REMOTE ROUTER

コマンドリファレンス

ヤマハ株式会社

1997. 12. 24

♣ 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 95 は米国 Microsoft Corporation 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 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 コンソールポートの速度の設定 5
3.10 コンソールの言語とコードの設定 6
3.11 コンソールの表示文字数の設定 6
3.12 コンソールの表示行数の設定 6
3.13 コンソールにシステムメッセージを表示するか否かの設定 7
3.14 コンソールのプロンプト表示の設定 7
3.15 SYSLOG を受けるホストの IP アドレスの設定 7
3.16 SYSLOG ファシリティの設定 8
3.17 NOTICE タイプの SYSLOG を出力するか否かの設定 8
3.18 INFO タイプの SYSLOG を出力するか否かの設定 8
3.19 DEBUG タイプの SYSLOG を出力するか否かの設定 9
3.20 TFTP によりアクセスできるホストの IP アドレスの設定 9
3.21 PP 毎の送信キューの長さの設定 9

4 ISDN 関連の設定 10

4.1 自分側の設定 10
4.1.1 PP 側の回線の種類の指定 10
4.1.2 自分の ISDN 番号の設定 10
4.1.3 課金額による発信制限の設定 11
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 11

4.1.5 終端抵抗の設定 11
4.1.6 PP と BRI のバインドの設定 12
4.1.7 PIAFS の発信を許可するか否かの設定 12
4.1.8 PIAFS の着信を許可するか否かの設定 12
4.2 相手毎の設定 13
4.2.1 相手 ISDN 番号の設定 13
4.2.2 相手への発信順序の設定 13
4.2.3 自動接続の設定 14
4.2.4 相手にコールバック要求を行なうか否かの設定 14
4.2.5 相手からのコールバック要求に応じるか否かの設定 14
4.2.6 着信許可の設定 14
4.2.7 発信許可の設定 15
4.2.8 バルク転送の設定 15
4.2.9 エラー切断後の再発信禁止タイマの設定 15
4.2.10 再発信抑制タイマの設定 16
4.2.11 コールバック要求タイプの設定 16
4.2.12 コールバック受け入れタイプの設定 16
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 17
4.2.14 コールバックタイマの設定 17
4.2.15 コールバック待機タイマの設定 17
4.2.16 ISDN 回線を切断するタイマ方式の指定 18
4.2.17 切断タイマの設定（ノーマル） 18
4.2.18 入力切断タイマの設定（ノーマル） 19
4.2.19 出力切断タイマの設定（ノーマル） 19
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 20
4.2.21 切断タイマの設定（ファスト） 20
4.2.22 切断タイマの設定（強制） 21
4.2.23 相手先毎の課金額による発信制限の設定 21

5 フレームリレー関連の設定 22

5.1 PP 側でのカプセル化の種類の設定 22
5.2 PP 側フレームリレーでの DLCI の設定 23
5.3 PP 側フレームリレーでの PVC 状態確認手順の設定 23
5.4 PP 側フレームリレーでの InARP 使用の設定 24

6 IP の設定 25

6.1 LAN,PP 共通の設定 . . . 25
6.1.1 IP パケットを扱うか否かの設定 . . . 25
6.1.2 IP パケットのフィルタの設定 . . . 25
6.1.3 IP パケットのフィルタの削除 . . . 27
6.1.4 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 . 27
6.2 LAN 側の設定 . . . 27
6.2.1 IP アドレスの設定 . . . 27
6.2.2 LAN 側のセカンダリ IP アドレスの設定 . . . 28
6.2.3 ネットマスクの設定 . . . 28
6.2.4 ブロードキャストアドレスの設定 . . . 28
6.2.5 経路情報の追加 . . . 29
6.2.6 経路情報の削除 . . . 29
6.2.7 動的経路制御の設定 . . . 30
6.2.8 RIP のフィルタリングの設定 . . . 30
6.2.9 RIP に関して信用できるゲートウェイの設定 . . . 31
6.2.10 LAN 側 RIP2 での認証の設定 . . . 31
6.2.11 LAN 側 RIP2 での認証キーの設定 . . . 31
6.2.12 Proxy ARP の設定 . . . 32
6.2.13 LAN 側でのフィルタリングによるセキュリティの設定 . . . 32
6.3 PP 側相手毎の IP の設定 . . . 33
6.3.1 自分の PP 側 IP アドレスの設定 . . . 33
6.3.2 相手の PP 側 IP アドレスの設定 . . . 34
6.3.3 リモート IP アドレスプールの設定 . . . 34
6.3.4 PP 側のネットマスクの設定 . . . 35
6.3.5 経路情報の追加 . . . 35
6.3.6 経路情報の削除 . . . 36
6.3.7 PP 側の動的経路制御の設定 . . . 36
6.3.8 回線接続時の PP 側の RIP の動作の設定 . . . 36
6.3.9 回線接続時の PP 側の RIP 送出の時間間隔の設定 . . . 37
6.3.10 回線切断時の PP 側の RIP の動作の設定 . . . 37
6.3.11 回線切断時の PP 側の RIP 送出の時間間隔の設定 . . . 37
6.3.12 回線切断時の動的経路制御情報の保持 . . . 37
6.3.13 RIP のフィルタリングの設定 . . . 38
6.3.14 RIP ホップ加算数の設定 . . . 38
6.3.15 RIP に関して信用できるゲートウェイの設定 . . . 38
6.3.16 PP 側 RIP2 での認証の設定 . . . 39
6.3.17 PP 側 RIP2 での認証キーの設定 . . . 39

6.3.18 PP 側でのフィルタリングによるセキュリティの設定 40
6.3.19 回線切断時の LAN 側への RIP 動作の設定 40

7 IPX の設定 41

7.1 LAN,PP 共通の設定 41
7.1.1 IPX パケットを扱うか否かの設定 41
7.1.2 IPX パケットのフィルタの設定 41
7.1.3 IPX パケットのフィルタの削除 43
7.1.4 静的な SAP テーブルの設定 43
7.1.5 静的な SAP テーブルの削除 44
7.1.6 IPX SAP Get Nearest Server Request に応答するか否かの設定 44
7.2 LAN 側の設定 45
7.2.1 イーサネットフレームタイプの設定 45
7.2.2 LAN 側の IPX ネットワーク番号の設定 45
7.2.3 経路情報の追加 45
7.2.4 経路情報の削除 46
7.2.5 LAN 側の RIP/SAP ブロードキャストの設定 46
7.2.6 LAN 側でのフィルタリングによるセキュリティの設定 46
7.3 PP 側相手毎の IPX の設定 47
7.3.1 IPX ルーティング許可の設定 47
7.3.2 PP 側 IPX ネットワーク番号の設定 47
7.3.3 経路情報の追加 47
7.3.4 経路情報の削除 48
7.3.5 回線接続時の PP 側の RIP/SAP の動作の設定 48
7.3.6 回線接続時の PP 側の RIP/SAP 送出の時間間隔の設定 48
7.3.7 回線切断時の PP 側の RIP/SAP の動作の設定 48
7.3.8 回線切断時の PP 側の RIP/SAP 送出の時間間隔の設定 49
7.3.9 回線切断時に RIP/SAP 情報を保持するか否かの設定 49
7.3.10 IPXWAN 使用の設定 49
7.3.11 Timer/Information Request の再送間隔と最大再送回数の設定 49
7.3.12 IPXWAN プライマリネットワーク番号の設定 50
7.3.13 Watchdog パケットに対する代理応答の設定 50
7.3.14 Watchdog 代理応答の時間間隔の設定 50
7.3.15 SPX キープアライブ代理応答を行うか否かの設定 50
7.3.16 SPX キープアライブ代理応答のタイマの設定 51
7.3.17 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 51
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 52

8 ブリッジの設定 53

8.1 LAN,PP 共通の設定 . . . 53
8.1.1 ブリッジ使用許可の設定 . . . 53
8.1.2 ブリッジのフィルタの設定 . . . 54
8.1.3 ブリッジのフィルタの削除 . . . 54
8.1.4 ブリッジする相手先の設定 . . . 55
8.1.5 MAC アドレスのラーニングを行なうか否かの設定 . . . 55
8.1.6 ラーニング情報消去タイマの設定 . . . 55
8.2 LAN 側の設定 . . . 56
8.2.1 ラーニング情報の設定 . . . 56
8.2.2 ラーニング情報の削除 . . . 56
8.2.3 LAN 側でのブリッジのフィルタリングの設定 . . . 56
8.3 PP 側相手毎のブリッジの設定 . . . 56
8.3.1 ラーニング情報の設定 . . . 56
8.3.2 ラーニング情報の削除 . . . 57
8.3.3 PP 側でのブリッジのフィルタリングの設定 . . . 57

9 PPP の設定 58

9.1 相手の名前とパスワードの設定 . . . 58
9.2 要求する認証タイプの設定 . . . 59
9.3 受け入れる認証タイプの設定 . . . 59
9.4 自分の名前とパスワードの設定 . . . 59
9.5 自分の名前の消去 . . . 60
9.6 相手の名前の削除 . . . 60
9.7 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 . . . 60
9.8 LCP 関連の設定 . . . 60
9.8.1 Address & Control Field Compression オプション使用の設定 . . . 60
9.8.2 Magic Number オプション使用の設定 . . . 61
9.8.3 Maximum Receive Unit オプション使用の設定 . . . 61
9.8.4 Protocol Field Compression オプション使用の設定 . . . 61
9.8.5 パラメータ lcp-restart の設定 . . . 62
9.8.6 パラメータ lcp-max-terminate の設定 . . . 62
9.8.7 パラメータ lcp-max-configure の設定 . . . 62
9.8.8 パラメータ lcp-max-failure の設定 . . . 62
9.8.9 専用線キープアライブを使用するか否かの設定 . . . 63
9.8.10 専用線キープアライブのログをとるか否かの設定 . . . 63
9.8.11 専用線キープアライブの時間間隔の設定 . . . 63
9.8.12 専用線ダウン検出時の動作の設定 . . . 64

9.9 PAP 関連の設定 64
9.9.1 パラメータ pap-restart の設定 64
9.9.2 パラメータ pap-max-authreq の設定 64
9.10 CHAP 関連の設定 64
9.10.1 パラメータ chap-restart の設定 64
9.10.2 パラメータ chap-max-challenge の設定 65
9.11 IPCP 関連の設定 65
9.11.1 Van Jacobson Compressed TCP/IP 使用の設定 65
9.11.2 PP 側 IP アドレスのネゴシエーションの設定 65
9.11.3 パラメータ ipcp-restart の設定 66
9.11.4 パラメータ ipcp-max-terminate の設定 66
9.11.5 パラメータ ipcp-max-configure の設定 66
9.11.6 パラメータ ipcp-max-failure の設定 66
9.11.7 IPCP の MS 拡張オプションを使うか否かの設定 67
9.11.8 WINS サーバの IP アドレスの設定 67
9.12 IPXCP 関連の設定 67
9.12.1 パラメータ ipxcp-restart の設定 67
9.12.2 パラメータ ipxcp-max-terminate の設定 68
9.12.3 パラメータ ipxcp-max-configure の設定 68
9.12.4 パラメータ ipxcp-max-failure の設定 68
9.13 BCP 関連の設定 68
9.13.1 LAN Identification 使用の設定 68
9.13.2 Tinygram compression 使用の設定 69
9.13.3 パラメータ bcp-restart の設定 69
9.13.4 パラメータ bcp-max-terminate の設定 69
9.13.5 パラメータ bcp-max-configure の設定 69
9.13.6 パラメータ bcp-max-failure の設定 70
9.13.7 パラメータ mscbcp-restart の設定 70
9.13.8 パラメータ mscbcp-maxretry の設定 70
9.14 CCP 関連の設定 71
9.14.1 全パケットの圧縮タイプの設定 71
9.14.2 パラメータ ccp-restart の設定 71
9.14.3 パラメータ ccp-max-terminate の設定 71
9.14.4 パラメータ ccp-max-configure の設定 72
9.14.5 パラメータ ccp-max-failure の設定 72
9.15 MP 関連の設定 72
9.15.1 MP を使用するか否かの設定 72
9.15.2 MP の制御方法の設定 72

9.15.3 MP のための負荷閾値の設定 . . . 73
9.15.4 MP の最大リンク数の設定 . . . 73
9.15.5 MP の最小リンク数の設定 . . . 73
9.15.6 MP のための負荷計測間隔の設定 . . . 74
9.15.7 MP のパケットを分割するか否かの設定 . . . 74
9.16 BACP 関連の設定 . . . 74
9.16.1 パラメータ bacp-restart の設定 . . . 74
9.16.2 パラメータ bacp-max-terminate の設定 . . . 74
9.16.3 パラメータ bacp-max-configure の設定 . . . 75
9.16.4 パラメータ bacp-max-failure の設定 . . . 75
9.16.5 パラメータ bap-restart の設定 . . . 75
9.16.6 パラメータ bap-max-retry の設定 . . . 75

10 DHCP の設定 76
10.1 DHCP の動作の設定 . . . 76
10.2 DHCP スコープの定義 . . . 77
10.3 DHCP スコープの削除 . . . 77
10.4 DHCP 予約アドレスの設定 . . . 78
10.5 DHCP 予約アドレスの解除 . . . 78
10.6 DHCP サーバの指定の設定 . . . 78
10.7 DHCP サーバの選択方法の設定 . . . 79
10.8 DHCP BOOTREQUEST パケットの中継基準の設定 . . . 79

11 SNMP の設定 80
11.1 読み出し専用のコミュニティ名の設定 . . . 80
11.2 読み書き可能なコミュニティ名の設定 . . . 80
11.3 認証失敗時 (authenticationFailure) にトラップを送信するか否かの設定 . . . 80
11.4 SNMP によるアクセスを許可するホストの設定 . . . 81
11.5 sysContact の設定 . . . 81
11.6 sysLocation の設定 . . . 81
11.7 sysName の設定 . . . 81
11.8 送信トラップのコミュニティ名の設定 . . . 82
11.9 トラップの受信ホストの設定 . . . 82

12 ICMP の設定 83
12.1 ICMP Echo Reply を送信するか否かの設定 . . . 83
12.2 ICMP Mask Reply を送信するか否かの設定 . . . 83
12.3 ICMP Parameter Problem を送信するか否かの設定 . . . 83
12.4 ICMP Redirect を送信するか否かの設定 . . . 84

12.5 ICMP Redirect 受信時の処理の設定 84
12.6 ICMP Time Exceeded を送信するか否かの設定 84
12.7 ICMP Timestamp Reply を送信するか否かの設定 84
12.8 ICMP Destination Unreachable を送信するか否かの設定 85

13 RADIUS の設定 86
13.1 RADIUS サーバの指定 86
13.2 RADIUS シークレットの設定 86
13.3 RADIUS 再送信パラメータの設定 86
13.4 RADIUS による認証を使用するか否かの設定 87
13.5 RADIUS によるアカウントを使用するか否かの設定 87

14 NAT の設定 88
14.1 NAT を使うか否かの設定 88
14.2 IP Masquerade を使用するか否かの設定 88
14.3 IP Masquerade 使用時に rlogin と rcp を許可するか否かの設定 89
14.4 静的 IP Masquerade エントリの設定 89
14.5 静的 IP Masquerade エントリの削除 89
14.6 NAT のグローバル IP アドレスの設定 90
14.7 NAT の対象とするプライベートアドレスの範囲の設定 90
14.8 NAT の IP アドレスマップの消去タイマの設定 90

15 DNS リゾルバの設定 91
15.1 DNS サーバの IP アドレスの設定 91
15.2 DNS ドメイン名の設定 91
15.3 SYSLOG 出力で DNS による名前解決をするか否かの設定 91
15.4 DHCP/IPCP MS 拡張で DNS サーバを通知する順序の設定 92

16 アナログ通信機能の設定 93
16.1 アナログポートの ISDN 番号の設定 94
16.2 アナログポートに接続する機器の指定 94
16.3 アナログポートの発信者番号を通知するか否かの設定 95
16.4 相手先番号による即時発信を許可するか否かの設定 95
16.5 グローバル着信を許可するか否かの設定 96
16.6 アナログポートでの識別着信をするか否かの設定 96
16.7 識別着信リストの登録 97
16.8 識別着信リストの削除 97
16.9 サブアドレス無し着信を許可するか否かの設定 97
16.10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 98
16.11話中着信を許可するか否かの設定 98

16.12優先着信機能の設定 99
16.13着信ベルリストの登録 99
16.14着信ベルリストの削除 99
16.15ダイヤル桁間タイマの設定 100
16.16フッキングを判定する時間の設定 100
16.17フッキング後にキー操作を受け入れる時間の設定 100
16.18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 101
16.19フレックスホン機能の使用パターンの設定 101
16.20着信転送先アドレスの設定 102
16.21着信転送トーキの設定 102
16.22着信転送を起動するタイミングの設定 103
16.23着信転送が拒否された時の動作の設定 103
16.24送話 PAD の設定 103
16.25受話 PAD の設定 104

17 操作 **105**
17.1 相手先情報番号の選択 105
17.2 設定に関する操作 105
17.2.1 管理ユーザへの移行 105
17.2.2 設定内容の保存 105
17.2.3 終了 105
17.2.4 相手先の初期化 106
17.2.5 相手先毎の設定の複写 106
17.2.6 設定の初期化 106
17.2.7 遠隔地のルータの設定 107
17.2.8 遠隔地のルータからの設定に対する制限 107
17.3 動的情報のクリア操作 107
17.3.1 ARP テーブルのクリア 107
17.3.2 IP の動的経路情報のクリア 108
17.3.3 IPX の動的経路情報のクリア 108
17.3.4 IPX の動的 SAP 情報のクリア 108
17.3.5 ブリッジのラーニング情報のクリア 108
17.3.6 ログのクリア 108
17.3.7 アカウントのクリア 108
17.3.8 相手先毎のアカウントの消去 109
17.3.9 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 109
17.3.10 InARP のクリア 109

17.3.11 DNS キャッシュのクリア . . . 109
17.4 スケジュール . . . 110
17.4.1 スケジュールの設定 . . . 110
17.4.2 スケジュールの削除 . . . 111
17.4.3 スケジュールの確認 . . . 111
17.5 その他の操作 . . . 112
17.5.1 相手先の使用許可の設定 . . . 112
17.5.2 相手先の使用不許可の設定 . . . 112
17.5.3 再起動 . . . 112
17.5.4 発信 . . . 112
17.5.5 切断 . . . 113
17.5.6 ping . . . 113
17.5.7 traceroute . . . 113
17.5.8 リモートホストによる時計の設定 . . . 114
17.5.9 NTP による時計の設定 . . . 114
17.5.10 telnet . . . 114

18 設定の表示 115
18.1 機器設定の表示 . . . 115
18.1.1 機器設定の表示 . . . 115
18.1.2 SYSLOG 関連の表示 . . . 115
18.1.3 TFTP 関連の表示 . . . 115
18.1.4 PP 毎の送信キューの表示 . . . 116
18.1.5 すべての設定内容の表示 . . . 116
18.1.6 PP 毎の設定内容の表示 . . . 116
18.2 相手先一覧の表示 . . . 117
18.2.1 相手先一覧の表示 . . . 117
18.3 ISDN 関連の表示 . . . 117
18.3.1 自分側設定の表示 . . . 117
18.3.2 相手側設定の表示 . . . 118
18.4 フレームリレー関連の表示 . . . 119
18.4.1 PP 側フレームリレー設定の表示 . . . 119
18.4.2 DLCI の表示 . . . 119
18.5 IP 関連の表示 . . . 119
18.5.1 IP パケットのフィルタの一覧表示 . . . 119
18.5.2 IP パケットのフィルタの表示 . . . 119
18.5.3 LAN 側 IP 設定の表示 . . . 120
18.5.4 PP 側 IP 設定の表示 . . . 121

18.6 IPX 関連の表示 121
18.6.1 IPX パケットのフィルタの一覧表示 121
18.6.2 IPX パケットのフィルタの表示 122
18.6.3 LAN 側 IPX 設定の表示 122
18.6.4 PP 側 IPX 設定の表示 123
18.7 ブリッジ関連の表示 123
18.7.1 ブリッジのフィルタの一覧表示 123
18.7.2 ブリッジのフィルタの表示 124
18.7.3 LAN 側ブリッジ設定の表示 124
18.7.4 PP 側ブリッジ設定の表示 124
18.8 PPP の設定の表示 125
18.8.1 認証関連の設定の表示 125
18.8.2 LCP 関連の設定の表示 125
18.8.3 PAP 関連の設定の表示 126
18.8.4 CHAP 関連の設定の表示 126
18.8.5 IPCP 関連の設定の表示 127
18.8.6 IPXCP 関連の設定の表示 127
18.8.7 BCP 関連の設定の表示 128
18.8.8 MSCBCP 関連の設定の表示 128
18.8.9 BACP 関連の設定の表示 129
18.8.10 CCP 関連の設定の表示 129
18.8.11 MP 関連の設定の表示 130
18.9 DHCP スコープの表示 131
18.10DHCP サーバの状態の表示 131
18.11SNMP 関連の設定の表示 132
18.12ICMP 関連の設定の表示 132
18.13RADIUS 関連の設定の表示 132
18.14NAT 関連の設定の表示 133
18.15DNS 関連の設定の表示 133
18.16アナログ関係の設定の表示 133

19 状態の表示 134

19.1 ARP テーブルの表示 134
19.2 LAN 側の状態の表示 134
19.3 PP 側の状態の表示 134
19.4 各相手先の状態の表示 135
19.5 IP の経路情報テーブルの表示 135
19.6 IPX の経路情報テーブルの表示 135

19.7 SAP テーブルの表示 136
19.8 IPXWAN の状態の表示 136
19.9 ブリッジのラーニング情報の表示 136
19.10NAT 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 136
19.11アナログ関係の状態の表示 137

20 ロギング **138**
20.1 ログの表示 138
20.2 アカウントの表示 138
20.3 相手先毎のアカウントの表示 138
20.4 アナログ関係のアカウントの表示 139

索 引

account threshold, 11
administrator, 105
administrator password, 3
analog arrive another-device permit, 98
analog arrive global permit, 96
analog arrive prior-port, 99
analog arrive restrict, 96
analog arrive restrict list add, 97
analog arrive restrict list delete, 97
analog arrive ring-while-talking permit, 98
analog arrive ringer-type list add, 99
analog arrive ringer-type list delete, 99
analog arrive without-subaddress permit, 97
analog device type, 94
analog hooking inhibit timer, 101
analog hooking timer, 100
analog hooking wait timer, 100
analog local address, 94
analog local address notice, 95
analog pad receive, 104
analog pad send, 103
analog rapid call, 95
analog supplementary-service, 101
analog supplementary-service call-deflection address, 101, 102
analog supplementary-service call-deflection reject, 103
analog supplementary-service call-deflection ringer, 103
analog supplementary-service call-deflection talkie, 102
analog wait dial timer, 100

bri line, 10
bri terminator, 11
bridge filter, 54
bridge filter delete, 54
bridge forwarding, 55
bridge lan filter, 56
bridge lan learning add, 56
bridge lan learning delete, 56
bridge learning, 55
bridge learning expire, 55
bridge pp filter, 57
bridge pp learning add, 56
bridge pp learning delete, 57
bridge use, 53

clear account, 108
clear arp, 107
clear bridge learning, 108
clear dns cache, 109
clear inarp, 109
clear ip dynamic routing, 108
clear ipx dynamic routing, 108
clear ipx dynamic sap, 108
clear log, 108
clear nat dynamic, 109
clear pp account, 109
cold start, 106
connect, 112
console character, 6
console columns, 6
console info, 7
console lines, 6
console prompt, 7
console speed, 5

date, 5
dhcp delete scope, 77
dhcp relay select, 76, 79
dhcp relay server, 76, 78
dhcp relay threshold, 79
dhcp scope, 76, 77
dhcp scope bind, 76, 78
dhcp scope unbind, 76, 78
dhcp service, 76
disconnect, 113
dns domain, 91
dns notice order, 92
dns server, 76, 91, 92
dns syslog resolv, 91

fr dlci, 22, 23
fr inarp, 22, 24
fr lmi, 22, 23

help, 3

ip filter, 25
ip filter delete, 27
ip filter source-route, 27

ip icmp echo-reply send, 83
ip icmp mask-reply send, 83
ip icmp parameter-problem send, 83
ip icmp redirect receive, 84
ip icmp redirect send, 84
ip icmp time-exceeded send, 84
ip icmp timestamp-reply send, 84
ip icmp unreachable send, 85
ip lan address, 27
ip lan broadcast, 28
ip lan netmask, 28
ip lan proxyarp, 32
ip lan rip auth key, 31
ip lan rip auth type , 31
ip lan rip filter, 30
ip lan rip listen, 31
ip lan route add, 29
ip lan route delete, 29
ip lan routing protocol, 30
ip lan secondary address, 28
ip lan secure filter, 32
ip pp hide static route, 40
ip pp hold routing, 37
ip pp local address, 33
ip pp netmask, 35
ip pp remote address, 34
ip pp remote address pool, 34
ip pp rip auth key, 39
ip pp rip auth type , 39
ip pp rip connect interval, 37
ip pp rip connect send, 36
ip pp rip disconnect interval, 37
ip pp rip disconnect send, 37
ip pp rip filter, 38
ip pp rip hop, 38
ip pp rip listen, 38
ip pp route add, 35
ip pp route delete, 36
ip pp routing protocol, 36
ip pp secure filter, 40
ip routing, 25
ipx filter, 41
ipx filter delete, 43
ipx lan frame type, 45
ipx lan network, 45
ipx lan ripsap broadcast, 46
ipx lan route add, 45
ipx lan route delete, 46
ipx lan secure filter, 46
ipx pp ipxwan primnet, 50
ipx pp ipxwan retry, 49
ipx pp ipxwan use, 49
ipx pp network, 47
ipx pp ripsap connect interval, 48
ipx pp ripsap connect send, 48
ipx pp ripsap disconnect interval, 49
ipx pp ripsap disconnect send, 48
ipx pp ripsap hold, 49
ipx pp route add, 47
ipx pp route delete, 48
ipx pp routing, 47
ipx pp secure filter, 52
ipx pp serialization filter, 51
ipx pp spx keepalive proxy, 50
ipx pp spx keepalive timer, 51
ipx pp watchdog interval, 50
ipx pp watchdog proxy, 50
ipx routing, 41
ipx sap add, 43
ipx sap delete, 44
ipx sap response, 44
isdn arrive permit, 14
isdn auto connect, 14
isdn bulk, 15
isdn call block time, 16
isdn call permit, 15
isdn call prohibit time, 15
isdn callback mscbcp user-specify, 17
isdn callback permit, 14
isdn callback permit type, 16
isdn callback request, 14
isdn callback request type, 16
isdn callback response time, 17
isdn callback wait time, 17
isdn disconnect input time, 19
isdn disconnect interval time, 20
isdn disconnect output time, 19
isdn disconnect policy, 18
isdn disconnect time, 18
isdn fast disconnect time, 20
isdn forced disconnect time, 21
isdn local address, 10
isdn piafs arrive, 12
isdn piafs call, 12

isdn remote address, 13
isdn remote call order, 13

leased backup, 11
leased keepalive down, 64
leased keepalive interval, 63
leased keepalive log, 63
leased keepalive use, 63
login password, 3
login timer, 4

nat address global, 90
nat address private, 90
nat masquerade, 88
nat masquerade rlogin, 89
nat masquerade static, 89
nat masquerade static delete, 89
nat timer, 90
nat use, 88
ntpdate, 114

ping, 113
pp account threshold, 21
pp auth accept, 59
pp auth clear myname, 60
pp auth delete username, 60
pp auth multi connect prohibit, 60
pp auth myname, 59
pp auth request, 59
pp auth username, 58
pp bind bri, 12
pp copy, 106
pp default, 106
pp disable, 112
pp enable, 112
pp encapsulation, 22
pp line, 10
pp queue length, 9
pp select, 105
ppp bacp maxconfigure, 75
ppp bacp maxfailure, 75
ppp bacp maxterminate, 74
ppp bacp restart, 74
ppp bap maxretry, 75
ppp bap restart, 75
ppp bcp lanid, 68
ppp bcp maxconfigure, 69
ppp bcp maxfailure, 70
ppp bcp maxterminate, 69
ppp bcp restart, 69
ppp bcp tinycomp, 69
ppp ccp maxconfigure, 72
ppp ccp maxfailure, 72
ppp ccp maxterminate, 71
ppp ccp restart, 71
ppp ccp type, 71
ppp chap maxchallenge, 65
ppp chap restart, 64
ppp ipcp ipaddress, 65
ppp ipcp maxconfigure, 66
ppp ipcp maxfailure, 66
ppp ipcp maxterminate, 66
ppp ipcp msext, 67
ppp ipcp restart, 66
ppp ipcp vjc, 65
ppp ipxcp maxconfigure, 68
ppp ipxcp maxfailure, 68
ppp ipxcp maxterminate, 68
ppp ipxcp restart, 67
ppp lcp acfc, 60
ppp lcp magicnumber, 61
ppp lcp maxconfigure, 62
ppp lcp maxfailure, 62
ppp lcp maxterminate, 62
ppp lcp mru, 61
ppp lcp pfc, 61
ppp lcp restart, 62
ppp mp control, 72
ppp mp divide, 74
ppp mp load threshold, 73
ppp mp maxlink, 73
ppp mp minlink, 73
ppp mp timer, 74
ppp mp use, 72
ppp mscbcp maxretry, 70
ppp mscbcp restart, 70
ppp pap maxauthreq, 64
ppp pap restart, 64

quit, 105

radius account, 87
radius auth, 87
radius retry, 86
radius secret, 86
radius server, 86

rdate, 114
remote setup, 107
remote setup accept, 107
restart, 112

save, 105
schedule at, 110
schedule delete, 111
security class, 4
show account, 138
show analog account, 139
show analog config, 133
show arp, 134
show auth, 125
show bridge filter, 124
show bridge filter list, 123
show bridge lan, 124
show bridge learning, 136
show bridge pp, 124
show command, 2, 3
show config, 116
show dhcp, 76, 131
show dhcp scope, 131
show dhcp status, 76, 131
show dlci, 22, 119
show dns, 133
show environment, 115
show fr, 22, 119
show ip filter, 119
show ip filter list, 119
show ip icmp, 132
show ip lan, 120
show ip pp, 121
show ip route, 135
show ipx filter, 122
show ipx filter list, 121
show ipx ipxwan, 136
show ipx lan, 122
show ipx pp, 123
show ipx route, 135
show ipx sap, 136
show isdn local, 117
show isdn remote, 118
show log, 138
show nat address, 136
show nat config, 133
show pp account, 21, 138
show pp config, 116
show pp queue, 116
show ppp bacp, 129
show ppp bcp, 128
show ppp ccp, 129
show ppp chap, 126
show ppp ipcp, 127
show ppp ipxcp, 127
show ppp lcp, 125
show ppp mp, 130
show ppp mscbcp, 128
show ppp pap, 126
show radius, 132
show remote list, 117
show schedule, 111
show snmp, 132
show status analog, 137
show status bri, 134
show status lan, 134
show status pp, 135
show syslog, 115
show tftp, 115
snmp community read-only, 80
snmp community read-write, 80
snmp enableauthentraps, 80
snmp host, 81
snmp syscontact, 81
snmp syslocation, 81
snmp sysname, 81
snmp trap community, 82
snmp trap host, 82
syslog debug, 9
syslog facility, 8
syslog host, 7
syslog info, 8
syslog notice, 8
sysname, 3

telnet, 114
tftp host, 9
time, 5
timezone, 5
traceroute, 113

wins server, 67

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**、**RT140i**、**RT102i** 及び **RT80i** プログラムの **Rev.2.02.19** 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。コマンドは大きく次のように分類して並べてあります。

分類	説明
ヘルプ	コンソールの使用方法やコマンドの説明に関するコマンドです。
機器の設定	ルーティングやブリッジングに関係のないルータシステムに関するコマンドです。
ISDN 関連の設定	回線との接続切断に関するコマンドです。
フレームリレー関連の設定	フレームリレー接続に関するコマンドです。
IP の設定	IP パケットのルーティングに関するコマンドです。
IPX の設定	IPX パケットのルーティングに関するコマンドです。
ブリッジの設定	ブリッジングに関するコマンドです。
PPP の設定	PPP 接続に関するコマンドです。
DHCP の設定	DHCP サーバと DHCP リレーエージェント機能に関するコマンドです。
SNMP の設定	ネットワーク管理に関するコマンドです。
ICMP の設定	ルータ本体における ICMP の動作に関するコマンドです。
RADIUS の設定	ルータを RADIUS クライアントとして使用する場合のコマンドです。
NAT の設定	NAT に関するコマンドです。
DNS リゾルバの設定	DNS リゾルバに関するコマンドです。
アナログ通信機能の設定	アナログ通信機能に関するコマンドです。
操作	グローバルなルータ操作に関するコマンドです。
設定の表示	設定内容の確認に関するコマンドです。
状態の表示	通信状態や各種テーブルの参照に関するコマンドです。
ロギング	通信結果の参照に関するコマンドです。

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]	このコマンドの入力形式を説明します。キー入力時には大文字と小文字のどちらを使用しても構いません。コマンドリファレンスでは小文字に統一してあります。コマンドの名称部分は太字 (**Bold face**) で、パラメータ部分は斜体 (*italic face*) で表してあります。
[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]	このコマンドの使用例を示します。

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** と **RT140i** では 1–100 までであり、**RT102i** と **RT80i** では 1–30 までです。

モデル	相手先情報番号の範囲
RT200i	1–100
RT140i	1–100
RT102i	1–30
RT80i	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、**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
RT140i	1, 2

3. **RT200i** 及び **RT140i** では複数の BRI ポートを装備してるため、**RT102i** 及び **RT80i** のコマンドパラメータとして使用できる PP 番号のキーワード **leased** を指定することはできません。
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。

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。

[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 コンソールポートの速度の設定

[入力形式] **console speed** *speed*

[パラメータ]
- *speed*
  - **1200** ... 1200bit/s
  - **2400** ... 2400bit/s
  - **4800** ... 4800bit/s
  - **9600** ... 9600bit/s

[説明] 設定用コンソールポートの速度を指定する。

[デフォルト値] **9600**

3.10 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**

3.11 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

3.12 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

3.13 コンソールにシステムメッセージを表示するか否かの設定

[入力形式] **console info** *info*

[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**

3.14 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

3.15 SYSLOG を受けるホストの IP アドレスの設定

[入力形式] **syslog host** *host*

[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**

3.16 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**

3.17 NOTICE タイプの SYSLOG を出力するか否かの設定

[入力形式] **syslog notice** *notice*

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

[説明] IP フィルタ、IPX フィルタ、ブリッジフィルタで落したパケット情報等を SYSLOG で出力するか否か設定する。

[デフォルト値] **off**

3.18 INFO タイプの SYSLOG を出力するか否かの設定

[入力形式] **syslog info** *info*

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

[説明] ISDN の呼制御情報等を SYSLOG で出力するか否か設定する。

[デフォルト値] **on**

3.19 DEBUG タイプの SYSLOG を出力するか否かの設定

[入力形式] **syslog debug** *debug*

[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**

3.20 TFTP によりアクセスできるホストの IP アドレスの設定

[入力形式] **tftp host** *host*

[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**

3.21 PP 毎の送信キューの長さの設定

[入力形式] **pp queue length** *length*

[パラメータ]
- *length* ... 送信キューの長さ (1..10000)

[説明] 選択されている相手について送信キューの長さを設定する。

[デフォルト値] 100

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*
2. **bri line** *bri line* ... RT200i, RT140i

[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

[説明] PP 側の回線を指定する。次の起動時に有効になる。

[デフォルト値] **isdn**

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* ... RT200i, RT140i
6. **bri local address** *bri isdn_number* ... RT200i, RT140i
7. **bri local address** *bri* /*sub_address* ... RT200i, RT140i
8. **bri local address** *bri* / ... RT200i, RT140i

[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。

[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 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**

4.1.6 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**

4.1.7 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*
  - **on** ... 許可する
  - **off** ... 拒否する

[説明] PIAFS の発信を許可するか否かを設定する。

[デフォルト値] **off**

4.1.8 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。

[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** ... 発信用
  - **arrive** ... 着信用
- *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。

[ノート] 2 個目以降の ISDN 番号は最大 15 桁まで設定でき、サブアドレスは最大 16 桁まで設定できる。

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** コマンドで設定した複数の ISDN 番号に発信する際、どのような順番にするかを設定する。
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、最初に設定された ISDN 番号で発信した際、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。また、この接続が終了した後には、再度最初に設定された ISDN 番号が発信に使用される。

[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 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**

4.2.5 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**

4.2.6 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**

4.2.7 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**

4.2.8 バルク転送の設定

[入力形式] **isdn bulk** *bulk*

[パラメータ]
- *bulk*
  - **1b** ... 1B で接続する
  - **2b** ... 2B で接続する
  - **any** ... 可能ならば 2B、できなければ 1B で接続する

[説明] 選択されている相手について ISDN の B チャネルを 1 本で使うのか 2 本で使うのか設定する。

[デフォルト値] **1b**

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。

[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、発信用の番号の設定もない場合には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] **isdn disconnect input time** または **isdn disconnect output time** コマンドの設定値が **isdn disconnect time** コマンドの設定値より短い場合には、短い方の設定値が自動的に **isdn disconnect time** コマンドの設定値に揃えられる。

[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] **isdn disconnect time** と併用した時は どちらかの短い方で切断される。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。
isdn disconnect input time または **isdn disconnect output time** コマンドの設定値が **isdn disconnect time** コマンドの設定値より短い場合には、短い方の設定値が自動的に **isdn disconnect time** コマンドの設定値に揃えられる。

[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] **isdn disconnect time** と併用した時は どちらかの短い方で切断される。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。
isdn disconnect input time または **isdn disconnect output time** コマンドの設定値が **isdn disconnect time** コマンドの設定値より短い場合には、短い方の設定値が自動的に **isdn disconnect time** コマンドの設定値に揃えられる。

[デフォルト値] 120

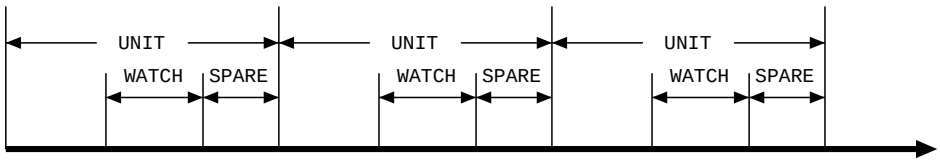
4.2.20 課金単位時間方式での課金単位時間と監視時間の設定

[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**
- *apare* ... 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。

[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。

[デフォルト値] **off**

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 32 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。

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**

[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

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 を空白で区切って並べたもの (32 個以内)

[説明] 選択されている相手で使用する DLCI(Data Link Connection Identifier) 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 (LMI;Local Management Interface) 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**

6 IP の設定

6.1 LAN,PP 共通の設定

6.1.1 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**

6.1.2 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** ... 一致すれば通す
  - **reject** ... 一致すれば破棄する
  - **restrict** ... 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
- *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。
- *mask* ... IP アドレスのビットマスク、省略した時は 0xffffffff と同じ
  - 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** 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。

[設定例]
```
# ip filter 3 pass 172.20.10.* 172.21.40.0/0xffffc000 tcp ftp
```

6.1.3 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。

6.1.4 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**

6.2 LAN 側の設定

6.2.1 IP アドレスの設定

[入力形式] 1. **ip lan address** *ip_address[/netmask]*

2. **ip lan 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, RT140i, RT102i
192.176.0.1 ... RT80i

6.2.2 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 lan 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**

6.2.3 ネットマスクの設定

[入力形式] **ip lan 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**

6.2.4 ブロードキャストアドレスの設定

[入力形式] **ip lan 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**

6.2.5 経路情報の追加

[入力形式] **ip lan 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。

6.2.6 経路情報の削除

[入力形式] **ip lan 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。

6.2.7 動的経路制御の設定

[入力形式] **ip lan 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**

6.2.8 RIP のフィルタリングの設定

[入力形式] **ip lan 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**

6.2.9 RIP に関して信用できるゲートウェイの設定

[入力形式] **ip lan 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**

6.2.10 LAN 側 RIP2 での認証の設定

[入力形式] **ip lan 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**

6.2.11 LAN 側 RIP2 での認証キーの設定

[入力形式] **ip lan 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
```

6.2.12 Proxy ARP の設定

[入力形式] **ip lan 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**

6.2.13 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] **ip lan 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**

6.3 PP 側相手毎の IP の設定

6.3.1 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。

6.3.2 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。

6.3.3 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、**RT140i** 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。

6.3.4 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**

6.3.5 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。

6.3.6 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。

6.3.7 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**

6.3.8 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**

6.3.9 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

6.3.10 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**

6.3.11 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

6.3.12 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**

6.3.13 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**

6.3.14 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

6.3.15 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**

6.3.16 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**

6.3.17 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] **none**

[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
```

6.3.18 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**

6.3.19 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 IPX の設定

7.1 LAN,PP 共通の設定

7.1.1 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**

7.1.2 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** ... 一致すればパケットを通す
  - **reject** ... 一致すれば破棄する
  - **restrict** ... 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
- *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 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。

7.1.3 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。

7.1.4 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。

7.1.5 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。

7.1.6 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**

7.2 LAN 側の設定

7.2.1 イーサネットフレームタイプの設定

[入力形式] **ipx lan 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。
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

7.2.2 LAN 側の IPX ネットワーク番号の設定

[入力形式] **ipx lan 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)

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

[デフォルト値] 0:0:0:1

7.2.3 経路情報の追加

[入力形式] **ipx lan 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。

[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。

7.2.4 経路情報の削除

[入力形式] **ipx lan 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。

7.2.5 LAN 側の RIP/SAP ブロードキャストの設定

[入力形式] **ipx lan 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。

[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

7.2.6 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] **ipx lan 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。

[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**

7.3 PP 側相手毎の IPX の設定

7.3.1 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**

7.3.2 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

7.3.3 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。

7.3.4 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。

7.3.5 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**

7.3.6 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

7.3.7 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**

7.3.8 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

7.3.9 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**

7.3.10 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**

7.3.11 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] $interval = 20$
$max = 3$

7.3.12 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

7.3.13 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**

7.3.14 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

7.3.15 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**

7.3.16 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

7.3.17 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**

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] **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**

8 ブリッジの設定

8.1 LAN,PP 共通の設定

8.1.1 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**

8.1.2 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** ... 一致すれば通す
  - **reject** ... 一致すれば破棄する
  - **restrict** ... 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
- *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** 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。

8.1.3 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。

8.1.4 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。
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 PP1 へのみブリッジされる。
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、**RT200i** の場合は **leased** は指定できない。

[デフォルト値] 1

8.1.5 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** ... ラーニングを行なう
  - **off** ... ラーニングを行なわない

[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**

8.1.6 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**

8.2 LAN 側の設定

8.2.1 ラーニング情報の設定

[入力形式] **bridge lan 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。

[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。

8.2.2 ラーニング情報の削除

[入力形式] **bridge lan 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。

8.2.3 LAN 側でのブリッジのフィルタリングの設定

[入力形式] **bridge lan 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。

[デフォルト値] **clear**

8.3 PP 側相手毎のブリッジの設定

8.3.1 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。

8.3.2 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。

8.3.3 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**

9 PPP の設定

9.1 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 *isdn1*、*isdn2* の両方を用い、どちらかと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。

[ノート] **RT200i** 及び **RT140i** の場合は、*isdn1*, *isdn2* として複数の ISDN 番号が設定可能。

9.2 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**

9.3 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**

9.4 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。

9.5 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。

9.6 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。

9.7 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**

9.8 LCP 関連の設定

9.8.1 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**

9.8.2 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**

9.8.3 Maximum Receive Unit オプション使用の設定

[入力形式] **ppp lcp mru** *mru*

[パラメータ]
- *mru*
  - **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 Maximum Receive Unit 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。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。

[デフォルト値] **on**

9.8.4 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**

9.8.5 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

9.8.6 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* ... 再送回数 (1..10)

[説明] 選択されている相手について [PPP,LCP] の terminate-request の再送回数を設定する。

[デフォルト値] 2

9.8.7 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* ... 再送回数 (1..10)

[説明] 選択されている相手について [PPP,LCP] の configure-request の再送回数を設定する。

[デフォルト値] 10

9.8.8 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* ... [PPP,LCP] の configure-nak を送る回数 (1..10)

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

[デフォルト値] 10

9.8.9 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**

9.8.10 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**

9.8.11 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] $interval = 30$
$count = 6$

9.8.12 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**

9.9 PAP 関連の設定

9.9.1 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

9.9.2 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 の再送回数を設定する。

[デフォルト値] 2

9.10 CHAP 関連の設定

9.10.1 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

9.10.2 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 の再送回数を設定する。

[デフォルト値] 2

9.11 IPCP 関連の設定

9.11.1 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**

9.11.2 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] 6.3.1自分の PP 側 IP アドレス設定コマンド、6.3.2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**

9.11.3 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

9.11.4 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* ... 再送回数 (1..10)

[説明] 選択されている相手について [PPP,IPCP] の terminate-request の再送回数を設定する。

[デフォルト値] 2

9.11.5 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* ... 再送回数 (1..10)

[説明] 選択されている相手について [PPP,IPCP] の configure-request の再送回数を設定する。

[デフォルト値] 10

9.11.6 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 を送る回数を設定する。

[デフォルト値] 10

9.11.7 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 95 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**

9.11.8 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**

9.12 IPXCP 関連の設定

9.12.1 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

9.12.2 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* ... 再送回数 (1..10)

[説明] 選択されている相手について [PPP,IPXCP] の terminate-request の再送回数を設定する。

[デフォルト値] 2

9.12.3 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* ... 再送回数 (1..10)

[説明] 選択されている相手について [PPP,IPXCP] の configure-request の再送回数を設定する。

[デフォルト値] 10

9.12.4 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 を送る回数を設定する。

[デフォルト値] 10

9.13 BCP 関連の設定

9.13.1 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**

9.13.2 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**

9.13.3 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

9.13.4 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* ... 再送回数 (1..10)

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

[デフォルト値] 2

9.13.5 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* ... 再送回数 (1..10)

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

[デフォルト値] 10

9.13.6 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 を送る回数を設定する。

[デフォルト値] 10

9.13.7 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

9.13.8 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

9.14 CCP 関連の設定

9.14.1 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-predictor** ... 圧縮タイプをまず Stac_LZS でネゴシエーションし、うまくいかない場合には predictor にフォールバックする
  - **predictor** ... predictor で圧縮する
  - **cpredictor** ... predictor で圧縮する (接続相手が Cisco ルータの場合)
  - **stac** ... Stac_LZS で圧縮する
  - **cstac** ... Stac_LZS で圧縮する (接続相手が Cisco ルータの場合)
  - **none** ... 圧縮しない

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

[ノート] **predictor** に設定していても相手に拒否された時は圧縮しない。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 predictor を使用する場合には、必ず **cpredictor** を選択し、それ以外の相手との間で predictor を使用する場合には **predictor** を選択する。**stac**、**cstac** も同様である。

[デフォルト値] **stac-predictor**

9.14.2 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

9.14.3 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* ... 再送回数 (1..10)

[説明] 選択されている相手について [PPP,CCP] の terminate-request の再送回数を設定する。

[デフォルト値] 2

9.14.4 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* ... 再送回数 (1..10)

[説明] 選択されている相手について [PPP,CCP] の configure-request の再送回数を設定する。

[デフォルト値] 10

9.14.5 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 を送る回数を設定する。

[デフォルト値] 10

9.15 MP 関連の設定

9.15.1 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**

9.15.2 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**

9.15.3 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

9.15.4 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。
最大 2B チャネルの **RT102i** ではリンク数は 2 までとなる。

[デフォルト値] 2

9.15.5 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

9.15.6 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

9.15.7 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。

[デフォルト値] **on**

9.16 BACP 関連の設定

9.16.1 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

9.16.2 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* ... 再送回数 (1..10)

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

[デフォルト値] 2

9.16.3 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* ... 再送回数 (1..10)

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

[デフォルト値] 10

9.16.4 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

9.16.5 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

9.16.6 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

10 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。

10.1 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,RT140i, RT102i
server... RT80i

[6] Dynamic Host Configuration Protocol; RFC1541

10.2 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
maxexpire *time* = 72

10.3 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。

10.4 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。

10.5 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。

10.6 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。

10.7 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筈である。**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**

10.8 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

11 SNMP の設定

11.1 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**

11.2 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**

11.3 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**

11.4 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**

11.5 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

11.6 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 リモートルータの管理者を表す 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

11.7 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

11.8 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**

11.9 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**

12 ICMP の設定

12.1 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**

12.2 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**

12.3 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**

12.4 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**

12.5 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**

12.6 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**

12.7 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**

12.8 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**

13 RADIUS の設定

13.1 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。

13.2 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。

13.3 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

13.4 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**

13.5 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**

14 NAT の設定

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。

14.1 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**

14.2 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

14.3 IP Masquerade 使用時に rlogin と rcp 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 と rcp を許可するか否かを設定する。

[ノート] **nat masquerade rlogin on** にすると、rlogin 及び rcp 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**

14.4 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。

[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
```

14.5 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。

14.6 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**

14.7 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**

14.8 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

15 DNS リゾルバの設定

15.1 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**

15.2 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。

15.3 SYSLOG 出力で DNS による名前解決をするか否かの設定

[入力形式] **dns syslog resolv** *resolv*

[パラメータ]
- *resolv*
  - **on** ... 名前解決を行う
  - **off** ... 名前解決を行わない

[説明] SYSLOG に出力されるメッセージに含まれる IP アドレスのうちの一部を、DNS により名前に変換して出力するか否かを設定する。

[デフォルト値] **off**

15.4 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

16 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 **RT80i** 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。**RT80i** 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。

アナログ通信機能は、**RT80i** 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一切使用できません。また、アナログ電話機を接続しても無音のままになります。

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。

RT80i 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。

RT80i 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コールウェイティングをサポートします。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、擬似コールウェイティング機能はそれと同様な機能を **RT80i** 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コールウェイティングの操作は、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。

RT80i 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。

16.1 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
- *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。

16.2 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
- *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**

16.3 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
- *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] **on**

16.4 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
- *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**

16.5 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
- *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] **off**

16.6 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
- *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**

16.7 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
- *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。

16.8 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
- *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。

16.9 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
- *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**

16.10 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
- *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] **off**

16.11 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
- *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。

[デフォルト値] **on**

16.12 優先着信機能の設定

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

[パラメータ]
- *port* ... アナログポート
  - *1* ... TEL1 ポート
  - *2* ... TEL2 ポート
  - **off** ... 平等に呼び出す

[説明] TEL1, TEL2 ポートの両方が着信可能状態の場合、どちらを優先的に呼び出すかを設定する。

[ノート] TEL1 ポートが優先着信の設定になっていて通信中の場合、更に着信があると TEL2 ポートが呼び出される。

[デフォルト値] **off**

16.13 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
- *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。

16.14 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
- *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。

16.15 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
- *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

16.16 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
- *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

16.17 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
- *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

16.18 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
- *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**

16.19 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** *func1 [func2] ... [func5]*
2. **analog supplementary-service pseudo** *pseudo_func*
3. **analog supplementary-service clear**

[パラメータ]
- *func1, func2, func3, func4, func5*
  - **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
- **pseudo** ... 擬似機能使用を示すキーワード
- *pseudo_func*
  - **call-waiting** ... 擬似コールウェイティング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**

16.20 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*

[パラメータ]
- *port* ... アナログポート
  - **1** ... TEL1 ポート
  - **2** ... TEL2 ポート
- *isdn_number* ... ISDN 番号

[説明] 着信転送先アドレスを登録する。

[ノート] サブアドレスを指定することはできない。

16.21 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
- *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、着信転送により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 **RT80i** 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。

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

16.22 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
- *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**

16.23 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
- *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**

16.24 送話 PAD の設定

[入力形式] **analog pad send** *pad*

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

[説明] 送話 PAD を設定する。

[デフォルト値] **off**

16.25 受話 PAD の設定

[入力形式] **analog pad receive** *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] 受話 PAD を設定する。

[デフォルト値] **off**

17 操作

17.1 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。

17.2 設定に関する操作

17.2.1 管理ユーザへの移行

[入力形式] **administrator**

[パラメータ] なし

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

17.2.2 設定内容の保存

[入力形式] **save**

[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。

17.2.3 終了

[入力形式] 1. **quit**
2. **quit 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。

17.2.4 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戻す。

[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。

17.2.5 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。

17.2.6 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。

17.2.7 遠隔地のルータの設定

[入力形式]
1. **remote setup** *isdn_number*/*sub_address* [**dlci**=*dlci_num*]
2. **remote setup** *isdn_number* [**dlci**=*dlci_num*]
3. **remote setup** *bri isdn_number*/*sub_address* [**dlci**=*dlci_num*] ... RT200i, RT140i
4. **remote setup** *bri isdn_number* [**dlci**=*dlci_num*] ... RT200i, RT140i

[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

[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。

17.2.8 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**

17.3 動的情報のクリア操作

17.3.1 ARP テーブルのクリア

[入力形式] **clear arp**

[パラメータ] なし

[説明] ARP テーブルをクリアする。

17.3.2 IP の動的経路情報のクリア

[入力形式] **clear ip dynamic routing**

[パラメータ] なし

[説明] 動的に設定された IP の経路情報をクリアする。

17.3.3 IPX の動的経路情報のクリア

[入力形式] **clear ipx dynamic routing**

[パラメータ] なし

[説明] 動的に設定された IPX の経路情報をクリアする。

17.3.4 IPX の動的 SAP 情報のクリア

[入力形式] **clear ipx dynamic sap**

[パラメータ] なし

[説明] IPX SAP テーブル中、動的に得られた SAP 情報をクリアする。

17.3.5 ブリッジのラーニング情報のクリア

[入力形式] **clear bridge learning**

[パラメータ] なし

[説明] 動的に受け取ったブリッジのラーニング情報をすべて消去する。

[ノート] **bridge 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。

17.3.6 ログのクリア

[入力形式] **clear log**

[パラメータ] なし

[説明] ログをクリアする。

17.3.7 アカウントのクリア

[入力形式] **clear account**

[パラメータ] なし

[説明] アカウントをクリアする。

17.3.8 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。

17.3.9 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。

17.3.10 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。

17.3.11 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。

17.4 スケジュール

17.4.1 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
- *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, pp select, ppp chap common secret, ppp chap individual secret, ppp pap add common userid, ppp pap add individual userid, ppp pap common password, ppp pap delete common userid, ppp pap delete individual userid, ppp pap individual password, ppp pap send userid, quit, remote setup, restart, save, schedule** で始まるコマンド, **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
```

17.4.2 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。

17.4.3 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。

17.5 その他の操作

17.5.1 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。

17.5.2 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。

17.5.3 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。

17.5.4 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。

17.5.5 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。

17.5.6 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。

17.5.7 traceroute

[入力形式] **traceroute** *host*

[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。

17.5.8 リモートホストによる時計の設定

[入力形式] **rdate** *host*

[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

[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。

17.5.9 NTP による時計の設定

[入力形式] **ntpdate** *ntp_server*

[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

[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。

17.5.10 telnet

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

[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
- *port* ... 使用するポート番号 (ニーモニックが使用可能)
- *abort* ... 強制終了のためのアボートキーの指定 (10 進数の ASCII)

[説明] TELNET クライアントを実行する。

[ノート] *port* パラメータを省略した時には 23(TELNET) が、*abort* パラメータを省略した時には 29(^]) となる。

18 設定の表示

18.1 機器設定の表示

18.1.1 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, RT140i

18.1.2 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

18.1.3 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

18.1.4 PP 毎の送信キューの表示

[入力形式] **show pp queue** *[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, RT140i
- pp queue length

[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。

18.1.5 すべての設定内容の表示

[入力形式] **show 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。

18.1.6 PP 毎の設定内容の表示

[入力形式] **show pp config** *[peer_number]* ... RT200i, RT140i

[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
- pp queue length

[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。

18.2 相手先一覧の表示

18.2.1 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。

18.3 ISDN 関連の表示

18.3.1 自分側設定の表示

[入力形式] 1. **show isdn local**

2. **show isdn local** *bri* ... RT200i, RT140i

[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

18.3.2 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, RT140i
- isdn remote address
- isdn bulk
- isdn remote call order ... RT200i, RT140i

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, RT140i
- 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。

18.4 フレームリレー関連の表示

18.4.1 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。

18.4.2 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。

18.5 IP 関連の表示

18.5.1 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。

18.5.2 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。

18.5.3 LAN 側 IP 設定の表示

[入力形式] **show ip lan**

[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

18.5.4 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。

18.6 IPX 関連の表示

18.6.1 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。

18.6.2 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。

18.6.3 LAN 側 IPX 設定の表示

[入力形式] **show ipx lan**

[パラメータ] なし

[説明] 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

18.6.4 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。

18.7 ブリッジ関連の表示

18.7.1 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。

18.7.2 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。

18.7.3 LAN 側ブリッジ設定の表示

[入力形式] **show bridge lan**

[パラメータ] なし

[説明] 以下の項目が表示される。

- bridge use
- bridge forwarding
- bridge learning
- bridge learning expire
- bridge lan filter

18.7.4 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。

18.8 PPP の設定の表示

18.8.1 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。

18.8.2 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。

18.8.3 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。

18.8.4 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。

18.8.5 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。

18.8.6 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。

18.8.7 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。

18.8.8 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。

18.8.9 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。

18.8.10 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。

18.8.11 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。

18.9 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

18.10 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)

18.11 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

18.12 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

18.13 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

18.14 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

[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。

18.15 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。

18.16 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

[説明] アナログ関係の設定を表示する。

19 状態の表示

19.1 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。

19.2 LAN 側の状態の表示

[入力形式] **show status lan**

[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

19.3 PP 側の状態の表示

[入力形式] 1. **show status bri**

2. **show status bri** *[bri]* ... RT200i, RT140i

[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

19.4 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。

19.5 IP の経路情報テーブルの表示

[入力形式] **show ip route** *[destination]*

[パラメータ]
- *destination* ... 相手先 IP アドレス
- 省略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。

19.6 IPX の経路情報テーブルの表示

[入力形式] **show ipx route**

[パラメータ] なし

[説明] IPX の経路情報テーブルを表示する。

19.7 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。
フレームリレーの場合は DLCI の値が表示される。

19.8 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。

19.9 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。

19.10 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。

[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。

19.11 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

[説明] アナログ関係の状態を表示する。

20 ロギング

20.1 ログの表示

[入力形式] **show 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。

20.2 アカウントの表示

[入力形式] 1. **show account**

2. **show account** *bri* ... RT200i, RT140i

[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

20.3 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。

20.4 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

[説明] アナログ関係のアカウントを表示する。