24.6.10 ping

[入力形式] **ping** *host [count]*

[パラメータ]
- *host*
  - ip_address ... ping をかけるホストの IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))
  - ping をかけるホストの名称
- *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_REQUEST を指定したホストに送出し、ICMP ECHO_RESPONSE 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。

24.6.11 traceroute

[入力形式] **traceroute** *host [***noresolv***]*

[パラメータ]
- *host*
  - ip_address ... traceroute をかけるホストの IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))
  - traceroute をかけるホストの名称

[説明] 指定したホストまでの経路を調べて表示する。キーワード **noresolv** を指定した場合には、DNS による解決を行なわない。

24.6.12 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*
  - ip_address ... リモートホストの IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))
  - ホストの名称
- **syslog** ... 出力結果を SYSLOG へ出力することを表すキーワード

[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。

[ノート] YAMAHA リモートルータ及び、ほとんどの 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。

24.6.13 NTP による時計の設定

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

[パラメータ]
- *ntp_server*
  - ip_address ... NTP サーバの IP アドレス (xxx.xxx.xxx.xxx (xxx は十進数))
  - NTP サーバの名称
- **syslog** ... 出力結果を SYSLOG へ出力することを表すキーワード

[説明] NTP を利用してルータの時計を設定する。

[ノート] インターネットに接続している時には、**rdate** コマンドを使用した場合よりも精密な時計合わせが可能になる。NTP サーバとしてはできるだけ近くの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 リモートルータ自身は NTP サーバとはなれない。
syslog キーワードを指定した場合には、コマンドの出力結果を INFO レベルの SYSLOG へ出力する。

24.6.14 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
  - 十進数
  - 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
  - **charactor** ... 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
  - 十進数の ASCII コード
  - 省略時は 29(^])

[説明] TELNET クライアントを実行する。

[ノート] **charactor** 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なう。行編集の終了は、改行コード (CR:0x0d または LF:0x0a) の入力で判断する。

ポート番号による機能自動選択について。

1. telnet 通信の動作モードの自動選択

   port 番号が 23 の場合は文字単位モードとなり、そうでない場合は行単位モードとなる。

2. telnet オプションのネゴシエーションの自動選択

   port 番号が 23 の場合はネゴシエーションし、そうでない場合はネゴシエーションしない。

[デフォルト値] *port* = 23
mode = **auto**
negotiation = **auto**
abort = 29 (^])

24.6.15 PRI のループバックの実行

[入力形式] 1. **pri loopback active** *pri* **a** *data*

2. **pri loopback active** *pri* **timeslot** *head num data*

[パラメータ]
- *pri* ...PRI 番号 (1)
- **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)
- *num* ... 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時に、管理パスワードを入力する必要がある。
キーワード **a** 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。
キーワード **timeslot** 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なう必要がある。
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。

24.6.16 PRI のループバック待ち受けの設定

[入力形式]

1. **pri loopback passive** *pri* **remote**
2. **pri loopback passive** *pri* **payload**
3. **pri loopback passive** *pri* **timeslot** *head num*
4. **pri loopback passive off**

[パラメータ]

- *pri* ...PRI 番号 (1)
- **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)
- *num* ... 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時に、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。
キーワード **remote** 及び **payload** 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。
キーワード **timeslot** 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。
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。

25 設定の表示

25.1 機器設定の表示

25.1.1 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
- イーサネットアドレス
- メモリの使用量 (%)
- date, time, timezone
- sysname
- security class
- remote setup accept
- login timer
- console speed
- console character
- console columns
- console lines
- console info
- account threshold
- leased keepalive log ... RT200i, RT140p, RT140f, RT140i, RT140e

25.1.2 SYSLOG 関連の表示

[入力形式] **show syslog**

[パラメータ] なし

[説明] 以下の項目が表示される。

- syslog host
- syslog facility
- 出力する SYSLOG のタイプ

25.1.3 TFTP 関連の表示

[入力形式] **show tftp**

[パラメータ] なし

[説明] 以下の項目が表示される。

- tftp host

25.1.4 すべての設定内容の表示

[入力形式] 1. **show config**

2. **less config**

[パラメータ] なし

[説明] システムのリビジョンとイーサネットアドレスを表示した後、デフォルト以外に設定されたすべての設定内容を表示する。

25.1.5 指定した PP の設定内容の表示

[入力形式] 1. **show config pp** *[peer_number]*

2. **less config pp** *[peer_number]*

[パラメータ]

- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は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。

[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。

25.1.6 PP 毎の設定内容の表示

[入力形式] **show pp config** *[peer_number]*

[パラメータ]

- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は選択されている相手について表示する

[説明] 以下の項目が表示される。

- pp bind bri ... RT200i, RT140p, RT140f, RT140i, RT140e
- pp queue length
- account threshold
- pp encapsulation

[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。

25.2 相手先一覧の表示

25.2.1 相手先一覧の表示

[入力形式] **show remote list**

[パラメータ] なし

[説明] 設定されている相手先情報番号と ISDN 番号、サブアドレスを表示する。

25.3 ISDN 関連の表示

25.3.1 自分側設定の表示

[入力形式]

1. **show isdn local** ... RT103i,RTA50i
2. **show isdn local** *bri*

[パラメータ]

- *bri* ... BRI 番号

[説明] 以下の項目が表示される。

- pp line
- bri terminator ... RT200i
- isdn local address

25.3.2 相手側設定の表示

[入力形式] **show isdn remote** *[peer_number]*

[パラメータ]

- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は選択されている相手について表示する

[説明] 以下の項目が表示される。

- pp bind bri ... RT200i, RT140p, RT140f, RT140i, RT140e
- isdn remote address
- isdn bulk
- isdn remote call order ... RT200i, RT140p, RT140f, RT140i, RT140e

以下の項目の内、有効なもののリスト。

- isdn auto connect
- isdn callback request
- isdn callback permit
- isdn arrive permit
- isdn call permit

以下のタイマ値等

- isdn call block time
- isdn call prohibit time
- isdn callback wait time
- isdn callback response time
- isdn disconnect time
- isdn disconnect input time
- isdn disconnect output time
- isdn fast disconnect time
- forced disconnect time
- isdn disconnect interval time
- leased keepalive use ... RT200i, RT140p, RT140f, RT140i, RT140e
- leased keepalive interval
- leased keepalive down
- leased backup

[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。

25.4 フレームリレー関連の表示

25.4.1 PP 側フレームリレー設定の表示

[入力形式] **show fr** *[peer_number]*

[パラメータ]
- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は選択されている相手について表示する

[説明] フレームリレー関連の設定内容を表示する。

25.4.2 DLCI の表示

[入力形式] **show dlci** *[peer_number]*

[パラメータ]
- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は選択されている相手について表示する

[説明] DLCI の値及び InARP の状態を表示する。
InARP が成功していれば相手の IP アドレスも表示される。

25.5 IP 関連の表示

25.5.1 IP パケットのフィルタの一覧表示

[入力形式] **show ip filter list**

[パラメータ] なし

[説明] IP パケットのフィルタの一覧を表示する。

25.5.2 IP パケットのフィルタの表示

[入力形式] **show ip filter** *filter_number*

[パラメータ]
- *filter_number* ... フィルタの番号 (1..100)

[説明] パラメータで指定した番号の IP パケットのフィルタの内容を表示する。

25.5.3 LAN 側 IP 設定の表示

[入力形式] 1. **show ip lan**

2. **show ip lan1**

3. **show ip lan2**

[パラメータ] なし

[説明] 以下の項目が表示される。

- ip routing
- ip lan address
- ip lan netmask
- ip lan broadcast
- ip lan proxyarp
- ip lan secure filter
- ip filter source-route
- ip lan routing protocol

ip lan routing protocol で **rip** が選択されている場合には、さらに以下の項目が表示される。

- ip lan rip filter
- ip lan rip listen

25.5.4 IP パケットの TOS フィールドの書き換え設定の表示

[入力形式] **show ip tos supersede**

[パラメータ] なし

[説明] IP パケットの TOS フィールドの書き換え設定について表示する。

25.5.5 PP 側 IP 設定の表示

[入力形式] **show ip pp** *[peer_number]*

[パラメータ]
- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は選択されている相手について表示する

[説明] 以下の項目が表示される。

- pp disable / pp enable の区別
- ip routing
- ip pp local address
- ip pp remote address
- ip pp netmask
- ip pp secure filter
- ip filter source-route
- ip pp routing protocol

ip pp routing protocol で **rip** が選択されている場合には、さらに以下の項目が表示される。

- ip pp rip connect send
- ip pp rip disconnect send
- ip pp rip disconnect interval ... **ip pp rip disconnect send** で **interval** が選択されている時のみ表示される。
- ip pp rip filter
- ip pp rip listen
- ip pp rip hop
- ip pp hold routing

[ノート] IP アドレスは、ネゴシエーションで決定されたアドレスと、**ip pp local address**、**ip pp remote address** コマンドで設定したアドレスの両方を表示する。後者は小括弧で示される。
複数 WAN ポートモデルでは **leased** を指定することはできない。

25.6 IPX 関連の表示

25.6.1 IPX パケットのフィルタの一覧表示

[入力形式] **show ipx filter list**

[パラメータ] なし

[説明] IPX パケットのフィルタの一覧を表示する。

25.6.2 IPX パケットのフィルタの表示

[入力形式] **show ipx filter** *filter_number*

[パラメータ] • *filter_number* ... フィルタの番号 (1..100)

[説明] パラメータで指定した番号の IPX パケットのフィルタの内容を表示する。

25.6.3 LAN 側 IPX 設定の表示

[入力形式] 1. **show ipx lan**

2. **show ipx lan1**

3. **show ipx lan2**

[パラメータ] なし

[説明] 複数 LAN ポートモデルでは [入力形式] の 2 または 3 番目の形式で設定する。
以下の項目が表示される。

- ipx routing
- ipx lan frame type
- IPX ネットワーク番号
- IPX ノード番号
- ipx lan secure filter
- ipx lan ripsap broadcast
- ipx sap response

25.6.4 PP 側 IPX 設定の表示

[入力形式] **show ipx pp** *[peer_number]*

[パラメータ]
- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は選択されている相手先について表示する

[説明] 以下の項目が表示される。

- pp enable / pp disable の区別
- ipx routing
- ipx pp routing
- IPX ネットワーク番号
- IPX ノード番号
- ipx pp secure filter
- ipx pp serialization filter
- ipx pp ripsap connect send
- ipx pp ripsap connect interval
- ipx pp ripsap disconnect send
- ipx pp ripsap disconnect interval
- ipx pp ripsap hold
- ipx pp ipxwan use
- ipx pp ipxwan retry
- IPXWAN プライマリネットワーク番号
- ipx pp watchdog proxy
- ipx pp watchdog interval
- ipx pp spx keepalive proxy
- ipx pp spx keepalive timer

[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。

25.7 ブリッジ関連の表示

25.7.1 ブリッジのフィルタの一覧表示

[入力形式] **show bridge filter list**

[パラメータ] なし

[説明] ブリッジのフィルタの一覧を表示する。

25.7.2 ブリッジのフィルタの表示

[入力形式] **show bridge filter** *filter_number*

[パラメータ]
- *filter_number* ... フィルタの番号 (1..10)

[説明] パラメータで指定した番号のブリッジのフィルタの内容を表示する。

25.7.3 LAN 側ブリッジ設定の表示

[入力形式]
1. **show bridge lan**
2. **show bridge lan1**
3. **show bridge lan2**

[パラメータ] なし

[説明] 複数 LAN ポートモデルでは [入力形式] の 2 または 3 番目の形式で設定する。
以下の項目が表示される。

- bridge use
- bridge forwarding
- bridge learning
- bridge learning expire
- bridge lan filter

25.7.4 PP 側ブリッジ設定の表示

[入力形式] **show bridge pp** *[peer_number]*

[パラメータ]
- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は選択されている相手について表示する

[説明] 以下の項目が表示される。

- pp enable / pp disable の区別
- bridge use
- bridge forwarding
- bridge learning
- bridge learning expire
- bridge pp filter

[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。

25.8 PPP の設定の表示

25.8.1 認証関連の設定の表示

[入力形式] **show auth** *[peer_number]*

[パラメータ]
- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は選択されている相手について表示する

[説明] 指定した相手先番号に対する認証関連の設定を表示する。

[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。

25.8.2 LCP 関連の設定の表示

[入力形式] **show ppp lcp** *[peer_number]*

[パラメータ]
- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は選択されている相手について表示する

[説明] 以下の項目が表示される。

- ppp lcp magicnumber
- ppp lcp mru
- ppp lcp authreq
- ppp lcp pap accept
- ppp lcp chap accept

相手先として **leased** が選択されている時には以下の 4 つの情報が表示される。

- leased keepalive use
- leased keepalive log
- leased keepalive interval
- leased keepalive down

以下は共通に表示される。

- ppp lcp restart
- ppp lcp maxconfigure
- ppp lcp maxterminate
- ppp lcp maxfailure

[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。

25.8.3 PAP 関連の設定の表示

[入力形式] **show ppp pap** *[peer_number]*

[パラメータ]
- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は選択されている相手について表示する

[説明] 以下の項目が表示される。

- ppp pap restart
- ppp pap maxauthreq

[ノート] **ppp pap arrive only** コマンドで **on** に設定されている時にのみ、“PAP の要求” の後ろに “(着信のみ)” または “(arrive only)” と表示する。
複数 WAN ポートモデルでは **leased** を指定することはできない。

25.8.4 CHAP 関連の設定の表示

[入力形式] **show ppp chap** *[peer_number]*

[パラメータ]
- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は選択されている相手について表示する

[説明] 以下の項目が表示される。

- ppp chap restart
- ppp chap maxchallenge

[ノート] **ppp chap arrive only** コマンドで **on** に設定されている時にのみ、“CHAP の要求” の後ろに “(着信のみ)” または “(arrive only)” と表示する。
複数 WAN ポートモデルでは **leased** を指定することはできない。

25.8.5 IPCP 関連の設定の表示

[入力形式] **show ppp ipcp** *[peer_number]*

[パラメータ]
- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は選択されている相手について表示する

[説明] 以下の項目が選択されていると、それがオプションとして表示される。

- ppp ipcp vjc
- ppp ipcp ipaddress

以下の項目が表示される。

- ppp ipcp restart
- ppp ipcp maxconfigure
- ppp ipcp maxterminate
- ppp ipcp maxfailure

[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。

25.8.6 IPXCP 関連の設定の表示

[入力形式] **show ppp ipxcp** *[peer_number]*

[パラメータ]
- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は選択されている相手先について表示する

[説明] 以下の項目が表示される。

- ppp ipxcp restart
- ppp ipxcp maxconfigure
- ppp ipxcp maxterminate
- ppp ipxcp maxfailure

[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。

25.8.7 BCP 関連の設定の表示

[入力形式] **show ppp bcp** *[peer_number]*

[パラメータ]
- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は選択されている相手先について表示する

[説明] 以下の項目が表示される。

- ppp bcp lanid
- ppp bcp tinycomp
- ppp bcp restart
- ppp bcp maxconfigure
- ppp bcp maxterminate
- ppp bcp maxfailure

[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。

25.8.8 MSCBCP 関連の設定の表示

[入力形式] **show ppp mscbcp** *[peer_number]*

[パラメータ]
- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は選択されている相手先について表示する

[説明] 以下の項目が表示される。

- ppp mscbcp restart
- ppp mscbcp maxretry

[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。

25.8.9 BACP 関連の設定の表示

[入力形式] **show ppp bacp** *[peer_number]*

[パラメータ]
- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は選択されている相手先について表示する

[説明] 以下の項目が表示される。

- ppp bacp restart
- ppp bacp maxconfigure
- ppp bacp maxterminate
- ppp bacp maxfailure
- ppp bap restart
- ppp bap maxretry

[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。

25.8.10 CCP 関連の設定の表示

[入力形式] **show ppp ccp** *[peer_number]*

[パラメータ]
- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は選択されている相手について表示する

[説明] 以下の項目が表示される。

- ppp ccp type
- ppp ccp restart
- ppp ccp maxconfigure
- ppp ccp maxterminate
- ppp ccp maxfailure

[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。

25.8.11 MP 関連の設定の表示

[入力形式] **show ppp mp** *[peer_number]*

[パラメータ]

- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は選択されている相手について表示する

[説明] 以下の項目が表示される。

- ppp mp use
- ppp mp maxlink
- ppp mp control
- ppp mp divide
- ppp mp timer
- ppp mp load threshold

[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。

25.9 DHCP スコープの表示

[入力形式] **show dhcp** *[***scope** *[scope_num]]*

[パラメータ] • *scope_num* ... スコープ番号 (1..65535)

[説明] DHCP サービスの設定内容を表示する。
show dhcp では全てが表示される。**show dhcp scope** では全スコープの情報が表示される。**show dhcp scope** *scope_num* では指定したスコープ番号の情報が表示される。
DHCP サービスタイプが **server** の場合、次の項目が表示される。

- DHCP サービスタイプ
- スコープ設定内容
  - スコープ番号
  - IP アドレスの範囲
  - ネットマスク
  - 除外 IP アドレス
  - ゲートウェイ
  - リース時間
  - 最大リース時間
  - 予約 IP アドレス

DHCP サービスタイプが **relay** の場合、次の項目が表示される。

- DHCP サービスタイプ
- DHCP サーバアドレス
- DHCP サーバ選択方式
- DHCP 中継閾値

25.10 DHCP サーバの状態の表示

[入力形式] **show dhcp status**

[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)

25.11 SNMP 関連の設定の表示

[入力形式] **show snmp**

[パラメータ] なし

[説明] 以下の項目が表示される。

- snmp host
- snmp community read-only
- snmp community read-write
- snmp trap host
- snmp trap community
- snmp enableauthentraps
- snmp syscontact
- snmp sysname(または sysname)
- snmp syslocation

25.12 ICMP 関連の設定の表示

[入力形式] **show ip icmp**

[パラメータ] なし

[説明] 以下の項目が表示される。

- ip icmp echo-reply send
- ip icmp mask-reply send
- ip icmp parameter-problem send
- ip icmp redirect receive
- ip icmp redirect send
- ip icmp time-exceeded send
- ip icmp timestamp-reply send
- ip icmp unreachable send

25.13 RADIUS 関連の設定の表示

[入力形式] **show radius**

[パラメータ] なし

[説明] 以下の項目が表示される。

- radius auth
- radius account
- radius server
- radius retry
- radius secret

25.14 DNS 関連の設定の表示

[入力形式] **show dns**

[パラメータ] なし

[説明] DNS 関連の設定を表示する。

25.15 WINS 関連の設定の表示

[入力形式] **show wins**

[パラメータ] なし

[説明] WINS 関連の設定を表示する。

25.16 アナログ関係の設定の表示

[入力形式] **show analog config** *[port]*

[パラメータ]

- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート

[説明] アナログ関係の設定を表示する。

26 状態の表示

26.1 ARP テーブルの表示

[入力形式] **show arp**

[パラメータ] なし

[説明] ARP テーブルを表示する。

26.2 LAN 側の状態の表示

[入力形式]
1. **show status lan**
2. **show status lan1**
3. **show status lan2**

[パラメータ] なし

[説明] LAN 側の状態を表示する。

- イーサネットアドレス
- MTU
- プロミスキャスモード
- 正常に送信したパケットの数
- 送信エラーの数と内訳
- 正常に受信したパケットの数
- 受信エラーの数と内訳

26.3 PP 側の状態の表示

[入力形式]
1. **show status bri** ... RT103i,RTA50i
2. **show status bri** *[bri]*

[パラメータ]
- *bri* ... BRI 番号

[説明] PP 側の状態を表示する。

- 現在接続している相手先情報番号
- 現在接続している相手先 ISDN 番号

26.4 PRI の状態の表示

[入力形式] **show status pri** *[pri]*

[パラメータ]
- *pri* ... PRI 番号 (1)
- 省略した時はすべての PRI ポートについて表示する。

[説明] PRI の状態を表示する。

26.5 各相手先の状態の表示

[入力形式] **show status pp** *[peer_number]*

[パラメータ]
- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は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時の状態を表示する。

- 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

[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。

26.6 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
- 省略した時は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。

26.7 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。

26.8 SAP テーブルの表示

[入力形式] **show ipx sap**

[パラメータ] なし

[説明] IPX SAP テーブルを表示する。
非 ASCII 文字は八進数で表示される。

26.9 IPXWAN の状態の表示

[入力形式] **show ipx ipxwan** *[peer_number]*

[パラメータ]
- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は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。

26.10 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。

26.11 アナログ関係の状態の表示

[入力形式] **show status analog** *[port]*

[パラメータ]
- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート

[説明] アナログ関係の状態を表示する。

26.12 IPsec の SA の状態の表示

[入力形式] **show ipsec sa**

[パラメータ] なし

[説明] IPsec の SA の状態を表示する。

27 ロギング

27.1 ログの表示

[入力形式] 1. **show log**

2. **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

[ノート] 電源を切るとそれまでのログはクリアされる。

27.2 アカウントの表示

[入力形式] 1. **show account** ... RT103i,RTA50i

2. **show account** *bri*

[パラメータ]

- *bri*
  - BRI 番号
  - **all** ... 全ての BRI 番号

[説明] 以下の項目が表示される。

- 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。

27.3 相手先毎のアカウントの表示

[入力形式] **show pp account** *[peer_number]*

[パラメータ]
- *peer_number*
  - 相手先情報番号
  - **anonymous**
  - **leased**
- *peer_number* を省略した時は選択されている相手について表示する

[説明] 選択されている相手のアカウントを表示する。

[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。

27.4 アナログ関係のアカウントの表示

[入力形式] **show analog account** *[port]*

[パラメータ]
- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
  - **3** ... TEL3 ポート

[説明] アナログ関係のアカウントを表示する。

[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。